Lecture Notes in Networks and Systems 89

G. Ranganathan
Joy Chen
Álvaro Rocha *Editors*

Inventive Communication and Computational Technologies

Proceedings of ICICCT 2019

Springer

Lecture Notes in Networks and Systems

Volume 89

The series “Lecture Notes in Networks and Systems” publishes the latest developments in Networks and Systems—quickly, informally and with high quality. Original research reported in proceedings and post-proceedings represents the core of LNNS.

Volumes published in LNNS embrace all aspects and subfields of, as well as new challenges in, Networks and Systems.

The series contains proceedings and edited volumes in systems and networks, spanning the areas of Cyber-Physical Systems, Autonomous Systems, Sensor Networks, Control Systems, Energy Systems, Automotive Systems, Biological Systems, Vehicular Networking and Connected Vehicles, Aerospace Systems, Automation, Manufacturing, Smart Grids, Nonlinear Systems, Power Systems, Robotics, Social Systems, Economic Systems and other. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution and exposure which enable both a wide and rapid dissemination of research output.

The series covers the theory, applications, and perspectives on the state of the art and future developments relevant to systems and networks, decision making, control, complex processes and related areas, as embedded in the fields of interdisciplinary and applied sciences, engineering, computer science, physics, economics, social, and life sciences, as well as the paradigms and methodologies behind them.

**** Indexing: The books of this series are submitted to ISI Proceedings, SCOPUS, Google Scholar and Springerlink ****

More information about this series at http://www.springer.com/series/15179

G. Ranganathan · Joy Chen · Álvaro Rocha
Editors

Inventive Communication and Computational Technologies

Proceedings of ICICCT 2019

Springer

Editors
G. Ranganathan
Electronics and Communication Engineering
Gnanamani College of Technology
Namakkal, Tamil Nadu, India

Joy Chen
Department of Electrical Engineering
Dayeh University
Chang-Hwa, Taiwan

Álvaro Rocha
University of Coimbra
Rio Tinto, Portugal

ISSN 2367-3370 ISSN 2367-3389 (electronic)
Lecture Notes in Networks and Systems
ISBN 978-981-15-0145-6 ISBN 978-981-15-0146-3 (eBook)
https://doi.org/10.1007/978-981-15-0146-3

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

We dedicated to all the participants of the conference ICICCT 2019

Foreword

We welcome you to the 2019 International Conference on *Inventive Communication and Computational Technologies* (ICICCT 2019) held on April 29–30, 2019, at Gnanamani College of Technology, Namakkal, Tamil Nadu. ICICCT 2019 provides a highly competitive forum for reporting the latest developments in the research and application of communication and computational technologies. We are pleased to present the proceedings of the conference as its published record.

The conference particularly encouraged the interaction of research students and developing academics with the more established academic community in an informal setting to present and to discuss new and current work. Their contributions helped to make the conference as outstanding as it has been. The papers contributed the most recent scientific knowledge known in the fields of modern communication systems which include informatics, data communication and computer networking, wireless communication, electronics, software engineering, machine learning and optimization, VLSI design and automation, networking, computing systems, social networks, Internet of things, cloud and big data.

We hope that this program will further stimulate research in advanced electronics and communication technologies, artificial intelligence and capsule networks, data communication and computer networking and communicating things networks. We feel honored and privileged to serve the best recent developments in all the areas of communication technologies to you through this exciting program.

We thank all the authors and participants for their contributions.

Namakkal, India

Dr. G. Ranganathan
Conference Chair
ICICCT 2019

Preface

The 2019 International Conference on *Inventive Communication and Computational Technologies* (ICICCT 2019) was held on April 29–30, 2019, at Gnanamani College of Technology, Namakkal, India. ICICCT 2019 aims to cover the recent advancement and trends in the area of communication and computational technologies to facilitate knowledge sharing and networking interactions on emerging trends and new challenges.

ICICCT 2019 tends to collect the latest research results and applications on data communication and computer networking, software engineering, wireless communication, VLSI design and automation, networking, Internet of things, cloud and big data. It includes a selection of 136 papers from 430 papers submitted to the conference from universities and industries all over the world. All of the accepted papers were subjected to strict peer-reviewing by 2–4 expert referees. The papers have been selected for this volume because of quality and the relevance to the conference.

We would like to express our sincere appreciation to all the authors for their contributions to this book. We would like to extend our thanks to all the referees for their constructive comments on all papers, especially we would like to thank the Organizing Committee for their hard work. Finally, we would like to thank the Springer publications for producing this volume.

Namakkal, India

Dr. G. Ranganathan
Conference Chair
ICICCT 2019

Acknowledgements

We would like to acknowledge the contribution made to the organization by its many volunteers. Members contribute their time, energy and knowledge at a local, regional and international level.

We also thank all the chair persons and conference committee members for their support.

Contents

Editors and Contributors

About the Editors

Dr. G. Ranganathan has been a Professor at Gnanamani College of Technology since 2017. Previously, he has worked at Ranganathan Engineering College and Jayalakshmi Institute of Technology. He has also worked as a Professor at RVS Technical Campus, Karpagam College of Engineering and P.R. Engineering College. He completed his Ph.D. and M.E. at the Information and Communication Engineering Department, Anna University. His areas of interest include biomedical signal processing, neural networks, fuzzy logic, networking and VLSI signal processing. He has published five books and numerous research papers in international journals.

Dr. Joy Chen received his B.Sc. in Electronics Engineering from the National Taiwan Technical University, Taipei, Taiwan, and his M.Sc. in Electrical Engineering from Dayeh University, Changhua, Taiwan, in 1985 and 1995, respectively. He completed his Ph.D. in Electrical Engineering at the National Defense University, Tao-Yuan, Taiwan, in 2001 and is currently a Full Professor at the Department of Communication Engineering, Dayeh University. Prior to joining Dayeh, he worked at the Control Data Company (Taiwan branch) as a Technical Manager from 1985 to 1996. His research interests include wireless communications, MIMO systems, OFDM systems, and wireless sensor networks. Dr. Joy I.-Z. Chen has published numerous SCI/EI journal papers and holds several patents in Taiwan.

Dr. Álvaro Rocha holds a Habilitation (postdoc) in Information Science, Ph.D. in Information Systems and Technologies, and M.Sc. in Information Management. He is currently a Professor of Information Systems and Software Engineering at the University of Coimbra, President of AISTI (the Iberian Association for Information Systems and Technologies), and Chair of IEEE SMC Portugal Section Society Chapter. He served as Vice-Chair of Experts for the European Commission's Horizon 2020 Programme, and as an expert at the Italian Ministry of Education, University and Research. His main research interests are information systems planning and management, maturity models, information system quality, online service quality, intelligent information systems, software engineering, e-government, e-health, and IT in education.

Contributors

Ahmed Raad Abbas Department of Information Technology Development (IT), University Institute of Engineering and Technology (UIET), Punjab University, Chandigarh, India

S. Abirami Department of Electronics and Instrumentation Engineering, Annamalai University, Chidambaram, India

Kinjal Adhvaryu Computer Engineering Department, Sankersinh Vaghela Bapu Institute of Technology, Gandhinagar, Gujarat, India

Shahid Afridi Department of Computer Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

Vimal Agarwal Apex Institute of Engineering & Technology, Jaipur, India

Harshit Agarwal Sarvajanik College of Engineering and Technology, Surat, India

Rekib Uddin Ahmed National Institute of Technology Meghalaya, Shillong, India

S. Ajay Kumar Department of Electronics and Communication Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India

B. Ajay Raj Department of Electronics and Communication Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India

Aparna Ajith Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, Kerala, India

Suthapalli Akhil Sri Harsha School of Electrical and Electronics Engineering, SASTRA Deemed to Be University, Thanjavur, India

Abdullah Al Noman Department of Computer Science and Engineering, International Islamic University Chittagong, Chittagong, Bangladesh

Mohammed Shamsul Alam Department of Computer Science and Engineering, International Islamic University Chittagong, Chittagong, Bangladesh

Phanindra Kumar Allada Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

Ali Jameel Al-Mousawi Information Technology Regulation Directory—Communication and Media Commission of Iraq (CMC), Baghdad, Iraq

M. Ameena Banu Department of Electronics and Communication Engineering, Sethu Institute of Technology, Pulloor, Virudhunagar District, Tamilnadu, India

S. D. Amrutha Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

R. Anand Department of Information Technology, KCG College of Technology, Chennai, India

R. Ani Department of Computer Science and Applications, Amrita Vishwa Vidyapeetham, Kollam, India

B. S. Anisha Information Science and Engineering, R.V. College of Engineering, Bengaluru, India

P. Anitha Dr. N.G.P. Institute of Technology, Coimbatore, India

T. Anjali Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

K. S. Anusha Department of Electronics and Communication Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India

Kompalli Anusha Branch of WMC, G. Narayanamma Institute of Technology and Science, JNTUH, Hyderabad, India

T. S. Aparna Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

L. Arockiam Department of Computer Science, St. Joseph's College, Trichy, India

M. Arulaalan CK College of Engineering & Technology, Cuddalore, India

V. Arulkumar Department of Information Technology, SSN College of Engineering, Chennai, India

P. Aruna Department of Software Engineering, Periyar Maniammai Institute of Science and Technology, Thanjavur, India

Vinit Asher Sardar Patel Institute of Technology, Mumbai, India

N. Ashokkumar Department of Electronics and Communication Engineering, Centre for VLSI and Embedded Systems, Sree Vidyanikethan Engineering College, Tirupati, India

Sigamani Ashokkumar Department of Computer Science and Engineering, Saveetha School of Engineering, SIMATS, Chennai, India

A. V. Aswin Muthoot Institute of Technology and Science, Ernakulam, India

H. S. Avani Department of Computer Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

Khairul Islam Azam Department of Computer Science and Engineering, International Islamic University Chittagong, Chittagong, Bangladesh

S. Balaji Department of Electronics and Communications Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

Vignesh Balakrishnan Department of Information Technology, KCG College of Technology, Chennai, India

A. Balakumar K. Ramakrishnan College of Engineering, Trichy, India

Ananthakrishnan BalaSundaram Department of Computer Science and Engineering, Saveetha School of Engineering, SIMATS, Chennai, India

R. M. Banakar BVB College of Engineering and Technology, Hubli, India

Amit Barve Ramrao Adik Institute of Technology, Navi Mumbai, India

Sujit Kumar Basak Université du Québec à Montréal (UQÀM), Montreal, Canada

K. Y. Basil Muthoot Institute of Technology and Science, Ernakulam, India

Vanshita R. Baweja Computer Science, PEC University of Technology, Chandigarh, India

Sushant Bawiskar Department of Embedded Technology, VIT, Vellore, India

Chaithra Bekal Department of Computer Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

Paul Bélanger Université du Québec à Montréal (UQÀM), Montreal, Canada

Sudhanshu Bhagat Information Technology, Terna Engineering College, Navi Mumbai, India

R. Bhairavi Department of Electronics and Communication Engineering, Pondicherry Engineering College, Puducherry, India

N. Bhalaji Department of Information Technology, SSN College of Engineering, Chennai, India

Rajiv R. Bhandari Department of Computer Science Engineering, Koneru Lakshmaiah Education Foundation Green Fields, Guntur District, Vaddeswaram, Andhra Pradesh, India

Rekha Bhandarkar Department of ECE, N.M.A.M.I.T, Nitte, India

Madiraju Akshay Bharadwaj Department of Electronics and Communication Engineering, Amrita School of Engineering, Kollam, Kerala, India

S. Bharath Departtment of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

N. Bhaskar Department of Information Technology, KCG College of Technology, Chennai, India

Rajesh Bhatia Computer Science, PEC University of Technology, Chandigarh, India

Prasenjit Bhavathankar Sardar Patel Institute of Technology, Mumbai, India

Sujata Bhavikatti Tontadarya College of Engineering, Gadag, India

K. Bhuvana Department of Computer Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

M. Bhuvaneshwar Department of Electronics and Communication Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India

Bhawani Sankar Biswal DST-FIST Bioinformatics Laboratory, IIIT Bhubaneswar, Bhubaneswar, India

Ranjit Biswas Department of Computer Science and Engineering, Jamia Hamdard, New Delhi, India

Tanmay Borade Ramrao Adik Institute of Technology, Navi Mumbai, India

M. Bowya Department of ECE, Vivekanandha College of Engineering for Women, Namakkal, India

P. S. Chaithanya School of Computing, Centre for Information Super Highway (CISH), SASTRA Deemed to be University, Thanjavur, Tamil Nadu, India

Ruthvik Chanda Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

K. Chandrasekaran Department of Computer Science and Engineering, National Institute of Technology Karnataka, Surathkal, Mangalore, India

G. Charles Babu Department of CSE, Malla Reddy Engineering College (Autonomous), Secunderabad, Telangana, India

Swati Chavan IT Department, Terna Engineering College, Mumbai University, Navi Mumbai, Maharashtra, India

Amruta Chavan Department of IT Engineering, RAIT, Nerul, Navi Mumbai, India

Keerthana Chigateri Department of CSE, N.M.A.M.I.T, Nitte, India

A. Christy Jeba Malar Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India

Dhananjay Dakhane Ramrao Adik Institute of Technology, Navi Mumbai, India

Pooja Dalvi IT Department, Terna Engineering College, Mumbai University, Navi Mumbai, Maharashtra, India

Neelam Dayal Department of Computer Science & Engineering, Centre for Advanced Studies, AKTU, Lucknow, India

Tribid Debbarma Department of Computer Science and Engineering, National Institute of Technology Agartala, Agartala, India

S. Deeksha Department of Computer Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

M. Deepthi Department of Computer Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

Smita Deshmukh IT Department, Terna Engineering College, Mumbai University, Navi Mumbai, Maharashtra, India

Santhosh L. Deshpande Department of Post Graduate Studies, Visvesvaraya Technological University (VTU), Belgaum, Karnataka, India

M. Deva Priya Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India

R. Devi Priya Department of Information Technology, Kongu Engineering College, Erode, India

K. Dhanya K. Ramakrishnan College of Engineering, Trichy, India

E. Dhivyaprabha Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India

J. Dhoulath Beegum Department of ECE, TKM College of Engineering, Kollam, Kerala, India

Ashwini Dhummal Department of Computer Science and Engineering, NMAMIT, Nitte, Karnataka, India

C. D. Divya Department of Computer Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

Nilima Dongre Department of IT Engineering, RAIT, Nerul, Navi Mumbai, India

Prutha Edwankar Department of Mechatronics Engineering, MPSTME, NMIMS University, Mumbai, India

Vijaya Eligar KLE Technological University, Hubballi, India

Sanjay Eligar BVB College of Engineering and Technology, Hubli, India

B. Maragatha Eswari Department of Electronics and Communication Engineering, Amrita School of Engineering, Kollam, Kerala, India

R. Eswari National Institute of Technology, Tiruchirappalli, India

C. Suganthi Evangeline Karunya Institute of Technology and Sciences, Coimbatore, India;
Vellore Institute of Technology, Vellore, India

R. Ezhilarasie School of Computing, SASTRA Deemed University, Thanjavur, India

K. Ben Franklin Department of Electronics and Communication Engineering, SRMIST, Kattankulathur, Chennai, India

Roopali Garg Associate Professor, UIET, Panjab University, Chandigarh, India

Mrudula Geddam Department of Electronics and Telecommunication Engineering, Fr. C.R.I.T, Vashi, Navi, Mumbai, India

Ravi Teja Geesala Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

K. Geetha SASTRA Deemed to be University, Thanjavur, India

A. George Department of Mathematics, Periyar Maniammai Institute of Science and Technology, Thanjavur, India

E. George Dharma Prakash Raj Bharathidasan University, Tiruchirappalli, Tamilnadu, India

Jatin Gharat Ramrao Adik Institute of Technology, Navi Mumbai, India

Tushar Ghorpade Ramrao Adik Institute of Technology, Navi Mumbai, India

Md. Golam Rabiul Alam Department of Computer Science and Engineering, BRAC University, Dhaka, Bangladesh

Vamsi Gontu Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

Nivetha Gopalakrishnan Department of Electronics and Communication Engineering, University College of Engineering Panruti, Panruti, Tamilnadu, India

Vinodhini Gopalakrishnan Department of Computer Science Engineering, Annamalai University, Chidambaram, Tamilnadu, India

Priyanka Gotter Computer Engineering and Technology, Guru Nanak Dev University, Amritsar, Punjab, India

B. N. Gowrishankar Department of Information Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

Aman Gupta Department of C.S.E, Guru Ghasidas Central University, Bilaspur, India

Saurabh Gupta Department of C.S.E, Guru Ghasidas Central University, Bilaspur, India

Sorjeeta Gupta Department of Information Technology, KCG College of Technology, Chennai, India

V. J. Haran Muthoot Institute of Technology and Science, Kochi, India

D. Harini SASTRA Deemed to be University, Thanjavur, India

A. Harish Information Science and Engineering, R.V. College of Engineering, Bengaluru, India

Abhilash P. Hasankar Department of E&CE, SDMCET, Dharwad, Karnataka, India

Haider K. Hoomod Computer Science Department, College of Education—Mustansiriyah University, Baghdad, Iraq

Mohammad Emdad Hossain Department of Business Administration, International Islamic University Chittagong, Chittagong, Bangladesh

B. J. Hubert Shanthan Department of Computer Science, St. Joseph's College, Trichy, India

Shivaraj Hublikar KLE Technological University, Hubballi, India

V. Indu Department of Electrical and Electronics Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

Akshaykumar Jadhav IT Department, Terna Engineering College, Mumbai University, Navi Mumbai, Maharashtra, India

Dipti Jadhav Department of IT Engineering, RAIT, Nerul, Navi Mumbai, India

Sandeep Jadhav KPIT Technologies Limited, Pune, Maharashtra, India

Ashish Jain Apex Institute of Engineering & Technology, Jaipur, India

Bhumika Jain Department of Computer Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

Aashish Jaisimha Information Science and Engineering, R.V. College of Engineering, Bengaluru, India

B. Janet National Institute of Technology, Tiruchirappalli, India

Gaurav Jariwala Sarvajanik College of Engineering and Technology, Surat, India

N. Jayapandian Department of Computer Science and Engineering, CHRIST (Deemed to Be University), Bangalore, India

C. Jeyalakshmi K. Ramakrishnan College of Engineering, Trichy, India

Saksham Jhawar Information Science and Engineering, R.V. College of Engineering, Bengaluru, India

Priyanka Jondhale Department of Electronics and Telecommunication Engineering, Fr. C.R.I.T, Vashi, Navi, Mumbai, India

Christy James Jose Government Engineering College, Barton Hill, Thiruvananthapuram, Kerala, India

Deepa Jose Electronics and Communication, KCG College of Technology, Chennai, India

K. Joseph Abraham Sundar Computer Vision & Soft Computing Lab, School of Computing, SASTRA Deemed University, Thanjavur, India

Bharti Joshi Ramrao Adik Institute of Technology, Navi Mumbai, India

K. Jyothsna Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

Poonam Kadam Department of Electronics and Telecommunication, Dwarkadas J. Sanghvi College of Engineering, Mumbai, India

Subhas Kadam Department of Computer Science and Engineering, NMAMIT, Nitte, Karnataka, India

Arun Kakhandki KLSs VDRIT, Haliyal, India

Md. Kalim Amzad Chy Department of Computer Science and Engineering, International Islamic University Chittagong, Chittagong, Bangladesh

G. Kanagaraj Kumaraguru College of Technology, Coimbatore, India

Kamalanathan Kandasamy Amrita Center for Cyber Security Systems & Networks, Amrita Vishwa Vidyapeetham, Amrita University, Kollam, Kerala, India

J. Kanimozhi Department of IT, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

A. Kannammal Department of Computer Science and Engineering, Jayam College of Engineering and Technology, Dharmapuri, TamilNadu, India

V. Karthick Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India

K. Karthika Department of Information Technology, Adhiyamaan College of Engineering, Hosur, India

A. Karthikeyan School of Electronics Engg, VIT, Vellore, Tamil Nadu, India; Department of Embedded System Technologies, VIT, Vellore, India

B. Karthikeyan Computer Vision & Soft Computing Lab, School of Computing, SASTRA Deemed University, Thanjavur, India

V. Karthikeyan Department of ECE, Vivekanandha College of Engineering for Women, Namakkal, India

Jaspreet Kaur Ramrao Adik Institute of Technology, Navi Mumbai, India

Kiranbir Kaur GNDU (Main Campus), Amritsar, India;
Department of Computer Engineering and Technology, Guru Nanak Dev University, Amritsar, Punjab, India

Mandeep Kau Department of Information Technology Development (IT), University Institute of Engineering and Technology (UIET), Punjab University, Chandigarh, India

Manjot Kaur GNDU (Main Campus), Amritsar, India

Preetjot Kaur PhD Research Scholar, UIET, Panjab University, Chandigarh, India

Tanveer Kaur Department of Computer Engineering and Technology, Guru Nanak Dev University, Amritsar, Punjab, India

R. Kavipriya K. Ramakrishnan College of Engineering, Tiruchirappalli, India

B. Keerthana Department of IT, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

Vaishali Khairnar Information Technology, Terna Engineering College, Navi Mumbai, India

Salman Khan Information Science and Engineering, R.V. College of Engineering, Bengaluru, India

Shahidul Islam Khan Department of Computer Science and Engineering, International Islamic University Chittagong, Chittagong, Bangladesh

Andrew Kidd Teesside University, Middlesbrough, UK

Akeem T. L. King ISPA Technology, Tampa, FL, USA

Steward Kirubakaran Department of Computer Science and Engineering, KCG College of Technology, Karapakkam, Chennai, India

Likhesh Kolhe Information Technology, Terna Engineering College, Navi Mumbai, India

K. S. Ananth Krishna Muthoot Institute of Technology and Science, Kochi, India

Arya Krishnan Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, Kerala, India

Venkatalakshmi Krishnan Department of Electronics and Communication Engineering, University College of Engineering Tindivanam, Tindivanam, Tamilnadu, India

P. Anand Krisshna Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

Vidya Kubde Department of Information Technology, Datta Meghe College of Engineering, Navi Mumbai, India

Ankit Kumar Information Technology, Terna Engineering College, Navi Mumbai, India

Manish Kumar Computer Science, PEC University of Technology, Chandigarh, India

R. Kumar Department of Electronics and Communication Engineering, SRMIST, Kattankulathur, Chennai, India

Rakesh Kumar Department of Computer Science and Engineering (CSE), M.M. M. University of Technology, Gorakhpur, U.P., India

Vinoth Babu Kumaravelu Vellore Institute of Technology, Vellore, India

Anshu Kumari Department of Computer Science & Engineering, Guru Ghasidas University, Bilaspur, India

Ashwini S. Kunte Department of Electronics and Telecommunication, Thadomal Shahani Engineering College, Bandra, Mumbai, India

Bineeth Kuriakose Muthoot Institute of Technology and Science, Ernakulam, India;
Oslo Metropolitan University, Oslo, Norway

K. N. Lakshmi Department of Information Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

Alan Lansy Muthoot Institute of Technology and Science, Kochi, India

Vignesh Loganathan Department of Information Technology, KCG College of Technology, Chennai, India

R. Mary Lourde Department of EEE, BITS Pilani Dubai Campus, Dubai, UAE

Revathi Mahadevan Ramrao Adik Institute of Technology, Navi Mumbai, Maharashtra, India

R. Mahaveerakannan Information Technology St. Peter's University, Chennai, India

K. Mahendran CK College of Engineering & Technology, Cuddalore, India

M. Maheswari K. Ramakrishnan College of Engineering, Tiruchirappalli, India

G. Manikannan CK College of Engineering & Technology, Cuddalore, India

B. R. Manju Department of Mathematics, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

R. Manjula PSGR Krishnammal College for Women, Coimbatore, India

Nilesh Marathe Department of IT Engineering, RAIT, Nerul, Navi Mumbai, India

R. Mary Lourde Department of EEE, BITS Pilani, Dubai Campus, Dubai, UAE

Abdul Kadar Muhammad Masum Department of Computer Science and Engineering, International Islamic University Chittagong, Chittagong, Bangladesh

M. Meera Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

Rajesh Kannan Megalingam Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

B. U. Meghana Department of Information Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

Natarajan Meghanathan Jackson State University, Jackson, MS, USA;
Computer Science, Jackson State University, Jackson, MS, USA

Alok Misra Dr. A.P.J. Abdul Kalam Technical University, Lucknow, India

N. Mohammed Muddasir Department of Information Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

Poornima Mohan Department of Electronics and Communication Engineering, Amrita School of Engineering, Kollam, Kerala, India

Anjali Mohapatra DST-FIST Bioinformatics Laboratory, IIIT Bhubaneswar, Bhubaneswar, India

Shubhankar Mohapatra DST-FIST Bioinformatics Laboratory, IIIT Bhubaneswar, Bhubaneswar, India

Md. Mokammel Haque Department of Computer Science and Engineering, Chittagong University of Engineering and Technology, Raozan, Chittagong, Bangladesh

Jash Mota Department of Mechatronics Engineering, MPSTME, NMIMS University, Mumbai, India

R. Muthulakshmi Department of IT, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

Sameena Naaz Department of Computer Science and Engineering, Jamia Hamdard, New Delhi, India

Deepak Nagalla Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

P. Nagarajan Department of Electronics and Communication Engineering, Centre for VLSI and Embedded Systems, Sree Vidyanikethan Engineering College, Tirupati, India;
Department of ECE, Vivekanandha College of Engineering for Women, Namakkal, India

Jolan Rokan Naif Informatics Institute for Postgraduate Studies-Baghdad, Baghdad, Iraq

Aswathy K. Nair Department of Electronics and Communications Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

K. Namitha Department of Electronics and Communication Engineering, Amrita School of Engineering, Kollam, Kerala, India

Gayathri Narayanan Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, Kerala, India

P. S. Narayanan Department of Computer Science and Applications, Amrita Vishwa Vidyapeetham, Kollam, India

G. Naveen Balaji Department of ECE, SNS College of Technology, Coimbatore, India

M. R. Naveen Kumar Department of Information Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

Ambidi Naveena Department of ETM, G. Narayanamma Institute of Technology and Science, JNTUH, Hyderabad, India

C. Nayak Department of Electronics and Communication Engineering, SRMIST, Kattankulathur, Chennai, India

Insha Naz Department of Computer Science and Engineering, Jamia Hamdard, New Delhi, India

N. Neema Department of Information Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

N. Neha School of Computing, Centre for Information Super Highway (CISH), SASTRA Deemed to be University, Thanjavur, Tamil Nadu, India

Katta Nigam Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

S. Nirmal Center for Computational Engineering and Networking (CEN), Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India

N. Nithya Department of Computer Science and Engineering, K. Ramakrishnan College of Engineering, Trichy, India

Khadheeja Niyas Department of Information Technology, KCG College of Technology, Chennai, India

S. Palaniappan Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India;
Department of Computer Science and Engineering, KCG College of Technology, Karapakkam, Chennai, India

Tanvi Pandhre Ramrao Adik Institute of Technology, Navi Mumbai, Maharashtra, India

Vignesh Parameswaran M. Tech. Embedded Systems, VIT, Vellore, India

Navrattan Parmar National Institute of Technology, Kurukshetra, Haryana, India

V. Parthipan Department of Computer Science and Engineering, KCG College of Technology, Karapakkam, Chennai, India

Ravi Kiran Pasumarthi Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

Kunal Sekhar Pati Department of Embedded Technology, School of Electronics Engineering, VIT University, Vellore, India

Deepti Patil Ramrao Adik Institute of Technology, Navi Mumbai, Maharashtra, India

Pratik Patil M.Tech Embedded Systems, VIT, Vellore, Tamil Nadu, India

Rahul Patil Department of Computer Science and Engineering, NMAMIT, Nitte, Karnataka, India

Rohan Patil Automation Department, Jain Irrigation Systems Ltd., Jalgaon, India

Narayan Patra Department of Computer Science and Engineering, Siksha O Anusandhan Deemed to be University, Bhubaneswar, India

Md. Kamrul Hossain Department of Computer Science and Engineering, Chittagong University of Engineering and Technology, Raozan, Chittagong, Bangladesh

P. Paul Jefferson Electronics and Communication, KCG College of Technology, Chennai, India

S. P. PavanKumar Department of Computer Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

M. Ponmani Raja Electronics and Communication Engineering, Jyothi Engineering College, Thrissur, India

M. R. Pooja Department of Computer Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

M. Pooja Lakshmi Department of Electronics and Communication Engineering, Sethu Institute of Technology, Pulloor, Virudhunagar District, Tamilnadu, India

P. Prabakaran CK College of Engineering & Technology, Cuddalore, India

R. Pradeep Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumkur, Karnataka, India

R. Pradheepa Department of Electronics and Communication Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India

C. Prajitha Department of Biomedical Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India

B. Bhanu Prakash Department of Electronics and Communications Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

S. Pramod Department of Mechanical Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

Pranesh VTU-RRC, Visvesvaraya Technological University (VTU), Belgaum, Karnataka, India

Prajith Kesava Prasad Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India

M. V. Prashanth Department of Information Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

S. Pravinraj School of Computing, Centre for Information Super Highway (CISH), SASTRA Deemed to be University, Thanjavur, Tamil Nadu, India

N. S. Prema Department of Information Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

T. Primya Dr. N.G.P. Institute of Technology, Coimbatore, India

D. Priya Department of Information Science, RV College of Engineering®, Bangalore, India

S. Priyanga School of Computing, Centre for Information Super Highway (CISH), SASTRA Deemed to be University, Thanjavur, Tamil Nadu, India

Kuppili Puneeth Department of Electrical and Electronics Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

A. D. Radhika Department of Computer Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

Md A. Rahman Computer Science, Jackson State University, Jackson, MS, USA

M. M. Anishin Raj Department of CSE, Viswajyothi College of Engineering & Technology, Vazhakulam, Kerala, India

Amrita Raj Department of Computer Science and Engineering (CSE), M.M.M. University of Technology, Gorakhpur, U.P., India

M. Rajalakshmi Department of Electronics and Communication Engineering, Sethu Institute of Technology, Pulloor, Virudhunagar District, Tamilnadu, India

K. Rajasekhar Department of Computer Science Engineering, Koneru Lakshmaiah Education Foundation Green Fields, Guntur District, Vaddeswaram, Andhra Pradesh, India

M. Rajasekhar Reddy School of Computing, SASTRA Deemed to Be University, Thanjavur, India

M. S. Rajasree APJ Abdul Kalam Technological University, Thiruvananthapuram, Kerala, India

Sreeja Rajendran Department of EEE, BITS Pilani, Dubai Campus, Dubai, UAE

Megalingam Rajesh Kannan Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

Manita Rajput Department of Electronics and Telecommunication Engineering, Fr. C.R.I.T, Vashi, Navi, Mumbai, India

M. Rakhee Muthoot Institute of Technology and Science, Kochi, India

Mohammed Golam Sarwar Rakib Department of Computer Science and Engineering, International Islamic University Chittagong, Chittagong, Bangladesh

R. Rama Devi Janson Institute of Technology, Coimbatore, India

P. Ramakanth Kumar Department of Computer Science and Engineering, R.V. College of Engineering, Bengaluru, India

Virender Ranga National Institute of Technology, Kurukshetra, Haryana, India

Krupa Rasane E&C Department, Jain College of Engineering, Belgavi, India

V. Ravi Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumkur, Karnataka, India

O. Rajasekhar Reddy Department of Electronics and Communication Engineering, Amrita School of Engineering, Kollam, Kerala, India

Basil Reji Muthoot Institute of Technology and Science, Ernakulam, India

S. Rethishkumar School of Computer Sciences, Mahatma Gandhi University, Kottayam, Kerala, India

S. Revathy Department of Information Technology, KCG College of Technology, Chennai, India

S. Rinesh Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India; Department of Computer Science and Engineering, KCG College of Technology, Karapakkam, Chennai, India

Narjala Rohith Department of Electrical and Electronics Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

G. R. Sagar Department of Computer Science and Engineering, CHRIST (Deemed to Be University), Bangalore, India

Prabir Saha National Institute of Technology Meghalaya, Shillong, India

H. P. Sahana Department of Information Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

Ronak Sahu Information Technology, Terna Engineering College, Navi Mumbai, India

A. Sai Hanuman Department of CSE, Gokaraju Rangaraju Institute of Engineering & Technology (Autonomous), Bachupally, Telangana, India

P. Sai Siddartha Reddy School of Computing, SASTRA Deemed to Be University, Thanjavur, India

Manisha Sampat Department of Mechatronics Engineering, MPSTME, NMIMS University, Mumbai, India

Kambhampati Sai Sandilya Department of Electronics and Communication Engineering, Amrita School of Engineering, Kollam, Kerala, India

T. R. Sangeetha Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, Kerala, India

M. S. Sanjana Department of Information Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

Kumar Sanjeev Centre for Development of Advanced Computing (C-DAC), Mohali, India

S. L. Sanjith Indian Institute of Management Tiruchirappalli, Tiruchirappalli, Tamilnadu, India

V. Sanju Department of Computer Science and Engineering, NMAMIT, Nitte, Karnataka, India

B. Sankara Babu Department of CSE, Gokaraju Rangaraju Institute of Engineering & Technology (Autonomous), Bachupally, Telangana, India

J. Vaishnu Saran Department of Electronics and Communication Engineering, Amrita School of Engineering, Kollam, Kerala, India

Moumita Sarkar DST-FIST Bioinformatics Laboratory, IIIT Bhubaneswar, Bhubaneswar, India

K. Sashi Rekha Dr. N.G.P. Institute of Technology, Coimbatore, India

J. Sasi Kiran Department of CSE, Farah Institute of Technology, Chevella, Telangana, India

Sasidharan Jiji Electronics and Communication Engineering, Jyothi Engineering College, Thrissur, India

S. Sathishkumar Department of Information Technology, Adhiyamaan College of Engineering, Hosur, India

Viraj Savaliya Department of Electronics and Telecommunication, Dwarkadas J. Sanghvi College of Engineering, Mumbai, India

Dattatray Sawant Department of Mechatronics Engineering, MPSTME, NMIMS University, Mumbai, India

Priyanka Sawant Department of Electronics and Telecommunication Engineering, Fr. C.R.I.T, Vashi, Navi, Mumbai, India

Rohan Sawant Vidyalankar Institute of Technology, Mumbai, India

Sudhir Sawarkar Department of Computer Engineering, Datta Meghe College of Engineering, Navi Mumbai, India

Pratishtha Saxena Department of Computer Science & Engineering, Centre for Advanced Studies, AKTU, Lucknow, India

Manjubala Sekar Amrita Center for Cyber Security Systems & Networks, Amrita Vishwa Vidyapeetham, Amrita University, Kollam, Kerala, India

Y. Chandra Sekhar Department of Electronics and Communications Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

R. Senthilnathan School of Computing, Centre for Information Super Highway (CISH), SASTRA Deemed to be University, Thanjavur, Tamil Nadu, India

Suresh Seshan School of Computing, Centre for Information Super Highway (CISH), SASTRA Deemed to be University, Thanjavur, Tamil Nadu, India

M. Sethupathi Department of ECE, SNS College of Technology, Coimbatore, India

Dharmil Shah Department of Electronics and Telecommunication, Dwarkadas J. Sanghvi College of Engineering, Mumbai, India

Henish Shah Department of Electronics and Telecommunication, Dwarkadas J. Sanghvi College of Engineering, Mumbai, India

Kalp Shah Department of Electronics and Telecommunication, Dwarkadas J. Sanghvi College of Engineering, Mumbai, India

Sohail Shaikh Information Technology, Terna Engineering College, Navi Mumbai, India

Ahmed Shan-A-Alahi Department of Computer Science and Engineering, International Islamic University Chittagong, Chittagong, Bangladesh

V. S. Shankar Sriram School of Computing, Centre for Information Super Highway (CISH), SASTRA Deemed to be University, Thanjavur, Tamil Nadu, India

M. Shanmugasundaram School of Electronics Engineering, VIT, Vellore, India; Department of Embedded Technology, VIT, Vellore, India

Ravindra Kumar Sharma Singhania University, Jhunjhunu, Rajasthan, India

Sunil Sharma Rajasthan Technical University, Kota, India

Rajashree Shedge Ramrao Adik Institute of Technology, Navi Mumbai, India

Yash Shetye Department of Mechatronics Engineering, MPSTME, NMIMS University, Mumbai, India

B. Simhachalam Naidu KPIT Technologies, Bengaluru, India

C. Sinchana Department of Computer Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

K. Sinchana Department of Computer Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

Sukhvir Singh Department of Information Technology Development (IT), University Institute of Engineering and Technology (UIET), Punjab University, Chandigarh, India

Sachin Kumar Singh Department of Embedded Technology, VIT, Vellore, India

Madhvi Singhal Department of Computer Science & Engineering, Guru Ghasidas University, Bilaspur, India

S. Sivagamasundari Department of Electronics and Instrumentation Engineering, Annamalai University, Chidambaram, India

V. Sivakumar Department of IT, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

N. Sivaramakrishnan Department of ECE, SNS College of Technology, Coimbatore, India

K. P. Soman Center for Computational Engineering and Networking (CEN), Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India

M. Someshwaran Electronics and Communication, KCG College of Technology, Chennai, India

Anshu Soni National Institute of Technology, Kurukshetra, Haryana, India

Siddaram Sonnagi Department of Computer Science and Engineering, NMAMIT, Nitte, Karnataka, India

V. Sowmya Center for Computational Engineering and Networking (CEN), Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India

Rajkumar P. Sreedharan Department of Electronics and Communication, Amrita Vishwa Vidyapeetham, Amritapuri, India

A. G. Sreejith Muthoot Institute of Technology and Science, Kochi, India

K. Vandith Sreenivas Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

R. Sridevi Department of Computer Science and Engineering, K. Ramakrishnan College of Engineering, Trichy, India

A. Srilakshmi SASTRA Deemed to be University, Thanjavur, India

S. Srimathi Department of Computer Science and Engineering, K Ramakrishnan College of Engineering Samayapuram, Trichy, India

M. Sai Srinivas Department of Electronics and Communications Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

S. Sruthi Department of ECE, TKM College of Engineering, Kollam, Kerala, India

Swaminathan Subbiah Department of Computer Science and Engineering, Saveetha School of Engineering, SIMATS, Chennai, India

Gopinath Subramani Department of Information Technology, KCG College of Technology, Chennai, India

Gnanou Florence Sudha Department of Electronics and Communication Engineering, Pondicherry Engineering College, Puducherry, India

T. Suganya Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India

R. Sujatha School of Electronics Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India

H. D. Sundresh RV College of Engineering®, Banglore, India

B. Sunil Department of Information Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

N. R. Sunitha Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumkur, Karnataka, India

Neha Supe Ramrao Adik Institute of Technology, Navi Mumbai, Maharashtra, India

S. Suresh Department of Computer Science and Engineering, P.a College of Engineering and Technology, Pollachi, Coimbatore, TamilNadu, India

C. Suresh Gnana Dhas Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai, India

Azhar Syed Department of EEE, BITS Pilani Dubai Campus, Dubai, UAE

Suyog Tambe Sardar Patel Institute of Technology, Mumbai, India

R. Tamilselvi Department of Electronics and Communication Engineering, Sethu Institute of Technology, Pulloor, Virudhunagar District, Tamilnadu, India

Hardik Thakkar Sardar Patel Institute of Technology, Mumbai, India

Neha Rupesh Thakur Department of Electronics and Telecommunication, Thadomal Shahani Engineering College, Bandra, Mumbai, India

Shivam Thakur Department of Embedded Technology, VIT, Vellore, India

S. Theeijitha Department of ECE, SNS College of Technology, Coimbatore, India

Ayushi Turkar Department of Computer Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

Mohammad Nazim Uddin Department of Computer Science and Engineering, International Islamic University Chittagong, Chittagong, Bangladesh

A. Umamakeswari School of Computing, SASTRA Deemed University, Thanjavur, India

A. Umapriya Department of ECE, Vivekanandha College of Engineering for Women, Namakkal, India

A. S. Umarfarooq Department of E&CE, SDMCET, Dharwad, Karnataka, India

Shree Rajesh Raagul Vadivel Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

Vandana Mansur School of Electronics Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India

P. Venkatramana Department of Electronics and Communication Engineering, Centre for VLSI and Embedded Systems, Sree Vidyanikethan Engineering College, Tirupati, India

Sushma Verma Defence Research and Development Organization, (SAG), New Delhi, India

Amarsinh Vidhate Ramrao Adik Institute of Technology, Navi Mumbai, India

K. P. Vidyashree Department of Information Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

M. S. Vijaya PSGR Krishnammal College for Women, Coimbatore, India

R. Vijayakumar School of Computer Sciences, Mahatma Gandhi University, Kottayam, Kerala, India

Rajilal Manathala Vijayan School of Computing, SASTRA Deemed University, Thanjavur, India

Putchala Vinay Department of Electrical and Electronics Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

Athira Vinod Amrita Center for Wireless Networks & Applications (AWNA), Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

C. Vinothini Dr. N.G.P. Institute of Technology, Coimbatore, India

S. V. Viraktamath Department of E&CE, SDMCET, Dharwad, Karnataka, India

L. R. Vishnu Vardhan Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India

D. Vishnu Vashista School of Electrical and Electronics Engineering, SASTRA Deemed to Be University, Thanjavur, India

Vimal P. Viswan Muthoot Institute of Technology and Science, Ernakulam, India

P. V. Vivek Sridhar Mallya Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, Kerala, India

Prasanth M. Warrier Department of Electronics and Communication, Amrita Vishwa Vidyapeetham, Amritapuri, India

Marguerite Wotto Université du Québec à Montréal (UQÀM), Montreal, Canada

Divakar Singh Yadav Institute of Engineering and Technology, Lucknow, UP, India

Nishi Yadav Department of Computer Science & Engineering, Guru Ghasidas University, Bilaspur, India

Prasant Kumar Yadav Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

Samarjeet Yadav Department of Computer Science & Engineering, Centre for Advanced Studies, AKTU, Lucknow, India

Surekha Yakatpure Electronics and Telecommunication Department, A G Patil Institute of Technology, Solapur, India

Vinayakgouda Yallappagoudar Department of E&CE, SDMCET, Dharwad, Karnataka, India

Kaki Yeswanth Department of Electronics and Communications Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

D. Yuvaraj Department of CSE, Chian University, Cihan University, Duhok, Kurdistan Region, Iraq

Prajakta Zodge IT Department, Terna Engineering College, Mumbai University, Navi Mumbai, Maharashtra, India

Enhanced Security Mechanism in Cloud Based on DNA Excess 3 Codes

Manjot Kaur and Kiranbir Kaur

Abstract Exchanging data over the system has generally utilized quick and solid hot spot for correspondence. Clients from wide devotion utilize this component for exchanging and retrieving the required data. Portability and operability inside cloud framework are achieved through disconnected and online mediums, which are persistently alluring, yet the issue of security emerges amid the transmission process. Security and unwavering quality are the key issues during the exchange process, which requires serious research consideration. Data security is achieved by utilizing the public and private key-enabled block-level DNA-based EX-3 code. The analysis is inferred on the disconnected information as well as on the online information, for example, Google Docs. Redundancy handling mechanism is utilized to guarantee space for the information storage supplier, which remains a minimum utilized characteristic as it considers the capacity utilization in DSP. With the proposed system, the overall space allocation for heavy documents is decreased and online data security has been improved by the utilization of byte-level DNA-based EX-3 code.

Keywords DNA · Ex-3 · Data security

1 Introduction

In recent years, due to the rapid development of media transmission and Web, data security turns out to be increasingly huge in nature. Cryptography is one of the most ideal paths for ensuring unknown data. Cryptosystems can be separated into two kinds, secret key cryptosystem and public key cryptosystem. The main sort (secret key cryptosystem) utilizes a similar encryption key to encipher the plaintext and decode the figure content. For this reason, this system is additionally called as symmetric cryptosystem. It has a few disadvantages like excessively numerous keys,

M. Kaur (✉) · K. Kaur
GNDU (Main Campus), Amritsar, India
e-mail: manjotk705@gmail.com

K. Kaur
e-mail: kiran.dcse@gndu.ac.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_1

key conveyance issue, verification and non-repudiation issue. The imperative kind which is the public key cryptosystem is created to take care of the issues of symmetric cryptosystem, and RSA cryptosystem emerges as the most prevalent approach. As of late, information security has turned into an essential issue for public, private and guard associations as a result of the extensive misfortunes of illicit information. To shield the secret information or data from unapproved access, illegal changes and propagation, different sorts of cryptographic strategies are utilized. One of these critical strategies is cryptography, which performs the investigation of writing in secret frame, and it is isolated into two sorts: symmetric cryptography and asymmetric cryptography.

Cloud computing is emerging a state-of-the-art storage technology in almost all the domains, but many experts argue about it [1]. Highly scalable services are provided by the cloud. Users can utilize the services on pay-per-use basis. Cloud computing theoretically provides infinite resources, but due to growing number of users, practically services and resources become limited. The services and resources required to be distinguished on the basis of scale of utilization along with cost. Further improvement in cloud services could lead to a better framework for concurrent users in order to access resources more than the capacity of the machine user hold which leads to more popularity and user community attracted towards cloud services [2].

Cloud interoperability is required during the transmission of data to and from the cloud servers. The cloud service provides ensures quality of service (QoS) through security mechanisms. The security mechanisms used may or may not use redundancy handling mechanism to conserve space. In the proposed system, security mechanism along with redundancy handling mechanism is enforced for ensuring quality of service. The attributes considered for evaluation are described below.

1.1 Attributes

Cloud computing is used widely from long time and provides opaque framework where services are visible to the user but internal working is hidden [3]. Key attributes in cloud computing are described in this section:

- **Service-Based**: The main objective of cloud is to provide a service-oriented framework by hiding details and showing only necessary features to the user. This mechanism is also termed as abstraction.
- **Scalable and Elastic**: Services associated with cloud are not fixed. Services can be added as and when required depending upon mass usage of services. In other words, scalable environment is provided by cloud computing [4]. Elasticity in framework indicates that the resources are provided on different platforms that remain accessible to multiple users at the same time. In other words, concurrency is supported through the use of cloud computing framework.

- **Shared** [5]: Pool of resources are provided by the use of advanced computing environment. The provided resources are not exclusive in nature. Exclusive resources cannot be shared, and that required accessing queue should be maintained.
- **Metered by Use**: Multiple payment modes are supported by the cloud infrastructures [6]. Services are accessed on pay-per-use basis. Service provider and clients are bound by the service-level agreement. User needs to pay for accessing the services mentioned within SLA.
- **Uses Internet Technologies**: Services are delivered to the user by the use of Internet. Protocol such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Terminal network (Telnet), etc., are used for this purpose [7].

Symmetric calculations are commonly viewed, and they are appropriate for preparing extensive stream of information. A portion of the popular and proficient symmetric calculations incorporate two fish, Serpent, AES, Blowfish and IDEA. Also, there are non-specific calculations that offer an elective system for encryption. Hereditary calculations contain three essential administrators; they are multiplication, hybrid and change. Furthermore, there are distinctive well-known and productive deviated calculations like RSA, NTRU and elliptic curve cryptography.

2 Related Work

Li et al. [8] describes IBE technique with outsourcing computation and also offloads the key generation operations to key update the cloud service provider. It also focuses on critical issues of identity revocation. It accomplishes consistent productivity for both calculations at PKG and private key size at client; user need not to contact with PKG amid key update. PKG is permitted to be disconnect and subsequent to send the disavowal rundown to KU-CSP; no protected channel or client verification is required amid key update amongst client and KU-CSP.

Seo et al. [9] proposed the main mCL-PKE scheme without blending operations and gave its formal security. Our mCL-PKE takes care of the key escrow and disavowal issue. Utilizing the mCL-PKE conspires as a key building block; it proposes an enhanced way to deal safely and share sensitive information out in the public clouds. This approach supports quick denial and guarantees the classification of the information put away in an untrusted open cloud while authorizing the entrance control strategies of the information proprietor. The exploratory outcomes demonstrate the productivity of fundamental mCL-PKE scheme and enhanced approach for people in general cloud. Further, for various clients fulfilling similar access control arrangements, the enhanced approach performs just a solitary encryption of every datum thing and lessens the general overhead at the information owner.

Wang et al. [10] proposed a variation of CP-ABE to effectively share the various hierarchical documents in distributed computing. The hierarchical documents are scrambled with an incorporated access structure, and the ciphertext parts identified with characteristics could be shared by the records. Thus, both ciphertext storage and time cost of encryption are saved. The proposed system has benefits that clients can decode all approval documents by figuring secret key once. Therefore, the time cost of decryption is also saved if the client needs to decode various documents. Additionally, the proposed plot is ended up being secure under DBDH suspicion.

Xu et al. [11] designed a virtual encryption card framework that gives encryption card usefulness in virtual machines. In this framework, it displayed the vEC-PPM, which deals with the encryption resource plan. It saved clients' information utilizing a trusted equipment of virtualization in view of TPM. It additionally settled a trusted chain amongst clients and encryption cards in the light of the composed protocols. The design of the virtual encryption card empowers the security and productivity of the encryption benefit. A usage examination shows that the effectiveness of framework is similar to that of the native mode. Later on, it proceeds with examination, trying to plan a virtual encryption cards bunch to help higher encryption speed and more reasonable similarity with virtualization.

Alabdulatif et al. [12] proposed a safe billing protocol for smart applications in distributed computing. It utilized homomorphic encryption through adjusting the Domingo-Ferrer's plan, which can perform different number arithmetic operations to fulfil smart grid billing necessities in a safe way. This plan keeps up the exchange off amongst security and versatility contrasted and other homomorphic plans that depend on either secure, yet inelastic in terms of arithmetic operations assortment. Additionally, it proposed an instrument that guarantees both security and integrity during correspondence between substances. The execution of the proposed system is very satisfactory; it is sufficiently productive to use in lightweight applications and can be helpfully connected to cloud-based applications.

Li et al. [13] proposed a CP-ABE scheme that gives outsourcing key-issuing, decryption and keyword search work. This scheme is productive since it just needs to download the fractional decryption ciphertext relating to a particular keyword. In this scheme, the tedious matching operation can be outsourced to the cloud specialist organization, while the slight operations should be possible by clients. In this way, the calculation cost at the two clients and trusted specialist sides is limited. Besides, the proposed plot supports the capacity of keywords look which can enormously enhance correspondence effectiveness and further ensure the security and protection of clients. It is difficult to stretch out given KSF-OABE plan to help get to structure represented by tree in [14]. In this paper, based on contingent intermediary communicate re-encryption technology, an encrypted information sharing plan for secure distributed storage is proposed. The plan not just accomplishes communication information sharing by exploiting communication encryption, yet in addition accomplishes dynamic sharing that enables adding a client to and expelling a client from sharing gatherings dynamically without the need to change encryption open keys. Besides, by utilizing intermediary re-encryption innovation, this scheme empowers the intermediary (cloud server) to specifically share encoded information to the objective clients without the intercession of information owner while keeping information security so significantly enhances the sharing execution. In the meantime, the rightness and the security are demonstrated; the execution is broke down, and the test comes about is appeared to confirm the possibility and the productivity of the proposed plot.

Liu et al. [15] proposed diagram encryption scheme which just makes utilization of lightweight cryptographic natives, for example, pseudo-arbitrary capacity and symmetric-key encryption, instead of moderate homomorphic encryptions. Accordingly, the proposed graph encryption scheme is well disposed to a wide arrangement of graph information-based distributed computing and edge registering applications, for example, interpersonal organizations, e-maps, criminal investigations and so on. Contrast with graph anonymization comes nearer from database group, the proposed system achieves higher security level as the chart itself is encoded and it does not make any suspicions on the sorts of attacks.

Song et al. [16] discussed the security enhancement mechanisms including symmetric, public key, and homomorphic cryptosystems to enable experts to comprehend encryption plans for information on distributed storage. AES is utilized as a part of most secure applications for information on distributed storage. Completely homomorphic encryption plans are promising for cloud condition however a long way from being useful due to their execution rate. Homomorphic assessment of AES has fascinating applications as a reasonable encryption conspires for information on distributed storage.

Veeraragavan [17] proposed an improved encryption calculation (EEA) for securing the data in cloud stockpiling. This is a symmetric encryption calculation. It utilizes same key for encoding and unscrambling the data previously put away into cloud. Xu et al. [18] proposed a lightweight accessible open key encryption (LSPE) conspired with semantic security for CWSNs. LSPE decreases countless calculation escalated operations that are received in past works; along these lines, LSPE has sought execution near that of some useful accessible symmetric encryption schemes. Tsai et al. [19] proposed a protected cloud data encryption framework, named the circulated ecological key (DENK in short), with which all records are encoded by one encryption key got from numerous coordinating keys which are keys got from approved clients' secret key keys and a believed PC's natural key. El-yahyaoui [20] proposed to present an effective and unquestionable FHE in the light of another mathematic structure that is without commotion.

Thomas [21] described the various ways used in cloud computing for data security. The information is stored on the incorporated area called data centres that have a substantial size of information storage. In this way, the customers need to put stock in the supplier on the accessibility and additionally information security. Before moving information into general society cloud, issues of security gauges and similarity must be tended to. A trusted screen introduced at the cloud server that can screen or review the operations of the cloud server. In limiting potential security trust issues and additionally sticking to administration issues confronting cloud computing, an essential control measure is to guarantee that a solid cloud computing service-level agreement (SLA) is set up and kept up when managing outsourced cloud service suppliers and particular cloud merchants. Cloud computing guarantees to change the financial matters of the server farm, yet before sensing and managed information move.

To resolve the problem with the existing literature, the proposed literature presents efficient solution. The encryption mechanism with the redundancy handling mechanism is proposed as described in the next section.

3 Methodology

The methodology of proposed work consists of registration process at first place. The registration in proposed system will be two-phase process. In the first phase, registration at data storage provider is made. After successfully registering, user can load files at data storage provider end. To generate keys, users require performing registration at key service provider. In order to retrieve the files, users must login to the DSP and then KSP. The keys generated could be used in order to decrypt the file. The mechanism also uses redundancy handling mechanism for preserving space for extra file loading. Also online source of files like Google Docs can be used to retrieve the files and perform encryption and decryption.

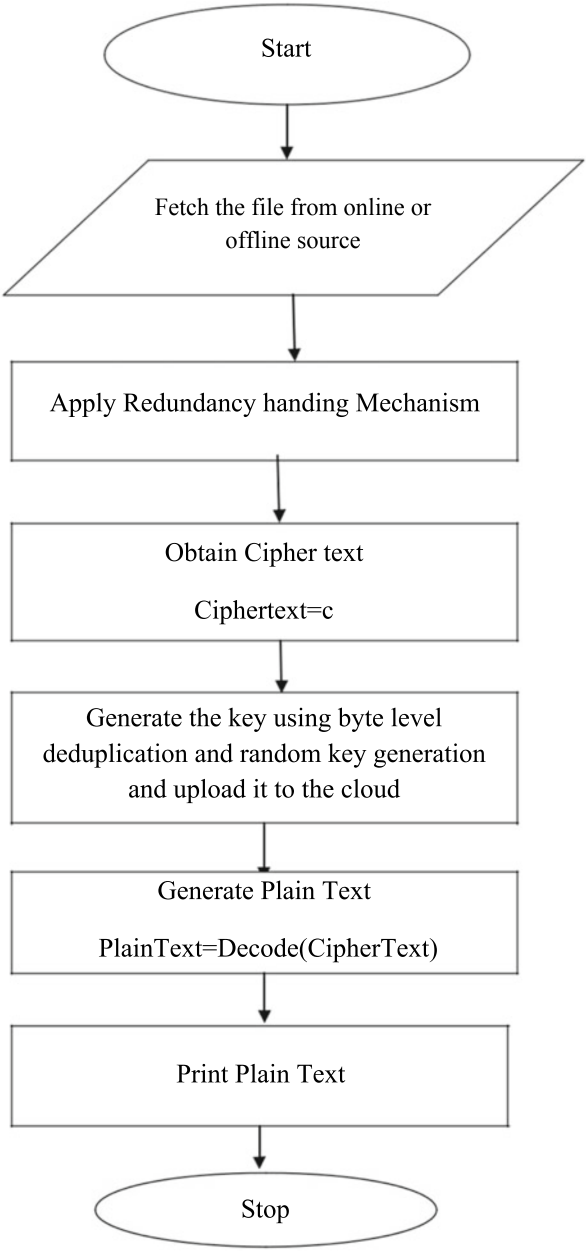
The detailed steps are described as under:

3.1 Registration at DSP

The registration at DSP comprises unique username and password. Username and password once registered at DSP can be used for accessing file uploading module.

3.2 Registration at KSP

Key service provider (KSP) is used in order to generate the keys for the file which is uploaded. The proposed system is capable of generating the keys for files generated from online source.


Start
Fetch the file from online or offline source
Apply Redundancy handing Mechanism
Obtain Cipher text
Ciphertext=c
Generate the key using byte level deduplication and random key generation and upload it to the cloud
Generate Plain Text
PlainText=Decode(CipherText)
Print Plain Text
Stop

3.3 Generating Keys

In order to generate keys, user must login to the KSP. The files uploaded are encrypted, and corresponding keys are generated. The redundant files are neglected, and rest of the files are uploaded with the public and private keys generated.

3.4 Encryption and Decryption

For encryption and decryption using byte-level DNA-based EX-3 code, algorithms are hybridized. The algorithm yields ciphertext after receiving files as plaintext. Verification of the overall procedure is in terms of time consumed and size of the file that can be uploaded.

4 Result and Performance Analysis

The result is presented in terms of file size that can be uploaded. Reliability of encryption and decryption in terms of time consumed is also a performance metric. The comparison in terms of quality is given below.

Space conservation is achieved using the proposed system. This space conservation is indicated through Table 1.

The plots correspond to the existing and the proposed literature are given in Fig. 1.

The result deviation obtained using the existing and the proposed system is also given through the line chart. The line chart is generated by feeding the values obtained from the simulation as shown in Fig. 2.

The execution time subsequently reduced as file size to be uploaded reduced. The execution time is estimated by subtracting the end time of simulation from start time of simulation. The comparison table for the same is given as Table 2.

The plot for the execution time is given using bar and line charts. The chart generation is done using the facility provided through excel and JFreeCharts (Fig. 3).

The simulation results obtained are also plotted using the line chart. The proposed system execution time is better as compared to the existing system. The proposed

Table 1 Simulation results with different file sizes

Simulation	Block level (KB)	Byte level (MB)
Sim 1	1046	678
Sim 2	1055	500
Sim 3	2010	878
Sim 4	1034	645
Sim 5	1074	788

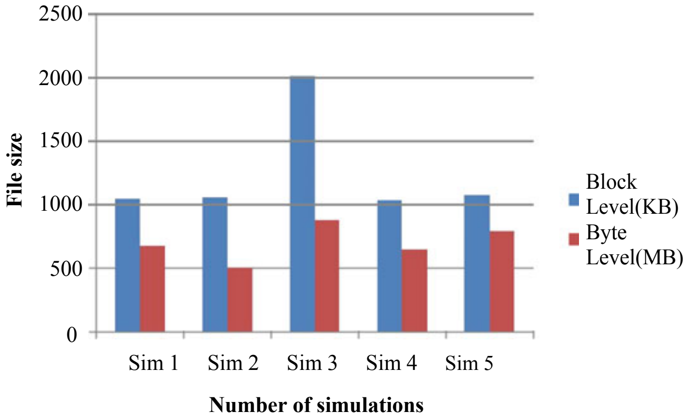


Fig. 1 Existing and the proposed file size comparison with bar chart

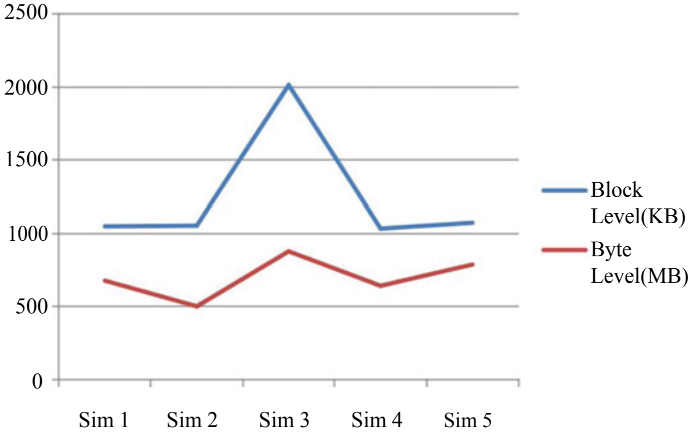


Fig. 2 Line chart corresponds to space used by existing and the proposed systems

Table 2 Simulation result of execution time

Simulation	Block level (ms)	Byte level (ms)
Sim 1	123	83
Sim 2	103	67
Sim 3	112	78
Sim 4	187	102
Sim 5	118	81

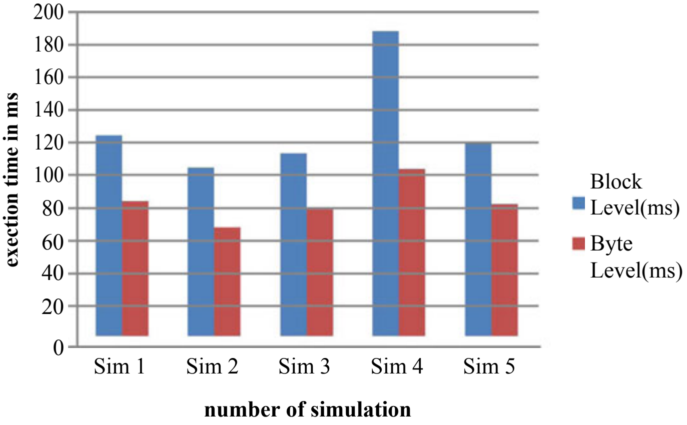


Fig. 3 Execution time of simulation corresponding to various simulations

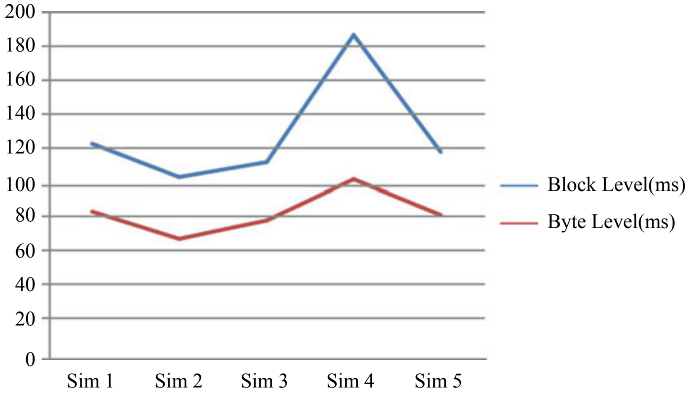


Fig. 4 Execution time corresponding to existing and the proposed systems

system uses the byte-level deduplication, and the existing system uses block-level deduplication (Fig. 4).

5 Conclusion

From this research paper, we conclude that the cloud computing not only provides the resources to the users but also develops major security challenge. There are security requirements for both users and cloud providers, but sometimes it may conflict in some way. Security of cloud depends upon trusted computing and cryptography. In our review paper, some issues are related to data location, security, storage, availability and integrity. Establishing trust in cloud security is the biggest requirement. The problems and corresponding solutions may require further investigation in terms of key size and complexity. Complexity of key can be further enhanced by the use of pseudo-random number generator within the key generation phase.

By incorporating complex key structure, cloud performance and user interaction can be further enhanced.

References

1. Hwang K, Bai X, Shi Y, Li M, Chen W-G, Wu Y (2016) Cloud performance modeling with benchmark evaluation of elastic scaling strategies. IEEE Trans Parallel Distrib Syst 27(1):130–143
2. Noor TH, Sheng QZ, Yao L, Dustdar S, Ngu AHH (2016) CloudArmor: supporting reputation-based trust management for cloud services. IEEE Trans Parallel Distrib Syst 27(2):367–380
3. Armbrust M et al (2010) A view of cloud computing. Commun ACM 53(4):50
4. Buyya R, Yeo CS, Venugopal S (2008) Market-oriented cloud computing: vision, hype, and reality for delivering IT services as computing utilities. In: Proceedings of 10th IEEE international conference on high performance computing and communications, HPCC 2008, pp 5–13
5. Nirmala SJ, Tajunnisha N, Bhanu SMS (2016) Service provisioning of flexible advance reservation leases in IaaS clouds, vol 3, no 3, pp 154–162
6. Marwan M, Kartit A, Ouahmane H (2016) Secure cloud-based medical image storage using secret share scheme. In: 2016 5th International Conference on Multimedia Computing and Systems (ICMCS), IEEE, pp 366–371
7. Dimitrov DV (2016) Medical internet of things and big data in healthcare. Healthc Inform Res 22(3):156–163
8. Li J, Li J, Chen X, Jia C, Lou W (2013) Identity-based encryption with outsourced revocation in cloud computing. IEEE Trans. Comput. 64(2): 425–437
9. Seo S, Nabeel M, Ding X, Bertino E (2013) An efficient certificateless encryption for secure data sharing in public clouds. IEEE Trans Knowl Data Eng 26(9): 2107–2119
10. Wang S, Zhou J, Liu JK, Yu J, Chen J, Xie W (2016) An efficient file hierarchy attribute-based encryption scheme in cloud computing. IEEE Trans Inf Forensics Secur 11(6): 1265–1277.
11. Xu D, Fu C, Li G, Zou D, Zhang H, Liu XY (2017) Virtualization of the encryption card for trust access in cloud computing. IEEE Access 5, 20652–20667
12. Alabdulatif A, Kumarage H, Khalil I, Atiquzzaman M, Yi X (2017) Privacy-preserving cloud-based billing with lightweight homomorphic encryption for sensor-enabled smart grid infrastructure. IET Wirel Sens Syst 7(6):182–190
13. Li J, Lin X, Zhang Y, Han J (2016) KSF-OABE: outsourced attribute-based encryption with keyword search function for cloud storage. IEEE Trans Serv Comput 10(5): 715–725
14. Jiang L, Guo D (2017) Dynamic encrypted data sharing scheme based on conditional proxy broadcast re-encryption for cloud storage. IEEE Access 5, 13336–13345.
15. Liu C, Zhu L, Chen J (2017) Graph encryption for top-k nearest keyword search queries on cloud. IEEE Trans Sustain Comput 2(4): 371–381
16. Song C, Park Y, Gao J, Nanduri SK, Zegers W (2015) Favored encryption techniques for cloud storage. In: 2015 IEEE First International Conference on Big Data Computing Service and Applications, IEEE, pp. 267–274
17. Veeraragavan N, Arockiam L, Manikandasaran SS (2017) Enhanced encryption algorithm (EEA) for protecting users' credentials in public cloud. In: 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), IEEE, pp. 1–6

18. Xu P, He S, Wang W, Susilo W, Jin H (2017) Lightweight searchable public-key encryption for cloud-assisted wireless sensor networks. IEEE Trans Ind Inf XX(XX):1–12
19. Tsai KL et al (2016) Cloud encryption using distributed environmental keys. In: Proceedings of 2016 international conference on innovative mobile and internet services in ubiquitous computing, IMIS 2016, pp 476–481
20. El-Yahyaoui A, El Kettani MD (2017) A verifiable fully homomorphic encryption scheme to secure big data in cloud computing. In: 2017 International Conference on Wireless Networks and Mobile Communications (WINCOM), IEEE, pp. 1–5
21. Thomas G, Jose V, Afsar P (2013) Cloud computing security using encryption technique, arXiv preprint, arXiv:1310.8392

TensorFlow-Based Semantic Techniques for Multi-cloud Application Portability and Interoperability

Tanveer Kaur and Kiranbir Kaur

Abstract Cloud computing permits plentiful access to shared pools of resources that are configurable and provide higher-level services to the user, which can be easily and hastily granted with minimal management effort. With the advancements in cloud computing, many cloud service providers have started using the distributed high-end servers to provide services to its users. However, while designing an efficient cloud environment, it has been found that the application portability is a key issue. Portability is usually offered to mitigate supplier lock-in. Nevertheless, shifting from a single method to an alternative for a minimum of work, seeing that is quite possible together with box companies, which can also improve the durability along with scalability. Therefore, in this paper, a novel TensorFlow-based semantic technique is designed and implemented to significantly port the applications between high-end servers. Extensive experiments have been carried out to evaluate the effectiveness of the proposed technique. Extensive experiments reveal that the proposed technique outperforms the existing techniques.

Keywords Cloud computing · Semantic · Multi-cloud · TensorFlow · Application portability · Vendor lock-in

1 Introduction

Application portability has the capability of an application to be compactly introduced, sent, got to and oversaw—independent of their conveyance display. This term communicates an application's adaptability when this is utilized on numerous distinctive stages or quickly got to from the Internet, a work area or system. Application portability coordinates various abilities of an application, and that application can be

T. Kaur (✉) · K. Kaur
Department of Computer Engineering and Technology, Guru Nanak Dev University, Amritsar, Punjab, India
e-mail: tanuhundal05@gmail.com

K. Kaur
e-mail: kiran.dcse@gndu.ac.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_2

got to over the Internet from a Web program. At the point when disconnected, application portability portrays an application's ability that is to be actualized on basic working framework (OS) conditions [1]. Application portability likewise alludes to an application that is transmitted and executed by means of versatile gadgets, for example, a Universal Serial Bus (USB) pen drive.

Portability. It is possible to move or transmit all portable apps between drives such as USB flash drive and carry anywhere. If you want to have your favourite programs available with you at all times, in this case this can be more helpful.

Better privacy. Since compact applications don't leave any utilization follows or remaining records behind and they don't should be introduced. This makes them quite fit for private usage scenarios.

Synchronization with cloud storage services. Portable applications can be synchronized with cloud storage services such as Dropbox. This is really helpful on the off chance that you utilize a distributed storage benefit on different PCs to match up your documents.

Custom application settings. The settings are typically spared with the application itself, when you indicate any custom settings for a versatile app (e.g. default download organizer for a compact browser). So you get a steady client encounter, regardless of the PC utilized for getting to the versatile application(s) [2].

Cloud Computing is often a model that gives consumers limitless computing electrical power that may be seen from anywhere based on consumer's convenience. User could incorporate rely the time like CPU, memory space, safe-keeping and also bandwidth along with demand for the reasoning provider [3]. User might also make use of prefabricated expert services like The amazon online marketplace Cognate, Supple Beanstalk supplied by this reasoning service provider in order to boost smooth operating regarding a questionnaire along with much less labour pool.

2 Technique Used

2.1 The Semantic-Based Approach

The overall model is a graph-based representation, structured into five conceptual layers. The five conceptual layers are [4]:

- This parameter level shows this criteria associated with the info sort changed between providers while input in addition to creation of this operations.
- The operations level shows these syntactic criteria in the operation and also benefits revealed by the cloud services (described through WSDL).
- The service level presents the particular semantic annotation of the vendor-dependent impair solutions (exposed via OWL-S) as well as the supporting ontologies necessary to find the particular cloud service provider reinforced operation, suggestions plus productivity parameters.

- The cloud pattern level represents this semantic explanation involving agnostic in addition to vendor-dependent cloud patterns becoming aware via an OWL representation. It contains habits in infrastructural level possibly at program level.
- The application pattern level symbolizes the actual account associated with behaviour expounding on the applying to be ported.

2.2 TensorFlow

TensorFlow is usually an open-source stockpile with regard to statistical computation. It was developed by Google in 2015. Offers allocated concurrent unit understanding based upon general-purpose dataflow graphs.

3 Related Work

Antoniades et al. [5], Enabling Cloud Application Portability, introduced the Cloud Application Requirement Language (CARL). CARL can be used for describing the application software and hardware requirements, information that is then encompassed into the TOSCA description of the cloud application, beside the application blueprint. CAMF's information service utilizes both these artefacts to provide IaaS-specific configurations that satisfy the user's requirements. Ranabahu et al. [6], Application Portability in cloud computing, November–December, survived an abstraction-driven way to deal with location the application convenience issues and spotlight on the application improvement process. It additionally surviving our hypothetical premise and involvement in two down to earth extends in which it connected the Abstraction driven methodology. Gunka et al. [7], Moving an Application to the Cloud, provided help understanding this issue by characterizing an evolutionary strategy to relocate a current application to the cloud. The principle ventures of this change are (1) porting the application to an IaaS, (2) including load adjusting the introduction and business rationale layer and (3) incompletely moving the application to a PaaS. Next to with every one of the means depicted multi-cloud methodologies will be considered keeping in mind the end goal to have the capacity to moderate dangers by using repetitive, free frameworks and to guarantee benefit vicinity for clients at various areas. Moreover, choice help is required to help recognizing the best-coordinating cloud stages for each progression. Kolba et al. [8], Towards Application Portability in Platform as a Service, arranged portability issues of PaaS; it portrays a model of current PaaS contributions and recognizes distinctive conveyability perspectives. Starting from the model, it infers an institutionalized profile with a typical arrangement of capacities that can be found among PaaS suppliers and relating with each other to check application transportability in view of biological system abilities. It approves our discoveries with a comprehensive informational collection of 68 PaaS contributions together with an electronic application for versatility coordinating. It additionally distinguishes advance convenience issues by moving the application to various PaaS merchants, approving biological community movability and giving indications to future research headings. Di Martino et al. [4]. Semantic Technique of Multi-cloud application portability and Interoperability 2016, presented a semantic-based representation of application patterns and cloud services exhibited, with a case of its utilization in a normal dispersed application, which shows how the proposed strategy can be effectively worked for the disclosure and arrangement of cloud services. Kostosk et al. [3], A New Cloud Services Portability Platform, proposed another cloud compactness benefit stage and gave an outline of the present patterns in the zone of cloud benefit portability, particularly breaking down the TOSCA's methodology. The new stage proposition depends on establishing a connector show, which offers the coveted cloud movability. The new arrangement characterizes the administrations by a XML TOSCA approach. Cretella et al. [9] discovered functionalities, APIs and assets required for the application improvement through semantic-based agnostic (vender independent) portrayals of such application segments, and re-aiming to fabricate a custom platform as a service (PaaS) that can acknowledge and exchange establishments of any convenient applications.

4 Gaps in Literature

- Getting a new progress, interconnected atmosphere is confronted with many obstacles, for example, provisioning, protection, acceptance and personality managing, flexibility, economic vitality proficiency and so forth;
- Vendor lock-in which ends from the possible lack of interoperability along with portability is said being a dominant obstacle in the route connected with realization connected with interclouds;
- Communications in Computer and Information Science (CCIS);
- The use of TensorFlow has been pushed aside by means of pre-existing examiner to provide more cost-effective brings about multi-cloud environment.

5 Proposed Methodology

This section contains the graphical representation of the proposed technique, consisting of various steps which are required to successfully accomplish the suggested algorithm shown in Fig. 1.

- Step 1. User sends a service request to cloud service provider;
- Step 2. Train the TensorFlow;

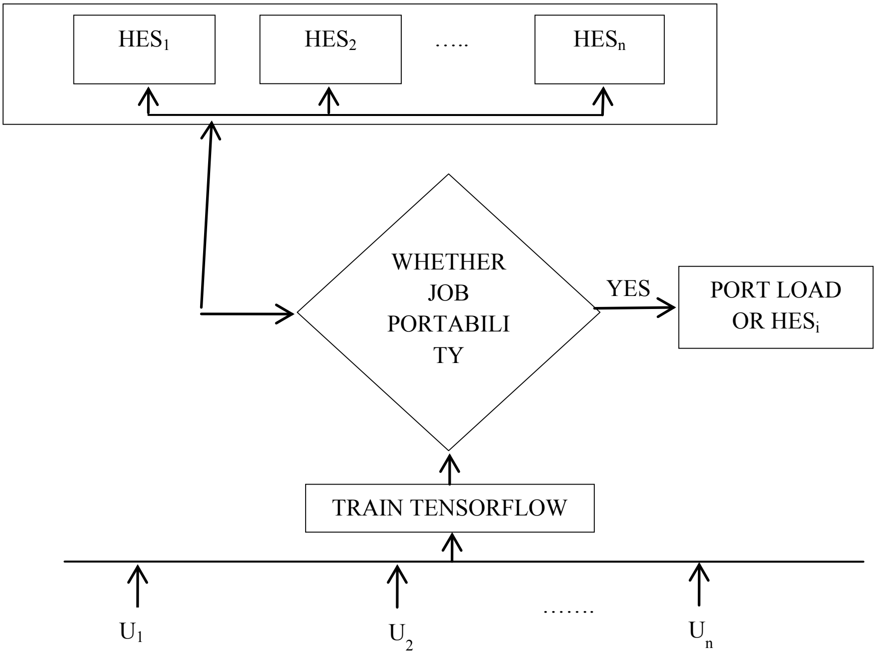


Fig. 1 Proposed block diagram

- Step 3. It checks that whether a job portability is required; if yes, then port load, and if no, then service request goes to high-end services (HES$_n$), and high-end service provided the services to users.

The proposed technique is designed using ANACODA. TCP uses a neural network to evaluate the T-worth function. The input for the system is the current, whereas the output is the relating T-worth for every one of the activity (Table 1).

Table 1 T leaning information

1	Activity (A_c): Altogether the conceivable moves that the specialist can take
2	State (S_t): Present circumstance reverted by environment
3	Reward (R_d): An instant return send back from the environment to assess the last activity
4	Strategy (π): The methodology that the specialist utilizes to decide the following activity dependent on the present state
5	Worth (V_e): The predictable lasting return with reduction, as opposed to the temporary reward R_d. $V_e\pi(c)$ is refer to as the expected lasting return of the present states under strategy π
6	T-worth or activity-worth (T): T-worth is like worth; then again, actually it takes an additional stricture, the present activity u

We train the network dependent on the T-learning inform condition. Review that the objective T-worth for T-learning is:

$$d + \gamma \max_{u'} Q\big(\varepsilon_{j+1,} u'; \sigma^{-}\big) \tag{1}$$

The ε is comparable to the state c, whereas the σ represents the strictures in the neural network, which is not in the space of our dialog. Along these lines, the loss function for the system is characterized as the squared error among target T-worth and the Q-worth output from the network.

Algorithm 1: Deep T-learning with experience replay

```
Originate replay memory M to capacity P
Originate activity-worth function T with random weights $\sigma$
Originate target activity-worth function $\widehat{T}$ with weight $\sigma^{-} = \sigma$
For incident = 1, M do
    Originate sequences $r_1 = \{m_1\}$ and pre-processed sequence $\varepsilon_1 = \varepsilon(r_1)$
    For t = 1, T do
        With probability $\varepsilon$ select a random activity $u_t$
        Otherwise select $u_t = argmax_a Q(\varepsilon(r_t), u; \sigma)$
        Execution action $u_t$ in emulator and observe reward $d_t$ and image $m_{t+1}$
        Set $r_{t+1} = r_{t,} u_t, m_{t+1}$ and pre-process $\varepsilon_{t+1} = \varepsilon(r_{t+1})$
        Store transition $\big(\varepsilon_{t,} u_{t,} d_t, \varepsilon_{t+1}\big)$ in D
        Sample random minibatch of transitions $\big(\varepsilon_{j,} u_{j,} d_{j,} \varepsilon_{j+1}\big)$ from D
        Set $n_j = \begin{cases} d_j & \text{if episode terminates at step } j+1 \\ d_j + \gamma \max_{u'} \widehat{T}\big(\varepsilon_{j+1,} u'; \sigma^{-}\big) & \text{otherwise} \end{cases}$
        Perform a gradient descent step on $\big(n_j - T\big(\varepsilon_j, a_j; \sigma\big)\big)^2$ with respect to the network parameters $\sigma$
        Every G steps reset $\widehat{T} = T$
    End For
End For
```

- Experience Replay: Since training samples in distinctive RL set-up are exceptionally corresponded and less data-efficient, it will tougher convergence for the network. An approach to resolve of the sample distribution issue is adopting background replay. Basically, the sample transitions are stowed, which will at that point be haphazardly chosen from the "transition pool" to refresh the knowledge.
- Separate Target Network: The objective T network has identical structure as the one that estimates worth. In each C step, as indicated by the above pseudocode, the target network is reset to another. Along these lines, the fluctuation becomes less severe, bringing about progressively steady trainings.

6 Proposed Methodology

This section defines the graph methodology with the help of parameters like execution time, number of swaps, load imbalance rate, and overhead time to describe the effective results in cloud computing environment. Another two strategies are likewise basic for training TCP.

Figure 2 shows the query execution on VMs, execution at VMs without any failure, failure at VMs, response to query (−ve) meaning not active and energy consumption by VMs.

Execution time. The execution time intended for an activity is described as how much time the whole usually takes to carry out confirmed job; this includes time utilized executing work time and also program products and services about its behalf. The particular apparatus and also system familiar with estimate execution time for a particular job are described as follows:

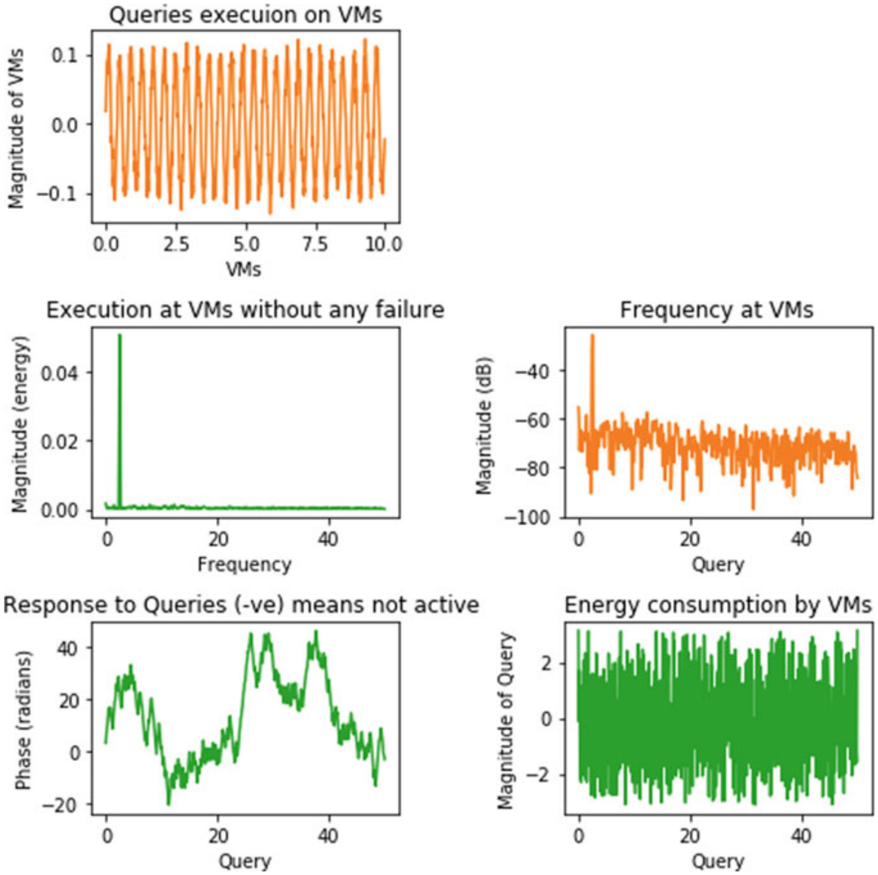


Fig. 2 Graphical representation of queries on VM's

Fig. 3 Execution time

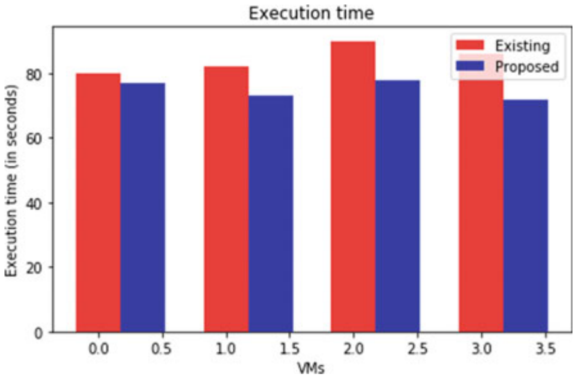
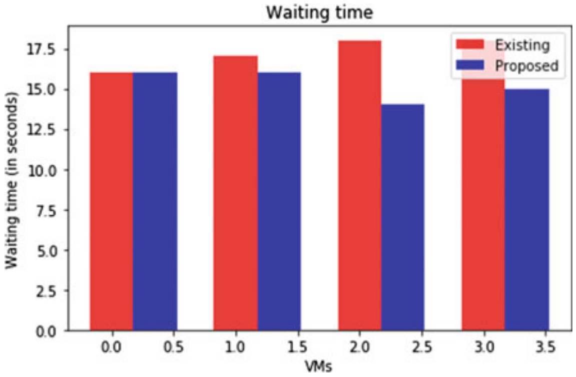


Fig. 4 Waiting time graph



$$\text{Execution Time} = \text{Stop Time} - \text{Start Time}$$

The below graphs show the comparison between the existing system and proposed system with respect to execution time. Figure 3 shows that existing system had consume more execution time than the proposed system. Figure 4 shows that existing system had consume more waiting time than the proposed system.

7 Conclusion

Interoperability is the capability regarding more than one devices or apps to switch details and also to mutually employ the details which were exchanged. Cloud interoperability is the ability of a customer's system to connect to a cloud program or the flexibility for one cloud that wants to connect to alternative cloud solutions by swapping details based on some given method to receive estimated results. The interoperability obstacles with each one of the clouds program classes (IaaS, PaaS plus

SaaS) might be different. That might be more challenging to realize behavioural interoperability over a couple of uses as opposed in order to connect a compute preferred to remote control storage, intended for example. In this paper, to enhance equally interoperability as well as portability, a new TensorFlow-based interpretability has been designed and implemented. It trains engines your semantic options that come with multi-cloud programs to boost the outcome further. Extensive experiments have been carried out to evaluate the effectiveness of the proposed technique. Extensive experiments reveal that the proposed technique outperforms the existing techniques.

References

1. Petcu D, Craciun C, Rak M (2011) Towards a cross platform cloud API. In: 1st international conference on cloud computing and services science, pp. 166–169
2. Arunkumar G, Venkataraman N (2015) A novel approach to address interoperability concern in cloud computing. Procedia Comput Sci 50:554–559
3. Kostoska M, Gusev M, Ristov S (2014) A new cloud services portability platform. Procedia Eng 69:1268–1275
4. Di Martino B, Esposito A (2016) Semantic techniques for multi-cloud applications portability and interoperability. Procedia Comput Sci 97(1): 104–113
5. Antoniades D, Loulloudese N, Foudoulis A, Sophokleous C, Trihinas D, Pallis G, Dikaiakos M, Kornmayer H (2015) Enabling cloud application portability. In: 2015 IEEE/ACM 8th international conference on utility and cloud computing (UCC), pp. 354–360
6. Ranabahu A, Maximilien EM, Sheth A, Thirunarayan K (2013) Application portability in cloud computing: an abstraction-driven perspective. IEEE Trans Serv Comput 8(6): 945–957
7. Gunka A, Seycek S, Kühn H (2013) Moving an application to the cloud: an evolutionary approach. In: Proceedings of the 2013 international workshop on Multi-cloud applications and federated clouds, ACM, pp. 35–42
8. Kolba S, Wirtz G (2014) Towards application portability in platform as a service. In: 2014 IEEE 8th international symposium on service oriented system engineering, pp. 218–229
9. Cretella G, Di Martino B (2015) A semantic engine for porting applications to the cloud and among clouds. Softw: Pract Exp 45(12):1619–1637
10. Gondis F, Simons AJH, Paraskakis I, Kourtesis D (2013). Cloud application portability: an initial view. In: Proceedings of the 6th balkan conference in informatics, ACM, pp. 275–282

Enhancing High Availability for NoSQL Database Systems Using Failover Techniques

Priyanka Gotter and Kiranbir Kaur

Abstract NoSQL allows fast processing of real-time large data applications. It allows database professionals to make use of elastic scalability of database servers. Most of these databases are created to perform on full throttle despite the presence of low-cost hardware. Users are able to create the database more quickly due to the non-relational nature of NoSQL. There is no need of developing the detailed (fine-grained) database model. As a result, it will save lots of development time. The primary aim of this paper is to present a novel data integration method as well as workflow that executes the data integration of various source systems in such a way that user does not require any programming abilities. Middleware is considered as main part of the proposed technique which provides high availability of data in case of failures by utilizing the checkpointing. Experimental results reveal that the proposed technique provides efficient results, especially in case of any kind of failures in distributed NoSQL servers.

Keywords NoSQL · High availability · Checkpointing · Failures

1 Introduction

The capacity to move duplicate or exchange information effectively from one database, stockpiling or IT condition to another in a safe and secure way without hindrance to usability is termed as data portability. The information must be in an organization that is interoperable between a few stages if we have to work with data portability [1, 2]. This concept comes forward to handle the issue of massive data. Data is increasing day by day and SQL databases are not able to manage this huge amount of data. There is a need of non-relational (often known as NoSQL) database management system since relational databases just work with organized

P. Gotter (✉) · K. Kaur
Computer Engineering and Technology, Guru Nanak Dev University, Amritsar, Punjab, India
e-mail: piyuprecious13@gmail.com

K. Kaur
e-mail: kiran.dcse@gndu.ac.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_3

information [8], which can manage both organized and semi-organized information. To compose the information, i.e., produced from different applications [4], social database and other customary databases take after unbending structure. However, NoSQL database gives adaptability in arranging the information that makes it simple to get to the information. They are not founded on a single model [5] (e.g., social model of RDBMSs), and every database is relying on the objective usefulness. ACID properties are imposed in SQL server [7]. Likewise, BASE property is imposed in NoSQL. The BASE acronym was characterized by Eric Brewer, who is likewise known for planning the CAP hypothesis. As per CAP hypothesis, in the meantime, a circulated PC framework cannot ensure the majority of the accompanying three properties in the meantime, i.e., consistency, availability and partition tolerance. NoSQL has recently come out and has developed interest and criticism [11]: interest simply because they manage specifications which can be significant within large-scale uses and criticism due to the analysis with popular relational achievements [3]. **Uniform data access** is a computational idea explaining an evenness of controllability along with connectivity across numerous target data sources. **Data integration** consists of mixing data residing in various sources and offers users with a unified view of them. This technique gets to be significant in a range of conditions, such as either industrial (such because if not one but two equivalent businesses should merge his) or her database and scientific (combining investigation comes from various bioinformatics repositories, to get example) domains. A **checkpoint** is a local state of a task kept on secure storage. Simply by routinely performing a checkpointing, one can possibly help you save a reputation of an activity with regular intervals. In case any node fails, one may resume computation from the earlier checkpoints, thereby avoiding restating execution from the beginning.

2 Related Work

This paper offers a novel integration methodology to be able to question information through different relational databases along with NoSQL repository system [12]. The recommended technique is dependent on meta-model strategy and it also protects the structural, semantic plus syntactic heterogeneities of origin system. To demonstrate the particular usefulness of recommended method, an Internet program is definitely designed, named hybrid DB. It possesses a database layer which provides whole database services over origin system. The parameters defined are entire running time, data retrieval time and native query time. Leavitt [6] learnt that many companies gather huge amount of client, scientific, sales and other details with regard to long-term evaluation. Traditionally, these types of companies have saved organized data in relational databases for long-term accessibility and evaluation. However, growing quantity of designers plus users has begun looking at various types of non-relational, right now frequently termed NoSQL databases. Different NoSQL databases carry various approaches. What we share can be that they are non-relational. Its major benefit is that contrary to relational databases, they hold unstructured information like files, mails and media efficiently. By using the advantages of NoSQL to migrate data, Nikam et al. introduce a framework that is helpful to map the MySQL query to MongoDB query format [9]. Soon after, it fetches the data faster by presenting a decision maker that chooses the database from which data can be fetched at a relatively faster rate, thus uplifting the system performance. The previous years have experienced an extreme rise in the quantity as well as the heterogeneity regarding NoSQL data stores [10]. As a result, researches along with comparison of such information stores have gotten difficult. Recently, several info-accessibility middleware programs with regard to NoSQL have emerged that include use of different NoSQL info stores out of standard APIs. Rafique et al. presented two complementary studies. First, Rafique et al. measure the efficiency overhead described by these systems for the CRUD operations. Second, costs of migration with and without these kinds of programs are usually compared.

3 Limitations of Earlier Work

Subsequent section describes the limitations of the existing work.

3.1 High Availability

When it is continuing to grow quickly, the NoSQL local community is actually innovative additionally along with falls short of the maturity on the MySQL end user base. Definitely, NoSQL will be quickly increasing, but it is experiencing the high availability issue.

3.2 Lack of Reporting Tools

The unavailability of reporting methods for evaluation and performance testing is the major issue with NoSQL databases. On the other hand, by using MySQL, you can acquire many reporting tools to aid you to validate your individual application's validity.

3.3 Lack of Standardization

To ensure that NoSQL is growing, it requires an average query language including SQL. This is a significant problem pointed out by experts at Microsoft, who seem to report that NoSQL's absence of standardization could cause an issue for the duration of migration. Apart from this, standardization will be very significant to the repository sector to be able to bring together themselves while in the future.

4 Proposed Methodology

This section contains the graphical representation of proposed technique, consisting of various steps which are required to successfully accomplish the suggested algorithm. Each time a checkpoint function happens, many unclean data file web pages for any repository are usually prepared for NoSQL web server (all web pages may have improved with memory since they were examined from NoSQL web server as well as the previous checkpoint), irrespective of the point of transaction that produced the particular transformation. Before the page is usually prepared for NoSQL web server, every log data including the new log data conveys a big difference for that web page that is usually prepared to NoSQL web server (yes, log records may be cached with RAM too).

Use of checkpointing:

- Preserve condition of task from steady intervals;
- Allow few CSP to supply higher access to your requests of clients in case of failure;
- Decrease the loss of calculations out while in the indication of failures.

To show the checkpointing structure, 2 metrics are used:

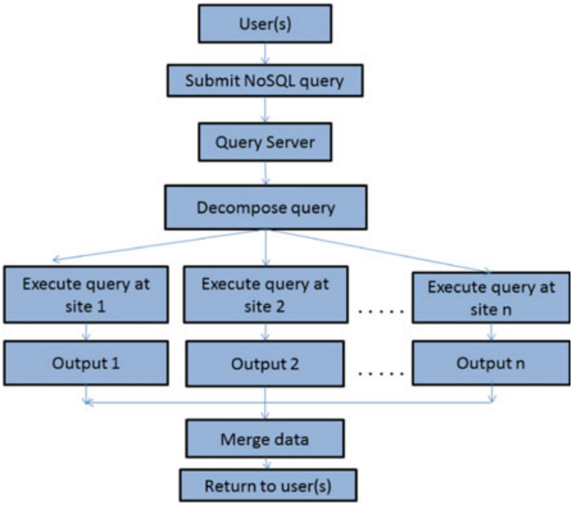
- Checkpoint overhead (due to checkpoint implementation, execution period of task is increased);
- Checkpoint latency (duration of their time needed in order to save lots of your checkpoints).

All the jobs are submitted by the clients to request manager. The given job is splitted into threads by request manager and also assigns one site (service manager) to threads and updating of global checkpoint took place. In First in First out (FIFO) fashion, the threads are selected by every site and casually loaded service node is assigned to it. That thread is executed by service nodes, or if the execution of any other thread is going on, then this thread may be added in its waiting queue. N1 in order to N12 is the service node which will supply services for the clients.

Algorithm:

- Step1: Clients send their tasks to distributed NoSQL service provider (DNSP) present at local site;
- Step2: DNSP split the task in threads. Then min loaded site is distributed to the jobs;
- Step3: After distribution of sites, updating of global checkpoint took place;
- Step4: Checkpoint will probably function periodically;

Fig. 1 Existing technique without failure



- Step5: By analyzing checkpoint DNSP, it checks whether any site has failed or no failure occurs. New save point is generated if no failure took place and checkpoint updating took place;
- Step6: The work is transferred from failed node to available site in case of failure and updating of checkpoint will take place.

Figure 1 shows the existing technique without failure. User submits the NoSQL query to the query server. Query server performed its job and it decomposes the query so that it can be run at their respective sites and generates the result. Later on, the output is fetched from each and every site so that final result is merged, and it will return back to the user. On the other hand, Fig. 2 describes what if the site 2 is crashed due to any reason. It will not generate its output. Other sites will wait for the output so that final result can be merged. This leads to increase the data retrieval time, and also, final result is not merged (Fig. 3).

This methodology introduces the checkpointing scenario.

The steps included are:

- Step1: Initially, the failures are monitored that are occurring due to any condition;
- Step2: Save the checkpoints that are used to recover the data later;
- Step3: If failure does not occur, it will return to the user back;
- Step4: If failure occurs, then rollback to save point is the phenomenon by which the availability of data got increased;
- Step5: If queries are terminated, the responses are automatically sent to the user, and if it is not, then repeat steps from starting.

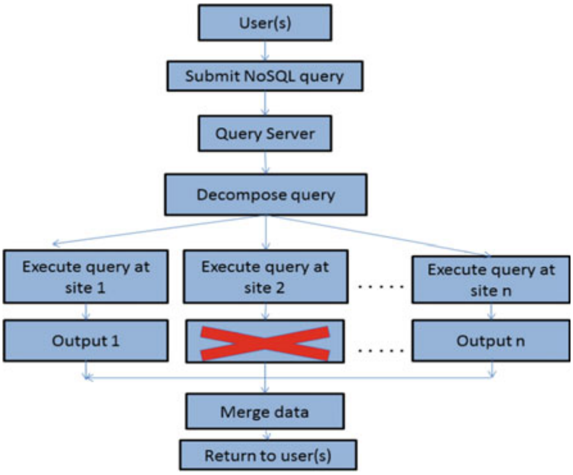


Fig. 2 Existing technique with failure

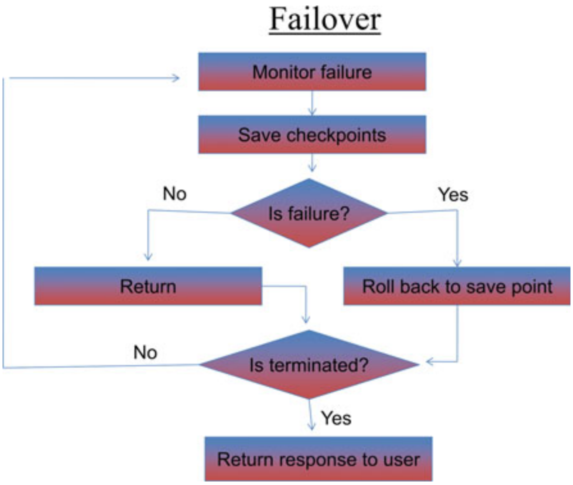


Fig. 3 Flowchart of proposed algorithm

Algorithm 1

```
$Algorithm\ initPPreDeCon\left(D_{buf}, d, \in, \mu, \lambda, €\right)$
    $/*\ every\ place\ in\ D\ is\ noted\ as\ unclassified\ and\ D_j\ is\ a$
    $collection\ of\ point\ Proce$
    $Processor\ n, 0 \le n < p\ do$
    $for\ each\ unclassified\ 0 \in D_{buf}\ do$
    $If\ \bar{C}_{ORE}{}^{pref}_{den}\ (h) then / * enlarge\ a\ new\ cluster * /$
    $build\ new\ microClus\ q - micro$
```

```
make new cluster ID
put entirey $\in \bar{N}_{\in}^{\bar{W}o}(h)$ in queueU;
While $U \neq \emptyset$ do
$p =$ initial point inU;
calculate $Z = \left\{ y \in D_{IR}R_{EACH_{den}^{pref}}(q, y) \right\}$;
for every $y \in Z$ do
if y is classified, in that case
put y in U;
allot present cluster ID to y
put y in microClus
eliminate p fromU;
otherwise
mark h as noise;
finish.
finish
Add $q - micro$ in $q - microClus$ record
finish.
//combine step
Processor $n$, $0 \leq n < P$ do
For every classified $m \in D_j$ do
if $|clusID| > 1$ in that case
//amount of clustered that point gets
put Min of them as clusID;
eliminate m point from microclus in record$l_j^p$
finish
```

Note: Q_Si = query size, QQ = query queue, QS = query status, AV_QQ = available query queue, AV_RS = available resources status, q_i = independent queries, R_CAP = resources capacity, vm = virtual machine, rvm = reconfigurable virtual machine, pr = available physical resources, mips = million instructions per seconds.

Algorithm 2

```
1. Initialize input parameters:
      $N_i \rightarrow$ Number of queries, $A_j \rightarrow$ arrival time of $N_i$, $rs \rightarrow$ resources
2. Sorting queries:
      $AV\_QQ[] = SORT[N_i, A_j]$
      $j = 0$;
      $AV\_RS =$ "ready"
      for every resources $R_s$ in resource group do
      while($R_s$ is in running state)
      skip and choose the next one
```

```
3. Select resources
      $If R_s[j] selected$
      $R_s selected[] = R_s[j]$
      $j + +;$
      $k = 0;$ //for every selected resources
4. Check query dependency:
      if (dependent queries in $R_s$ selected[])
      assign $AV\_QQ[k]$ to $R_s$ selected[]
5. Check available resources:
      if $(R\_CAP > Q\_size)$
      submit queries to selected resources
      elseif $(R\_ CAP < Q\_ size)$ &&$(AV\_ RS =$ 'terminated')
      make new vm to match the $Q\_Si$
6. Check vm status:
      If (vm failure = true)in that case
      make new vm from rvm
      check
      if (New vm's capacity(mips) $> Q\_Si$)
      assign queries
      otherwise

   6.1 make vm using one PR to satisfy the Q_size
         If $(Q\_size < avail\_(PR))$
         Create vm
         Update vm pool
   6.2 Create vm from combining PR to satisfy the Q_size
         //for$(i = 0; i < +n\_PR; i + +)$
         //for$(j = 1; j < n\_PR; j + +)$
         elseif $(avail\_(PR_{ij}) > Q\_size)$
         create new $vm_i + vm_j$

7. Check status of dependent queries:
      if $qs$ = executed process $Q_i$
      else
      repeat the process from step 5
8. Queuing independent queries based on priority:
      Select $Q_i$ and replicate the similar process from step 5
9. Check status of each and every query:
      If $(qs$ = executed & &$QQ$ = empty)
      then stop the process
```

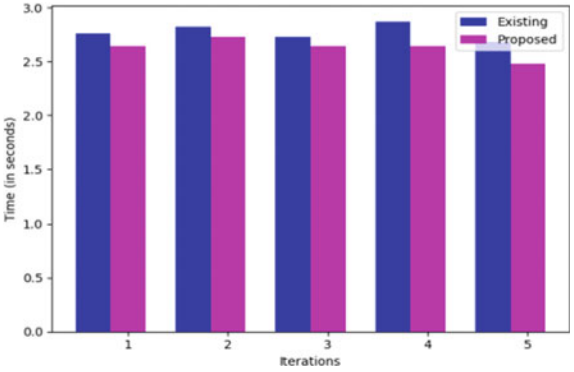


Fig. 4 Entire running time analysis

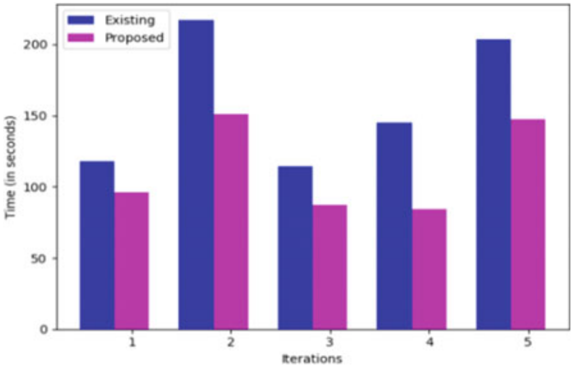


Fig. 5 Data retrieval time analysis

5 Results

This section defines the graph methodology by using the following parameters:

- Entire running time defines the time taken by the queries to give appropriate results according to the values;
- Data retrieval time defines the time at which the data is retrieved from the database management system and there are many options to store the retrieved data like files.

The comparison between the existing system and proposed system with respect to native query time, data retrieval time and entire running time is shown in Figs. 4 and 5.

6 Conclusion

A NoSQL checkpoint is a kind of test operation that verifies data retrieved from the database by comparing that data with the baseline copy stored in your project. That may be needed, for example, when you test an application that modifies a database and want to verify that the appropriate tables are updated correctly. Baseline data used by the checkpoint for verification is stored at middleware end. Each element contains connection settings for a database and a baseline copy of the data to be used for verification. Experimental results reveal that the proposed technique provides efficient results, especially in case of any kind of failures in distributed NoSQL servers.

References

1. Alomari E et al (2015) CDPort: a portability framework for NoSQL datastores. Arab J Sci Eng 40(9):2531–2553
2. Androcec D (2018) Data portability among providers o platform as a service. Res Pap Fac Mater Sci Technol Slovak Univ Technol 21(Special-Issue):7–11
3. Arora R, Aggarwal RR (2013) An algorithm for transformation of data from MySQL to NoSQL (MongoDB). Int J Adv Stud Comput Sci Eng 2(1):6–12
4. Atzeni P et al (2014) Uniform access to non-relational database systems: The SOS platform. Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence, Lecture Notes in Bioinformatics), vol 7328, pp 160–174
5. Chaure SD et al (2015) Web based ETL approach to transform relational database to graph database, 7
6. Leavitt N (2010) Will NoSQL databases live up to their promise? Computer (Long Beach Calif) 43(2):12–14
7. Lotfy AE et al (2016) A middle layer solution to support ACID properties for NoSQL databases. J King Saud Univ—Comput Inf Sci 28(1):133–145
8. Mior MJ et al (2017) NoSE: schema design for NoSQL applications. IEEE Trans Knowl Data Eng 29(10):2275–2289
9. Nikam P et al (2016) Migrate and map: a framework to access data from Mysql, Mongodb or Hbase using Mysql Queries. IOSR J Comput Eng 18(3):13–17
10. Rafique A et al (2018) On the performance impact of data access middleware for NoSQL data stores a study of the trade-off between performance and migration cost. IEEE Trans Cloud Comput 6(3):843–856
11. Rith J et al (2014) Speaking in tongues: SQL access to NoSQL systems. In: Proceedings of 29th Annual ACM Symposium on Applied Computing—SAC ’14, pp 855–857
12. Vathy-Fogarassy Á, Hugyák T (2017) Uniform data access platform for SQL and NoSQL database systems. Inf Syst 69:93–105

Implementation of Automated Bottle Filling System Using PLC

S. V. Viraktamath, A. S. Umarfarooq, Vinayakgouda Yallappagoudar and Abhilash P. Hasankar

Abstract Automatic bottle filling using programmable logic controller (PLC) constitutes a user-specified volume selection, in which the user can input the desired amount of liquid or water to be inserted in the bottles. It is generally used where many bottles of same volume are to be filled by passing bottles over the conveyor belt. PLC is a main functional block in the automation which tries to minimize the complexity and increases safety and cost reduction. Using of PLC in filling the bottles allows us to select the required amount of liquid by the ladder language. Filling is done by using motor, sensors, conveyor belt, PLC, solenoid valve, and so on. The whole system is more flexible and time saving. The process of filling is carried out for packaging of liquid and beverages. This is an interdisciplinary branch of engineering which includes mechanical, computer, and electronics parts. The process also enhances the knowledge of fabrication, programming, design, planning, and presentation skills. The PLC is gaining popularity because it is easy for troubleshooting which makes programming easier and reduces downtime.

Keywords Automation · PLC · Sensor · Solenoid valve · Glass motor

S. V. Viraktamath · A. S. Umarfarooq (✉) · V. Yallappagoudar · A. P. Hasankar
Department of E&CE, SDMCET, Dharwad, Karnataka, India
e-mail: umarfs0707@gmail.com

S. V. Viraktamath
e-mail: svvmath@gmail.com

V. Yallappagoudar
e-mail: vinayakgouda1997@gmail.com

A. P. Hasankar
e-mail: abhilashhasankar2@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_4

1 Introduction

Automation is the use of control system for operating equipment's and information technology with minimal or reduced human intervention in the production of goods and services [1, 2]. Apart from manufacturing, the automation has found a notable impact in industries. Automation has been achieved by various means including mechanical, hydraulic, pneumatic, electrical, electronic devices, and computers, usually in combination. Major part of the world economy is played by automation. Automation finds its application in the field where a liquid must be filled continuously for fixed interval or based on volume of the bottle such as soft drinks and other beverage industries [3, 4]. The work presented is an application of automation, and the processes are controlled using the PLC. The PLC that was used in this work is Rexroth-L20. This PLC operates on 24 V DC and variable number of inputs and outputs.

2 Literature Survey

Control engineering has been the best field of engineering [1–4]. In the past, humans were employed for controlling the system [5, 6]. Always, there is an eagerness in human beings to develop better technique in any working process to attain or to provide less mental stress and more comfort to the operators. The PLC is selected based on scan time, communication protocol, memory size, and software loaded into it. Nowadays, electricity is being used as control for automation, but in older days relays were used as control automation. Relays are very expensive, since they are mechanical devices it has limited usage and lifetime. The improvements of low-cost computers have changed trends in the automation fields. The programmable logic controller was started in the 1970s and has become the most common choice for the large-scale manufacturing controls in all automation industries [7, 8].

3 Component Description

3.1 Inputs

Infrared (IR) sensor is used as an input. An IR sensor is a device that senses changes in its surrounding. An IR sensor can sense the heat, and it can detect the motion. In our project, IR sensor is used to detect the bottle position [7]. The IR sensor is shown in Fig. 1.

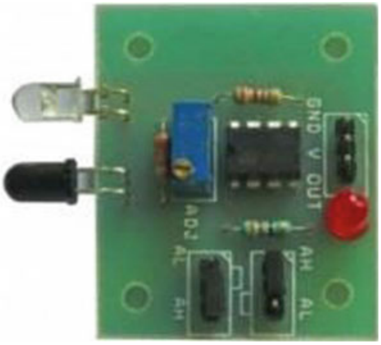


Fig. 1 IR sensor

3.2 Outputs

The various output devices used are motor and solenoid valve. The motor is used to drive the conveyor in forward direction. One end of solenoid is connected to the tank and other for filling process [9, 10]. A solenoid valve operates electromechanically. Electric current controls functioning of the valve. In fluidics, solenoid valves are used most commonly to control elements. Their functions are to close, open, distribute, or mix liquids. Solenoids offer good reliability, easy switching, compatibility with other devices, and small size. The solenoid valve is shown in Fig. 2.

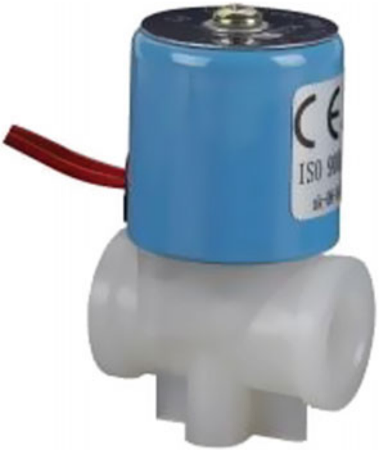


Fig. 2 Solenoid valve

3.3 Regulator

The outputs that are obtained from PLC cannot be directly fed to the output devices. Hence, regulators are used in order to supply with the amount of voltage that is required by the output devices. In this work, 12-V regulator has been used to step down the output from 24 to 12 for the motor that was used to drive the conveyor belt. The regulator is covered by a heat sink in order to control the amount of heat dissipated while transferring the regulator 7812 IC as shown in Fig. 3.

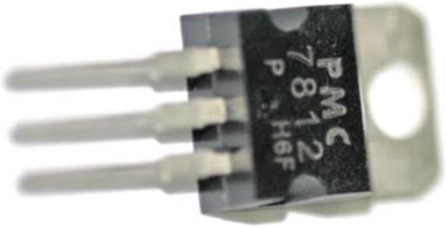
4 Methodology

Bottles are placed in required position on a conveyor belt. When the power is switched, the conveyor belt starts to move along with the bottles on it. Once the bottles appear in front of IR sensor which is placed to detect the bottle, conveyor belt stops making the bottle positioned still below the solenoid valve. After 7-s time interval, solenoid valve opens. This results in flowing of liquid from reservoir to bottle through solenoid valve. Up to 20 s, liquid will be continuously flowing into the bottle making it full. After 7 s, the conveyor starts to move and carries away the filled bottles unless and until next bottle is detected. This process continues till the power is on [11] as shown in Fig. 4.

5 Description

The filling operation takes place when the bottles are kept in sequential manner on a conveyor belt. The bottles are filled one at a time irrespective of number of bottles on the conveyor belt. The process is also provided with a volume defined by the user by adjusting the time interval provided to fill the bottle. The block diagram is shown in Fig. 5.

Fig. 3 7812 regulator



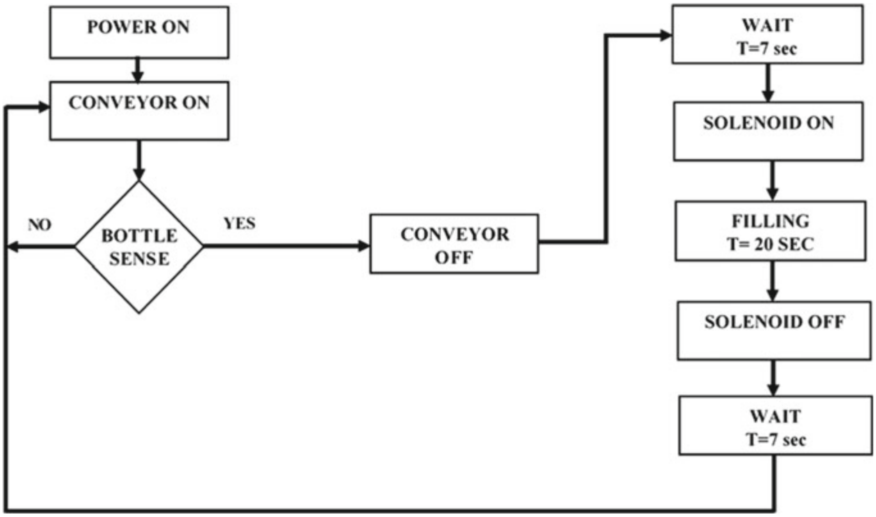
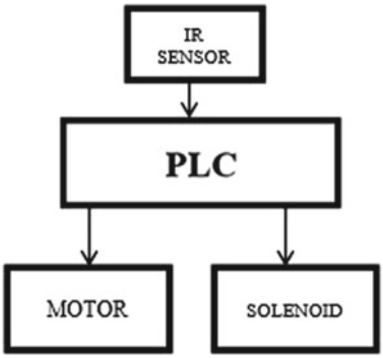


Fig. 4 Flowchart of bottle filling system

Fig. 5 Block diagram of PLC interfacing



5.1 Bottle Detection Using IR Sensor

Bottles are kept in position over the conveyor belt at the input side. IR sensors are used to detect the presence of bottles. The sensor will detect their position based on bottle motion. The IR sensor sensing the bottle is shown in Fig. 6.

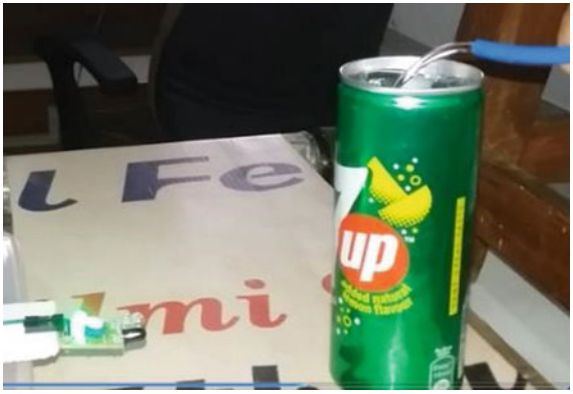


Fig. 6 IR sensor sensing the bottle and filling

5.2 *Bottle Filling Operation*

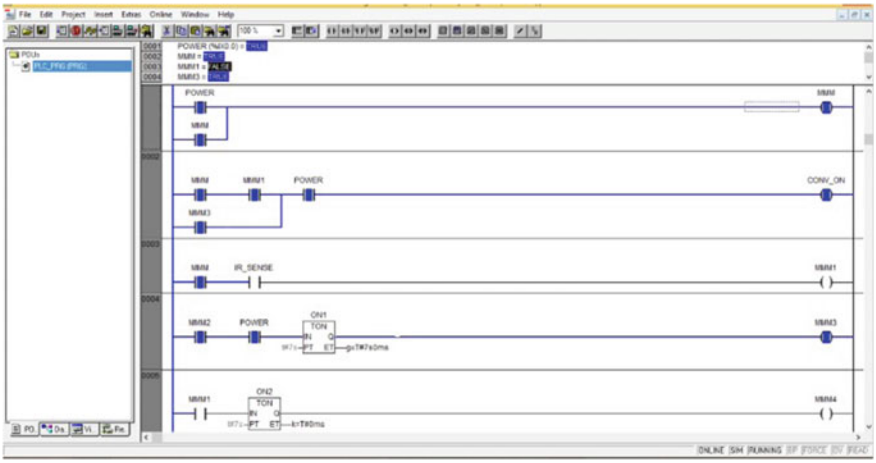
Once the bottles are in front of IR sensor, they are detected. Once the bottle reaches the desired position, the conveyor belt stops, and filling operation begins after 7 s of delay. Seven seconds of delay is provided to settle the bottle over the conveyor belt.

5.3 *Specified Volume of Liquid Introduced*

The filling operation is associated with the volume defined by the user. The desired volume of liquid is fed into the bottle depending on the volume that is already stored in the program. In this work, the preset value of timer is defined which ensures the solenoid opening for that time instant. This process continues until there are bottles on the conveyor belt. The overall setup is power dependent; hence, once the power is turned off, the system stops. When the bottles are on the conveyor and the power is on, the process of filling simply continues.

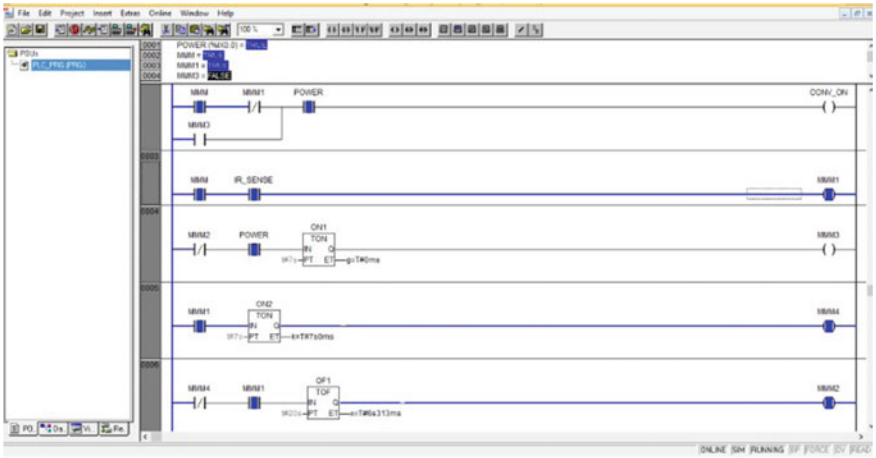
6 Simulation Results

a. When power is switched on, conveyor belt starts moving as shown in Fig. 7.
b. When IR sensor is on, the bottle is sensed as shown in Fig. 8.
c. Solenoid valve opens and closes after filling the bottle as shown in Fig. 9.



```
0001 POWER (%IX0.0) = TRUE
0002 MMM = TRUE
0003 MMM1 = FALSE
0004 MMM3 = TRUE
```

Fig. 7 Conveyor belt ON



```
0001 POWER (%IX0.0) = TRUE
0002 MMM = TRUE
0003 MMM1 = TRUE
0004 MMM3 = FALSE
```

Fig. 8 IR sensor is ON

7 Advantages

- Compact and Portable system [12].
- Economical system.

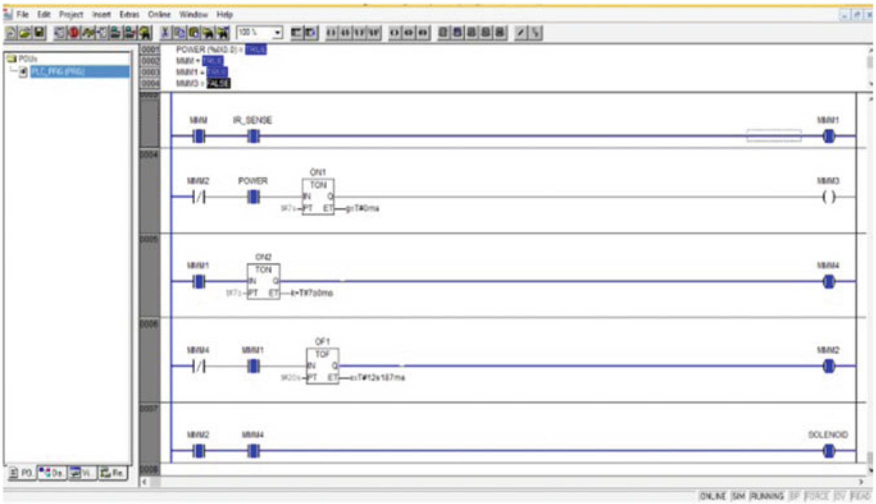


Fig. 9 Solenoid valve opens and closes after filling the bottle

8 Limitations

- It uses electronic components and circuits; any amount of water leakage will be dangerous.
- Using this system, only one bottle can be filled at a time.

9 Future Scope

As a future scope, the project can also be employed with various sizes, shapes, and weights of the bottles and densities of the liquid. A level sensor can be used to detect the level of liquid filled. Instead of filling one bottle at a time, it can be made to fill the multiple bottles at a time reducing the time, but design complexity increases. The process can also be extended to stuffing of definite quantity of capsules in bottles. The process can be made more efficient using flow sensor which detects the water flow. The process can be implemented on other controllers and the cost factors. The system can be made more feasible with advancement in technology. The automation system finds wide range of applications.

10 Conclusion

This paper describes a method to develop an automated bottle filling system based on user-defined volume. The process is controlled by PLC. The entire system is more flexible. Implementation of automated system increases the productivity and economy. The language used to design this model is easy and understandable by common people. This system can be used in every industry. With this work, it is possible to design other applications of automated system.

References

1. Somavanshi AP, Austkar SB, More SA (2013) Automatic bottle filling using microcontroller volume correction. Int J Eng Res Technol (IJERT) 2(3)
2. Saeed AUA, Al Mamun M, Zadidul Karim AHM (2012) Industrial application of PLCs in Bangladesh. Int J Sci Eng Res (IJSER) 3(6). ISSN: 2229-5518
3. Kalaiselvi T, Praveena R (2012) PLC based bottle filling and capping using user defined volume selection. ISSN: 2250-2459
4. Mashilkar B, Khaire P, Dalvi G (2015) Automated bottle filling system. IRJET 02(07). ISSN: 2395-0072
5. Chakraborty K, Roy I, De P (2015) Controlling process of a bottling plant using PLC and SCADA. Indonesian J Electr Eng Inf (IJEEI) 3(1):39–44. ISSN: 2089-3272
6. Boyer SA (2009) SCADA—supervisory control and data acquisition, 4th edn. International Society of Automation, USA
7. Ahuja H, Singh A, Tandon S, Shrivastav S, Patil S (2014) Automatic filling management system for Industries. IJETAE 4(Special Issue 1)
8. Dakre A, Sayed JG, Thorat EA, Chaudhary AMA (2015) Implementation of bottle filling and capping using PLC and SCADA. IRJET 02(9). ISSN: 2395-0072
9. Mallaradhya HM, Prakash KR (2013) Automatic liquid filling to bottles of different heights using programmable logic controller. ISSN: 23202092
10. Savita, Lokeshwar (2012) Implementation and performance analysis of bottle filling plant using ladder language. ISSN: 2319-7064
11. Patel J (2015) Based automatic bottle filling. ISSN: 2091-2730
12. Katre S, Hora J (2016) Microcontroller based automated solution filling module. Int Res J Eng Technol (IRJET) 03(05)

An Integrated Approach to Network Intrusion Detection and Prevention

B. Bhanu Prakash, Kaki Yeswanth, M. Sai Srinivas, S. Balaji, Y. Chandra Sekhar and Aswathy K. Nair

Abstract At present, with the expansion of size of the internet, security plays a crucial role in computer networks. Also with the advancement of Internet of things, earlier technology like firewall, authentication and encryption are not effective in ensuring the complete security. This has lead to the development of Intrusion Detection Systems (IDS) which monitors the events in computer networks to recognize the threats that violates computer security. With the help of various machine learning algorithms we have carried out the implementation of IDS. Machine learning technique increases the accuracy of anomaly detection in real-time scenario. This work focuses on K-Nearest Neighbor (KNN) classifier and Support Vector Machine (SVM), which classify the program behavior as intrusive or not. To prevent DoS (Denial-of-Service) attacks, a new method is implemented in this paper. The KNN classified data which provides malicious IP address are blocked in routers through Standard Access-list.

Keywords Computer security · Intrusion detection · KNN

1 Introduction

Computer security vulnerabilities prevail as long as we have flawed security measures, insecure software programs, weak authentication mechanisms, and network protocols. Almost all types of information are communicated and stored in public

B. B. Prakash (✉) · K. Yeswanth · M. S. Srinivas · S. Balaji · Y. C. Sekhar · A. K. Nair
Department of Electronics and Communications Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India
e-mail: bhanu_18@yahoo.com

K. Yeswanth
e-mail: kyeswanth1@gmail.com

S. Balaji
e-mail: balu9198@gmail.com

A. K. Nair
e-mail: aswathyscorp@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_5

switched communication network. This may lead to illegal interception, wiretapping and tampering thereby, damage the entire system that results in irreparable loss [1, 2]. Security products and Intrusion Detection System (IDS) are the existing methods to tackle the threats in computer networks. The latter is more intelligent as it gathers all the information and study the behavior and finally based on that it could characterize a program's normal behavior [3]. IDS detects network intrusions and protects the computer network from unauthorized access. It helps in distinguishing the bad connections called Intrusions and good connections [4]. The distinguishing is done by using different machine learning tools such as KNN-Classification, K-means clustering, and probabilistic measures [5]. The term machine learning is a branch of Computer Science that is closely related to data mining. It is a study of algorithms and statistical models to improve the performance of a specific task [6]. These algorithms are used in applications of Intrusion Detection in Computer Networks, spam emails and some other areas where it is impracticable to develop an algorithm for performing the tasks [7–9]. There are many ways in which the machine learns, but the three important ways are:

A. *Supervised Learning*

It is the branch of machine learning that maps an input variable (x) to an output variable (Y) based on the labeled training data. The algorithm is intelligent enough to map the function, $f(x)$ when we have a new input data, x and we could predict the output, Y. As the name implies the supervised learning algorithm acts as a supervisor which teaches the machine using well-labeled data and when a new set of data is given as input it could predict the correct output from labeled data [10, 7].

B. *Unsupervised Learning*

It is the branch of machine learning that tests the data which has not been labeled or categorized as in the case of supervised learning. Here the role of algorithm is to classify or group the unsorted data itself based on patterns, similarities or differences [11]. The algorithm has to draw the inference by itself from the data set and because of this such type of algorithm is used in exploratory data analysis.

C. *Reinforcement Learning*

It is the branch of machine learning that works on the principle of feedback of the data given. Reinforcement agent has to learn from the environment and it is bound to learn from its own experience [12]. There are various issues in intrusion detection that is still needed to be addressed in detail. This paper has adopted two methods. One is to detect the intrusion based on KNN algorithm. To increase the authenticity and reliability of the system a second phase of IP filtering technique is also added. The paper is organized as follows. Section 2 describes the methods adopted for intrusion detection. Section 3 gives the implementation method of the system and Sect. 4 discusses results and analysis and the paper is concluded with Sect. 5.

2 Methods Adopted

Intrusion detection is performed using KNN algorithm which is the simplest one and has less complexity compared to other algorithms. Using KNN classifier, it is able to classify the program behavior in the network as normal or intrusive. The KNN detection system is integrated with IP filtering technique that increases the reliability of the system. In IP filtering method, the system is designed to block the incoming connections which are malicious.

The data set for intrusion detection is obtained from KDD cup99 database which contains a large sample of attacked data set. For KNN based intrusion detection, the data set is split into training and testing data set using suitable split ratio. Based on the distance between the attributes, the class votes are given with respect to the majority. The Intrusive classes are classified out based on the attributes. After KNN classifier, an IP filtering is performed in the router. We have performed a simulation test network for IP filtering using Cisco Packet Tracer software. In Cisco Packet Tracer, IP address of malicious nodes are listed out and the router is bounded to filter out the malicious connection with the help of Internet Service Provider (ISP). These methods are given in Fig. 2.

*2.1 KNN (*K*-Nearest Neighbors)*

KNN is one of the simplest algorithms used for classification and it is also most used learning algorithm. KNN classifiers need two parameters: K value and threshold value. K value denotes the number of adjacent neighbors and threshold value is used for the judgment of abnormal neighbors. KNN uses the KDD CUP database which contains data points that are separated into two separate classes to predict the classification of a new data point. The model structure is formed from the data by providing data set along with training data. The KNN was initially executed for random samples in training set and having observed the accuracy, the same was performed on test data. The similarity between the know class and unknown class (unclassified) are identified using Euclidean-distance. Based on nearest neighboring (Euclidean distance) it allocates new unclassified data point to one of the cluster.

2.2 Cisco Packet Tracer-Blocking Malicious IP Address

Metropolitan Area Network and Malicious IP addressing is implemented in Cisco Packet Tracer. It is a Simulation tool that allows users to create their own network topologies. This software also allows user to simulate the configuration of router and switches using user interface and command-line interface.

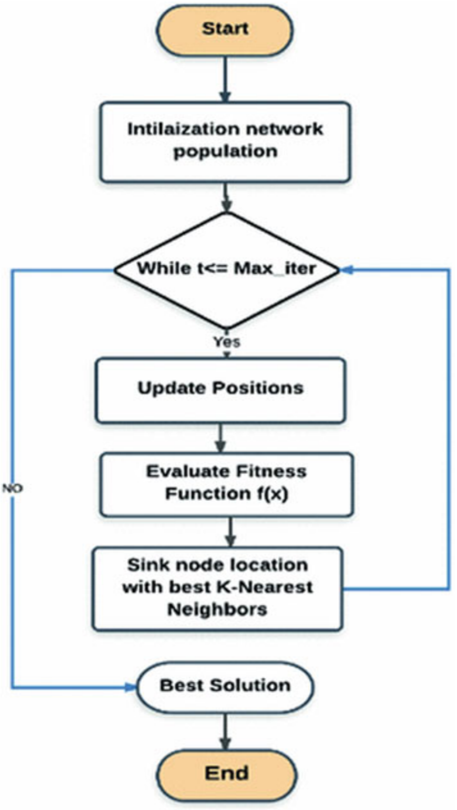

Start
Intilaization network population
While t<= Max_iter
Yes
NO
Update Positions
Evaluate Fitness Function f(x)
Sink node location with best K-Nearest Neighbors
Best Solution
End

Fig. 1 Flowchart of KNN

3 Implementation

3.1 KNN-Classification

The flow chart for KNN is shown in Fig. 1. We have implemented the *K*-Nearest Neighbor Algorithm with the combination of defining several methods

(i) *Importing Data*: We have defined a method in Python language to import the data in csv. format. This is for the ease of implementation so that we could extract the data set smoothly.

(ii) *Classifying the data into Training Set and Testing Set*: We have used the split ratio as 0.66:0.33; to split the data, and made use of an inbuilt-function random() which returns the next floating-point number in the range [0.0, 1.0). We have classified the data set into Training Set if the value of random.random is greater than the split value.

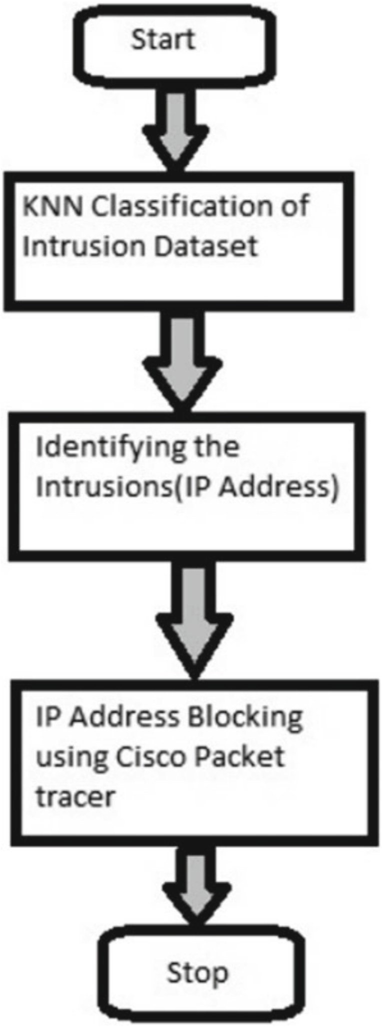
(iii) *Calculating the Euclidean-Distance*: Calculated the Euclidean-Distance by Implementing the Distance formula.

(iv) *Extracting the Neighbors based on the K value*: Calculated distances are sorted and the *K*-nearest neighbors are appended in a list. The *K* parameter plays an important role in this method.

(v) *Extracting the Response from the K-Nearest Neighbors*: Based on the majority votes from the neighbors, we return the most up-voted class as the predicted class.

(vi) *Calculating the Accuracy*: Based on the ratio of the correct value and predicted value the accuracy is measured.

Fig. 2 Overview of intrusion detection and prevention system


Start
KNN Classification of Intrusion Dataset
Identifying the Intrusions(IP Address)
IP Address Blocking using Cisco Packet tracer
Stop

3.2 IP Filtering

In this technique, the router will filter out the malicious IP address that is listed in the router local database before the route is announced. This is performed using Access Control List (ACL) that works like filters and deny the packet entering into the network. The ISP (Internet Service Provider) learns the blacklisted IP address that is not delegated by IANA (Internet Assigned Numbers Authority) and based on this router takes the decision for input filtering the malicious IP address. Establishing MAN in Cisco Packet Tracer using multistep procedure.

(1) *Assigning IP address and Configuration*: For proper communication in network, every Personal Computer (PC) is assigned with IP address, Subnet Mask, Default gateway. PC of same network ID are connected through Switch. Switches helps to forward the data between PCs and it also forwards and receives the data packets of Router. In this step, each PC, router, and gateway are assigned IP addresses.

(2) *Router Configuration*: Router helps to communicate between Remote Networks (PC of different Network). PC of one network tries to access web server located at another network, it should communicate through Routers. Every router forms its own routing table so that it provides path for data packet to reach destination. Each router has knowledge of only networks that are connected to it. So, in this step PCs belong to different networks are connected through routers. Default gateway at PC helps to reach the router it has connected. Also, configuration of router hops is performed in this step.

(3) *Connection Establishment*: Step1 and step 2 make successful connection establishment between PCs of different networks. In this step 3, we are going to check whether receiving data packets of one PC to another are in same network or in remote network through PING command. In cisco packet tracer every PC is provided with terminal. In that terminal ping IP address helps us to know whether proper network is established between them.

(4) *Malicious IP address detection*: Malicious IP Address blocking using Standard Access-list is performed here. In this step PC with malicious IP address are blocked in the router of sever located. Access Control List (ACL) works like filters and enables to control packets that is permitted in or denied out of a network. Every Router in Cisco packet tracer is provided with CLI (Command Line Interface). Commands for denying the IP address in router through standard access-list are en helps to enable the router, configure terminal helps us to configure terminal, sh access-lists gives list of access-list created, access-list no deny IP address wildcard subnet blocks the specified IP address the router, access-list no permit any permits all the IP address in network except the blocked IP address.

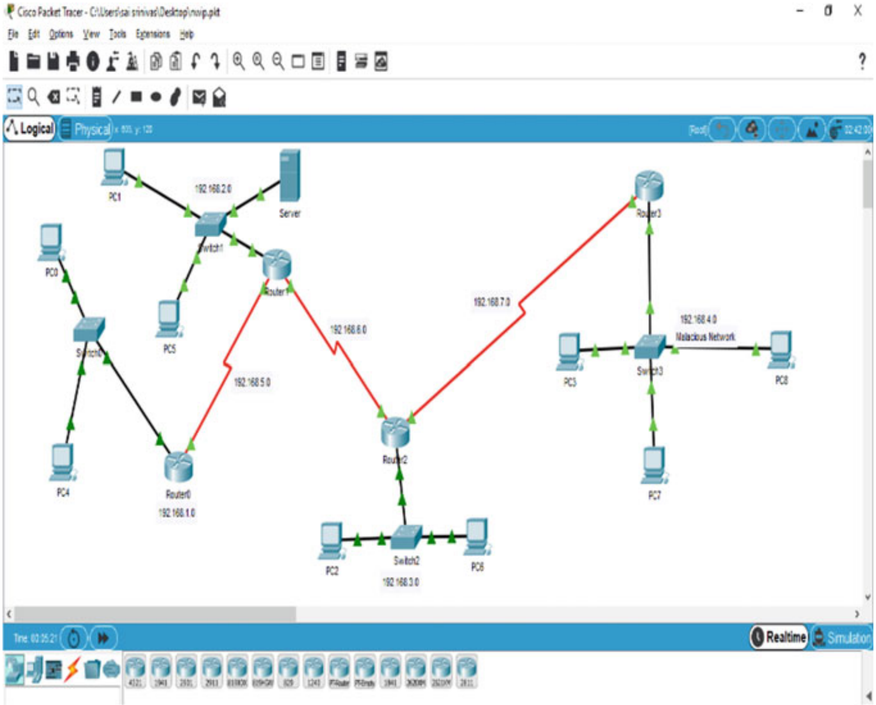


Fig. 3 Metropolitan area network in Cisco Packet tracer

4 Results and Analysis

The KNN classifier was run for different values of K, and for each K, the algorithm studies the network features and anomaly detection. After running the program multiple times, the best K value is chosen that gives less false rate. Simulation result of number of neighbors, K in KNN versus accuracy is plotted in Fig. 4.

The schematic diagram and configuration of a simulation test network using packet tracer is given in Fig. 3 Cisco Packet.

Based on several characteristics and observations, most reliable value of K (Nearest Neighbors) is chosen. Figure 4 shows the accuracy obtained from KNN which is 89.09%. The screenshot obtained from Python code is given as accuracy = 89.09 (Fig. 5).

Tracer is simulated in a Metropolitan Area Network (MAN). All communicating nodes in Metropolitan Area Network tries to access web server through Routers and Switches which are created in our simulation. So we identify the PCs with malicious IP address and block those PCs in Router. Figure 6 shows that connections from malicious node addresses to one of the PC is denied at the router.

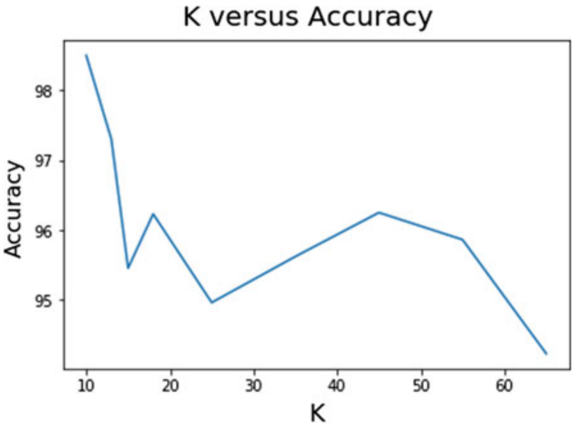
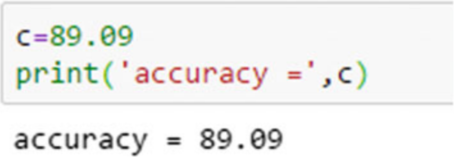


Fig. 4 Accuracy versus *K*-neighbors



```
c=89.09
print('accuracy =',c)
```

```
accuracy = 89.09
```

Fig. 5 Accuracy report of KNN algorithm

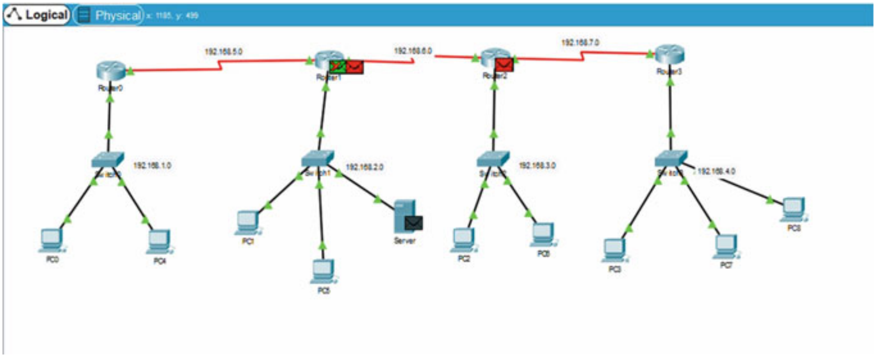


Fig. 6 Blocked IP address denied by router

5 Conclusion

In this project, we have used KNN algorithm for identifying the program behavior and label as intrusion or not. To increase the reliability of the system, an IP filtering technique is also integrated with the system. Using IP filtering the incoming connections which are malicious are blocked. For experimental findings, we have worked on Denial of Service (DoS) attack. Our results give a good accuracy for intrusion detection using KNN algorithm and decreased false rate. The work may be extended to time-stamping method for accuracy and better detection of DoS attack.

References

1. Prem Sankar AU, Poornachandran P, Ashok A, Manu RK, Hrudya P (2017) B-secure: a dynamic reputation system for identifying anomalous BGP paths. Adv Intell Syst Comput 515:767–775
2. Sankaran S, Sridhar R (2015) Modeling and analysis of routing for IoT networks. In: International conference on computing and network communications (CoCoNet). IEEE, Trivandrum, India
3. Hindy H, Brosset D, Bayne E, Seeam A, Tachtatzis C, Atkinson R, Bellekens X A Taxonomy and survey pf intrusion detection system, design techniques, network threats and datasets
4. Vijayarani1 S, Sylviaa M Assistant Professor and M. Phil Research Scholar from the Department of Computer Science Intrusion detection system a study. Bharathiar University, Coimbatore
5. Paliwal S, Gupta R (2012) Denial-of-service, probing remote to user (R2L) attack detection using genetic algorithm. Int J Comput Appl
6. Panda M, Patra MR Network intrusion detection using naive bayes. Department of E TC Engineering, G.I.E.T, Gunupur, India and from Department of Computer Science, Berhampur University, Berhampur, India
7. Zhang M, Xu B, Gong J (2015) An anamoly detection model based on one-class SVM to detect network intrusions. In: 11th conference on mobile ad-hoc and sensor networks
8. Xiaofeng Z, Xiaohong H (2017) Research on intrusion detection based on improved combination of k-means and multi-level SVM. In: K. Elissa (ed) 17th international conference on communication technology. Title of paper if known, unpublished
9. Ghanem K, Aparacio Navarro FJ, Chambers JA (2017) Support vector machine for network intrusion and cyber-attack detection. IEEE 2017
10. Seo J, Lee C, Shon T, Cho K-H, Moon J (2005) A new DDoS detection model using multiple SVMs and TRA, IFIP
11. Hutchins E, Cloppert M, Amin RM (2011) Intelligence-driven computer network defence informed by analysis of adversary campaigns and intrusion kill chains, USA. In: 6th International conference on warfare and security
12. Yan F, Jain-Wen Y, Lin C (2015) Computer network security and technology research. IEEE 2015

A New Design of Equiangular Circular Cum Elliptical Honeycomb Photonic Crystal Fiber

Ashish Jain, Ravindra Kumar Sharma, Vimal Agarwal and Sunil Sharma

Abstract The design of Silica Glass photonic crystal fiber is proposed for lowering the chromatic dispersion. For this design, Finite Difference Time Domain (FDTD) methodology along with the transparent boundary condition (TBC) is applied. This method produces zero dispersion at 0.5 to 1.5 μm diameter of circular and elliptical air holes. These types of PCFs have high potential as like the dispersion compensating fiber (DCF) in optical window. The refractive index is calculated with Sellmeier equation in this method which is equal to the conventional silica glass, i.e., 1.457. The proposed design is also used to show the non-linear effects of the material used.

Keywords Photonic crystal fiber (PCF) · Chromatic dispersion · Transparent boundary condition (TBC) · FDTD (Finite Difference Time Domain)

1 Introduction

Photonic crystal fibers are available as an independent and new technology which acts as a pioneered in the filled of communication. It was pinned by Phillip Russell. These are available in the form of a finite element, two-dimensional or three-dimensional photonic crystals that have a defect in the center core region. Basically the photonic crystals are classified into solid core and hollow-core fibers. Number of parameter can be varied to design a photonic crystal fiber. It includes the lattice symmetry structure, the hole to hole distance, i.e., pitch and hole size which can be varied by varying the diameter of hole. The solid core types of fibers shows a high-index profile of solid core with a lower effective index surrounding medium known as cladding. On the other hand the hollow core fibers have a lower index profile than

A. Jain · V. Agarwal
Apex Institute of Engineering & Technology, Jaipur, India

R. K. Sharma (✉)
Singhania University, Jhunjhunu, Rajasthan, India
e-mail: ravindra.8810@gmail.com

S. Sharma
Rajasthan Technical University, Kota, India

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_6

the surrounding medium of cladding. These Photonic crystals can be widely used as periodic optical nanostructures. They show high bandwidth range and lower attenuation characteristics. The optical transmission wavelengths available are 850, 1310, and 1550 nm.

2 Design Considerations for Fiber Optics

It is very important to know about design parameters before designing any type of fiber optic system. Some key factors must be taken into consideration for this design. The prime consideration of this design is to transmit lossless signals over the wide range of channels so that we can have a better reception of signals.

So we must be aware about:

- Modulation and multiplexing techniques that must be used.
- Enough signal strength or power level must be known of the receiver signal, i.e., power budget.
- Rising time along with bandwidth must be known.
- What type of fiber/amplifier is best suited for the application?
- Cost-Effectiveness.
- Design structure of the system.
- Dispersion profile of the system.
- Confinement Loss of the system.
- Refractive Index profile of material used for the system design.

Among all these parameter here we have consider dispersion, confinement loss, refractive index, and design structure for the proposed work.

3 Proposed Structure

The proposed structure is designed by considering various parameters like air hole diameter is varying from 0.5 to 1.5 μm range. The air hole spacing, i.e., pitch is maintaining at 2 μm for nine-layer structure (Fig. 1).

This proposed structure is used to minimize dispersion along with maintaining refractive index equal to the silica material, i.e., 1.457 (Figs. 2, 3).

Above Figs. 4, 5, 6 and 7 shows the 3D viewer of the proposed structure but with varying parameters. All the above-mentioned figures are showing changes with respect to change in dimensions and parameters selections. They also show variation in the amplitude and phase accordingly.

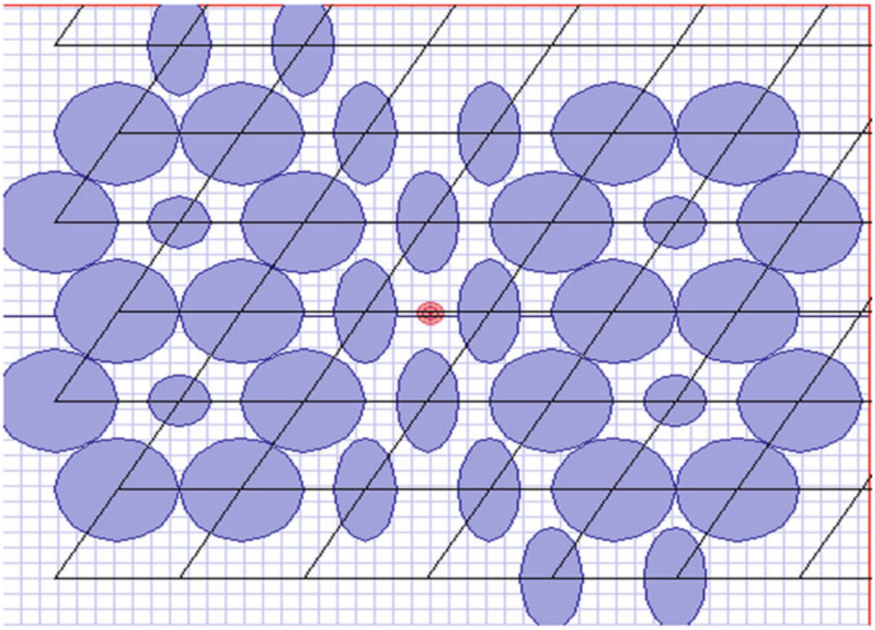


Fig. 1 Proposed structure of silica glass

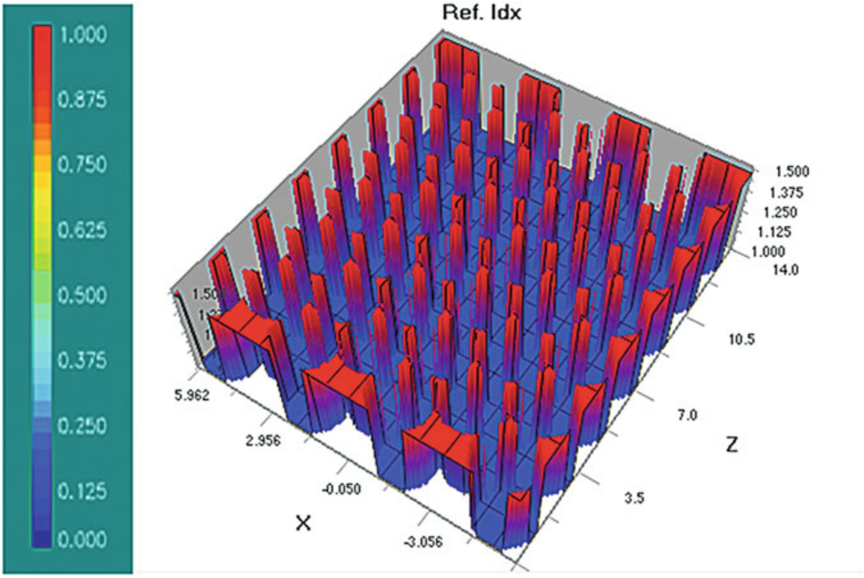


Fig. 2 2D structure of proposed design

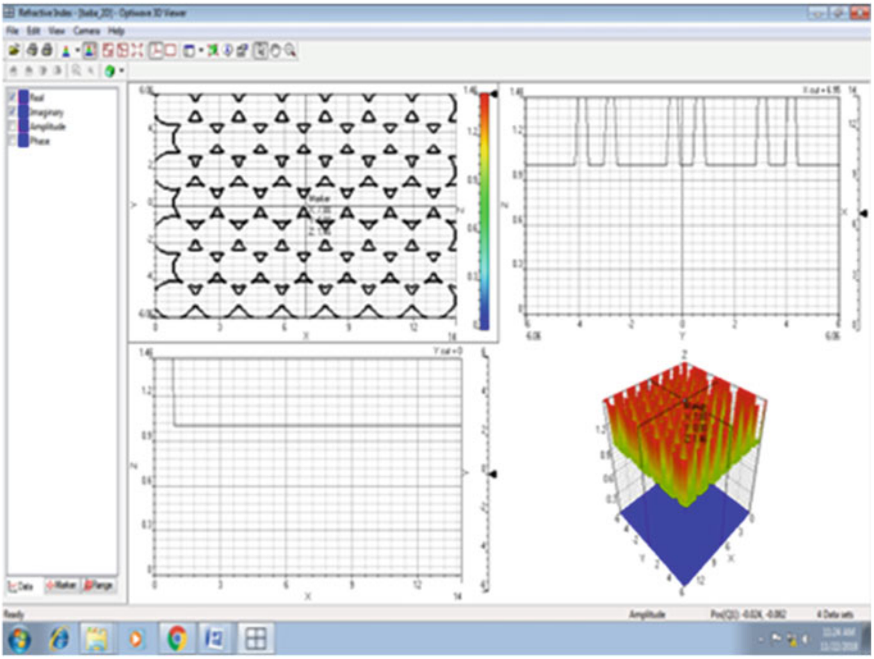


Fig. 3 3D viewer of proposed design

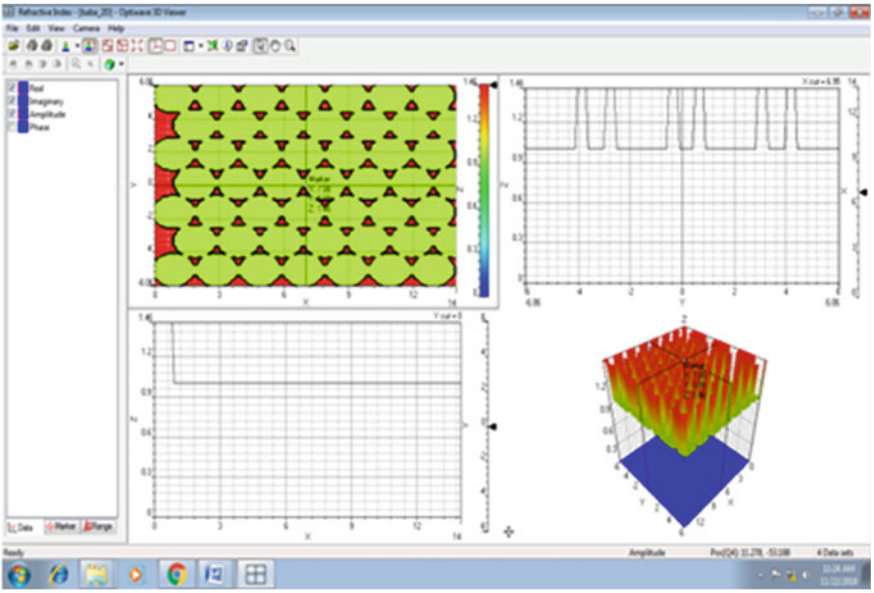


Fig. 4 3D viewer of proposed design

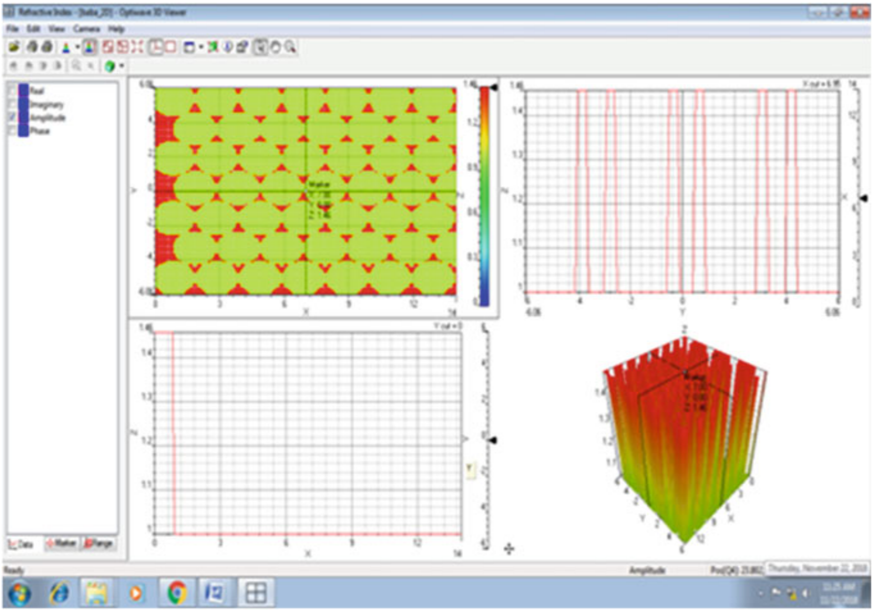


Fig. 5 3D viewer of proposed design

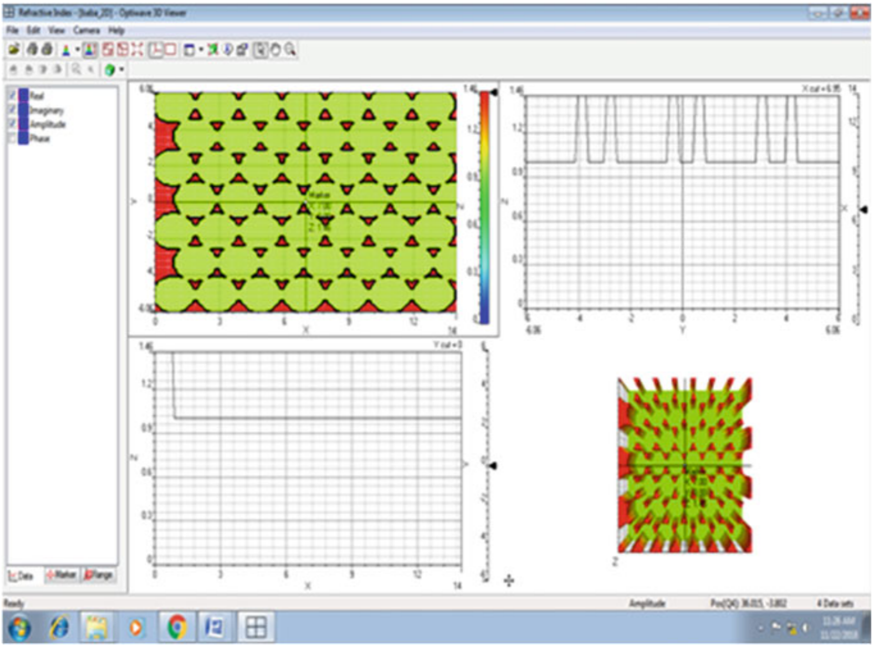


Fig. 6 3D viewer of proposed design

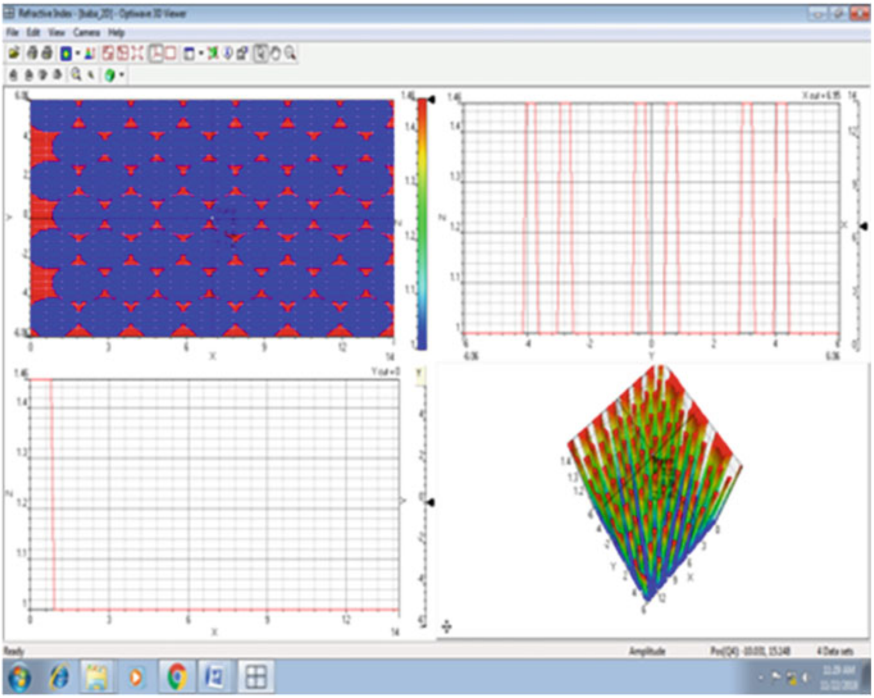


Fig. 7 3D viewer of proposed design

4 Results and Discussions

For the proposed structure of silica glass fiber, the dispersion is so obtained and a graph is plotted for the design which shows that it is zero for the selected diameter range. The variation of dispersion is shown below in Fig. 8.

The refractive index profile of the proposed structure is obtained and plotted in a graph which shows that it is quite similar to the silica glass, i.e., 1.457. It is shown above in the Fig. 9.

The transmission curve of the proposed structure is shown below in Fig. 10.

5 Conclusion

Finally, it is concluded that the fiber parameters selected are yield to optimize and analyze the best-suited results among the data available. The discrepancy may observe somewhere which is only due to higher wavelength region. Since we know that the refractive index profile of the material and the effective cladding index are wavelength dependent. It is also observed that silica glass PCF provides much better

Fig. 8 Dispersion obtained of proposed design

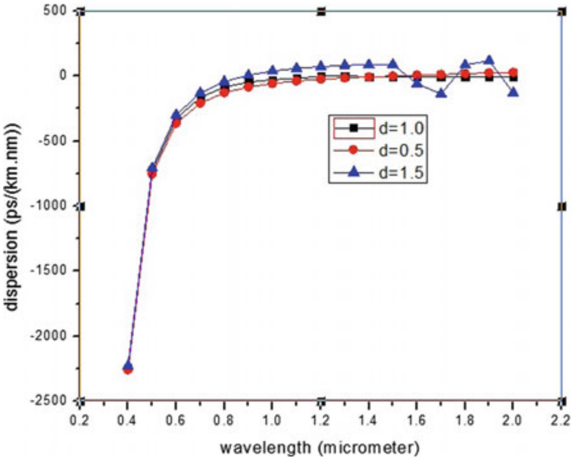


Fig. 9 Refractive index

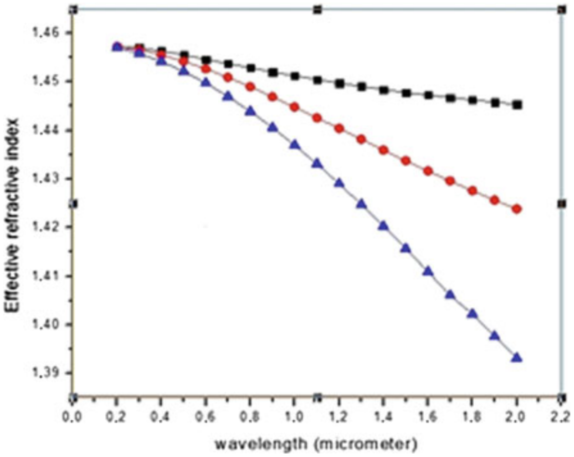
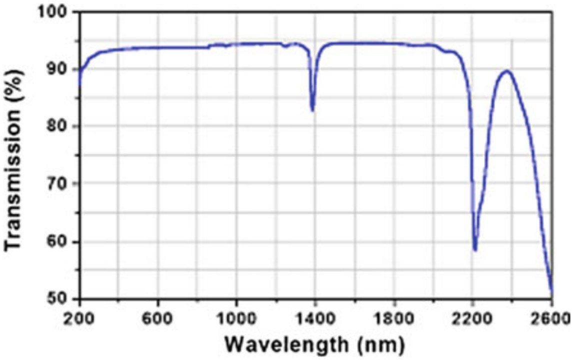


Fig. 10 Transmission curve of proposed design



dispersion results as compared to others of the same structure and parameters. Here we get nearly zero dispersion in between 0.6 and 1.6 μm wavelength region. We also have a refractive index of silica as 1.457 at 0.2–1.2 μm wavelength region. Around 90% data transmission capability is assumed with the proposed structure.

Survey of Different Countermeasure on Network Layer Attack in Wireless Network

Amruta Chavan, Dipti Jadhav, Nilesh Marathe and Nilima Dongre

Abstract In recent times, wireless network builds a bridge between the physical and virtual worlds. It poses security threats at different layers. The most vital security issue is observed on the network layer on different wireless networked systems. Defense mechanisms are used to shield the network layer from these repetitive malicious attacks. Malicious hubs are detected and differentiated along the network by using these mechanisms. These networks truly require a unified security answer for ensuring both course and information transmission tasks on the network layer. Without a suitable security solution, malicious nodes in the network can disturb rapidly across the network. This just irritates the system activity from exact delivery of packets and malevolent hubs that can disturb transmissions or drop all packets going through them. The main objective is to outline the different attacks and the countermeasures used to ensure the network security against pernicious attacks.

Keywords Security · Wireless network · Network layerattack · Countermeasure

1 Introduction

Security has been described as a safe environment to remain free from dangers posed by adversaries purposefully or unknowingly. With the recent technological advances, the systems never remain safe from assailants and from any unprotected framework

A. Chavan (✉) · D. Jadhav · N. Marathe · N. Dongre
Department of IT Engineering, RAIT, Nerul, Navi Mumbai, India
e-mail: amruta.chavan1994@gmail.com

D. Jadhav
e-mail: dipti.jadhav@rait.ac.in

N. Marathe
e-mail: nilesh.marathe@rait.ac.in

N. Dongre
e-mail: nilimraj@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_7

which can undoubtedly be disregarded from unapproved sources to take the data for malignant purposes.

Network security alludes to the usage of network management for monitoring and specialized measures to guarantee that information protection, integrity, and accessibility, which can be ensured in a network domain. The security of the PC network covers two viewpoints: physical safety and logical security. However, the network suppliers are concerned with network data security, as well as how to manage sudden catastrophic events, for example, a military strike against system equipment harm, and how to reestablish network communication and keep up network communication coherence in unusual circumstances.

The main advantage of a wireless network over a wired network is that the users can move freely within the network with their wireless devices and access the internet wherever they need. Users are allowed to share files between devices without a physical connection. The installation time and cost of wireless networks are low when compared to wired networks. In addition to these advantages, the wireless networks are prone to several vulnerabilities discussed in subsequent sessions.

1.1 The Need for Security

The security is needed for the following given reasons:

- To protect vital information while still enabling access to trading secrets, medical records, etc.
- To provide resource authentication and access control.
- To guarantee resource availability.

2 Analysis of Different Attack on Network Layer

2.1 Attacks

1. **Blackhole Attack**. In this assault, a pernicious node drops all data packets through this as matter and energy go away in a black hole from our universe. In the event, the assault node is connected between nodes of two parts of that arrange, isolates the network, it separates the network effectively into two disengaged segments. All of the data from the fooled neighbor is sent to the deceitful node instead of the destined base station. The sensor network's specialized communication pattern and multi-hop nature make it susceptible to this attack.
2. **Wormhole Attack**. This type of assault involves receiving information packets on some point and invokes them to a different fake node. There is a channel or tunnel between the two nodes called a wormhole attack [1]. The tunnel forms

between one or more malicious nodes during this attack. The distant nodes appear as close neighbors so that this node's energy resources are quickly exhausted. This attack is effective when combined with selective forwarding and Sybil attack, where detection is very difficult.

3. **Sybil Attack**. The attacker fools neighboring nodes with several identities [2]. By hacking the identities of the neighboring nodes, the attackers have access to the corresponding node information. A defective hub or an opponent might have several identities into show up and work as various separate nodes. The opponent can then overhear communication or act maliciously after becoming part of the network. The enemy can control the network significantly by displaying multiple identities [3].
4. **Grayhole Attack**. The assailant draws in the information packets by publicizing himself the smallest way to the goal and after that captures and drops the information packet. This assault is otherwise called a misbehavior attack, which prompts to messages being dropped. The hubs drop the packets selectively in this attack [4]. In the main phase, the hub advertises itself as having a substantial route to the destination, while in the second phase, the hubs drop intercepted packets with a specific likelihood.
5. **Denial of Service Attack**. An opponent tries to disturb communication in a network by flooding the network with a large number of packages, for example. When a service attack is denied, the attackers try to temporarily make the network resources or a node or machine unavailable to their actual users. They send false requests to the target so that it is unavailable to serve its intended users. The target may be temporarily down or destroyed in such attacks. The routing process can be interrupted on the network layer by changing the packet control routing, dropping selectively, overflowing the table or poisoning [5].
6. **Selective Forwarding Attack**. In this attack, only certain packets are selectively dropped by a malicious node. Usually, messages received are faithfully forwarded by nodes in sensor networks. The message or information received and sent should be the same for reliable and secure communication. When some compromised node refuses to forward and this result in loss of important data [2].
7. **Information Disclosure Attack**. During the communication process, every confidential exchange of information must be protected. Critical information stored in nodes must also be protected against unauthorized access. Control data are sometimes more important for safety than traffic data. A node may release secret or critical information into unapproved network hubs. Such data may contain data on the topology of the system, the geographical area of hubs or ideal routes to authorized hubs in the system.

Table 1 Comparative study of attacks in network layer

Types of attacks	Attack threat	Affects on	Purpose	Attack goal
Sybil	Availability, authenticity, integrity	Routing, voting, fair resource allocation, distributed storage	Unfairness; disrupt the authentication	Control traffic attack
Warm hole	Confidentiality, authenticity	Reveres engineering, cipher breaking	Unfairness; disrupt communication to be authenticated	Control traffic attack
Selective forwarding	Availability, integrity	Multi-hoping protocols	Unfairness	Data traffic attack
Dos attack	Availability, integrity, confidentiality, authenticity	Essential services	Disrupt service to be authenticate	Control traffic attack
Gray hole	Availability, authenticity, integrity	Normal communication, network node, network partition	Unfairness	Data traffic attack
Information disclosure	Confidentiality, authenticity	Normal communication	Disrupt communication to be authenticate	Data traffic attack

2.2 Comparative Study of Attacks in Network Layer

As network layer is susceptible against dissimilar routing assaults, they can gain access to routing paths and redirect the traffic, propagating fake routing information into the system. The following Table 1 compares routing attacks on the network layer based on a threat model, purpose, and security services.

3 Countermeasure Against Attack of Network Layer

3.1 Protection Against Blackhole Attacks

A Detection, Prevention and Reactive AODV (DPRAODV) are considered a black hole attack countermeasure. Topology graph-based anomaly detection (TOGBAD) is planning a new centralized approach for identifying hubs attempting to make a black hole. Adhoc routing protocol (SAR), which can be utilized to protect beside black hole attacks, is also proposed. The black hole is a kind of steering attack in which a vindictive node has the shortest route to all hubs in the earth by sending a phony course response Thus, the noxious hub can deny the first hub traffic.

DPRAODV (Detection, Prevention, and Reactive AODV): In the Detection, Prevention and Reactive AODV protocol, the threshold value is dynamically updated [2]. It is intended to counteract black hole security dangers by telling different hubs in the occurrence network. It also hinders the rehashed response from the malevolent hub by diminishing system activity and in this manner, it disconnects the malignant hub from the network. The results of the simulation in NS2 show that this convention anticipates black hole attacks as well enhances the general execution of (typical) within the sight of black hole attacks.

TOGBAD: It a new concentrated methodology utilizing topology diagrams to detect black hole nodes. Utilize entrenched strategies to pick up learning of network topology and utilize this information to perform believability minds on the routing data spread through the network hubs. In this methodology must consider a hub that generates false data about routing as pernicious. So, if the plausibility check fails, this method must trigger an alarm. In addition, a hopeful first recreation result is present. With this new methodology, the attempt to create a black hole can already be detected before the actual impact before the genuine effect takes place.

SAR (Security-Aware Ad Hoc Routing Protocol): It can be utilized to secure beside black hole attacks. The ad hoc routing protocol for security-aware depends on request protocols, for example, AODV or DSR. In the greater part of the routing protocol, they primarily expect to discover the most routes from source to goal, which is the length of the route only. A security metric is extra to the RREQ bundle in SAR and another route detection process is utilized. Intermediate hubs get an RREQ bundle at a certain level of security or hope. In the event that the security metric or hope level is fulfilled in intermediate nodes, the hub processes the RREQ bundle and propagates it to its neighbors by means of prohibited floods. If not, the RREQ bundle is dropped. If you can find a way with the required security properties, the target will create an RREP bundle with the particular security metric. In the event that the destination node does not discover a course with the required level of security or confidence, it sends a warning to the sender and allows the sender to the sender and enables the sender to modify the dimension of security to discover a route.

3.2 Protection Against Wormhole Attacks

To prevent the wormhole attack, WAP (Wormhole Attack Prevention) without utilizing particular equipment is proposed. A TrueLink mechanism, a planning-based defense for the wormhole assault is proposed. A packet with a leash protocol is considered a treatment to the wormhole. The SECTOR component is proposed for recognizing wormholes without synchronization of the timer. Directional antennas are likewise designed to avert attacks with the wormhole.

Wormhole Attack Prevention (WAP): To prevent the wormhole attack, WAP without utilizing particular equipment is planned. Not exclusively does the WAP detect the phony route, but it also takes defensive measures next to the reappearance of wormhole nodes amid the disclosure phase. The consequences of the simulation demonstrate that wormholes can be detected and remotely detected during the route detection stage.

Packet Leashes: Packet leashes for detecting wormhole attacks are proposed [6]. Mainly leashes mean a packet which limits a packet's maximum transmission space. A transitory packet leash sets a limit to a packet's lifetime, which adds a limit to its movement remove. A sender incorporates the time and area of transmission in the note. The recipient checks if the packet has ventured to every part of the separation between the sender and itself inside the period among receipt and transmission. Transitory packet leashes require tight tickers and exact area information. In geographic leashes, ensure that the receiver of the packets is some tickers and exact area information. The area data and inexactly synchronized timekeepers confirm the neighboring relationship in geographical leashes.

SECTOR Mechanism: This mechanism is primarily founded on separation bordering procedures single-way hash chains and the hash tree of Merkle. It can be used with no clock synchronization or area information to avoid wormhole attacks on the Wireless network. It can also be utilized to anchor routing protocols in the wireless network through recent encounters and to detect checks through topology following.

3.3 Protection Against Denial of Service Attacks

A DoSP-MAC convention is proposed to enhance network equality. A new firewall-based format is offered as a countermeasure. In order to prevent a DoS attack, a DoS moderation procedure utilizing a digital signature is proposed. Efficient on-the-fly search technology to track DoS attackers was also proposed.

DoSP-MAC Protocol: The execution of the MAC (Media Access Control) protocol in wireless networks majorly affects generally network performance. In MAC protocols dependent hubs' access to the common channel isn't synchronized and they battle for the channel when packets are ready to be sent in their buffers. The quick forward mechanism and the quick trade system are used to reduce self-contention; however, these mechanisms exacerbate the issue of equality. It will, in this manner, prompt refusal of DoS attacks on the grounds that the last champ is constantly supported among neighborhood battling nodes, a continually transmitting node can generally catch the channel and cause other nodes to perpetually disappear. In this context, a DoSP-MAC protocol is proposed to enhance the reasonableness of the network in order to improve its execution. This can enhance the medium usage dramatically [7].

Novel System: A novel system dependent on a firewall. This firewall can discriminate against the assault packets from the bundles sent by authentic clients dependent on the packet's stamping quality and along these lines sift through the greater part of the assault packets. Our system is very efficient and has a very low cost of deployment compared to other package marking solutions. In implementing this scheme, only about 10% of Internet routers would need to cooperates in the checking procedure and servers would need to make encrypted markings for secure transmission [6]. The plan enables the firewall to be identified and keeps the first packet assaults on the DDoS [8, 9].

Mitigation Technique: The digital signature mitigation method for confirming legitimate packets and crash packets that do not pass the verification. Since nodes are narrowing minded, they can't verify the overhead so they can abstain from paying. A terrible packet escaping verification throughout the entire network way will carry a punishment for all its forwarders. A network diversion can be developed in which hubs along a system way are urged to act all in all to modify terrible packets with the end goal to improve their very own advantages. Analytical outcomes show that Nash balance can be achieved for players in the proposed game, in which important advantages can be given to with the goal that a significant number of the terrible packets are verified.

4 Comparison of Different Countermeasure Techniques

Table 2 describes the attack type, merits, demerits and detection mechanism used in each technique. Here each technique is proposed in order to detect and prevent attacks at the network layer.

5 Conclusion

Although there are many strategies to counter security attacks, technological upgrades are still required. The attacks act against secure communication data availability target. They drain the energy of the nodes and reduce the life of the network. In this report, we endeavored to examine attacks and presented countermeasures of security attacks on the network layer in the wireless system. Existing network layer attacks like Sybil attack, Wormhole attack, Dos Attack, Selective forwarding attack, Grayhole attack, and Information Disclosure attack are analyzed. These attacks affect voting, routing, network resources, multi-hope protocols and so on. A comparative study of the network layered attacks is based on the security classes, the location of security, the nature of the attacker, the target of the attacker. In future, based on the analysis of these vulnerabilities, an efficient intrusion detection mechanism can be proposed to overcome most of these attacks.

Table 2 Comparison of different countermeasure techniques

Name of algorithm	Attack type	Detection technique	Merits	Demerits	Remark
DPRAODV	Blackhole	Checks if the destination sequence number of RREP is higher than the threshold value or not	Blackhole detection	Identifies normal node as a malicious node and enter to blacklist ALARM broadcast make network overhead	Fixed the threshold value
TOGBAD	Blackhole	Compares the number of neighboring nodes it has with a number of neighboring nodes in accordance with topology graph	Blackhole detection	The method is ineffective in reacting protocol	Decrease delay time
SAR	Blackhole	Nodes checks if security metrics or requirements are satisfied or not	Blackhole detection	Cannot guarantee shortest route discovery	Decrease detection time
TELSA	Wormhole	Checks if the recipient is in certain distance or not	Wormhole detection	Strict requirements in timing	Detect in required time only
SECTOR	Wormhole	Bounding maximum distance between two neighboring nodes by series of fast one-bit exchange	Wormhole detection	Need special hardware to ensure the accuracy of time	Maintain the accuracy
DoSP-MAC protocol	DoS	Nodes access to the shared channel is not synchronized, and they contend for the channel whenever there are packets in their buffers ready to be sent	DoS detection	exacerbate the issue of equality	Improve equality of network services

(continued)

Table 2 (continued)

Name of algorithm	Attack type	Detection technique	Merits	Demerits	Remark
Novel system	DoS	Compared to other packet-marking based solutions	DoS detection	Enables to be identified and keeps the first packet attack on the DDoS	Improve detection framework
Mitigation technique	DoS	The digital signature mitigation method to confirm legitimate packets and crash packets that don't pass the verification	DoS detection	Confirm only legitimate packets	Maintain packet delivery ratio

References

1. Singh RK, Nand P (2016) Literature review of routing attacks in MANET. In: 2016 international conference on computing, communication and automation (ICCCA). Noida, pp 525–530. https://doi.org/10.1109/ccaa.2016.7813776
2. Meddeb R, Triki B, Jemili F, Korbaa O (2017) A survey of attacks in mobile ad hoc networks. In: 2017 international conference on engineering & MIS (ICEMIS). Monastir, pp 1–7
3. Yao et al Y (2018) Multi-channel based sybil attack detection in vehicular ad hoc networks using RSSI. In: IEEE Trans Mob Comput. https://doi.org/10.1109/tmc.2018.2833849
4. Kumar S, Goyal M, Goyal D, Poonia RC (2017) Routing protocols and security issues in MANET. In: 2017 international conference on Infocom technologies and unmanned systems (trends and future directions) (ICTUS). Dubai, pp 818–824
5. Wang Q, Dunlap T, Cho Y, Qu G (2017) DoS attacks and countermeasures on network devices. In: 2017 26th wireless and optical communication conference (WOCC). Newark, NJ, pp 1–6
6. Korde S, Sarode MV (2017) Review on network layer attacks detection and prevention techniques in mobile ad hoc networks. In: 2017 international conference on inventive systems and control (ICISC). Coimbatore, pp 1–5
7. Chang S, Hu Y (2017) SecureMAC: securing wireless medium access control against insider denial-of-service attacks. IEEE Trans Mob Comput 16(12):3527–3540
8. Simpson S, Shirazi SN, Marnerides A, Jouet S, Pezaros D, Hutchison D (2018) An inter-domain collaboration scheme to remedy DDoS attacks in computer networks. IEEE Trans Netw Serv Manage 15(3):879–893
9. Wang A, Chang W, Chen S, Mohaisen A (2018) Delving into internet DDoS attacks by Botnets: characterization and analysis. In: IEEE/ACM Trans Netw. https://doi.org/10.1109/tnet.2018.2874896
10. SunilKumar KN, Shivashankar (2017) A review on security and privacy issues in wireless sensor networks. In: 2017 2nd IEEE international conference on recent trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, pp 1979–1984. https://doi.org/10.1109/rteict.2017.8256945
11. Zhang L, Nie G, Ding G, Wu Q, Zhang Z, Han Z (2018) Byzantine attacker identification in collaborative spectrum sensing: a robust defense framework. In: IEEE Trans Mob Comput. https://doi.org/10.1109/tmc.2018.2869390

12. Surya SR, Magrica GA (2017) A survey on wireless networks attacks. In: 2017 2nd international conference on computing and communications technologies (ICCCT), Chennai, pp 240–247
13. Soliman JN, Mageed TA, El-Hennawy HM (2017) Countermeasures for layered security attacks on cognitive radio networks based on modified digital signature scheme. In: 2017 eighth international conference on intelligent computing and information systems (ICICIS). Cairo, pp 2–8
14. Kumar P, Tripathi M, Nehra A, Conti M, Lal C (2018) Safety: early detection and mitigation of TCP SYN flood utilizing entropy in SDN. In: IEEE Trans Netw Serv Manage. https://doi.org/10.1109/tnsm.2018.2861741
15. Deeksha AK, Bansal M (2017) A review on VANET security attacks and their countermeasure. In: 2017 4th international conference on signal processing, computing and control (ISPCC). Solan, pp 580–585
16. Santhi G, Sowmiya R (2017) A survey on various attacks and countermeasures in wireless sensor networks. Int J Comput Appl 159(7):0975–8887
17. Sinha P, Jha VK, Rai AK, Bhushan B (2017) Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: a survey. In: 2017 international conference on signal processing and communication (ICSPC). Coimbatore, pp 288–293. https://doi.org/10.1109/cspc.2017.8305855
18. Tomić I, McCann JA (2017) A survey of potential security issues in existing wireless sensor network protocols. IEEE Internet Things J 4(6):1910–1923. https://doi.org/10.1109/JIOT.2017.2749883
19. Chen K, Zhang Y, Liu P (2018) Leveraging information asymmetry to transform android apps into self-defending code against repackaging attacks. IEEE Trans Mob Comput 17(8):1879–1893
20. Moudni H, Er-rouidi M, Mouncif H, Hadadi BE (2016) Secure routing protocols for mobile ad hoc networks. In: 2016 international conference on information technology for organizations development (IT4OD). March 2016, pp 1–7
21. Moubarak J, Filiol E, Chamoun M (2018) On blockchain security and relevant attacks. In: 2018 IEEE middle east and north africa communications conference (MENACOMM). Jounieh, pp 1–6. https://doi.org/10.1109/menacomm.2018.8371010

Internet of Things: Service-Oriented Architecture Opportunities and Challenges

G. R. Sagar and N. Jayapandian

Abstract "Internet of Things" is now a subject that is increasingly growing on both the job and modern devices. It is a concept that maybe not just get the potential to influence how we live but in addition how we work. Intelligent systems in IoT machines in many cases are used by various events; consequently, simultaneous information collection and processing are often anticipated. Such a characteristic that is exclusive of systems has imposed brand new challenges towards the designs of efficient data collection processes. This article is to be discussing various layers in Internet of things. Those layers are sensing layer, network layer, service layer and application layer. Various data processing techniques are integrated along with data filtering and data conversion. Protocol transformation is also feeling the major challenges faced by enterprises wanting to shift to the style in brand new technology.

Keywords Internet of things · Service-oriented architecture · Security · Protocol · IoT layers

1 Introduction

The shift is in regards to both understanding and thinking about IoT. The IoT is holds: IoT is really a network of connected devices which includes unique identifiers in respect of an IP along with inbuilt technologies which help them to collect, feeling information and communicate about the surroundings by which they prevail. But within the broader sense and between the shifts pointed out, the IoT definition does matter much if not seen with a bigger viewpoint [1]. Now it is perhaps not the proper time for definitions, and it is time for development, value, business and IoT in action. Over the last few years, there has been a great development in the area of

G. R. Sagar · N. Jayapandian (✉)
Department of Computer Science and Engineering, CHRIST (Deemed to Be University), Kengeri Campus, Bangalore, India
e-mail: jayapandian.n@christuniversity.in

G. R. Sagar
e-mail: sagar.r@btech.christuniversity.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_8

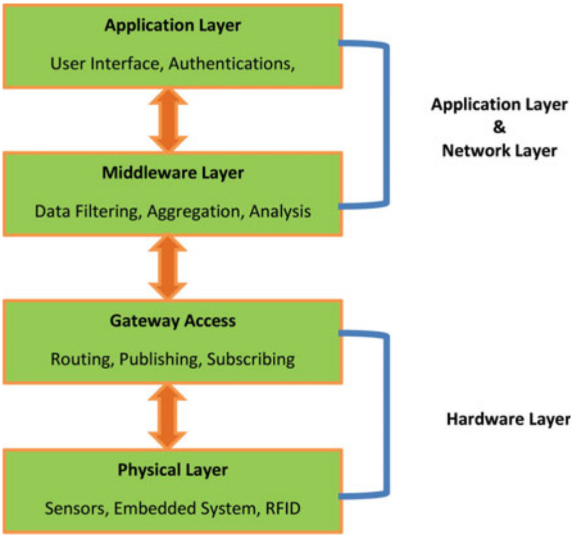
science and technology which has major impact on our daily lives either directly or indirectly. Internet of things is one such technology which has major contribution to this development. This IoT is mainly implemented in healthcare industry [2]. The main idea of IoT is to connect the objects to Internet which will create a path for an efficient interaction between the physical objects and the cyber-systems which are also termed as cyber-physical-systems (CPS) [3]. The term IoT gained its popularity by the value that it promises to create a scalable market and predict the future trend. This will indeed create smart objects which can understand the user requirements and act accordingly without explicit instructions. The term IoT has several definitions as each author tries to concentrate on any one of its fundamental characteristics. Due to this, it is often depicted as Web of Things allowing exchange of data. Although this is the fundamental characteristic of IoT, the application of it is so diverse because the solutions developed are totally dependent on the end-user needs which vary from user to user. IoT can be broadly classified as consumer IoT (CIoT) and industrial IoT (IIoT) where CIoT is more user-centric, that is, the interaction is between the user and the objects which improve the awareness of the surroundings and saving both money and time [4]. But IIoT is all about digital and smart manufacturing that is creating a platform for operational technology and information technology to interact [5]. As a consequence, digital manufacturing focuses on product life cycle and creates ability to counter the dynamic changes in the requirement. Along with this, the machine-oriented architecture of IIoT finds its application in different market sectors. This in turn creates a path for understanding the manufacturing process and enables sustainable and efficient production. In the past, ad hoc solutions were used by the industries as it provided the necessary flexibility and scalability for IoT communications. Recently, new standards such as WirelessHART and ISA100.11a were introduced, and cellular technologies such as 4G and 5G are capable of connecting devices over long range [6]. However, the limitations in terms of scalability and long-range communications are to be solved as even the cellular technologies require large infrastructure support and licence band. The large heterogeneous devices are connecting and it provides following features, that is low cost, low power, reliable and security.

2 State of Art

IoT has been built on various layers such as edge layer, gateway access layer, Internet layer, middleware layer and application layer which are stacked upon each other. This architecture is designed to meet the requirements of various domains such as industries, governments, healthcare and so on. The architecture covers various aspects such as scalability, modularity and interoperability among different devices using different technologies. Physical layer—this is the bottommost layer in the stack [5]. This layer is similar to the network physical layer to convert the human sensor signals into machine language. This physical layer is a main protocol of this IoT device, because most of the IoT device is automated signal detection. This type of auto-detection helps to convert the machine language. It is made up of sensor networks, RFID and embedded systems which are deployed on the field to capture the data. This sensor is the heart of the IoT, and without this sensor, there is no meaning in IoT device. This IoT technology is the combination of computer and electronic devices. This combination is implemented in mechanical, electrical, transport, logistics and buildings. This sensor is also fixed in smart city, and the concept of smart city is to detect the building activity and send it to the server. This signal is stored by cloud computing technology. The combined IoT and cloud computing is not having local server; it's always depend on third party service provider. The purpose of third party is to maintain the quality and lower the cost. Gateway access layer—next on the stack is gateway layer. This gateway is an interface between one particular device and server. This gateway is using some protocol system, and this protocol helps to provide the better security. This security system is using some encryption algorithm. The reason for using this algorithm is providing the information security while data stored in cloud server. The reason for using this algorithm is third-party cloud server usage [2] (Fig. 1).

This layer consists of various routers which are used for routing, publishing and performing cross-platform communication when needed. The first level of data handling takes place in this layer. Middleware layer—over the gateway layer comes the middleware layer. This middleware is the concept of interconnecting the device mechanism. This device middleware is used to establish and monitor the different types of IoT device. There are many companies producing the IoT product in same application. In that kind of situation, this middleware layer is helped to connect different devices with different company products. The most critical functions such as information management, design management, data filtering, semantic analysis and

Fig. 1 Internet of things layer


Application Layer
User Interface, Authentications,
Middleware Layer
Data Filtering, Aggregation, Analysis
Gateway Access
Routing, Publishing, Subscribing
Physical Layer
Sensors, Embedded System, RFID
Application Layer & Network Layer
Hardware Layer

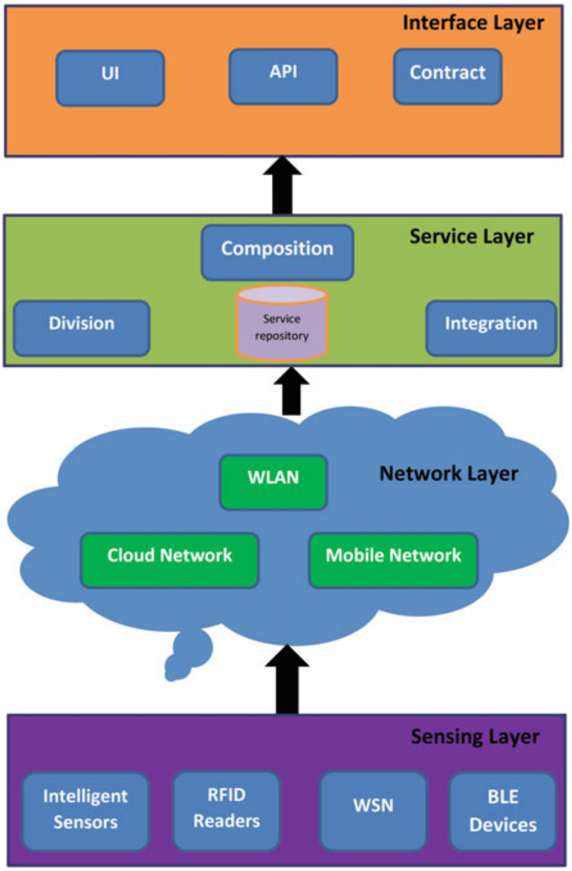
access control are taken care by this layer. As it is located in-between the hardware layer and application layer, it also enables the bidirectional flow of data by acting as an interface. Application layer—on the top comes the application layer which is responsible for creating a platform for different users to access the data. These are all some important layers of IoT device to enhance the network and device connection. The individual device ID sensors are generating the encryption key for the purpose of device authentication [7]. The healthcare industry is also using this IOT device to monitor patients' health information [8]. These layers are used in some fingerprint-based security system [9].

3 Service-Oriented Architecture in IoT

Service Oriented Architecture (SOA) concept is used in different parts of IoT. This is working on various domain and interoperability between complex heterogeneous devices. This method is used to reuse software and impose any specific technology during software implementation [10]. Sensing layer is smart sensors, and RFID tags are connected to devices to gather the data automatically and provide information exchange among heterogeneous devices. As number of sensors increases, the complexity of connecting devices reduces. The IoT device is having the unique ID that technology named as Universal Unique Identifier (UUID). This UUID is used to track and monitor the IoT device. The goal and working principle of network layer is to establish the connection in heterogeneous system in inter- and intra-network. As IoT deals with heterogeneous environments, it is also important to involve QoS management and control according to clients' requirements. Security and privacy issues are addressed in this layer along with other key features such as energy efficiency, data and signal processing and QoS. This security problem is dealt with symmetric and asymmetric encryption [11]. This QoS is major parameter in hybrid encryption [12]. The middleware layer is a functional and important layer in service layer structure. This particular layer is providing higher cost-effective platform in both software and hardware [13]. It also takes care of other service-oriented issues such as identification of devices that offer the required services, developing APIs that can manage the interoperability among different services, data management and information exchange and storage [14]. Interface layer IoT deals with heterogeneous devices and many problems related to interoperability and information exchange arises. This layer consists of user interface and application APIs [15]. This architecture also creates platform where every object's functionality can be offered as a standard service, and each service can be uniquely identified by a virtual element. The IoT service-oriented protocol middleware problem is to solve various solutions. The probabilistic protocol is one of the best solutions for this problem. Then face heterogeneity is also dealt with this problem [16] (Fig. 2).

An emerging trend is to develop production systems integrated with sophisticated electronics, interconnecting them and using them in the traditional business IT systems. As a result, IIoT creates a platform for flexible, low cost and resource-saving

Fig. 2 Service-oriented architecture layer



productions. With the help of smart services, IoT can also improve the efficiency of real-time data processing and can reduce the gap between the heterogeneous components in current digital economy. Industries deployed with IoT systems follow greener business models, are more profitable and optimise the resource usage. The acceptance of this green technology totally depends on the protection of the private data and information, the trust mechanism, communication security and security of services and applications. This is also a major challenge in IoT because inter- and intra-communications between every “thing” is via Internet, and the main source of internet for IoT is through the conventional mobile networks and sensor networks. Most of the services which are provided are for consumer IoT, and the same cannot be used for the IIoT because the number of attack vectors increases rapidly. As industrial applications require a reliable and secure data transfer methods, a number of research studies have been done to overcome these major challenges. Based on the properties of spatial correlation, low-ranked structure and temporal stability, a data monitoring algorithm for packet loss and re-establishing of sensor network was proposed by Kong et al. Lu et al. designed a digital watermarking technique to establish secure communication. The problem of continuous data collections where the lower bounds for a single set of data and continuous data collections is derived and also shortened the data collection process using multiple transceivers. Unlike in traditional WSNs where the devices are maintained by one user, in IoT applications the devices can be communicating with several devices deployed and users due to which data aggregations and processing have to be executed concurrently on same set of nodes. The delay-aware network structure can reduce the delays of collecting data simultaneously.

4 Challenges and Opportunities

The only reason for accepting IoT by the industries is to increase their efficiency and enhance their productions. Even though IoT promises to improve efficiency and productions, there are major challenges that industries have to look in before they leap in. These challenges are listed below. Real-time processing is one of the main features of IoT which attracted the industries. This real time processing unit is facing different challenges. That challenges are maintain reliability which help to satisfy the end-to-end connection. Various packets scheduling algorithms such as time-slotted packet scheduling are developed to achieve the desired QoS. As the growth of IIoT was dramatically increased in terms of scale and complexity, the level of difficulty in ensuring real-time performance has also increased. Inter- and Intra-device communications devices being connected are increasing rapidly interconnecting all devices and tracking them becomes a major challenge. To overcome these, smart devices which can detect, classify and migrate are required. The lack of interoperability among the devices increases the cost factor and complexities of the system deployment. Due to this achieving, seamless communication will be even more complicated. Energy efficiency as IoT devices are deployed on site should be constantly on for long years and the major power source is batteries, and it is an important factor which cannot be ignored. Therefore, green networking plays an important role in IIoT to develop a low power consuming and efficient devices at low cost. Although there are numerous technologies developed for low power consumption for WSN, these cannot be directly applied for IoT. Due to this, we need to establish a high power energy generating units which can also produce high density energy and use with the present low power nano-circuits and allows designing self-powered smart sensors. Security and privacy are two major factors which define how powerful the IoT system. Due to the large number of sensors and mobility, overcoming these challenges is complex. Even though there exist a large number of encryption algorithms, they have to be redesigned to make it faster and consume less power. Privacy is the next factor which is causing hurdles for IoT. Heterogeneous devices used in fields add more complexity to achieve privacy. Anonymity for data and network has to be provided, and powerful authentication systems have to be developed. The major significant of IoT device are connectivity, compatibility and longevity.

The communication devices and platforms are centred on the fundamental idea and are being changed such that clients do not go through serious communication issues. Currently, if a community utilising the client-server, users can communicate through different channels. Issue that is primary would be the fact that it is well suited for a number that is large. This technology should increase the quality of service up to the maximum level. A problem that is similarly independent of the connectivity would be the scalability. The final outcome of this method is not maintaining security parameter in designing and development phase. Machines which are manufactured keeping the security of the product in requirement documents get services and products, and this can be generic. They don't come because of the storage that's needed is capability, computation energy, and system that is operating. This single application device technology is used in many latest devices that is named as WiFi. Also same technology is used in ZigBee. The heterogeneous devices are used to collect the information during this process device compatibility is one of the major issue. The applications required for connection purposes will not support the hardware used. As there is huge amount of research and development happening all over the globe, the technology being used today might not be reliable in the coming up years. There is a huge scope for researchers in IoT because the technology has its applications in various domains. Few of the areas are scalable communications, privacy and security, identification technology, authentication, interoperability of heterogeneous devices; powerful energy-efficient devices, etc. Developing a context-aware IoT middleware is another area where a lot of research has to be done. Combining IoT, AI and cloud can develop smart objects which are self-configured, self-healing, self-protection and more capabilities.

5 Conclusion

IoT is made up by bringing multiple technologies such as information technology, network and communications and heterogeneous devices all connected to Internet, thus creating a new era of smart things. This study should take from nationwide federal government report. This report helps to improve the future IoT development. The main development of IoT technology is depending on technological revolution. This technology should provide energy efficient in heterogeneous devices. The primary advantage of this technology is decreasing computational cost and secondary advantage is increasing device efficiency. The growth associated with the IoT revealed many brand new difficulties like the not enough fundamental principle encouraging, ambiguous design and immature criteria. To satisfy these difficulties, we provide a structure that is four-layer systems. This technology is maintaining standard protocol; this protocol helps to establish the quality connections between one device to other device. The continuing future of IoT will undoubtedly be anticipated to be unified, smooth and pervading. Large-scale solution implementation has to be framed in just a pair of requirements. Therefore, the improvements of IoT being a system that is smart to be continuing with interoperability, power durability, privacy and safety. IoT has grown to be a style that is unavoidable of data business, which bound to create brand new changes in the way we live.

References

1. Whitmore A, Agarwal A, Da Xu L (2015) The internet of things—a survey of topics and trends. Inf Syst Front 17(2):261–274
2. Bitra VS, Jayapandian N, Balachandran K (2018) Internet of things security and privacy issues in healthcare industry. In: International conference on intelligent data communication technologies and internet of things (ICICI) 2018. Lecture notes on data engineering and communications technologies 26. Springer
3. Lee EA (2008) Cyber physical systems: design challenges. In: Proceedings of symposium on object oriented real-time distributed computing (ISORC). IEEE, pp 363–369
4. Garge GK, Balakrishna C, Datta SK (2018) Consumer health care: current trends in consumer health monitoring. IEEE Consum Electron Mag 7(1):38–46
5. Palattella MR, Accettura N, Grieco LA, Boggia G, Dohler M, Engel T (2013) On optimal scheduling in duty-cycled industrial IoT applications using IEEE802. 15.4 e TSCH. IEEE Sens J 13(10):3655–3666
6. Petersen S, Carlsen S (2011) WirelessHART versus ISA100. 11a: the format war hits the factory floor. IEEE Industr Electron Mag 5(4):23–34
7. Sridhar S, Smys S (2017) Intelligent security framework for IoT devices cryptography based end-to-end security architecture. In: Proceedings of inventive systems and control (ICISC). IEEE, pp 1–5
8. Bitra VS, Jayapandian N, Balachandran K (2018) Internet of things security and privacy issues in healthcare industry. In: Proceedings of intelligent data communication technologies and internet of things. Springer, pp 967–973
9. Jayapandian N, Rahman AMZ, Koushikaa M, Radhikadevi S (2016) A novel approach to enhance multi level security system using encryption with fingerprint in cloud. In: Proceedings of futuristic trends in research and innovation for social welfare (startup conclave). IEEE, pp 1–4
10. Teixeira T, Hachem S, Issarny V, Georgantas N (2011) Service oriented middleware for the internet of things: a perspective European conference on a service-based internet. In: Proceedings of European conference on a service-based internet. Springer, pp 220–229
11. Jayapandian N, Rahman AMZ, Radhikadevi S, Koushikaa M (2016) Enhanced cloud security framework to confirm data security on asymmetric and symmetric key encryption. In: Proceedings of futuristic trends in research and innovation for social welfare (startup conclave). IEEE, pp 1–4
12. Jayapandian N, Rahman AMZ (2017) Secure and efficient online data storage and sharing over cloud environment using probabilistic with homomorphic encryption. Cluster Comput 20(2):1561–1573
13. Duan R, Chen X, Xing T (2011) A QoS architecture for IOT. In: Proceedings of internet of things (iThings/CPSCom), cyber, physical and social computing. IEEE, pp 717–720
14. Grønbæk I (2008) Architecture for the internet of things (IoT): API and interconnect. In: Proceedings of sensor technologies and applications SENSORCOMM'08. IEEE, pp 802–807
15. Krco S, Pokric B, Carrez F (2014) Designing IoT architecture (s): a European perspective. In: Proceedings of internet of things (WF-IoT). IEEE, pp 79–84
16. Issarny V, Bouloukakis G, Georgantas N, Billet B (2016) Revisiting service-oriented architecture for the IoT: a middleware perspective. In: Proceedings of service-oriented computing. Springer, pp 3–17

Performance Comparison of Multicast Routing Protocols Based on Route Discovery Process for MANET

Kinjal Adhvaryu

Abstract Performance of routing protocols used for multicasting is highly depending on its route searching approach, which is the first step of routing process. Expanding ring search (ERS) is one of the widely used concepts for route searching process which is also used to reduce the broadcast overhead in MANET. To understand the effect of route discovery process on the performance of routing protocols, we have considered two different multicast routing protocols, namely energy-efficient ERS (E^2ERS) and Multicast Ad hoc On-demand Distance Vector Protocol (MAODV) which are widely used for multicasting in MANET. MAODV uses ERS approach whereas E^2ERS has modified the ERS approach by modifying the transmissions of RREQ during route discovery process. Here, we have used different parameters like end-to-end delay, goodput and packet delivery fraction for varying node speed and varied TTL_Increment values for varied number of receivers to compare the performance of MAODV and E^2ERS protocols.

Keywords Goodput · Control overhead · Broadcasting · Ad hoc network

1 Introduction

Multicasting is one of the efficient ways to set up the group communication when one sender node wants to send same set of data/messages to more than one receiver. Performance of routing protocols used for multicasting is highly depending on its route-finding approach which is the first step of routing process. The goal of the ERS during route-finding process is to find mobile nodes that have the required route information to the destination mobile node in their route table or the destination mobile node by flooding of the route request packets (RREQs) in a controlled manner [1–4]. To restrict the flooding of RREQs, TTL-based ERS is used by various routing protocols in MANET. ‘The ERS based on TTL restricts its searching range by giving

K. Adhvaryu (✉)
Computer Engineering Department, Sankersinh Vaghela Bapu Institute of Technology, Gandhinagar, Gujarat, India
e-mail: kinjalvk@yahoo.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_9

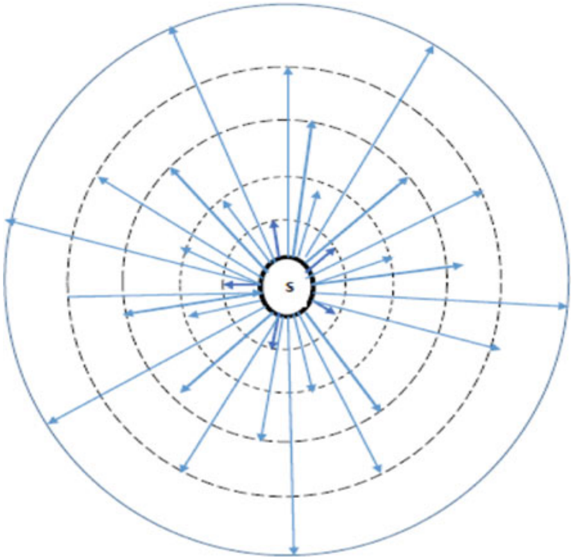


Fig. 1 Route discovery in MAODV

RREQs with a predefined TTL value. The TTL value indicates the radium of a searching space. Each time if it fails to find any destination node or any node that has route information to the destination node, the source node rebroadcasts the RREQ with an increased TTL number to allow the RREQ to encoder a larger area. Even with the controlled manner of flooding, expanding ring search still suffers from high overhead because each time route discovery process starts from the source node. Research says that when a larger area of the network needs to be searched, the cost drastically increases' [1, 4].

Figure 1 shows the working of ERS which is used by MAODV protocol. Here, we assume that node S wants to find the destination node. Then it will start its searching process by broadcasting the RREQ to all nodes which are one hope away, if TTL_START = 1. Else if the target node is not found, then TTL will be incremented based on TTL_Increment value. Based on the updated TTL value, again node S will broadcast the RREQ. Node S will repeat the same process until TTL crosses the TTL_Threshold or in between destination node is found [4–8]. From Fig. 1, we can see that more number of RREQ packets is required during the route discovery process.

2 Energy-Efficient ERS Expanding Ring Search (E^{2}ERS)

Here, an alternative energy-efficient ERS scheme is proposed which reduces the overhead during route discovery, and in this way, it reduces the processing load on mobile nodes and provides support to reactive types of MANET protocols. The

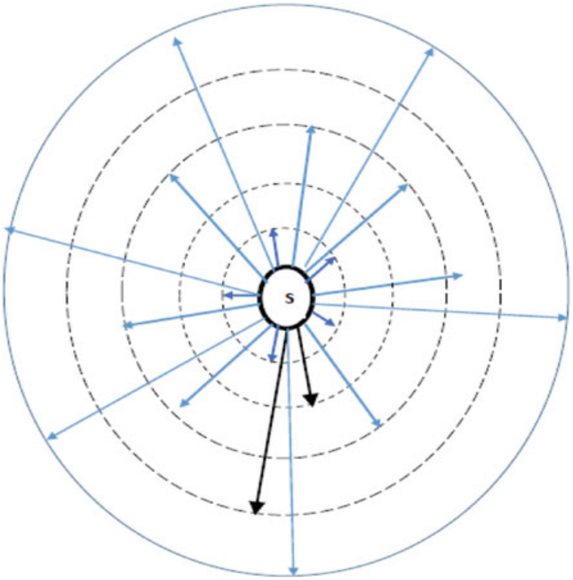


Fig. 2 Route discovery in E^2ERS

basic route-finding structure of energy-efficient ERS (E^2ERS) is similar to that of the TTL-based ERS. Main differences from the TTL-based ERS are that the E^2ERS does not transmit the RREQ every time during its routing search procedure from the sender/source node to all other mobile nodes. Instead of that E^2ERS unicast the RREQ, if destination/target node is not found then it broadcast the RREQ and find the destination/target node. Still destination/target node is not found then unicast the RREQ and find the destination/target node. In this way, alternatively unicasting and broadcasting of RREQ will be done instead of every time broadcasting of the RREQ to search the destination/target node during path searching process.

In Fig. 2, optimized ERS based on modifying the forwarding RREQ packets is shown. Instead of broadcasting the RREQ packets, E^2ERS is unicasting the RREQ, then broadcasting the RREQ, then unicasting the RREQ, then broadcasting the RREQ and so on until interested node is found. Black arrow shows the unicasting the RREQ, and blue arrows show the broadcasting the RREQ. During unicasting, RREQ will be forwarded to furthest node from the neighbor list based on current TTL value. To justify the proposed concept, assume ad hoc network with network diameter 5 and consider total of 5 mobile nodes in radio range of every node, where network diameter is the longest path between any two mobile nodes. To find out the route to the farthest node located 5 hops away from the source node, broadcasting RREQ will start with TTL equal to 1 and increasing by TTL_Increment with each re-broadcast of RREQ up to the predefined network diameter or TTL_Threshold.

Now for designed network, total $4 + 8 + 20 + 32 + 68 = 132$ transmission of RREQ will be required by E^2ERS instead of $4 + 16 + 52 + 160 + 484 = 716$ transmissions of RREQ done by TTL-based ERS (as shown in Table 1) which shows the effective reduction in control overhead during route discovery process. Due to

Table 1 Required transmissions of RREQ

Diameter: 5, 5 nodes in radio range of every node					
TTL	Traditional ERS		Modified ERS		
1	4	4	Unicasting and broadcasting alternatively	4	4
2	4 + (4 * 3)	16		4 + 4	8
3	4 + 12 + (4 * 3 * 3)	52		4 + 4 + (4 * 3)	20
4	4 + 12 + 36 + (4 * 3 * 3 * 3)	160		4 + 4 + 12 + 12	32
5	4 + 12 + 36 + 108 + (4 * 3 * 3 * 3 * 3)	484		4 + 4+ 12 + 12 + (12 * 3)	68
Total PKTS	4 + 16 + 52 + 160 + 484 = 716		4 + 8 + 20 + 32 + 68 = 132		

reduction in control overhead, processing load on mobile node will be reduced, and in this way, lifespan of mobile node will be prolonged. And this difference in reduction will go on increasing for bigger values of network size.

3 Performance Comparison

The performance of E^2ERS-based protocol is compared with the known multicast routing protocol MAODV which uses the TTL-based ERS. For the simulation of the E^2ERS-based protocol, NS-2.26 simulator has been used. Data traffic was generated using constant bit rate (CBR) UDP traffic with 32 network size with one sender and 2, 5 and 10 varying mobile nodes acting as receivers in the multicast group. All wireless mobile nodes are randomly distributed in a square of 500 m × 500 m. The nodes use the IEEE 802.11 radio and MAC model provided by the CMU extensions. Each simulation executes for 200 s [5, 6, 9, 10]. The number of receiver mobile nodes is varied from 2 to 10 nodes to see the effect of the number of receiver nodes on the performance on the system performance. Also other parameter TTL_Increment value is varied to see the performance of proposed concept. TTL_Increment value is varied with 1, 2, 3, 4 and 5 and each time, proposed concept is compared with original approach for various performance metrics. To analyze the effect of number of receiver nodes, another node speed parameter is also considered with 4, 12 and 20 m/s varying values. The metrics used for performance evaluation are: (i) Packet delivery fraction—'the ratio obtained by dividing the number of data packets correctly received by the destination by the number of data packets originated by the source' [5]. (ii) Goodput—'which is also known as throughput [8, 9, 11–13] of the network.' (iii) Average end-to-end delay—'this includes all possible delays caused by queuing delay at the interface, buffering during route discovery, retransmission delays at the MAC, propagation and transfer times' [2, 3, 9, 14, 15].

Figures 3, 4 and 5 show the comparison between E^{2}ERS and MAODV protocols for 2, 5 and 10 receiver nodes for varying node speed values for all three metric values. From results, it is clear that E^{2}ERS gives better results compared to MAODV for more number of receiver nodes with increasing node speeds.

Figures 6, 7 and 8 show the comparison between E^{2}ERS and MAODV protocols for 2, 5 and 10 receiver nodes for varying TTL_Increment values for all three metric values. From results, it is clear that E^{2}ERS gives better results compared to MAODV for more number of receiver nodes with increasing TTL_Increment values.

Fig. 3 PDF improvements

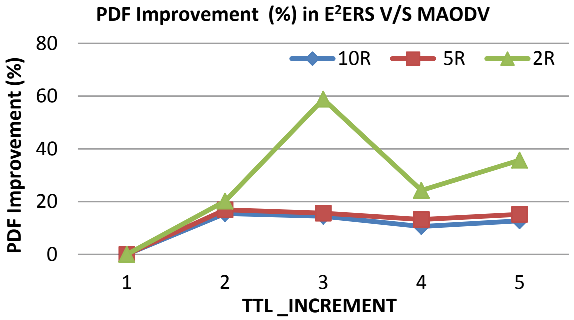


Fig. 4 Goodput improvements

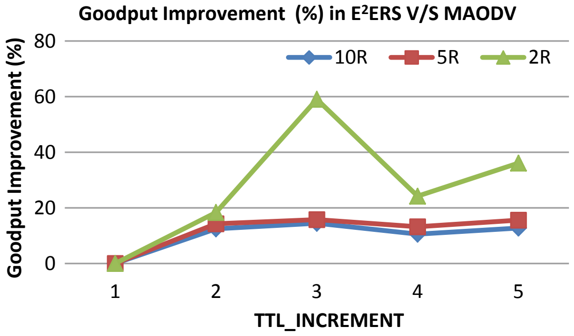


Fig. 5 E2E delay decrement

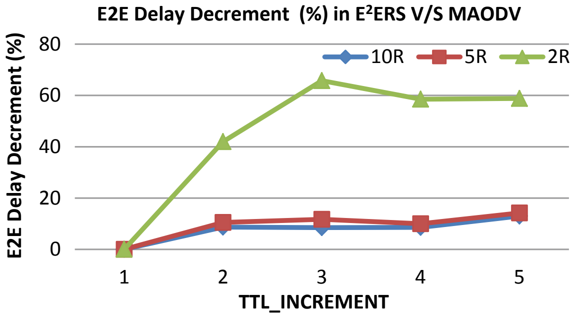


Fig. 6 PDF improvements

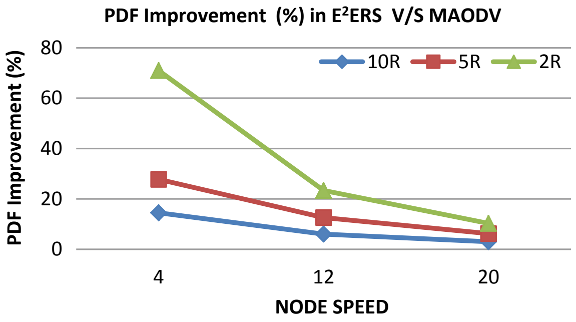


Fig. 7 Goodput improvements

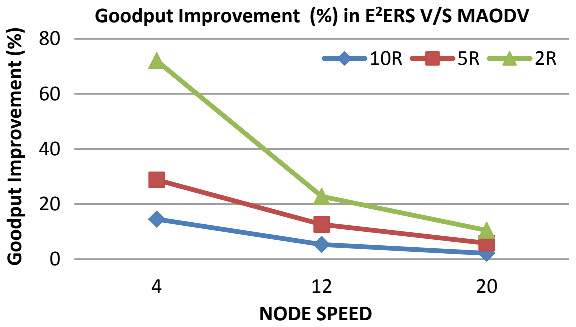
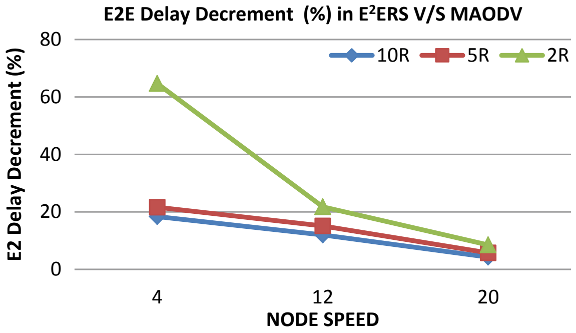


Fig. 8 E2E delay decrement



4 Conclusion

From the presented results, it is clear that selection of route discovery process affects the performance of routing protocols. Apart from it, number of receiver nodes and selection of node speed also affect the outcome of multicast routing protocols. It is also clear that E^{2}ERS, by modifying the expanding ring search technique which is used by MAODV, which is state of the art tree-based multicast routing protocol, reduces the transmission of RREQ packets. Due to reduction in required transmissions of RREQ during route discovery process, processing load on mobile nodes decreases and so that the lifetime of mobile nodes and of network is also prolonged. It also leads less chance of network clogging and less overheads as well and makes routing process more energy efficient.

References

1. Junhai L, Danxia Y, Liu X, Mingyu F (2009) A survey of multicast routing protocols for mobile ad-hoc networks. IEEE Commun Surv Tutorials 11(1)
2. Moh S, Yu C, Lee B, Youn HY (2002) Energy efficient and robust protocol for mobile ad hoc networks. In: Proceedings of the 2002 Pacific Rim international symposium on dependable computing (PRDC'02), IEEE. 0-7695-1852-4/02
3. Hwang I-S, Pang W-H (2007) Energy efficient clustering technique for multicast routing protocol in wireless ad hoc networks. IJCSNS Int J Comput Sci Netw Secur 7(8)
4. Pu I (2007) Energy efficient expanding ring search. In: First Asia international conference on modelling & simulation (AMS 07), 03/2007
5. Bakht H (2011) Survey of routing protocols for mobile ad-hoc network. Int J Inf Commun Technol Res 1(6)
6. Wang N-C, Chen Y-S A power-aware dual-tree-based multicast routing protocol for mobile ad hoc Networks. IET Commun 6(7):724–732
7. Adhvaryu KU, Kamboj P (2017) Performance comparison between multicast routing protocols in MANET. In: IEEE international conference on electrical, computer and electronics—2017 (UPCON 2017). GLA University, Mathura, 26–28 Oct 2017
8. Sreedhar GS, Damodaram A (2011) Tree based multicast routing protocols for mobile ad hoc networks and current state of the art. Int J Sci Adv Technol
9. Nagaratna M, Kamakshi Prasad V, Raghavendra Rao C (2011) Performance evaluation of tree—based multicast routing protocols in MANETs. IJCST 2(3)
10. Vassileva N, Barcelo-Arroyo F (2008) A survey of routing protocols for maximizing the lifetime of ad hoc wireless networks. Int J Softw Eng Appl 2(3); Young M (2002) The technical writer's handbook. Mill Valley, CA
11. Wei W, Zakhor A (2007) Multiple tree video multicast over wireless ad hoc networks. IEEE Trans Circ Syst Video Technol 17(1)
12. Moustafa H, Labiod H (2003) A performance comparison of multicast routing protocols in ad hoc networks. In: Proceedings of IEEE personal, indoor and mobile radio conference, pp 497–501
13. Adhvaryu KU, Kamboj P (2017) Effect of node speed on performance of multicast routing protocols in MANET. In: IEEE international conference on telecommunication, power analysis and computing techniques—2017 (ICTPACT—2017). Bharath Institute of Higher Education & Research, Chennai, 6–8 Ap 2017
14. Qabajeh MM, Abdalla A, Khalifa O, Qabajeh LK (2011) A tree-based QoS multicast routing protocol for MANETs. In: 2011 4th international conference on mechatronics (ICOM)
15. Adhvaryu KU, Kamboj P (2013) Survey of various energy efficient multicast routing protocols for MANET. In: Fifth international conference on advances in recent technologies in communication and computing, ARTCom2013. Bangalore published by IET, Elsevier
16. Adhvaryu KU, Kamboj P (2016) Efficient multicast routing in mobile ad-hoc network. J Mob Comput Commun Mob Netw 3(3). ISSN: 2349-901X (online)

New Complex Hybrid Security Algorithm (CHSA) for Network Applications

Haider K. Hoomod, Ali Jameel Al-Mousawi and Jolan Rokan Naif

Abstract The raising of Cyberwarfare level require to have the maximum protection levels in the networks and its applications. Therefore, these systems must be protected from unauthorized usage of their data using the most powerful security algorithms. Many and growing challenges facing cybersecurity require cryptographers and data security engineers to develop stronger and more powerful algorithms to resist this type of attack. There are many characteristics that measure the strength of the electronic security system, including the speed of the algorithm and the strength of the system against the cryptanalysis. This paper discusses the design, building, and implementation of a new hybrid algorithm that combines a number of security algorithms in order to obtain the best results in terms of resistance to multiple cyber-attacks. This paper also contains an analytical study of the algorithms used and their effectiveness in resistance to attacks represented by statistical results and graphs.

Keywords Hybrid algorithm · Cybersecurity · Network security · System security

1 Introduction

Many electronic systems around the world have been exposed to cyber breaches by hackers or by some malicious programs that have enabled hackers to access these systems and use their data unauthorized. Most electronic systems rely on the principle of encryption algorithms to protect their data and convert clear data into encrypted

H. K. Hoomod (✉)
Computer Science Department, College of Education—Mustansiriyah University, Baghdad, Iraq
e-mail: dr.haiduh@uomustansiriyah.edu.iq; drhjnew@gmail.com

A. J. Al-Mousawi
Information Technology Regulation Directory—Communication and Media Commission of Iraq (CMC), Baghdad, Iraq
e-mail: aburgiefali@yahoo.com

J. R. Naif
Informatics Institute for Postgraduate Studies-Baghdad, Baghdad, Iraq
e-mail: newjolan@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_10

data that can not be decoded into using special arguments called cryptographic keys. These systems vary according to the nature of the security algorithms used. Some of them use cryptographic algorithms of great complexity and high strength. They are not fast, and those who use fast security algorithms are relatively less safe compared to their complex predecessors [1].

In order to design a new algorithm, consider the analytical studies of existing or previously used algorithms and compare them to find the strengths and weaknesses of each algorithm. As it is known, each algorithm has a number of features and some disadvantages. The hybrid algorithm is a combination of the properties of the existing algorithms to take advantage of the characteristics of these algorithms in improving the results of the new algorithm [2]. For example, when combining two cryptographic algorithms, one of these algorithms has certain disadvantages, and their integration with another algorithm may be a reason to address these disadvantages. It is also possible that new defects will emerge as a result of the process of integration of the algorithms, so the process of hybridization of algorithms in the case of increased disadvantages is unsuccessful.

The characteristics of the hybrid algorithm depend mainly on the type of selected Algorithms. In the hybridization process [3]. The more powerful algorithms are selected, the better the results are obtained. There are systems based on speed in the work where the speed is a sensitive issue cannot be compromised in terms of work so not all algorithms can work efficiently in this type of systems, an example these systems are wireless systems and most of the Web sites. On the other side, there is another type of system that requires maximum security regardless of time. It requires security algorithms with a very high level of complexity and a high level of security in order to provide the security requirements of information and data such as military systems and research facilities systems [4].

There are some basic characteristics that must be met in cryptographic algorithms. One of the most important features is its strength in the face of code analysis and randomization in generating cryptographic keys, increasing randomization and confusion within the algorithm's body and other properties. Algorithms that are adopted on systems of a sensitive nature must have these characteristics at their highest levels [5].

2 Related Work

In this section of this research, it is important to look at the previous studies in this area, i.e., the most prominent security algorithms in which there is a kind of hybridization in order to know what characteristics have emerged and what are the disadvantages that emerged as a result of the hybridization process in the security algorithms.

Jignesh R. Patel, Rajesh S. Bansode and Vikas Kaul have invented a hybrid encryption system based on a block cipher [6]. This system was built based on two main block cipher algorithm which is advanced encryption standard (AES) and data encryption standard (DES) by merging the two techniques together attempting to have both advantages of both systems. In this experiment, a hybrid block cipher algorithm deals with 64-bit input message were each input message that exceeded 64 bit will be divided into equal size 64-bit blocks. The key size of the algorithm is 128-bit size. The results showed that the hybrid algorithm takes more time to process the data then each of its components because the processing time increased compared with the single algorithm. The resultant from the hybridization process shows that the complexity level increased and the security level increased compared with its component.

Kirtiraj Bhatele, Amit Singhal, and Mayank Pathak in their paper design an architecture for a hybrid encryption system using multiple algorithms [7]. The algorithms used are AES, RSA, Elliptic Curve (EC), and additionally, it uses an MD5 algorithm for hashing the component of the encryption algorithm. This architecture also takes into consideration the use of duel RSA algorithm and its effect compared with normal RSA. The proposed hybrid system generates a hash value using MD5 and places it within the encryption algorithms. Meanwhile, the plaintext enters the AES, RSA and Elliptic curve cryptographic function in order to be encrypted by using the encryption key. The plaintext is retrieved at the end of the algorithm and by using of MD5 authentication. When the hash value approved, the Ciphertext decrypted to retrieve the original plaintext. The resulting ciphertext of this system is resistance to the square attacks. The algorithm use high bandwidth and low power consumption as a measurable advantage of this hyper system. A disadvantage of this system it is noted that the expected execution time is as twice as the normal execution time of its component. This make this algorithm suitable for a high-security system but in the same time it is unsuitable for applications and systems that require real-time execution or fast execution of security algorithm.

Prabhat K. Panda and Sudipta Chattopadhyay create a hybrid encryption algorithm based on RSA and public-key cryptographic systems [8]. The merging in this process made by using four prime numbers in order to generate both of public and private keys so as the complexity in key generation increased. The hybrid RSA (HRSA) results produced from the experiments made by the researchers show that HRSA is more secure than normal RSA and also the time taken for the encryption and decryption process is close to the original execution time of normal RSA. The hybridization came from the idea of inserting new arguments to the original RSA by using the properties of prime numbers to generate secure keys. Another focal point that is noticed in this algorithm is that the randomness in key generation increased and as a result of that affect the attack resistance capability increased because whenever the randomness period increased the more powerful the algorithm will be resistance to all attacks that depend on the predictability.

2.1 Proposed Work (CHSA Design)

Each algorithm has a specific structural security representation that determines the mode of data flow within it. The more algorithm structure parts correlated together the more algorithm is faster in execution. The algorithms whose structure is interconnected have a fast execution time (encryption–decryption) because of this correlation. On the unrelated or low-correlation algorithms implementation time will be more than the previous one, but the complexity and strength of the algorithm will be very large because the process of code analysis will be very difficult resulting from the structural parts of this algorithm are not understood intelligently. There is a kind of interconnection between the structural parts of the algorithm that is incomprehensible to the normal algorithm tracer or is very difficult for the code analyst, which makes this algorithm has a strong structure and thus will be difficult to break. The general structure of CHSA consists of six basic classes summarized as follows:

1. **Block cipher**: the truncating of the message made by using block cipher. The message truncated into the equal-sized block in order to be processed by the other algorithm steps [9]. All message types processed by the algorithm withier if it is a multimedia or a string file. The string file truncated into blocks and processed to the other steps as a binary string while the multimedia file are encoded and converted into equal size binary blocks. Meanwhile, a conversion method used to convert the converted binary message into a hexadecimal form. For mathematical and programming reasons, all messages need to be in hexadecimal form to be compatible with other algorithm arguments.
2. **Stream cipher**: after processing the truncated message into hexadecimal blocks the next step is to process the block in stream cipher form. Each character in the block processed one-by-one using a stream cipher algorithm. The stream cipher increased the speed in execution time and therefore it decreased the overall time needed to encrypt the message and convert it into ciphertext form. Stream cipher algorithm needs to have an initial seed to encrypt the message using this seed as a key for the encryption process. This step considers the first encryption in the CHSA using a stream cipher method. The stream cipher key generated using the CHSA key generation method. CHSA provided with a method for the random key generation whatever it is requested. The stream cipher algorithm used in this step is RC4 [10]. The algorithm sends a request to the key generation method within CHSA in order to receive a random key according to the algorithm type (more details in Sect. 3).
3. **S-Box confusion**: one of the basic steps in all cryptographic algorithms is the confusion [11]. The confusion added by using the s-box matrix. Normal algorithms use pre-build s-boxes in order to distribute the change over the current data chunk. S-boxes in CHSA is randomly generated by the key generation method. The generated pattern will be organized into a matrix. The main objective of the s-boxes in CHSA is to increase the confusion of the message structure and process the message to the next step. The increase in confusion makes it harder to analyze the data chunk in case of sniffing during the data transmission or cryptanalysis attack.
4. **Add encryption key**: this is the stage where the message is truly encrypted. Each encryption algorithm takes its strength from the encryption key. The more the encryption key is strong the more strength will gain against cryptanalysis

and more resistance to all known attack types. At this stage, CHSA requesting from the generation center the encryption key to encrypt the current block. The complexity of the hybrid algorithm is that CHSA requests a key for each block that is under process. This would add a lot of complexity to the system meanwhile it required to generate multiple encryption keys (the same number of blocks). This behavior within CHSA is similar to the behavior of one-time pad algorithm [12] which considered unbreakable algorithm since the generated encryption key is as long as the message and used only once in encryption and decryption and then destroyed. The generated hexadecimal key added to the current block which himself is a hexadecimal quantity and therefore an X-OR operation performed in this stage. Generated ciphertext blocks transferred into another step to perform the chaining process within other blocks.

5. **Block organization**: the resultant blocks from the previous step will be organized into a chain of the block. Each message block enters the algorithm separately from the other blocks. CHSA works in the parallel mode were each block processed and encrypted independently from other blocks. Each block of the data needs to correlate with other blocks in order to produce the final block cipher. The known methods for the block cipher called mode of operations. These modes used to join the blocks after they are encrypted in a manure that can be decrypted later using the same method in reverse. However, the chaining process of the block cipher considered a focal point in the algorithm secrecy [13]. CHSA joining the blocks in a random pattern way generated by the generation center of CHSA. When the block generated and attended to be chained with other blocks the algorithm generate a request to the generation center and receive a pattern of the block order to join the blocks together and when decrypt the original message it will use the same pattern generated previously to retrieve the original blocks.
6. **Probability distribution**: in mathematics, the probability is the mean of an event that may or may not occur according to a specific condition [14]. Adding probability distribution to the algorithms increases the confusion level along with the randomness of the hall encryption systems [15]. CHSA added this feature to the ciphertext by using CSHA probability distribution sector in the algorithm body. This processing method generating a random pattern for the distribution of the ciphertext algorithm. The input block will be permutated according to the generated pattern from the distribution center. Probability plays a central role in the changing event of the block cipher parts. After the chaining process completed, the ciphertext block enters the probability distribution stage which examines the ciphertext block according to the pattern. If the probability occurs then the block is merged with the distribution pattern generated from the probability distribution center. Probability distribution center have a communication link with the block organization stage because of shared objectives, the distribution center request from the block organizer to provide the distribution center with the block boundaries in order to identify the block border and act according to this border [14, 16]. Whenever the block boundaries received a pattern will be generated automatically and randomly. Ciphertext changed according to this pattern. The form of change occurs by the probability distribution pattern is multi-form change. What

this means is that it contain multiple actions to change the ciphertext like shifting, simple stream cipher encryption, substitution encryption, or transposition encryption. The generated pattern need a key in case of substitution, transposition, or even stream cipher so this step needs to be provided with keys from the generation center within CHSA.

All details of CHSA algorithm structure and general design appear clearly in Fig. 1. Connections, steps, and data flow is represented in details.

2.2 CHSA Generation Center (GC)

The GC is the main nerve of the new hybrid algorithm as it generates all kinds of keys and patterns used by the algorithm in the performance of various functions. GC receives the generation requests from the joints of the system. Each of these joints has a special request to the GC to generate the cryptographic keys. It generates the patterns of the process of reallocating the bits in the encoded text during the conversion process from its current form to a more complicated one. The process of reallocating bits in the current message form requires a pattern generated by the GC for each step that requires reallocation. Mainly, there are three main steps in CSHA that requires a pattern for the distribution process. In another hand, there are three main phases that require keys for encryption.

The hybrid chaotic system used in this proposed system is composed of the Logistic system (Eq. 1) and Lorenz system (Eqs. 2, 3, and 4) as shown in Fig. 2. The Logistic chaos outputs are used in two manners (as KS1 and KS5). First, they are used for encryption processing. Second, they are used to initialize the Lorenz chaotic system. The last significant number of each result from the Logistic chaotic system is added to the initial periods of the Lorenz initial conditions

$$f(k_{n+1}) = r \cdot k_n(1 - k_n) \tag{1}$$

$$x_{n+1} = a \cdot (y - x_n) \tag{2}$$

$$y_{n+1} = c \cdot x - x \cdot z - y \tag{3}$$

$$z_{n+1} = x \cdot y - b \cdot z \tag{4}$$

where a, b, c, r is the chaos parameters. While x_0, y_0, z_0, $k_{0,}$ and v_0 is the initial conditions for chaos map.

The GC consists mainly of two main sectors. The first sector is the Chaos Random Generation Center (CRGC) which is responsible for providing random keys from hybrid chaotic system, the patterns depending on random key and pattern generation algorithm. Blum-Blum algorithm summarized in the following equation:

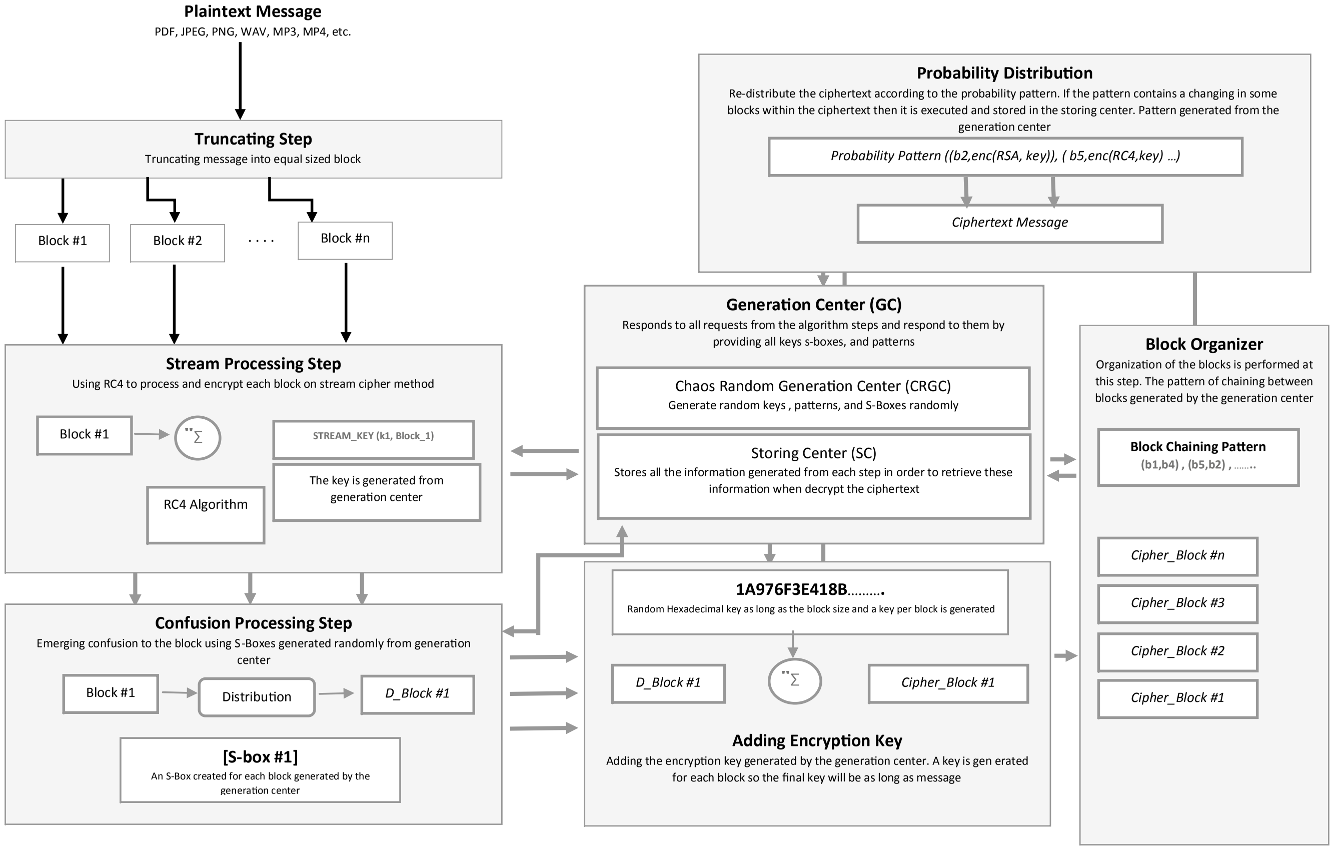

Plaintext Message
PDF, JPEG, PNG, WAV, MP3, MP4, etc.
Truncating Step
Truncating message into equal sized block
Block #1
Block #2
. . . .
Block #n
Stream Processing Step
Using RC4 to process and encrypt each block on stream cipher method
Block #1
Σ
STREAM_KEY (k1, Block_1)
The key is generated from generation center
RC4 Algorithm
Confusion Processing Step
Emerging confusion to the block using S-Boxes generated randomly from generation center
Block #1
Distribution
D_Block #1
[S-box #1]
An S-Box created for each block generated by the generation center
Probability Distribution
Re-distribute the ciphertext according to the probability pattern. If the pattern contains a changing in some blocks within the ciphertext then it is executed and stored in the storing center. Pattern generated from the generation center
Probability Pattern ((b2,enc(RSA, key)), (b5,enc(RC4,key) …)
Ciphertext Message
Generation Center (GC)
Responds to all requests from the algorithm steps and respond to them by providing all keys s-boxes, and patterns
Chaos Random Generation Center (CRGC)
Generate random keys , patterns, and S-Boxes randomly
Storing Center (SC)
Stores all the information generated from each step in order to retrieve these information when decrypt the ciphertext
1A976F3E418B………
Random Hexadecimal key as long as the block size and a key per block is generated
D_Block #1
Σ
Cipher_Block #1
Adding Encryption Key
Adding the encryption key generated by the generation center. A key is gen erated for each block so the final key will be as long as message
Block Organizer
Organization of the blocks is performed at this step. The pattern of chaining between blocks generated by the generation center
Block Chaining Pattern
(b1,b4) , (b5,b2) , …….
Cipher_Block #n
Cipher_Block #3
Cipher_Block #2
Cipher_Block #1

Fig. 1 General CSHA structure with the details of each step

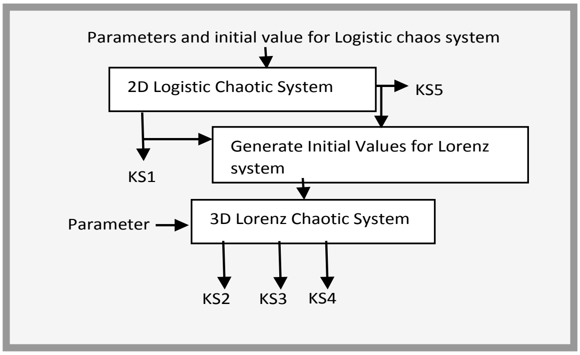
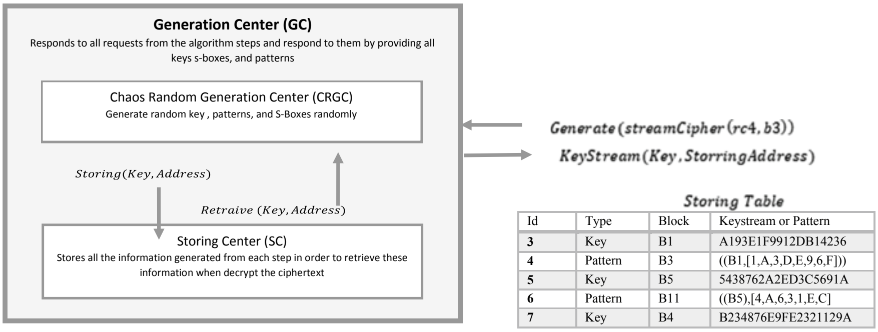

Parameters and initial value for Logistic chaos system
2D Logistic Chaotic System
KS5
Generate Initial Values for Lorenz system
KS1
Parameter
3D Lorenz Chaotic System
KS2
KS3
KS4

Fig. 2 The hybrid chaotic system used in the proposed system

$$z_{n+1} = z_n^2 \bmod M \tag{5}$$

where $M = p * q$ and p, q are two large prime numbers. The seed z_n^2 should be an integer value that its value is co-prime with M. The main purpose behind using Blum-Blum hybrid chaotic system algorithm is its properties of generating a random number that approximates the properties of the true random number generation from hybrid chaotic system [13, 17].

The second sector in the GC is the Storing Center (SC) which is responsible of storing form holding the key streams and patterns generated by the CRGC. The storing strategy takes the form of table with identifiers in order to identify the type of storing operation. Each record in the database of the system contains key streams or a pattern composed with it the type of the algorithm that request it and the step of the request. Figure 3 shows a detailed structural view of the GC and its components.


Generation Center (GC)
Responds to all requests from the algorithm steps and respond to them by providing all keys s-boxes, and patterns
Chaos Random Generation Center (CRGC)
Generate random key , patterns, and S-Boxes randomly
Storing(Key, Address)
Retraive (Key, Address)
Storing Center (SC)
Stores all the information generated from each step in order to retrieve these information when decrypt the ciphertext
Generate(streamCipher(rc4, b3))
KeyStream(Key, StorringAddress)
Storing Table

Id	Type	Block	Keystream or Pattern
3	Key	B1	A193E1F9912DB14236
4	Pattern	B3	((B1,[1,A,3,D,E,9,6,F]))
5	Key	B5	5438762A2ED3C5691A
6	Pattern	B11	((B5),[4,A,6,3,1,E,C]
7	Key	B4	B234876E9FE2321129A

Fig. 3 GC internal design and storing strategy inside SC unit in the GC saves the data on a table with type of the storing element, block that is related to the stored element, and the generated stream or pattern

2.3 CHSA Syntax

The data flow within CHSA goes from truncated blocks and ending with ciphertext blocks. The encryption process takes six basic steps. All steps within CHSA are represented in the following algorithm.

a. CHSA Encryption

Below the proposed CHSA encryption algorithm.

Algorithm 1: CHSA Encryption Syntax

```
Input: $PlainText$
Output: $FinalCipher$

1-  $GC\_Generate$ =Generate chaos keys using hybrid chaotic system(k1, k2,k3,k4, and k5)
2-  Truncating ($PlainText$, size)        // Truncating plaintext into equal sized blocks
    Divide ($PlainText, Size_{block}$)
    $Padding_{Pattern} = GC\_Generate(Rand(random_{pattern}))$
    $Store = GC\_Generate(Store(Padding_{Pattern}))$        // store the padding pattern in the database
    Padding ($PlainText_{lastBlock}, Padding_{pattern}$)        // Appending padding operation
3-  StreamCipher ($PlainText_{lastBlock}$)
    $For\ i = 1\ to\ Count(Plaintext_{blocks})$        // a loop for processing all the blocks
    $StreamKey_{i=} GC\_Generate(K1)$        // Generate a stream cipher key from the generation center
    $Store = GC\_Generate(Store(StreamKey))$        // store the key stream in the database
    $ESB_{i=} RC4(Plaintext^{i}_{block}, StreamKey_{i})$        // implement stream cipher encryption
    End for
4-  ConfusionProcessing ($ESB$)
    $For\ i = 1\ to\ Count(ESB)$
    $ConfusionPattern_{i=} GC\_Generate(K2, (ConfusionPattern_{i}))$        // generate a confusion pattern
    $Store = GC\_Generate(Store(ConfusionPattern_{i}))$        //  store the confusion pattern
    $C_{ESB_{i=}} Distribute\ (ESB_{i}, ConfusionPattern_{i})$        //  Distribute the encrypted block
    End for
5-  AddingEncryptionKey ($C_{ESB}$)
    $For\ i = 1\ to\ Count(C_{ESB})$
    $EK_{i=} GC\_Generate(K3)$        // generate a Pseudo-random key
    $Store = GC\_Generate(Store(EK_{i}))$        //  store the key stream
    $Cipher\_C_{ESB_{i=}} Encode\left(C_{ESB_{i}}, EK_{i}\right)$        //  Adding the key to the specified block
    End for
6-  Organize ($Cipher\_C_{ESB}$)
    $For\ i = 1\ to\ Count(Cipher\_C_{ESB})$
    $join_{pattern_{i=}} GC\_Generate(K4, \left(organize_{pattern_{i}}\right))$        // generate a random pattern
    $Store = GC\_Generate(Store(join_{pattern_{i}}))$        //  store the generated pattern
    $^{Orginized}Cipher\_C_{ESB_{i=}} Join\left(Cipher\_C_{ESB_{i}}, join_{pattern_{i}}\right)$        //  Re-Arrange all ciphertext parts
    End for
7-  Distribution ($^{Orginized}Cipher\_C_{ESB}$)
    $For\ i = 1\ to\ Count(Cipher\_C_{ESB})$
    $DistributionPropability_{pattern_{i=}} GC\_Generate(k5, \left(Probability_{pattern_{i}}\right))$
    $Store = GC\_Generate(Store(DistributionPropability_{pattern_{i}}))$
    $FinalCipher;_{i=} Process\ \left(^{Orginized}Cipher\_C_{ESB_{i}}, DistributionPropability_{pattern_{i}}\right)$
    End for
```

The encryption process takes an action under *for* loop as long as the block size in order to process all blocks within the plaintext message.

b. CHSA Decryption

The decryption process as in all encryption standards and algorithms performed by the inverse of the encryption process was all process taken place in reverse order to retrieve the original plaintext. CHSA decrypts the ciphertext through the use of stored keys and patterns inside GC. GC provides the CHSA with all necessary terms for the decryption process.

Algorithm 2: CHSA Decryption Syntax

```
Input: $FinalCipher$
Output: $Plaintext$

1-  Redistribute ($FinalCipher$)        // redistribution function
    $for\ i = 1\ to\ FinalCipher_{length}$
    $Distrbution_P = retraive\ (Address_{pattern_{distrbution}}, Distrbution_{pattern,} Orginized_{Cipher_{C_{ESB_i}}})$
    $Orginized_{Cipher_{C_{ESB_i}}}$ = Redistribute ($Distrbution_P, FinalCipher_i$)
    $end\ for$
2-  Reorganize ($Orginized_{Cipher_{C_{ESB_i}}}$)
    $for\ i = 1\ to\ length(Orginized_{Cipher_{C_{ESB_i}}})$
    $Join_p = retraive\ (Address_{pattern_{organizing}}, join_{pattern_i})$
    $Cipher_{C_{ESB}} = reorganize\ \left(join_{pattern_i}, Orginized_{Cipher_{C_{ESB_i}}}\right)$        // reorganizing the distributed patterns
    $end\ for$
3-  Decrypt_Key ($Cipher_{C_{ESB}}$)
    $for\ i = 1\ to\ length\ (Cipher_{C_{ESB}})$
    $KeyStream_i = retraive\ (Address_{Key}, KeyStream_i)$        // retrieve the key stream of the ciphertext
    $C_{ESB\ i} = Decryption\ (KeyStream_i, Cipher_{C_{ESB}})$
    $end\ for$
4-  De_confusion ($C_{ESB\ i}$)
    $for\ i = 1\ to\ length\ (C_{ESB\ i})$
    $Confusion_p = retrieve\ \left(Address_{Confusion}, ConfusionPattern_i\right)$
    $ESB_i = redistbute\ (C_{ESB\ i}, Confusion_p)$        // retrieve the distribution of the blocks
    $end\ for$
5-  DecryptStreamCipher ($ESB_i$)
    $for\ i = 1\ to\ length\ (ESB)$
    $StreamKey_i = retraive\ (Address_{Stream}, StreamK_i)$        // retrieve the stream key
    $ESB_{i =} Decrypt\ (ESB, StreamKey_i)$        // decrypt the stream cipher block using the key
    $end\ for$
6-  PlaintextRetrieve ($ESB$)
    $padding_p = retrieve\ (Address_{Pattern_{padding}}, Padding_{Pattern})$        // retrieve the padding pattern
     $Plaintext_{message} = join\ \left(ESB_i, padding_p\right)$        // padding the last block
7-  DestroyPatterns ($padding_p, Confusion_p, Join_p, Distrbution_P$)        // destroy all patterns in the GC
8-  DestroyKey ($StreamKey, KeyStream$)        // destroy all keys in the GC
```

The decryption process within CHSA depends on the reverse processing and storing center within GC. All key streams and patterns stored in SC. The process of specifying the address of the pattern or the key is performed using Address record stored in the GC. SC contain a special table called *AddressTable* that containing the full address of each block and each pattern. The *Address* of the block stored to be retrieved by the desirable phase.

The complexity of the encryption/decryption process came from the mathematical processing and pseudo-random pattern and key generation. The chaining process, confusion process, distribution process, and organizing process make it very hard and complex for the cryptanalyst to attempt retrieving all the system arguments because each block has a key that differs from the other keys stored in the SC.

3 Implementation and Results Analysis

The process of implementation of the new algorithm requires a programming language with a large capacity to deal with data of all kinds and also must have the ability to deal with networks in order to secure the files and transmission over the network to the recipient. A new system was implemented to implement the new hybrid algorithm within the Visual Studio environment. The algorithm succeeded in encrypting the data in a new way. It worked on splitting the clear text and then coding it using the RC4 algorithm and then integrating the key and some additional processes to get the encrypted text. Table 1 shows the results for each of the algorithm's operations for, as well as the total duration of several types of experiments represented in Table 2.

In Table 2, it is possible to note that the time taken to perform encryption operations ranges between 0–2 s and 12 s as the maximum time in the encryption process and the maximum encoding process can be observed in video files which are the largest file types in size in network applications. Table 2 represents the time taken by each encryption process within the hybrid algorithm for the creation of encoded text since each process has a different key from the other because of the key generation center, which gives each algorithm a different key depending on the semi-random generation algorithms. Table 3 shows the results of organization information and S-box distribution operation performed by the CHSA.

Because the last stage of the algorithm is the probability distribution variable by semi-random pattern, we find that it is found in Tables 2 and 3. This phase contains several sub-phases, such as RSA and process stages to increase the randomness and strength of the encoded text Permutation. Overall, the processes in Table 3 took relatively less time than the encodings in Table 2 because the mathematical structure of these processes was less than the coding processes. Figure 4 illustrates the results gained from the encryption algorithms in CHSA with file encryption and the operations of CHSA on files.

These results were in terms of files within the operating systems within the computers either in the network systems, the implementation of the algorithm is through the use of PHP programming language as a common language in the applications of the Internet and networks and various applications of the internal sharing of files. The CHSA algorithm was built by the PHP programming language and also performed file encryption experiments during the transmission and receiving process. The results showed that the time spent in the encryption process exceeded what it was in the operating system due to the time it took to load the file and the time it took to convert the file to the formula And finally the time spent in the process of sending to the receiving party and all these additional times increased the overall time spent in the encryption process using the CHSA algorithm. Table 4 shows the time spent in encrypting data using the CHSA algorithm for network applications as well as Fig. 5 that illustrate the difference between the OS operation and network operation in CHSA.

Table 1 Results came from string encryption when using CHSA

Data type	Block cipher	Stream cipher	Adding encryption key	Probability distribution
String plaintext	65537d410d00c52ed7d34dd7e03563345997cf61d872be2c9451e2c03abb69156af664ad7619d24d	93dd6077dd2424e64effffd31993826635ce2f98cc5c7a6734f28370ab502ce9ae539ac9936ac2	ba65567b3ac7b100767b582fb6af11d244a14184ba8c57772a37ee128acad2881461cc911001d1cbf58e4956d9516e	5ad0abb839b660c3b5f423eb395cbed3aa239d3f4ef7ffb1b87af977c21a89f253291938ab9121581d9253488d0b893d5a1b707e9e59998cebd5e42f37bc8707742f217ddff693da73ade9e21324f75580cf2350079e4547eabd33543de7b37

Table 2 Results came from file encryption when using CHSA

Data type	File size	Block cipher (s)	Stream cipher (s)	Adding encryption key (s)	Probability distribution (s)
String plaintext	180 character	0.2	0.2	0.3	0.4
.TEXT	4 KB	0.5	0.8	0.6	1
.DOC	12 KB	0.9	0.7	0.9	1
.PNG	40 KB	3	3.5	4	2
.PDF	231 KB	7	8	7	8
.MP4	3240 KB	10	11.3	12	10.2

Table 3 Results came from file encryption when using CHSA (organization processes)

Data type	File size	S-box (s)	Block organizer (s)	Probability distribution (s)
String plaintext	180 character	0.3	0.11	0.4
.TEXT	4 KB	0.51	0.55	1
.DOC	12 KB	0.7	0.76	3
.PNG	40 KB	1	2.15	1.5
.PDF	231 KB	4	3.9	4
.MP4	3240 KB	5	4.16	1.2

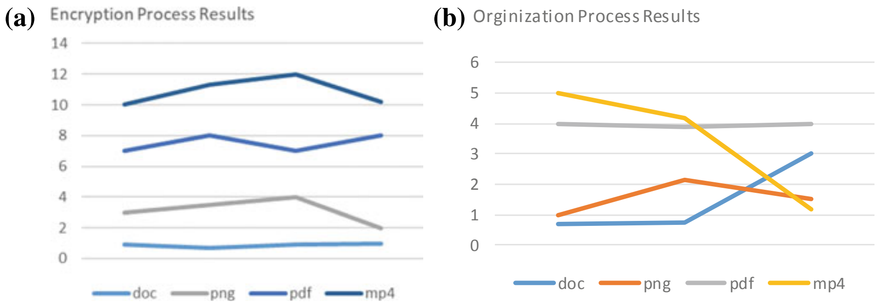


Fig. 4 CHSA results from both encryption and security functions

4 Conclusion

The hybrid algorithm is the process of integrating more than one algorithm at a time in order to take advantage of the existing features in each algorithm. The purpose of increasing the complexity of the CHSA algorithm is to increase data security. The greater the complexity, the greater the security of the data. The structure of the algorithm consists of 6 main parts in each of these parts is a mathematical algorithm

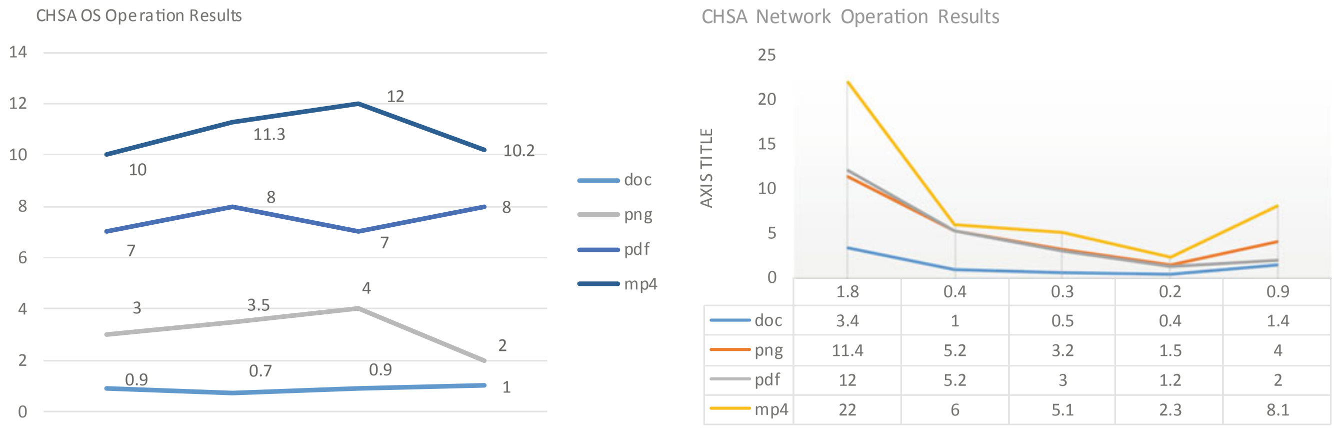
Table 4 Results came from file encryption when using CHSA (network application using PHP)

File type	File size	Upload time (s)	Conversion time (s)	Block cipher (s)	Stream cipher (s)	S-box (s)	Adding encryption key (s)	Probability distribution (s)
String data	220 character	0.4	0.1	0.2	0.2	0.1	0.4	0.2
.TEXT	3 KB	1	0.3	0.5	0.4	0.3	0.2	0.9
.DOC	15 KB	1.6	0.5	1.3	1	0.5	0.4	1.4
.PDF	1 MB	4	3	5	5.2	3	1.2	2
.PNG	1.4 MB	4.3	3.1	4	5.2	3.2	1.5	4
.MP4	4 MB	9	6.3	7	6	5.1	2.3	8.1

specialized in data security. In the first part, the algorithm divides the clear text into blocks in order to be passed to the other stages. This is known as a block cipher since the data is cut into blocks of equal size. The data then flows to the stream cipher process, which in turn encodes the blocks that were cut at the beginning of the algorithm. The third stage is to add more randomness to the system using the S-box. The fourth stage is to add the key-encryption key to clear text parts. The fifth stage is the process of redistributing the blocks, which are scattered in a random order. The sixth and final stage is the process of authentication or coding at random according to the pattern sent by the generation center.

The CHSA algorithm contains a special center for generating keys called the generation center, which is responsible for generating all types of keys for all algorithms within the CHSA. Each of the six algorithms has special keys that differ from the other algorithms. Therefore, the task of the generation center is to provide these algorithms with the necessary keys to perform their functions. As for the method of storage of these keys, there is a storage facility located within the center of the generation used to store the keys that are generated through the center of generation and use by other algorithms. The storage unit at the generating station shall be responsible for storing and retrieving these keys at the time of need in the decryption process for the recipient in the case of network systems and for the user if he uses the same operating system.

The algorithm was tested by encrypting a number of files within the operating system. These files were text string, text file, images, video, and e-books in pdf format. The algorithm showed its ability to encrypt data in such a complex way that it is difficult to analyze the code for the algorithm. The results showed that the minimum time spent in the encryption process in the CHSA algorithm is 0.5 s, which is the total time spent in the coding process of the text string, which is the simplest input type for the encryption algorithm, while the largest time taken by the algorithm is about 32 s when encrypting video files in mp4 format which are considered The largest input type of the algorithm in terms of size and found that the algorithm in total takes more time than the rest of the algorithms is relative because of the multiple stages of encryption contained in the algorithm and because of these multiple stages, the encryption takes more time than in traditional algorithms. However, the



	1.8	0.4	0.3	0.2	0.9
doc	3.4	1	0.5	0.4	1.4
png	11.4	5.2	3.2	1.5	4
pdf	12	5.2	3	1.2	2
mp4	22	6	5.1	2.3	8.1

Fig. 5 CHSA results comparison between OS application and network application

most important feature of the CHSA algorithm is the strength in encryption and complexity of the encoded text, since the process of parsing the code is almost impossible given the number of random processes contained in the algorithm and its encryption algorithms and reliability.

After obtaining results and statistics for the CHSA algorithm, it is necessary to mention the effect of this algorithm in the face of attacks targeting both the operating system and network applications. Here lies the real strength of security algorithms in responding to these attacks. The CHSA algorithm proved effective against Trojans and viruses that open the gaps between the victim's operating system and the hacker to analyze the code as the data will be useless for the hacker. As for the network's many attacks, the most powerful types of attacks that network systems may face and the application of the algorithm have been chosen to determine their effectiveness in preventing these attacks. It has proven that it has been able to prevent 3 of the 4 attacks considered the most dangerous in the network world.

As a future development of the CHSA algorithm, two main directions must be developed to develop its work. The first is to increase the complexity of the algorithm by adding new and complex stages in order to increase the strength in the face of as many attacks on both the operating system and the network applications. Work on increasing the speed of the algorithm to make it more suitable for applications that require real-time processing process, i.e., video applications over networks, which require high-speed encryption algorithms so increasing the speed of implementation of this algorithm is an important trend very in the development process.

References

1. Ismail M, Gerard C (2012) Evaluation of different cryptographic algorithms on wireless sensor network nodes. IEEE Int Conf Wirel Commun Undergr Confin Areas. https://doi.org/10.1109/ICWCUCA.2012.6402500
2. Timothy DP, Santra AK (2017) A hybrid cryptography algorithm for cloud computing security. Int Conf Microelectr Dev Circ Syst (ICMDCS), IEEE. https://doi.org/10.1109/ICMDCS.2017.8211728
3. Li X, Li X, Wei L (2013) The application of hybrid encryption algorithm in software security. In: 3rd international conference on consumer electronics, communications and networks, IEEE. https://doi.org/10.1109/CECNet.2013.6703419
4. Yu L, Wang Z, Wang W (2012) The application of hybrid encryption algorithm in software security. In: Fourth international conference on computational intelligence and communication networks, IEEE. https://doi.org/10.1109/CICN.2012.195
5. Mandal AK, Parakash C, Tiwari A (2012) Performance evaluation of cryptographic algorithms: DES and AES. In: IEEE students' conference on electrical, electronics and computer science, IEEE. https://doi.org/10.1109/SCEECS.2012.6184991
6. Patel JR, Bansode RS, Kaul V (2012) Hybrid security algorithms for data transmission using AES-DES. In Int J Appl Inf Syst (IJAIS) 2(2). ISSN: 2249-0868 Foundation of Computer Science FCS, New York, USA
7. Bhatele KR, Sinhal A, Pathak M (2012) A novel approach to the design of a new hybrid security protocol architecture. In: IEEE international conference on advanced communication control and computing technologies, IEEE. https://doi.org/10.1109/ICACCCT.2012.6320816

8. Panda PK, Chattopadhyay S (2017) A hybrid security algorithm for RSA cryptosystem. In: 4th international conference on advanced computing and communication systems (ICACCS), IEEE. https://doi.org/10.1109/icaccs.2017.801464
9. Mitchell CJ (2016) On the security of 2-key triple DES, IEEE transactions on information theory 62(11). https://doi.org/10.1109/TIT.2016.2611003
10. Weerasinghe TDB (2013) An effective RC4 stream cipher. In: IEEE 8th International conference on industrial and information systems, IEEE. https://doi.org/10.1109/ICIInfS.2013.6731957
11. Ahmad A, Farooq M, Amin M (2016) SBoxScope: a meta s-box strength evaluation framework for heterogeneous confusion boxes. In: 49th Hawaii international conference on system sciences (HICSS), IEEE. https://doi.org/10.1109/HICSS.2016.685
12. Wang X, Wang S, Zhang Y, Luo C (2018) A one-time pad color image cryptosystem based on SHA-3 and multiple chaotic systems. Optics Lasers Eng 103:1. https://doi.org/10.1016/j.optlaseng.2017.11.009
13. Vybornova YD (2017) Password-based key derivation function as one of Blum-Blum-Shub pseudo-random generator applications. Proc Eng 201. https://doi.org/10.1016/j.proeng.2017.09.669
14. AL-Mousawi AJ, AL-Hassani HK (2017) A survey in wireless sensor network for explosives detection. Comput Electr Eng. https://doi.org/10.1016/j.compeleceng.2017.11.013
15. Narasimha Mallikarjunan K, Muthupriya K, Mercy Shalinie S (2016) A survey of distributed denial of service attack. In: 10th international conference on intelligent systems and control (ISCO), IEEE. https://doi.org/10.1109/isco.2016.7727096
16. Smyth D, McSweeney S, O'Shea D, Cionca V (2017) Detecting link fabrication attacks in software-defined networks. In: 26th international conference on computer communication and networks (ICCCN), IEEE. https://doi.org/10.1109/ICCCN.2017.8038435
17. Shaikh AA (2016) Attacks on cloud computing and its countermeasures. International conference on signal processing, communication, power and embedded system (SCOPES), IEEE. https://doi.org/10.1109/SCOPES.2016.7955539

Performance Assessment of Various Encoding Schemes with Bit Stuffing

S. Bharath and Gayathri Narayanan

Abstract This paper discusses the implementation of a novel technique of encoding data bits using the concept of bit stuffing in addition to the conventional methods of source coding. This technique can be applied to any of the existing methods of source encoding under controlled conditions. In particular, the method is very efficient when the encoded bits have more number of ones or zeros than a predefined threshold, at any point of time and in any part of the stream. Usually, bit stuffing is a common method used for data compression in data communication layers to reduce the bandwidth. In this paper, we have attempted to incorporate bit stuffing in various encoding schemes and have compared the improvement in performance with and without bit stuffing. The software used for simulation is MATLAB. The primary motivation of this work is to determine the maximum amount of bandwidth savings that can be achieved due to bit stuffing for a random series of alphabets.

Keywords Arithmetic encoding · Bit stuffing · Huffman coding · Redundancy

1 Introduction

Source encoding is the process of encoding the data bits and preparing it for transmitting across the channel length in an efficient manner so as to decrease the overall bandwidth and increase the data rate. Source encoding is done to eliminate redundancy. Redundancy translates to the wastage of bandwidth in the channel. Source encoding is accomplished by reducing redundancy and compressing the data before it is sent to the channel while channel encoding adds redundancy to ensure reliable reception of data stream. Channel encoding is done to overcome the effect of noise in the channel. A source encoding scheme is applied to a system based on some specific pattern that the source follows, which could be either the probability of each symbol

S. Bharath (✉) · G. Narayanan
Departtment of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India
e-mail: bharath.jsk@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_11

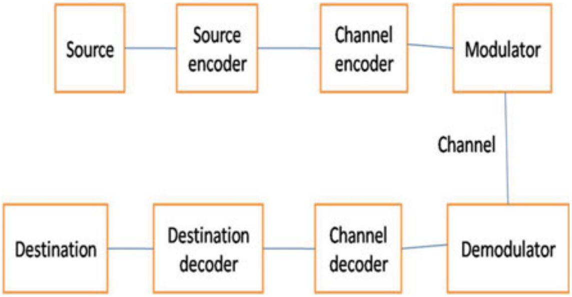


Fig. 1 Model of a simple digital communication channel

or uniqueness in the occurrence of the symbols. Any source encoding scheme should generally satisfy the following properties:

- Uniqueness
- Prefix free
- Instantaneous

The coding scheme should provide unique code words to each symbol used. A prefix code is a code that follows 'prefix property' for example, a code with code words [4 0 15] may be said to be a prefix code while another code with code words [4 0 41] does not follow prefix property. The code word of any symbol should not be a prefix of a code word for another symbol. A prefix code is usually uniquely decodable because given a complete sequence the receiver can identify each word without requiring a marker between each word. The final code should be instantaneously decodable which means that the decoded data should not be ambiguous. In arithmetic encoding scheme, we transmit a tag value based on the probability distribution in each symbol instead of making code words for each symbol. The concept of 'Information' in Information Theory deals with the amount of uncertainty in an event. Average entropy is the average rate at which information is produced by a particular stochastic source. Redundancy is then referred to be the difference of entropy $H(X)$ of an ensemble X and its maximum possible value, i.e. if there are N ensembles for equal probability distribution, then (Fig. 1).

$$R = H(X) - \log_2(1/N)$$

2 Related Works

There are certain encoding schemes where probability distribution is not used for coding the data bits like the Lempel Ziv method [1]. This paper focuses on Huffman and Arithmetic encoding schemes by incorporating bit stuffing. Considering the whole set of existing encoding schemes Huffman and Arithmetic encoding are considered to be the most effectual based on the compression efficiency. Bit stuffing is a novel idea as presented in [2] where we insert a non-informative bit in between the data stream so as to break a common pattern followed in the data stream. Bit stuffing is useful only if the data stream follows a specific pattern. There are some existing works on the use of bit stuffing in steganography [3] to improve the encryption of data. The above-mentioned paper is about 'graphstega' using Huffman encoding to hide a potential secret. Bit stuffing is also found useful for crosstalk avoidance in high-speed switching [4].

Huffman code is a particular optimum variable-length prefix code usually used in the lossless data compression. It is based on the probabilities of each symbol used in the stream. In one of the reference papers [5], the authors suggest a modified Huffman coding to improve its performance and redundancy based on the minimum variance Huffman coding. A universal design of arithmetic coding algorithm using the software and hardware design is presented in [2] where 256 ASCII codes of distinct symbols, as a particular example, are accommodated in the alphabet. Accordingly, both the coding equations are modified by indicating the code values as the lower end-point value of the coding range and the width of this range. Thus the flow of sending output codes, solving the so-called underflow problem, and updating the coding range can be integrated and simply controlled by the value of the coding range.

Various variants of arithmetic coding schemes are now available for different purposes like image and audio compression. In [6], a method of context-based adaptive arithmetic coding is suggested for compression of image. The concept is based on parallel leading zero detection and bit stuffing handling where the symbols are encoded and decoded in one cycle. In this paper, we deal with text as the data entity and encoding it according to its probability distribution. We present three main functional blocks namely, 'arithmetic encoding and decoding', 'bit stuffing', 'bit de stuffing' to compare the efficiency of transmitted data after source encoding with arithmetic and Huffman method.

3 Proposed Work

3.1 Arithmetic Encoding and Decoding

The state of the art in source encoding is arithmetic encoding scheme as it represents the data more compactly. It has an optimal performance without the need for blocking of input data. It encourages a clear separation between the model for representing data and the encoding of information with respect to that model. In arithmetic encoding, the message output data is represented by an interval between 0 and 1. The range of this interval reduces as the size of the message data is bigger. As the size of this interval reduces more no of bits are required to represent the data. In this paper, simulation is done with MATLAB and we found that it's difficult to figure out the tag number if direct arithmetic coding is applied to an audio signal. Many modified arithmetic logics are presented before like [7] which could compress an image, audio or video. This paper is to account for a pattern observed in arithmetic encoded sequences where it's common to have observed more number of consecutive similar bits in the code. As the message size increases this pattern is observed to increase. Consecutive symbols of the message reduce the size of the interval according to the symbol probabilities generated by the model. The more probable symbols reduce the range lesser than the least probable symbols adding fewer bits to represent the data.

3.2 Bit Stuffing

As in bit stuffing concepts normally used, it is a method of data compression that takes care of a certain known pattern used repeatedly in a sequence of data. If a pattern repeats in a binary sequence, then it could eventually be replaced by a bit '1' stuffed in between the sequence. This requires that a code must check for a certain pattern regularly and stuff either a '0' for absence or '1' for presence of that pattern. The encoder and decoder should know the pattern followed and the method used for bit stuffing so as to decode the message accurately. There are many existing papers on modification to bit stuffing algorithm as in [8] which are applied in different contexts. There are some existing works [9] about deriving lower bounds on the capacity of certain two-dimensional constraints by considering bounds on the entropy of measures induced by bit stuffing encoders.

In this module used for simulation, the program searches for five consecutive one's or zero's if two of them are already found successively. The module writes the first two consecutively repeated bits for transmitting and adds an extra bit that says if the third, fourth and fifth bits are being repeated the same value. This module adds or stuffs '1' if they are repeated and '0' for the other condition. If the stuffed bit is '1' then the further third fourth and fifth repeated bits are ignored. On the other hand, if the stuffed bit is '0' no bit is ignored. Thus, if two bits repeating pattern are more in our sequence with no five-bit repeating pattern, it leads to a considerable increase in bandwidth.

3.3 Bit De-Stuffing

This is the process by which the bit stuffed sequence at encoder is recovered at the destination decoder. Here whatever modifications made for bit stuffing which accounts for the extra stuffed bits indicating the presence or absence of the pattern is eliminated. In this module used for simulation, every third bit that comes after two repeated bits is ignored. Also that if this third bit is '1' three repeated 1's are stuffed instead of this ignored third bit.

4 Result Analysis

MATLAB is one of the most widely used programming platforms in which a wide range of operations can be performed on the input signals and their functions can be plotted. MATLAB considers any signal as a matrix of numbers and performs operations on them. This paper focuses on encoding text messages where the probabilities of individual symbols are taken from Pavel Mika's database which cites Robert Leward's cryptological mathematics. For arithmetic encoding, the probabilities of individual symbols are calculated according to their occurrences and frequencies in the sentence. Before transmitting anything the range of the message is from 0 to 1, i.e. $0 \leq x < 1$. An extract from Stephan Hawking's 'A Brief History Of Time' is taken as the message for the simulation purpose. The basic procedure for arithmetic encoding is demonstrated below with a simple example as shown in Table 1. Suppose that 'HOUSE' is to be coded under arithmetic encoding scheme. We have the individual probability distribution of '*H*', '*O*', '*U*', '*S*', '*E*' as 0.2, 0.2, 0.2, 0.2, 0.2 taking probabilities based on their occurrence frequencies of each alphabet. As each alphabet occur only once in the message string, the probability of each alphabet is assumed to be the same. Initially, both the encoder and decoder know the entire range to be [0, 1]. As each alphabet is coded the range to be considered decreases. The range for each letter is assigned by taking the cumulative probability for the ascending order of alphabets. Thus the range for these alphabets will lie as in Table 1.

When the encoder see '*H*' it limits the range to [0.2, 0.4] and sets the new range. When '*O*' is sensed the range further narrows to the third one-fifth of the above range and it goes on until the end of the message. Finally, the encoder is left with a range whose difference is called the tag which is transmitted in arithmetic encoding scheme.

This binary tag is passed through bit stuffing to realize that the bandwidth is reduced considerably. Similarly, a Huffman coded sequence is passed through the bit stuffing module and was found that the bandwidth decrease was less compared to arithmetic code which gives insight to the pattern followed in the sequence as mentioned above.

It's found that bit stuffing has less effect on Huffman coding or rather it may increase the bandwidth of encoded message for short messages. Considering a text message of length 5 in MATLAB, length of coded bits is 20 bits without bit stuffing but the length increases to 27 bits on bit stuffing indicating the presence of 7 stuffed

Table 1 Sample alphabet set and their probabilities

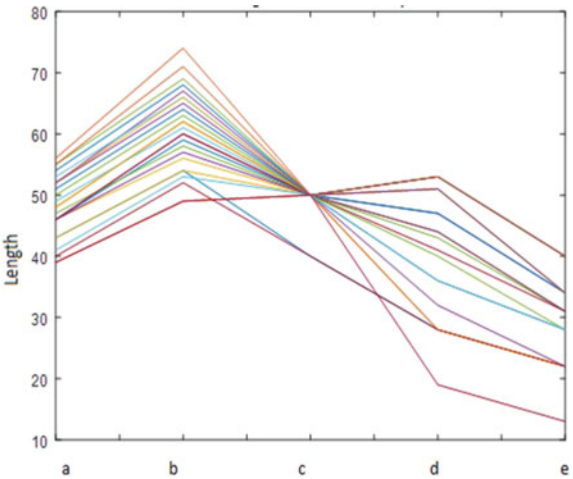
Alphabet	Probability	Range
E	0.2	[0, 0.2]
H	0.2	[0.2, 0.4]
O	0.2	[0.4, 0.6]
S	0.2	[0.6, 0.8]
U	0.2	[0.8, 1]

0's and no bit savings. For a length 10 text message, the bit stuffed code indicates the presence of 13 stuffed 0's and no bit savings. But when the length of the text message increased to 15, Huffman coded sequence saved 24 bits indicating 12 stuffed 1's and added an extra 6 bits indicating 6 stuffed 0's through bit stuffing. Thus 18 net saved bits are found with bit stuffing. This says that as the size of the message increases bit stuffing has a considerable effect on Huffman encoding.

In case of arithmetic coding, bit stuffing has a considerable effect on any length of message. For a length 5 text message in MATLAB, the coded sequence is 24 bits long without bit stuffing but it reduced to 16 bits after bit stuffing indicating the presence of more consecutive similar bits. Similarly, for a length 10 text message, the code length was 28 bits without bit stuffing which reduced to 22 bits after bit stuffing. For a length 15 text message the code length reduced from 64 bits before bit stuffing to 43 bits after bit stuffing. Length of the code varies depending on the text message and the frequency of each letters in them but this trade-off is taken care off by suppling similar messages in each case. Thus, arithmetic encoding scheme stands out as better data compression with bit stuffing.

For random text messages of size 10 and 20 the graphs in Figs. 2 and 3 shows the effect of the length of Huffman code without bit stuffing, length of an arithmetic code without bit stuffing, traditional encoding with N bits for 2^n symbols without bit stuffing, normal arithmetic code without bit stuffing, normal arithmetic code with bit stuffing respectively for a, b, c, d and e shown in X-axis. Figure 2 is about 25 different, random, size 10, text messages generated by 'rand' command in MATLAB environment. Figure 3 is about 7 different, random, size 20, text messages. Comparing the two figures, one can observe that as the text size of the message increased the bit stuffing gets more effective. More sequences are given here to generalize the concept. We also observe that we have a common convergence point which is because of the fact that MATLAB software random function generates equal no of different letters

Fig. 2 Code lengths of 25 different, random, size 10, text messages



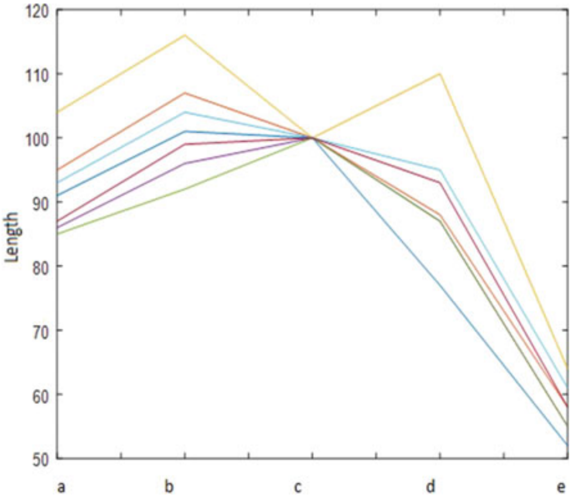


Fig. 3 Lengths of 7 different, random, size 20, text messages

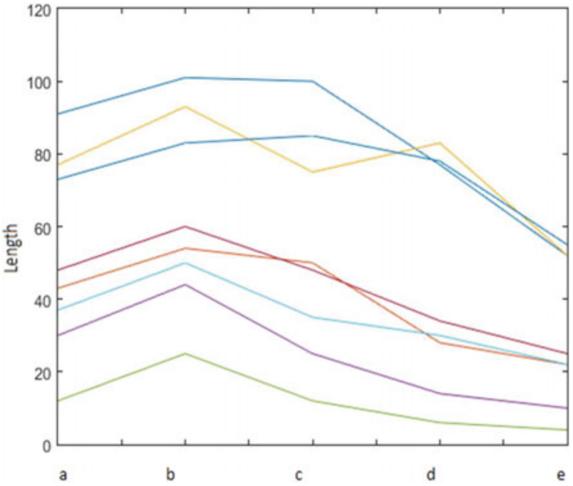


Fig. 4 Length of varies code for the size of text messages $N = 5$, 10, 15, 20 and 25

most of the time. Figure 4 clearly shows that as size of text message increases bit stuffing becomes more efficient in arithmetic codes.

5 Conclusion

This work presents a performance analysis of various encoding schemes like Huffman and Arithmetic encoding with bit stuffing. The chosen schemes are the most efficient in terms of their source encoding efficiency. This work attempts to improve the efficiency of Huffman and Arithmetic coding schemes by incorporating the concept of bit stuffing, under chosen conditions. It shows the importance of bit stuffing in data compression as the length of the text message increases. The simulation studies were carried out using MATLAB software. It was observed that arithmetic encoding with bit stuffing stands out in performance as a better data compression or source encoding scheme.

References

1. Savari SA (1997) Bell Labs Lucent Tehnol Murray Hill USA: redundancy of the Lempel Ziv codes. In: Proceedings of IEEE international symposium for information theory
2. Jiang J (1995) Novel design of arithmetic coding for data compression. IEEE Proc Comput Digital Technol 142(6):419
3. Akhter F (2016) Secured word-by-word graph steganography using Huffman encoding. In: 2016 international conference on computer communication and informatics (ICCCI)
4. Chang C-S, Cheng J, Huang T-K, Huang X-C, Lee D-S, Chen C-Y (2015) Bit-stuffing algorithms for crosstalk avoidance in high-speed switching. IEEE Trans Comput 64(12):3404
5. Sandeep GS, Sunil Kumar BS, Deepak DJ (2015) An efficient lossless compression using double Huffman minimum variance encoding technique. In: International conference on applied and theoretical computing and communication technology (iCATccT)
6. Ong KK, Chang W-H, Tseng Y-C, Lee Y-S, Lee C-Y (2002) A high throughput context-based adaptive arithmetic codec for JPEG2000. IEEE 2002
7. Marpe D, Schwarz H, Wiegand T (2003) Context-based adaptive binary arithmetic coding in the H.264/AVC video compression standard. IEEE Trans Circ Syst Video Technol 13:620
8. Aviran S, Siegel PH, Wolf JK (2005) An improvement to the bit stuffing algorithm. IEEE Trans Inf Theory 51(8):2885
9. Halevy S, Chen J, Roth RM, Siegel PH, Wolf JK (2004) Improved bit-stuffing bounds on two-dimensional constraints. In: Proceedings IEEE international symposium on information theory

3D(Dimensional)—Wired and Wireless Network-on-Chip (NoC)

N. Ashokkumar, P. Nagarajan and P. Venkatramana

Abstract Network on Chip is a special unique case of parallel computing systems defined by the tight constraints such as availability of resources, area, cost of the NoC architecture and power consumption. NoC is designed with three main components: switches, Network Interfaces (NIs) and links. NoC is used for several application domains, such as multi-media processing, consumer electronics, biological applications, etc. NoC is the technology proposed to solve the shortcoming of buses. This technique is used to design communication subsystem among IP cores (Intellectual property core) in a SoC design. In this chapter, we have discussed about 3D integrated circuits, 3D wired and wireless NoC, Emerging Technologies, and Literature Survey.

Keywords 3D NoC (3Dimensional Network-on-Chip) · TSV (Through silicon via) · Wired and wireless NoC · Topology

1 Introduction 3D-ICS

The issues connected with the high wiring network necessities of large scale joining circuit configuration is investigated in [1] alongside how 3D ICs improve availability while decreasing the quantity of long interconnects. So also, the creators of [2, 3] research how 3D ICs can be utilized to battle the developing proportion of interconnect to entryway delay as highlight sizes diminish. A general diagram of 3D innovations and the inspirations driving outlining 3D coordinated circuits is introduced in [4]. The vertical interconnect innovations contain micro bumps, wire

N. Ashokkumar (✉) · P. Nagarajan · P. Venkatramana
Department of Electronics and Communication Engineering, Centre for VLSI and Embedded Systems, Sree Vidyanikethan Engineering College, Tirupati, India
e-mail: ashoknoc@gmail.com

P. Nagarajan
e-mail: nagarajan.pandiyan@gmail.com

P. Venkatramana
e-mail: pvramana2406@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_12

holding remote interconnects utilizing capacitive/inductive coupling, and through-silicon vias (TSVs), of which TSVs suggest high-thickness vertical interconnects and are by a wide margin the most encouraging method [5]. The advantages of utilizing 3D NoC rather than 2D NoC are investigated by Feero and Pande [6]. These work approaches on the performance and area effects of the network structures rather than the power and performance tradeoffs of various technologies. 3D ICs gives an equivalent set by long inbuilt through stacking active silicon layer. In this manner, one can expect huge increments in execution and lessening in force utilization and territory with conceivable integration of CMOS circuits with different innovations [5, 7, 8]. 3D ICs suggest various favorable positions contrasted with 2DICs. These incorporate:

- Shorter global interconnects
- Superior performance
- Smaller area (footprint)
- Low power consumption
- Scope of mixed-technology ICs
- Higher packing density.

In any case, 3D ICs have huge worries as warm thought. While the general force dispersal in 3D ICs might be lower because of shorter and less worldwide interconnects, the force thickness is much higher because of vertically stacked silicon layers. Thusly, capable warm organization is the best approach to guarantee the execution redesigns offered by 3D ICs. For more unmistakable cognizance on this subject, Emerging Interconnect Technologies for 3D Networks-on-Chip per users are referred to the distinctive warm methodologies, for instance, physical arrangement streamlining, usage of warm vias, and microfluidic cooling of the vertical stack reported in the writing [9–11].

The 3D reconciliation innovation we utilized depends on Tezzaron [7] that utilizations TSV for fringe IOs and microbumps for bury bite the dust associations. The two-level 3D stacking technique depends on wafer-to-wafer holding, up close and personal technique with by means of first approach as outlined in Fig. 1. The between kick the bucket micro bumps give high interconnection thickness up to 40,000 per mm^2 without interfering to FEOL (front-end-offline) device or routing layers. It is additionally conceivable to execute four levels by stacking through consecutive utilizing TSV of the two face to face stacking so as to have higher outline many-sided quality yet it won’t be secured in this work.

In advanced technology, we analyze the 3D NoC architectures we select 45 nm standard library from ST Microelectronic [8]. We utilize comparative 3D structure for between level associations utilizing microbumps as a part of Tezzaron innovation however we replace the 130 nm technology of Global Foundries with 45 nm ST Microelectronic standard library. The 45 nm innovation utilized as a part of this study has seven metal layers where metal seven is utilized for holding and the steering is constrained until metal six.

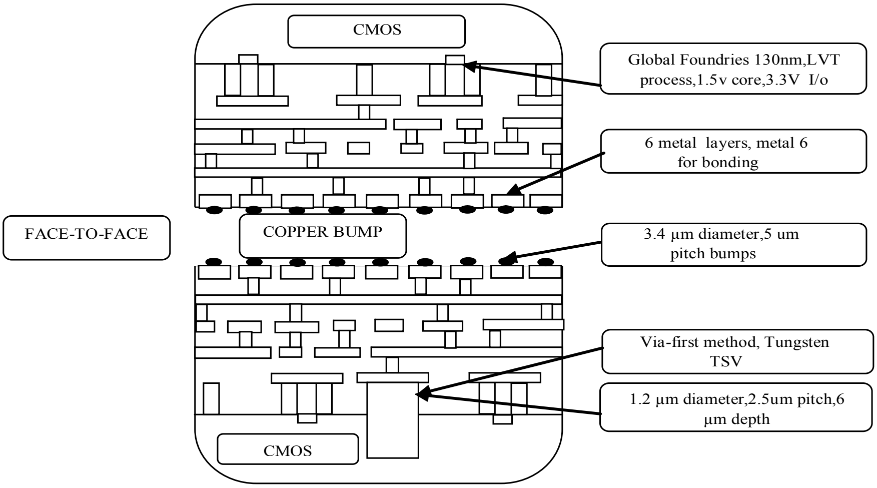

CMOS
Global Foundries 130nm,LVT process,1.5v core,3.3V I/o
6 metal layers, metal 6 for bonding
FACE-TO-FACE
COPPER BUMP
3.4 μm diameter,5 um pitch bumps
Via-first method, Tungsten TSV
1.2 μm diameter,2.5um pitch,6 μm depth
CMOS

Fig. 1 Cross section of Tezzaron 3D IC technology with corresponding parameters

2 3D-Wired and Wireless NoC

2.1 Wired NoC

As one of the more well known vertical network technologies, through silicon via (TSVs) and some of their manufacturing methods are described in [5] alongside TSV electrical characteristics extraction and demonstrating. TSVs add extra many-sided quality to the fabricating process for 3D ICs yet they lead to offer power, performance of execution, and chip range qualities.

2.2 Wireless NoC

In [7], a low power and high information rate inductive coupling transceiver is proposed. Inductive coupling is a vertical technology innovation that does not require adjustments to the assembling procedure, however, the force, execution, and chip range overheads are regularly restrictive to the appropriation of the innovation. The design and implementation of a capacitive coupling handset is broke down in [8] where the force, execution, and region overheads are examined and also limitations that capacitive coupling joins put on how the layers of the 3D ICs are collected. Capacitive coupling additionally does not oblige changes to the assembling procedure but rather confines vertical scaling to two layers put confronted to confront rather than numerous layers put face to back. It too displays poor performance, execution, and chip zone overheads in respect to inductive coupling what's more, wired procedures.

3 Emerging Technologies

Some experimental advances show potential for being powerful at decreasing vitality utilization and increase execution yet are not secured in this work. One of the all the more encouraging innovations is photonic interconnects. Photonic interconnects exchange information by sending signals over optical waveguides. In [5], TSVs and a reconfigurable photonic system are used to decrease vitality utilization while looking after execution. Photonic interconnects have the advantage of their data transfer capacity being autonomous of the correspondence separation. Lamentably, there are additional fabricating steps that are required to assemble circuits that incorporate photonic interconnects. These additional strides add to the unpredictability and general expense of these frameworks. Another innovation for associating centers in a framework uses remote interconnects. Radio recurrence handsets can be incorporated with the chip and used to transmit information crosswise over bigger separations with less power and less inertness than customary wires. Little world systems and millimeter-wave remote systems on chip are investigated in [9, 10]. In [11], remote interconnects that use CDMA to permit different remote handsets to work in the meantime are reenacted to break down their execution and vitality qualities. Remote interconnects can likewise be used for exchanging information between layers of 3D ICs as in [12].

Previously, the possibility of remote correspondence in planar 2D NoCs has been proposed by a couple of researchers. A remote direct in 2D NoCs wears down high data transfer capacity, single-skip, long-go correspondence, as against multihop correspondence in steady wired NoCs, realizing lower stillness, lower power use, besides, less difficult controlling arrangements. The possibility of remote correspondence in 2D NoCs was at first highlighted by Floyd et al., where a clock dispersal framework was executed using remote interconnects. In addition, the remote 2D NoCs using an ultra-wideband coincidence plan have been suggested. Consistently, a remote redirect in a planar NoC has an accepting wire, framework building, and handset circuits as its key definitive parts. The idea here is to divide the system into various subnets with wired intra-subnet correspondence and remote joins conferring between the subnets. Each subnet involves a base station for setting up the remote association. Customary wired NoCs (WiNoCs) have an individual subnets, distinctive structures and heterogeneous configuration also those outcomes in essentially made strides inertness and throughput.

The thought of 3D remote NoC using inductive coupling was first illustrated and the planned systems predict a 4 × 4 × 3 3D network system. We have used a coordination based handset circuit for inductive coupling. The intralayer associations are

32 bits wide, and the guiding system is dimensional wormhole controlling. Particular switches have eight data handsets and a solitary clock handset. The handset has separate twists for data and clock transmission with a resultant vertical association of transfer speed of 8 bits. The total region of the six-port switch in 90 nm development is 0.13 mm^2, which consolidates a region spending arrangement of 0.03 mm^2 for the nine twists.

4 Survey Results

Many issues in 2D NoC designing and it's have been concentrated on over the previous years by covering different perspectives, for example, plan stream, usage assessment, and configuration space investigation. Nonetheless, examine in 3D NoC is still new and numerous issues stay unexplored particularly in genuine configuration and usage. Outline space investigation of 3D NoC topologies through cycle-exact reproduction have been performed demonstrating the advantages of 3D outline as far as throughput, idleness and vitality dispersal for cross-section based, what's more, tree-based NoC engineering [1]. In [2], zero load latency also, control utilization expository models of different 3D NoC, topologies have been assessed demonstrating the benefits of consolidating 3D IC with 3D NoC engineering. We base upon this writing to examine further the outcomes by doing investigation from physical configuration execution results. Another work [3] proposed a novel 3D switch engineering by disintegrating the switch into various measurements to give better execution over other 3D NoC structures. We contrast from the past reported fills in as we concentrate on apportioning 3D NoC models and assess their execution through design level netlist for more exact investigation of wire length, timing, territory and force utilization.

In [13], the study of various 3D situation strategies on the execution of three 3D designs demonstrated that genuine 3D position strategy produces the most elevated execution change over other strategies at old innovation (130 nm) denote the significance of 3D-mindful apparatuses to get most extreme advantages of 3D combination. Be that as it may, no past work has been given nitty-gritty execution assessment on different physical configuration measurements (wirelength, timing, effect of wire length) of 3D NoC engineering specifically with 3D Mesh-based NoC engineering. In the course of the most recent quite a while, there has been a developing enthusiasm for 3D ICs as a way to reduce the interconnect bottleneck as of now confronting 2D ICs. A key test with 3D ICs is their high warm thickness due to various centers being stacked together, that can unfavorably affect chip execution and unwavering quality. In this way a few scientists have proposed warm mindful floor planning systems for 3D ICs [7, 8]. A couple of specialists have investigated interconnect designs for 3D ICs for example, 3D work and stacked cross-section NoC topologies [5] and a half breed transport NoC topology [9]. Some late work has taken a gander at breaking down centers (processors [12], NoC switches [10], and on-chip reserve [11]) into the third measurement which permits decreasing wire dormancy at the intra-center level, rather than the between center level. Circuit level models for TSVs were introduced in [14]. A couple of later works have investigated the framework level effect of utilizing half and half electro-photonic interconnect models and proposed half and half Cu-photonic crossbars (Corona, Firefly), Clos systems, fat-trees and torii. This paper portrays the advantages and disadvantages of various creation techniques including up close and personal holding and face-to-back holding. With a SOI face-to-back procedure, the through pitch is minimized, at 0.4 m with a partition of 2 m between layers of SOI gadgets [15]. Jacob et al. [16] propose utilizing 3D ICs to enhance the execution of chip by shaping a processor memory stack. They demonstrate that the mix of processor worries by applying genuine movement designs in a cycle-precise recreation and by measuring execution through set up measurements for 3D NoC structures. In [17], 3D ICs were proposed to enhance execution of chip multiprocessors. Drawing upon 3D IC research, they picked a hybridization of transports and systems to give the interconnect fabric amongst CPUs and L2 reserves. The execution of this combination of NoC and transport models was assessed utilizing standard CPU benchmarks. Be that as it may, this examination relates just to chip multiprocessors and does not consider the utilization of 3D system structures for application-particular SoCs. Three-dimensional NoCs are broke down as far as temperature in [5]. Pavlidis and Friedman [9] contrasted 2D MESH structures and their 3D partners by breaking down the zero-load inertness and force utilization of every system. This is an assessment that demonstrates a portion of the benefits of 3D NoCs, yet it not one or the other applies any genuine activity design nor does it gauge other significant execution measurements. We intend to address these worries by applying genuine movement designs in a cycle-precise reproduction and by measuring execution through built-up measurements for 3D NoC structures.

References

1. Bayan AF, Wan T, Ramadass S (2010) Delay analysis and system capacity control for mobile WiMax relay networks. J Comput Sci 6(10):1137
2. Bazzi L, Richardson R, Urbanke R (2001) Exact thresholds and optimal codes for the binary symmetric channel and Gallager’s decoding algorithm. IEEE Trans Inform Theory 47
3. Benini L, Bertozzi D (2005) Network-on-chip architectures and design methods. IEE Comput Digit Tech 152(2):272
4. Benini L, Micheli G (2002) Networks on chips: a new SoC paradigm. Computer 35(1):70–78
5. Brooks L, Fife K (2004) Hardware efficient lossless image compression engine. Proc IEEE Int Conf Acou Speech Sign Process 5:17–21
6. Badrouchi S, Zitouni A, Torki K, Tourki R (2005) Asynchronous NoC router design. J Comput Sci 1(3):429–436
7. Bollobas B (1978) Extremal graph theory. Academic Press, New York
8. Bollobas B (1985) Random graphs. Academic Press, Londan
9. Burshtein D, Miller G (2001) Expander graph arguments for message-passing algorithms. IEEE Trans Inform Theory 47:782–790
10. Byers J, Luby M, Mitzenmacher M, Rege R (1998) A digital fountain approach to reliable distribution of bulk data. In: Proceedings of ACM SIGCOMM’98

11. Cantor D, Gerla M (1974) Optimal routing in a packet-switched computer network. IEEE Trans Comput 23(10):1062–1069
12. Chandra A (2002) Test data compression and decompression based on internal scan chains and Golomb coding. IEEE Trans Comput Aided Design Integr Circ Syst 21(6):715–722
13. Berrou C, Glavieux A, Thitimajshima P (1993) Near Shannon limit error correcting coding and decoding: turbo-codes. In: Proceedings of the IEEE international conference on communication technical program, May 23–26, IEEE Xplore Press, Geneva, pp 1064–1070. https://doi.org/10.1109/icc.397441
14. Charles RKJ, Vanchinathan T, Kharthik K (2013) Design of serdes transceiver with fixed and high throughput implementation on FPGA. Life Sci J 10:2849–2857
15. Denecker K, Ville DVD, Habils F, Meeus M, Brunfaut M, Lemahieu I (2002) Design of an improved lossless halftone image compression codec. Signal Process: Image Commun 17(3):277–292
16. Di C, Proietti D, Telatar E, Richardson T, Urbanke R (2002) Finite-length analysis of low-density parity-check codes on the binary erasure channel. IEEE Trans Inform Theory 48:1579
17. Divsalar D, Jin H, McEliece R (1998) Coding theorems for 'Turbo-like' codes. In: Proceedings of the Allerton conference, p 210

Performance Analysis of Unified Threat Management (UTM)

Jatin Gharat, Amarsinh Vidhate and Amit Barve

Abstract With the substantial increase in the internet usage and the growing threat of hackers to infect as many devices as possible, security has become important to prevent data breaches and industrial sabotage. Unified Threat Management are the Next-Generation network security appliances that include multiple security features along with the performance required for future networks. But packet processing usually consumes 70% of the CPU time and during heavy load it degrades the UTM performance by dropping important packets. To overcome such limitations, many techniques and algorithms have been proposed by the researchers. In this paper, survey and numerical analysis of each technique is done based on the overall packet processing time. Based on the numerical analysis, we suggest the best technique to reduce the overall packet processing time in UTM and hence reduce the load under heavy traffic conditions.

Keywords UTM · Splay tree · Multicore · Graphics processing unit

1 Introduction

With the recent increase in cyber-attacks and security breaches, more security features are required inside the network. Increasing the number of security devices makes it difficult to manage each device separately and consumes other resources. A unified threat management (UTM) is a device used to incorporate number of network and security features like firewall, packet classification, bandwidth management, etc. in a single device [1]. Generally, UTM includes functions like firewall, intrusion

J. Gharat (✉) · A. Vidhate · A. Barve
Ramrao Adik Institute of Technology, Nerul, Navi Mumbai, India
e-mail: jatin.gharat87@gmail.com

A. Vidhate
e-mail: vidhate.amarsinh@gmail.com

A. Barve
e-mail: barve.amit@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_13

detection, and prevention (IDS), anti-spam, anti-spyware, anti-virus, content filtering, virtual private network, and other security functions.

We will look into the major application of UTM, i.e., packet processing. Some packets are targeted to pass through the entire packet filter rule list to finally get rejected. This can effectively decrease the UTM performance. Also, under severe load conditions, for example, unwanted traffic, DoS attack, etc. efficiency of UTM decreases considerably. To improve the efficiency, we need to search for good possible solutions which can reduce the load on UTM under such extreme conditions. Hence, we need to study and implement improved packet filtering techniques to provide up-to-date security.

Subsequent sections are organized in the following order: In Sect. 2 we perform literature survey giving an overview on the work done in this field. In Sect. 3, we study some techniques used to improve UTM performance. In Sect. 4, we perform analysis on the techniques used by authors. Finally, in Sect. 5 we conclude this study.

2 Literature Survey

The research areas in UTM are divided into packet filtering, firewall enhancements and other techniques like using multicore functionality of CPU and GPU. While these techniques have resulted in great successes, a lot of problems are yet to be resolved.

Trabelsi et al. [1] have proposed a hybrid approach using Splay Filters and DPI Rules Reordering (SFRO) algorithm to dynamically optimize the order of splay tree filters such that network packets are either early accepted/rejected to reduce the redundancy introduced by multiple filters in UTM. Gummandi et al. [2] used OpenMP parallelization methods to reduce the overload on UTM by scheduling logical CPUs for packet processing, firewall, spam filtering, and other security features. Recent firewall devices are considered complex, time-consuming and error-prone thus resulting in slow filtering action. Sahoo et al. [3] have presented a unique approach using CUDA programming for GPU which processes packet in parallel thread blocks and handles firewall security efficiently.

Trabelsi et al. [4] proposed Dynamic Rule and Rule-Fields Ordering with Decision (DR-RFOD) algorithm to improve the firewall performance and packet classification by optimizing the firewall filtering rules and rule-fields using network traffic statistics. Another algorithm proposed by Trabelsi et al. [5] uses Statistical Splaying Filters with Binary Search on Prefix Length (SSF-BSPL) to optimize the matching time for wanted/unwanted traffic packets. Neji et al. [6] proposed Self-Adjusting Binary Search on Prefix Length (SA-BSPL) which can easily find matching for protocol field, range matching for port numbers, and prefix matching for IP address by dynamic packet filtering. Adel El-Atawy et al. [7] have proposed Relaxed Policy Expression (RPE) technique which uses Binary Decision Diagrams (BDD) data structure to reduce packet matching cost by dynamically changing the pre-filter phase that can reside on top of any filtering mechanism.

Harvath et al. [8] proposed pNEGI (parallel NEGI) to parallelize the process of NEGI, a software SoR simulator, to analyze the layer-7 information using DPI which is generally difficult. Yunchun Li et al. [9] states that with the increasing demand for more bandwidth by applications, packet processing capabilities decreases in serial processing systems. Hence the authors have proposed a parallel processing model and compared with serial processing system to analyze the performance. Chonka et al. [10] states that implementing security, in general, affects the performance of the application. Hence the authors propose a multicore defense framework to deal with the performance issues.

Shuai Mu et al. [11] states that there always has been a trade-off between throughput and programmability in modern IP router designs. To overcome these limitations, the authors have proposed a technique using GPU, prefix matching and string-matching algorithms to achieve a much higher performance. Che-Lun Hung et al. [12] have provided a solution to the computationally intensive process of pattern matching [19] on CPU by using the computational power of graphics processing unit to accelerate pattern-matching operations. Kang Kang et al. [13] states that high-performance routers use proprietary hardware to classify packets but are excessively costly, consume more power and are less scalable. Hence the authors proposed GPU based linear search framework which uses metaprogramming technique to enhance packet processing efficiency. Present network intrusion detection systems (NIDS) must handle increasing network traffic and more complex packet processing task. Giorgos Vasiliadis, et al. [14] proposed a prototype system Gnort, which utilizes computational capabilities of graphics card to perform packet processing operations.

2.1 Survey Analysis

From the literature analysis, we found that we can categorize the papers according to the techniques used. Hence, we divided the papers into three different categories. The detailed survey analysis for the three categories is provided below:

- **Category I**: The first category is based on only the algorithmic techniques used to enhance the overall packet processing performance. The papers in this category [1, 4–7] mostly use tree filters as a mechanism to early accept or reject a packet by checking against a set of rules. The use of network traffic to adapt the changing traffic load helps to achieve better efficiency.
- **Category II**: The second category is based on the use of multicore functionality of CPU based system [2, 8–10]. Multiple functions in UTM like packet processing, URL filtering, spam filtering, etc. can be processed simultaneously thus increasing the performance of UTM.
- **Category III**: The third category is based on the usage of Graphics Processing Unit (GPU) system as a special packet processing device [3, 11–14]. The development of CUDA programming architecture has made it easy to perform the general task more efficiently. Because the number of threads present in GPUs surpasses any other

device, the packet processing operation gains considerable amount of performance improvement from the GPU system.

3 Techniques to Improve UTM Performance

UTM appliances maintain a database of rules for packet classification. Each packet classification rule consists of a prefix (or range of values) for each possible header field, which matches a subset of packets. Thus, when a packet arrives, UTM finds a rule that matches the packet headers; however, if more than one match is found; the first matching rule is applied.

The main disadvantage of such an approach is the poor scalability since the time to perform a classification increases substantially with the number of rules in the rule set. This issue can be resolved by either adjusting the rule set or by using some parallel processing techniques.

Here we study three techniques: Splay trees with network statistics, Parallel Processing using OpenMP, and Parallel Processing using GPU.

3.1 Splay Trees with Network Statistics

Splay trees are self-adjusting binary data structure which makes use of splaying property such that the frequently accessed node (element) is splayed to the root of the tree. Several authors [1, 4–6] made use of network traffic statistics to effectively monitor the performance in real-time and predict the patterns of rule and rule-fields that best suit the next traffic window. Filtering rules and rule-fields orders are updated if the stability test reaches a certain threshold.

To decide which rule applies to a given packet, five filters, i.e., protocol, source IP address, destination IP address, source port, and destination port are used. Nodes that are frequently accessed are given position close to the root of the splay-tree. The longest matching prefix is updated whenever a match is found. When a leaf is encountered, the search process stops the best length node is splayed to the root (splaying property). This results in early acceptance of repeated packets with limited memory access. Similarly, a packet will be rejected if node with minimum length in splay tree does not match the corresponding packet value. Decision whether the current splay filters order should be preserved or not for the next traffic window is taken on the basis of traffic statistics.

3.2 Parallel Processing Using OpenMP

Parallel processing is a type of computation in which many calculations or the execution of processes are carried out simultaneously. Large problems can often be divided into smaller ones, which can then be solved at the same time. A multicore processor is a processor that includes multiple processing units (called "cores") on the same chip. A multicore processor can issue multiple instructions per clock cycle from multiple instruction streams.

Multiple independent processes in UTM can be parallelly processed using OpenMP [18]. Assigning different CPU cores to perform different packet processing operations like URL filtering, spam filtering, etc. parallelly can reduce the overall time consumption in heavy traffic conditions.

3.3 Parallel Processing Using GPU

A graphics processing unit (GPU) is a specialized electronic circuit designed to rapidly manipulate and alter memory accelerating the computations in a frame buffer intended for output. General-purpose computing on graphics processing units (GPGPU) is the use of a GPU, which typically handles computation only for computer graphics, to perform computation in applications traditionally handled by the central processing unit (CPU). A single GPU-CPU framework provides advantages that multiple CPUs on their own do not offer due to the specialization in each chip. CUDA is a parallel computing platform and application programming interface (API) model created by Nvidia. The CUDA platform is a software layer that gives direct access to the GPU's virtual instruction set and parallel computational elements, for the execution of compute kernels. The general process flow of data between CPU and GPU is as follows:

1. Copy input data from CPU memory to GPU memory.
2. Load GPU program and execute, caching data on-chip for performance.
3. Copy results from GPU memory to CPU memory.

4 Comparative Analysis

In this section, we perform comparative analysis on different techniques proposed by authors. Table 1 shows the notations used for analysis.

Table 1 Notations

Notation	Description
P	Total number of packets
S	Size of a single packet segment/queue
T_1	Number of threads in a GPU
T_2	Number of threads in a multicore system
m	Cost of memory latency
T_{in}	Time taken to modify/queue incoming packet
T_{out}	Time taken to update result/rule set
t_{lock}	Cost of thread locking
t_{unlock}	Cost of thread unlocking
T_{total}	Total packet processing time in ms
t_{update}	Cost of the rule/result table update
T_{process}	Time taken to process packet using an algorithm/technique
C_{switch1}	Cost of context switching in GPU
C_{switch2}	Cost of context switching in the CPU

4.1 Analysis

Let T_{total} be the total time taken for packet processing. T_{total} can be represented as:

$$T_{\text{total}}(\text{ms}) = T_{\text{in}} + T_{\text{process}} + T_{\text{out}} \tag{1}$$

where T_{in} is the time taken to queue/modify a packet or transfer it to threads. T_{process} is the time taken to process packet using an algorithm, and T_{out} time required update the result/rule set.

Category I: Packet Processing Using Splay Trees and Other Algorithms

In Category I, we consider the techniques which make use of different algorithms for packet processing. The methods discussed in this category do not use the multi-threading. Hence, cost of context switching is not involved.

In the paper, proposed by Trabelsi [1], considering Eq. (1) and rewriting it, we get:

$$T_{\text{total}} = (P/S) + (P \times 2m) + \left(P \times t_{\text{update}}\right)/S \tag{2}$$

where $T_{\text{in}} = P/S$, here P/S represents number of incoming packet segments, $T_{\text{process}} = P \times 2\ m$, here m represents memory access provided for each packet which is at most two memory accesses, and $T_{\text{out}} = (P \times t_{\text{update}})/S$, where t_{update} is time required to update the splay tree filter only if previous traffic is not same. Hence, we consider the update for different packet segments S.

In a similar paper proposed by Trabelsi [4], considering Eq. (1) and rewriting it, we get:

$$T_{\text{total}} = (P/S) + (P \times m) + \left(P \times 2 \times t_{\text{update}}\right)/S \tag{3}$$

where $T_{in} = P/S$, here *P/S* represents number of incoming packet segments, $T_{\text{process}} = P \times m$, here *m* represents memory access provided for each packet, and $T_{\text{out}} = (P \times 2 \times t_{\text{update}})/S$, where t_{update} is time required to update the splay tree filter only if previous traffic is not same and to calculate the optimum window size. Hence, we consider the update for different packet segments *S*.

Again, in paper [5], considering Eq. (1) and rewriting it, we get:

$$T_{\text{total}} = (P/S) + (P \times 2m) + \left(P \times t_{\text{update}}\right)/S \tag{4}$$

where $T_{\text{in}} = P/S$, $T_{\text{process}} = P \times 2\ m$, here *m* represents memory access provided for each packet, $T_{\text{out}} = (P \times t_{\text{update}})/S$, where t_{update} is time required to update the splay tree filter order.

Evaluating paper [6], considering Eq. (1) and rewriting it, we get:

$$T_{\text{total}} = (P/S) + (P \times 4m) + \left(P \times t_{\text{update}}\right) \tag{5}$$

where $T_{\text{in}} = P/S$, $T_{\text{process}} = P \times 4\ m$, since memory access is frequent for the greater number of rules, and $T_{\text{out}} = (P \times t_{\text{update}})$, here, splay filter gets updated more frequently.

Evaluating paper [7], considering Eq. (1) and rewriting it, we get:

$$T_{\text{total}} = (P/S) + (P \times 15m) + (P \times (t_{\text{update}} + 2m)) \tag{6}$$

where $T_{\text{in}} = P/S$, $T_{\text{process}} = P \times 15\ m$, here memory is accessed more frequently and packet needs to be converted to boolean form, and $T_{\text{out}} = (P \times (t_{\text{update}} + 2\ m))$, updating the filter, calculating the network statistics requires memory usage.

Category II: Parallel Processing Using Multicore Processors

Multicore Processors can parallelly process packets by assigning them to multiple threads. We evaluate the techniques used in this section. Here context switching with CPU usage is involved. The thread locking and unlocking delays are ignored in some techniques (included wherever necessary) since it is very small compared to other delays.

In the paper [2], considering Eq. (1) we can write:

$$T_{\text{total}} = (P \times C_{\text{switch}\,2}) + (P/T_2) + \left(P \times t_{\text{update}}/T_2\right) \tag{7}$$

where $T_{\text{in}} = (P \times C_{\text{switch2}})$, the context switching associated with each packet, $T_{\text{process}} = P/T_2$, T_2 represents number of threads created in CPU, and $T_{\text{out}} = P \times t_{\text{update}}/T_2$, t_{update} represent the time to update the accepted/rejected packet list.

For paper [8], evaluating Eq. (1) we get,

$$T_{\text{total}} = (P \times 2 \times C_{\text{switch}\,2} \times t_{\text{lock}}/S) + (P/T_2) + \left(P \times \left(t_{\text{update}} + t_{\text{unlock}}/S\right)\right) \tag{8}$$

where T_{in}= ($P \times 2 \times C_{\text{switch2}} \times t_{\text{lock}}/S$), here the main thread creates child threads and queues are locked before multithreading, T_{process}= P/T_2, T_{out}= ($P \times$ (t_{update}+ t_{unlock}/S)), here t_{unlock} represents cost of thread unlocking.

Similarly, for paper [9], the threads are queued according to the stream they belong to. The queues need to be locked to protect them. Hence rewriting Eq. (1) we get,

$$T_{\text{total}} = (P \times C_{\text{switch}\,2} \times t_{\text{lock}}/S) + (P/T_2) + \left(P \times \left(t_{\text{update}}/T_2 + t + t_{\text{unleck}}/SS\,)\right) \tag{9}$$

where T_{in}= ($P \times C_{\text{switch2}} \times t_{\text{lock}}/S$), T_{process}= P/T_2, T_{out}= ($P \times$ (t_{update}/T_2+ t + t_{unlock}/S)), here let t be the delay caused by asynchronous computation between threads. Let $t = m$ and then we can rewrite Eq. (9) as:

$$T_{\text{total}} = (P \times C_{\text{switch}\,2} \times t_{\text{lock}}/S) + (P/T_2) + \left(P \times \left(t_{\text{update}}/T_2 + m + t_{\text{unlock}}/S\right)\right) \tag{10}$$

Using the technique presented in paper [10] and re-evaluating Eq. (1) we get,

$$T_{\text{total}} = (P \times C_{\text{switch}}) + (P/T_2) + \left(P \times \left(t_{\text{update}} + t + 2m\right)\right) \tag{11}$$

where T_{in}= ($P \times C_{\text{switch2}}$), T_{process}= P/T_2, T_{out}= ($P \times$ (t_{update}+ t + 2 m)) here let t represent the intercommunication delay and m is the memory latency involved. Let $t = m$, then Eq. (11) becomes

$$T_{\text{total}} = (P \times C_{\text{switch}\,2}) + (P/T_2) + (P \times (t_{\text{update}} + 3m)) \tag{12}$$

Category III: Parallel Processing Using GPU

In this category, we consider the techniques which make use of highly efficient Graphic Processing Unit (GPU) for packet processing. The context switching, C_{switch1}, in the following papers do not involve CPU time since the packets are transferred using Direct Memory Access (DMA).

In the paper [3], considering Eq. (1) we can write:

$$T_{\text{total}} = (P \times C_{\text{switch}\,1}) + (P/T_1) + \left(P \times t_{\text{update}}/T_1\right) \tag{13}$$

where, T_{in}= $P \times C_{\text{switch1}}$, here only the context switching time for packet queue is involved, T_{process}= P/T_1, packets are distributed among threads for processing, and T_{out}= $P \times t_{\text{update}}/T_1$ is the time taken to update the list of accepted/rejected packets. This process happens in GPU itself.

For paper [11], evaluating Eq. (1) we get,

$$T_{\text{total}} = (P \times C_{\text{switch}}) + (P/T_l) + \left(P \times \left(4 \times t_{\text{update}} + m\right)\right) \tag{14}$$

where, $T_{\text{in}} = P \times C_{\text{switch1}}$, the context switching time for packet queue is involved, $T_{\text{process}} = P/T_1$, $T_{\text{out}} = (P\, x\, (4 \times t_{\text{update}} + m))$, here transition table has to be accessed frequently. Hence the algorithm is memory bound.

Similarly, for paper [12], rewriting Eq. (1) we get,

$$T_{\text{total}} = (P \times C_{\text{switch}}) + (P/T_l) + (P \times t_{\text{update}}) \tag{15}$$

where $T_{\text{in}} = (P \times C_{\text{switch1}})$, $T_{\text{process}} = P/T_1$, $T_{\text{out}} = (P \times t_{\text{update}})$, here the result of list of packets are updated in the host.

Using the technique presented in paper [13] and re-evaluating Eq. (1) we get,

$$T_{\text{total}} = (P \times C_{\text{switch}}) + (P/T_1) + (P \times (t_{\text{update}} + 2m)) \tag{16}$$

where $T_{\text{in}} = P \times C_{\text{switch1}}$, $T_{\text{process}} = P/T_1$, $T_{\text{out}} = (P \times (t_{\text{update}} + 2\, m))$, here metaprogramming involves compilation time of the C Program in CPU. Linear Search also require some time to find the exact match.

Evaluating paper [14] using Eq. (1) we get,

$$T_{\text{total}} = (P \times C_{\text{switchl}}) + (P/T_l) + \left(P \times \left(4 \times t_{\text{update}} + m\right)\right) \tag{17}$$

where $T_{\text{in}} = P \times C_{\text{switch1}}$, $T_{\text{process}} = P/T_1$, $T_{\text{out}} = (P \times (4 \times t_{\text{update}} + m))$, here four additional factors are required to be checked to correctly identify packets. This process is done in the CPU.

4.2 Numerical Analysis Results

In this study, we used a dataset consisting of 32,506 packets containing 97.6% TCP, 2.3% UDP, and 0.1% ICMPv6 of the total traffic. The average packet size is 730 bytes with 528.5 packets per second. Let us assume that the traffic window contains S segments with each segment containing 8 packets. For the context switching time, we can say that $C_{\text{switch1}} < C_{\text{switch2}}$. This is because while transferring packets from host to GPU we use DMA technique which reduces the switching time. This is not the case in multicore CPU systems where CPU processing cost is involved. From paper [17], we can approximate the values of $C_{\text{switch1}} \approx 4.2\ \mu\text{s}$ and $C_{\text{switch2}} \approx 5\ \mu\text{s}$. The memory latency involved is approximated to be $m \approx 100\ \mu\text{s}$ [15]. The table update cost is approximated [15] to be around $t_{\text{update}} \approx 50\ \mu\text{s}$. The thread locking/unlocking delay is approximately taken around $t_{\text{lock}} = t_{\text{unlock}} \approx 100$ ns [16]. We consider number of threads in multicore system, $T_2 = 16$ while that in Graphics Processing Unit, taking 32 warps and each warp can execute 32 threads concurrently, $T_1 = 1024$.

The results are shown in Tables 2, 3 and 4. We compare the total packet processing time (in ms) for each method.

Table 2 Results for Category I

S. No.	Title	Result (in ms)
1	Hybrid mechanism towards network packet early acceptance and rejection for unified threat management [1]	4064.10
2	Dynamic traffic awareness statistical model for firewall performance enhancement [4]	4064.31
3	Multilevel early packet filtering technique based on traffic statistics and splay trees for firewall performance improvement [5]	4064.10
4	Dynamic scheme for packet classification using splay trees [6]	4066.18
5	Adaptive early packet filtering for depending firewall against DoS attack [7]	4070.40

Table 3 Results for Category II

S. No.	Title	Result (in ms)
1	Effective utilization of multicore processor for unified threat management functions [2]	2031.89
2	Parallel packet processing on multicore and many-core processors [8]	2033.25
3	A parallel packet processing method on multicore systems [9]	2033.58
4	Protecting information systems from DDoS attack using multicore methodology trees [10]	2034.39

Table 4 Results for Category III

S. No.	Title	Result (in ms)
1	Firewall engine based on graphics processing unit [3]	31.88
2	IP routing processing with graphic processors [11]	38.71
3	An efficient parallel-network packet pattern-matching approach using GPUs [12]	33.51
4.	Scalable packet classification via GPU metaprogramming [13]	34.16
5	Gnort: high-performance network intrusion detection using graphics processors [14]	38.71

From the above analysis, we can conclude the following:

- In Category I, the method presented in paper [1] is more efficient than others (see Fig. 1). The memory access time is limited in this technique to at most two accesses which helps in faster packet processing.
- In Category II, the method proposed in paper [2] is more efficient (see Fig. 2). This is due to the fact that multicore functionality is implemented not only for packet processing but also for packet reception/transmission. Also, the memory is highly managed to further improve the system.

Fig. 1 Category I

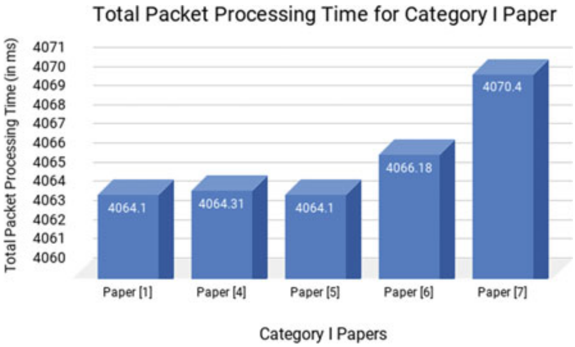
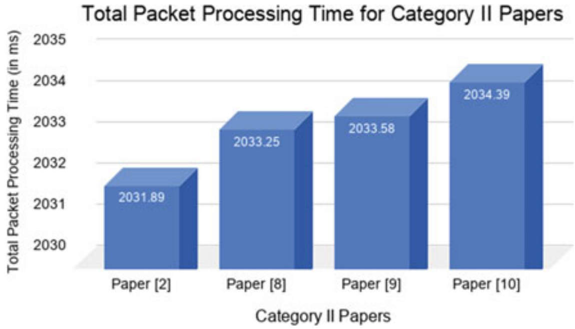


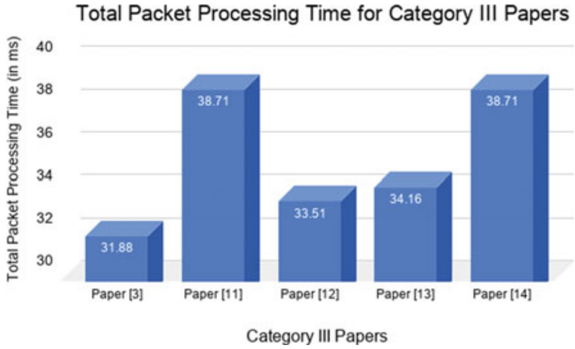
Fig. 2 Category II



- In Category III, the method proposed in paper [3] is most efficient compared to other techniques (see Fig. 3). The GPU handles most of the network traffic efficiently and using the zero-copy technique the transferring time is greatly reduced.

In our further analysis, we compare the best paper in all three categories. From the overall analysis (see Fig. 4) we can conclude that the technique presented by Sahoo et al. [3] is most efficient in terms of total packet processing time. Thus, by

Fig. 3 Category III



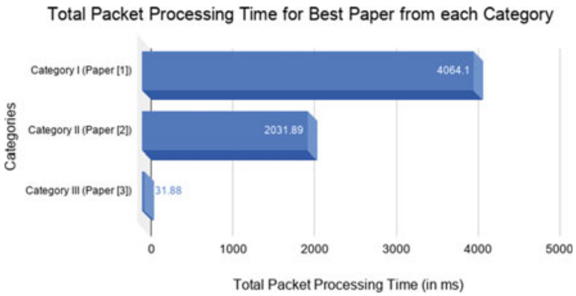


Fig. 4 Overall comparison

incorporating the processing power of Graphics Card, we can substantially increase the packet processing speed and improve the system performance to the next level.

5 Conclusion

A UTM device provides high-end security in a single device. We have seen that an increase in network traffic can create problems and it consumes almost 70% of the resources. From our analysis, we can conclude the following.:

- The performance can be increased by using multicore functionality in the device itself. From the analysis, it can be noticed that the processing capabilities of GPU system outperform any other device capability. Hence, we can say that incorporating GPUs in our UTM system, we can drastically improve the performance and overcome any load situations arising as a result of heavy traffic.
- In our future work, we plan to use the multicore functionality of CPU for other UTM functions like anti-virus, anti-spam detection, etc. once the packet processing results are received from GPU. Also, we plan to use a self-adjusting tree data structure for rule-fields ordering in GPU and compare the results for dynamically changing traffic environment especially for DoS attacks.

Acknowledgements We would like to extend our sincere thanks to Dr. Ramesh Vasapanavara, Principal, Ramrao Adik Institute of Technology for his constant encouragement and generous support throughout the completion of this work.

References

1. Trabelsi Z, Zeidan S, Masud MM (2017) Hybrid mechanism towards network packet early acceptance and rejection for unified threat management. IET Inf Secur 11(2):104–113
2. Gummandi S, Shanmugasundaram R (2012) Effective utilization of multicore processor for unified threat management functions. J Comput Sci 8(1):68–75

3. Sahoo AK, Das A, Tiwary M (2014) Firewall engine based on graphics processing unit. ISBN No. 978-1-4799-3914-5, IEEE ICACCCT
4. Trabelsi Z, Zhang L, Zeidan S, Ghoudi K (2013) Dynamic traffic awareness statistical model for firewall performance enhancement. Comput Secur 39:160–172
5. Trabelsi Z, Zeidan S (2012) Multilevel early packet filtering technique based on traffic statistics and splay trees for firewall performance improvement. IEEE international conference on communications (ICC)
6. Neji NB, Bouhoula A (2009) Dynamic scheme for packet classification using splay trees. J Inform Assur Secur 4:133–141
7. El-Atawy A, Al-Shaer E, Tran T, Boutaba R (2009) Adaptive early packet filtering for depending firewall against DoS attacks. IEEE INFOCOM
8. Harvath A, Nishi H (2015) Parallel packet processing on multi-core and many-core processors. International conference on parallel and distributed processing techniques and applications
9. Li Y, Qiao X (2011) A parallel packet processing method on multi-core systems. In: IEEE 10th international symposium on distributed computing and applications to business, engineering and science
10. Chonka A, Zhou W, Knapp K, Yang X (2008) Protecting information systems from DDoS attack using multicore methodology. In: IEEE 8th international conference on computer and information technology workshops
11. Mu S, Zhang X, Zhang N, Lu J, Deng YS, Zhang S (2010) IP routing processing with graphic processors. IEEE 2010 Des Autom Test Eur Conf Exhib
12. Hung Che-Lun, Lin Chun-Yuan, Wang Hsiao-Hsi (2014) An efficient parallel-network packet pattern-matching approach using GPUs. Elsevier J Syst Archit 60:431–439
13. Kang K, Deng YS (2011) Scalable packet classification via GPU metaprogramming. IEEE 2011 Des Autom Test Eur
14. Vasiliadis G, Antonatos S, Polychronakis M, Markatos EP, Ioannidis S (2008) Gnort: high performance network intrusion detection using graphics processors. In: International workshop on recent advances in intrusion detection
15. Stackoverflow. https://stackoverflow.com/questions/4087280/approximate-cost-to-access-various-caches-and-main-memory
16. .NET Reference Guide. The cost of locks. https://web.archive.org/web/20140619205834/http://www.informit.com/guides/content.aspx?g=dotnet&seqNum=600
17. Li C, Ding C, Shen K (2007) Quantifying the cost of context switch. In: ExpCS'07 proceedings of the 2007 workshop on experimental computer science
18. Wikipedia. OpenMp. https://en.wikipedia.org/wiki/OpenMP
19. Rathod PM, Marathe N, Vidhate AV (2014) A survey on finite automata based pattern matching techniques for network intrusion detection system (NIDS). In: 2014 international conference on advances in electronics, computers and communi cations (ICAECC)

Development of an Efficient Nondestructive Grading Method for Pomegranate Using Magnetic Resonance Imaging and Neural Network

Surekha Yakatpure and Krupa Rasane

Abstract The pomegranate fruit has gained popularity due to its nutritional values and pharmacological properties. India ranks high among growers of pomegranates across the world and hence there is tremendous potential for its export. Here in our work the Bhagwa, a prime Indian pomegranate cultivar was studied. Total soluble solids (TSS) were measured experimentally. Internal images of the fruit were obtained nondestructively using Magnetic Resonance Imaging (MRI). The textural features from image were given as input to the nonlinear autoregressive neural network. The results showed that T1-weighted MR images were sensitive to physical and chemical changes. The R-value for measured TSS and model-predicted TSS for training data was 0.99 and testing data was 0.92. This study shows that MRI has higher potential for nondestructive method of grading pomegranate fruit based on the chemical values which are the basis for determining the maturity of the fruit.

Keywords Pomegranate · Nondestructive · MRI · Texture · Neural network

1 Introduction

India ranks high among growers of pomegranates across the world as per the statistics of APEDA [1] and therefore India can use this natural produce to increase the export of this fruit [2]. To increase exports, it is necessary to improve the quality. If we make improvement in the quality of fruit then only we can cater the ever-increasing need and stand tall in the market. For the obvious reason there is demand of developing innovative non-destructive techniques to characterize internal quality attributes to cater the ever-increasing market throughout the year by further extending the shelf-life. To gain consumer appreciation and increase local and export marketing supply of

S. Yakatpure (✉)
Electronics and Telecommunication Department, A G Patil Institute of Technology, Solapur, India
e-mail: surekha.sakhare@gmail.com

K. Rasane
E&C Department, Jain College of Engineering, Belgavi, India
e-mail: kru_ran@yahoo.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_14

graded and sorted fruits becomes a norm. Outer quality attributes considered are size, shape, color, tenderness, hardness can be obtained by just observations and touch senses. But these methods which are thus conventionally graded can lead to a risk of internal faults as pale arils, dead tissues and browning, which go undetected, as they are not externally seen. This marks a grave problem to the food processing units based on fruits and also endangers the export market causing rejections and reputation of the cultivar used for export to the destination country. Much work has been done to estimate the maturity index and quality of fruit, analytically. In many works, data analysis has been done over different physiochemical values as total soluble solids (TSS), pH, weight, titratable acidity (TA), etc. were obtained from the instruments in the laboratory which are laborious, cause loss of fruit and above all much slower and hence less efficient for speedy quality determination. Nondestructive detection of internal quality factors is a great challenge. Researchers have been working to develop new methods which can determine the internal quality attributes without breaking the product under observation. The various techniques based on operating principles of optics, acoustics, and ultrasonics do model few physical values related to quality. Moreover, where some nondestructive techniques as X-ray and CT used for interpreting internal qualities of fruit, turn hazardous for the biological cells due to electromagnetic radiations. On the other side, safer techniques of optic and acoustic result in lesser penetration in the fruit due to varying thickness of skin and pulp. These methods are not able to measure internal physicochemical values required for grading based on internal qualities [3]. Magnetic resonance imaging (MRI) has been introduced around middle of 1980s for studying internal physiochemical values of various vegetables and fruits. MRI had certain limitations used for inline grading, firstly due to the small sample size, secondly the rate of processing. As today's medical field needed improved power magnets, technology has devised the higher end requirements for them and hence these facilities can be used for other application as for nondestructive method for literally diagnosing the fruit internally and thoroughly for quality grading.

1.1 Magnetic Image Processing Techniques Used for Fruits

The operating principle of MRI consists of secured interaction among radio waves and hydrogen from the water molecules in the fruit under the influence of strong magnetic field made available in the assembly. Unlike X-ray and CT imaging, it bears least ill effects concerned with the magnetic field. MRI, as is sensitive to hydrogen nuclei, present ample in any biological cell, every detail can be observed inside the soft tissues of the fruit. Highest benefits of MRI are its potential to vary the contrast of the images far better than X-ray and CT. With the advancement of MRI hardware and efficient algorithms for the acquired data and improved methods of analyzing data, the applications based on MRI have spread the tentacles in the domain of food science and technology including the fruit industry [11, 12]. Various work done are summarized in Table 1.

Table 1 Physiochemical values determination and grading for fruits and food using MRI as nondestructive method

S. No.	Purpose	Type of fruit/food	Author	Reference
1	Mealiness assessment and internal breakdown	Apple and peach	P. Barriero	[4]
2	Water-core	Apples	Wang S. Y., Herremans,	[5, 6]
3	Internal damage	Tomato	Milczarek	[7]
4	Internal quality	Orange	Wasiu A. Balogun,	[8]
5	TSS	Pomegranate	Khusroo	[10, 11]
6	Physiochemical values	Loin	Daniel Caballero	[12]

Mealiness in apple has been detected using MRI technique [4]. In the apples, those features representing mealiness were correctly obtained as markers of affected fruit. Here skewness in histogram was checked and it was observed that the effected ones were having more skewness than those which are not affected by mealiness. Water core in apple fruit was related with increased water content and was observed by MRI technique. It was seen in the image that water core-affected tissues generally got obvious due to increased intensity for the corresponding region in the image [5]. The study was done over many varieties and a classifier was modeled using gray-scale histograms of MRI images to classify the water core apples from the unaffected ones [6]. Neural network method was used to classify MRI image of orange fruit into defect or good classes based on pixel intensity level. Here evaluation of models performance was tested based on R-value and mean squared error [8]. Using this method study was carried out to make the prediction of those features of the pomegranate which define its internal quality. In the study, it was concluded that MRI method can estimate many quality features which can be used for grading [9]. Also, this technique has provided greater knowledge of the internal variations taking place throughout the stages of growth in pomegranate and has helped detect maturity in pomegranate fruits [10]. Image attributes were quantified using eleven co-occurrence matrix texture features and five run-length matrix texture features extracted from the MRI images of pomegranates. In another work of same author, the features were used as input to a MLP Neural networks and predicted the maturity with correlation coefficient, $R = 0.93$ and $R = 0.90$ for training and test data, respectively [11]. Recently, researchers have devised the model to predict the physicochemical values of loins and related them with 3D features of features obtained from the MRI imaging. [12]. The aim for this present study is to optimize the work done for correlation coefficients [11] and develop an efficient method of grading pomegranate using MRI as a nondestructive method based on the maturity index which is defined by the physiochemical values. In the work here a model is developed wherein texture attributes from MRI of pomegranate, combined with nonlinear autoregressive neural networks technique to improve the correlation coefficient for training and testing data increasing the grading potential of the model.

2 Materials and Methods

Pomegranates of "Bhagwa", cultivar which is a prime export variety in India, had been collected from local market at normal temperature and sent to Shri Markandaya Solapur, Sahakari Rugnalya and Research Center, for scanning purpose. We have used a 1.5T MRI scanner (Siemens) with 2D spin-echo sequence for our study. Table 2 shows the comparative table of the parameters for the sample of our project and the reference work [11]. Figure 1 shows magnetic resonance image of the pomegranate.

Table 2 Comparative parameters used in study

Author	MRI scanner	TR (ms)	TE (ms)	FOV (cm)	Slice thickness (mm)	Inter slice gap (cm)	Total slices	Matrix
Alireza Khoshroo	1.5T scanner	800	18	29.6	3	1.56	12	336 by 512
Our sample	1.5T scanner	800	18	29.6	3	1.56	18	256 by 256

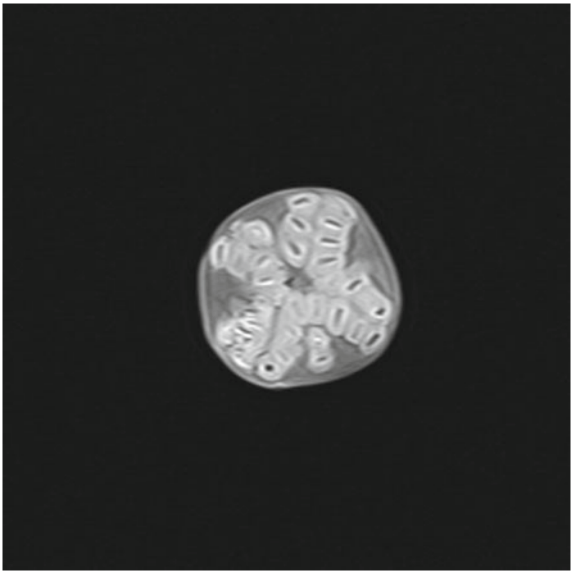


Fig. 1 Magnetic resonance image of the pomegranate

After MRI imaging as shown as an example in Fig. 1, TSS of fruits are obtained from laboratory of National Research Center of Pomegranate, Solapur. In this study, to estimate total soluble solids of pomegranates, texture features which are obtained from texture analysis of magnetic resonance images after preprocessing are combined with regressive neural network, along with the laboratory values.

Here we have considered a dynamic neural network for our study, where this model having memory help predict the new coming value of TSS, based on the past input values. The model can be defined in a simple manner mathematically as

$$y(t_o) = f\{y(t_o - 1), y(t_o - 2), y(t_o - 3), u(t_o - 1), u\,(t_o - 2), u\,(t_o - 3)\ldots u\,(t_o - n)\}$$

where the next outcoming value is obtained by feedback of the past output and the corresponding input. The new output is based on these new inputs to the neural network. Again the two-layered feed-forward network which is used for correctly approximating the function defined over the inputs has an advantage that it is best suited for the training purpose. Also the added grace is that inputs to this second layer are very accurate. Here the neurons required were 20, and epochs for the improved correlation were 12.

2.1 Methodological Steps in Detail

Step 1 Pre-processed all images using imadjust which assign I image of particular intensity values to that of different intensity values present in J image, wherein this newly formed image shows improved contrast.

Step 2 Our thresholding function

$$\hat{f}_{(i,j)} = \begin{cases} f_{(i,j)} \geq Tr \\ 0 \quad \text{otherwise} \end{cases}$$

Here, $f_{(i,j)}$ being original and $\hat{f}_{(i,j)}$ the filtered image and Tr is thresholding value, here we applied $Tr = 100$

Step 3 Calculated GLCM 4 features using GLCM function

Step 4 Created feature vector and target vector based on TSS values

Step 5 Experimental setup: Database is divided into 50, 15, and 35% for training, validation, and testing. Created neural network model and then tested for the generated feature space with target values of TSS from the lab values, which finally predicted TSS values. Later calculated correlation coefficient using both values and obtained the results. The comparative steps involved in the experiments and with the experiment performed in the earlier work [10, 11] referred with due courtesy are shown in Table 3.

Table 3 Comparison of experimental steps for the referred work and present work

Author	Pre-processing	Parameter	Feature extraction	Classification	Post-processing	Outcomes
AlirezaKhoshroo [10, 11]	NA	TSS	GLCM 10 feature using MaZda 2.11 and RLM (run length matrix) 5 feature	Neural network LR = 0.1 Momentum = 0.7–0.7 Neurons = 16 Epoch = 5000 Transfer function = hyperbolic-tangent	Correlation coefficient Between Experimental TSS and Predicted TSS	Training = 0.93 Testing = 0.90
Ours	Noise removal (using stdfil, modified thresholding filter), image enhancement (histogram stretching)	TSS	GLCM 4 features (using Matlab 17)	Neural network LR = 0.1 Momentum = 0.7–0.7 Neurons = 20 Epoch = 12	Correlation coefficient between experimental TSS and predicted TSS	Training = 0.99 Testing = 0.92

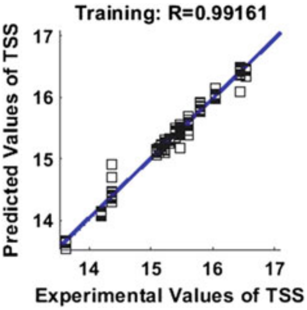


Fig. 2 *R* values obtained while training of the data

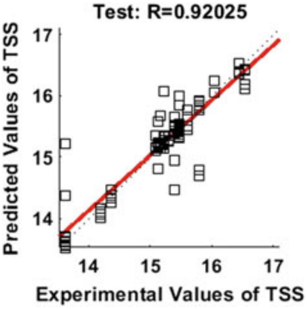


Fig. 3 *R* values obtained while testing of the data

3 Results

For the experiment, from 324 images of pomegranate, 162 images for training, 113 images for testing and 49 images for cross-validation were used. Textural features extracted from the images were given as input to the network. The R-value for measured TSS and model-predicted TSS for training data was 0.99 and testing data was 0.92, and are shown in Figs. 2 and 3 in the order. Experimentation has been done with Matlab 17.

4 Conclusions

Nondestructive imaging of pomegranate based on magnetic resonance imaging provides a greater potential to determine maturity and internal breakdown, which are controlled by the internal physiochemical values. For the internal attributes, four co-occurrence matrix texture features were extracted from the images. These features were provided as input to the NARX neural network which predicted higher correlation coefficient, $R = 0.99$ and $R = 0.92$ for training and test data, respectively, as compared to the MLP architecture. With the improved correlation results obtained, the proposed future work for grading the pomegranate based on physiochemical values satisfying those of export values can be carried out. With the advent of deep learning neural network techniques, fruit grading for different cultivars of pomegranate can be implemented to predict the maturity and internal breakdown of the fruit extending the availability of the fruit in the market. The improved results states that MRI as nondestructive method of grading is evolving with a promising technique for on-line sorting of pomegranate fruit and with ever-increasing improvement in MRI facilities this goal will be achievable in near future.

Acknowledgements I admire the technical support of National Research Center on Pomegranate (NRCP), Solapur. I express my gratitude to Dr. Jyotsna Sharma, Director In charge, NRCP and Dr. K. Dhinesh Babu, Principal Scientist, for their support.

References

1. The Agricultural and Processed Food Products Export Development Authority (APEDA)
2. Ganeshkumar Rede, Santosh Yumnam (2016) Performance of pomegranate export from India. Econ Aff 61:575–580. https://doi.org/10.5958/0976-4666.2016.00071.1
3. Kim SM, Chen P, McCarthy MJ, Zion B (1999) Fruit internal quality evaluation using online nuclear magnetic resonance sensors. J Agric Eng Res 74:293–301
4. Barriero P, Ruiz-Cabello J, Fernandez-Valle ME, Ortiz C, Ruiz M (2000) Mealiness assessment in apples and peaches using MRI techniques Article. Magn Reson Imag 18(9):1175–1181
5. Wang SY, Wang PC, Faust M (1988) Non-destructive detection of water-core in apple with nuclear magnetic resonance imaging. Scientia Hortic 35:224–234
6. Herremans E, Melado-Herreros A, Defraeye T, Verlinden B, Hertog M, Verboven P, Nicolai BM (2014) Comparison of X-ray CT and MRI of water core disorder of different apple cultivars. Postharvest Biol Tech 87:42–50
7. Milczarek R (2009) Multivariate image analysis: an optimization tool for characterizing damage-related attributes in magnetic resonance images of processing tomatoes. Ph.D. dissertation, University of California, Davis, CA., USA
8. Balogun WA, Salami MJE, McCarthy MJ, Mustafah YM, Aibinu AM (2013) Intelligent technique for grading tropical fruit using magnetic resonance imaging. Int J Sci Eng Res 4(7):216 (ISSN 2229-5518)
9. Zhang L, McCarthy MJ (2013) Assessment of pomegranate postharvest quality using nuclear magnetic resonance. Postharvest Biol Technol 77:59–66
10. Khoshroo A, Keyhani A, Zoroofi RA, Rafiee S, Zamani Z, Alsharif MR (2009) Classification of pomegranate fruit using texture analysis of MR images. Agric Eng Int CIGR E J. 11:1182
11. Khoshroo A, Keyhani A, Zoroofi RA, Yaghoobi G (2011) Non-destructive Inspection of pomegranate maturity using magnetic resonance imaging and neural networks. CIGR Section VI international symposium on towards a sustainable food chain food process, bio processing and food quality management
12. Caballero Daniel, Antequera Teresa, Durán Marisa, Caro Andres (2017) Applying 3D texture algorithms on MRI to evaluate quality traits of loin. Art J Food Eng 222:258–266

Implementation of Differential Privacy Using Diffie–Hellman and AES Algorithm

P. V. Vivek Sridhar Mallya, Aparna Ajith, T. R. Sangeetha, Arya Krishnan and Gayathri Narayanan

Abstract Differential privacy is a method adopted to check for any privacy breach that occurs during communication for the exchange of confidential information. Here, in this work, differential privacy is being implemented in the context of vehicular ad hoc networks (VANETs). In this paper, we implement the concept of differential privacy using the Diffie–Hellman key exchange algorithm and the advanced encryption standards (AES) algorithms that are very powerful in terms of their performance. Algorithms like Laplace and Gaussian algorithms, which are currently the most commonly implemented algorithms, have been used for verification. The algorithms were analyzed by considering a situation where an initial location and final location have been defined and these have been encrypted using the mentioned algorithms and the privacy has been preserved.

Keywords Differential privacy · VANETs · Diffie–Hellman algorithm · AES

1 Introduction

Differential privacy helps us obtain accurate data from a collected set of data and also to handle the privacy issues connected to it while dealing with data. One common application of this concept is with regard to individual database. Differential privacy aims in identifying the difference within the database of each and every individual. Even if the individual is an active or passive entry in the database, there should not be any difference to the individual. An adversary should not be able to access anything new from the database containing the information of the individual. For this purpose, different algorithms have been adopted such as Diffie–Hellman key exchange algorithm and advanced encryption algorithm.

At first, we consider a few set of auxiliary information of a particular individual. The auxiliary information of the individual or group like name, occupation, etc.,

P. V. Vivek Sridhar Mallya · A. Ajith · T. R. Sangeetha (✉) · A. Krishnan · G. Narayanan
Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, Kerala, India
e-mail: tr.sange@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_15

constitutes the statistical database. The statistical database contains the private information of a particular group which has been collected by a particular entity. This information might be medical reports of an individual or routine information which are associated with the identity of a person. A privacy breach occurs when an adversary hacks this particular data. The adversary hacks this information by accessing a statistical database [1].

Privacy is of supreme importance, especially in today's transparent society. It demands the protection and safe handling of data associated with individuals. The concept of differential privacy aims at maximizing the correctness of the queries from the defined databases while measuring how the privacy is affected on individuals whose information is stored in the database. Search engines, hospital records, corporate firms, and other such institutions possess large amounts of data much of which are very sensitive. Such data are no longer just important to their domain agencies but are becoming widely common to all those who use that data. In making the data available for public, they also need to face the consequences in terms of the legal, financial, and moral pressure since they are also bound to protect the identities of the individuals. Hence, a trade-off between privacy and utility is of great importance.

2 Differential Privacy

2.1 Need for Differential Privacy

Consider a situation in which we want to take the medical records of a person "K." If a privacy breach occurs and all identifiable information such as name, identity proof number, mobile number, etc., had to be removed from the original data set, then the available records would contain only information such as date of birth, gender, and address details. These fields are more than sufficient to provide a unique combination that they are often required to identify an individual from the database. The technique used here is to pick out the information that is linked with "unidentified" records by tagging it with some additionally available data. Generally, when people are asked for their personal information, they are hesitant to provide it, for fear of the data being misused in some way or the other. Nevertheless, if the data are used in a differentially private manner, then the individual can be assured that the data will be virtually hidden and that it will not be available to any third party for misuse. This would prompt the users to provide their data since they know that it is secured in the right sense.

2.2 Epsilon-Differential Privacy

Dwork, McSherry, Nissim, and Smith in 2006, in their article, introduced the concept of epsilon-differential privacy. The main agenda behind the definition of epsilon-differential privacy in 2006 is that it is not possible to sacrifice the privacy of an individual by a statistical release of their data from the database. So, the goal here is to provide each and every individual the same privacy that would result from having their data removed; that is, the statistical functions running on the database should not depend too much on their data of any of the individual. A mechanism provides differential privacy if for all databases x, x' which are adjacent and for all $z \in Z$, we have

$$\frac{P(K = z/X = x)}{P(K = z/X = x')} \leq e^{\epsilon}$$

The result is the ϵ-differential privacy [2]. Here, ϵ (privacy parameter) is a positive real number. ϵ can be viewed as a relative measure of privacy. Its value can be chosen upon analyzing the goal of hiding any person's presence or absence in a given database [3].

2.3 Application Scenario—VANETs

VANETs or vehicular ad hoc networks are exchange networks where data packets are exchanged between vehicles which are commonly referred to as common nodes traveling on defined constrained path. In vehicular networks, there is a chance of privacy risks where vehicles could be tracked by the information transmitted by the vehicle-to-vehicle (v2v), vehicle-to-infrastructure (V2I), or vehicle-to-x (V2X) communications implemented with the dedicated short-range communications (DSRC) standards operating at 5.9 GHz. VANET requires fully decentralized network control since no central entity could or should organize the network [4].

In VANETs, the nodes, which are vehicles, are installed with on-board units (OBUs) to them to communicate with other vehicles in the vicinity and also to stationary structures as the application demands. VANETs therefore form a special case of sensor networks. Here, in wireless sensor networks (WSNs) the sensor nodes are installed near the roadside to monitor the road condition and to send the information about dangerous conditions to vehicles regardless of the connectivity of the VANET. Each vehicle has the functionality of being a packet transmitter, receiver, or router which enables the vehicles to communicate with other vehicles or access points which form the stationary roadside units (RSUs) [4].

There are three main types of vehicular communication system. They are:

1. **Vehicle-to-Vehicle (V2V)**—Using vehicle-to-vehicle, a vehicle can detect the position of and movement of other vehicles which are half a kilometer away.

This topology allows mobile-to-mobile interface among vehicles. Pure ad hoc communication is actually vehicle-to-vehicle communication. Each vehicle in V2V communication has a lot of gadgets attached to global positioning system (GPS) networking devices, sensors, and digital map which contain the route map and relevant information and computing devices. These vehicles communicate with neighboring vehicles by sensing its own traffic messages and sending beacon messages to the other vehicles periodically. The data communication techniques implemented in V2V communication are unicast and multicast packet forwarding techniques between the source and destination vehicles. Here, unicast means sending or receiving packets to and from its own direct neighbors. Unlikely, multicast forwarding helps to exchange packets with remote vehicles also by making use of intermediate vehicles as relays.

2. **Vehicle-to-Infrastructure (V2I)—**V2I is the intelligent technology for the next generation. This topology allows interface between vehicles and roadside units. Here, the infrastructure plays an important role in coordinating the communication by collecting local or global information on the traffic conditions in the road and then suggesting some of the behaviors on a group of vehicles. For example, one technique which employs V2I is the ramp metering. It requires limited sensors and actuators for measuring the traffic density. V2I communication which is enabled by a system of hardware, software, and firmware, by nature is wireless. The major implication is that infrastructure components such as lane markings, signboards, and traffic signals or any other infrastructure can wirelessly provide information to the vehicle and vice versa.
3. **Vehicle-to-X (V2X)**—It is referred to as vehicle-to-everything communication. In V2X communication, information from various sensors on the OBUs and other sources travel via a large bandwidth, low latency, and high-reliability links, giving the experience of fully autonomous driving. All the other types of networks fall under this topology. By following this type of network configuration, vehicles can easily communicate with other vehicles, to infrastructural units like traffic signals or smart parking lots, to pedestrians holding their cell phones, and also to central hubs or data centers using cellular networks.

3 System Model and Implementation

Trajectories are generated by vehicles in large numbers, which are significantly different from pedestrian locations. Assuming $T = \{$location 1, location 2, location 3, ..., location $n\}$, where T is a set consisting of vehicular locations appearing in a sequential manner. Every point denotes a location in trajectory, which is an ordered pair comprising of longitude and latitude. In order to conform to the standards that are required to be met in order to ensure the protection of privacy, some interference items are added to generate the published trajectory $\mathrm{TR} = \{T1, T2, T3, \ldots, Tn\}$. By referring to the map, the third-party hackers can clip the interference items because of the limitation of roads in VANETs [5]. The most precarious of the situation would be that if the hackers are able to obtain even a small set of values out of the total location space, they will be able to interpolate the points in between and thereby generate a trajectory which will bear a very close resemblance to the original trajectory. Keeping this in perspective, this project aims at creating a cost-effective indoor localization and tracking system that does not require any infrastructure assistance. Just with the help of smartphones, the user can be localized.

A differential privacy protection protocol is implemented in the Java language based on the Diffie–Hellman key exchange algorithm and the (AES) Advanced Encryption Standard 256 algorithm. Firstly, a symmetric key is generated by the D–H key exchange algorithm, and then, the AES 256 algorithm is used to encrypt the transmitted content, thereby protecting the privacy of the user information. The idea of the differential privacy protection prototype can be understood with the help of a simple observation: when the data set D contains the individual Alice, it is set to perform random query operations on D (such as counting, summing, mean, median, interquartile range, or other related queries). The result obtained is $f(D)$. On carrying out the operation, if the result yielded on querying Alice's information from D is still $f(D)$, it can be considered that Alice's information is not included in data set D. In the middle of it creates additional risks. Differential privacy protection is to ensure that any individual in the data set or in the data set has little impact on the final published query results. The goal of differential privacy is to maximize query accuracy and minimize the risk of privacy breaches [6].

The Diffie–Hellman key exchange algorithm, denoted as D–H algorithm, is a very powerful protocol in public-key encryption. It allows the parties to institute a key over an unsecured channel with no previous intimation from the other party. The advantage being that this key can be used as a tool, a symmetric key, to encrypt the communication content in ensuing communications [7].

3.1 D–H Key Exchange Algorithm

Consider a scenario where we have Alice, Bob, and Eve as shown in Fig. 1. Alice and Bob are exchanging some sort of data among each other, and Eve being an intermediator who is constantly watching Alice and Bob. But, here Eve, she does not disturb the subject or content of the communication. Now, consider a public prime base say $g = 3$ which is known to all the three. Next, consider a public data known to Alice, Bob, and Eve which are $p = 12$. Now, consider Alice's key (private key) which is known to her alone which is $a = 6$. Next, consider Bob's private key known only to Bob as $b = 15$.

Let A denotes the public key of Alice known to Alice, Bob, and Eve where

$$A = \left(G^{a}\right) \bmod p = 9$$

Let B denotes the public key of Bob known to Alice, Bob, and Eve where

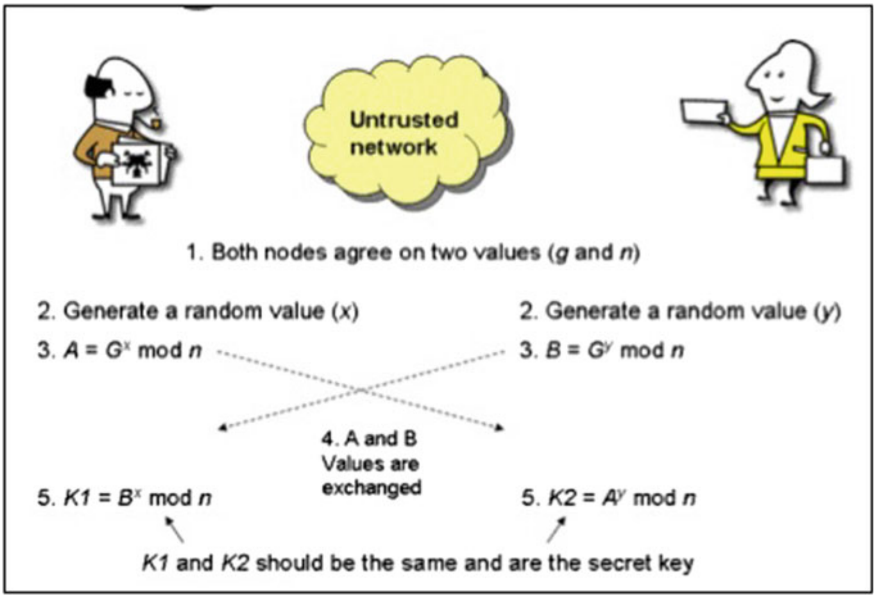

Untrusted network
1. Both nodes agree on two values (g and n)
2. Generate a random value (x)
3. A = G^x mod n
2. Generate a random value (y)
3. B = G^y mod n
4. A and B Values are exchanged
5. K1 = B^x mod n
5. K2 = A^y mod n
K1 and K2 should be the same and are the secret key

Fig. 1 Conceptual representation of the D–H algorithm

$$B = \left(G^{b}\right) \bmod p = 7$$

Next, Alice and Bob exchange each of their public keys. Let s denotes the shared secret key common to both Alice and Bob, but which is not known to Eve.

For Alice,

$$s = \left(B^{a}\right) \bmod p = 1$$

For Bob,

$$s = \left(A^{b}\right) \bmod p = 1$$

So, even if a hacker attacks, he will not be able to provide the actual data because he does not know the key to decode it. In real scenario, consider Alice and Bob represent two vehicular ad hoc networks, while Eve represents the transmitting medium or mediator. Thus, the above algorithm is real-life implementation of VANETs [8].

3.2 Advanced Encryption Standard Algorithm

The advanced encryption standard is an encryption method in which the characters are replaced by some other kind of operation such as addition, subtraction, exclusive-or, or any such similar operators. By this, it is possible to produce infinite number of combinations. Subbytes, shiftrows, mixcolumns, and addroundkey are some of the techniques which can be used for making rotations. The AES algorithm consists of AES-128, AES-192, and AES-256 block ciphers. The three variants of AES are based on different key sizes (128, 192, and 256 bits) [9].

4 Results

This section shows the results that have been taken in terms of the location values, encrypted and protected. The values considered are assumed to be data taken from the on-board unit of a car which conveys the exact location of the vehicle. As can be seen, the initial location conveyed is the location of the house, assuming that the car is parked at the house and is starting from there (Figs. 2 and 3).

In this work, we are presenting the comparison between the above algorithms for the following choice of values as shown below:

k = 28

q = 117686837408564885453421841793708809347228146689137677955112976
839435485865199857879508580012979773101731109967631730935911488 33
98783565332648805327907105 7

p = 3295231447439816792695811570223846661722388107295854982743163351
504193604225596020626240240363433646848471079093688466205521673516 5
939829314166549181398959 7

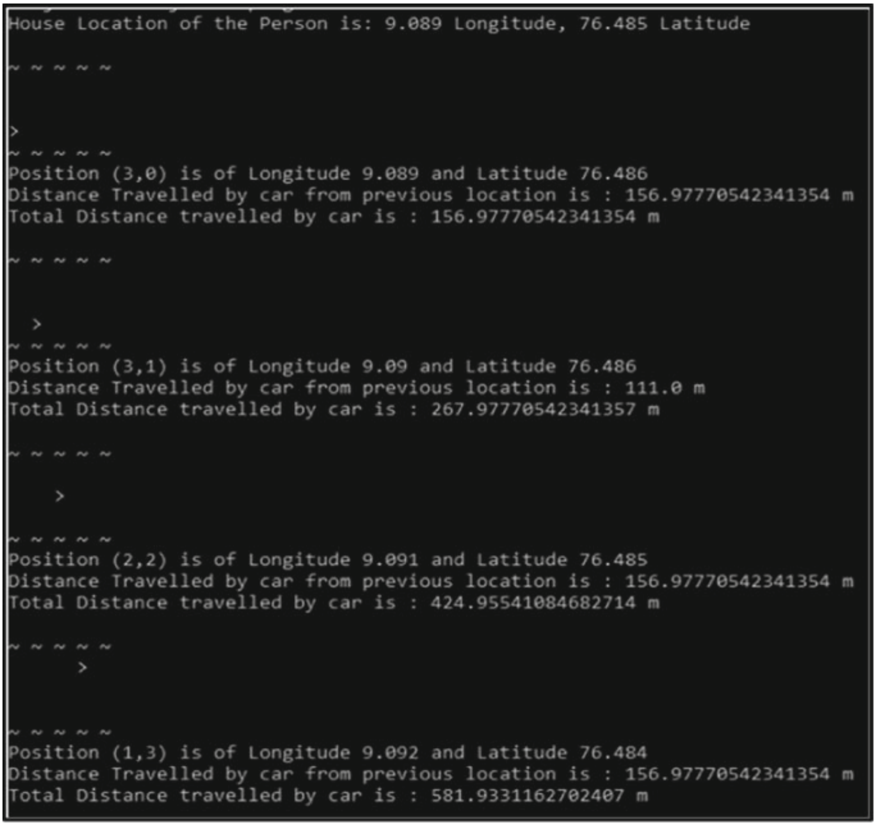
g = 2936079689421990213596959618831699609892128325127375389414219745
98430263629524708683392530750033382195532008794395609507801074545519
29347513371119440534090946249252931698618289251122473408140692956145
461002165727325675275594633569549480757345505452885932494365176852 80
1351301781101072492804530356854258269466 16

Setup:

k01 = 7288733984413185487103013941394791506761763938864255344085195 02
482517961481001673652539036349530544763229427728477957609143936517 09
753160645210747308527 43

N = 50

Setup use time is 95 ms



```
House Location of the Person is: 9.089 Longitude, 76.485 Latitude

~ ~ ~ ~ ~


>
~ ~ ~ ~ ~
Position (3,0) is of Longitude 9.089 and Latitude 76.486
Distance Travelled by car from previous location is : 156.97770542341354 m
Total Distance travelled by car is : 156.97770542341354 m

~ ~ ~ ~ ~


  >
~ ~ ~ ~ ~
Position (3,1) is of Longitude 9.09 and Latitude 76.486
Distance Travelled by car from previous location is : 111.0 m
Total Distance travelled by car is : 267.97770542341357 m

~ ~ ~ ~ ~

    >

~ ~ ~ ~ ~
Position (2,2) is of Longitude 9.091 and Latitude 76.485
Distance Travelled by car from previous location is : 156.97770542341354 m
Total Distance travelled by car is : 424.95541084682714 m

~ ~ ~ ~ ~
      >


~ ~ ~ ~ ~
Position (1,3) is of Longitude 9.092 and Latitude 76.484
Distance Travelled by car from previous location is : 156.97770542341354 m
Total Distance travelled by car is : 581.9331162702407 m
```

Fig. 2 Output data as computed by the algorithm

ke1 = 0

Phase 2: Encrypt use time is 7 ms

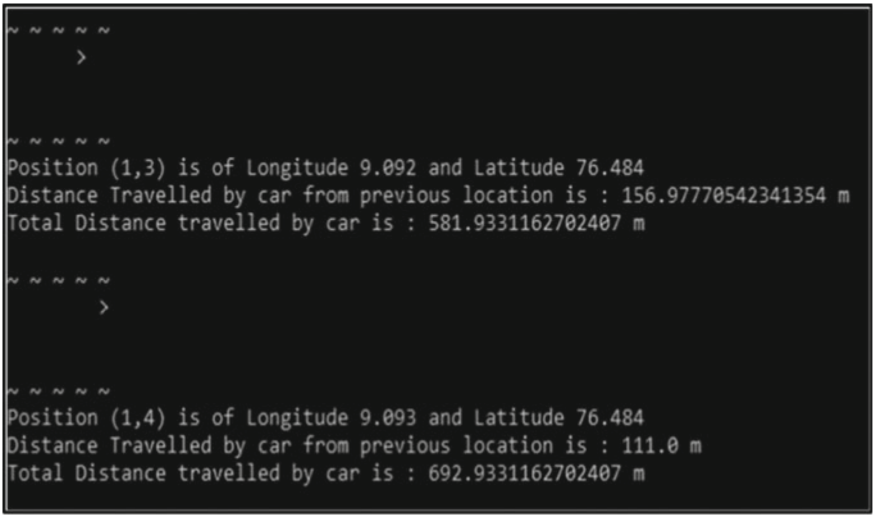
ke2 = 0

Encrypt xN = 26520

Decrypt xN = 26520

Decrypt use time is 9 ms

k is the number of bits in the data, p and q are the encryption key known to two vehicles, and g is known to vehicles and the adversary. After using Diffie–Hellman algorithm and advanced encryption method, keys are produced which is not known to adversary; that is k01, ke1, and ke2 are the key used for encryption. The encryption time and decryption time have also been calculated [10].



```
~ ~ ~ ~ ~
      >


~ ~ ~ ~ ~
Position (1,3) is of Longitude 9.092 and Latitude 76.484
Distance Travelled by car from previous location is : 156.97770542341354 m
Total Distance travelled by car is : 581.9331162702407 m

~ ~ ~ ~ ~
        >


~ ~ ~ ~ ~
Position (1,4) is of Longitude 9.093 and Latitude 76.484
Distance Travelled by car from previous location is : 111.0 m
Total Distance travelled by car is : 692.9331162702407 m
```

Fig. 3 Output data as computed by the algorithm

5 Conclusion

Differential privacy can be effectively used to ensure security in vehicular ad hoc networks. The contribution of the work is that this approach has been implemented in the context of security in vehicular ad hoc networks. The implementation of the algorithms for finding the trajectory of motion of vehicle when start and end longitude and latitude is available along with a matrix defined containing the locations nearby is obtained. Also, the comparison between Laplace algorithm and Median algorithm was done which are commonly used to implement differential privacy in VANETs. Along with this, we also obtained the result for the implementation of two currently used algorithms Diffie–Hellman key exchange algorithm and advanced encryption standards algorithm. In today's society driven by big data, where these data hold enormous significance, it is necessary to ensure that privacy is not compromised. This work is a small attempt in that direction. The project aims at creating a cost-effective indoor localization and tracking system that does not require any infrastructure assistance. Thus, just with help of smartphones, the user can be localized. Although it is a promising area of research and one of extreme importance, this concept has not been explored to its full capability due to limitations in understanding it completely and also due to its non-trivial method of implementation.

References

1. Roth A (2010) Algorithms for preserving differential privacy, CMU-CS-10-135 (references)
2. Kressner D, Implementing differential privacy. Institute of Information System, School of Business and Economics Humboldt University of Berlin, Term paper for the IT Security Seminar
3. Ding Z, Wang Y, Wang G, Zhang D, Kifer D (2019) Detecting violations of differential privacy. arXiv:1805.10277v4 [cs.CR]
4. Baldini G, Giuliani R (2017) Analysis of the privacy threat in vehicular ad-hoc networks due to radio frequency fingerprinting
5. Nelson B, Olovsson T (2017) Introducing differential privacy to the automotive domain: opportunities and challenges. In: 2017 IEEE 86th vehicular technology conference. https://doi.org/10.1109/vtcfall.2017.8288389
6. Pradeep LN, Bhattacharjya A (2013) Random key and key dependent S-box generation for AES cipher to overcome known attacks. In: Security in computing and communications. Berlin, Heidelberg
7. Hay M, Machanavajjhala A, Mikalu G, Chen Y, Zheng D, Principled evaluation of differentially private algorithms using D.P Bench
8. Diffie-Hellman key exchange. https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
9. The Advanced Encryption Algorithm. https://www.commonlounge.com/discussion/e32fdd267aaa4240a4464723bc74d0a5
10. Neha, Kaur M (2016) Enhanced security using hybrid encryption algorithm. Int J Innovative Res Comput Commun Eng 4(7)
11. Rewagad P, Pawar Y (2013) Use of digital signature with Diffie Hellman key exchange and AES encryption algorithm to enhance data security in cloud computing. In: Proceedings of the international conference on communication systems and network technologies
12. Ganesh AR, Manikandan PN, Sethu SP, Sundararajan R, Pargunarajan K (2011) An improved AES-ECC hybrid encryption scheme for secure communication in cooperative diversity based wireless sensor networks. In: International conference on recent trends in information technology, ICRTIT 2011, Chennai, pp 1209–1214

Implementation of Neural Signals in MATLAB (Thought Signals)

Kambhampati Sai Sandilya, Poornima Mohan, Madiraju Akshay Bharadwaj, B. Maragatha Eswari, K. Namitha, O. Rajasekhar Reddy and J. Vaishnu Saran

Abstract The most intelligent creatures on the earth are homosapiens since their brain is gifted with the ability of thinking and expressing emotions through different means. The human brain is a universe consisting of a cluster of neurons connected to each other. There are about 100 billion neurons in the human brain. Estimated that a neuron connection transmits at least one signal per second, and some theories proved that some of the specialized connections transmit up-to 10,000 signals per second [1]. Briefly, we can say that when we experience something through sense organs which are having direct contact with our brain, release some or other chemical called hormones. For instance, if we feel something 'very good to our heart!' or like start loving something by sensing anything, our brain produces a hormone called 'oxytocin'. As there is an extraction of this hormone happens in a 'Patterned' manner from an import gland of our human body called as the pituitary gland, the pattern creates an electrical signal/impulse which transmitted to our brain in a fraction of seconds, making us experience the emotion called love on that particular object or

K. S. Sandilya (✉) · P. Mohan · M. A. Bharadwaj · B. M. Eswari · K. Namitha · O. R. Reddy · J. V. Saran
Department of Electronics and Communication Engineering, Amrita School of Engineering, Kollam, Kerala, India
e-mail: knvsspss@springer.com

P. Mohan
e-mail: poornimamohan@am.amrita.edu

M. A. Bharadwaj
e-mail: akshaybharadwaj98@springer.com

B. M. Eswari
e-mail: maragathaeswari@springer.com

K. Namitha
e-mail: namitha96k@springer.com

O. R. Reddy
e-mail: orsr97@springer.com

J. V. Saran
e-mail: jvaishnusaran@springer.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_16

person. The electrical impulse created here and transmitted to the brain is nothing but a thought/emotion signal. Our main aim is to extract a converted written text or an image of the electrical impulse created, this electrical impulse is extracted out from a human brain through EEG signals.

Keywords EEG signals · Patterned signals · Electrical impulses · Neurons

1 Introduction

1.1 What Is a Thought Signal?

Thoughts are the effect of simulation that happens when we feel touch, smell, taste, sound or sight through the five sense organs namely skin, nose, tongue, ears and eyes. These stimuli when we sense something will have direct neural contact with the brain generating a special kind of fluid from the glands present in our body known as the hormones. The amount of production, the speed, and timing of the production of these hormones produce stimuli or an electrical impulse in our brain, which are generally a form of signals in electronics terminology and are known as thoughts in general case. These can also be ideas, believes on self or on others. Assume, the human body as a machine made up of a microcontroller called the brain, which is made of some sensors or microprocessors called sense organs which can send and receive the impulses or signals from the brain. These signals are passed through a medium for which these sensors are connected to the brain, which is called nerves. Every sensor is made up of a very large scale integrated circuits (VLSI circuits) called transistors [2]. Similarly, our nerves are made of nerve cells or neurons [3, 4]. Let us consider an example of a tennis player playing a tennis match. As the player watches the approaching ball, two types of senses activate immediately, his/her sight on the ball, and the sound of the air through which the ball is coming [5, 6]. Then the impulses are sent to the brain and the brain sends some signals to the motors of the machine that our hands and legs to move, to hit the ball. Everything and every thought process happen the same [7, 8]. But, it is not known how to visually look at these signals, which are in our mind. Let us have an assumed theory, to visually find our thoughts. With this, we have another application also, we can see our dreams as an image signal [9, 10] (Fig. 1).

The above figure illustrates how a thought signal is generated in a tennis player when he is standing in the tennis court and the ball is running towards him.

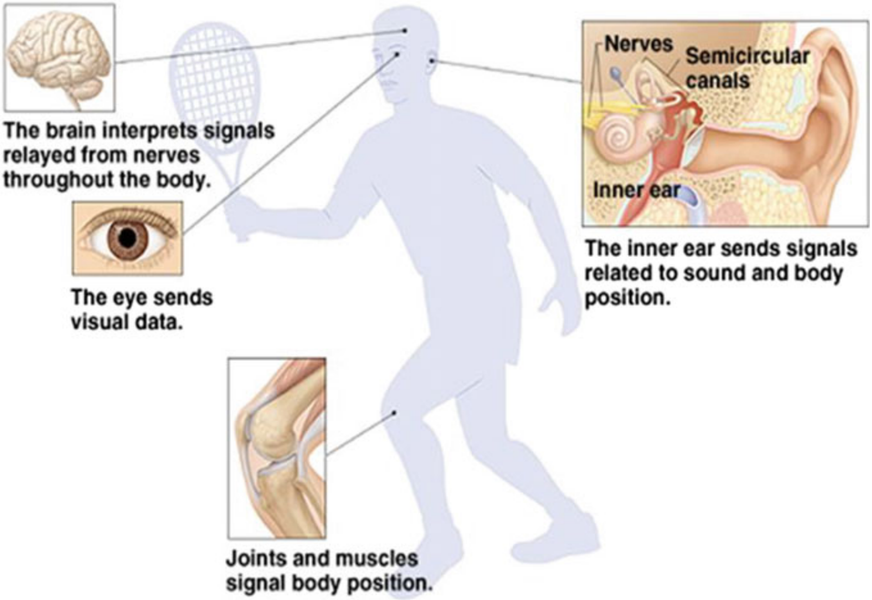

The brain interprets signals relayed from nerves throughout the body.
The eye sends visual data.
Nerves
Semicircular canals
Inner ear
The inner ear sends signals related to sound and body position.
Joints and muscles signal body position.

Fig. 1 Stimulation of thought signals in a tennis player

2 Methodology

2.1 Brain and Computer Interface (BCI)

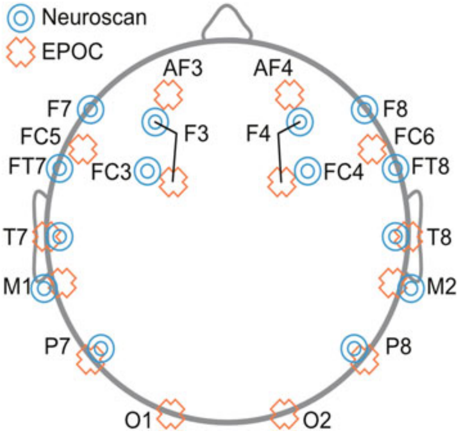
At present in the field of Biomedical Engineering, Brain and Computer Interface (BCI) has a huge demand [11]. BCI technique is that creates a great link between the computer and the human brain. Nowadays BCI technique is mostly used in Artificial Intelligence (AI), that is in controlling robots, through the human brain, mobility commanding system, the best example is Stephen Hawking's chair and communication fields. Here the signals are captured as an Electroencephalography (EEG) signals through a device called EMOTIV EPOC EEG amplifier [1] (Fig. 2).

This amplifier consists of electrodes that are fit to the head of the subject and extracts the signal. This raw signal is transferred into the computer through a Bluetooth interface and saved as a .edf file [11].

2.2 Methods to Implement

Selecting the Subjects. The EEG information to be collected from some people aged 20–30 years approximately [11].

Fig. 2 EEG measurement positions on the head



Training the Subjects. The subjects are given with different kind of inputs. For instance, Subject *A* is given something to look at, and similarly, all other subjects are given something to sense with so that their brains start producing the electrical impulse [11] (Fig. 3).

Collecting and Storing the Signal. The generated signal is collected from the EMOTIV EPOC EEG amplifier and stored into the computer in the form of .edf or .mat files through Bluetooth and taken into MATLAB for further evaluation. The EEG measurements on the brain are explained in the following Table 1.

Signal and Image Processing. EEG signals are generated in the form of Analog signals. Analog Signals are continuous signals which have time-varying quantities.

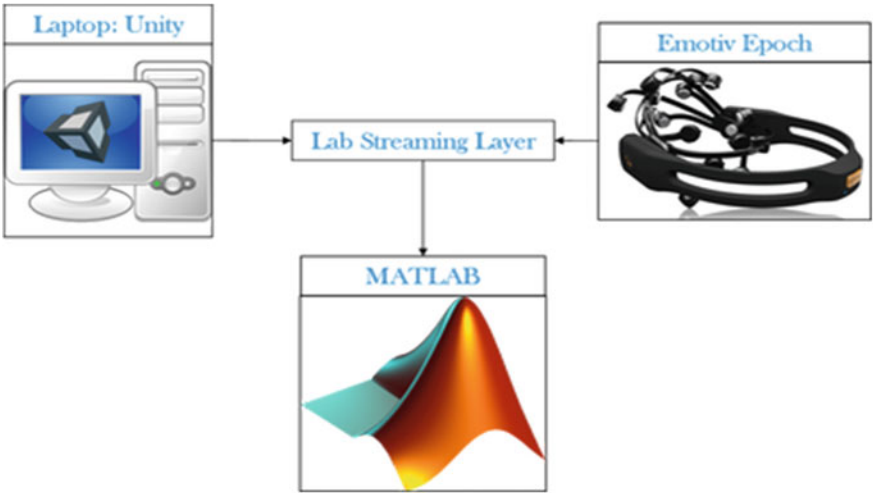


Fig. 3 Block diagram illustrating the signal transmission into MATLAB

Table 1 The EEG functional measurements on the brain [11]

Lobe	Function	EMOTIV EEG (positions/channels)
Frontal	Emotions, cognition	AF3, AF4, F3, F4, F7, F8, FC5, FC6
Parietal	Movement	P7, P8
Occipital	Sight, vision	O1, O2
Temporal	Hearing	T7, T8

EEG signals vary from 5 to 500 Hz of the sampling frequency. As the .edf file is converted into the .mat form, it can be directly used into the MATLAB. To plot the EEG signal in MATLAB, initially, after loading the .mat file into the MATLAB, subtract the value provided ‘Gain’ and divide the whole value with the provided ‘Base’.

$$val = load(\text{‘}Subject00\_2\_edfm.mat\text{’}) \tag{1}$$

$$eeg = (val - Gain)/Base; \tag{2}$$

Now for plotting the cure, we need to calculate the time of the curve with the provided sampling frequency and obtained signal.

$$time = (0 : length(eeg) - 1)/Fs \tag{3}$$

$$Fs = Sampling\ Frequency$$

When we try to plot the signal with these specifications given, a continuous analog signal with about (1 × 5000) double length is plotted as shown in (Fig. 4)

Now, the signal is generated as an Analog signal. This Analog signal needs to be converted to Digital signal using Analog to Digital conversion (ADC) technique. In ADC technique, calculate the quantization value with the given needs range and number of bits of the required plot.

$$q = r/\left(2^n - 1\right); \tag{4}$$

q = quantization, r = range of the signal, n = number of bits.

Now, we divide the signal with the obtained quantization value and will get a quantized signal, and use decimal to binary conversion of the quantized analog values, which will convert the analog values of the quantized EEG signal into binary values. Plot the binary values with respect to the original raw EEG plot, with a decrease in the number of values in the original signal to make the process easy. But, the drawback in the method is we need to take the absolute values of the original signal

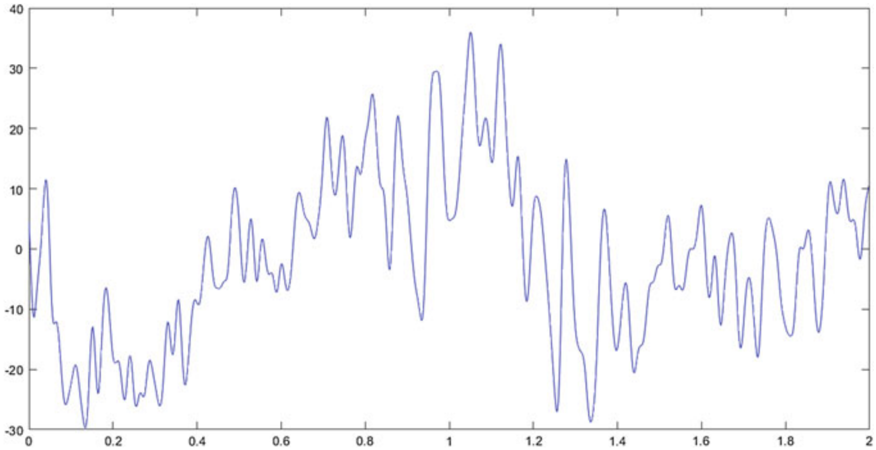


Fig. 4 Plot of raw EEG signal

to plot the binary plot. The below plot represents the binary converted EEG signal [12] with respect to the original raw signal.

Figure 5 represents the plot of digitalized EEG signal with respect to the absolute raw signal.

Figure 6 represents the illustration of the only Digitalised EEG signal. This is the plot of all the converted digital values of quantized Analog values.

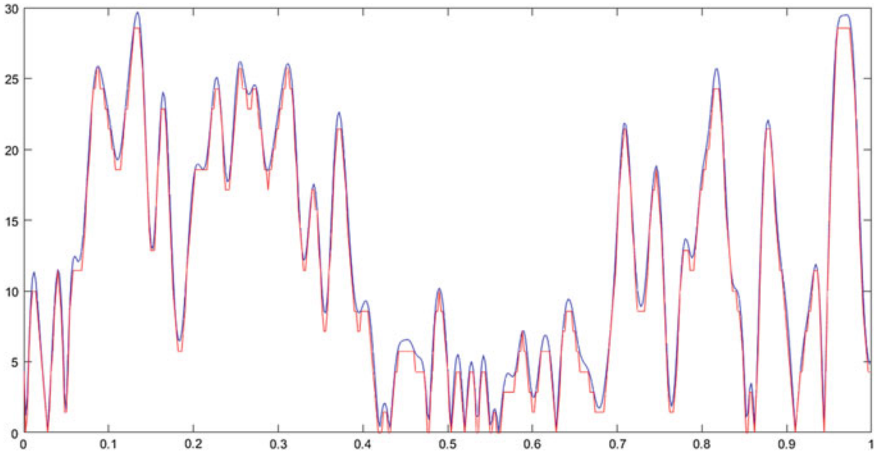


Fig. 5 Plot of a digitalized EEG signal with respect to raw EEG signal

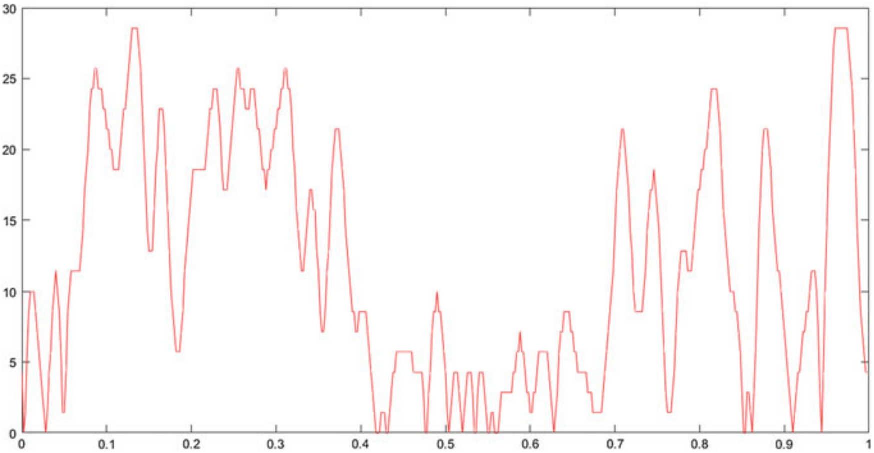


Fig. 6 Plot of a digitalized EEG signal

3 Results and Future Scope

3.1 Results

After digitalizing the signal, modulate the digital signal either in Amplitude (AM) or Frequency (FM) format if needed. Digital values are obtained from the digitalized signal. These digitalized values are arranged as a matrix, such that when the matrix is plotted in the form an image using '*imshow*', an in-built command in MATLAB, converts the produced matrix into an image by considering each value in the matrix as a pixel. Here, a rough sketched image of the digitalized EEG signal is generated, where '0' value of the signal is taken as black colour and '1' value as white and displays a pixelated image.

Figure 7 Interpreters an object that is shown to '*Subject00_2*', one of the subject in the experiment.

3.2 Future Scope

This BCI (Brain and Computer Interface) can be improved further and can be used in getting a visual image of the dreams of people. Most of its applications can be used for those people who are in the state called 'COMA', but can hear and couldn't respond to the outer world. Their thoughts can be reconstructed as an image and can rectify what the problem is. Involving the machine learning concept to this may increase the accuracy and speed of the resultant.

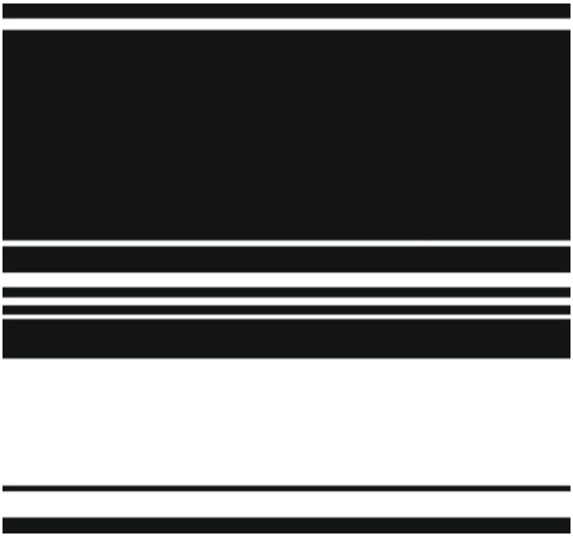


Fig. 7 Plot of a digitalized EEG signal in the form of an image signal

4 Conclusion

The above-mentioned research work clearly explains, how a EEG thought signal collected from a human brain can be interpreted as an image. The output must be furthermore modelized in a more equipped and developed apparatus, like increasing the pixels of the image and using other image processing techniques such that the subjects' thoughts are purely displayed as an image in either black and white or RGB frame.

References

1. Thomas T, James M, Shaji RR, Pillai BC (2016) Interpretation of human stages from EEG signals using LabVIEW. Int J Adv Res Comput Commun Eng 5(3)
2. Soman KP, Manikandan S, A novel method for detecting R-peaks in electrocardiogram (ECG) signal. J Biomed Sig Process Control
3. Gurumurthy S, Mahit VS, Ghosh R (2013) Analysis and simulation of brain signal data by EEG signal processing technique using MATLAB. Int J Eng Technol 5:2771–2776
4. Sutradhar S, Sayadat N, Rahman A, Munira S, Fazlul Haque AKM, Sakib S (2017) IIR based digital filter design and performance analysis:1–6. https://doi.org/10.1109/tel-net.2017.8343596
5. Joy J, Peter S et al (2013) Denoising using soft thresholding. Int J Adv Res Electr Electron Instrum Eng 2(3):1027–1031
6. Walters-Williams J, Li Y (2012) BMICA independent component analysis based on B-Spline mutual information estimation for EEG signals. Can J Biomed Eng Technol 3(4):63–79
7. Kroupi E, Yazdani A et al (2011) Ocular artifact removal from EEG: a comparison of subspace projection and adaptive filtering methods. In: 19th European signal processing conference. Barcelona, Spain

8. Akhtar MT et al (2009) Focal artifact removal from ongoing EEG-A hybrid approach based on spatially constrained ICA and wavelet denoising. In: 31st annual international signal conference of the IEEE EMBS Minneapolis, Minnesota, USA, 2–6 Sept 2009
9. Prasad VVKDV et al (2013) A new wavelet packet based method for denoising of biological signals. Int J Res Comput Commun Technol 2(10):1056–1062. Simranpreet Kaur1 IJECS Volume 3 Issue 8 August, 2014 Page No.7965-7973 Page 7973
10. Abdullah H et al (2013) Double density wavelet for EEG signal denoising. In: 2nd international conference on machine learning and computer science, Kuala Lumpur, Malaysia, 25–26 Aug 2013
11. Sulaiman N, Hau CC, Hadi AA, Mustafa M, Jadin S (2014) Interpretation of human thought using EEG signals and LabVIEW. In: E2014 IEEE international conference on control system, computing and engineering, Penang, Malaysia, 28–30 Nov 2014
12. Kazi MM, Rode YS, Dabhade S, Dawla NAl, Mane AV, Manza RR, Kale KV, Image retrieval and interested image detection for thought processing using EEG signals. UACEE Int J Comput Sci Appl 2(2). [ISSN 2250 - 3765]

A Framework for Formal Verification of Security Protocols in C++

R. Pradeep, N. R. Sunitha, V. Ravi and Sushma Verma

Abstract Every communication system is a safety-critical system, in which the communicating entities share the confidential data over the untrusted public network by using a set of cryptographic security protocols (CSPs). Many security protocols proved secure were cracked within a short span of time, and the best example is Needham–Schroeder authentication protocol. The quality assurance about the correctness of security protocols is one of the key challenges. In software testing, it is not possible to prove the correctness of security protocols, because testing has got major drawbacks and the tester cannot predict what knowledge an attacker may gain about the communication system by interacting with several runs of the protocol, and also testing shows the presence of bugs but can never show the absence of bugs. Formal verification has proved to be a reliable solution as the correctness of the CSP can be proved mathematically. In the proposed work, a new framework is proposed, which includes a library of functions to specify a security protocol in C++ by following a set of rules (syntax and semantics), a interpreter to interpret the C++ code to security protocol description language (SPDL), and finally a model checker Scyther backend verification engine. The proposed framework is successful in identifying the attacks on IKE version-1. Also the Skeme and Oakley versions were verified for their correctness.

Supported by Defence Research and Development Organisation (DRDO), SAG, New Delhi.

R. Pradeep (✉) · N. R. Sunitha · V. Ravi
Department of Computer Science and Engineering,
Siddaganga Institute of Technology, Tumkur 572103, Karnataka, India
e-mail: pradeepr@sit.ac.in

N. R. Sunitha
e-mail: nrsunitha@sit.ac.in

V. Ravi
e-mail: ravi@sit.ac.in

S. Verma
Defence Research and Development Organization, (SAG), New Delhi, India
e-mail: sushmaverma@sag.drdo.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_17

Keywords Formal verification · Model checking · Internet Key Exchange (IKE) · Scyther · Skeme · Oakley · CSP

1 Introduction

CSPs help to achieve secure communication between the communicating agents. They are at the core level of most of the communication systems, such as secure Internet communications, bank transactions, or any electronic way of fund transfers. Such applications should not be delivered without verifying the crypto-analytic weaknesses of the underlying algorithms.

Security protocols are difficult to design, even under the assumption of perfect cryptography. Many CSPs claimed as safe and used for many years were "cracked" within a short span of time, one such protocol is Needham–Schroeder authentication protocol [1] proposed in 1978, and this protocol was used for decades to provide authentication for agents using a hybrid method which involves both public-key and symmetric-key cryptosystems. The Needham–Schroeder protocol was cracked by Galvin-Lowe [2] in 1995 using FDR [3], and a new updated version called Needham–Schroeder-Lowe protocol was released. This shows that there is a need for formal verification of security protocols.

In the development phase of security protocols, if the design errors or functionality errors are introduced, then it is very difficult to detect and debug with testing. To detect and correct the design errors and to achieve high reliability of CSP, formal verification is one of the key solutions and it gives a mathematical proof for the correctness for the security protocols. There are three main approaches for formal verification of security protocols [4]: 1. BAN-logic, 2. Casper/FDR (model checking), and 3. Stranspace. BAN-logic is a light-weight method under the assumption of honest agents and a passive intruder. The Casper/FDR approach translates a high-level description of a security protocol along with its security requirements and a particular instantiation into CSP that can be machine-verified using the FDR model checker [5], and the intruder is in control of the network and is allowed to participate as one of the agents. The same holds for the strand space approach which is basically a Dolev-Yao model [6] which represents a strong adversary and his capabilities. For of all these three approaches, the state space explosion problem is a challenge, in which for a system with "N" number of concurrent processes the number of states increases in the global state graph may grow exponentially with N. [7] Explains a solution to avoid state explosion problem with the help of temporal logics.

In order to use the CSPs in network devices like router, switch, and modems, the protocols have to be implemented using a programming language like C, C++, or any other similar high-level programming language. But there is no mechanism available to formally verify a security protocol which is implemented using a programming language C++. In the proposed work, a new framework is proposed to perform formal verification of security protocols in which a library of security primitives is specified in C++ by following a set of rules (syntax and semantics). A new interpreter is proposed, which converts a CSP specified in C++ language to security protocol description language (SPDL), and a library of APIs is proposed to support cryptographic primitives for CSP specification. In the proposed framework, the Scyther model checker [8] is used as back end verification engine, Scyther has support for multiprotocol black-box analysis mechanism, it is efficient in handling state space explosion problem, and Scyther uses Dolev-Yao channel to model the adversary and guarantees termination of verification process.

To communicate securely over a public network, computers make use of virtual private network (VPN), and VPNs use IKE security protocol to exchange keys between the agents, to authenticate mutually without revealing the identities of the agents. This protocol needs to be formally verified because the agents will be sharing private data over a VPN which is created over a public network. The main challenge in formal verification of security protocols is, building abstract models from the formal specifications, identifying the security properties to be satisfied by a security protocol. In the proposed framework, the secrecy and authentication security properties can be verified for the security protocols, for verification of IKE protocol, the formal specifications are drawn from the RFC 2409 [9], the framework is successful in verifying the IKE version-1, Skeme [10], and Oakley. The framework is successful in identifying the attacks for IKE version-1. The Oakley and Skeme version security properties are proved safe.

2 Proposed Framework to Formally Verify Security Primitives of CSP Coded in C++

Formal verification is a challenging task and requires a lot of effort and knowledge, but the automated tools help to perform verification with ease, these tools are called model checkers, and the verification technique is called formal verification using model checking. A model checker is required to evaluate the security properties by searching through the state space to check whether even a single state violates the security properties specified.

The main challenge in formal verification of security protocols is generating the abstract CSP model and identifying the security properties to be verified. Building an abstract CSP model depends totally on the model checker being used, it changes from one model checker to other, and there is no mechanism to verify a CSP implemented in a high-level language. To solve this problem, in the proposed work, a new framework for specifying a security protocol in C++ language is developed and it is interpreted to the backend model checker Scyther using an interpreter program. Figure 1 shows the architecture of the proposed framework, in which the CSPs will be represented in an abstract level and the implementation details are hidden in order to build the CSP model easily. Using this framework, the CSP model can be specified in C++ language using a set of cryptographic library functions. The library contains all the cryptographic primitives such as generation of keys, nonces values, encryption,

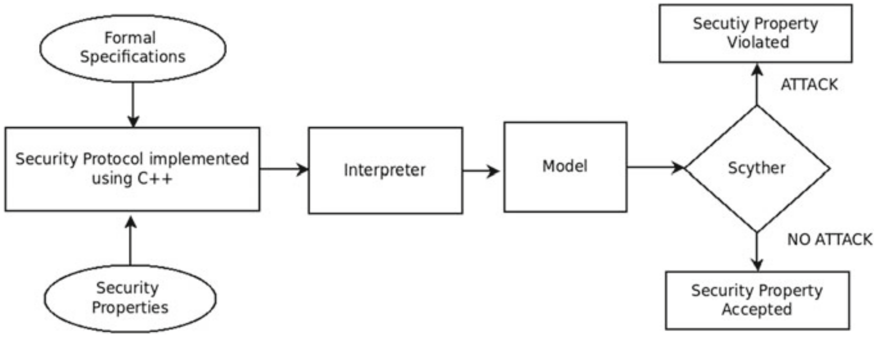

Formal Specifications
Security Protocol implemented using C++
Security Properties
Interpreter
Model
Scyther
ATTACK
Secutiy Property Violated
NO ATTACK
Security Property Accepted

Fig. 1 Framework architecture

decryption, hash functions, key exchange, send, and recv. The library is extendable for user requirements and the definitions for the library functions can be changed based on the user requirements.

To build a CSP model using the proposed framework, a protocol structure has to be followed as shown in Listing 1.1. The nesting of classes is used to bind the communicating agent behaviors in a single class. The outer class represents the protocol name along with the communicating role names, and the inner classes represent the communicating agents named as roles. The agents communicate with each other by sending and receiving messages. This takes place by calling the send and recv functions.

The role definition is the set of library function calls, which are bind in a single-member function. The role objects communicate by calling the single-member function, and thereby, all the communication takes place. Listing 1.2 gives an overview about the CSP specification using the proposed framework.

2.1 Scyther Model Checker as Verification Engine

Scyther is a formal analysis and verification tool, and it uses black-box analysis technique for verification of CSPs under the perfect cryptography assumption, which states that adversary learns nothing from the ciphertext unless he has the decryption key. The tool is basically used to identify the design errors of the security protocols. The protocols either proved correct or attacks will be detected.

Scyther uses Dolev-Yao threat model [11] as channel to model the adversary, on which the agents communicate, and the adversary has the upper hand and he can eavesdrop every message, perform reply attacks, can have knowledge about the cryptographic primitives, can remove sent messages and examine their contents, insert his own messages, or reroute or simply retransmit messages.

The key feature of Scyther is multiprotocol analysis, in which during the communication between the roles, the communicating agents use multiple CSPs in parallel, and then the attacker can gain the knowledge about the cryptographic primitives from one protocol run and can successfully perform an attack on the other. Scyther helps to perform formal analysis and verification of multi-protocols CSPs as well as a single CSP in isolation.

2.2 Dolev-Yao Channel

Dolev-Yao adversary model [11] is used to model the adversary, on which the agents (communicating parties either a sender or receiver) communicate, and the adversary has the upper hand and he can eavesdrop every message, perform reply attacks, can have knowledge about the cryptographic primitives, can remove sent messages and examine their contents, insert his own messages, or reroute or simply retransmit messages.

The Dolev-Yao adversary model will be running in parallel with the security protocol model. This model views the message space as a term algebra. Term derivation rules specify how agents can obtain new terms from old ones. Fix countable sets A, N, K, and V, denoting the set of agents, nonces, keys, and variables, respectively. The set of basic terms is B = A ∪ N ∪ K. For each A, B ∈ A, assume that sk(A), pk(A) and shk(A,B) are keys. Further, each k ∈ K has an inverse defined as follows: inv(pk(A)) = sk(A), inv(sk(A)) = pk(A), and inv(k) = k for the other keys.

The important features of the Dolev-Yao model are: 1. secrecy properties, 2. stateless parties, 3. concurrent execution, and 4. public-key cryptography and infrastructure. [11] Explains all these features in detail.

The intruder has access to all public information and can block and replay any terms sent by honest agents. The intruder is essentially the network itself—any terms sent by honest agents are received by the intruder and then forwarded onto the intended recipient (or not), and any terms received by honest agents are assumed to have come from the intruder. He can also send terms under masquerade, in the name of any agent (all agents' names are public). The intruder can send out any terms he can derive from the set of terms he has access to. An agent A might send out a term t for the intended recipient B, and the intruder might send a term t to B, pretending to be A, thereby effecting a forgery in A's name. A key component in checking for what terms the intruder can get access to is solving the derivability problem. The DY channel helps to model the channel which gives a strong adversary for verification of CSP.

2.3 The C++ to SPDL Interpreter

Formal verification cannot be done directly for a CSP implemented in a high-level language like C++, because the model checker cannot process C++ code. In order to overcome this language mismatch and to use a model checker for verification of CSP in C++ language, an interpreter is required which can convert C++ code to security protocol description language (SPDL) code. In the proposed framework, to specify a protocol in C++ a set of rules (syntax and semantics) must be followed. The protocol structure will be as follows.

Listing 17.1 Protocol structure

```
hashfunction g();
class protocol_protocolname_rolename1_rolename2       //Outer class
{
   class rolename1        //Inner class1
   {
     void function1()
     {

     }
   };

   class rolename2        //Inner class2
   {
      void function2()
      {

      }
   };
};
int main()
{
  protocol_protocolname_rolename1-rolename2::rolename1 obj1;
  protocol_protocolname_rolename1-rolename2::rolename2 obj2;
  obj1.function1();
  obj2.function2();
  return 0;

}
```

The communication between the agents takes place by sending and receiving messages, and this is specified in the protocol description by using send and receive functions. The syntax for send and recv functions is as follows:
$send(sequence - number, Sender - role - name, Receiver - role - name, data)$;
$recv(sequence - number, Sender - role - name, Receiver - role - name, data)$;
sequence-number—is a message sequence number, Sender-role-name- class name of Sender role, Receiver-role-name- class name of Responder role.

An example of message exchange is illustrated in Listing 1.2

Listing 17.2 Message exchange

```
hashfunction g();
class protocol_demo_role_Initiator_role_Responder
{
 class role_Initiator
 {
     fresh x;
     void fun1()
     {
       send(1,Initiator , Responder, encrypt(g(x),k(I,R)));
       claim( Initiator , Secret, x );
     }
 };
 class role_Responder
 {
    var x;
     void fun2()
     {
       recv(1,Initiator , Responder, decrypt(g(x),k(I,R)));
       claim( Responder, Secret, x );
     }
 };

};
```

The data can be sent with encryption or without encryption during the communication by using send function. If the data has to be sent securely, then encryption can be used, and this is done using an encryption function in the data field of send function, as shown in Listing 1.2. For the encryption function, the last parameter must be a key, either a public key, secret key, or a session key, and its syntax is as follows.

encrypt(parameters... , key);
decrypt(parameters... , key);

The encryption function encrypts all the parameters passed to it by using the key which is the last parameter in the encryption function, and it returns a ciphertext. In the proposed framework, the RSA encryption/decryption algorithm is used for public-key encryption and 128-bit AES algorithm is used for symmetric-key encryption.

Keys—pk(I) represents the long-term public key of role I, sk(I) represents the long-term secret key, and k(I,R) represents the long-term session key of role I and role R. If a public key or secret key is used to encrypt the data, then a public-key encryption function RSA is called. If a symmetric key is used to encrypt the data, then AES encryption library function is called. To use a cryptographic hash function, a hash function has to be declared as global functions as shown in Listing 1.2, in order to use it by the roles. In the proposed framework, MD5 hash algorithm is used to generate unique hash values. Finally, the security properties to be formally verified are represented using the claim functions as shown in Listing 1.2. The syntax for claim function is as follows:

claim(Role-name,Security-Property,data);

Role-name: The name of the role which is claiming the property, Security-Property: Property to be satisfied by the role for the data (the different security properties are discussed in the below paragraph), data: The data on which the property to be checked.

Security properties for CSPs are very important, and to verify a CSP, one should know the exact security properties to be satisfied by a CSP. The security properties are represented in claim functions, and its mathematical meaning is as follows.

Claim—Let γ be a claim role event of a protocol P. For a security property, it is required that some predicate Q on traces(P) × ClaimRunEv holds for each instance of γ in all traces of P. A property is true for the protocol if and only if: $\forall$ t $\in$ traces(P) $\forall$(inst, γ) $\in$ t : Q(t, (inst, γ)) where we use the notation e $\in$ t as an abbreviation for $\exists$ i: $t_i = $ e. There will be many security properties for a particular CSP to be proven correct, and the proposed framework focuses on secrecy and authentication.

Secrecy property states that the sent or received message must be secretly delivered to the honest agent without revealing the message to the intruder.

Authentication is identification of the right communication partner across the public network. There are three forms of authentication, namely 1. aliveness, 2. synchronization, and 3. message agreement.

Aliveness is checking of the existence of communication partner.

Synchronization verifies the sequence of messages exchanged between the agents, and thereby, the behaviors of the communicating agents are checked. In the presence of an active adversary, other behavior (not defined by the protocol description) might occur. For example, if there is no agent performing a certain role, this contradicts the protocol description. We consider any behavior that is not specified, to be unauthenticated. This leads to a natural definition of strong authentication, which is called synchronization.

Message Agreement requires that the contents of the received messages correspond to the sent messages, as specified by the protocol. As a result, after the execution of the protocol the contents of the variables will be exactly as specified by the protocol. After the execution of the protocol, the parties agree on the values of variables. Modex [12] is a tool to extract verification models from implemented C code to the SPIN model checker. The proposed interpreter works similar to Modex by interpreting each line of CSP C++ code, with help of regular expressions and pattern matching the C++ code is converted to SPDL code, Finally, the generated model is executed by the Scyther (Figs. 2 and 3).

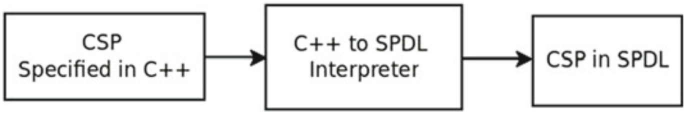


Fig. 2 Interpreter

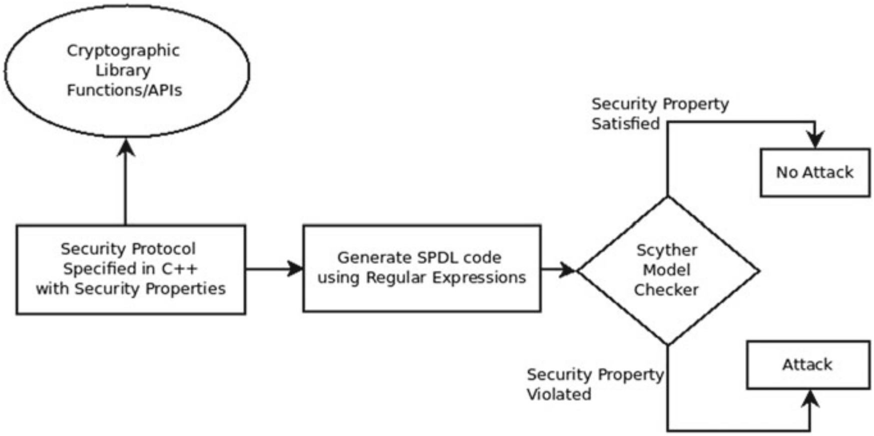

Cryptographic Library Functions/APIs
Security Protocol Specified in C++ with Security Properties
Generate SPDL code using Regular Expressions
Scyther Model Checker
Security Property Satisfied
No Attack
Security Property Violated
Attack

Fig. 3 Interpreter architecture

3 IKE-Internet Key Exchange Protocol

For formal verification of IKE protocol, the formal specifications are drawn from the RFC-2409 [9], and the security properties to be verified are also obtained from the same RFC. IKE is the protocol used to set up a security association (SA) in the IPsec protocol suite. IKE builds upon ISAKMP, Oakley, and Skeme. It uses X.509 certificates for authentication and uses either pre-shared or distributed keys using DNS and a Diffie–Hellman key exchange to set up a shared session secret from which cryptographic keys are derived. IKE is used in most of the communication devices to provide authentication and key exchange between the agents, particularly in establishing a VPN connection to a remote host by hiding the identities of the end parties. It uses two basic methods to establish an authenticated key exchange—Main Mode and Aggressive Mode. [9] Gives the details about these modes. The ISAKMP SA is the shared policy and keys used by the negotiating peers in IKE protocol to protect the communication. Oakley and Skeme each define a method to establish an authenticated key exchange. Oakley defines modes, and Skeme defines "phases." IKE uses public-key encryption for authentication and exchanges key between the entities with the help of Nonces. SA is a negotiation payload with one or more security proposals provided by the sender. An initiator can provide multiple proposals for security negotiation, but the responder must reply with only one SA. IKE uses hash functions to uniquely identify the messages, and prf() is the pseudo-random function—often a hash function—used to generate a deterministic output that appears pseudo-random. prfs are used both for key derivations and for authentication. Listing 1.3 shows the IKE communications. HDR is an IKE header whose exchange type is the mode, HDR* indicates payload encryption, SA is an SA negotiation payload with one or more proposals, and KE is the key exchange payload which contains the public information exchanged in a Diffie–Hellman exchange. The IKE Oakley version uses three modes—1. Main Mode, 2. Aggressive Mode, and 3. Quick Mode. [9] Explains these three modes in detail along with packets exchanged.

Listing 17.3 IKE message exchanges

```
Initiator                  Responder
-----------                ------------

HDR, SA              —>      HDR, SA
                     <—

HDR, KE, Ni          —>      HDR, KE, Nr
                     <—

HDR*, IDii, HASH_I   —>      HDR*, IDir, HASH_R
                     <—
```

4 Verification

A model checker is required to generate all possible behaviors of protocol under verification, it is called state space or search space, and it is stored in a tree structure. The verification of each security property is done by the model checker by searching through the state space for each security property represented as claim events. For search operation, the model checker uses a DFS or BFS algorithm. The claim events represent the safety property of verification, which states something bad is never going to happen. For a security property, if there is a trace pattern in the state space which violates the claim, then the corresponding attacks can be obtained with the help of model checker by traversing from the initial state to the state where the claim property was failed, the path or trace gives the execution or behavior of the system which violates particular property, and the trace includes the detail how the claim got failed and the possible attack can be derived from the attack graph. If there is no trace pattern which violates the security property claim, then it is proved safe. A trace is a partially ordered set of symbolic events, and a pattern represents a set of traces. The set of pattern events or Event is defined by the following BNF grammar:

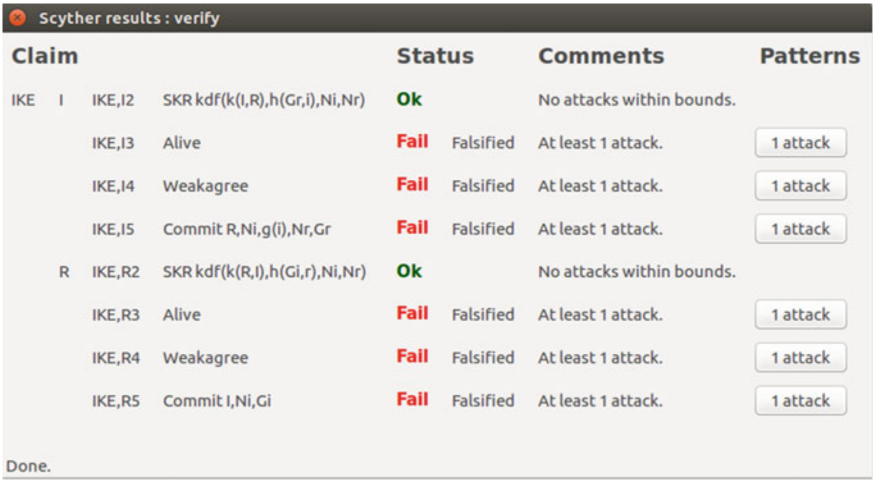
```
AdvEvent ::= decr ({| RunTerm |} RunTerm ) |
encr ({| RunTerm |} RunTerm ) |
app (Func(RunTerm* )) | init | know (RunTerm),
SendRecv ::= send | recv ,
RolePos ::= Role^#RID | Agent,
CommEvent ::= SendRecv Label (RolePos, RolePos,RunTerm)^RID ,
ClaimEvent ::= claim Label (RolePos, Claim [ , RunTerm]),
AgEvent ::= CommEvent | ClaimEvent,
PatternEvent ::= AdvEvent | AgEvent.
```

5 IKE Verification Results

The IKE version-1 in main mode is vulnerable to the brute force attack on keys exchanged between the agents. The agents share a set of (falsely) authenticated symmetric keys with the attacker, the attacker gets the symmetric keys, and the authentication security property gets violated. The proposed framework successfully identified this attack on IKE version-1, and it is shown in Fig. 4. IKE Oakley and Skeme version uses quick mode for security association negotiation and exchange of nonces to provide protection against replay attack. The nonces are used to generate fresh key material and prevent replay attacks from generating bogus security associations, with the help of nonces and Diffie–Hellman key exchange, and the protocol is proved safe in Skeme and Oakley. The results for Skeme and Oakley versions were shown in Figs. 5 and 6, respectively.

6 Conclusion and Future Work

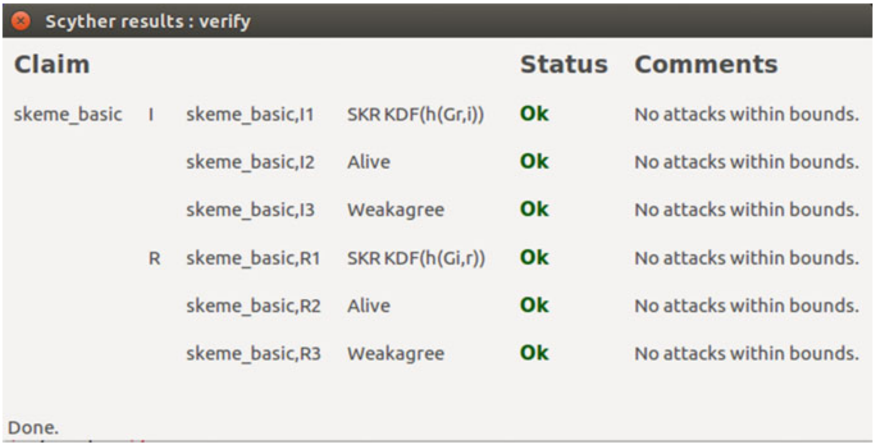
The formal verification of cryptographic security protocols has the potential to improve the reliability of the security protocols and can give mathematical proofs for CSP's correctness. Building the model for the security protocols and identifying the security properties is one of the key challenges in formal verification of CSP. By using the proposed framework, the CSP models and its security properties can be easily specified and verified for CSPs specified in C++. The IKE security protocol is formally verified using the proposed framework, and the results are obtained



Claim				Status		Comments	Patterns
IKE	I	IKE,I2	SKR kdf(k(I,R),h(Gr,i),Ni,Nr)	Ok		No attacks within bounds.	
		IKE,I3	Alive	Fail	Falsified	At least 1 attack.	1 attack
		IKE,I4	Weakagree	Fail	Falsified	At least 1 attack.	1 attack
		IKE,I5	Commit R,Ni,g(i),Nr,Gr	Fail	Falsified	At least 1 attack.	1 attack
	R	IKE,R2	SKR kdf(k(R,I),h(Gi,r),Ni,Nr)	Ok		No attacks within bounds.	
		IKE,R3	Alive	Fail	Falsified	At least 1 attack.	1 attack
		IKE,R4	Weakagree	Fail	Falsified	At least 1 attack.	1 attack
		IKE,R5	Commit I,Ni,Gi	Fail	Falsified	At least 1 attack.	1 attack

Done.

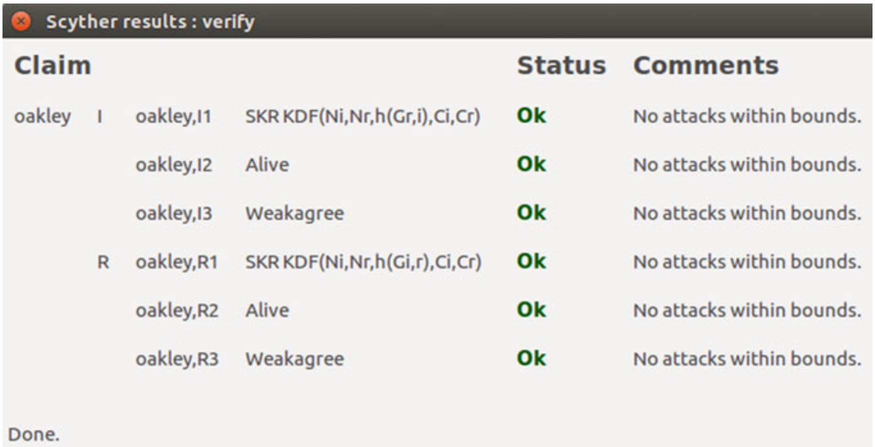
Fig. 4 IKE version-1 verification result



Claim				Status	Comments
skeme_basic	I	skeme_basic,I1	SKR KDF(h(Gr,i))	Ok	No attacks within bounds.
		skeme_basic,I2	Alive	Ok	No attacks within bounds.
		skeme_basic,I3	Weakagree	Ok	No attacks within bounds.
	R	skeme_basic,R1	SKR KDF(h(Gi,r))	Ok	No attacks within bounds.
		skeme_basic,R2	Alive	Ok	No attacks within bounds.
		skeme_basic,R3	Weakagree	Ok	No attacks within bounds.

Done.

Fig. 5 IKE-Skeme version verification result



Claim				Status	Comments
oakley	I	oakley,I1	SKR KDF(Ni,Nr,h(Gr,i),Ci,Cr)	Ok	No attacks within bounds.
		oakley,I2	Alive	Ok	No attacks within bounds.
		oakley,I3	Weakagree	Ok	No attacks within bounds.
	R	oakley,R1	SKR KDF(Ni,Nr,h(Gi,r),Ci,Cr)	Ok	No attacks within bounds.
		oakley,R2	Alive	Ok	No attacks within bounds.
		oakley,R3	Weakagree	Ok	No attacks within bounds.

Done.

Fig. 6 IKE Oakley version verification result

as shown in Figs. 4, 5, and 6. The framework shows how a model checker can be used to verify CSP code specified using a high-level programming language C++. Finally using proposed framework, we can achieve high reliability of the CSPs. The framework can be further extended to additional security property requirements, and the same methodology can be incorporated to specify CSPs in other high-level programming languages like Java and Python, and the new interpreters are required to interpret CSPs specified in high-level languages like Java or Python with different model checkers.

References

1. Needham RM, Schroeder MD (1978) Using encryption for authentication in large networks of computers. Commun ACM 21(12):993–999. https://doi.org/10.1145/359657.359659, http://doi.acm.org/10.1145/359657.359659
2. Lowe G (1996) Breaking and fixing the Needham-Schroeder public-key protocol using FDR. In: Margaria T, Steffen B (eds) Tools and algorithms for the construction and analysis of systems. Springer, Berlin, pp 147–166
3. Gibson-Robinson T, Armstrong P, Boulgakov A, Roscoe AW (2014) FDR3—a modern refinement checker for CSP. In: Ábrahám E, Havelund K (eds) Tools and algorithms for the construction and analysis of systems. Springer, Berlin, pp 187–201
4. Cremers C, Mauw S, de Vink E (2003) Formal methods for security protocols: three examples of the black-box approach. NVTI Newsl 7:21–32. Newsletter of the Dutch Association for Theoretical Computing Scientists
5. Roscoe AW (1994) Model-checking CSP. In: A classical mind. Prentice Hall International (UK) Ltd., Hertfordshire, UK, pp 353–378. http://dl.acm.org/citation.cfm?id=197600.197628
6. Herzog J (2005) A computational interpretation of Dolev-Yao adversaries. Theor Comput Sci 340(1):57–81
7. Clarke EM, Grumberg O (1987) Avoiding the state explosion problem in temporal logic model checking. In: Proceedings of the sixth annual ACM symposium on principles of distributed computing. ACM, pp 294–303
8. Cremers C, Mauw S (2012) Operational semantics and verification of security protocols. Springer
9. Carrel D, Harkins D (1998) The Internet Key Exchange (IKE). RFC 2409. https://doi.org/10.17487/RFC2409, https://rfc-editor.org/rfc/rfc2409.txt
10. Krawczyk H (1996) Skeme: a versatile secure key exchange mechanism for internet. In: Proceedings of the 1996 symposium on network and distributed system security (SNDSS '96). SNDSS '96, IEEE Computer Society, Washington, DC, USA, p 114.http://dl.acm.org/citation.cfm?id=525423.830460
11. Herzog J (2005) A computational interpretation of Dolev-Yao adversaries. Theor Comput Sci 340(1):57–81. https://doi.org/10.1016/j.tcs.2005.03.003, http://www.sciencedirect.com/science/article/pii/S0304397505001179. Theoretical Foundations of Security Analysis and Design II
12. Holzmann G (2003) The spin model checker: primer and reference manual, 1st edn. Addison-Wesley Professional

Locality—Aware Scheduling for Containers in Cloud Computing

G. Charles Babu, A. Sai Hanuman, J. Sasi Kiran and B. Sankara Babu

Abstract The cutting edge scheduler of containerized cloud administrations considers load balance as the main rule, numerous other imperative properties, including application execution, are ignored. In the period of Big Data, applications advance to be progressively more information escalated and subsequently performed inadequately when conveyed on containerized cloud administrations. With that in mind, this paper means to enhance the present cloud administration by considering application execution for the cutting edge compartments. The more explicitly, in this work we fabricate and break down another model that regards both burden equalization and application execution. Dissimilar to earlier examinations, our model edited compositions the predicament between burden equalization and application execution into brought together steaming issue and after that utilizes a factual technique to effectively settle it. The most difficult part is that some sub-issues are amazingly unpredictable (for instance, NP-hard) and heuristic calculations must be formulated. To wrap things up, we actualize a framework model of the proposed planning procedure for containerized cloud administrations. Exploratory outcomes demonstrate that our framework can fundamentally support application execution white safeguarding generally high burden balance.

Keywords Cloud computing · Load balance · Containerized cloud administration · Safeguarding · NP-hard

G. Charles Babu (✉)
Department of CSE, Malla Reddy Engineering College (Autonomous), Secunderabad, Telangana, India
e-mail: Charlesbabu26@gmail.com

A. Sai Hanuman · B. Sankara Babu
Department of CSE, Gokaraju Rangaraju Institute of Engineering & Technology (Autonomous), Bachupally, Telangana, India

J. Sasi Kiran
Department of CSE, Farah Institute of Technology, Chevella, Telangana, India

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_18

1 Introduction

The previous couple of years have seen a developing number of versatile and sensor applications that depend on Cloud support. The job of the Cloud is to enable these asset constrained gadgets to offload and execute a portion of their register serious undertakings in the Cloud for vitality sparing and additionally quicker preparing. Notwithstanding, such offloading to the Cloud may result in high system overhead which isn't reasonable for some portable/sensor applications that require low idleness. In this paper, we propose a territory mindful burden-sharing method that permits edge assets to share their remaining task at hand so as to keep up the low inertness necessity of Mobile-Cloud applications. In particular, we examine how to figure out which edge hubs ought to be utilized to impart the remaining task at hand to and the amount of the outstanding burden ought to be shared to every hub. Our trials demonstrate that our region mindful burden-sharing procedure can keep up low normal start to finish idleness of portable applications with low inertness variety while accomplishing great use of assets within the sight of a dynamic remaining task at hand.

Objectives

- To examination prescient investigation of territory mindful storage tier information obstructs over Hadoop;
- To plan area mindful burden part taking in versatile distributed computing;
- To structure toward territory mindful planning for containerized cloud administrations;
- To examination territory mindful booking for holders in distributed computing.

2 Literature Review

2.1 Structuring Your Paper

LaValle et al. [1] the term “Enormous Data investigation's alludes to an extensive scale answer for overseeing mammoth datasets in a parallel domain. Hadoop is a biological community that forms vast datasets in appropriated processing situation. The biological community is additionally classified into four sub-ventures, for example, HDFS, MapReduce, YARN, and Hadoop Commons. The Hadoop Distributed File System (HDFS) is a spine of biological system, which helps putting away and handling substantial datasets. As of late, HDFS is moved up to heterogeneous capacity level condition that adapts to information square handling over various capacity gadgets for example Plate, SSD, and RAM. The square position strategy dispatches information squares to the gadgets without figuring I/O exchange parameters and territory points of view. In addition, HDFS chooses arbitrary Datanodes that could be situated into the following rack having longer way than neighborhood rack. This expands the information square handling dormancy and results in a colossal postponement for reproduction the board in heterogeneous capacity level. To determine this issue, we propose a prescient examination that fabricate a territory mindful capacity level hub outline and anticipate the most adjacent accessible capacity level for square occupation preparing. The test assessment delineates that the proposed methodology diminishes information square exchange time overhead, copy exchange time overhead and diminishes hub ways to an ideal availability over the bunch.

Cloudera [2] in this paper, we propose a system for security safeguarding redistributed medication revelation in the cloud, which we allude to as POD. In particular, POD is intended to enable the cloud to safely utilize different medication recipe suppliers" medication equations to prepare Support Vector Machine (SVM) given by the logical model supplier. In our methodology, we configuration secure calculation conventions to enable the cloud server to perform generally utilized number and division calculations. To safely prepare the SVM, we plan a safe SVM parameter choice convention to choose two SVM parameters and develop a safe consecutive negligible enhancement convention to secretly invigorate both chose SVM parameters. The prepared SVM classifier can be utilized to decide if a medication substance compound is dynamic or not in a security safeguarding way. In conclusion, we demonstrate that the proposed POD accomplishes the objective of SVM preparing and concoction compound order without protection spillage to unapproved parties, just as exhibiting its utility and productivity utilizing three certifiable medication datasets.

Kala Karun and Chitharanjan [3] cloud-helped Internet of Things (IoT) gives a promising answer for information blasting issues for the capacity imperatives of individual items. Nonetheless, with the influence of cloud, IoT faces new security challenges for information commonality between two gatherings, which is presented without precedent for this paper and not as of now tended to by customary methodologies. We research a protected cloud-helped IoT information overseeing technique to keep information classification when gathering, putting away, and getting to IoT information with the help of a cloud with the thought of clients increase. The proposed framework novelly applies an intermediary re-encryption plot, which was proposed in \cite{XJW15}. Henceforth, a protected IoT under our proposed strategy could oppose most assaults from the two insiders and untouchables of IoT to break information classification, and in the interim with consistent correspondence cost for re-encryption against gradual size of IoT. We further demonstrate the technique is handy by numerical outcomes.

Abbas et al. [4] Information spillage is the coincidental revelation of delicate data through relationship of records from a few databases/accumulations of a cloud information distribution center. Vindictive insiders represent a genuine danger to cloud information security and this legitimizes the emphasis on data spillage because of maverick representatives or to pariahs utilizing the qualifications of authentic workers. The exchange in this paper is confined to NoSQL databases with an adaptable construction. Information encryption can lessen data spillage, however, it is illogical to scramble huge databases and additionally all fields of database records. Encryption restricts the tasks that can be carried on the information in a database. It is along these lines, basic to recognize touchy reports in an information stockroom and focus on endeavors to secure them. The limit of a spillage divert presented in this work evaluates the instinctively evident intends to trigger cautions when an insider aggressor utilizes unreasonable PC assets to correspond data in various databases. The Sensitivity Analysis dependent on Data Sampling (SADS) presented in this paper adjusts the exchange offs between higher effectiveness in recognizing the dangers presented by data spillage and the exactness of the outcomes gotten by testing vast accumulations of reports. The paper gives an account of trials surveying the viability of SADS and the utilization of specific disinformation to confine data spillage. Cloud administrations distinguishing touchy records and decreasing the danger of data spillage are additionally talked about.

Tsuruoka [5] with the appearance of distributed computing, an ever-increasing number of individuals will in general re-appropriate their information to the cloud. As a basic information use, secure watchword look over scrambled cloud information has pulled in light of a legitimate concern for some specialists as of late. Be that as it may, the majority of existing looks into depend on a perfect suspicion that the cloud server is "interested however genuine", where the list items are not checked. In this paper, we think about an all the more difficult model, where the cloud server would most likely carry on unscrupulously. In view of this model, we investigate the issue of result confirmation for the protected positioned catchphrase seek. Not the same as past information confirmation plans, we propose a novel obstacle based plan. With our cautiously formulated check information, the cloud server can't know which information proprietors, or what number of information proprietors trade stay information which will be utilized for confirming the cloud server's rowdiness. With our methodically structured confirmation development, the cloud server can't know which information proprietors' information are installed in the check information support, or what number of information proprietors' confirmation information are really utilized for confirmation. All the cloud server knows is that when he carries on untrustworthily, he would be found with a high likelihood, and rebuffed truly once found. Besides, we propose to enhance the estimation of parameters utilized in the development of the mystery confirmation information cradle.

3 Methodology

The predictive analysis consists of two phases, i.e., (i) Storage-tier summary container and (ii) Predict the most nearby Datanode.

The storage-tier summary container collects all the Datanode and storage media information, i.e., computing capacity and storage-tier devices with volume statistics. Moreover, the media predictor performs training sessions over the dataset and predicts the most nearby Datanode with available storage-tier media as seen from Fig. 1.

Fig. 1 Storage tier predictive analysis over HDFS cluster

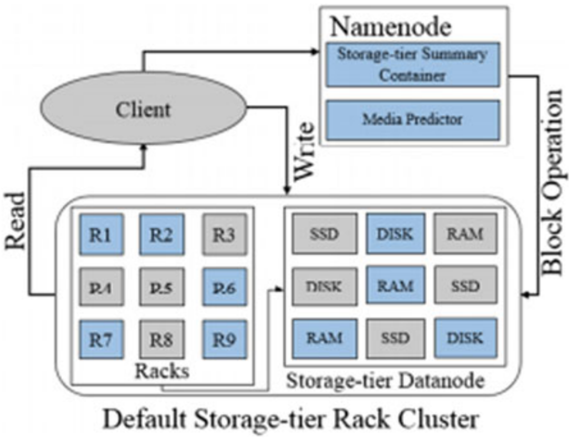
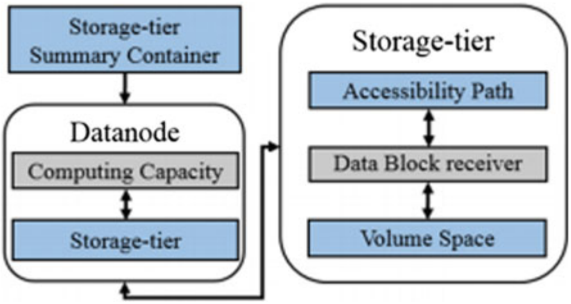


Fig. 2 Storage-tier summary architecture



Storage-tier Summary Container

The summary container consists of Datanode information, i.e., CPU, storage media, accessibility time, 1 MB data block receiving time and volume sizes of each storage (Fig. 2).

4 Results

Environment

The biological community comprises of Intel Xeon processor with 8 CPUs, 32 GB memory, and capacity gadgets, for example, 1 TB Hard plate drive and 128 GB Samsung SSD. Notwithstanding that, we use Intel center i5 with 4 Core, 16 GB memory and capacity gadgets for example 1 TB Hard circle drive and 128 GB Samsung SSD. We introduce 5 virtual machines having virtual box 5.0.16 as observed from Table.

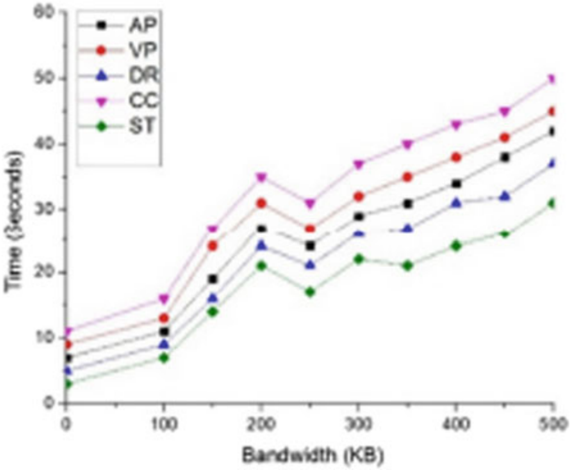


Fig. 3 Storage-tier summary container message collector

The exploratory dataset comprises of:

(i) 250 arbitrary SSD word check information squares of 64 MB (40 GB size),
(ii) 250 irregular DISK word tally information squares (40 GB size) and
(iii) 250 arbitrary RAM word check information squares (40 GB size).

Storage-tier Summary Collector

The collector fetches event traces of computing capacity, storage-tier I/O, Accessibility Path timestamp, Datablock receiver timestamp and Volume Space statistics over container. The message length varies between $0.5 \leq \text{size} \geq 5$ KB and consumes a resource between $0.2 \leq \text{Bandwidth} \geq 500$ KB/s. The summary container stores 2.7 GB of log information over 120 GB data blocks as observed from Fig. 3.

After generating container messages, we perform prediction simulations over three "250" random data blocks. In the first hour of simulation, we observe that predictor detects pattern of "109" SSD data blocks, "78" DISK data blocks and "63" RAM data blocks. In the second hour of simulation, we use "500" random data blocks and analyze that predictor observes pattern of "211" SSD data blocks, "192" DISK data blocks and "97" RAM data blocks. In the third hour of simulation, we evaluate "750" random data blocks and evaluate that predictor observes pattern of "322" SSD data block, "219" DISK data blocks and "109" RAM data blocks as observed from Fig. 4.

The media predictor depicts locality-aware nearby Datanode statistics with available functional media. The predictor lists processing timestamp, accessibility timestamp, and completion timestamp of data blocks over respective storage media. As a result, we calculate locality-aware path and observes that proposed processing, node, and storage-tier approaches are 39.1, 54.7, and 22.9% efficient than default data block processing. This reduces storage-tier latency, node latency, and overall processing latency as observed from Fig. 5.

Fig. 4 Storage-tier media block job prediction

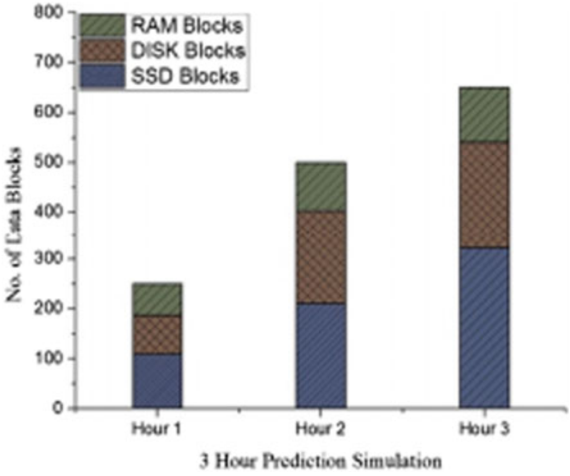
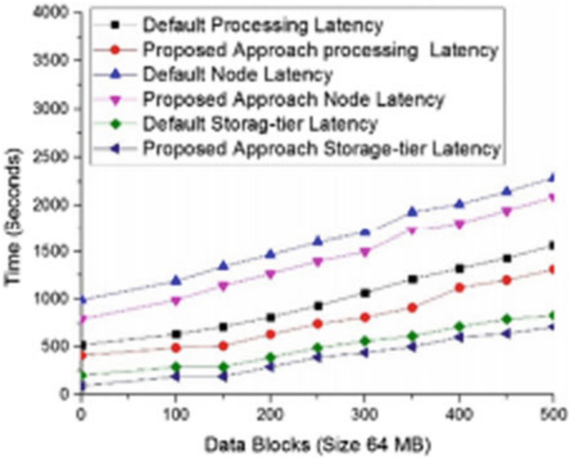


Fig. 5 Latency optimization over HDFS cluster



5 Conclusion

In this paper, we think about the issue of burden-sharing to deal with runtime elements in a Mobile-Edge Computing (MEC) condition. Our inspiration depends on the dynamic property of the outstanding burden in MEC alongside the low idleness prerequisite for a considerable lot of the present portable/IoT applications. The Edge Cloud stage that has been proposed to give computational loading backing to versatile applications faces extra difficulties in taking care of outstanding burden elements since the hubs in Edge Clouds are ordinarily associated by WAN with high system inertness and constrained transmission capacity. We propose a region mindful burden-sharing method that permits edge hubs to share their outstanding task at hand to different hubs to meet the low dormancy prerequisite of the versatile applications on account of remaining task at hand increments. Our heap sharing system enables hubs to

(1) Intelligently decides if to share their outstanding burden to different hubs,
(2) Selectively picks which hubs the outstanding burden ought to be imparted to, and
(3) Determines the amount of the remaining burden ought to be shared. Our trial results dependent on a genuine Twitter's follow demonstrate that our territory mindful burden-sharing strategy can keep the general dormancy of versatile applications near the applications' ideal objectives just as better use assets even on account of dynamic outstanding task at hand.

Headings should be capitalized (i.e., nouns, verbs, and all other words except articles, prepositions, and conjunctions should be set with an initial capital) and should, with the exception of the title, be aligned to the left. Only the first two levels of section headings should be numbered. Kindly refrain from using "0" when numbering your section headings.

References

1. LaValle S et al (2011) Big data, analytics and the path from insights to value. MIT Sloan Manag Rev 52.2:21
2. Cloudera (2016) The modern platform for data management and analytics, Cloudera [Online]. Available http://www.cloudera.com/. Accessed 13 Mar 2017
3. Kala Karun A, Chitharanjan K (2013) A review on Hadoop—HDFS infrastructure extensions. In: 2013 IEEE conference on information and Communication Technologies
4. Abbas A, Wu Z, Siddiqui IF, Lee SUJ (2016) An approach for optimized feature selection in software product lines using union-find and genetic algorithms. Indian J Sci Technol 9(17)
5. Tsuruoka Y (2016) Cloud computing—current status and future directions. J Inf Process 24(2):183–194
6. Welcome to Apache™ Hadoop®! (2014) [Online]. Available http://hadoop.apache.org/. Accessed 13 Mar 2017
7. M. Technologies, "Featured customers" (2016) [Online]. Available https://www.mapr.com/. Accessed 13 Mar 2017
8. Apache Hadoop 2.7.2—Apache Hadoop YARN (2016) [Online]. Available https://hadoop.apache.org/docs/r2.7.2/hadoopyarn/hadoop-yarn-site/YARN.html. Accessed 13 Mar 2017
9. Apache Hadoop 2.7.2—MapReduce Tutorial (2016) [Online]. Available https://hadoop.apache.org/docs/stable/hadoopmapreduce-client/hadoop-mapreduce-clientcore/MapReduceTutorial.html. Accessed 13 Mar 2017
10. Apache Hadoop 2.7.2—HDFS users guide (2016) [Online]. Available https://hadoop.apache.org/docs/stable/hadoopprojectdist/hadoophdfs/HdfsUserGuide.html. Accessed 13 Mar 2017
11. Abbas A, Siddiqui IF, Lee SUJ (2016) Multi-objective optimization of feature model in software product line: perspectives and challenges. Indian J Sci Technol 9(45)

12. Abbas A, Siddiqui IF, Lee SUJ (2017) Contextual variability management of IoT application with xml-based feature modelling. J Theor Appl Inf Technol 95(6)
13. Rodríguez-Quintana C, Díaz AF, Ortega J, Palacios RH, Ortiz A (2016) A new scalable approach for distributed metadata in HPC. In Algorithms and architectures for parallel processing. Springer Nature, pp 106–117
14. White T (2012) Hadoop: the definitive guide. O'Reilly Media, Inc

TorBot: Open Source Intelligence Tool for Dark Web

P. S. Narayanan, R. Ani and Akeem T. L. King

Abstract The dark web has turned into a dominant source of illegal activities. With several volunteered networks, it is becoming more difficult to track down these services. Open source intelligence (OSINT) is a technique used to gather intelligence on targets by harvesting publicly available data. Performing OSINT on the Tor network makes it a challenge for both researchers and developers because of the complexity and anonymity of the network. This paper presents a tool which shows OSINT in the dark web. With the use of this tool, researchers and Law Enforcement Agencies can automate their task of crawling and identifying different services in the Tor network. This tool has several features which can help extract different intelligence.

Keywords Dark web · Osint · Security · Tor

1 Introduction

We know that the Internet is an ocean of data that is scattered across the Internet. Open source intelligence (OSINT) is a technique used to analyze this scattered data hastily by identifying meaningful relationships among data points to get meaningful information [1].

Data becomes valuable when it disseminates information, and unfortunately, all data is not self-descriptive and requires context to reveal information. The Internet has been a major source of this type of data in large quantities, and we can generate valuable information if we can provide context to it. OSINT refers to the analysis

P. S. Narayanan (✉) · R. Ani
Department of Computer Science and Applications, Amrita Vishwa Vidyapeetham, Amritapuri, Kollam, India
e-mail: thepsnarayanan@gmail.com

R. Ani
e-mail: anir@am.amrita.edu

A. T. L. King
ISPA Technology, Tampa, FL, USA
e-mail: akeemtlking@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_19

of unclassified information that is spread across the Internet [2]. OSINT plays an important role in criminal investigations. There are many OSINT tools available to gather intelligence, for example,

- Maltego, an inbuilt tool in Kali Linux, helps to perform a significant reconnaissance against targets.
- Recon-Ng, which is also included in the Kali Linux distribution, has various inbuilt modules.
- Shodan, a search engine for hackers, gives a huge footprint of IoT devices which are connected to the Internet.
- Reaper [3], a credential and threat intelligence automation tool.

A smaller portion of the Internet exists which is surreptitious from the normal web traffic. This part can be accessed only using special software like Tor, I2P [4], etc. This hidden part is known as the dark web. It comprises numerous unindexed web pages. This is so because the traditional web crawlers and spiders are not able to access this part of the Internet [5, 6]. The dark web has been entertaining criminals for performing many illicit activities and deploying illegal services. Identifying such actions is not a simple procedure, especially doing so with the dark web. Information gathering is one way to identify the relations among dark web contents. Law Enforcement Agencies and researchers rely on the manual investigation, which is time-consuming and thus inefficient [7, 8].

Similarly, there exists a larger portion of the Internet known as the deep web. Deep web may be defined as the part of the network in which the contents are not indexed by standard search engines. It is a reference to any web page that cannot be accessed using a conventional search engine, such data remains obscured from the users.

The Tor network ensures a better privacy and security for Internet users by creating a series of virtual tunnels for communication rather than making a direct connection. Tor is a tool which secures the users from surveillance otherwise identified as traffic analysis by distributing the requests and responses over several places on the Internet. Tor allows the data to be incorrigible and does not lose its integrity. Tor is mainly used by individuals, journalists, whistleblowers, etc. [9, 10].

TorBot is an open source intelligence tool developed in Python which primarily focuses for the dark web content. It simplifies the process of identification and analysis of onion services and gathers intelligence about dark web service. Manual intelligence collection and classification in the dark web is not efficient. To speed up the process and to help researchers, we developed TorBot. Extensive use of dark web for communication of terrorism-related information makes it a challenge for Law Enforcement Agencies. TorBot should be able to fetch data and later using the data on different machine learning algorithms, and it should be able to identify such illegal activities that are happening in this encrypted network. Therefore, this tool will be able to ease the task of finding such activities by an intelligence group or researchers, thus making this the main objective of TorBot.

2 Literature Review

2.1 Challenges

Brian Nafziger has presented a study in which he discussed the challenges when collecting open source intelligence data from the Darknet. This includes using a specialized set, refining, and evaluation tools. He proposed an automation tool set that helps us to scan across the Darknet connecting, gathering, refining, and analyzing the data. The tool is created on behalf of anonymity system, the collection of intelligence using a web crawler system, the refining using a big data system, and the evaluation by implementing an NLP technique and a relational linking system [11].

2.2 Accessing Dark Pages

Another research by Ahmed T. Zulkarnine et al. proposed an enhanced Dark Crawler. It was able to access the Tor network while accessing the surface Internet. It searches services within the Tor network based on a set of pre-defined keywords, then stores this unprocessed data in a database. Some challenges they have faced are a high volume of data, low-quality content, and unintentional DOS attack when crawling. They have also discussed and implemented solutions for these problems. For this, they have used a dataset containing over 10,000 distinct Tor domains and 50,000 Tor web pages. After that, they have constructed a directed graph using Tor web pages it got where each web page is treated as a vertex and the hyper-links as edges [8].

2.3 Analysis of Tor Hidden Services

In a study conducted by Iskander Sanchez-Rola et al., the design and privacy analysis of Tor hidden service is measured using a dedicated analysis platform which they applied it to crawl and analyze millions of Tor URLs. According to their study, Tor services are organized in an infrequent but highly connected graph. They have also discussed about the connection that exists between Tor services and the surface web. Their design of dark web crawler was implemented on top of the headless browser PhantomJS. For privacy, they have implemented a number of advanced hiding techniques. Using their tool, they randomly extracted a sample of the initial seed domains and evaluated the page loading time [12].

2.4 Open Source Intelligence

The research conducted by Blake Butler et al. proposed a tool named REAPER for automated threat intelligence and OSINT. Their primary aim was to find the distribution and source of where a credential dump first appeared while also maintaining an in-depth study into the intelligence data that can be achieved by examining the criminal activities associated with it. They measured the effectiveness of the tool using 30 unique credential dumps which were found from different sources across the surface web and dark web. Then, the focus was given primarily to the identification of an earlier release, identification of 'Dark' domains associated with the dump, identification of additional dumps, and finally, the number of credentials identified per-domain [3].

3 Design and Methodology

The TorBot includes several modules, and the core functionality is its crawler and the visualizer module. This section provides a closer look into our tool design and features.

3.1 Crawler

TorBot's crawler is designed such that it crawls the dark pages fast and recursively through a breadth-first exploration. It further identifies other links, e-mails along with metadata, and text. It utilizes the multi-threading feature for improved performance. It has a sub-module called randomizer which randomizes the header information and IP address after every '*n*' requests. This helps in maintaining anonymity. Moreover, this helps prevent IP blocking from certain Web sites which are protected by web application firewalls (Fig. 1).

The crawler by default checks for '*onion*' domains only. But, this can be overridden by specifying the additional domains using TorBot's '-*e*' flag. Before adding a link to the queue, it checks whether the site is live or not. This is simply by sending a request to the site address and analyzing the response.

```
URLs = input(url)
while (URLs is not empty) do
    dequeue url
    request page
    parse for Links
    for (link in Links) do
        if link is live && link is not visited then
            add link to URLs
    store page content
```

Fig. 1 Pseudo code for crawling the page

3.2 Intelligence Extractor

A typical OSINT tool comprises several modules which makes it a perfect tool. One such module is the intelligence collection module. Just as it sounds, it collects Intel from the parsed web page. This Intel can be later used for classification or to find some key information. The TorBot's Intel module collects as much information as possible. It collects scripts, robots, files, e-mails, fuzz URLs and checks for basic web vulnerabilities [13–15]. The output is stored for future reference.

- Robots.txt: This function checks for Robots.txt file. This file is created by webmasters to instruct web robots how to crawl their Web site. It is included in the robots exclusion protocol (REP). The basic structure of Robots.txt is:

  User-agent: [user-agent name]

  Disallow: [URL string not to be crawled]

  This function checks for URLs in the robots.txt file, and then, the new URLs (if present) are added to the queue.
- E-mails: The Intel module searches for e-mails in the page using regex. This e-mail can be used as Intel information. E-mails often help to map the link with surface web. Therefore, e-mail plays a vital role in open source intelligence.
- Files: Files present in web pages are fetched using this feature. This includes images, PDFs, etc.
- Bitcoin Hashes: Bitcoin is unregulated peer-to-peer virtual currency [16]. Bitcoin hashes are more widely present in the dark web than in the surface web.

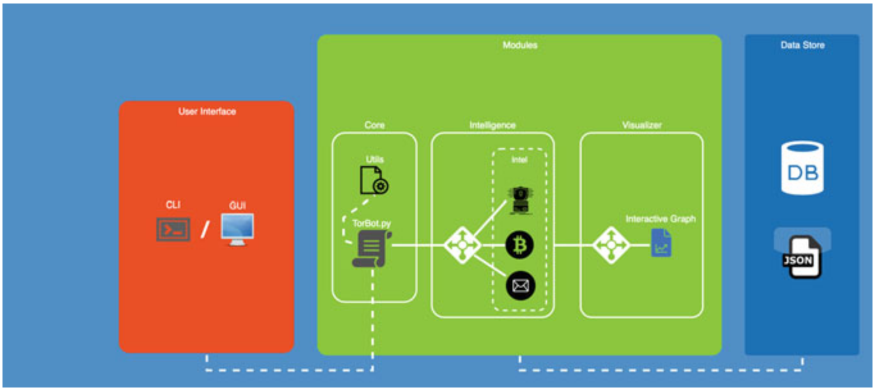


Fig. 2 Architecture diagram of TorBot

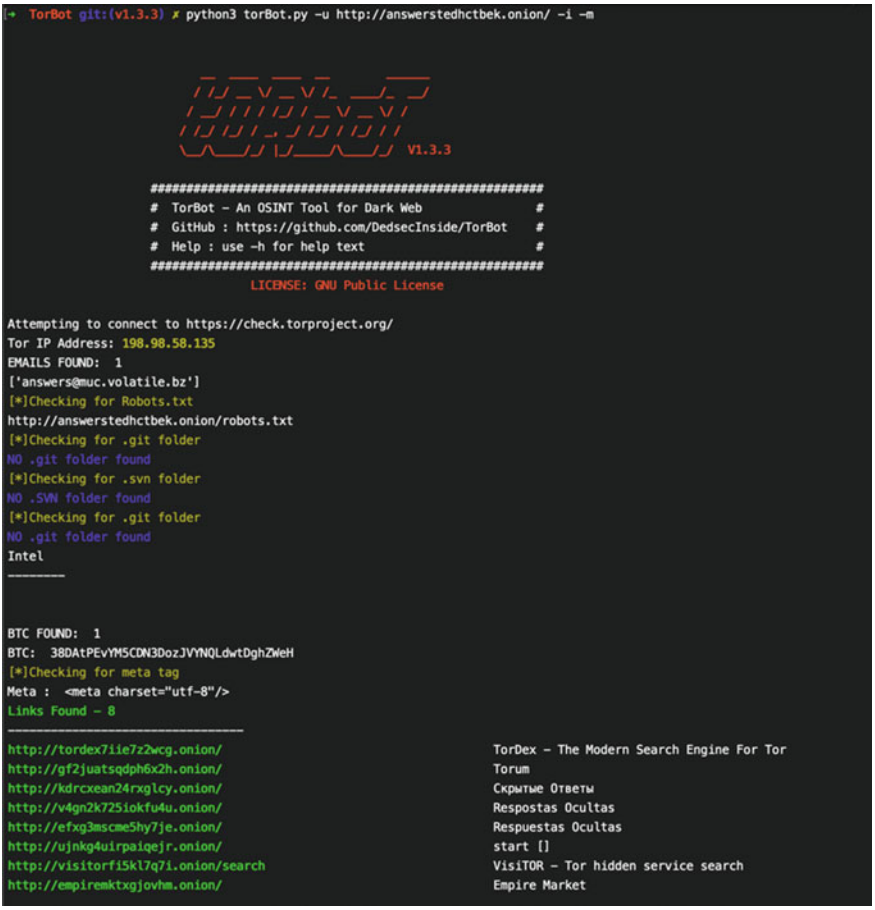
3.3 Visualizer

The data harvested by TorBot is presented visually using this module. It has the ability to examine the relationship of links using a tree with the given link as the root node. Currently, it is capable of checking the length of the tree if a link exists within the tree. The visualizer module creates an interactive tree graph and displays it to the user (Fig. 2).

The generated tree can be saved as PNG, SVG, or PDF.

4 Results and Discussion

The result presented here is the final output of extracting information from a given random Tor service. After successful execution, we can see that it extracted an e-mail address associated with the page along with URLs and a Bitcoin address as shown in Fig. 3. The e-mail address extracted is an address associated with a surface web. Therefore, this hidden service can be mapped with the corresponding surface web. The visualizer was able to produce a tree graph of the links after further crawling the dark page as shown in Fig. 4. The crawler was able to find over 200 links which were directly or indirectly related to the given Tor service. After analyzing, the Bitcoin hash extracted from the service, and we found a Silkroad transaction, which was one of the best-known drug markets in the dark web.



```
[→ TorBot git:(v1.3.3) ✗ python3 torBot.py -u http://answerstedhctbek.onion/ -i -m


                __  ____  ____  __        ______
               / /_/ __ \/ __ \/ /_  ____/_  __/
              / __/ / / / /_/ / __ \/ __ \/ /
             / /_/ /_/ / _, _/ /_/ / /_/ / /
             \__/\____/_/ |_/_.___/\____/_/  V1.3.3

          #####################################################
          #  TorBot - An OSINT Tool for Dark Web              #
          #  GitHub : https://github.com/DedsecInside/TorBot  #
          #  Help : use -h for help text                      #
          #####################################################
                        LICENSE: GNU Public License

Attempting to connect to https://check.torproject.org/
Tor IP Address: 198.98.58.135
EMAILS FOUND:  1
['answers@muc.volatile.bz']
[*]Checking for Robots.txt
http://answerstedhctbek.onion/robots.txt
[*]Checking for .git folder
NO .git folder found
[*]Checking for .svn folder
NO .SVN folder found
[*]Checking for .git folder
NO .git folder found
Intel
--------


BTC FOUND:  1
BTC:  38DAtPEvYM5CDN3DozJVYNQLdwtDghZWeH
[*]Checking for meta tag
Meta :  <meta charset="utf-8"/>
Links Found - 8
--------------------------------
http://tordex7iie7z2wcg.onion/                         TorDex - The Modern Search Engine For Tor
http://gf2juatsqdph6x2h.onion/                         Torum
http://kdrcxean24rxglcy.onion/                         Скрытые Ответы
http://v4gn2k725iokfu4u.onion/                         Respostas Ocultas
http://efxg3mscme5hy7je.onion/                         Respuestas Ocultas
http://ujnkg4uirpaiqejr.onion/                         start []
http://visitorfi5kl7q7i.onion/search                   VisiTOR - Tor hidden service search
http://empiremktxgjovhm.onion/                         Empire Market
```

Fig. 3 TorBot intelligence report

5 Conclusion and Future Work

In this paper, we introduced a tool that can be used for crawling and extracting deep web contents. Furthermore, it provides a visual module which represents the data in tree form. GUI for TorBot is currently in development, and users can expect a simple beginner-friendly GUI for easy interaction.

Currently, TorBot does not have a machine learning model to classify the services and images. A good ML model could help in classification of services as well as images [17–21]. Other specific directions for future work are to integrate social media with TorBot which could help generate more information and to create a data collection feature for creation of datasets for classification and analysis.

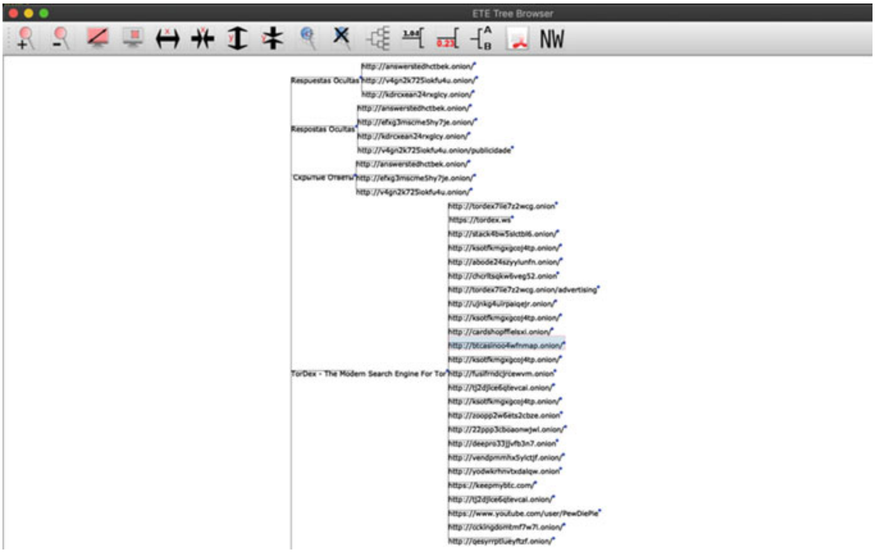

ETE Tree Browser
NW
Respuestas Ocultas
http://answerstedhctbek.onion/
http://v4gn2k72Siokfu4u.onion/
http://kdrcxean24rxglcy.onion/
Respostas Ocultas
http://answerstedhctbek.onion/
http://efxg3mscme5hy7je.onion/
http://kdrcxean24rxglcy.onion/
http://v4gn2k72Siokfu4u.onion/publicidade
Скрытые Ответы
http://answerstedhctbek.onion/
http://efxg3mscme5hy7je.onion/
http://v4gn2k72Siokfu4u.onion/
TorDex - The Modern Search Engine For Tor
http://tordex7iie7z2wcg.onion
https://tordex.ws
http://stack4bw5slctbl6.onion/
http://ksotfkmgxgcoj4tp.onion/
http://abode24szyylunfn.onion/
http://chcrltsqkw6veg52.onion
http://tordex7iie7z2wcg.onion/advertising
http://ujnkg4uirpaiqejr.onion/
http://ksotfkmgxgcoj4tp.onion/
http://cardshopffielsxi.onion/
http://btcasinoo4wfnmap.onion/
http://ksotfkmgxgcoj4tp.onion/
http://fusifmdcjrcewvm.onion
http://tj2djice6qtevcal.onion/
http://ksotfkmgxgcoj4tp.onion/
http://zoopp2w6ets2cbze.onion
http://22ppp3cbuaonwjwl.onion/
http://deepro33jjvfb3n7.onion
http://vendpmmhx5ylctjf.onion/
http://yodwkrhnvtxdalqw.onion
https://keepmybtc.com/
http://tj2djice6qtevcal.onion/
https://www.youtube.com/user/PewDiePie
http://cckingdombmf7w7l.onion/
http://qesyrrptlueyftzf.onion/

Fig. 4 Visualizer tree graph

References

1. Glassman M, Kang MJ (2012) Intelligence in the internet age: the emergence and evolution of open source intelligence (OSINT). Comput Human Behav 28(2):673–682
2. Bradbury D (2011) In plain view: open source intelligence. Comput Fraud Secur 2011(4):5–9
3. Butler B, Wardman B, Pratt N (2016) Reaper: an automated, scalable solution for mass credential harvesting and OSINT. APWG Symp Electron Crime Res 1–10
4. Zantout B, Haraty RA (2014) I2P Data communication system I2P data communication system. April 2002
5. Qin J, Zhou Y, Lai G, Reid E, Sageman M, Chen H (2005) The dark web portal project: collecting and analyzing the presence of terrorist groups on the web. In: Proceedings of the 2005 IEEE international conference on intelligence and security informatics, pp 623–624
6. Moore D, Rid T (2016) Cryptopolitik and the Darknet. Survival 6(3):38
7. Weimann G (2016) Going dark: terrorism on the dark web. Stud Confl Terror 39(3):195–206
8. Zulkarnine AT, Frank R, Monk B, Mitchell J, Davies G (2016) Surfacing collaborated networks in dark web to find illicit and criminal content. In: IEEE conference on intelligence and security informatics (ISI), pp 109–114
9. Minárik T, Osula A-M (2016) Tor does not stink: use and abuse of the Tor anonymity network from the perspective of law. Comput Law Secur Rev 32(1):111–127
10. Loesing K, Murdoch SJ, Dingledine R (2010) A case study on measuring statistical data in the {T}or anonymity network. In: Proceedings of the workshop on ethics in computer security research (WECSR)
11. Nafziger B (2017) Data mining in the dark: Darknet intelligence automation
12. Sanchez-Rola I, Balzarotti D, Santos I (2017) The onions have eyes: a comprehensive structure and privacy analysis of tor hidden services. In: Proceedings of the 26th international conference on world wide web, pp 1251–1260
13. Mouli VR, Jevitha KP (2016) Web services attacks and security-a systematic literature review. Proced Comput Sci 1(93):870–877

14. Cova M, Felmetsger V, Vigna G (2007) Vulnerability analysis of web-based applications. In: Test and analysis of web services, Springer, Berlin, Heidelberg, pp 363–394
15. Holland BR (2012) Enabling open source intelligence (OSINT) in private social networks
16. Nakamoto S (2009) Bitcoin: a peer-to-peer electronic cash system. Cryptogr. Mail. List https://www.metzdowd.com
17. Wesam M, Nabki A, Fidalgo E, Alegre E, De Paz I (2017) Classifying illegal activities on Tor network based on web textual contents, vol 1, pp 35–43
18. Sathyadevan S, Gangadharan S (2014) Crime analysis and prediction using data mining. In: 2014 first international conference on networks and soft computing (ICNSC), August 19, IEEE, pp 406–412
19. Chau M, Chen H (2008) A machine learning approach to web page filtering using content and structure analysis. Decis supp syst 44(2):482–494
20. Ani R, Jose J, Wilson M, Deepa OS (2018) Modified rotation forest ensemble classifier for medical diagnosis in decision support systems. In: Progress in advanced computing and intelligent engineering, Springer, Singapore, pp 137–146
21. Ani R, Augustine A, Akhil NC, Deepa OS (2016) Random forest ensemble classifier to predict the coronary heart disease using risk factors. In: Proceedings of the international conference on soft computing systems, Springer, New Delhi, pp 701–710

A Novel Approach to View and Modify Data in Cloud Environment Using Attribute-Based Encryption

Swaminathan Subbiah, S. Palaniappan, Sigamani Ashokkumar and Ananthakrishnan BalaSundaram

Abstract The Big data and cloud integration is a challenging Task. To enhance the data security issues, ABE can be deployed. In proposed model, a improved concept has been implemented and the integration of cloud and Big data is achieved. Security is the major threat for cloud computing applications. Every user has to feed user name, password, and primary key for Data access into the cloud data center. Data owner generates a new key to the users for accessing the data. Policy updating is also implemented in the proposed system, that is the accountability for the data access has also been implemented. In case of the change of policy, the altered data stored in the cloud is not affected. In addition to that, admin generates policy key based on the user's profile. If any user tries to misbehave, an immediate alert is sent to the data owner. Data owner can change the policy key and access policy in the run time. Our system should be able to update its policy automatically.

Keywords Big data · Cloud computing · ABE

1 Introduction

Big data is described using 3 V's, they are volume, velocity, variety and this was defined in the year of 2011. In the year of 2013, in addition to that, another V's are introduced, namely veracity, variability, visualization, and value. Nowadays, the Big data is getting humongous in size. It also provides a way to process a large quantity

S. Subbiah (✉) · S. Palaniappan · S. Ashokkumar · A. BalaSundaram
Department of Computer Science and Engineering, Saveetha School of Engineering, SIMATS, Chennai, India
e-mail: subbussp2007@gmail.com

S. Palaniappan
e-mail: s.palani.in@gmail.com

S. Ashokkumar
e-mail: sashokkumarkavi@gmail.com

A. BalaSundaram
e-mail: balawins2day@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_20

of data that are stored in the cloud server and also uses analytics. Hadoop is one of most important frameworks to process the big data. It is used to save a file and also process the file. To save the file, it uses hadoop distributed file system and to process or to do analytics, it uses map reduce algorithm. Hadoop helps to handle modification process. In this concept, Big data helps to modify the content dynamically without waiting for process to complete. It also has grains of what are all modifications done. It also used for processing the variety of gathered information in high velocity. The speed of processing this kind of data is faster than comparing with other previous database management systems. Big data also recovers and discovers the select data that user wants to do. It helps to improve the decision making and error detection dynamically. Because of this high velocity data processing in big data is introduced because previous database management tools are not suitable for process that kind of large data. For this kind of processing, big data uses cloud to store and process these large data sets. This can be accessed using efficient way by user. So that user can process this data at anytime and anywhere. After storing this processed data. In cloud, security is major threat . Sometimes, data owners not trusted the cloud parties. Attribute-based encryption (ABE) is one of the most important techniques used in the cloud. It helps to provide end-to-end data security when the data stored in the cloud. It allows user to have access polices, using that user or data owner can encrypt and decrypt the data according to their access policies. When multiple organizations and enterprises stores data into the cloud, then changing the policy becomes a major issue as data access policies may be changed dynamically and frequently by users or data owners. If the data is transferred back to the local site from the cloud, again the encrypted data contains new access policy after updating that policy it should be moved back to the cloud server.

2 Issues and Limitations

In the existing system contains policy update issue, but we can neglect this using attribute-based encryption method [1]. Because, once data owner farm out the data into cloud server, they won't store in client system or their own system. To modify the policy of cipher text in the data storage unit, it helps to get the data and reencrypt under the new outcome policy, and then send it back to the cloud server. But it contains some difficulties like high communication overhead and heavy computation on data owners.

In this system also takes more time for updating, using ABE we can easily update the policy. That is when we go for any integration in cloud and big data it is somehow a challenging task. Because during that time, we must shut the cloud server access it also takes more time.

For example: If we enter into any college portal, it provides different data for different users, if you are a student most of time, you do not have to update in your portal. In case of Professor or Head of department, sometimes, they need to update some data (like attendance, exam marks, exam timetable, etc….) during that time they should have their own user ID, password and secret key using this they can login it also provides security. In case of any content updating by data owner in cloud server they cannot allow to modify or view the data. To neglect that we created view and modify policy, During the normal time, if user login through their account, it shows two buttons one for view only and another one for view and modify, If any of updating take place by data owner then data which are all present in the cloud server before the update is transferred to secondary server.

So in that time users only allowed viewing that content they cannot allow them to do update.

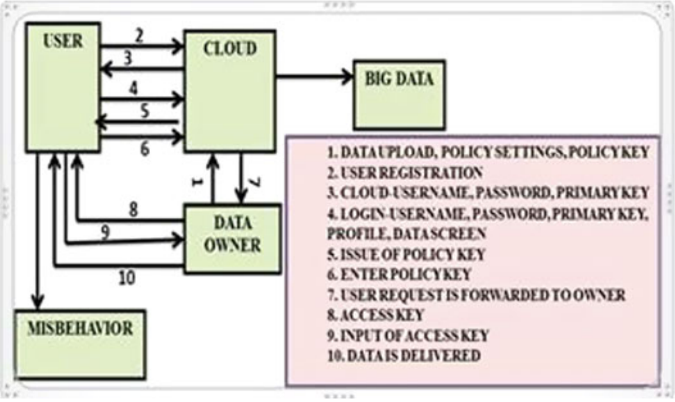
3 Modified Approach

It is already known that, admin generates policy key based on the User's Profile. Some would have view policy and others would have modify policy. If any user tries to misbehave, automatically their secret key will be changed by the data owner. Data owner can change the policy key and access policy dynamically. So the misbehaved user does not have time to do move further. This policy is provided according to their role in the organization and their role decides to limit the authentication, i.e. if the person is working as a Professor or Head of the department in a desired institution, their limit only resides in their department, they will not get access to view or modify beyond their limits. If he or she tries to access their policy key, it will be immediately changed. If the person is a student, he gets view policy and he will not be allowed to mody the content. To find their role in the organization, we are using big data which used to analyze the streaming of data. In this paper, we have introduced policy method but usually we have two methods, one is view policy and another one is modify policy. Using this modify policy, we can modify the data in cloud; the view policy is used for read only access. In case of content change or implementation, the modify policy is unbuttoned. So, we cannot allow doing any changes at a time. We can only allow viewing and once the implementation is done, it allows users to work normally.

4 Data Flow Explanation

Data owner uploaded the data, policy settings, and policy key for user based on their user profile. This user profile explains the role and responsibility of each user. The secret policy is also generated by the data owner, it helps to find out the misbehaved user. Once it is done, the data is stored in the cloud server. When the user login through the search engine, the cloud displays login form and it contains the identity field; after submitting the form with the relevant information, the browser checks and encrypt the data and send to the relevant cloud server. If the entered are authenticated, then it allows the user to access the data according to their access policy. After that, it asks user to type their policy key, then this policy is forwarded to the data owner. Then, data owner sends access key to the user mobile or any other devices. Then, it asks the user to enter the access key then it allows the user to modify the contents or data that resides within their access limit. Data manipulation is done.

5 Architecture Diagram


USER
CLOUD
BIG DATA
DATA OWNER
MISBEHAVIOR
1
2
3
4
5
6
7
8
9
10
1. DATA UPLOAD, POLICY SETTINGS, POLICY KEY
2. USER REGISTRATION
3. CLOUD-USERNAME, PASSWORD, PRIMARY KEY
4. LOGIN-USERNAME, PASSWORD, PRIMARY KEY, PROFILE, DATA SCREEN
5. ISSUE OF POLICY KEY
6. ENTER POLICY KEY
7. USER REQUEST IS FORWARDED TO OWNER
8. ACCESS KEY
9. INPUT OF ACCESS KEY
10. DATA IS DELIVERED

User
Data owner
Misbehavior
Cloud
Big data

(1) User

A person who utilizes resources (like computer, software product, websites, etc…) is called user. User often has an account, it contains identity like username, login ID, password, etc. It helps to know authorized user and accessing the data. User often called as end user, they also defined as operators. This user identity also helps to create unique ID for each user. They login their account by submitting the identity, sometimes password, fields are defined as case sensitive, it does not allow special characters. In this paper, user is people, who viewing and modifying the data in the cloud server.

(2) Data owner

A person who can authorize or deny the access to certain data, he is also responsible for accuracy, security, integrity, and authentication. It is act of having legal rights and overall control over a single or set of data elements. He has the ability to create a new data field for user, it helps to edit, modify, and share over the networks. He can also be allowed to restrict access for particular elements and also distributed the policy. Sometimes, they uses legal actions to claim the copyrights, because if there any illegitimately breached by unknown users. In this paper, data owner stores data in cloud server.

(3) Misbehavior

Here, the details of the misbehaved users will be stored for the reference of the data owner. Then only the system will identify the users when they request for the key generation, the policy will be taken whether they can be allowed to allocate the policy to modify/view the data. Due to this, the data stored in the cloud server will be kept in the safe environment as well as the unwanted modifications of the data can be avoided.

(4) Cloud server

Cloud is a centralized storage. It is also known as on-demand computing and ubiquitous computing. The information, data, and resources are shared with other computer and other devices (e.g. network, servers, storage, applications, and services) if they want. Cloud is used for storage purpose and sharing the resources. It also helps the large companies to avoid upfront infrastructure costs and focus on projects. Nowadays, cloud computing has become a highly demanded service, because it provides high-speed computation, less cost and easy to maintain characteristics. Security is the major threat in the cloud computing. It provides three categories of service such as Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service (SaaS). It helps the user to work on any software product at any platform without any cost. In this, the cloud server is used for data storage which is created by the data owner and provides multiuser access through the network.

(5) Big data

Big data is the term used to define large amount of both structured (traditional data) and unstructured data (like images, text, audio, video, etc…). It reduces the challenges like analysis, searching, sharing, storage, querying, etc…). Big data overcomes the challenges that were faced in the traditional method. Because in the traditional data processing method, we use database management system (DBMS) and (relational database management system (RDBMS), which processes only the business data. The business data is arranged in the form of table (intersection of rows and columns). Each row holds record, each column is called as tuple. In that, storing the large amount of unstructured data is a major problem because of that manipulation of data. To overcome that, we have introduced big data and its capacity to store terabytes. Hadoop is the open-source framework used to develop distributed storage and distributed data processing. In this, hadoop is used to perform analytics in user profile to know their access policy limitations and modify the new contents.

6 Modules

A. User registration
B. Big data deployment
C. Dynamic policy generation misbehavior detection
D. Cloud deployment
E. Policy key generation

A. User Registration

Once the user creates an account, they are allowed to login into their account to access the applications. Based on the user's request, the server will respond to the user. All the user details will be stored in the database of the server. Every time user tries to login, this checks the authentication of the username and password.

Special characters and ASCII value are not allowed in the password; therefore, password becomes case sensitive in nature. This password is used for security purpose and also used to check whether the authorized user is accessing the data.

B. Big data deployment

Big data is described using 3 V's they are volume, velocity, variety, this was given in the year of 2011. In the year of 2013, in addition to that, another V's are introduced veracity, variability, visualization, and value. In day by day, the quantity of big data emerges in the form of increasing orders. It also provides a way to process a large quantity of data that are stored in the cloud server and also uses analytics. Hadoop is one of most important frameworks to process a big data. It is used to save a file and also process the file, inorder to save the file, it uses hadoop distributed file system and to process or to do analytics, it uses map reduce algorithm. Hadoop helps to handle the modification process. In this concept, Big data helps to modify the content dynamically without waiting for the process to complete.

C. Dynamic policy generation misbehavior detection

In this module, we create a dynamic policy generation, i.e. data owner will give the file access permission to some data user to view and some user to edit, if they edit without the permission or misbehave, then the policy can be changed dynamically. After that, if the user enters previous key, he or she will not be allowed to access data.

D. Cloud deployment

Cloud is a centralized mobile data access center. We can use any device to access the cloud data. It also provides platform as a Service (PaaS), Software as a Service (Saas) and Infrastructure as a Service (Iaas) platforms. Multi and different devices connected using cloud; this provides unique and different information for a particular entity. Cloud also provides data storage. Hence, the data can be accessed at anywhere and at anytime.

E. Policy key generation

In cloud, policy key generation is the most important paradigm and it is an efficient way to secure the data from the external and internal attacks. It is also used to tackle that kind of attacks. The cloud server will set the policy key for each and every user based on their designation. So that, legitimate users can view the data stored in the cloud only up to their privilege level. They are not allowed to view the data beyond their privileges. This policy key is also used for developing an unique identity. The format of the policy key differs according to their departments. The first two digits are used to identify their department and the next one digit is used for their designation. It improves the data security for both data owner and users.

7 ABE Implementation

ABE is defined has attribute-based encryption, it is one of the public key encryptions in which the secret key depends upon the attributes or characteristics (like person name, age, account number, etc…). It can be also used for log encryption. Instead of encrypting each part of a log with the keys of all recipients, it is possible to encrypt the log only with attributes that match recipient's attributes. For the decryption process, the same key can be used. This primitive can also be used for broadcast encryption in order to decrease the number of keys used.

8 Conclusion and Future Work

In this paper, cloud and big data integration challenges are explained. Analysis has been done on the policy updating problem by using the big data control systems and derived some challenging tools that are needed to solve this problem. We have also created an useful model to update the date in the server, which can satisfy all the needs in the big data process. We have also explained a detailed attribute-based access control for big data in the cloud server, and designed policy updating algorithms for different types of access policies. Furthermore, we can use this method to check the data integrity. Data security in the cloud environment has been much improved by the proposed model and also monitors and records the misbehaved users. Hence, the system can improve its decision making when it goes for the new key assignment to the users by this the system and also avoids the unauthorized user access into the system.

References

1. Goyal V, Pandey O, Sahai A (2006) Attribute-based encryption for fine-grained access control of encrypted data. In: CCS'06. ACM, pp 89–98
2. Bethencourt J, Sahai A, Waters B (2007) Ciphertext-policy attribute based encryption. In: S&P'07. IEEE, pp 321–334
3. Waters B (2011) Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. In: PKC'11. Springer, pp 53–70
4. Lewko AB, Okamoto T, Sahai A (2010) Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption. In: EUROCRYPT'10. Springer, pp 62–91
5. Lewko AB, Waters B (2011) Decentralizing attribute-based encryption. In: EUROCRYPT'11. Springer, pp 568–588
6. Yu S, Wang C, Ren K et al (2010) Achieving secure, scalable, and fine-grained data access control in cloud computing. In: INFOCOM'10. IEEE, pp 534–542
7. Yang K, Jia X, Ren K (2013) Attribute-based fine-grained access control with efficient revocation in cloud storage systems. In: AsiaCCS'13. ACM, pp 523–528
8. Yang K, Jia X, Ren K, Zhang B, Xie R (2013) DAC-MACS: Effective data access control for multiauthority cloud storage systems. IEEE Trans Info Forensics Secur 8(11):1790–1801
9. Yang K, Jia X (2014) Expressive, efficient, and revocable data access control for multi-authority cloud storage. IEEE Trans Parallel Distrib Syst 25(7):1735–1744
10. Sahai A, Seyalioglu H, Waters B (2012) Dynamic credentials and ciphertext delegation for attribute-based encryption. In: CRYPTO'12. Springer, pp 199–217
11. Subbiah S, Selvamuthukumaran S, Ramkumar T (2015) An approach for enhancing secure cloud storage using vertical partitioning algorithm. Middle-East J Sci Res 23(2):223–230. ISSN:1990-9233
12. Subbiah S, Selvamuthukumaran S (2015) Distributed data security for data prevention in cloud computing using one time password for user authentication. J Environ Sci Comput Sci Eng Technol 4(4):752–758. E-ISSN: 2278-179X
13. Roshan, MR, Kumar, MS, Magesh S, Palaniappan S (2017) Forwarding secured data in cloud interface systems. Int J Pure Appl Math 116(23):179–183

Root Cause Detection of Oscillation in Shell and Tube Heat Exchanger Process

S. Abirami and S. Sivagamasundari

Abstract The key emphasis on Control Loop Performance Monitoring (CLPM) includes the detection of oscillations in control systems. Oscillations are the results of plant performance degradation and are a very common problem that occurs in the control loops of the process. This paper discusses the technique for detecting oscillations in process variables. The occurrence of oscillation in control loops, results in deviation from the setpoint, hence reducing the productivity and thus the profitability. Oscillations in control loops may be due to several causes such as aggressive tuning of the controller, external disturbances and sometimes may be due to stiction in control valve. Low maintenance of valves frequently produces large oscillations in a process which in turn affects the throughput. In time domain, detection of oscillations is tough when the signal includes disturbances. In frequency domain, Bispectrum analysis is a great tool for the detection and analysis of oscillations. To detect the oscillatory behaviors, the Modified Bispectrum tool was applied to a highly nonlinear Shell and Tube Heat Exchanger (STHX) process.

Keywords CLPM · Oscillations · Plant performance degradation · Control loops · Control valves · Modified bispectrum · STHX

1 Introduction

Root-cause detection of oscillations in process control loop is still a problem at the current juncture; with which one detects the malfunctions of a loop in many conditions [1]. Poor control loop performance is commonly the result of unnoticed deterioration arising in control valves and external disturbances. The field of data-driven approaches for Control loop Performance Monitoring (CPM) is significantly

S. Abirami (✉) · S. Sivagamasundari
Department of Electronics and Instrumentation Engineering, Annamalai University, Chidambaram 608002, India
e-mail: abiramiselvaraju@gmail.com

S. Sivagamasundari
e-mail: sivagamasundari67@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_21

improved by having comparable and standardized sets of data which is used for testing. They [2] anticipated that companies involved in production gradually and steadily use CPM tools to tackle loop performance problems. Stiction is the frequently found control valve problem in process industries. Several attempts have been made to understand, model and then detect stiction in control valves. The data-driven method of valve stiction [3, 4] is used with regular plant model to get the required oscillating data. HOSA with closed-loop data detects the root cause for poor control loop performance utilizing its tools namely cumulants or moments, bispectrum and bicoherence to develop the non-gaussianity and the nonlinearity indices so as to detect and quantify the source of nonlinearity [5]. The techniques of HOSA have been extensively used in various fields. One such major contribution includes the bio-medical area [6].

The works done in this paper has been originated from the ideas gained by surveying the literature, specifically from the various chapters of [7–10]. This paper emphases on the detection of oscillations present in the control loops of STHX process using modified bispectrum analysis.

2 Mathematical Modeling

2.1 Energy Balance Equations

The Energy Balance Equations derived from "Rate of energy stored in the control volume is equal to the rate of gain of energy from neighboring control volume", for shell-side and tube-side [11], respectively, are given below.

$$\text{Shell Side: } \frac{\rho_s C_s V_s}{N} * \frac{dT_{co}}{dt} = \dot{m}_s C_s (T_{ci} - T_{co}) + \frac{h_s A_s}{N}(T_{ho} - T_{co}) \tag{1}$$

$$\text{Tube Side: } \frac{\rho_t C_t V_t}{\mathrm{N}} * \frac{dT_{ho}}{dt} = \dot{m}_t C_t (T_{hi} - T_{ho}) + \frac{h_t A_t}{N}(T_{co} - T_{ho}) \tag{2}$$

2.2 Process Parameters and PID Controller Parameters

The controller parameters are calculated using the process parameters by Zeigler Nichols tuning technique [11]. The process and PID controller parameters for various operating regions are computed and specified in Table 1.

Table 1 Process and PID controller parameters

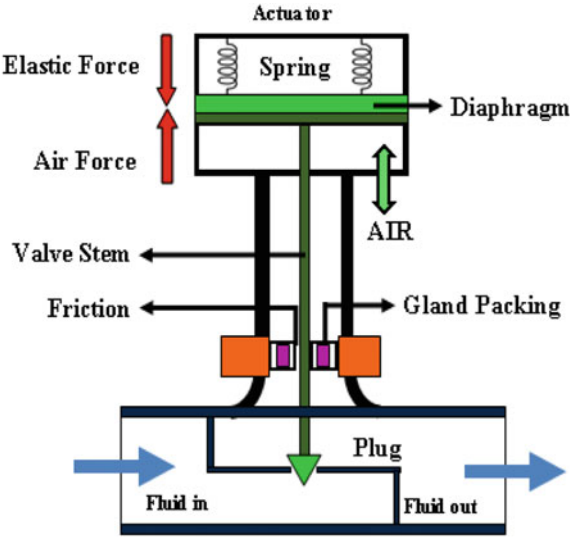
Flow rate (lps)	Operating region (°C)	Gain (°C/lps)	Time constant (s)	Time delay (s)	Kc	Ki	Kd
0.02–0.04	44.96–45.5	−33.3	0.827	0.137	−0.218	−0.796	−0.0149
0.04–0.06	44.65–44.96	−15.5	0.773	0.134	−0.447	−1.668	−0.0299
0.08–0.10	44.42–44.52	−5.5	0.606	0.122	−1.084	−4.443	−0.066
0.12–0.10	44.41–44.34	−3.5	0.335	0.161	−0.7134	−2.216	−0.057
0.08–0.06	44.65–44.5	−7.5	0.776	0.159	−0.781	−2.456	−0.0621
0.06–0.04	44.96–44.5	−14	0.816	0.192	−0.3643	−0.949	−0.03497

3 Valve Stiction Model

3.1 Structure of Pneumatic Control Valve

Figure 1 shows the general structure of a pneumatic control valve. The valve is opened by air force and closed by elastic pressure. The position of the plug regulates the balance between elastic pressure and air force thus regulating the flow rate. The valve stem connected to the plug is moved in contrary to static force caused by gland packing, a device which is sealed to prevent process fluid leakage.

Fig. 1 Structure of pneumatic control valve



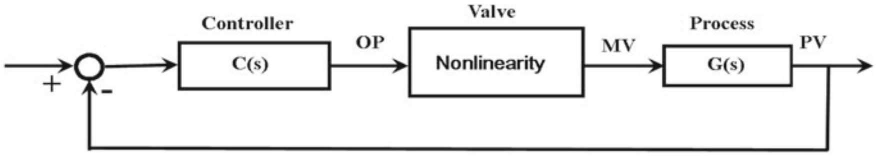


Fig. 2 Closed loop system with valve stiction model

3.2 Closed Loop System with Valve Stiction Model

Figure 2 shows the block diagram of closed-loop system with the control valve stiction model. The controller chosen here is PID controller and the process taken is Shell and Tube Heat Exchanger. The single parameter model [12] is utilized for valve nonlinearity as valve stiction model.

3.3 One Parameter Model

The actual valve position (x_t) differs from the control signal (u_t) if the valve undergoes stiction, hence resulting in a poor control loop performance. For detection problem, a simple valve model uses model-based approach [12]. The actual valve position (x_t) is considered to be piecewise constant, as a function of time.

$$x_t = \begin{cases} x_{t-1}, & \text{if} |u_t - x_{t-1}| \le d \\ u_t, & \text{otherwise} \end{cases} \tag{3}$$

4 Oscillation Detection

4.1 Bispectrum Analysis

Scrutinizing the nonlinear signals in Higher Order Statistics encloses the relations between phase components. The bispectrum $B\,(f_1,f_2)$ of a non-Gaussian signal, $x\,(t)$, is a 2-D Fourier transforms of the third-order cumulants gives the info not presented by the spectral domain is defined as

$$C(m,n) = E\;[x(k)\,x(k+m)\,x(k+n)] \tag{4}$$

where E is the Expectation function. The bispectrum formula related to (4) is:

$$B(f_1, f_2) \triangleq E\;[X(f_1)X(f_2)X*(f_1+f_2)] \tag{5}$$

where $X\ (f)$ is the Fourier transform of $x\ (t)$ and * represents its complex conjugate. Bispectrum contains the facts about the relation of phase between the frequency components at f_1,$f_{2,}$ and f_1 +f_2 [11].

4.2 Modified Bispectrum Analysis

In Eq. (5) some modifications are made to bispectrum formula and hence termed as Modified Bispectrum analysis, which is used to detect the root cause for process control loop oscillations of STHX process.

$$B_M(f_1, f_2) \triangleq E\ [X(f_2 + f_1)\ X(f_2 - f_1)X(f_2)X*(f_2)X*(f_2)] \tag{6}$$

The total phase of modified bispectrum is,

$$\varnothing_M(f_1, f_2) = \varnothing(f_2 + f_1) + \varnothing(f_2 - f_1) - \varnothing(f_2) - \varnothing(f_2) \tag{7}$$

As the two components f_1 and f_2 are in coupling, their phases are related as

$$\begin{aligned} \varnothing(f_2 + f_1) &= \varnothing(f_2) + \varnothing(f_1) \\ \varnothing(f_2 - f_1) &= \varnothing(f_2) - \varnothing(f_1) \end{aligned} \tag{8}$$

By substituting Eq. (7) in (6) for modulated signal bispectrum, the total phase is zero and modulated signal bispectrum amplitude is the product of the four magnitudes, which contributes to the maximum of the complex product. Therefore, a bispectral peak appears at (f_1,f_2) [13]. For checking the probable presence of a nonlinear element in control loop, the process variable (PV) data is used by the modified bispectrum.

5 Results and Discussions

Detection of oscillations in process control loop is essential as it reduces the plant profitability. Root causes for oscillations are not only due to the occurrence of nonlinearities (Dead band, Hysteresis, Stiction, etc.,) but also due to external disturbances. The stiction in control valve causes the process output to oscillate around the set point. The manipulated variable considered in the STHX process is cold water flow rate and the controlled variable is hot water outlet temperature. White noise is introduced in the closed-loop to collect datasets due to external disturbance. For getting nonlinearity induced oscillatory data, a stiction model is introduced in control loop with known values of stiction parameters. From these responses simulated sets of data were collected and used as input vector for modified bispectrum analysis. Modified bispectrum plots of external oscillatory disturbance for various operating regions in STHX (PV) are displayed from Figs. 3, 4, 5, 6, 7 and 8. Modified bispectrum plots of stiction (both weak and strong stiction) for various operating regions in STHX (PV) are presented from Figs. 9, 10, 11, 12, 13 and 14. The estimated modified bispectrum values for external oscillatory disturbance and for stiction are presented in Tables 2 and 3.

The bispectral amplitude with graphical plots has been used to diagnose the root causes for the bad performance of control loops. The threshold value is specified to be 0.1. If the bispectrum value exceeds the threshold value, nonlinearity can be confirmed. The threshold limit for nonlinearity detection is chosen based on the experience of using this tool in process performance diagnosis and for this case clearly detects the stiction nonlinearity present in the process output. Comparing the plots, highest bispectrum value is observed for the PV data which is affected by the existence of stiction in control valve, i.e., the higher value indicates significant

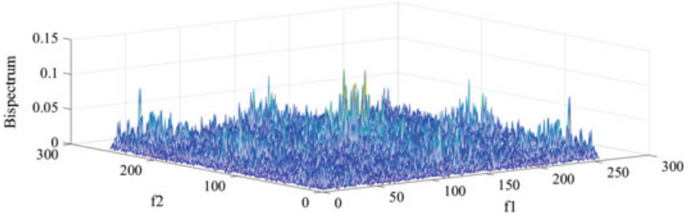


Fig. 3 Positive step change—Region 1 (44.96–45.5)

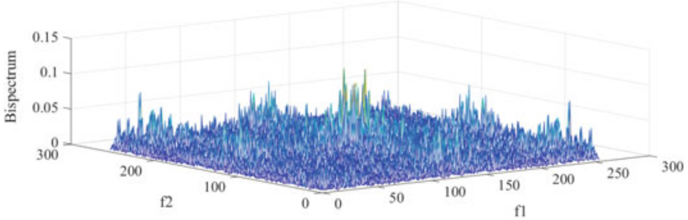


Fig. 4 Positive step change—Region 2 (44.65–44.5)

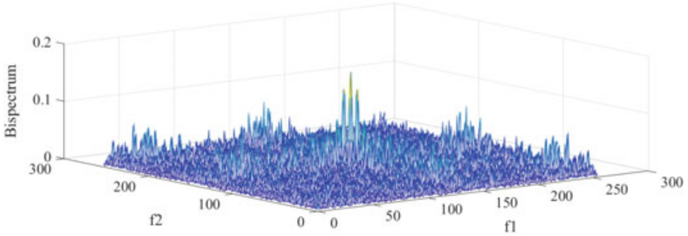


Fig. 5 Positive step change—Region 3 (44.41–44.34)

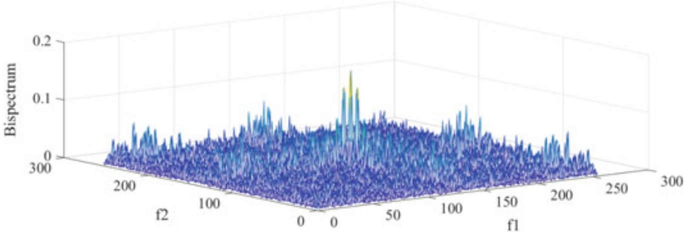


Fig. 6 Negative step change—Region 1 (44.96–44.5)

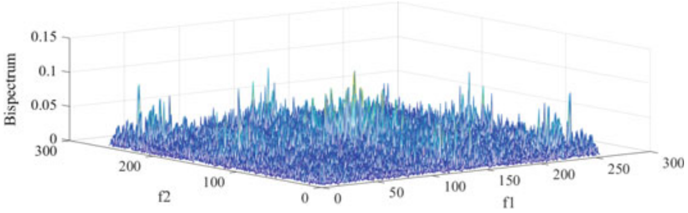


Fig. 7 Negative step change—Region 2 (44.65–44.5)

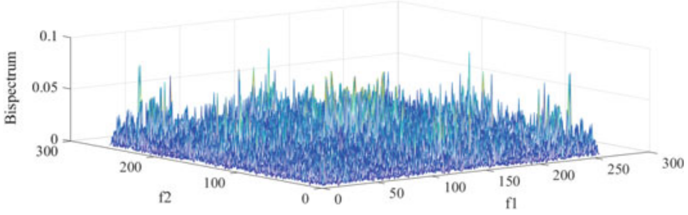


Fig. 8 Negative step change—Region 3 (44.41–44.34)

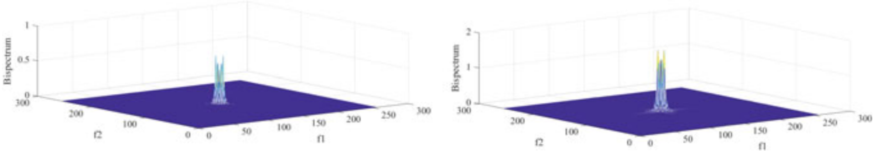


Fig. 9 Weak and strong stiction for [positive step change—Region 1 (44.96–45.5)]

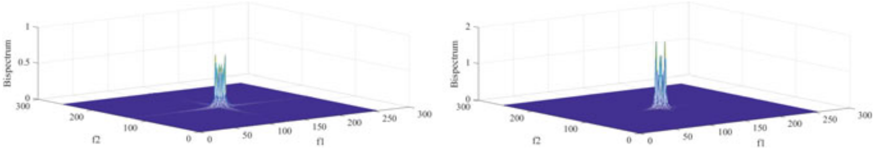


Fig. 10 Weak and strong stiction [positive step change—Region 2 (44.65–44.5)]

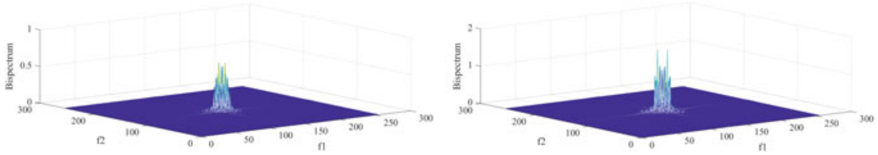


Fig. 11 Weak and strong stiction [positive step change—Region 3 (44.41–44.34)]

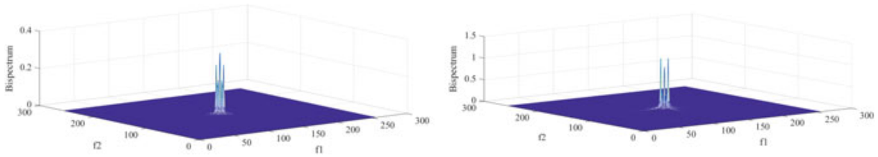


Fig. 12 Weak and strong stiction [negative step change—Region 1 (44.96–44.5)]

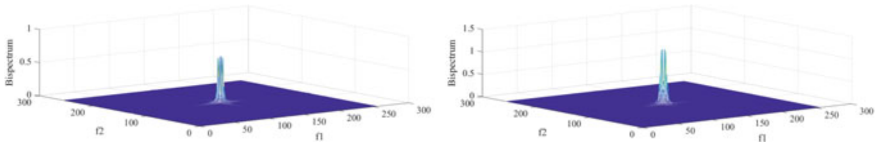


Fig. 13 Weak and strong stiction [negative step change—Region 2 (44.65–44.5)]

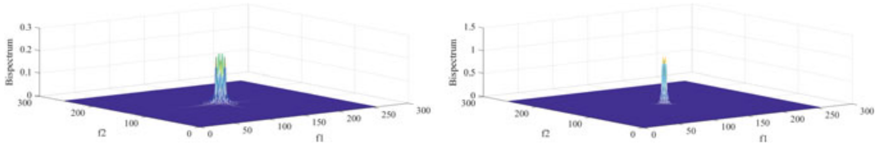


Fig. 14 Weak and strong stiction [negative step change—Region 3 (44.41–44.34)]

Table 2 Estimated modified bispectrum values for external disturbance

Disturbance	Positive step change			Negative step change		
	Region 1 (44.96–45.5)	Region 2 (44.65–44.96)	Region 3 (44.42–44.52)	Region 1 (44.96–44.5)	Region 2 (44.65–44.5)	Region 3 (44.41–44.34)
Modified bispectrum	0.064	0.068	0.08	0.098	0.069	0.07

Table 3 Estimated modified bispectrum values for stiction

Regions		Modified bispectrum values	
		Weak stiction	Strong stiction
Positive step change	Region 1 (44.96–45.5)	0.37	0.99
	Region 2 (44.65–44.96)	0.4	1
	Region 3 (44.42–44.52)	0.35	0.88
Negative step change	Region 1 (44.96–44.5)	0.15	0.68
	Region 2 (44.65–44.5)	0.37	0.65
	Region 3 (44.41–44.34)	0.12	0.57

nonlinearity. The bispectrum values less than 0.1 is due to external disturbance. In this case, the bispectrum is found to have multiple peaks with lesser amplitude.

5.1 Modified Bispectrum of External Disturbance Induced Oscillations for Various Operating Regions in STHX (PV)

See Figs. 3, 4, 5, 6, 7 and 8.

5.2 Modified Bispectrum of Stiction (Weak Stiction and Strong Stiction) Induced Oscillations for Various Operating Regions in STHX (PV)

See Figs. 9, 10, 11, 12, 13 and 14.

6 Conclusion

Higher Order Statistical technique such as bispectrum is used in this paper to detect the oscillations present in the process variable for STHX process. The bispectral values with graphical plots have been used to diagnose the root causes for the bad performance of control loops. The magnitude of bispectrum indicates the presence or absence of process nonlinearity. The results clearly shows that modified bispectral analysis gives promising results for oscillation detection. The future scope of this work involves compensating techniques to overcome stiction nonlinearity present in control valves.

References

1. Bauer M, Horch A, Xie L, Jelali M, Thornhill N (2016) The current state of control loop performance monitoring—A survey of application in industry. J Process Control 38:1–10
2. Bauer M, Auret L, le Roux D, Aharonson V (2018, May 9–11) An industrial PID data repository for Control Loop Performance Monitoring (CPM). In: Preprints of the 3rd IFAC conference on advances in proportional-integral-derivative control, Ghent, Belgium, pp 823–828
3. Choudhury MAAS, Thornhill NF, Shah SL (2005) Modelling valve stiction. Control Eng Pract 13:641–658
4. Shoukat Choudhury MAA, Jain M, Shah SL (2008) Stiction—definition, modelling, detection and quantification. J Process Control 18:232–243
5. Shoukat Choudhury MAA, Shah SL, Thornhill NF (2004) Diagnosis of poor control-loop performance using higher-order statistics. Automatica 40:1719–1728
6. Goshvarpour A, Goshvarpour A (2013) Comparison of higher order spectra in heart rate signals during two techniques of meditation: Chi and Kundalini meditation. Cogn Neurodyn 7:39–46
7. Shoukat Choudhury MAA, Shah SL, Thornhill NF (2008) Diagnosis of process nonlinearities and valve stiction-data driven approaches. Advances in industrial control. Springer, Berlin, Heidelberg
8. Matsuo T, Sasaoka H, Yamashita Y (2003) Detection and diagnosis of oscillations in process plants. In: Palade V, Howlett RJ, Jain L (eds) Knowledge-based intelligent information and engineering systems, KES 2003, vol 2773. Lecture notes in computer science. Springer, Berlin, Heidelberg, pp 1258–1264
9. Karra S, Karim M (2010) Oscillation root-cause detection and quantification under multiple faults. In: Jelali M, Huang B (eds) Detection and diagnosis of stiction in control loops. Advances in industrial control. Springer, London, pp 267–293
10. Karra S, Jelali M, Karim M, Horch A (2010) Detection of oscillating control loops. In: Jelali M, Huang B (eds) Detection and diagnosis of stiction in control loops. Advances in industrial control. Springer, London, pp 61–100
11. Abirami S, Sivagamasundari S (2018) Comparison of controller tuning techniques for a temperature control of STHX Process. Int J Comput Sci Eng 6(8):316–320
12. Stenman A, Gustafsson F, Forsman K (2003) A segmentation-based method for detection of stiction in control valves. Int J Adapt Control Sig Process 17:625–634
13. Shaeboub A, Gu F, Lane M, Haba U, Wu Z, Ball AD (2017) Modulation signal bispectrum analysis of electric signals for the detection and diagnosis of compound faults in induction motors with sensorless drives. Syst Sci Control Eng 5(1):252–267. https://doi.org/10.1080/21642583.2017.1331769

Performance Assessment of Spread Spectrum Communication Receivers

P. Anand Krisshna, K. Vandith Sreenivas and Gayathri Narayanan

Abstract This paper mainly focuses on implementing a new approach rather than using the conventional method of generating an intermediate frequency in a mixer. The ordinary mixer is compared with a switching mixer through several techniques in order to strengthen the point that switching mixers have a better performance. Theoretically, we know that switching mixers are more efficient but here we also give it a practical justification through this paper. Software such as MATLAB and Proteus has been used for the same. The main objective of this research work is to determine the maximum amount of noise that can be removed to obtain a good reconstruction of the input signal.

Keywords AGWN · Monte-Carlo simulation · Modulation schemes · BER · SNR, DSSS, FHSS

1 Introduction

A mixer is a basic electronic circuit that mixes a radio frequency signal with a local oscillator signal and produces the sum and difference frequency as the output. The output port is also called as the Intermediate Frequency port. The mixer is an important component of the receiver in any given communication system. The Fig. 1 gives a mathematical representation of a mixer circuit.

$$f_{\mathrm{IF}} = f_{\mathrm{LO}} \pm f_{\mathrm{RF}}$$

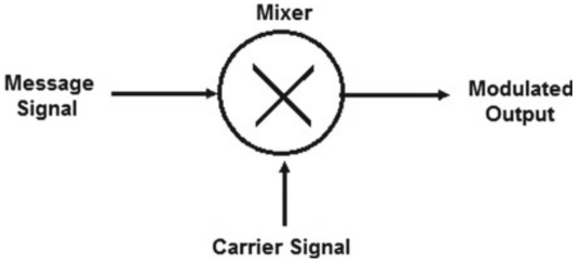
They limit the dynamic range of a system through the following specifications mentioned below

- Noise figure and LO noise
- Power compression

P. A. Krisshna · K. V. Sreenivas (✉) · G. Narayanan
Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India
e-mail: vandithsreenivas@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_22

Fig. 1 Model of a simple mixer



- Conversion Efficiency
- Port to port isolation
- Single tone inter-modulation distortion
- Multi-tone inter-modulation distortion.

There are basically two ways in which the process of mixing is done, one is the non-linear way and the other is by switching depending upon the local oscillator signal. The non-linear frequency mixer creates new frequencies from the two applied signals, whereas the switching mixer aims to perform linear operations on the signal by hard switching that will be driven by the local oscillator.

2 Related Work

Commercially switching mixers are preferred to non-linear ones and the advantage that it gives is a lower noise figure along with a larger conversion gain, by applying the same effort, because the switching diodes act like an open switch as well as a closed switch and in both the case only a minimal noise will be added [1]. Switching mixers are the mixers that are most used in the field and theoretically it has around 3.9 dB efficiency. They are roughly split up into two, the passive and the active. The passive ones can further be divided to diode based and FET based. The noise generated in mixers is caused due to the diodes, transistors, and agitation of electrons in conductor that cause resistive losses which further becomes thermal noise. Mixers have a large range of applications in communication systems. The Super-heterodyne receiver as well as the direct conversion receiver architectures use mixers at the input to down-convert and demodulate the digital information [2]. Therefore mixers are widely used in analog or RF front end of receivers. They can be used for demodulation and also as analog multipliers. The application of spread spectrum techniques is not restricted to mixers. Here, the signal is prone to jamming, which affects transfer of information, especially in critical cases such as the transmission of encrypted data. As reference [3] suggests, a Frequency Hopping Spread Spectrum (FHSS) system is often deployed to protect wireless communication from jamming or to hinder undesired reception of the signal. [4] suggests a scheme of combining spread spectrum technology with the MSK-LFM waveforms. The spread spectrum technology is applied to the radar signal, which can remarkably improve the performance of the signal ambiguity function. Using adaptive frequency hopping, a system implemented to enhance immunity toward frequency interference by avoiding usage of congested frequency channels in hopping sequence [5]. CMOS mixers can also be used to implement these techniques and they perform well in noisy environments [6]. In Cognitive Radio (CR) networks, less utilized spectra can be detected using spread spectrum techniques due to their ability to cover wider spectra [7]. Conventionally, Additive White Gaussian Noise (AWGN) is the noise type that will be encountered during transmission, so analysis of AWGN helps in simulation of the technique in MATLAB [8]. BSIM models are used for transistor design (MOSFETS), designed by UC Berkeley. These transistors hare hence used in receiver circuits [9]. SDR (Software Defined Radio) reduces hardware and maintenance costs due to the majority of its functionality being software. In particular RTL_SDR (Realtek Software Defined Radio) reduces the cost further thus making it a good option for transmission of signals over a channel [10].

As mentioned above, CMOS Radio Frequency (RF) circuits are used in transmitters and receivers [11]. A bandpass sampling receiver of a certain design will help in efficient transmission of signals over multi-channel networks; these radio receivers can be built using switching mixers for lesser BER [12].

3 Proposed Work

The principal objective of this work is to compare the spread spectrum techniques by using both ordinary and switching mixers and to verify that the bit error rate (BER) of the switching mixer is lesser than that of the ordinary mixer, thus implying that switching mixers are more efficient. The verification is done using MATLAB, where a random value is chosen for further operations.

For effective communication, the transmitted signal has to be received as it is on the other side. This is ideal, since over a channel (in most cases air), the signal may experience the effect of noise, which will hamper its efficiency. The interference of noise may be unintentional, such as another signal being transmitted over the same channel, or intentional, such as a signal jammer or an enemy trying to intercept signals. One type of technique that can avoid this kind of interference is the ‘Spread Spectrum ‘technique. This technique creates a special code for the transmitted signal that increases its bandwidth substantially and makes it look like a noise signal in itself. This code is known only to the transmitter and receiver. The most commonly used techniques are DSSS (Direct Sequence Spread Spectrum) and FHSS (Frequency Hopping Spread Spectrum).

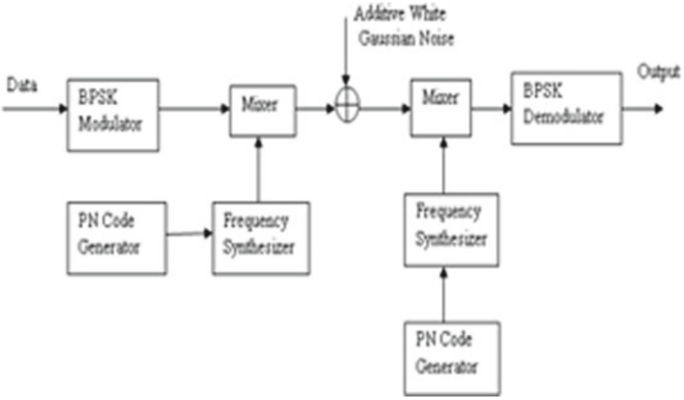


Figure A. FHSS

Bandwidth and power are the major shortcomings faced in the study of digital communication systems. These important parameters need to be improved in order to achieve effective performance. But, there is a trade-off in this efficiency in order to provide an important objective in communications i.e., Security. There will be no meaning for a system, where messages can be detected by unwanted listeners. The major advantage of Spread Spectrum (SS) is its ability to counter interference whether unintentional (i.e. another user trying simultaneously to transmit over the channel) or intentional (i.e. a jammer or interceptor).

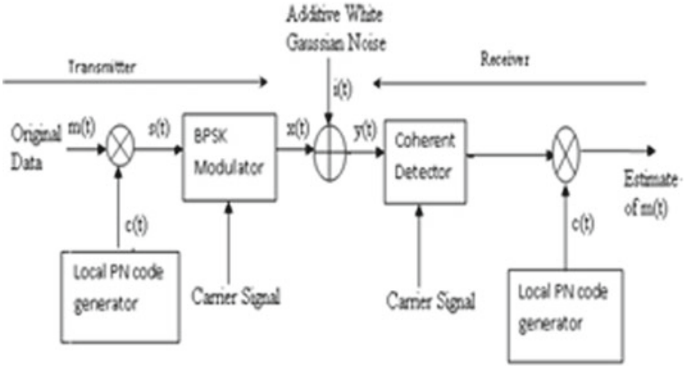


Figure B. DSSS

4 Result Analysis

A. *Signal Generation Using Different Modulation Schemes*

MATLAB is one of the most commonly used programming languages in which different operations are performed on the input data or signals and their functions can be plotted. In order to analyze the difference between a normal frequency mixer and a switching mixer, we have used three kinds of modulation schemes (BPSK, QPSK, and QAM). In BPSK modulation a carrier wave and a binary sequence is multiplied and it is further given as the input. According to the value of the binary input the phase of the output changes from 0° to 180°. In QPSK modulation there is a two-bit input in which the even and the odd bit are separately multiplied by the same carrier. The output signal will have a 90-degree phase shift. In QAM the number of input bits can be two or more. The input signal for each of these schemes was generated respectively. The signal that reaches the mixer usually contains noise as it passes through the receiver channel. Since the input signal is randomly generated and the continuous probability distribution of thermal noise is Gaussian, thus the noise in MATLAB is represented by Additive White Gaussian Noise (AWGN). Noise is added to the transmitted signal and the power spectral density of the noise is constant and has a Gaussian distribution of power spectral density. Inside the mixer the input signal gets multiplied with the LO signal and turns out to give an IF signal as the output. In a normal mixer the LO signal is usually a sine wave whereas in a switching mixer it is a square pulse. On comparing the outputs from the two, it is evident that the switching mixer output contains lesser noise and gives a much better reconstruction of the input signal as compared to the normal frequency mixer.

Figures 2, 3, 4, 5, 6, 7, 8, and 9 represents the time and frequency domain effects of various kinds of modulation schemes. As is the principal objective of the paper, the responses of the modulation exhibited by both the ordinary and switching mixers are compared.

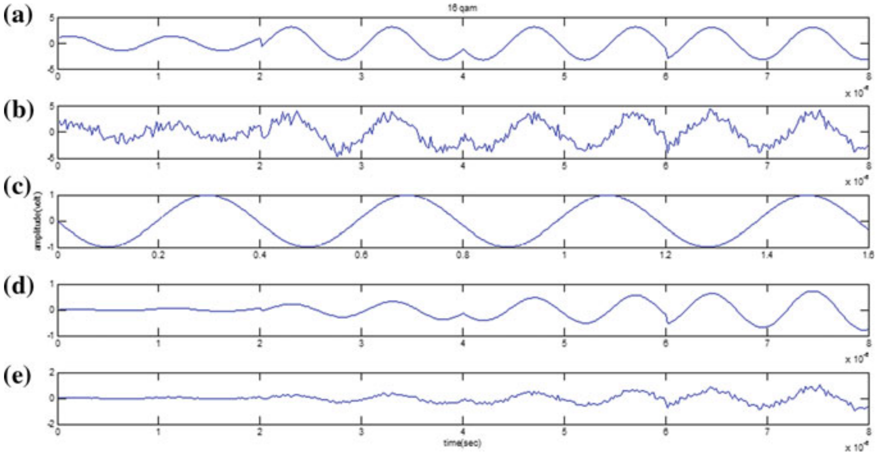


Fig. 2 Time domain analysis of ordinary mixer **a** QAM input signal, **b** input signal with noise, **c** LO signal, **d** mixer output without noise, **e** mixer output with noise

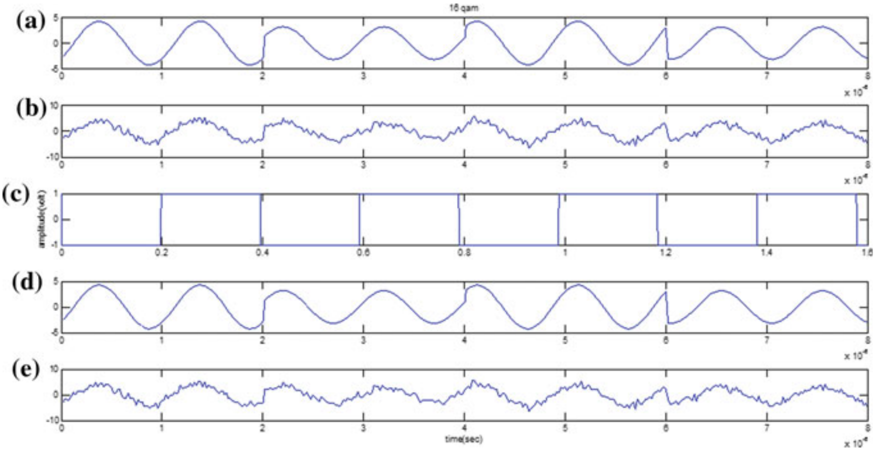


Fig. 3 Time domain analysis of switching mixer **a** QAM input signal, **b** input signal with noise, **c** LO signal, **d** mixer output without noise, **e** mixer output with noise

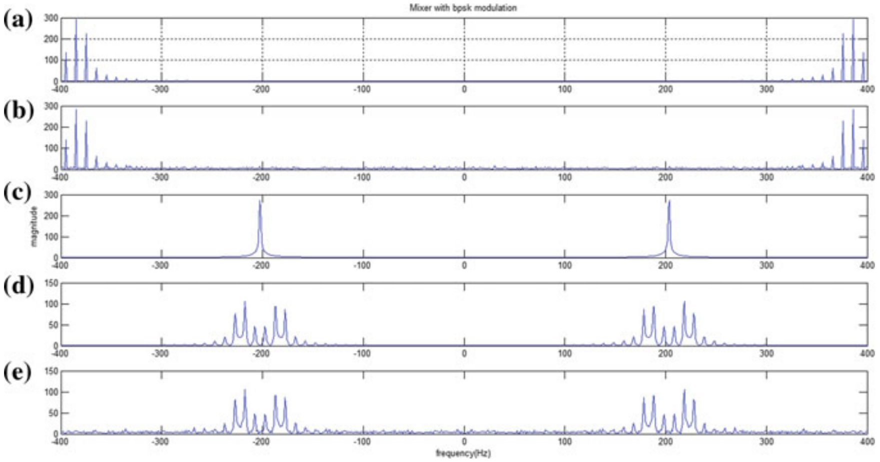


Fig. 4 Frequency spectrum of ordinary mixer **a** BPSK input signal, **b** input signal with noise, **c** LO signal, **d** mixer output without noise, **e** mixer output with noise

B. *Comparison of Responses*

Figures 2 and 3 show the time domain analyses of a QAM modulated signal for ordinary and switching mixers respectively. The output with noise is the last plot in each figure, this is the signal that will be acted upon using spread spectrum techniques to give a noise like appearance. From here on, Figs. 4, 5, 6, 7, 8, and 9 show frequency spectra. Figures 4 and 5 show BPSK modulated outputs with noise for both mixers. Figures 6 and 7 show QPSK modulated outputs for ordinary and switching mixers respectively. It is observed that the switching mixer gives a better amplitude than that

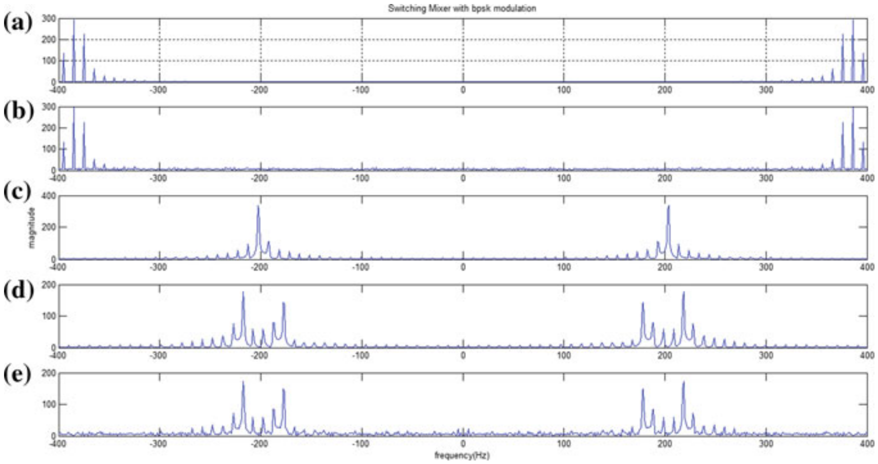


Fig. 5 Frequency spectrum of switching mixer **a** BPSK input signal, **b** input signal with noise, **c** LO signal, **d** mixer output without noise, **e** mixer output with noise

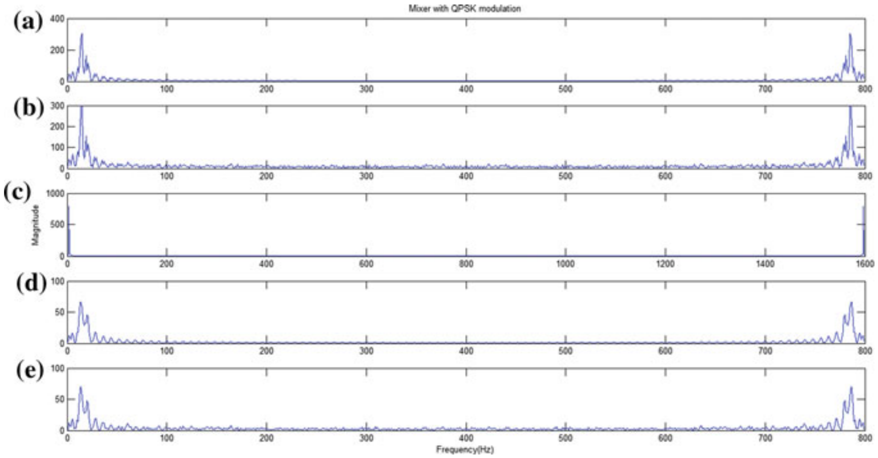


Fig. 6 Frequency spectrum of ordinary mixer **a** QPSK input signal, **b** input signal with noise, **c** LO signal, **d** mixer output without noise, **e** mixer output with noise

of the ordinary mixer. Figures 8 and 9 show frequency responses of QAM modulated signals for both the ordinary and switching mixers, respectively.

The responses show that using a switching mixer will produce better plots attributed to the switching by the local oscillator (LO).

C. *Performance Analysis*

In order to compare the performance of the different modulation schemes, the SNR vs. BER curve is plotted as shown in Figs. 10 and 11. BER gives the number of

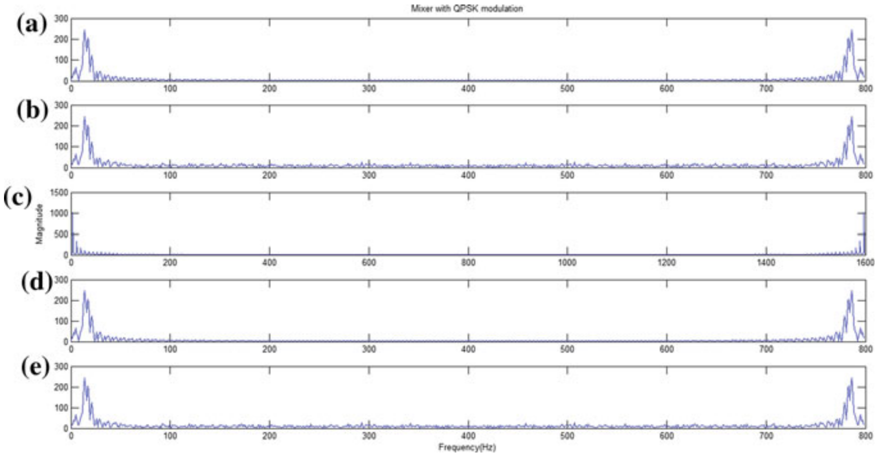


Fig. 7 Frequency spectrum of switching mixer **a** QPSK input signal, **b** input signal with noise, **c** LO signal, **d** mixer output without noise, **e** mixer output with noise

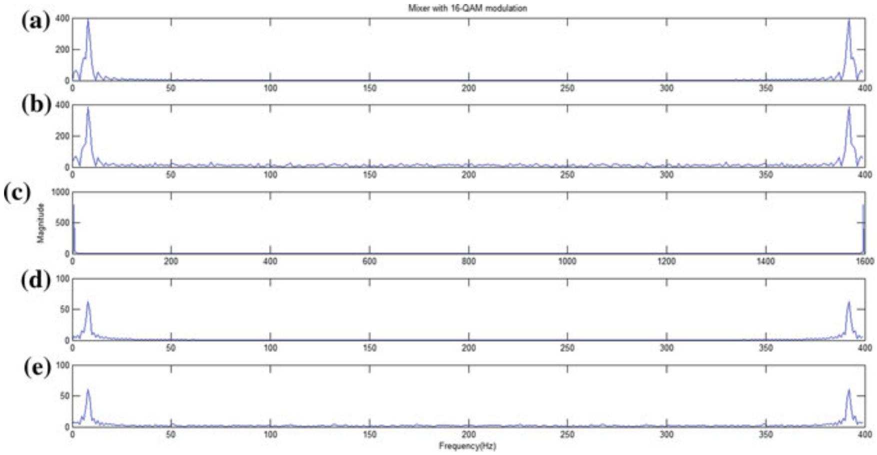


Fig. 8 Frequency spectrum of ordinary mixer **a** QAM input signal, **b** input signal with noise, **c** LO signal, **d** mixer output without noise, **e** mixer output with noise

bits that are in error or have variations due to noise as it passes through the AWGN channel. SNR is a ratio of the signal uncorrupted by noise to the amount of noise present. An increase in the SNR value indicates that there is more of the signal and less amount of noise and a decrease in BER. BER varies for the different modulation schemes. The BER of communication receivers operating in AWGN Monte Carlo Simulations are used. This is commonly used when there is interference from a large number of random variables and at the same time model the probability of different outcomes in a process that cannot be easily determined.

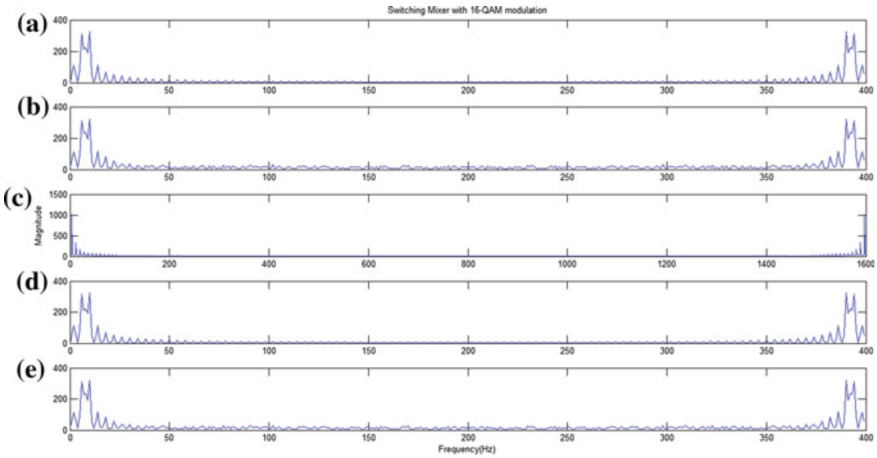
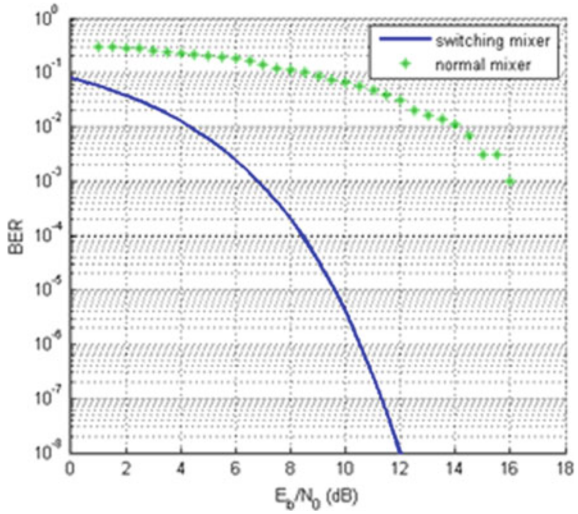


Fig. 9 Frequency spectrum of switching mixer **a** QAM input signal, **b** input signal with noise, **c** LO signal, **d** mixer output without noise, **e** mixer output with noise

Fig. 10 Mixer and switching mixer output for QPSK



D. *Application of Spread Spectrum Schemes*

Frequency Hopping Spread Spectrum (FHSS) is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels, using a pseudo-random sequence known to both transmitter and receiver (as shown in Figure A). The FHSS output is shown in Fig. 12. The spread signal resembles a noise signal, and thus ensures uninterrupted transmission. Inclusion of Additive White Gaussian Noise (AWGN) in the technique creates a noise-like pattern that can trick the intercepting party into thinking that the transmitted signal is just some random noise

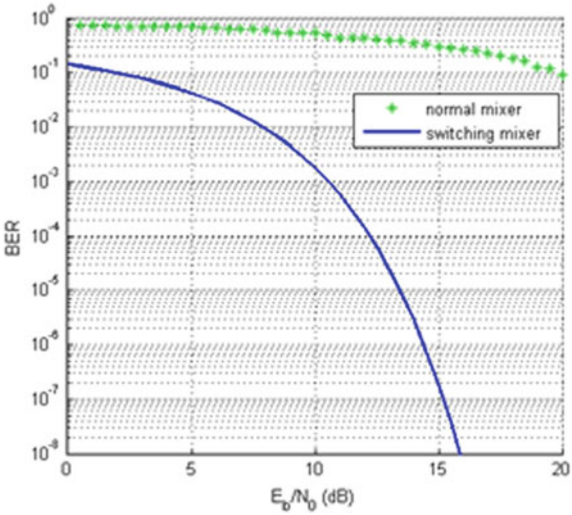


Fig. 11 Mixer and switching mixer output for 16 QAM

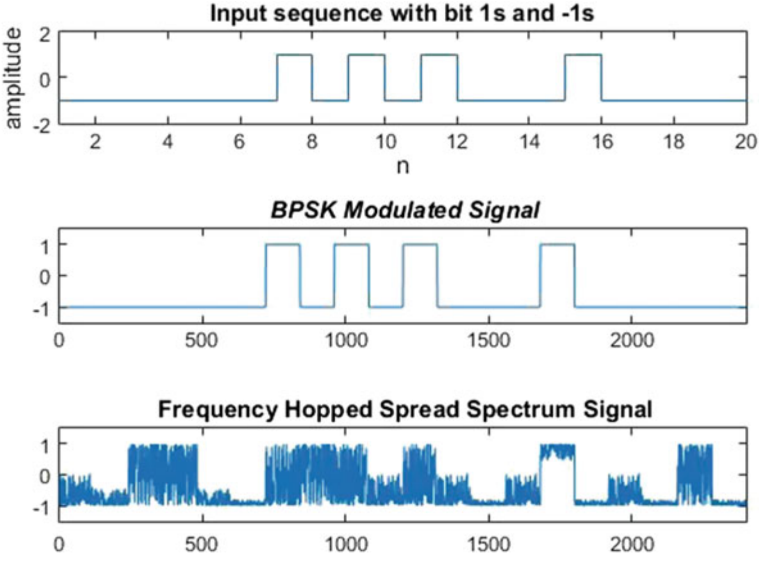


Fig. 12 FHSS spread signal

signal. Direct Sequence Spread Spectrum (DSSS) is a spread spectrum technique whereby the original data signal is multiplied with a pseudo-random noise spreading code (as shown in Figure B). This spreading code has a higher chip rate (this the bit rate of the code), which results in a wide band time-continuous scrambled signal. Figure Fig. 13 shows the reconstructed signal.

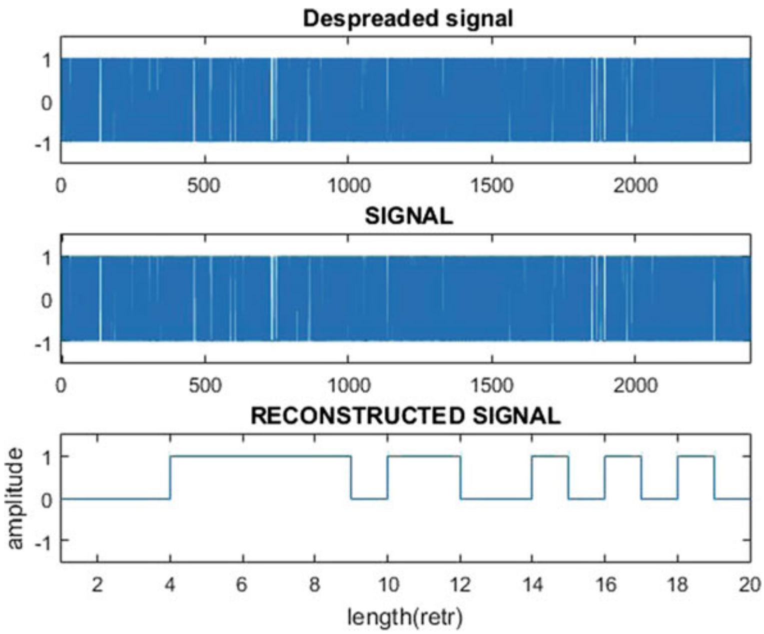


Fig. 13 DHSS spread and reconstructed signal

5 Conclusion

This work aims at simulating the performance of the conventional and switching mixer receivers in communication systems which employ spread spectrum modulation techniques. The simulations were carried out in MATLAB and the objective was verified. It was observed that the BER is higher in the case of the conventional mixer as compared to switching mixer receivers and hence we see that the performance of switching mixer is much more efficient. Thus usage of switching mixers can help achieve better results.

References

1. Marki F, Marki C (2001) T3 mixer primer: a mixer for the 21st century. MarkiMicrowaven, Morgan Hills, CA, http://www.markicrowave.com/menus/appnotes/t3_primer.pdf
2. Amita M, Anjali G, Kurup DG (2015) Combined amplitude and phase noise effects in QAM direct conversion receivers. In: International conference on microwave, optical and communication engineering (ICMOCE), IIT-Bhuvaneshwar
3. Ebrahimzadeh A, Falahati A (2013) Frequency hopping spread spectrum security improvement with encrypted spreading codes in a partial band noise jamming environment. J Inf Secur 4(1):1–6

4. Dou Z, Zhong XK, Zhang WX (2017) Radar-communication integration based on MSK-LFM spread spectrum signal. Int J Commun Netw Syst Sci 10:108–117. https://doi.org/10.4236/ijcns.2017.108B012
5. Motlagh N (2010) Performance improvement of wireless communications using frequency hopping spread spectrum. Int J Commun Netw Syst Sci 3(10):805–810
6. Terrovitis M, Meyer R (1999, June) Noise in current-commutating CMOS mixers. IEEE J Solid-State Circ 34(6):772–783
7. Mahamuni S, Mishra V (2014) Performance evaluation of spectrum detection in cognitive radio network. Int J Commun Netw Syst Sci 7:485–496
8. http://www.radio-electronis.com/info/RF-technology-design/noise/thermal-johnson/nyquist/basics-tutorial
9. http://www.agilent.com/homepagefind/ees of BSIM3 model
10. Sruthi MB, Abirami M, Manikkoth A, Gandhiraj R, Soman KP (2013) Low cost digital transceiver design for software defined radio using RTL-SDR. In: Proceedings—2013 IEEE international multi conference on automation, computing, control, communication and compressed sensing, iMac4 s 2013. Kerala, pp 852–855
11. Lee TH (2004) The design of CMOS radio-frequency integrated circuits, 2nd edn. Cambridge University Press
12. Avantika S, Devika SK, Gomathy V, Manjukrishna SKSA, Kurup DG (2015) Design and experimental characterization of a bandpass sampling receiver. In: International conference on communication systems, ICCS-2015, American Institute of Physics (AIP), Pilani, India

Computationally-Light Metrics to Quantify Link Stability in Mobile Sensor Networks

Natarajan Meghanathan

Abstract We propose three innovative location and mobility-independent computationally-light metrics to quantify the stability of links in mobile sensor networks (MSNs). The proposed metrics (Normalized Neighbor Degree: NND, One Hop Two Hop Neighbors: OTH, and Fraction of Shared and Unshared Neighbors: FSU) are computed on the egocentric network of an edge and the hypothesis is that larger the extent of shared neighborhood between the end vertices of an edge, larger the stability (lifetime) of the link in the MSN. The computation times of all the three metrics are about 15–40 times lower than the computation times of the bipartivity index (BPI) and algebraic connectivity (ALGC) metrics that were adapted from Network Science in an earlier research to quantify link stability in MSNs. The lifetimes of the DG trees obtained with the proposed computationally-light link stability metrics are appreciably larger or comparable to that of the ALGC and BPI-based DG trees.

Keywords Link stability · Computationally-light metrics · Computationally-heavy metrics · Mobile sensor networks · Data gathering

1 Introduction

A mobile sensor network (MSN) is a distributed network of dynamically changing topology and the communication structures of the sensor nodes (like network-wide data gathering trees) need to be frequently reconfigured. In an earlier paper [1] as well as this paper, we address the problem of quantifying the stability of links in a MSN using the neighborhood information of the nodes. In [1], we adapted two Network Science metrics (such as Bipartivity Index: BPI [2] and Algebraic Connectivity: ALGC [3]) and computed them on the egocentric network of an edge [1] to quantify the stability of the edge (also referred to as 'link') in a MSN. The egocentric network of an edge includes the end vertices and their neighbors as *vertices* and the edges

N. Meghanathan (✉)
Jackson State University, Jackson, MS 39217, USA
e-mail: natarajan.meghanathan@jsums.edu

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_23

connecting the end vertices with their neighbors as the *edges*. The lifetimes of the BPI′ (=1 − BPI) based data gathering (DG) trees were observed [1] to be significantly larger than those of the predicted LET (link expiration time [4, 5], adapted from mobile ad hoc networks [6])-based DG trees.

Prior to [1], the LET approach [4, 5] was the only well-known approach to determine stable DG trees in MSNs. However, the LET metric requires the mobility and location information of the nodes. Other relevant approaches (such as self-healing [7]) proposed in the literature of wireless networks also cannot be adapted for MSNs as these would also require the location information of the nodes. On the other hand, one does not require the mobility and location information of the nodes to compute the BPI′ and ALGC metrics. However, a major weakness of these two metrics is that they are computationally-heavy and could impose a significant burden on the resource-constrained sensor nodes. Hence, the motivation is to develop computationally-light metrics (that are also location- and mobility-independent, like BPI′ and ALGC) to quantify the stability of links in MSNs. Our hypothesis is that the link whose end vertices are closer is likely to be more stable (i.e., exist for a longer time) than the link between two end vertices that are farther away from each other. The above hypothesis was observed to be true [1] for both BPI′ and ALGC, and we anticipate it to hold true for the computationally-light link stability assessment metrics proposed in this paper.

The rest of the paper is organized as follows: Sect. 2 introduces the three computationally-light metrics to quantify the stability of a link in a MSN. Section 3 presents simulation results for computation times incurred with the five metrics (including BPI′ and ALGC), explores the rank-based correlation between the computationally-light and computationally-heavy metrics and compares the DG tree lifetimes incurred using the link stability scores quantified using these metrics. Section 4 summarizes the contributions of this work and concludes the paper. Throughout the paper, we interchangeably use the terms: ‘link’ and ‘edge’, ‘node’ and ‘vertex’, ‘network’ and ‘graph’. They mean the same.

2 Metrics to Quantify Link Stability

Our hypothesis is that larger the extent of shared neighborhood between the end vertices of an edge (u, v), the larger the stability of the link (edge). We use the notion of “egocentric network of an edge” proposed in our earlier work [1] for all the analysis. From notation point of view, for an edge (u, v): let $N(u)$ represent the set of neighbors of a vertex u and let $Ego_N(u, v)$ represent the set of vertices (vertices u, v and their neighbors, with each vertex, represented exactly once) that are part of the egocentric network of the edge.

2.1 Normalized Neighbor Degree (NND)

For an edge (u, v), its NND (see formulation 1 below) is the ratio of the square root of the sum of the squares of the degrees of the neighbor nodes and the number of neighbor nodes in its egocentric edge network. The neighbor nodes of the end vertices u and v in the egocentric network of edge (u, v) could have a degree of either 1 or 2. If a neighbor node has degree 2, it implies the node is a neighbor of both u and v and is part of the shared neighborhood. If a neighbor node has degree 1, then the node is not part of the shared neighborhood. Hence, the larger the number of neighbor nodes with degree 2, the larger the extent to which the neighborhood is shared.

$$\mathrm{NND}(u, v) = \frac{\sqrt{\sum_{i \in \mathrm{Ego}_N(u,v)-\{u,v\}} k_i^2}}{\left|\mathrm{Ego}_N(u, v) - \{u, v\}\right|} \qquad (1)$$

2.2 One Hop Two Hop (OTH) Neighborhood

For an edge (u, v), its OTH is computed on the basis of the number of one hop and two hop neighbors of the end vertices u and v in its egocentric edge network. From the point of the end vertices u and v, it is desirable that all the vertices in $\mathrm{Ego}_N(u, v)$ be their one hop neighbors. However, if a vertex in $\mathrm{Ego}_N(u, v)$ is not present in the neighborhood of either u or v, then it becomes a two hop neighbor of the corresponding end vertex. The presence of two hop neighbors in an egocentric edge network decreases the extent with which the neighborhood is shared; on the other hand, the presence of one hop neighbors increases the extent of shared neighborhood. We propose an auxiliary metric called *weighted neighborhood hop* count (WNH) as a weighted sum of the one hop and two hop neighbors of the end vertices u and v (see formulation 2). As seen in the WNH formulation for an end vertex, we complement the end vertex for having one hop neighbors and penalize for having two hop neighbors (by a factor of 2). In other words, the presence of two hop neighbors is modeled to weaken the stability of the neighborhood and negate the advantage that comes with the presence of one hop (shared) neighbors.

We opine the sigmoid function (typically used in the formulation of the cost function for logistic regression [8] or artificial neural networks [9]) to be an appropriate function to introduce the needed non-linearity (a stronger decay or a stronger ascent even for egocentric edge networks with moderate differences in the number of one hop and two hop neighbors) that is not incorporated in the WNH linear formulation. The OTH for an edge (u, v) is thus computed using a sigmoid formulation (see formulation 3) involving the WNH scores of u and v. Also, a sigmoid formulation will transform the input (WNH values) to an output that is confined in the range of (0, …, 1).

$$
\begin{aligned}
\mathrm{WNH}(u) &= |N(u)| - 2 * \left|\mathrm{Ego}_N(u, v) - N(u)\right| \\
\mathrm{WNH}(v) &= |N(v)| - 2 * \left|\mathrm{Ego}_N(u, v) - N(v)\right|
\end{aligned}
\tag{2}
$$

$$
\mathrm{OTH}(u, v) = \frac{1}{1 + \mathrm{e}^{-(\mathrm{WNH}(u)+\mathrm{WNH}(v))}} \tag{3}
$$

2.3 Fraction of Shared and Unshared (FSU) Neighbors

For an edge (*u*, *v*): let f_u^{shared} and f_u^{unshared} denote respectively the fraction of shared neighbors and fraction of unshared neighbors among the neighbors of vertex *u*; likewise, let f_v^{shared} and f_v^{unshared}, respectively denote the fraction of shared and unshared neighbors of vertex *v*. The fraction of shared neighbors for an end vertex *u* (or *v*) in an edge (*u*, *v*) is the ratio of the number of neighbors that are shared by both the two end vertices *u* and *v* and the number of neighbors of the end vertex *u* (or *v*), excluding the other end vertex *v* (or *u*). Likewise, the fraction of unshared neighbors for an end vertex *u* (or *v*) in an edge (*u*, *v*) is the ratio of the number of neighbors of *u* (or *v*) that are not shared with the other end vertex *v* (or *u*) and the number of neighbors of the end vertex *u* (or *v*), excluding the other end vertex *v* (or *u*). We define an auxiliary metric called "shared unshared ratio (SUR)" as shown in formulation (4) that is in turn used to compute the FSU metric for edge (*u*, *v*): see formulation (5). The SUR ratio values could range from −1 to 1; the FSU formulation basically transforms the SUR values to a scale of 0 to 1.

Like in the case of WNH metric (see above), we can notice in the formulation for SUR(*u*, *v*) that the presence of unshared neighbors for a vertex could be considered to negate the advantages that come with the presence of shared neighbors. However, the difference lies in the extent of penalty given for the presence of unshared neighbors. The SUR/FSU metric uses a linear penalty alone, whereas the WNH/OTH metric incorporates both linear and non-linear penalties.

$$
\mathrm{SUR}(u, v) = \frac{\left(f_u^{\text{shared}} + f_v^{\text{shared}}\right) - \left(f_u^{\text{unshared}} + f_v^{\text{unshared}}\right)}{\left(f_u^{\text{shared}} + f_v^{\text{shared}}\right) + \left(f_u^{\text{unshared}} + f_v^{\text{unshared}}\right)} \tag{4}
$$

$$
\mathrm{FSU}(u, v) = \left\{\frac{1 + \mathrm{SUR}(u, v)}{2}\right\} \tag{5}
$$

3 Simulations

We conducted exhaustive simulations to evaluate the following aspects with respect to the proposed computationally-light metrics (vis-a-vis BPI′ and ALGC) to quantify link stability as a measure of the extent with which the neighborhood is shared: (1) Computation time (2) Correlation (3) Stability of DG trees. The node mobility model used is the Random Waypoint model [10]; the maximum velocity ($v_{\max}$) of the nodes is varied with values of 1 m/s (low mobility), 5 m/s (low-moderate mobility), 10 m/s (moderate-high mobility) and 30 m/s (high mobility). The number of nodes is varied with values of 50 (low density) and 100 (high density). We generated 100 mobility profile files for each of the above combinations of node mobility and density scenarios, with the simulation time being 1000 s. We averaged the results for the following for each of the above scenarios and each of the five metrics: (1) the Computation time (on a per-edge basis); (2) the Spearman's correlation coefficient (at randomly sampled time instants in the mobility profile files) between any two of the five metrics; (3) the lifetime of the DG trees. The computer on which the simulations are ran is a Dell workstation with Intel i-2620 M CPU @ 2.70 GHz and 8 GB RAM.

3.1 Computation Time

Table 1 presents the average computation times (in microseconds) to determine the link stability score for an edge with respect to each of the five metrics. For this purpose, we sampled a total of 1000 randomly chosen edges in the network at randomly chosen time instants in each of the 100 mobility profile files and averaged the computation times. The OTH metric incurs the lowest computation time for both low-density and high-density networks. The computation times for the FSU metric has been observed to be slightly larger than the OTH metric. The NND metric incurs the largest computation time among the three computationally-light metrics proposed in this research. The computation times for the NND metric are about 2–3 times larger than the computation times of the OTH and NND metrics. The computation time for the ALGC metric is the largest among all the five location and mobility-independent

Table 1 Computation times (in microseconds) for the link stability metrics

Condition	BPI′	ALGC	NND	OTH	FSU
50 nodes, $v_{\max} = 10$ m/s	38.177	42.643	6.514	2.450	2.771
50 nodes, $v_{\max} = 30$ m/s	36.255	39.889	6.181	2.419	2.596
100 nodes, $v_{\max} = 10$ m/s	83.839	93.825	4.902	1.967	2.062
100 nodes, $v_{\max} = 30$ m/s	79.574	89.133	4.960	1.881	2.230

metrics. Between BPI′ and ALGC, for a given node velocity: the difference in the computation times increases as the node density increases.

The computation times for BPI′ and ALGC are about 15 and 40 times larger than that of OTH and FSU in low-density networks and high-density networks, respectively. For a given node velocity, the computation times for BPI′ and ALGC almost double (i.e., increase by a factor of 2 or more) as the number of nodes is increased from 50 to 100. On the other hand, for a given node velocity, the computation times for the three computationally-light metrics (NND, OTH, and FSU) decreases (by about 20–25%) as the number of nodes is increased from 50 to 100. As a result, we can say that the time savings obtained with the computationally-light metrics (vis-a-vis the computationally-heavy metrics) increase with increase in node density.

3.2 Rank-Based Correlation

We determined the Spearman's rank-based correlation coefficient values [11] for the edges between the computationally-heavy versus computationally-light link stability metrics for every second during the simulation time of 1000 s in each of the 100 mobility profile files and averaged these correlation coefficient values for each pair of the link stability metrics (as reported in Table 2). For each of BPI′ and ALGC, we identify the computationally-light metric for which the largest value for the correlation coefficient is obtained (the entries in Table 2 are shaded). We observe BPI′ to be very strongly correlated with OTH for all the four scenarios (in each case, the correlation coefficient is above 0.90). We thus establish OTH to be a computationally-light alternative to rank the edges in lieu of the computationally-heavy BPI′. In the case of ALGC, it is strongly correlated with NND in low-density scenarios and with FSU in high-density scenarios. The ALGC-FSU correlation in high-density scenarios is more stronger than the ALGC-NND correlation in low-density scenarios. For a given node mobility, with increase in node density, the correlation coefficients associated with ALGC increase and the correlation coefficients associated with BPI′ decrease.

Table 2 Spearman's rank-based correlation coefficient between computationally-heavy versus computationally-light link stability metrics

Scenarios		NND	OTH	FSU
50 nodes, $v_{\max} = 10$ m/s	BPI′	0.3283	0.9566	0.9260
	ALGC	0.8029	0.7183	0.7766
50 nodes, $v_{\max} = 30$ m/s	BPI′	0.2985	0.9514	0.9287
	ALGC	0.7946	0.7389	0.7878
100 nodes, $v_{\max} = 10$ m/s	BPI′	0.2583	0.9252	0.8444
	ALGC	0.8168	0.8185	0.9051
100 nodes, $v_{\max} = 30$ m/s	BPI′	0.2414	0.9291	0.8487
	ALGC	0.8045	0.8158	0.9054

3.3 Data Gathering Tree Lifetime

In Fig. 1, we report the normalized values of the DG tree lifetimes (normalized using the square root of the sum of the squares of the raw lifetime values) incurred with the five metrics. The lifetimes of the DG trees determined based on each of the three computationally-light metrics are greater than that of the ALGC-based DG trees. Between BPI′ and ALGC, the BPI′-based DG trees incurred the largest lifetime for both networks of low density and high density. The largest tree lifetimes incurred with the {NND, OTH, FSU} metrics are very much comparable with the largest tree lifetimes incurred with the {ALGC, BPI′} metrics. The maximum difference in the tree lifetimes could be observed in the low mobility and high-density scenario ($v_{\max} = 1$ m/s and 100 nodes). For a given mobility level of the nodes, the DG tree lifetimes for all the five metrics increases with increase in network density, due to the increase in the extent of shared neighborhood (and thereby an increase in the stability of the links). Among the three computationally-light metrics, the OTH-based DG trees incurred the largest lifetime in low-density networks that is almost the same (or even sometimes larger) as the lifetime of the BPI′-based DG trees. The FSU-based DG trees incurred the largest lifetime in high-density networks that is also almost the same (or even sometimes larger) as that of the BPI′-based DG trees. Thus, the OTH and FSU metrics could, respectively, be computationally-light alternatives for BPI′ in low and high-density networks.

Note that a common theme among the BPI′, OTH and FSU metrics is that they follow the strategy of penalizing the link stability score (LSS) of an edge if its egocentric network comprises of unshared neighbors and rewarding if the egocentric network comprises of shared neighbors. The relatively larger normalized lifetime values for the BPI′, OTH, and FSU-based DG trees (vis-a-vis the ALGC and NND-based DG trees) could be attributed to such a combined strategy of rewarding as well as penalizing the LSS scores of the edges depending on the extent of shared and unshared neighborhoods, respectively. On the other hand, the ALGC and NND metrics follow the strategy of just rewarding the LSS score of an edge if it comprises

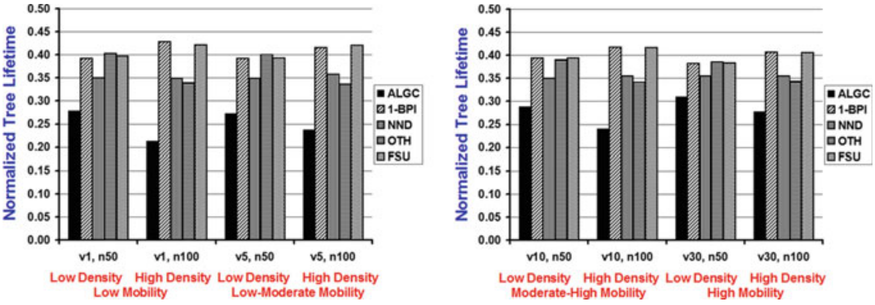


Fig. 1 Normalized lifetime of the data gathering trees with respect to link stability metrics

of egocentric networks with shared neighborhood and not penalizing if the egocentric networks comprise of unshared neighborhood.

4 Conclusions and Future Work

We have developed three computationally-light metrics (NND, OTH, and FSU), two of which are shown to be potential alternatives (OTH and FSU) to the computationally-heavy metrics BPI′ and ALGC. The computation times of BPI′ and ALGC are 15–40 times larger than that of OTH and FSU (the difference increases with increase in node density). On the other hand, we observe strong-very strong positive correlation (for ranking the edges) between OTH and BPI′ as well as between FSU and ALGC. The lifetimes of the data gathering (DG) trees determined using the OTH and FSU metrics (as the link stability scores) are observed to be as large as those determined using the BPI′ metric in low-density and high-density networks, respectively. In an earlier research [1], the BPI′ metric was observed to determine the most stable DG trees for mobile sensor networks (when compared to the use of the predicted link expiration time, LET [4, 5]). Thus, we are very confident to have identified two computationally-light metrics based on the extent of shared neighborhood to quantify link stability in mobile sensor networks. In future, we plan to predict the actual BPI′ values for the links using their OTH and FSU values itself so that we could determine BPI′-based DG trees by avoiding a heavy computation overhead. We also plan to incorporate computationally-light secure encryption techniques (like [12]) to exchange the neighborhood information of the nodes for building the egocentric edge networks.

References

1. Meghanathan N (2018) Complex network analysis-based graph theoretic metrics to determine stable data gathering trees for mobile sensor networks. Comput J 61(2):199–222
2. Estrada E, Rodriguez-Velazquez JA (2005) Spectral measures of bipartivity in complex networks. Phys Rev E 72(046105):1–6
3. Fiedler M (1973) Algebraic connectivityh of graphs. Czechoslov Math J 23(98):298–305
4. Meghanathan N (2012) Link expiration time and minimum distance spanning trees based distributed data gathering algorithms for wireless mobile sensor networks. Int J Commun Netw Inf Secur 4(3):196–206
5. Su W, Gerla M (1999) IPv6 flow handoff in Ad hoc wireless networks using mobility prediction. In: IEEE Global Telecommunications Conference, pp. 271–275. IEEE Press, New York
6. Abolhasan M, Wysocki T, Dutkiewicz E (2004) A review of routing protocols for mobile ad hoc networks. Ad Hoc Netw 2(1):1–22
7. Smys S, Raj JS (2015) A self-organized structure for mobility management in wireless networks. J Comput Electr Eng 49C:153–163
8. Osborne J (2014) Best practices in logistic regression, 1st edn. Sage Publications, Thousand Oaks
9. Agarwal CC (2018) Neural networks and deep learning strategies, 1st edn. Springer, Berlin

10. Bettstetter C, Hartenstein H, Perez-Costa X (2004) Stochastic properties of the random-way point mobility model. Wirel Netw 10(5):555–567
11. Strang G (2016) Introduction to linear algebra, 5th edn. Wellesley-Cambridge Press, Wellesley
12. Praveena A, Smys S (2016) Efficient cryptographic approach for data security in wireless sensor networks using MES V-U. In: 10th international conference on intelligent systems and control, pp 1–6. IEEE Press, New York

MockRest—A Generic Approach for Automated Mock Framework for REST APIs Generation

Anshu Soni, Virender Ranga and Sandeep Jadhav

Abstract Mock is an object that replicates the behavior of a real object in a disciplined way and improves unit testing. Unit testing is a testing where each individual or component is tested. The purpose of unit testing is to validate each unit of designed software and allow to verify the generated code is working properly, regardless of its dependencies. A system under test has some external dependencies like APIs and creating a mock object based on that kind of dependencies would be efficient rather than generate a test case on the actual instance of the dependencies. A real working system such as banking, autonomous vehicles, online-supply chain businesses, and E-commerce platforms are heavily dependent on a server and facing difficulty while testing with a real server. Mock server helps in testing by simulating the behavior of a real server. Mocks could be used for testing and developing the front-end even when the back-end is not available. The aim of our research work is to propose a generic approach in which we propose a mock framework named MockRest for REST API in Java. The main reason to propose such kind of framework is to get a consistent response while real API is down at the moment by creating a mock of REST API as it allows the developer to stay constructive while the API is being implemented. Application Programming Interface (API) allows interaction between software programs, exchanges their information while REST is an architectural style, and applies to the design of API. A Web API that follows the standards of REST architectural style is a REST API. Based on the description of Web services by its interface, Mock simulates its behavior.

Keywords MockRest · Mock · REST API · Unit testing · Framework · WireMock · SOAP UI · Jersey · JAX-RS · Tomcat · JAXB

A. Soni (✉) · V. Ranga
National Institute of Technology, Kurukshetra, Haryana, India
e-mail: anshusoni1995@gmail.com

V. Ranga
e-mail: virender.ranga@nitkkr.ac.in

S. Jadhav
KPIT Technologies Limited, Pune, Maharashtra, India
e-mail: sandeep.jadhav@kpit.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_24

1 Introduction

Unit testing targets to test a single unit of a program individually. It is difficult to test in isolation as code can interact with external dependencies such as a server, database, and API. For example, test a unit that interacts with external dependencies, which requires "real" file to be existed or to be created in order to ensure unit testing. A Java Web application consists of two constituents—front-end and back-end server. Both are dependent on each other and run simultaneously. The front-end developer depends on the back-end for a server, third-party APIs, database, and other external services required. For effective and efficient testing, a major challenge is to handle the various dependencies such as external data, third-party services, and external libraries. In unit testing, tester tests the software component without incorporation of external dependencies. In a real, system such as banking, autonomous vehicles, online-supply chain businesses, and E-commerce platforms exchanges their data through a server and a database where customer services are handled by a different server, and admin handled their services through another server. It would be burdensome for tester as well as for a developer to do testing. During the development phase, in order to ensure test with a real server, it would be difficult to evaluate test cases by a tester or a developer. So, to provide effective testing, there is a requirement of a mock server. It will remove the dependency on a real server and allows testing by the developer itself. Figure 1 gives a visual representation of a mock server in place of a real server. Client or any Web application sends HTTP request to the real server and server return HTTP response get back to the client over the Internet. Now, in order to effectively utilize our time and improve testing mechanism, there is a requirement of a mock server that behaves as a real server and mimics its dependencies. In order to simulate external dependency and model the environment, developers can create a mock.

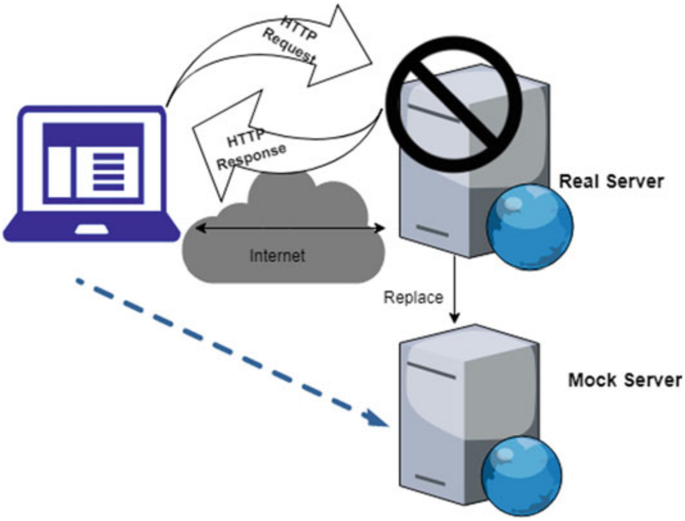


Fig. 1 Mock server

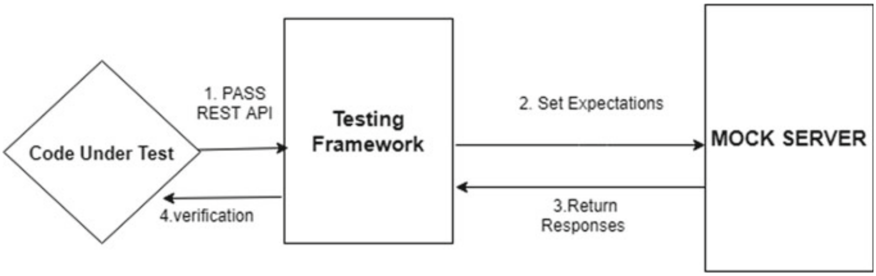


Fig. 2 Mock server

Mock objects can be used to reconstitute the real software dependencies by mimicking the admissible feature of software dependency. Reduction of time takes place while testing software development by the creation of mock objects. Some of the mocking frameworks available to unit test java application are Jmock, Mockito, and EasyMock.

REST stands for "Representational State Transfer," an architectural style for developing Web services. API is a software intermediary that allows two applications to talk to each other. RESTful Web services in Java applications have been developed by JAX-RS with jersey.

When front-end and back-end developers work parallelly, then front-end developer needs mock responses even API is not available or not implemented yet. By mocking REST API, simply means creating a mock server which returns pre-defined responses and other parameters such as status codes and headers on matching request by the client.

This research paper proposes a framework of our generic approach that generates a mock of REST API. Wiremock and SoapUI are the existing tools available generating REST API mock, but they have some limitations as they are not creating mock responses as many REST APIs simultaneously, and generate stub responses. There is a lack of study that explores REST API mock creation; this paper gives an idea of framework creation for mock REST API. Figure 2 shows the behavior of mock server.

As discussed above a generic idea of mock server and the basic steps used to implement a mock server is shown below:

1. Pass the REST API to the framework that is created with the code.
2. Expectations can be set in the mock server according to our requirements.
3. Mock server returns responses according to the API defined and pre-defined responses.
4. Finally, code under test verifies the responses by the mock server without including dependency of real server.

2 Related Work

Mock object is a technique that assists unit testing by simulating the real object. Thomas et al. [1] is the well-known literature about mock objects. This paper demonstrates the usage of mock objects. These mock objects can be used when real objects have non-deterministic behavior, difficult to set up, has a user interface. When a real object does not exist yet, then there is a need of mock objects.

Kim et al. [2] identify a mock object model for test-driven development(TDD). They identify the features and limitations of the existing mock object model and propose a new model to overcome limitations of previuos proposed work.

Spadini et al. [3] observe why developers apply mock objects after conducted a survey over 105 developers from software testing communities. They have done interviewed of developers to understand why some dependencies were mocked and some are not as well creation of MockExtractor,a tool that extracts a list of mocked and non-mocked dependencies in test suites. We have observed the following facts after doing the literature review thoroughly:

- Database, Web services, and external dependency are mocked dependencies. Domain objects are only ∼36% mocked.
- In integration testing, mock is not used.
- Interfaces are mocked so that there is no need to depend on specific implementations.
- Test support and Java libraries are not mocked.

While creating mock, developers faced most of the challenges that are maintaining mock behavior of original class along with its compatibility. Mocking with legacy system (where architecture is not well developed) is the major challenge.

Mostafa et al. [4] have given a study on four most popular mocking frameworks, i.e., EasyMock, Mockito, JMock, JMockit by considering 5000 Github open-source software projects. They have also found out that how developers have used mocking frameworks in open-source software projects. They have shown that 23% of software projects used mocking frameworks.

Singhal et al. [5] propose an approach that quickly generates a mock in front-end that behaves exactly like an actual back-end. It makes front-end and back-end developer independent and utilizes their time effectively.

Ashikhmin et al. [6] describe a architecture and its implementation which can generate mock services based on RAML specification and deploy with Docker container. Define Gateway, Request validator, Path Resolver, and Response Generator are the four components in mock services as well give an overview of microservices.

Adamczyk [7] distinguishes two architectural styles REST and SOAP and explains briefly about the RESTful Web services and demonstrates four principles of REST coined by Roy Fielding based on a survey of existing Web services.

Simple rules have been defined to design Web services as discussed in [8]. The authors also discuss why REST API should be designed and configured and define the tips to address the client's needs.

Kao et al. [9] introduce the performance testing framework for REST-based Web applications and provide software tester an integrated process from test case design, generation of test scripts to the execution of tests. This framework decreases the effort to understand the design and implementation of application.

Haupt et al. [10] provide a framework for structural analysis of REST APIs which consists of metrics and graphical representation of APIs. They also convert the description of REST API, present in different languages into a canonical model that describes the structure of REST API explicitly.

Ed-douibi et al. [11] focus on REST API automated test case generation by using OpenAPI for automatic REST API development. They have proposed an approach to generate test cases automatically and test API specifications according to the requirements and provide a tool for testing 91 OpenAPI specifications. They conclude that 41% test APIs are failed. Their approach depends on a model-based procedure to automate test case generation.

Arcuri [12] considers the testing at the development phase by the developers having full code access. They have proposed an approach that uses an evolutionary algorithm for automatic test case generation based on white-box testing approach. They have done their experiments of proposed approach on EvoMaster, open-source tool.

Munonye and Martinek [13] analyzed the performance of REST Web services based on Java and .Net implementations and concluded their performance. On various test scenarios, they found that Java-based Web services perform better for GET method around 80.36%, and .Net performs better for PUT method and performance is 11.6% lower. They came across the conclusion that Java-based Web services should be used on business-to-business purposes while .Net-based Web services preferable on forms updating applications having user involvement regular update and deletion takes place.

Sinha et al. [14] scrutinize a new approach for application integration on cloud with REST Web services.

Giessler et al. [15] identify best practices for developing REST services and clarify the usage of Web services on different applications. This paper illustrates eight different categories of Web services and 23 best practices.

Qiu et al. [16] simplify the usage of API in Java programming language. They discuss how API engages in software projects. They have done the empirical analysis on 5000 open-source Java projects, understand the core API and third-party API in Java, knowing the concept of API libraries. They conclude that core API is not widely used, most of the APIs that are deprecated are still used.

3 Background Study

3.1 Unit Testing

A chunk of code written by a developer that handles a very tiny, specific area of code being tested comprises unit testing [17]. Unit testing basically done over different methods or classes. It is done to prove that chunk of code does exactly what developers think. It should be done over all modules independently before two modules combine together. Will make developer's life easier by reducing the amount of time spent on debugging. Use assertion to check whether a chunk of code behaves exactly as a developer wants. An assertion is a method that verifies whether testing statement returns true or not. For the Java programming language, JUnit framework is used. There are frameworks available for Java are NUnit, TestNG, and many more. Many assert methods available in JUnit library like

assertEquals(String[message],expected,actual),

assertTrue(string[message],boolean condition) and much more.

The objective of the testing is to exercise one method at a time, but when method depends on the external database, third-party APIs, then there is a need of mock objects to reduce time handling these external services. Figure 3 shows a flow chart of unit testing and our focus on testing with mock.

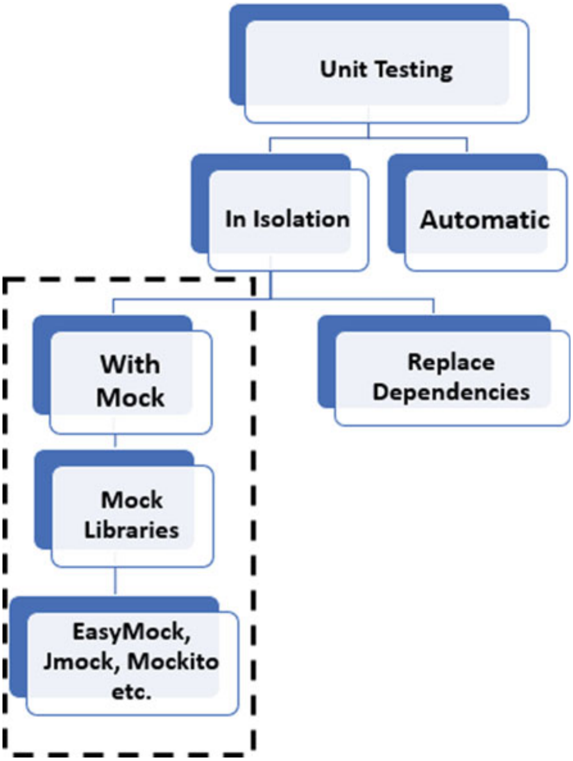
3.2 Mock Objects

Mock objects are referred to as a simulated object that simulates the nature of real objects in a disciplined way. To simulating the required environment, mock objects [17] are required. It is essential for test case generation. EasyMock, Mockito, PowerMock, and JMock are the Java mocking frameworks available. The purpose of a mock object is to enable unit testing by testing the code if it has interaction with external dependencies by simulating them.

Interfaces are the basic concept in object-oriented systems. Interfaces are language constructs that contain only a set of methods signature, expected behavior of the object, does not contain any implementation details [18]. Their implementation is defined by its class. The system adopts interfaces have three characteristics: Flexibility, Extensibility, Pluggability.

For unit testing, mock objects can be used in place of real objects by simulating the interfaces required. Mocks are easiest to use while interface-based design systems. Test suites and domain code can be improved by mock objects used in unit testing. Term Endo-Testing [19] have been announced, in which code has been tested from inside where mock objects are passed to the target domain code. Mock objects are the good technique to make testing easy for developers without interfering with external dependency, third-party server when they are not available and not yet been implemented. There is some pattern to be followed for unit testing with mock objects:

Fig. 3 Unit testing flow diagram



- Build an instance of mock object.
- Define states of mock objects.
- Prescribed expectations, responses in mock objects.
- Set mock object as parameter under domain code.
- Verify mock objects under testing.

3.3 REST API

An architectural style for developing Web services is REST(Representational State Transfer) was first conferred by Roy Fielding in 2000. It defines a set of constraints for developing Web services. Fielding [20] defines seven constraints described below in their dissertation report:

- **Starting with NULL style**: It is an empty set of constraints. It is the starting point to describe REST.
- **Client—Server**: separation of client and server architectural style to evolve independently of each other, thus improves the portability under user interface and scalability by facilitating server components.

- **Stateless**: Communication between client and server must be stateless. Any request of the client will not be saved. No session nor history be made of a client request. Management of resources is not required. This constraint brings about the properties of scalability, visibility, and reliability.
- **Cache**: To improve network efficiency, cache constraint is added between client and server communication. This constraint requires that response is declared as cacheable or non-cacheable explicitly or implicitly. Cacheable response requires the client to reuse the response. Caching improves the performance over client-side and scalability be improved over server-side.
- **Uniform Interface**: REST architectural style different from other network style is through uniform interface constraint. It decouples and simplifies the architecture, which enables to evolve independently. Four interface constraints have been defined, i.e., identification of resources, manipulation of resources through representations, self-descriptive messages, and hypermedia as the engine of application state (HATEOAS).
- **Layered System**: To improve Internet-scale requirements, the layered constraint has been added. In this, architecture is composed of hierarchical layers so that each component was not able to view beyond the immediate layer toward they were connected. A layered constraint is applied to enclose legacy services. The disadvantage over this system is that it increases the overhead and delay to the data processing.
- **Code-on-demand**: Functionality be added under REST to downloading and executing code. It allows the client to reduce features that would be needed to be pre-implemented. This constraint improves system extensibility.

API (Application Programming Interface) acts as an interface that allows communication between two software programs. API that uses HTTP protocol for interaction between different programs are Web services. Basically, the interaction of Web services is the request and response type between client and server. An API follows REST rules or standard for creating Web services, which are REST API. REST is an architectural style, not a protocol that develops over HTTP. For request and response, REST [11, 12] uses HTTP (HyperText Transfer Protocol) to define the desired action. To allow communication, there are resource methods or request types available:

- GET: Retrieve resource information.
- POST: Create new resource.
- PUT: Update the existing resource.
- DELETE: Delete the existing resource.

Figure 4 represents REST API workflow following HTTP methods and returns response to clients in JSON/XML format. HTTP methods described above can be safe and idempotent [15] as well.

Table 1 exhibits the properties of HTTP methods which are idempotent and safe. Idempotent methods are those HTTP methods that can be called as many times without any effect on stored data, whereas safe methods are those HTTP methods which do not update the resources, these methods are read-only.

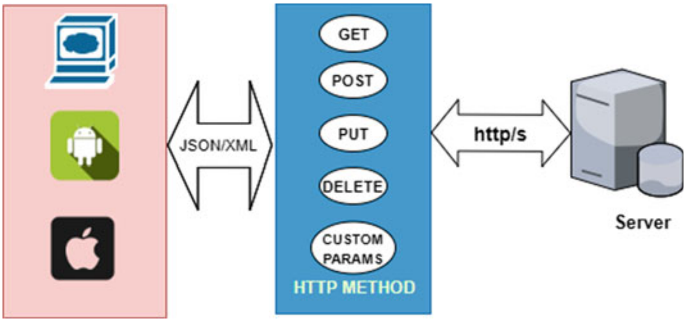


Fig. 4 REST flowchart

Table 1 Properties of HTTP Methods

HTTP methods	Idempotent	Safe
GET	Yes	Yes
POST	No	No
PUT	Yes	No
DELETE	Yes	No

The representation of state can be in JSON or XML format. Usually, today most preferable response format will be in JSON format. There is some structure [8] that is to be followed while creating a REST API.

- Base URI: To identify resources Uniform Resource Identifier(URI) be used.
  Example: http://api.example.com
  URI format:
  scheme"/"authority"/"path["?"query]["#"fragment]
- Resource modeling: Representation of data is called resource. It can be a singleton or can be a collection, and it may contain sub-resources also. Resource modeling can be separated by a forward slash in the URI path.
  Example: http://api.example.com/customers/{customerid}
- Query Design(Parameter): Query string is separated by "?" symbol. It contributes to the identification of resources uniquely. It contains parameters that identify hierarchically along with path segment.
  Example: http://api.example.com/customer?item=pen

Figure 5 shows rest API structure consists of BaseURI, resources, Parameters, and Query String.

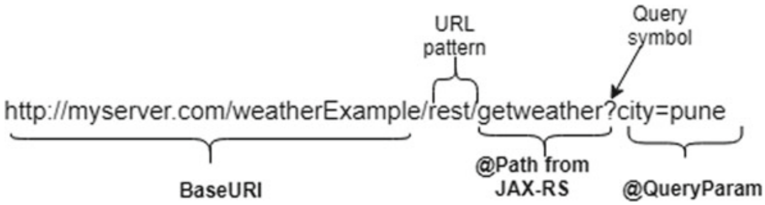

URL pattern
Query symbol
http://myserver.com/weatherExample/rest/getweather?city=pune
BaseURI
@Path from JAX-RS
@QueryParam

Fig. 5 REST API structure with example

4 Existing Tools

4.1 WireMock

WireMock [21] is an HTTP mock server, a simulator for APIs. It can be used to mock API for testing. Today's, mocking REST services are necessary for our development. It can give the canned responses (known as Stubbing) to an individual request matching. It is considered as a mock server or service virtualization tool. It facilitates to stay productive when API not yet developed or down at a time. By any JVM application, it can be used as a library or can be used as a standalone and configured via JAVA API, JSON files, or JSON over HTTP.

To include wiremock into test cases can be configured with JUnit rule. With default port (8080), basic usage of wiremock into test cases by @Rule annotation described below.

```
@Rule
public WireMockRule wireMockRule = new WireMockRule();
```

With programmatically, it can create, start, and stop as specified with command. It can do stubbing with stubFor method which takes HTTP methods and URL for request matching and will return a response in JSON mapping format. It is a bit faster as it avoids sending a command over HTTP. It will concur with a third-party server and record tested API and response as a cache. Basically, it behaves like a cache while API testing. For one API server, one wiremock instance is configured. It will not create a client object if anyone can want to mock multiple services it should be declared as a rule(@Rule) per service. It will deploy as a WAR into a servlet container.

Limitations

- Too slow and complicated as don't test for the same database again and again.
- Daily update Wiremock if it has date function calls.
- All test cases can't be mapped in one set.
- Mocking is done with only one instance of wiremock. If a client wants to connect to more than one server, multiple wiremock instances run on different ports and pointing to one proxy server.

– If user resets the API, then it cannot turn back to original API could be done by restarting the server again.

4.2 SOAP UI

A tool is used for testing Web services. It is a complete Automation framework for API (SOAP or REST) testing. It contains many features like inspection Web services, development, Mocking API, and simulation. It will create a static mock implementation in seconds and also create a Load and Functional tests of mock Web service before their actual implementation. With SOAP UI, multiple responses depending on request by scripting and also allows different status codes according to the request and response defined. With scripting, modify the mock response headers, contents at the time dispatching to a client. Able to add more than one responses according to the request initiated dynamically.

Limitations

– Assertion to JSON response not easy.
– Having a delay in response.
– Don't handle different REST API at a time and generate mock server accordingly.

5 Motivation

As discussed before, we can use mock objects to test code in isolation without integrating with external dependencies. To verify the interaction of class under test (CUT), the mock objects are used. It returns responses to method calls that are predefined under the mock framework. While testing, developer has to decide accordingly whether to test a unit in isolation by simulating all of its dependencies or test along with its dependencies together. By simulating its dependencies, developers gain focus over testing a single unit not on its dependencies as far as testing without simulations slows down the execution of a test, testers require full control over external dependencies, and it is costly to prepare for testing. For getting a quick and consistent response, there is a need to mock REST API. Back-end service that is slow to respond should be mocked. Not to get dependent on back-end developers, front-end developers require dummy data or response.

As shown in (Fig. 6), the process of developing REST API or any other software gone through these steps without mock.

1. Define interface of REST API, their Base URI.
2. Implement REST API resource methods their associated parameters, query string along with Base URI.
3. Development server testing has been done by the developers. It is an essence layer in software development where all set up like hardware, software, and other necessary component required to debugging and test the code directly by developers.

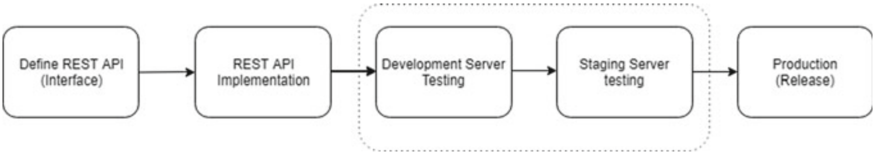


Fig. 6 Development process without Mock

4. Stagging server testing is a pre-deployment process. In this server, simulation is set up as a real environment for testing, all production configuration has been set up. It is the endwise step before final production of software.
5. Production server where Web site, REST API get deploy and hosted, also referred to as a live server. Its environment is actually identical to staging server. It is the terminal for all the accomplished task which has been done.

In this complete development process cycle, development server testing takes almost 3 h, and staging server takes around 4 h for testing the REST API. Without creating a mock object takes lots of time and efforts for development. By creating a mock object, we save our time and utilize it efficiently. This research paper gives an idea of how we can create a mock of REST API. There are already existing tools available like wiremock and SoapUI for mock REST API, but they have limitations while creating mock. They don't create different instances of mock of different REST APIs. They worked efficiently for only one instance at a time. To overcome these limitations and save time during development, there is a need of mock.

6 Proposed Approach

6.1 Challenges

In this research paper, we have shown a general approach to create a mock framework for REST API. Getting independence from back-end services and improving the execution of a class under test is done by creating a mock server. For creating mock objects, most common Java frameworks available are JMock and EasyMock. They allow us to create mock objects and define the behavior of it, exactly what you expect when we call methods on the mock object. This research work proposes an approach of how a mock framework of REST API is generated so that there is no need to interfere with the real server code according to our need. We create a framework of mock server and use it according to our requirements. Our mock server takes input data through a XML file which is not hard-coded in the framework design.

6.2 MockRest Framework

In our proposed approach, we define a framework of a mock server that mock the third-party component in which expectations are already defined according to our requirements against API. We have tested our system against API and got a response from the mock server accordingly. We propose a framework that makes it easier to generate mocks for REST API services. Our approach supports as many API calls as required. Our framework allows taking data through an XML file not to be hard-coded in the framework design. Return responses, throw exceptions, events for API call if required and allows Test Driver to verify REST API calls, their behavior with the mock server not with the real server.

An approach described in Fig. 7 gives MockRest Framework operations and methods and their behavior while generating mock instances. As said above, framework takes their data through an external document containing XML/JSON data and generating instances of mocked REST.

A mock server contains all those mocked instances and return responses with the status code, exceptions, and events as defined according to the requirements when test case runs. To assert with test cases, mocked instances have to pass as an argument of the constructor of the code under test. This is how Mocked REST API helps in testing during the development phase. Figure 8 shows the document containing XML data that would be passed in a MockRest framework to read data through an XML file by JAXB. Figure 10 shows the sequence diagram of RestMock (Fig. 9).

6.3 Create REST API with Java (JAX-RS) Using Jersey

Jersey is an open-source framework for developing REST services in java that supports JAX-RS APIs. JAX-RS has been designed to make it easier for development of RESTful Web services in java.

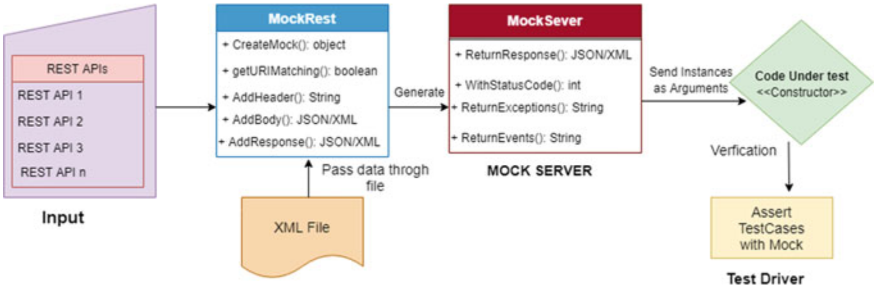
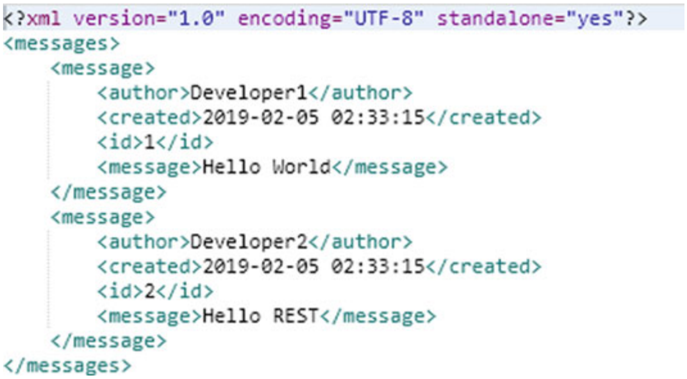
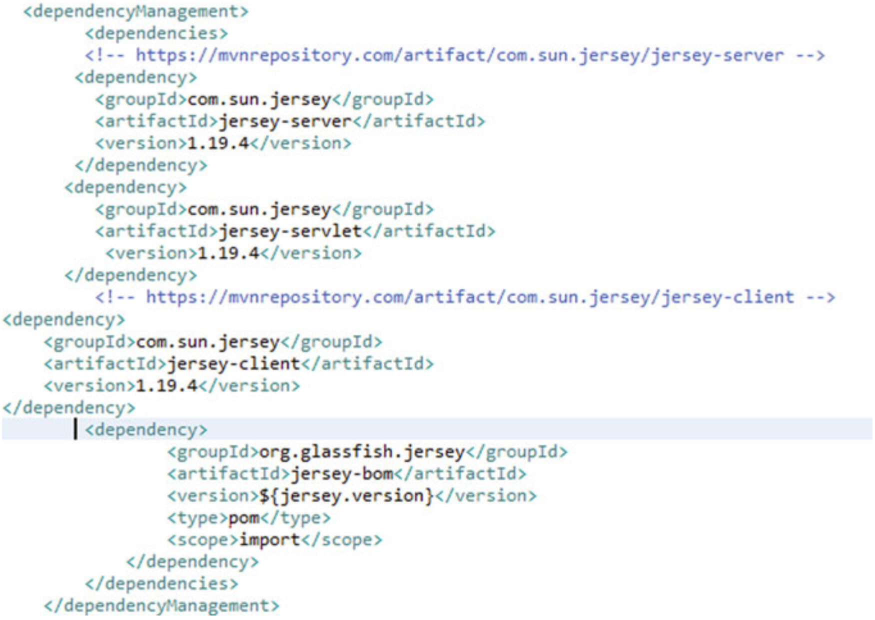


Fig. 7 Approach of MockRest framework



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<messages>
    <message>
        <author>Developer1</author>
        <created>2019-02-05 02:33:15</created>
        <id>1</id>
        <message>Hello World</message>
    </message>
    <message>
        <author>Developer2</author>
        <created>2019-02-05 02:33:15</created>
        <id>2</id>
        <message>Hello REST</message>
    </message>
</messages>
```

Fig. 8 input.xml



```
   <dependencyManagement>
         <dependencies>
         <!-- https://mvnrepository.com/artifact/com.sun.jersey/jersey-server -->
        <dependency>
          <groupId>com.sun.jersey</groupId>
          <artifactId>jersey-server</artifactId>
          <version>1.19.4</version>
        </dependency>
       <dependency>
          <groupId>com.sun.jersey</groupId>
          <artifactId>jersey-servlet</artifactId>
           <version>1.19.4</version>
       </dependency>
          <!-- https://mvnrepository.com/artifact/com.sun.jersey/jersey-client -->
<dependency>
    <groupId>com.sun.jersey</groupId>
    <artifactId>jersey-client</artifactId>
    <version>1.19.4</version>
</dependency>
        <dependency>
                <groupId>org.glassfish.jersey</groupId>
                <artifactId>jersey-bom</artifactId>
                <version>${jersey.version}</version>
                <type>pom</type>
                <scope>import</scope>
            </dependency>
        </dependencies>
    </dependencyManagement>
```

Fig. 9 Jersey dependencies in maven

Technolgies used:

- Jersey version—2.25
- Apache Maven—3.8.0
- Tomcat 7.0
- Eclipse Java IDE Mars 2.0.

In order to add jersey in Maven Project creating REST API, dependency should be added as shown in Fig. 9.

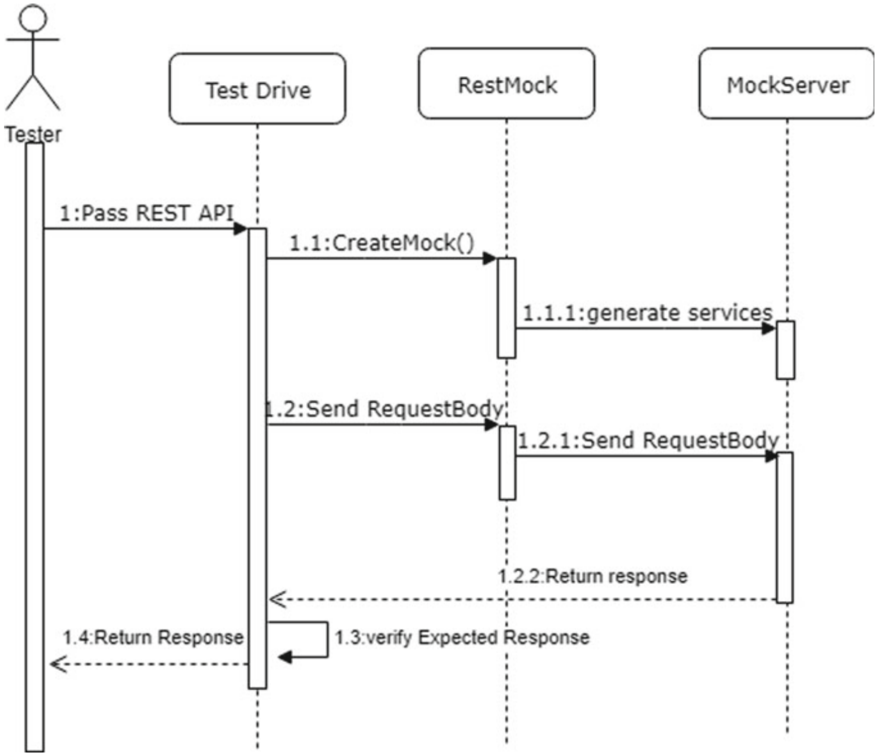
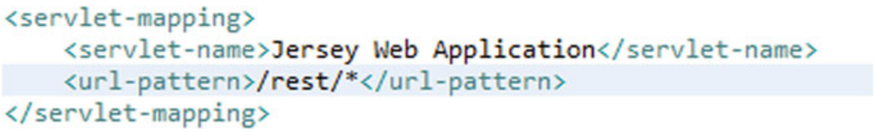


Fig. 10 Sequence diagram of RestMock



```
<servlet-mapping>
    <servlet-name>Jersey Web Application</servlet-name>
    <url-pattern>/rest/*</url-pattern>
</servlet-mapping>
```

Fig. 11 web.xml

Under the web.xml, these changes to be reflected while creating REST service with URL Pattern “rest” as shown in Fig. 11. Table 2 describes some of the annotations by JAX-RS.

6.4 *Read XMl File Through JAXB*

JAXB is a Java standard that defines API to convert Java object to and from XML. It stands for Java Architecture for XML Binding. It provides structure to write(marshal) Java objects into XML and unmarshal(read) XML into Java object. There are no

Table 2 JAX-RS annotations

Annotations	Description
@Path	Specify the URI path
@GET	Annotate HTTP GET request method
@POST	Annotate HTTP POST request method
@DELETE	Annotate HTTP DELETE request method
@PathParam	Extract URI path parameters
@QueryParam	Extract URI path query parameters
@Produces	Specify media type to be produced
@Consumes	Specify media type to be produced by REST

Table 3 JAXB annotations

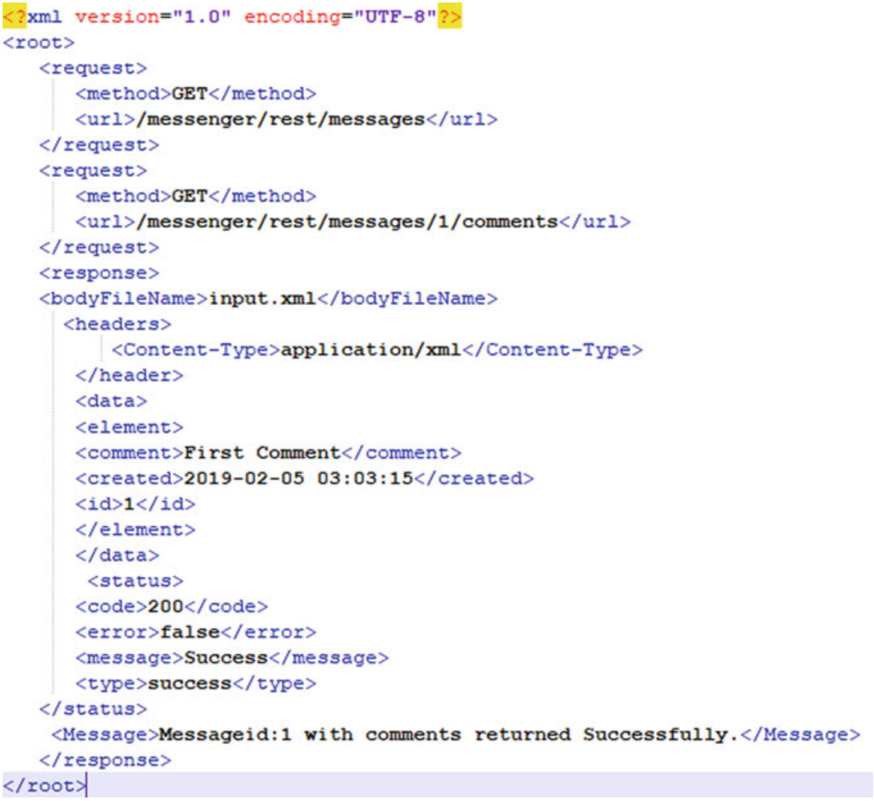
Annotations	Description
@XmlRootElement(namespace = "namespace")	Define the global(root) element of xml tree
@XmlElement	Annotate field that need to be in output
@XmlType	Mention order of xml elements
@XmlAttribute	Maps java Bean property to xml attribute

external libraries for JAXB as long as jersey builds on the project. There are some of the annotations required to support XML binding described in Table 3. To convert XML data into Java objects, Unmarshal() method to be used. In JAXB, there is an abstract class named JAXBContext that provides client's entry point to the JAXB API, gets initialized with the class used, creates Unmarshaller, and returns an unmarshaller object that can be used to convert the XML data. Unmarshaller interface provides client XML data and converts into Java object by the function named unmarshal().

7 Results Observed

Two REST APIs created dependent on each other.
http://myserver.com/messenger/rest/messages
and
http://myserver.com/messenger/rest/messages/1/comments

Both REST API for messenger one for retrieving messages and other for retrieving comments are given by messageid. As shown above, comments are dependent on message-id. By giving message-id in the REST API, comments are retrieved by Get Http method. File input.xml shown in Fig. 8 has been passed into the framework, and mock server generates expected result after creating mock of REST API as shown in Fig. 12. As observed, mock server returns comment and its created date with



```
<?xml version="1.0" encoding="UTF-8"?>
<root>
   <request>
      <method>GET</method>
      <url>/messenger/rest/messages</url>
   </request>
   <request>
      <method>GET</method>
      <url>/messenger/rest/messages/1/comments</url>
   </request>
   <response>
   <bodyFileName>input.xml</bodyFileName>
     <headers>
         <Content-Type>application/xml</Content-Type>
      </header>
      <data>
      <element>
      <comment>First Comment</comment>
      <created>2019-02-05 03:03:15</created>
      <id>1</id>
      </element>
      </data>
       <status>
      <code>200</code>
      <error>false</error>
      <message>Success</message>
      <type>success</type>
   </status>
    <Message>Messageid:1 with comments returned Successfully.</Message>
   </response>
</root>
```

Fig. 12 Result after creating Mock

status code 200, a status message with type Success and header of application/xml and mocked response as a message with message-id “Messageid:1 with comments returned Successfully.” in response tag.

8 Conclusion

This research work proposed a generic approach to create a mock framework for REST API. The MockRest framework generated a mocked object of REST APIs. Mock server generated a pre-defined response, events, and exceptions to improve testing by the developers without getting involved with a real server. Mocked APIs could be used by testers to simulate external dependencies and make efficient testing with mocked APIs.

The MockRest framework has also taken the dependent list of APIs and generated mocked objects on existing mock server which are not been able to do as they have a one-to-one relationship. Future benefits of RestMock are that it could manage third-party services, speed up the testing and development, and speed up the generation of test cases.

References

1. Thomas D, Hunt A (2002) MOCK objects. IEEE Softw (Published in Journal) 19(3):22–24
2. Kim T, Park C, Wu C (2006) Mock object models for test driven development. In: Fourth international conference on software engineering research, management and applications (SERA06). IEEE
3. Spadini D, Aniche M, Bruntink M, Bacchelli A (2017) To mock or not to mock? An empirical study on mocking practices. In: IEEE/ACM 14th international conference on mining software repositories (MSR), pp 402–412
4. Mostafa S, Wang X (2014) An empirical study on the usage of mocking frameworks in software testing. In: 2014 IEEE 14th International conference on quality software. https://doi.org/10.1109/QSIC.2014.19
5. Singhal N, Jain H (2016) Automock: automated mock backend generation for javascript based applications, vol. 16, Issue 7 Version 1.0. Online ISSN: 0975-4172 & Print ISSN: 0975-4350
6. Ashikhmin N, Radchenko G, Tchernykh A (2017) RAML-based mock service generator for microservice applications testing. https://doi.org/10.1007/978-3-319-71255-0
7. Adamczyk P, Smith PH, Johnson RE, Hafiz M (2011) REST and web services: in theory and in practice. Springer Science+Business Media, New York. https://doi.org/10.1007/978-1-4419-8303-9_2
8. Masse M (2011) Designing consistent RESTful web services interface. OReilly Media. ISBN: 978-1-449-31050-9
9. Kao CH, Lin CC, Chen JN (2013) Performance testing framework for REST-based web applications. In: 2013 IEEE 13th international conference on quality software. https://doi.org/10.1109/QSIC.2013.32
10. Haupt F, Leymann F, Scherer A, Vukojevic-Haupt K (2017) A framework for the structural analysis of rest APIs. In: IEEE international conference on software architecture. https://doi.org/10.1109/ICSA.2017.40
11. Ed-douibi H, Izquierdo JLC, Cabot J (2018) Automatic generation of test cases for REST APIs: a specication-based approach. In: IEEE 22nd international enterprise distributed object computing conference. https://doi.org/10.1109/EDOC.2018.00031
12. Arcuri A (2017) RESTful API automated test case generation. In: IEEE international conference on software quality, reliability and security
13. Munonye K, Martinek P (2018) Performance analysis of the microsoft .net- and java-based implementation of REST web services. In: IEEE 16th international symposium on intelligent systems and informatics, Subotica, Serbia, 13–15 September 2018
14. Sinha R, Khatkar M, Gupta SC (2014) Design & development of a REST based web service platform for applications integration on cloud. IJISET—Int J Innov Sci Eng Technol 1(7):385-389
15. Giessler P, Gebhart M, Sarancin D, Steinegger R, Abeck S (2015) Best practices for the design of RESTFul web services. In: Tenth international conference on software engineering advances, Barcelona
16. Qiu D, Li B, Leung H (2016) Understanding the API usage in Java. In: Information and software technology, Elsevier, Amsterdam, pp 81–100

17. Hunt A, Thomas D (2003) Pragamatic unit testing with JUnit, First printing, September 2003. ISBN 0-9745140-1-2
18. Nandigam J, Gudivada VN, Hamou-Lhadj A, Tao Y (2009) Interface-based object-oriented design with mock objects. In: 2009 IEEE sixth international conference on information technology: new generations, pp 713–718
19. Mackinnon T, Freeman S, Craig P (2001) Endo-testing: unit testing with mock objects
20. Fielding RT (2000) Architectural styles and the design of network-based software architectures. Dissertation
21. WireMock (2018). http://wiremock.org/. Accessed 8 September 2018
22. Marri MR, Xie T, Tillmann N, de Halleux J, Schulte W (2009) An empirical study of testing file-system-dependent software with mock objects. In: ICSE workshop on automation of software test, AST 2009, pp 149–153
23. SoapUI (2018). https://www.soapui.org. Accessed 12 October 2018
24. Jersey (2018). https://jersey.github.io/. Accessed 5 Oct 2018

Syntactic Interoperability in Real-Time Systems, ROS 2, and Adaptive AUTOSAR Using Data Distribution Services: An Approach

Navrattan Parmar, Virender Ranga and B. Simhachalam Naidu

Abstract DDS is a real-time protocol for fast communication. It implements Data-Centric Publish–Subscribe (DCPS) implementation and an optional higher-layer Data Local Reconstruction Layer (DLRL). DCPS ensures the reliability of message delivery to proper recipient and uses in syntactic interoperability in different platforms and languages. ROS is a widely used platform to develop robots, drones, and other cyber–physical systems (CPSs). ROS 2 is built on top of middleware DDS and provided abstraction in communication. Adaptive AUTOSAR (Automotive Open System Architecture) also adopted the DDS standards as one of the communication bindings. This research paper proposes connection establishment and interoperability between ROS 2 and Adaptive AUTOSAR software using DDS as a middleware. Interoperability is the major challenge with the increasing number of IoT devices, being solved by DDS. The outcome of this research is useful for autonomous cars, and the proposed concept can be extended for fog computing and other interoperability problems. DDS will bring a revolution in the near future in automotive industry, smart grid, smart homes, and other smart applications.

Keywords Syntactic interoperability · DDS · Adaptive AUTOSAR · ROS 2.0 · Fog computing · Cyber–physical system (CPS) · Electric control unit (ECU) · Automotive software stack · Adaptive application (AA) · Adaptive Platform (AP) · Inter-process communication (IPC)

N. Parmar (✉) · V. Ranga
National Institute of Technology, Kurukshetra, Haryana, India
e-mail: parmarnavrattan@gmail.com

V. Ranga
e-mail: virender.ranga@nitkkr.ac.in

B. Simhachalam Naidu
KPIT Technologies, Bengaluru, India
e-mail: B.Naidu@kpit.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_25

1 Introduction

DDS is a decentralized messaging architecture where we need not worry about interface interaction from the development point of view. It is persistent, scalable, and fault tolerant. It can control throughput, data latency, data availability, and data delivery. Now, with the support of DDS in many softwares, it is possible to communicate between them.

1.1 ROS 2.0 and Adaptive AUTOSAR

Robot Operating System (ROS) is the widely used platform nowadays to develop robots, drones, and other cyber–physical systems (CPSs) as explained previously. It is a very popular middleware that can provide abstraction at communication level. ROS is maintained by Open Source Robotics Foundation (OSRF) and Willow Garage. It uses publish–subscribe transport method [1, 2], multiple libraries (e.g., rcl, OpenCV, and the Point Cloud Library (PCL) [3]), and tools to help low-level abstraction and enhance the productivity.

Adaptive AUTOSAR is the automotive software stack that provides standard interfaces. It is currently being used in automotive industry for developing state-of-the-art ECUs running on multi-core processors. Its interfaces allow the equipment manufactures to implement autonomous driving, over-the-air updates, IoT features, media streaming, and other advanced services.

The main aim of this research work is to propose an approach to solve interoperability problem using DDS. In this research paper, a systematic approach is proposed for syntactic interoperability between ROS 2.0 and Adaptive AUTOSAR. Our work demonstrates the publisher–subscriber method and communication between them. Figure 1 shows a communication model through DDS.

2 Related Work

In the new era of communications, for a large number of IoT devices, people from different domains, systems, and knowledge are required to communicate with each other [4] and heterogeneity is the major problem. It can be solved by DDS. Next section shows the literature review done by us.

2.1 ROS Literature Review

ROS is the middleware that was initially used to build small robots, but it is now being used to make drones' applications as well as in large projects. Our proposed research

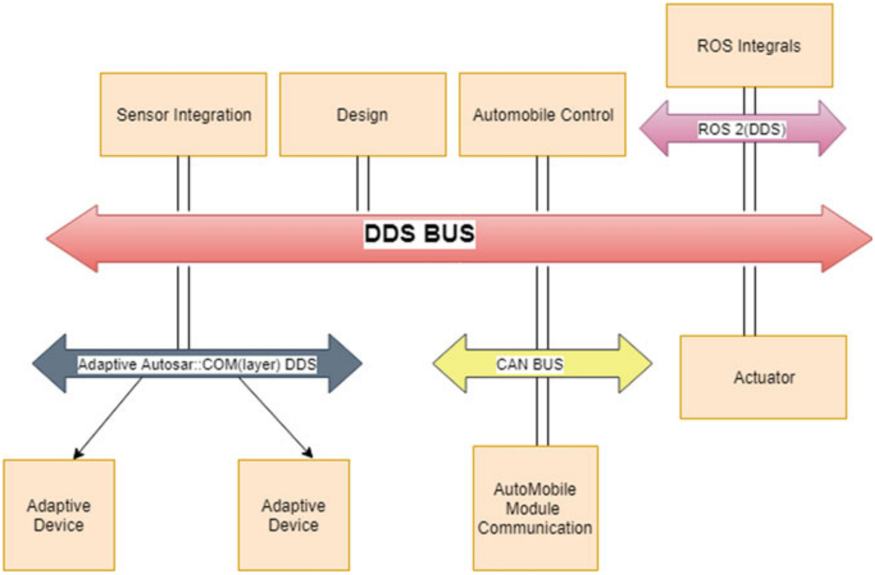


Fig. 1 Communication via DDS bus

work aims to integrate ROS [5–7] with Adaptive AUTOSAR for autonomous drive capabilities in automobile industry.

Rhoades et al. [8] describe ROS, CAN, and QRE to enable control vehicle via ROS and enable the independent development and communication. The authors use RX63n board for evaluation and control. RX63n is used to send message to ROS master. ATV and QRE are used to receive the messages from ROS master and controlled the vehicles.

Mauyama et al. [9] give in-depth overview of ROS 2. With the adaptation of DDS in ROS 2, there is an evolution in the ROS. Now, it can be used for real-time communication. This paper analyzes the DDS capabilities and evaluates various challenges, overhead, and constraints of DDS and ROS. ROS adopts DDS only for inter-process communication. The experimental part shows the capability and efficiency of DDS in ROS 2, and it shows that data is not lost even if message size is 4 MB. The authors evaluate the performance of ROS 2 and ROS 1 in various cases of remote and local communication and also evaluate the parameter of QoS in ROS 2, number of threads, memory consumption, throughput, and latencies. Finally, this paper concludes the advantages of using DDS. The authors show that DDS makes ROS real time and capable of running on multiple platforms.

Liu et al. [6] observe DDS in ROS 2. They conduct the experiments for the messages of high priority and come up with the result that it would be great if the system could buffer six or more messages. The authors propose a non-preemptive system and analyze its properties using auto-meta. It is noted that the high-priority nodes can preferentially transfer data with system deadlock-free and secure also.

Mishra et al. [5] propose a robot–human interaction with an experimental setup. They use TurtleBot platform for the simulation and rtabmap_ros for mapping and localization. They propose a Adaptive Monte Carlo Localization for navigation and visualized using rviz. They show that robot can run successfully by navigating itself to target even if robot is placed at any different locations.

Dauphin et al. [10] brief about the implementation, evaluation, and design of a system for mini-bots. They use ROS 2 on top of RIOT and aim to reduce gap between robotics and IoT. Their research work investigates the future of open-source robotic platform with IoT to command mini-bots.

Reliability and Achievements of ROS 2 This section focuses on finding most appropriate background of ROS 2 applications. In the implementation:

- We evaluate latency and throughput performance of ROS 2.
- We conduct the experiment on DDS and VPN, and compare them.
- We implement Real Time Publish–Subscribe (RTPS) communication standards, under middleware ROS 2.

Returning to general OpenSSL library with FIPS module may refine target module's security and its security functions. It is emanated from research that VPN may be a better choice for simple system architecture.

2.2 Data Distribution Services

Koksal and Tekinerdogan [11] propose a well-organized review paper. They have done a large review of 468 papers. They introduce the study on DDS, because DDS has a huge scope. They categorize DDS into 11 topics for a systematic study. Their classification is shown below:

- Problems in DDS.
- Conduct, quantification, and progress in DDS.
- Execution of DDS protocol.
- DDS incorporation in WAN.
- DDS use in wireless network and mobile computing.
- Ability to communicate among different DDS vendors.
- Data uniformity in DDS.
- Security and robustness of DDS.
- Scaling-up of nodes in DDS.
- Certainty and reliability of DDS protocol.
- Integration of DDS with real-time systems (Table 1).

Yim et al. [12] propose a paper in the category of DDS in real-time system. They deal with the interoperability and heterogeneity problems in data/services/events. Following is the description of topic given by the authors on DDS as illustrated in Fig. 2.

Table 1 Integration of real-time systems with DDS

Research papers	Years	Important points
S.A. Hadiwardoyo et al.	2018	Information passing between the train wagon and station
		Adding more number of subscribers does not effect
Y. Park et al.	2015	High-level architecture for vehicles-to-everything communication using OpenSlice DDS
		Experiments using SUMO v0.22.0 for traffic simulation and OMNeT++ v4.6 for network simulation
		It achieves interoperability and workability of HLA features
		Research affix control functions of network QoS, network conduct, and scalability from DDS features
H. Perez et al.	2016	A point of view to use DDS and hypervisor technologies in multi-core systems is suggested
		DDS design is consistent with ARINC-analogous segregated systems
		They endorse through a dossier from the energy domain
P. Bellavista et al.	2013	It is the comparison of different DDS implementations (PrismTech and RTI)
		We can infer that OpenSplice has superior execution for small data
		RTI scale-up adeptly due to a better accomplishment message split-up and memory management tasks
Z. Heng et al.	2017	Application of DDS, i.e., live virtual and constructive training used in US Army
		It is the real-time integration concept presented and reliability test for DDS
		DDS uses Interface Description Language (IDL) which makes it platform independent
W. Zeyu et al.	2017	Designs the test system for DDS
		It is the real time integration testing presented and reliability test for DDS
M. Takrouni et al.	2017	Designed a Simulink DDS blockset
		It solves the problem of manually setting up the publisher–subscriber in DDS
		They also explained the XML Script to understand functioning of blockset
A. Alaerjan et al.	2017	Practical conduct of DDS using Object Constraint Language (OCL)
		It defines briefly distinct layers in the DDS, i.e., DLRL, DCPS, and RTPS and conduct of DCPS
		DCPS behaviors are explained for generating entities and publish–subscribe data
T. Chen et al.	2018	They used ARINC 653 (Avionics Application Standard Software Interface) and VxWorks boards
		DDS was integrated into VxWorks
		ARINC 653 and VxWorks were integrated via AFDX bus
		Setup had a delay due to VxWorks and AFDX drivers which is noticeable
		DDS integration inside ARINC 653 is a difficult task according to researchers
H. Yuefeng	2018	DCPS data transmission
		Experiment was conducted in VxWorks5.5 environment
		Transmission of data was steady and reliable
		Conclusion: DDS can be used for real-time systems
A. Alaerjan et al.	2018	DDS in smart grid
		Transmission of data was steady and reliable
		Conclusion: DDS can be used for real-time systems

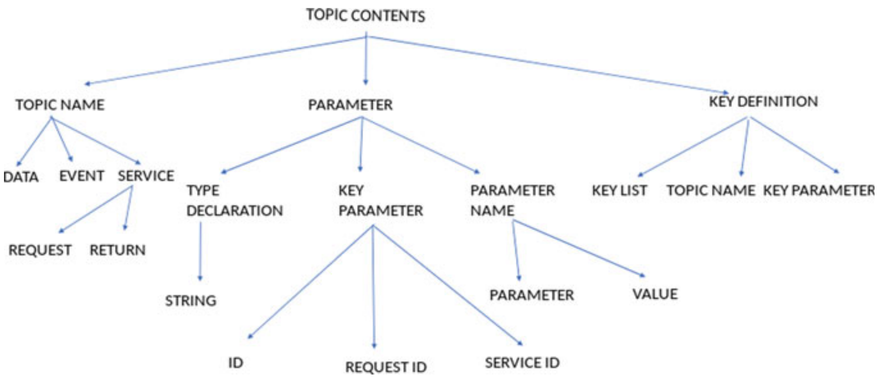


Fig. 2 Topic description file structure

2.3 Adaptive AUTOSAR

Adaptive AUTOSAR is a automotive software that is being used for automation of driving, over-the-air updates, and car-to-everything architectures (Car-2-X). Here is the literature review of Adaptive AUTOSAR. Furst et al. [13] describe Adaptive AUTOSAR for automotive and its characteristics as well. Adaptive AUTOSAR is a very well-suited platform for adapting and accepting the new challenges.

- It is very well suited for different software platforms.
- The mode of communication, i.e., service-oriented and signal-based communication, was inefficient for huge volumes of dynamic data.

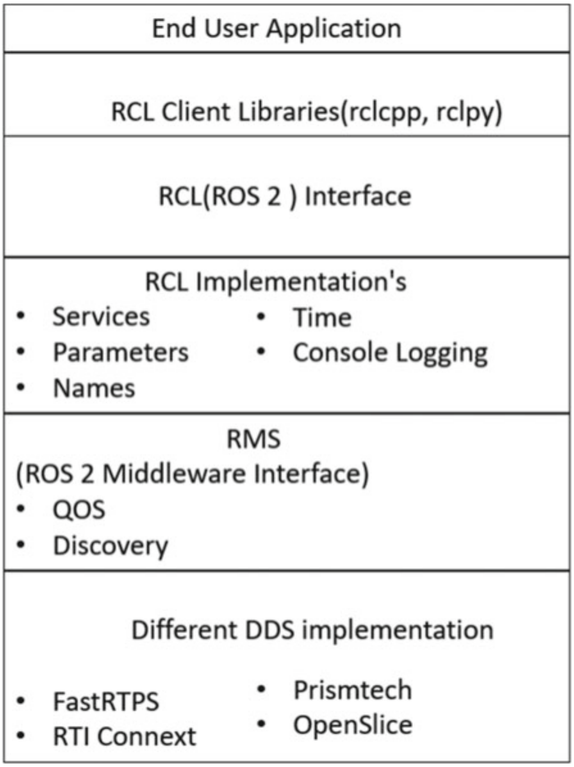
Han et al. [1] describe TCP/IP analysis in Adaptive AUTOSAR. The average number of ECUs in vehicles are increasing rapidly. In order to fulfill its needs, Adaptive Platform is developed to enhance the performance of some of features of TCP/IP. Address Resolution Protocol (ARP) cache entries should be updated based only on ARP packets. When service is not provided by the peer at the requested protocol or port, it should respond with RST (reset) rather than responding with port unreachable.

3 Background Study

3.1 Robot Operating System (ROS)

In contrast to ROS 1, many proposed changes are adopted in ROS 2 as it inculcated DDS in its architecture. ROS 2 does not require a master for publish–subscribe communication, thus making it more secure.

Fig. 3 Architecture Of ROS



ROS Architecture. Figure 3 illustrates ROS architecture.

- Nodes: It is individualistic module of userland code.
- Topics: Identification of message/data between publisher–subscriber.
- Message: Message in ROS and ROS 2 is very similar to C structs. It sends complete table for communication. So, we do not need different interfaces.
- Publisher: Sender of the data/client.
- Subscriber: Receiver of data/server.
- Package: ROS 2 software stack is composed of packages, where each package provides important functionality.

ROS 2 is middleware for development of small/large robots. User code is built on top of ROS client libraries. ROS provides rclcpp for C++ and rclpy for Python as the basic client libraries for development. Support for other languages is being provided by the community. Client libraries are responsible for the execution of a thread, IPC, services, parameters, console, and logging. RCL and RMW implementation are bound by a library. RMW is the ROS middleware implementation. RMW is responsible for different DDS implementations, QoS, and discovery.

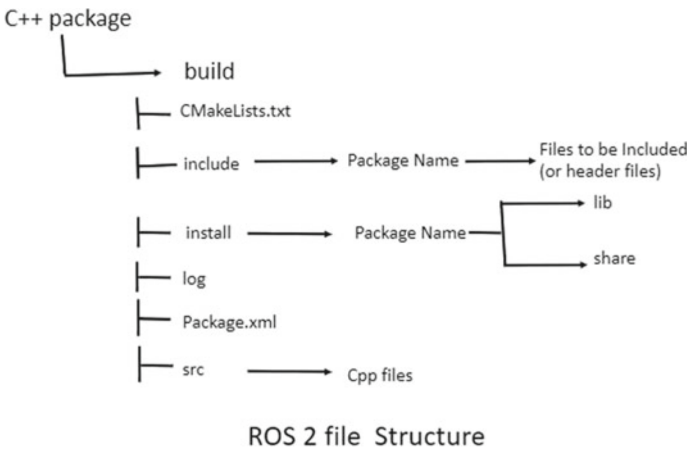


Fig. 4 ROS 2 file structure

ROS 2 File Structure. File structure of C++ package of ROS is shown in Fig. 4:

- build: Temporary files are generated during the build. It can be used to check the built files.
- CMakeLists.txt: This folder contains package dependencies and how to build them, how to generate binaries and libraries, and where to store them.
- install: It contains files to be included in its subfolders, i.e., lib and share.
- include: Stores all the necessary files/directories for building and linked in cmake.
- log: Contains information about build.
- package.xml: It tells us about the type of build and dependencies.
- src: It contains the files developed by the ROS 2 developer.

File structure of Python packages in ROS 2 is very similar to C++ package, but only difference is CMakeLists.txt does not exist in Python package; instead, setup.py file is used. setup.py performs similar function.

3.2 Data Distribution Services

DDS stack has three layers: Data Local Reconstruction Layer (DLRL), Data-Centric Publish–Subscribe (DCPS), and Real-Time Publish–Subscribe (RTPS). DCPS is compulsory for interaction of DDS components. DLRL is a discretionary layer. RTPS supports interoperability between different DDS layers. DDS architecture is depicted in Fig. 5. DCPS contains modules, and each of the modules has multiple classes for its operations.

- Domain Module: It manages various DDS modules through domain ID differentiation. It has the following classes.

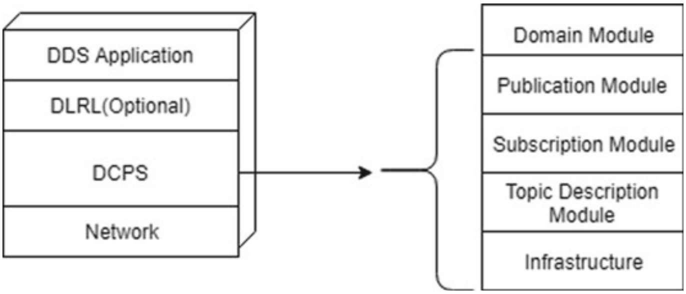


Fig. 5 Architecture of DDS

  - DomainParticipantListener (interface)
  - DomainParticipant
  - DomainParticipantFactory

- Publisher Module: It aids publication.
  - Publisher
  - Publication type specific classes
  - PublisherListener (interface)
  - DataWriterListener (interface)

- Subscriber Module: This module contains all the support for subscription.
  - Subscriber
  - Subscription type specific classes
  - Subscription type specific classes
  - DataSample
  - SampleInfo (struct)
  - SubscriberListener (interface)
  - DataReaderListener (interface)
  - ReadCondition
  - QueryCondition

- Topic Description Module: It specifies topic objects and specifies quality of service for them has the following classes.
  - TopicDescription (abstract)
  - Topic
  - ContentFilteredTopic
  - MultiTopic
  - TopicListener (interface)

- Infrastructure Module: This module contains the abstract classes and interfaces, which are used by the different modules. It assists interoperability between the application and the Data Distribution Service. Interaction between DDS and application may be event- or state-based. It contains the following classes.

- QosPolicy (abstract, struct)
- Listener (interface)
- Status (abstract, struct)
- WaitSet
- Condition
- GuardCondition
- StatusCondition
- Entity (abstract)
- DomainEntity (abstract).

3.3 Adaptive AUTOSAR

The software platform, AUTOSAR Adaptive Platform (AP), provides a software stack for development of automotive and other ECUs. AP offers high computing functions and communication and offers flexible software design based on software-oriented architecture (SOA), e.g., to support software update over the air, distributed architecture, hybrid and central fusion. Figure 6 shows the modules of AP which are listed below.

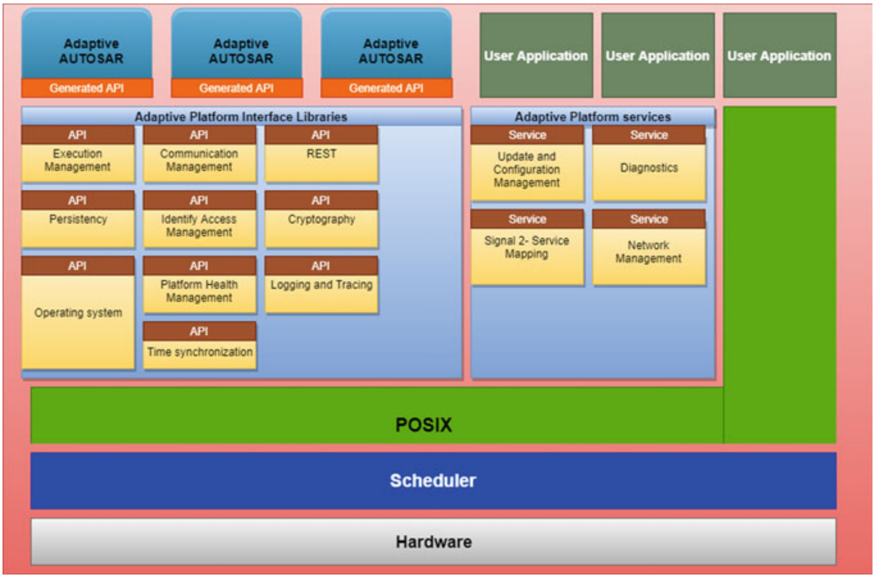


Fig. 6 Physical architecture of Adaptive AUTOSAR

- AP uses Operating System Interface (OSI) rather than building its own OS. OSI is POSIX compliable interface. Adaptive application (AA) shall use PSE51 as an OSI. Scheduling is also defined under POSIX standard, and OS provides multithreading and multi-process support. AP provides "freedom of interferences" among functional clusters and adaptive application. Multiple processes can run together, and multiple instance of a single process can run in different address spaces.
- Execution Manager (EM): It is responsible for start and shutdown of application. It views all the functional clusters and an application as well. EM is responsible for application life cycle.
- Communication Module (CM): It is responsible for IPC and application interaction. There is no direct communication between adaptive applications.
- RESTful Communication: ara::com and ara::rest are used for communication between AAs. It ensures interoperability with non-AUTOSAR clients, as an example ara::rest service can transfer data with a adaptable client and vice versa.
- Persistency: It provides mechanism to store data and makes available Key-Value Storage, File-Proxy Storage on the device, and the combination of two. Persistent data is always private to each application.
- Time Synchronization: TS performs synchronization between adaptive applications, ECUs, and other entities.
- Update and Configuration Management : It handles all the update request. Its function is same as to dpkg or YUM in LINUX.
- Diagnostics: It perceives ISO 14229-5 (UDSonIP). ISO 14229-5 is based on ISO 14229-1 (UDS) and ISO 13400-2 (DoIP).

4 Motivation

- Hussain et al. [4] propose a detailed study of various issues in IoT like scalability, interoperability, heterogeneity, quality of service, and security. The proposed research work focuses on heterogeneity.
- In automotive industry, "interoperability between ROS 2.0 and Adaptive AUTOSAR will bring two heterogeneous softwares to communicate among themselves to increase automation, efficiency, and ease of development."
- This research provides a lot of innovative ideas with DDS.
- It will be boon to the students and researchers as it will give them a direction and quick start in world of autonomous vehicles. There is only a limited literature available for the Adaptive AUTOSAR and ROS 2.
- This work will not only help in automotive but also make the us aware scope of DDS.
- Adaptive AUTOSAR and ROS are having high cohesion and low coupling. AAs are developed independently on different machines and OS. So, there is a scope of syntactic interoperability if DDS implementation is carried in IPC of ROS and adaptive.

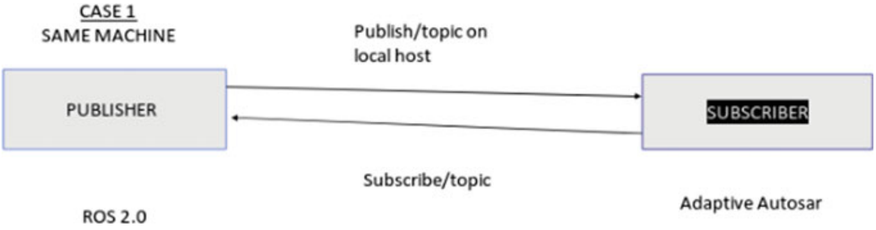


Fig. 7 Case 1

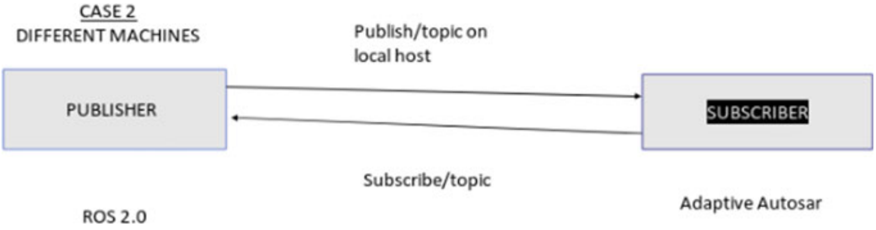


Fig. 8 Case 2

5 Approach

After the ROS 2 is integrated with DDS and Adaptive AUTOSAR is also adopted the DDS standard. Many papers in the literature propose the idea and feasibility of syntactic interoperability between ROS and Adaptive AUTOSAR. Figures 7 and 8 give an idea of communication between ROS 2 and Adaptive AUTOSAR by considering two different cases with first on the same machine and second on different machines, respectively.

5.1 Communication Management in Adaptive AUTOSAR: Network Socket

AP can be depicted as follows in Fig. 9.

Layer named ara::com is responsible for AA communication. Service-oriented communication, i.e., in addition to the operating system such as intra-/inter-machine communication, is also carried out by com layer.

Illustration of application registry and discovery services in adaptive is shown in Fig. 10.

Language binding is carried out by a source code generator that is provided by the service interface definition (ARXML) file. It defines how service is translated into available identifiers by implementing target language characteristics. ARXML is the interface description and fed as input to tools for code generation. It is strongly

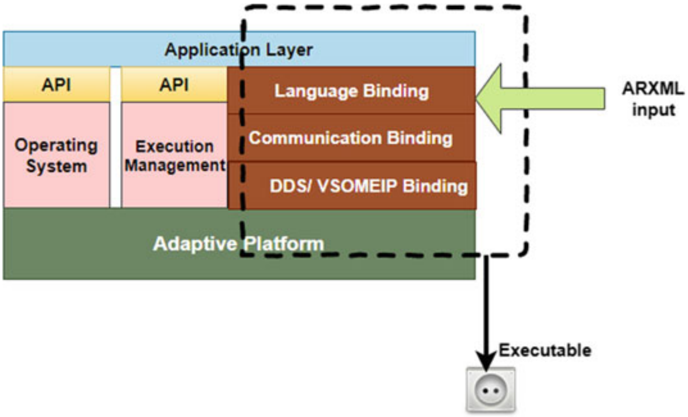


Fig. 9 Socket approach of Adaptive AUTOSAR

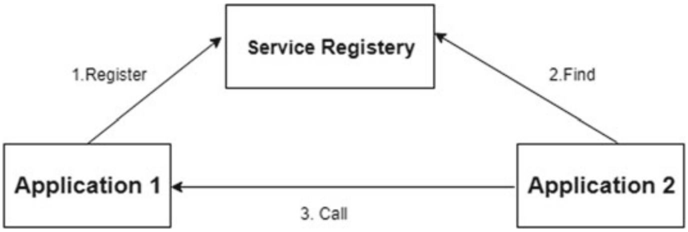


Fig. 10 Service registry and discovery of an application

typed, i.e., all arguments are pre-defined. Network binding in ara::com can be using SOME/IP (default), IPC using DDS, or other transport layers.

Network binding in ara::com can be using SOME/IP (default), REST, DDS or other Transport Layers.

5.2 *ROS 2 Publish–Subscriber*

The following steps may be followed for workflow in ROS 2

- Create the ROS node: Initialize the ROS client library you want to use and create node using create_node() method.
- Publish it: After the contents and parameter of ROS topic is decided, we publish it.
- rmw and rmw_implementation: ROS message is converted to DDS message and published.
- Adaptive Platform understands the message and decodes it.

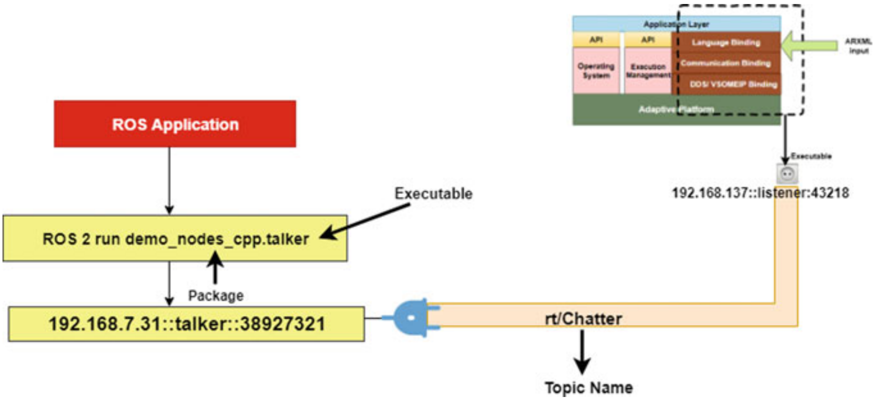


Fig. 11 Plug and socket approach for connection

5.3 *The Connection*

Figure 11 shows the view connection. We explain the connection using plug and socket approach, where either of ROS or adaptive can act as plug/socket.

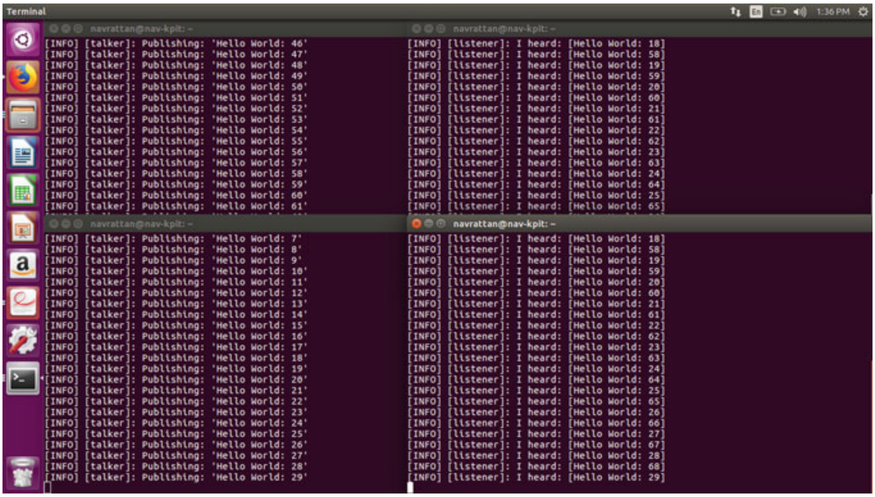
6 Results

We have conducted many experiments with the talker and listener scenario in our system and observed the results on the same machine and different machines. The following results have been achieved. Figure 12 depicts the talker and listener instances on a same machine.

We compare RTPS and UDP based on different parameters as shown in Fig. 13.

- Reliability: It is measured as overall consistency of a protocol. It is shown that UDP is an unreliable protocol, whereas DDS offers abstraction on TCP/IP or UDP and is reliable protocol.
- QoS Setting: It is observed that DDS offers Process Interface Management (PIM), configuration, and interoperability. It can use both TCP and UDP and can have a large set of QoS setting as well.
- Latency: It is observed that UDP has less latency over an unreliable network, but if we want to offer reliability in the protocol itself, the latency of DDS is the same.
- Interoperability: The pub–sub concept itself was designed to solve the problems of interoperability. By having different configurations, it can communicate.
- Complexity: DDS is easier to implement because of abstraction it offers.

Figure 14 shows talker and listener instances on different machines.



```
[INFO] [talker]: Publishing: 'Hello World: 46'
[INFO] [talker]: Publishing: 'Hello World: 47'
[INFO] [talker]: Publishing: 'Hello World: 48'
[INFO] [talker]: Publishing: 'Hello World: 49'
[INFO] [talker]: Publishing: 'Hello World: 50'
[INFO] [talker]: Publishing: 'Hello World: 51'
[INFO] [talker]: Publishing: 'Hello World: 52'
[INFO] [talker]: Publishing: 'Hello World: 53'
[INFO] [talker]: Publishing: 'Hello World: 54'
[INFO] [talker]: Publishing: 'Hello World: 55'
[INFO] [talker]: Publishing: 'Hello World: 56'
[INFO] [talker]: Publishing: 'Hello World: 57'
[INFO] [talker]: Publishing: 'Hello World: 58'
[INFO] [talker]: Publishing: 'Hello World: 59'
[INFO] [talker]: Publishing: 'Hello World: 60'
[INFO] [talker]: Publishing: 'Hello World: 61'
```

```
[INFO] [listener]: I heard: [Hello World: 18]
[INFO] [listener]: I heard: [Hello World: 58]
[INFO] [listener]: I heard: [Hello World: 19]
[INFO] [listener]: I heard: [Hello World: 59]
[INFO] [listener]: I heard: [Hello World: 20]
[INFO] [listener]: I heard: [Hello World: 60]
[INFO] [listener]: I heard: [Hello World: 21]
[INFO] [listener]: I heard: [Hello World: 61]
[INFO] [listener]: I heard: [Hello World: 22]
[INFO] [listener]: I heard: [Hello World: 62]
[INFO] [listener]: I heard: [Hello World: 23]
[INFO] [listener]: I heard: [Hello World: 63]
[INFO] [listener]: I heard: [Hello World: 24]
[INFO] [listener]: I heard: [Hello World: 64]
[INFO] [listener]: I heard: [Hello World: 25]
[INFO] [listener]: I heard: [Hello World: 65]
```

```
[INFO] [talker]: Publishing: 'Hello World: 7'
[INFO] [talker]: Publishing: 'Hello World: 8'
[INFO] [talker]: Publishing: 'Hello World: 9'
[INFO] [talker]: Publishing: 'Hello World: 10'
[INFO] [talker]: Publishing: 'Hello World: 11'
[INFO] [talker]: Publishing: 'Hello World: 12'
[INFO] [talker]: Publishing: 'Hello World: 13'
[INFO] [talker]: Publishing: 'Hello World: 14'
[INFO] [talker]: Publishing: 'Hello World: 15'
[INFO] [talker]: Publishing: 'Hello World: 16'
[INFO] [talker]: Publishing: 'Hello World: 17'
[INFO] [talker]: Publishing: 'Hello World: 18'
[INFO] [talker]: Publishing: 'Hello World: 19'
[INFO] [talker]: Publishing: 'Hello World: 20'
[INFO] [talker]: Publishing: 'Hello World: 21'
[INFO] [talker]: Publishing: 'Hello World: 22'
[INFO] [talker]: Publishing: 'Hello World: 23'
[INFO] [talker]: Publishing: 'Hello World: 24'
[INFO] [talker]: Publishing: 'Hello World: 25'
[INFO] [talker]: Publishing: 'Hello World: 26'
[INFO] [talker]: Publishing: 'Hello World: 27'
[INFO] [talker]: Publishing: 'Hello World: 28'
[INFO] [talker]: Publishing: 'Hello World: 29'
```

```
[INFO] [listener]: I heard: [Hello World: 18]
[INFO] [listener]: I heard: [Hello World: 58]
[INFO] [listener]: I heard: [Hello World: 19]
[INFO] [listener]: I heard: [Hello World: 59]
[INFO] [listener]: I heard: [Hello World: 20]
[INFO] [listener]: I heard: [Hello World: 60]
[INFO] [listener]: I heard: [Hello World: 21]
[INFO] [listener]: I heard: [Hello World: 61]
[INFO] [listener]: I heard: [Hello World: 22]
[INFO] [listener]: I heard: [Hello World: 62]
[INFO] [listener]: I heard: [Hello World: 23]
[INFO] [listener]: I heard: [Hello World: 63]
[INFO] [listener]: I heard: [Hello World: 24]
[INFO] [listener]: I heard: [Hello World: 64]
[INFO] [listener]: I heard: [Hello World: 25]
[INFO] [listener]: I heard: [Hello World: 65]
[INFO] [listener]: I heard: [Hello World: 26]
[INFO] [listener]: I heard: [Hello World: 66]
[INFO] [listener]: I heard: [Hello World: 27]
[INFO] [listener]: I heard: [Hello World: 67]
[INFO] [listener]: I heard: [Hello World: 28]
[INFO] [listener]: I heard: [Hello World: 68]
[INFO] [listener]: I heard: [Hello World: 29]
```

Fig. 12 Running instances of ROS on single machine

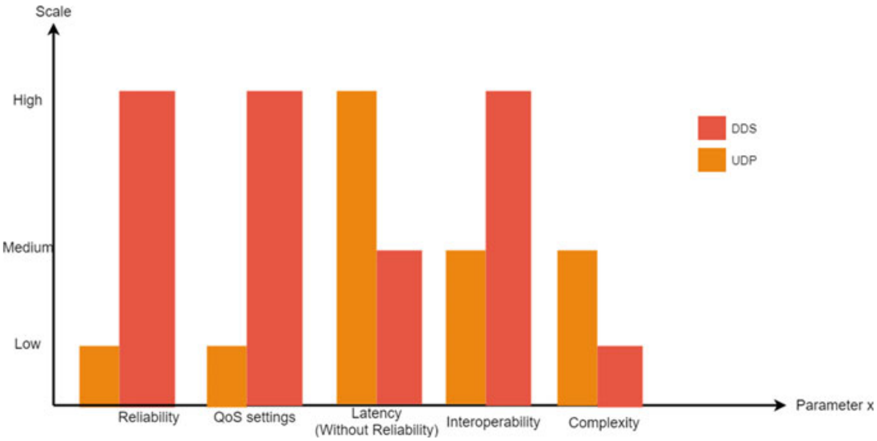


Fig. 13 Comparison of DDS (RTPS) and UDP

7 Conclusion and Future Work

- It is possible to connect two different software stacks using DDS.
- IPC implementation in both ROS 2 and Adaptive AUTOSAR needs to be implemented for syntactic interoperability between ROS 2 and Adaptive AUTOSAR. It is clear from the study of ARINC 650 [14, 15] that there is a need to have build support DDS inside your software.
- DDS can be implemented on top of unreliable protocol like UDP, but it offers reliability setup over it. It can use unicast or multicast, depending on the network.

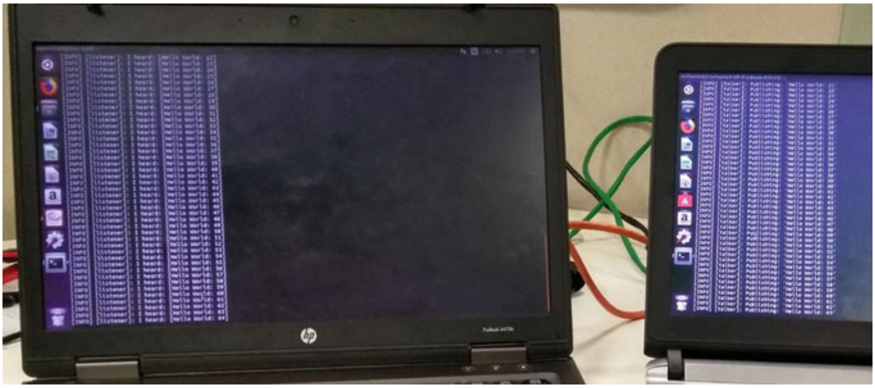


Fig. 14 Running instances of ROS on different machines using Ethernet cable

- Interoperability is solved using DDS by using different mechanisms, QoS services, shared space, etc. DDS is easier to implement due to abstraction. It also offers implementation in many different programming languages.
- Our research gives full conceptual view on DDS, AP, and ROS 2. Even more softwares can be integrated according to need of the future.
- DDS in Fog Computing: If we want to shift our computing from cloud to edge, interoperability could be a major challenge addressed by DDS. Fog computing is also another critical part of autonomous vehicles in remote areas, large farms using autonomous vehicles in a slow connection.
- As the number of IoT devices are increasing day by day at a very fast rate, DDS can solve such interoperability and heterogeneity problem.
- We feel that DDS will bring a revolution in IoT in the near future.

References

1. Han S et al (2016) On AUTOSAR TCP/IP performance in in-vehicle network environments, automotive networking and applications. IEEE. https://doi.org/10.1109/MCOM.2016.1500167CM
2. Zeyu W, Jinsong Y, Wubin S (2017) Distributed test system based on publish/subscribe middleware. In: IEEE 13th international conference on electronic measurement & instruments
3. DDS Security, Object Management Group (OMG) Std. ptc/17-09-20, Rev. 1.1, September 2018. http://www.omg.org/spec/DDS-SECURITY/1.1/
4. Hussain MI. Internet of Things: challenges and research opportunities. Published in international conference on dependable systems and networks workshops, vol 35, pp 123–126
5. Mishra R et al (2018) ROS based service robot platform. In: 2018 4th international conference on control, automation and robotics. https://doi.org/10.1109/iccar.2018.8384644
6. Liu Y, Guan Y, Wang R, Zhang J, Li X (2018) Formal analysis and verification of DDS in ROS2. In: 16th ACM/IEEE international conference on formal methods and models for system design (MEMOCODE). IEEE. https://doi.org/10.1109/MEMCOD.2018.8556970

7. Bellavista P, Corradi A, Foschini L, Pernafini A (2013) Data distribution service (DDS): a performance comparison of open splice and RTI implementations. In: IEEE symposium on computers and communications (ISCC). IEEE. https://doi.org/10.1109/ISCC.2013.6754976
8. Rhoades BB et al. Design and development of a ROS enabled CAN based all-terrain vehicle platform
9. Maruyama Y, Kato S, Azumi T (2016) Exploring performance of ROS2. ACM. https://doi.org/10.1145/2968478.2968502. ISBN 978-1-4503-4485-2/16/10
10. Dauphin L, Baccell E, Adjih C (2018) RIOT-ROS2: low-cost robots in IoT controlled via information-centric networking. IFIP
11. Koksal O, Tekinerdogan B (2017) Obstacles in data distribution service middleware: a systematic review. Futur Gener Comput Syst ScienceDirect 68(2017):191–210. https://doi.org/10.1016/j.future.2016.09.020
12. Yim H-J, Seo D, Jung H, Back M-K, Kim I, Lee K-C (2017) Description and classification for facilitating interoperability of heterogeneous data/events/services in the Internet of Things. Science Direct. https://doi.org/10.1016/j.neucom.2016.03.115
13. Furst S et al (2016) AUTOSAR for connected and autonomous vehicles. In: 46th annual IEEE/IFIP international conference on dependable systems and networks workshops. https://doi.org/10.1109/DSN-W.2016.24
14. Perez H (2017) Handling heterogeneous partitioned systems through ARINC-653 and DDS. Comput Stand Interf ScienceDirect. https://doi.org/10.1016/j.csi.2016.10.012
15. Chen T, Hu X, Zhang G, Xiao J (2018) Implementation of data distribution service interface based on ARINC653 system. In: 13th IEEE conference on industrial electronics and applications (ICIEA). https://doi.org/10.1109/iciea.2018.8397755
16. Kim J, Smereka JM, Cheung C, Nepal S, Grobler M (2018), Security and performance considerations in ROS 2: a balancing act. Cornell University. arXiv:1809.09566
17. eProsima Fast RTPS Performance. eProsima, June 2018. http://www.eprosima.com/index.php/resources-all/performance/40-eprosima-fast-rtps-performance
18. Kim J et al (2018) Security and performance considerations in ROS 2: a balancing act
19. Vignesh UP (2017) ROS based stereo vision system for autonomous vehicle. In: IEEE international conference on power, control, signals and instrumentation engineering (ICPCSI-2017). https://doi.org/10.1109/icpcsi.2017.8392121
20. Auliya RS, Sheu RK, Liang D, Wang WJ (2018) IIoT testbed: a DDS-based emulation tool for industrial IoT applications. Int Conf Sys Sci Eng (ICSSE). https://doi.org/10.1109/ICSSE.2018.8520091
21. Alaerjan A, Kim DK, Kafaf DA (2017) Modeling functional behaviors of DDS. IEEE
22. Yuefeng H (2018) Study on data transmission of DCPS Publish–Subscribe model. In: 2018 2nd IEEE advanced information management,communicates, electronic and automation control conference (IMCEC 2018)
23. Shokrollahi S, Shams F (2017) Rich Device-Services (RDS): a service-oriented approach to the Internet of Things (IoT). Wireless Pers Commun (2017) 97:3183–3201. https://doi.org/10.1007/s11277-017-4669-2
24. Heng Z, Jianguo H, Xiaoyuan Z, Hanqiang D (2017) Research on LVC real-time integration based on DDS. In: 2017 4th international conference on information science and control engineering. https://doi.org/10.1109/ICISCE.2017.131
25. Alaerjan A, Kim DK, Ming H, Malik K (2018) Using DDS based on unified data model to improve interoperability of smart grids. In: 2018 the 6th IEEE international conference on smart energy grid engineering
26. Priyadarshi D, Behura A (2018) Analysis of different IoT protocols for heterogeneous devices and cloud platform. In: International conference on communication and signal processing
27. Park Y, Min D (2015) Distributed traffic simulation using DDS-communication based HLA for V2X. In: 2015 seventh international conference on ubiquitous and future networks. https://doi.org/10.1109/ICUFN.2015.7182584
28. Takrouni M, Gdhaifi M, Hasnaoui A, Mejri I, Hasnaoui S (2017) Design and implementation of a simulink DDS blockset and its integration to an active frame steering blockset conformed to

SAE ElectricVehicle. In: 2017 IEEE/ACS 14th international conference on computer systems and applications

29. Hadiwardoyo SA, Gao L (2018) Integrating a middleware DDS application for safety purposes in an underground railway environment. In: 2018 3rd international conference on computer and communication systems
30. Lera FJR, Llamas CF, Guerrero AM, Olivera VM (2017) Cybersecurity of Robotics and Autonomous Systems: Privacy and Safety. In: Dekoulis G (ed) IntechOpen Robotics—legal, ethical and socioeconomic impacts, Chapter 5
31. Source code using ROS2 evaluations. https://github.com/ros2/ros2/releases/tag/release-ardent-20180307

IoT-Enabled Water Quality Monitoring System

G. Kanagaraj, T. Primya, K. Sashi Rekha, C. Vinothini and P. Anitha

Abstract In case of water quality monitoring, smart solutions are gaining more importance with communication technology. By using a specific equipment, the quality of water is tested on each attributes like minerals, temperature and so on. This process consumes more time to complete for the given sample. This paper contains two main activities. In application side, a detailed survey on recent work has been carried out to perform smart water quality monitoring in terms of application, communication technology used, and types of sensors employed. The next is by using controller with inbuilt Internet connectivity module to monitor parameters such as temperature and turbidity using low cost and less complex smart water quality monitoring system. The system contains an appropriate webpage for enhancing the user convenience on the deviation of water quality parameters.

Keywords Arduino · Ethernet shield · ThinkSpeak · Turbidity sensor

1 Introduction

Due to the enormous sources of pollutants, ensuring the safety of water is considered as a major challenge. Water over exploitation of natural resources is the main cause for it. Water pollution to a large extend is due to the rapid industrialization and agricultural growth. Sometimes, the problem is aggravated due to the non-uniform distribution of rainfall. To determine the quality of water, individual practices play a major role [1].

The point and non-point sources of pollution tend to adversely affect the water quality, which includes discharge from sewage, industrial discharge, agricultural fields' run-off and run-off from urban. The next level sources of water contamination include droughts and floods and user's lack of awareness and education. To maintain

G. Kanagaraj
Kumaraguru College of Technology, Coimbatore, India

T. Primya (✉) · K. Sashi Rekha · C. Vinothini · P. Anitha
Dr. N.G.P. Institute of Technology, Coimbatore, India
e-mail: primyacse@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_26

the quality of water resources, user involvement needed in the areas such as hygiene, storage of critical elements, disposal of waste materials and environmental sanitation. Diseases can spread through poor quality water, which may lead to death and also socio-economic progress hampers [2].

In order to provide data, contents such as define real-time conditions and trend happenings are taken into account at specified locations and ordered intervals. The aim of water quality monitoring through online contains critical water quality measurement parameters such as physical and chemical properties, microbial, to identify parameters deviations and supply early warning hazards identification. The monitoring system provides actual time investigation of data composed and suggests suitable corrective measures [1].

2 Automated Water Quality Monitoring System

2.1 Using Raspberry PI

The use of raspberry pi along with Arduino kit helps in the storage of data in a Secure digital card (SD card) and then inspected when the memory is full or at a periodic time. The data sent from the sensors are collected from the Arduino and the raspberry pi stores the data along with the time in a specified format for retrieval. This type of storing the data and analysing it in a periodic interval are possible if the water quality is measured for a small range or it is measured near to the analysis area.

Drawbacks

The raspberry pi can be used as a storage for the sensor data but there is no constant maintenance of the values when the tanks are placed at a distance. And if there are more than one storage places, SD card should be provided to all the places and the collection of SD cards after memory is full or it should be done at periodic intervals. This is a difficult task [1].

2.2 Digital LCD Display

The digital LCD form of display can be utilized for viewing the values that are read from the sensors. This LCD display helps in the real-time monitoring of data that are produced by the sensors. Any change in sensor value can be seen and the rectifying steps can be taken within minutes. The LCD display is a module connected to the Arduino. Sensors provide data to the Arduino and Arduino helps in viewing the data in the LCD display. LCD display can be mounted on the central maintenance or the place where there is a constant maintenance of the tanks.

Drawbacks

For a small project with one/two storage spaces, it is easy to manipulate the data from the LCD display. But it cannot be maintained for a large scale like colleges as there are more number of storage tanks. Thus, the usage of LCD display appears as a major drawback [3].

3 IoT-Enabled Water Quality Monitoring System

Water is utilized for numerous activities such as utilization, gardening, and travel, which may concern mainly on the water quality. The water quality monitoring is essential, which includes numerous substance parameters like alkaline, redox potential, conductivity, dissolved oxygen, ammonium and chloride ion amount.

The existing system will observe the water bodies, and it is agreed that the methods used in laboratory are too unhurried to develop a running response and it does not provide a plane of public health fortification in real time. Owing to the infinite increase in output of the global industry, and the over-utilization of terrain and marine property, the excellence of water available to public has been deteriorated deeply.

The overall decrease of water quality has internationally contributed with the high use of fertilizers in farms and other chemicals in sectors like withdrawal and production. Water is an important necessitate for human endurance and there must be mechanisms position in place to powerfully analyse the quality of water that has been offered for drinking in urban and municipality. The accessibility of superior eminence water is overriding to prevent water-borne diseases as fit as recovering the worth of life. The surface water monitoring improvement in network is an essential element in the evaluation and fortification of water quality. A prototype is developed for easy to mount expertise by which the diverse surface water value indicators can be considered [4].

With the help of Ethernet shield, the details will be uploaded constantly in real time from the Arduino board. The management and upload of this data to cloud and the daily report will be published in the website specially designed for this project.

3.1 Architectural Design

Figure 1 shows the architectural design of IOT-enabled water quality monitoring system which consists of the subsequent key components (Fig. 2).

3.2 Implementation

The implementation of quality monitoring is explained by the flow chart given in Fig. 3.

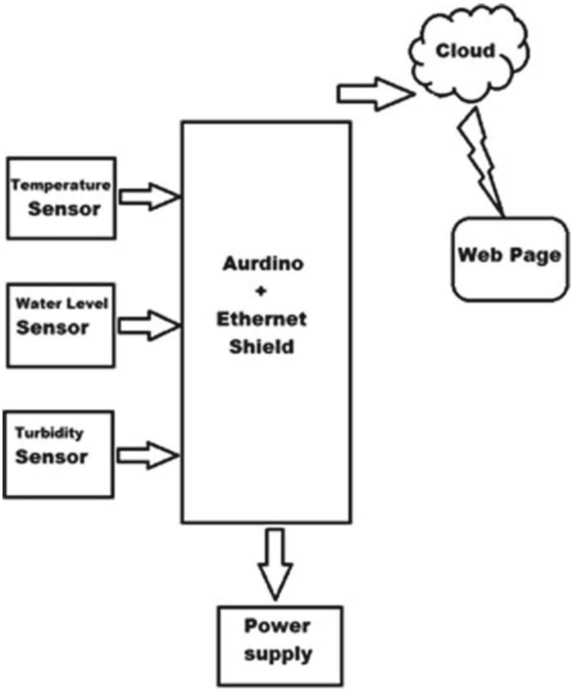


Fig. 1 Architecture design

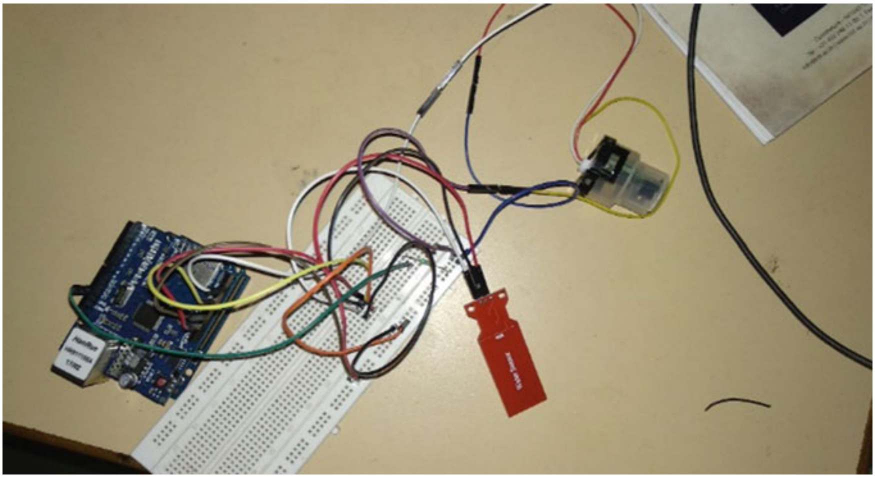
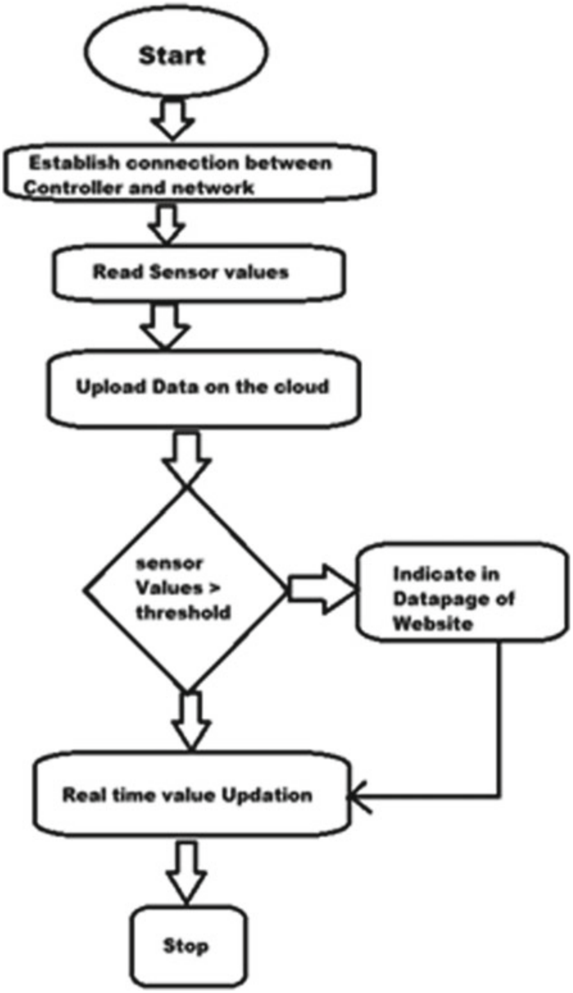


Fig. 2 Architectural view

Fig. 3 Implementation design


Start
Establish connection between Controller and network
Read Sensor values
Upload Data on the cloud
sensor Values > threshold
Indicate in Datapage of Website
Real time value Updation
Stop

4 Components Involved

4.1 Data Retrieval

The data retrieval is a module to collect all the measurement data at a periodic interval from the storage and sent it directly to the Arduino. This module can only collect the data. It cannot do further processing from the data collected. The further process with the data can be taken care of the Arduino board. The data retrieval is done using different types. Here, we use the sensors to collect the data from the storage tanks. The sensors are connected to the Arduino and programmed in a way that the entire sensor sense the environment at the time of filling of tanks and sent the sensed data to the Arduino. The model diagram for the data retrieval is shown Figs. 4, 5 and 6.

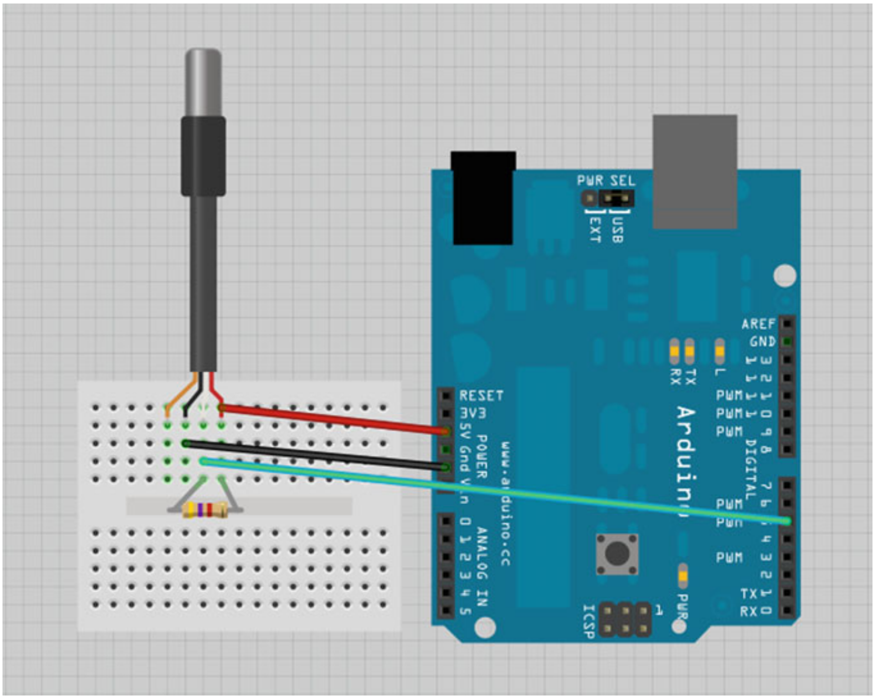
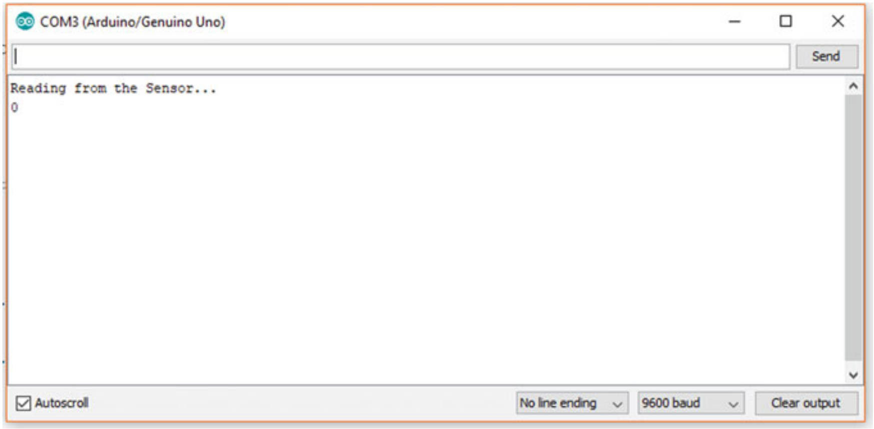
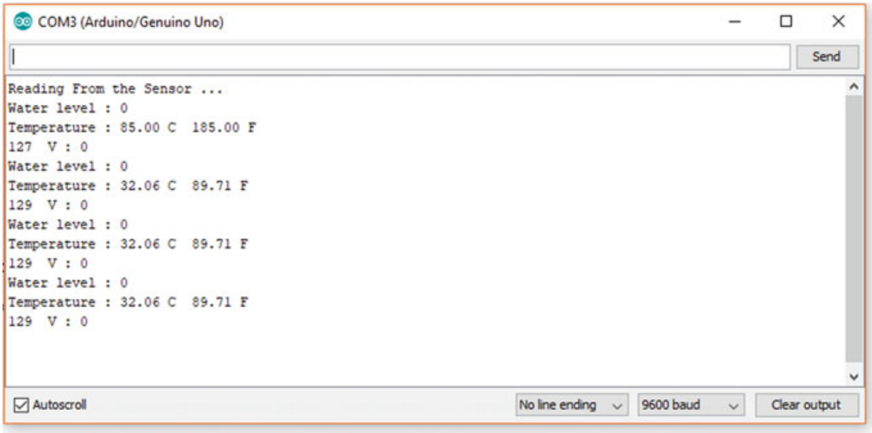


Fig. 4 Arduino connection to temperature sensor



```
Reading from the Sensor...
0
```

Fig. 5 Data retrieval from temperature sensor



```
Reading From the Sensor ...
Water level : 0
Temperature : 85.00 C  185.00 F
127  V : 0
Water level : 0
Temperature : 32.06 C  89.71 F
129  V : 0
Water level : 0
Temperature : 32.06 C  89.71 F
129  V : 0
Water level : 0
Temperature : 32.06 C  89.71 F
129  V : 0
```

Fig. 6 Data retrieval from other sensors

This is the connection of the Arduino with the temperature sensor that can send the temperature of the water at the particular time. The measurements are sent to the Arduino and it is then uploaded to the cloud.

4.2 Ethernet Shield Connectivity

To connect the Ethernet shield with Arduino hardware and PC, the Ethernet shield is placed firmly on the Arduino hardware. An Ethernet shield stacked on the Arduino hardware is shown. The Ethernet shield can be connected to a network router, or to computer, using an RJ45 cable (Figs. 7 and 8).

An Arduino board is linked with Internet using Arduino Ethernet Shield 2. The WiZnet W5500 provides a complex stack consist of mutual TCP and UDP. It supports up to eight concurrent socket relations. The Ethernet library is second-hand to inscribe sketches that join to the Internet by means of the shield. The Ethernet Shield 2 connects to an Arduino board with long wire-wrap headers throughout the shield. It keeps the pin arrangement intact and allows a different shield to be stacked on the peak of it.

4.3 ThinkSpeak–Cloud Connectivity

The cloud architecture used to store the data here is ThinkSpeak. The collected information from the sensors is then send to the Arduino where the records are sent to cloud services with the aid of Ethernet shield.

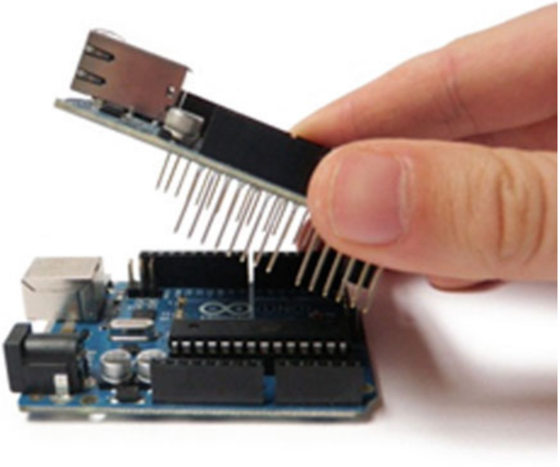


Fig. 7 Ethernet shield connectivity

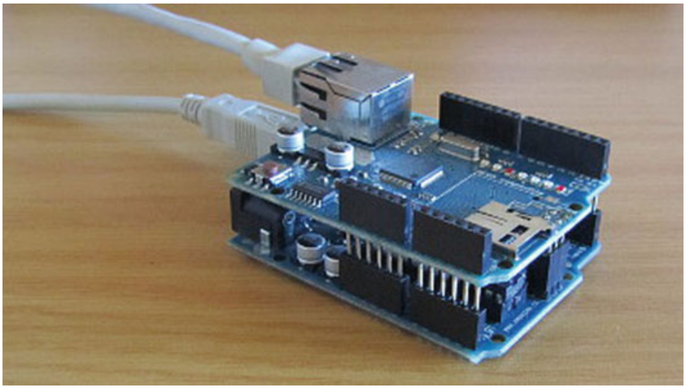


Fig. 8 Arduino with Ethernet shield

The statistics is maintained in the cloud and the periodic information is sent to the management team in that particular area who maintains the water quality system. Any deviation in measurements is intimated to the team in order to take quick actions (Figs. 9 and 10).

ThinkSpeak is an IoT analytics podium service that allows aggregating, visualizing and analysing survive statistics streams in the cloud. It gives immediate visualizations of facts posted by the devices to ThingSpeak. To perform MATLAB code in ThingSpeak, carry out online examination and dispensation of the data as it comes inside. ThingSpeak is worn for prototyping and evidence of idea IoT systems that need analytics.

ThingSpeak Key Features

The IoT Cloud Platform

Fig. 9 Cloud inculcated with IOT

Fig. 10 ThinkSpeak with IOT

The key capabilities of ThingSpeak include the capability to:

- Simply configure devices to convey data to ThingSpeak by means of trendy IoT protocols.
- Envisage the sensor data in real time.
- Collective data on-demand beginning third-party sources.
- Use the power of MATLAB to make sense of your IoT data.
- Scamper IoT analytics repeatedly based on schedules or actions.
- Example and construct IoT systems without location up servers or initial Web software.

4.4 Website Creation

The website is created to provide easy maintenance and to get the real-time values updated as a graph so that the management can easily view the current situation happening in the place where this project is set. The site is done offline and site

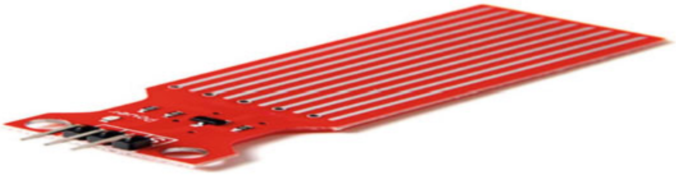


Fig. 11 Water level sensor

is hosted in the heroku hosting platform. Heroku, a container-based Platform as a Service (PaaS) in cloud.

The developers use Heroku to organize, administer and extent modern applications. Its platform is graceful, supple and effortless to use, offering developers the simplest path to getting their apps to market. It is completely managed give developers the liberty to centre on their middle creation lacking the disruption of maintaining servers, hardware, or communications. The Heroku understanding gives forces, equipment, workflows and linguist sustain, all considered to improve developer efficiency.

In this heroku hosting the heroku hosting customer for windows have to be downloaded from the executive site. Then once setting up, the command line can be worn for easy hosting after login in the command prompt.

5 Hardware Requirements

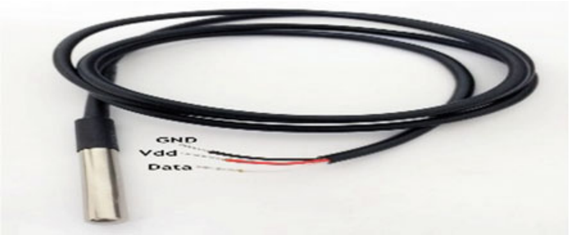
5.1 Water Level Sensor

Without any affecting parts, the liquid plane sensor calculates the fluid level in tanks, reservoirs and in its surroundings. The sensing probe element comprises of an extraordinary wire cable which is accomplished for truthfully sensing the exterior level of almost any fluid, together with water, salt water and oils. Sensor element is electrically insulated and secluded from the water into which it is inserted, and will not deteriorate in the overload of time. Contrasting other sensors, the quantity range is changeable from a few cm to a few metres. The appraisal is reported back as an analogue voltage ranging from 0 to 3 V where 0 V represent the non-immersed sensor, and 3 V represents the highest water level (Fig. 11 and 12).

5.2 Temperature Sensor

It includes a humidity sensing component, a NTC temperature sensor and an IC on the reverse side of the sensor. The humidity sensing component is used to measure humidity, which has two electrodes with dampness holding substrate among them.

Fig. 12 Temperature sensor



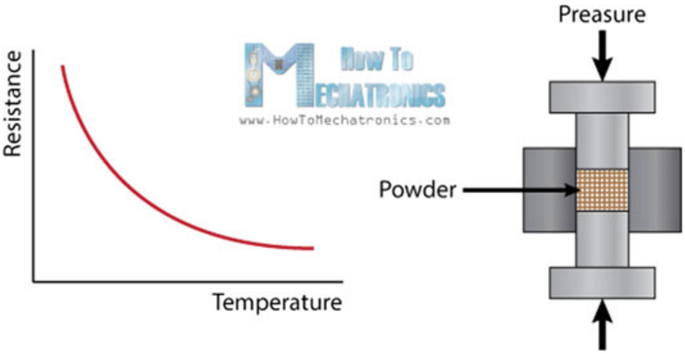


Fig. 13 Temperature graph

The conductivity of the substrate varies or the resistance among these electrodes varies as the humidity changes. The variation in resistance is calculated and processed by the IC which makes it prepared to be converted by a microcontroller.

To assess temperature, NTC temperature sensor or a thermistor is used. A thermistor is a changeable resistor that varies its resistance with variation of the temperature. This type of sensors is finished by sintering of semi conductive equipment such as ceramics or polymers in order to supply overweight changes in the resistance with just tiny changes in warmth. The term “NTC” means “negative temperature coefficient”, which income that the confrontation decreases with augment of the high temperature (Fig. 13).

5.3 Turbidity Sensor

In a fluid, turbidity is the quantitative enumerate of pending particles. It may be soil in water or chocolate flake in favourite milk shake. While chocolate is somewhat so wanted in our drinks, soil particles are completely undesired. There are several manufacturing and family circle solutions that make use of water in some or other way keeping aside the moveable purposes. A car use water to unsoil the windshield, a power plant desires it to cool the reactors, washing machines and dish washers

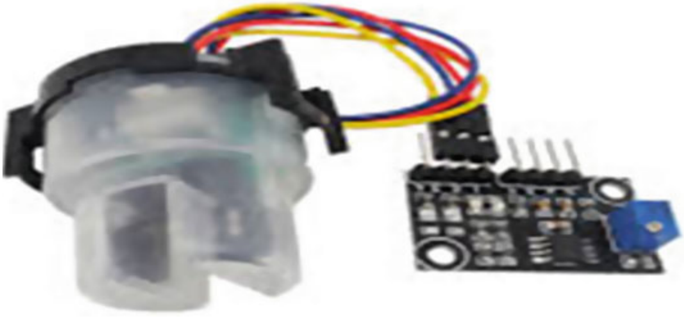


Fig. 14 Turbidity sensor

Fig. 15 Arduino UNO

depends on water like fish. How does this equipment get to be familiar with concerning the turbidity? The nature's evolutionary contribution of senses to discover soil in the water, but what about washing machines? No eyes to see, no tongue to taste, no skin to feel but just a plastic body with some buttons and motor inside. How does it so elegant to work as per soil deferment? Turbidity sensor, which the length of with a micro controller unit, takes care of turbidity capacity. It is craft with synthetic and some metal-alloy traces, turbidity sensor uses light to put across in sequence in relation to turbidity in water (Figs. 14 and 15).

5.4 Arduino Uno

Arduino Uno is a microcontroller board based on the ATmega328P. It includes 14 digital input/output pins, 6 analogue inputs, a 16 MHz quartz crystal, a USB connection, a power jack, an ICSP header and a reset button. The ATmega328 on the Arduino Uno comes pre-programmed with a boot loader that allows uploading innovative code to it devoid of the use of an external hardware programmer. It communicates during the original STK500 procedure. The board can be power-driven via the USB connection or with an outside power supply. The power source is particular by design. It can activate on an external contribute from 6 to 20 volts. If it is complete with less than

7 V, the 5 V pin may used to supply less than 5 volts and the board may become unbalanced. The use of more than 12 V, the voltage regulator may overheat and injure the board. The suggested range is 7 to 12 V. Arduino/Genuino Uno contains quantity of facilities for communicating with a computer, another Arduino/Genuino board or other microcontrollers. The ATmega328, provides UART TTL (5 V) serial communication, is accessible on digital pins 0 (RX) and 1 (TX).

5.5 Ethernet Shield

Arduino board is used to connect the Arduino Ethernet Shield 2 with the Internet. The WiZnet W5500 provides a network stack capable of together TCP and UDP. It chains up to eight concurrent socket connections. The Ethernet library is used to inscribe sketches that attach to the Internet by means of the shield (Fig. 16).

The Ethernet Shield 2 connects to an Arduino board with long wire-wrap headers from end to end the shield. It keeps the pin layout unbroken and allows a different shield to be stacked on apex of it. The current modification of the panel exposes the 1.0 pinout on rev 3 of the Arduino UNO Board. It has a paradigm RJ-45 connection, with an incorporated line transformer and Power greater than Ethernet enabled. It gives an onboard micro-SD card slot, it can be used to store files for helping over the network and it is well-suited with the Arduino Uno and Mega using the Ethernet library.

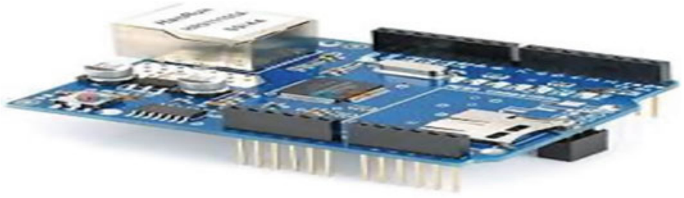


Fig. 16 Ethernet shield

6 Software Requirements

6.1 Arduino IDE

For a compiler, a program for Arduino may be printed in any programming language that produces binary machine code for the objective processor. It gives a development surroundings for their microcontrollers, AVR Studio and the newer Atmel Studio.

6.2 HTML

To create Web pages and Web applications, Hypertext Markup Language (HTML) is the standard markup language The Web browsers, obtain HTML documents from a Web server or from local storage space and provide the permit into multimedia Web pages. Hypertext Markup Language defines the constitution of a Web page semantically and initially included cues for the exterior of the document. HTML may embed programs written in a scripting language such as JavaScript which affects the performance and substance of Web pages. Insertion of CSS defines the appear and design of content.

6.3 CSS

Cascading Style Sheets, referred to as CSS, is a trouble-free design language intended to make things easier the process of making Web pages reasonable. CSS controls the colour of the text, the style of fonts, the spacing among paragraphs and it explains how columns are sized and laid out.

6.4 Bootstrap

For faster and easier Web development Bootstrap is an authoritative front–end framework. It too comprises HTML- and CSS-based design templates for familiar user interface components like Dropdowns, Alerts, Modals Typography, Forms, Buttons, Tables, Accordion, Carousel Navigations, Tabs, and many other as well as optional JavaScript extensions.

7 Summary

The result of the proposed project lies in developing a water monitoring IOT set-up with a website linked to the set-up to provide a real-time management of the quality of water. The scope of the project lies in integrating the hardware sensors using Internet of things and the software part of the website. It also helps all the people in management team to know the current status through the website. The use of the website hosted is very helpful in monitoring the quality of water and ease of use.

8 Snapshots

See Figs. 17, 18 and 19.

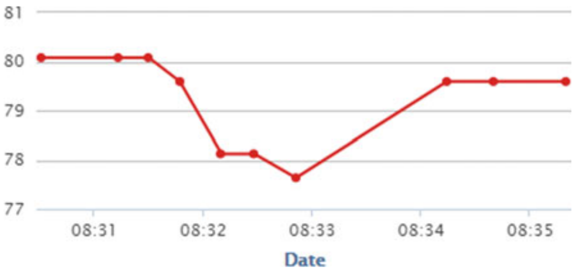
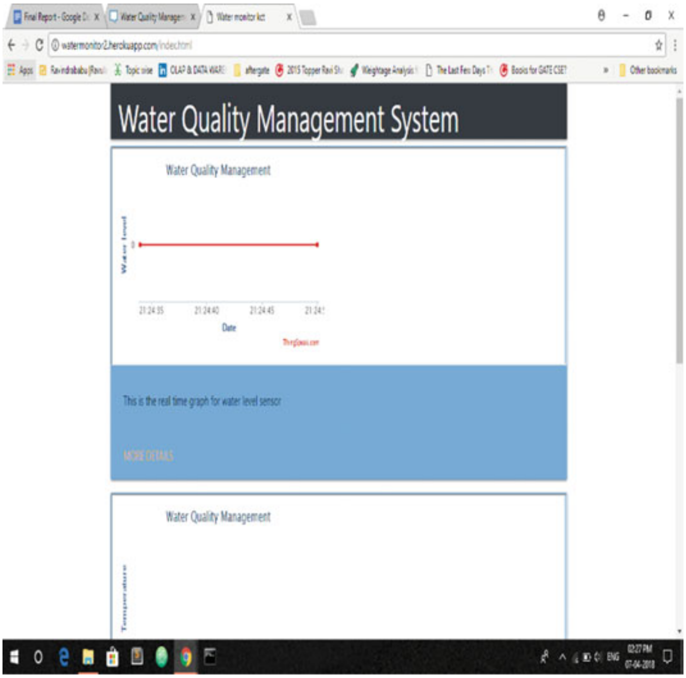


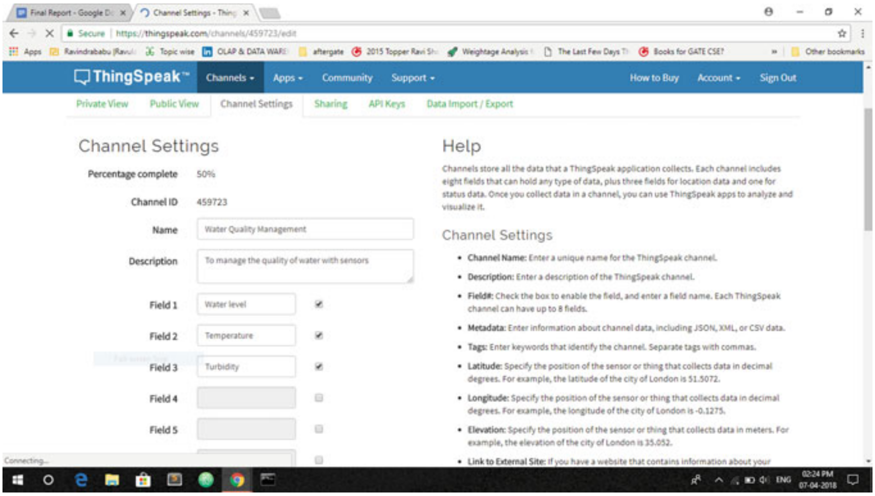
Fig. 17 Data retrieval



Water Quality Management System

This is the real time graph for water level sensor

Fig. 18 Website creation



Channel Settings

Percentage complete 50%

Channel ID 459723

Name Water Quality Management

Description To manage the quality of water with sensors

Field 1 Water level ☑

Field 2 Temperature ☑

Field 3 Turbidity ☑

Field 4 □

Field 5 □

Help

Channels store all the data that a ThingSpeak application collects. Each channel includes eight fields that can hold any type of data, plus three fields for location data and one for status data. Once you collect data in a channel, you can use ThingSpeak apps to analyze and visualize it.

Channel Settings

- **Channel Name:** Enter a unique name for the ThingSpeak channel.
- **Description:** Enter a description of the ThingSpeak channel.
- **Field#:** Check the box to enable the field, and enter a field name. Each ThingSpeak channel can have up to 8 fields.
- **Metadata:** Enter information about channel data, including JSON, XML, or CSV data.
- **Tags:** Enter keywords that identify the channel. Separate tags with commas.
- **Latitude:** Specify the position of the sensor or thing that collects data in decimal degrees. For example, the latitude of the city of London is 51.5072.
- **Longitude:** Specify the position of the sensor or thing that collects data in decimal degrees. For example, the longitude of the city of London is -0.1275.
- **Elevation:** Specify the position of the sensor or thing that collects data in meters. For example, the elevation of the city of London is 35.052.
- **Link to External Site:** If you have a website that contains information about your

Fig. 19 ThingSpeak water monitoring

References

1. Purohit A, Gokhale U (2014) Real time water quality measurement system based on GSM. IOSR (IOSR-JECE) 9(3), Ver. V
2. Lom M, Pribyl O, Svitek M (2016) Industry 4.0 as a part of smart cities. 978-1-4673-9948-7/16 © IEEE
3. Kedia N (2015) Water quality monitoring for rural areas—a sensor cloud based economical project' by in (NGCT-2015) 4–5. 978-1-4673-6809-4/15/$31.00 ©2015 IEEE
4. Daigavane VV, Gaikwad MA (2017) Advances in wireless and mobile communications, vol 10, no 5, pp 1107–1116. ISSN 0973-6972
5. Bhatt J, Patoliya J (2013) Real time water quality monitoring system. 978-1-47990792-2/13/$31.00 © IEEE
6. Kartakis S, Yu W, Akhavan R, McCann JA (2015) Adaptive edge analytics for distributed networked control of water systems. In: IEEE first international conference on internet-of-things design and implementation (IoTDI)
7. Daigavane VV (2017) IoT based water quality monitoring system. Int J Ind Electron Electr Eng 4. ISSN: 2347-6982
8. Sun Z, Li CH, Bisdikian C, Branch JW, Yang B (2013) QOI-aware energy management in IoT sensory environments, pp 1–9. https://doi.org/10.1109/SECON.2010.5508203
9. Karthik Kumar R, Chandra Mohan M, Vengateshapandiyan S, Mathan Kumar M, Eswaran R (2014) Solar based advanced water quality monitoring system using wireless sensor network. Int J Sci Eng Technol Res (IJSETR) 3(3):385–389
10. Cheng P, Wang X-L (2010) The design and implementation of remote-sensing water quality monitoring system based on SPOT-5. In: Second IITA international conference on geoscience and remote sensing, pp 6–10
11. Nagarajan R, Dhanasekaran R (2013) Implementation of wireless data transmission in monitoring and control. In: International conference on communication and signal processing, India, April, pp 83–87
12. Primya T (2018) Hybrid algorithm based user authentication and data security using image comparison and OTP. Asia Pac J Res I(LXXXVII)

Energy-Efficient Routing-Based Clustering Approaches and Sleep Scheduling Algorithm for Network Lifetime Maximization in Sensor Network: A Survey

Rajiv R. Bhandari and K. Rajasekhar

Abstract Along with number of problems associated with WSNs, one of the major issue we chose to study is their clustering topology and energy utilization techniques. Both these parameters are very much responsible in determining the life of nodes, quality of service, delay in data transmission, etc. So, it is very important to examine the cluster-based routing protocols and energy optimization protocols. The cluster routing is based on the selection of cluster head nodes for data transmission, and the parameters which are used for the making of an optimized network mainly depend on number of nodes, position of base station, and the network size. So, a well-settled cluster is tried to be designed with the study of various algorithms early proposed. And for energy optimization of network, we studied "sleep/wake-up" algorithm, which makes the nodes sleep during its ideal mode and wake it up when data transmission is to be done. With this sleep/wake-up algorithm important point to be kept an eye is the delay during this shifting between sleep and wake up or making sure that the selected path should not be engaged as well as it must be shortest path from base station. So, based on these two protocols, various papers are studied, and the comparative result of this protocol in various scenarios is carried out.

Keywords Routing · Clustering · Wireless sensor network · Sleep/wake up

1 Introduction

In WSN, network is formed by sensor nodes that are aligned arbitrarily or in immobile manner according to the network application [1]. The typical working of WSN is that the sensor nodes sense data and transmit it to neighbor node or to sink node within network or outside the network which totally depends upon the application. Since this sensor nodes are running on the battery, and hence, due to this limitation of energy, it must be optimized in order to give a better durability of these sensors. So

R. R. Bhandari (✉) · K. Rajasekhar
Department of Computer Science Engineering, Koneru Lakshmaiah Education Foundation Green Fields, Guntur District, Vaddeswaram, Andhra Pradesh 522502, India
e-mail: rajivrbhandari@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_27

sensor nodes are designed with consideration parameters like tiny node size, minimal costing, etc. These are considered in order to improve the efficiency of sensors and also make the network fast and steady. So, to overcome such network issues we come with the comparative study of many algorithms so as to make a fully optimized network which is smart as well as responsive when needed. For this, we are mainly looking forward to two types of protocols one is cluster-based routing protocol and another one is sleep/wake-up protocol.

In routing based cluster protocol most of the time depends on network structure and can be roughly divided into two categories: hierarchical and uniform routing. In a uniform topology, all nodes accomplish same jobs and have same functionalities of every node within network. In this topology, data communication is achieved in hop-by-hop, flooding, and gossiping manner. In a hierarchical topology, different nodes performed different tasks and are well organized in cluster according to specific requirements or metrics. Generally, there is cluster head along with other member ordinary nodes, and all are arranged in hierarchical levels. The communication and data processing are carried out by a monitoring node called as cluster head node (CH), and all other nodes are called as member nodes and are used for sensing the information. Among many routing protocols which are used in WSNs, low-energy adaptive clustering hierarchy (LEACH) is the classic one. Here, we are making comparative study of various such routing protocols. And we have also made a study based on sleep/wake-up protocols too, which aims to minimize idle processing time [2]. In order to study sleep/wake-up protocols, adjustments of sleep and awake time for sensors during particular period are important to study. Basically, during ideal state of node, the energy supplied is wasted as during this ideal time it won't transmit any data. Hence, the motto of sleep/wake-up scheduling is to minimize or make the adjustment in wake time of sensor. These methodologies for wake-up methods are classified into three types: (1) on-demand, (2) synchronous, and (3) asynchronous. So, the comparative study of various algorithms associated with the energy optimization and time scheduling is also done here.

1.1 Clustering and Routing in WSN

The basic structure of standard cluster consists of number of sensors (for data capturing and analysis) and transceiver (to transmit data through gateway node), power source (mainly batteries), sink node (to sense data and communicate with base station), and many other parts. Figure 1 shows a simple cluster-based network. In intra-cluster, the communication is done between a node within a cluster, but in inter-cluster, communication is carried out between one cluster head with other and with the sink. This is to be done so as to save significant energy required for all the nodes. With the use of these techniques, we can make communication between clusters so that all the nodes need not to be active all the time and also the range of particular base station is increased as nodes from one cluster can communicate with other node within different cluster. This technique is very useful in making an

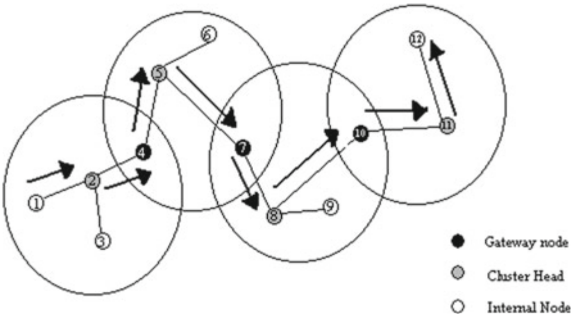


Fig. 1 Cluster and routing system

efficient WSN routing. Moreover, this technique allows not only reduction in routing tables calculations for both CH selections as well as for member nodes selection but also making the bandwidth reusability possible.

Here, in this figure, we can see the inter-cluster and intra-cluster communication is done. It makes a system energy efficient as we can see we do not need all this node to be awakened, and the range of particular cluster is extended.

Calculation for the cluster head selection depends on its score, as node with higher score has priority to be elected as CH and other nodes join this CH in its proximity. The calculation of score is done by the following Eq. (1).

$$\text{score}(v) \leftarrow \sum_{i=1}^{\text{number of neighbours}} \frac{1}{\text{dist}^2(v,i)} \tag{1}$$

In Eq. (1), the score of node v is calculated. Basically, the selection depends up to two metrics-node degree (defines number of neighbors in cluster range) and node centrality (centrality of a node among its neighbor). Cluster head formation is dependent on the value of this node v calculated from the neighboring node, and if this distance is small, ultimately, the value of score(v) is increased and this value also depends on the number of nodes (proportionally increases). So, we can say node v is more likely to be CH and creates the intense network. For applications, creating more closely compacted clusters is very supportive to group nodes in close locality.

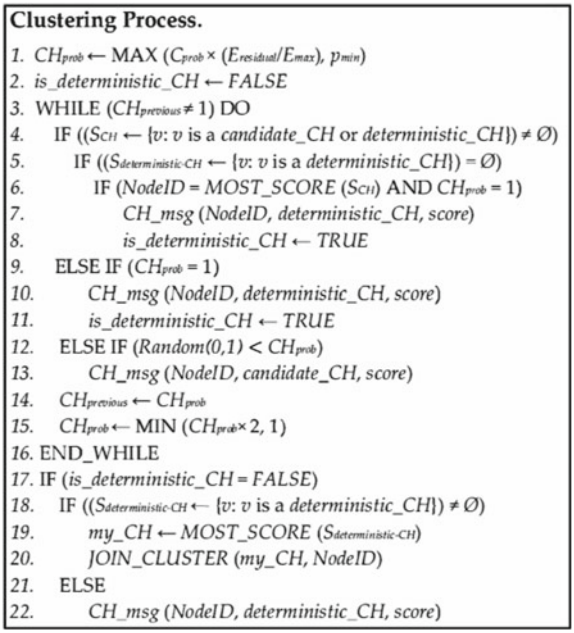
The basic steps involved in cluster routing are shown in Fig. 2.

Figure 2 shows the complete procedure of the clustering process algorithm in which the selection of CH is calculated by using the following equation:

$$\text{CH}_{\text{prob}} = \text{MAX}(C_{\text{prob}} * \left(\frac{E_{\text{residual}}}{E_{\max}}\right), p_{\min}) \tag{2}$$

where E_{residual} is current energy of node and $E_{\max}$ is maximum energy. It is to note that the value of CH_{prob} should fall below $p_{\min}$. After this, the while loop is iterated (from Fig. 2). Up to step 8, the node decision took place means whether the node will become a CH or will join any other CH. Next iteration is performed

Fig. 2 Clustering process



```
Clustering Process.
1. $CH_{prob}$ ← MAX ($C_{prob}$ × ($E_{residual}/E_{max}$), $p_{min}$)
2. is_deterministic_CH ← FALSE
3. WHILE ($CH_{previous}$ ≠ 1) DO
4.    IF (($S_{CH}$ ← {v: v is a candidate_CH or deterministic_CH}) ≠ Ø)
5.       IF (($S_{deterministic-CH}$ ← {v: v is a deterministic_CH}) = Ø)
6.          IF (NodeID = MOST_SCORE ($S_{CH}$) AND $CH_{prob}$ = 1)
7.             CH_msg (NodeID, deterministic_CH, score)
8.             is_deterministic_CH ← TRUE
9.    ELSE IF ($CH_{prob}$ = 1)
10.         CH_msg (NodeID, deterministic_CH, score)
11.         is_deterministic_CH ← TRUE
12.   ELSE IF (Random(0,1) < $CH_{prob}$)
13.         CH_msg (NodeID, candidate_CH, score)
14.   $CH_{previous}$ ← $CH_{prob}$
15.   $CH_{prob}$ ← MIN ($CH_{prob}$ × 2, 1)
16. END_WHILE
17. IF (is_deterministic_CH = FALSE)
18.   IF (($S_{deterministic-CH}$ ← {v: v is a deterministic_CH}) ≠ Ø)
19.         my_CH ← MOST_SCORE ($S_{deterministic-CH}$)
20.         JOIN_CLUSTER (my_CH, NodeID)
21.   ELSE
22.         CH_msg (NodeID, deterministic_CH, score)
```

after collecting the coded and doubled value of CH_{prob} from pervious iteration level. When the $CH_{previous}$ reaches value 1, the respective node will terminate the loop. So, termination of node with higher energy level will be done prior to other nodes with lower energy. After successful execution of 17–20 steps, member nodes having lower energy level will join the deterministic CH. But, it is to be noted that during this complete cluster formation, every deterministic CH or candidate CH can send CH_msg only once. Hence, like this, we can form the more efficient routing protocol for WSN.

1.2 Sleep/Wake-up Algorithm

Another protocol is sleep/wake-up protocol, which is mainly used to make system energy efficient. In this protocol, the nodes are made sleep while in its ideal mode, means it consumes very less amount of energy. In order to make system energy efficient, during this ideal mode, the node won't transfer any data but wakes up whenever needed with very low response time. The sleep/wake-up algorithm mainly depends upon the duty cycle. Figure 3 shows the duty cycle working of node.

In this figure, we can see how the sleep and wake-up switching is done. The packet transmits and receive is done whenever required after listen and in rest of the time, the node is in ideal state or sleeping state. Energy in MAC-based sleep/wake-up protocol is determined by its sleep time. In time slot T_R, for some period, time interval is given

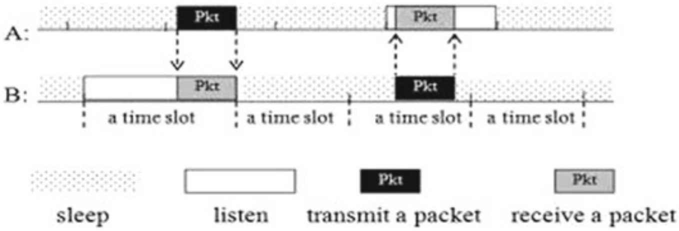


Fig. 3 Duty cycle of node

as (1 − waketime) × T_R. A new node will be in sleeping phase for entire time length, and during this interval, there will be no transmission of data taking place. The time interval for this protocol is given as:

$$t = \frac{E(0)T_R}{T} \times d$$

where T stands for frame duration and d is for duty cycle.

In this system, energy saved by each node can be calculated as:

$$E_{\text{save}} = \frac{E(0) \times T_R \times d \times P_{\text{idle}} \times \left[\left(\frac{n_g-1}{n_g}\right)^{2\times n_h}\right]}{T}$$

where P_{idle} represents power consumption of node during its ideal state. And the power of "*n*" number of nodes can be easily calculated by multiplying the above energy-saving equation with this number of nodes, i.e., "*n*" [3].

Based on these two protocols, we have studied number of papers which have done research on same topics.

2 Literature Survey

2.1 Worked Based on Clustering Protocols

This paper presents a study of WSN clustering protocols in order to make more reliable and optimized network. Various routing indoor and outdoor network protocols are presented in below section.

Amjad et al. [4], in that paper, presented a quality of service-based routing method for heterogeneously clustered WSNs which is done by using nodes with different level of energies and also having different initial energy. So, minimal energy is the point to be calculated in order to achieve the energy optimization of network. The simulated results show improvement in terms of network life, consistency, throughput, and delay minimization.

Kang et al. [5], in that paper, presented a distributed delay-efficient scheme named DEDAS-D to address the MLAS problem in duty-cycled WSNs. DEDAS-D covers two new algorithms for data accumulation, tree construction, and scheduling. This method while addressing MLAS problem gives better simulation results like reduction in data aggregation, and delay of DEDAS-D is reduced by 50.95%.

Zhou et al. [6], in that paper, proposed a new clustering protocol in which the relay nodes are used to share the load of the cluster heads, and for energy optimization, they proposed an improved PSO algorithm which improves the efficiency of cluster structure for longer distance coverage. The improvement in cluster energy management is successfully shown by simulation results.

Wang et al. [7], in that paper, presented a load-balancing and routing protocol which is a multilayered and multihop routing protocol. Although TLCBMH have more message and protocol complexity than RDCA, but still, they both have similar clustering power. In this TLCBMH-based process, the base station access is done via multihop frequency and it makes the system robust. The result comparison of both these techniques shows that the TLCBMH provides better service as it does not lose any clustering ability.

Deepa et al. [1], in that study, presented a routing algorithm analysis with or without data aggregations called as hybrid hierarchal cluster-based secure (HHCS) routing algorithm. The method provides good level of nodal level security as it consists of both group key and pair wise key. Also, it reduces traffic of the network using data aggregation method. The comparative result with LEACH algorithm showed that this HHCS algorithm is more secure as well as more energy efficient.

Sreevidya et al. [8], in this paper, suggested a new energy monitoring and optimization technique for cluster-based routing protocol. In this algorithm, mainly, the energy in data transfer is optimized and end-to-end delay is also optimized, which increase overall lifespan of network. The comparative results with that of AODV protocol show that the life of nodes is enhanced after implementation of this new protocol.

Gnanambigai et al. [9], in this paper, suggested a new hybrid algorithm in order to reduce the energy of system and improve the durability of system and they called this system as QBLEACH. This algorithm limits the usage of number of active nodes for transmission of data which is done in order to reduce the energy required to transmit the data. The simulation results precisely describe the energy required to transfer data, and accordingly, the distribution is done. Depending upon this energy, the distribution path and the number of nodes selection are done which ultimately improve the life of sensor as well as the better energy optimization is observed.

Behera et al. [10], in this paper, defined a best-suited cluster for IoT applications. This algorithm works in the selection of shortest path for data transmission and also selects minimum distance between the active cluster heads. This method gives very efficient results by optimizing lot of energy while transferring data to base station or vice versa. They also proved that the results obtained from this protocol are quite better than that of HEED, PEGASIS, HEER, and TEEN.

Xiao et al. [11], in this paper, introduced the 6LoWPAN hierarchical routing protocol which is based on a switched hierarchical structure. In this protocol, the transport path is merged with the IP address which stores very small amount of routing information. In this protocol, the data can be transferred from any node within cluster as well as outside the cluster to another node of different cluster even cluster in like a node. Another benefit of this protocol is that even if any node gets fail, then the network failure will not affect as data will be passed through another node. The compared result with the traditional RPL protocol shows that the HCPR has faster efficiency of transmission and has less storage of routing information.

Shaha et al. [12], in this paper, defined the new routing protocol for optimizing the routing path for transmission of data from cluster head to respective nodes and finally to sink. And if the node is in direct contact with sink, then the information will be directly sent to sink itself. They used shortest path algorithm to define the most optimized path and faster delivery of packets. They also grouped the nearby nodes in such a way that all these nodes are combined to form a greater network.

Acharjee et al. [13], in this paper, suggested a modified hierarchical cluster-based routing protocol which works in reducing the load on the mesh point portal and group heads. In this algorithm, they introduced helping nods for cluster head, means in case, if the cluster head fails, then this assistant cluster head will take the responsibility of the defined CH node. This algorithm is mainly useful for large area network and hence is more independent and reliable and also gives more throughput than older network. The result of this algorithm has much better throughput for larger network, but for less number of nodes, packet delivery ratio is less than that of HWMP, but for larger number of nodes, it provides lower PDR than BATMAN algorithm.

Misra et al. [14], in that paper, surveyed the clustering-based algorithms based on the state of art. Comparative study based on energy competence, cluster stability/reliability, and load balancing is carried out with respect to this proposed algorithm and other algorithms. This algorithm serves and educates in terms of clustering techniques which is a concern for both military and civil applications. This algorithm is utilized for various applications like security surveillance, environment monitoring, and healthcare system.

Lenka et al. [15], in this paper, suggested a cluster-based rendezvous routing protocol. With respect to this algorithm, the clusters are structured within the rendezvous area in order to achieve scalability and to maintain network load. To find the sink position, not only cluster heads are part of communication, but also nodes are not involved in sink selection. But, in other protocols like LBDD, ring routing, railroad and rendezvous routing protocol, all the nodes inside the virtual infrastructure are involved in transmitting the information from source to sink and vice versa. But, in this proposed strategy, only cluster heads establish the efficient route to send the data to the sink.

Pant et al. [16], in that paper, proposed a routing algorithm which is based on multihop routing technique and uses an EEBCDA method. In this work, sensor nodes along the network are divided into unequal grid as on EEBCDA and this division is done in such a way that grid which is away from the sink has a larger size and has more number of sensor nodes within this network. The formation of grids and the structure of this grid are well elaborated in this framework, also, the path for the hop is defined, and all these works improve the stability, coverage, and overall lifetime and efficiency of network.

Based on the above study, the following algorithms are compared with each other as given in Table 1.

2.2 Worked Based on Sleep/Wake-up Protocols

The study of sleep/wake-up protocol is very important as it deals with the energy optimization of network node. It is important to study because many times the node may be located at remote geography, so many times it is not possible to keep a watch on supply, and network may get interrupted due to power cutoff. So, to avoid such issues, sleep/wake-up protocol is an healthy approach to extend the life of power source by making node sleep while it is in ideal state and wake it up when data is to be transmitted. Here is some part of the study done based on this protocol.

Ye et al. [2], in that paper, suggested a self-adaptive sleep/wake-up scheduling algorithm. In prior works, the duty cycle technique was used, which fails to deliver the expected result in terms of both packet delivery wait and also energy optimization. But, the suggested system is fast enough and energy efficient too as it is not based on duty cycling. The proposed technique is corroboration for learning-based technique, in which each node decides its individual role means weather it will sleep, listen, or transmit data for particular time slot and in distributed manner during each time slot in a decentralized way. Hence, this paper discourses a good knowledge regarding sleep/wake-up algorithm, and the results lead to energy efficiency of system as well.

Panahi et al. [17], in that paper, worked on the power consumption of base stations (BSs) by the use of sleep/wake-up algorithm. For base stations (BSs) of a heterogeneous network (HetNet), energy-proficient sleep/wake-up protocol is suggested using a fuzzy Q-learning (FQL). This system works by monitoring the BSs, means the less used BSs will get switched off in accordance with the local traffic profile, required area coverage, and cell EE, and all this leads to energy efficiency of system as less number of nodes are active. Their result shows much improvement in energy consumption.

Kovásznai et al. [18], in that paper, proposed a satisfiability modulo theories (SMT) validation for WSNs, which is used in and is based on sleep/wake-up scheduling algorithm for solving various network issues. This method can only be used with optimization modulo theories (OMT) which is another WSN sleep/wake-up scheduling. They addressed the energy optimization issues by using graph standards and examined their associations with the degree of challenge for OMT solvers.

Panahi et al. [19], in their paper, proposed a methodology for energy conservation in WSN. They used device-to-device (D2D)-based communication in order to enlarge the network coverage area so that the area of which the BS is not in working condition also gets network service. An energy optimization is also done with the help of this methodology.

Table 1 Comparison of routing protocols

S. No.	Name	Author	Algorithms/techniques used	Result
1	For wireless sensor networks, QoS-aware, and heterogeneously clustered routing Protocol	Muh. Amjad	Energy-efficient routing protocol	Simulation results gives improvement in many aspects like network life, constancy, efficiency, and minimal end-to-end stay
2	A distributed delay-efficient data aggregation scheduling for duty-cycled WSNs	B. Kang	Aggregation tree construction algorithm, fast distributed aggregation scheduling algorithm	The proposed system solves MLAs problem and gives better result as compared with other algorithms
3	Clustering hierarchy protocol in wireless sensor networks using an improved PSO algorithm	Y. Zhou	Energy-efficient and life-extending routing algorithm	The simulation result of this protocol gives better energy efficient results
4	A multilayer Layer Clustering-based multihoping routing protocol	K. Wang	Establishment of cluster protocol	Simulation shows TLCBMH improves the WSNs lifetime
5	HHCS: hybrid hierarchical cluster-based secure routing protocol for wireless sensor networks	C. Deepa	Hybrid hierarchical cluster-based secure routing (HHCS) protocol and LEACH protocol	HHCS algorithm gives more energy efficient and secured results than LEACH algorithm
6	Enhanced energy-optimized cluster-based on-demand routing protocol for wireless sensor networks	Sreevidya B	CBRP	Results show overall improvement in terms of energy efficiency, better throughput, and reduction in end-to-end delay
7	An improved hierarchical cluster-based routing approach for wireless mesh network	T. Acharjee	Hierarchical routing protocol	For small number of nodes, this protocol gives lower delay as compared with BATMAN protocol
8	Cluster-based rendezvous routing protocol for WSN	R. K. Lenka	Rendezvous routing protocol	With 1 hopping communication, this method consumes less energy and also reduces delay

Lin et al. [20], in this paper, elaborated the use of body area networks (BANs) which enable the data exchange and monitoring between wearable/implanted devices. Due to lack of channel fluctuation consideration in many previous techniques, the improper information is inefficient in a BAN. Along with this, channel-aware polling-based MAC protocol CPMAC is also used which heals the network failure or loses of packets issues. These techniques trigger sensors to spread or receive data whenever the channel is sufficiently strong to promise fast, steady, and more unfailing transmission. This is really very important problem-solving techniques having very efficient results.

Latif et al. [3], in their paper, proposed a communication protocol for small area network like home. This method targets to solve issues like energy wastage during the idle heeding, crashing situation, and overhearing processes. The suggested algorithm performs various tasks like reducing the energy of each node, eases communication for stable traffic, and provides adaptive regulated load for fluctuating traffic load. The results based on this MAC protocol give better results as compared with other older techniques.

Alhalaf et al. [21], in that paper, presented an energy cross-layer design for WSN which they named "green task-based sensing" (gTBS) scheme. In the suggested gTBS techniques, they blend the sleep and wake-up techniques with power adjustment which active or evoke the active nodes. The use of gradient-oriented unicast technique helps to get over the synchronization issue of data transmission, diminishes network traffic issues, and reduces the whole general energy utilization of the network. The result output shows the improvement in network energy.

Vaiyshnavi et al. [22], in their proposed paper, specified a scheduling method called (LECSA) load and energy consumption-based scheduling algorithm. In this algorithm, the cluster heads have the power to decide the path for data transmission, means based on the certain calculations, the CH will derive the nearest active node which transfers the data. The dynamic selection of nearest node is calculated by using an energy balanced tree construction, and this schedule is dependent on load and residual energy at that particular moment. The improvement by use of this algorithm is seen in the result obtained.

Kuo et al. [23], in their paper, elaborated the working of WSN using asynchronous sleep-wake scheduling algorithm. This method is an effective tool to optimize the overall energy consumption as this method defines the sleep schedule for sensor nodes. The proposed system is designed with combinations of two algorithms which are asynchronous sleep-wake schedules and opportunistic routing called ASSORT. The simulation results with the use of ASSORT lead to lifetime extension.

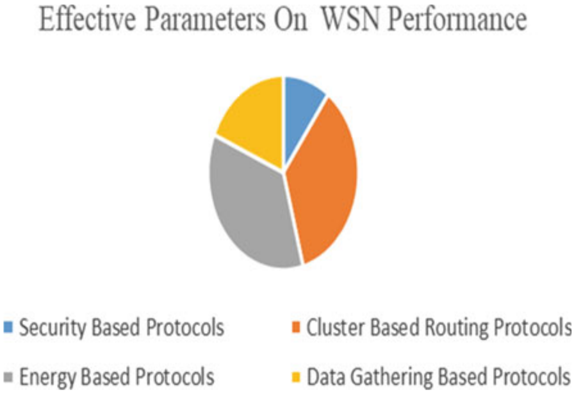
Zheng et al. [24], in their paper, proposed an organized method for designing asynchronous wake up of sensor nodes for an ad hoc network. This work revolves around power management with consideration of two factors: on slot-bases and on-demand bases, combining these factors gives better overall power enhancement. This algorithm addresses various wake-up problems and forms an efficient network.

Kumar et al. [25], in their paper, tried to solve the problem of lesser life span of sensors in a WSN by defining a more optimal algorithm. This algorithm not only results in lifetime improvement of sensor but also deals with maintaining barrier coverage and also provides options for fault-tolerant connectivity.

Zhang et al. [26], in this paper, introduced a general intermittent energy-aware (IEA) and (EH-WSN) energy-harvesting wireless sensor network platform. The system works as it adopts a double-stage capacitor structure to make sure node's synchronization without energy harvesting, and an integrator is used in order to achieve ultra-low power measurement. Number of experiments is performed to verify performance of IEA in terms of life and reliability of network. The results of IEA platform utilized show ultra-low power consumption and high accuracy (Table 2).

3 Conclusion

This paper offers protocols which make relative study and give appropriate solutions for various WSN issues. But, among various network problems, the main concentration of the study is to find appropriate cluster routing protocols and the sleep/wake-up protocol for more optimized network. The main motto of this study is to make them more reliable and energy-efficient network, and after this study, the utilization of more trusted protocol is done in the future implementation. The comparison of these two protocols with the other parameters used in optimization of WSNs is shown in graphical manner as follows:



From the above study, we come to know that we can design an optimized and more reliable WSN by working on these two parameters (cluster routing and sleep/wake-up). Other parameters like network lifetime, security, and data gathering also play important part in making healthy WSN, but these two play a very durable and more efficient role in terms of network lifetime betterment and energy management, as we can see with the improvement in these two protocols, the overall improvement in WSN is seen.

Table 2 Comparison of the various algorithms is done here

S. No.	Name	Author	Algorithm/techniques used	Results
1	A self-adaptive sleep/wake-up approach for wireless sensor networks	D. Ye	1. Sleep/wake-up protocol 2. During each time, the slot packet transmission depends upon the node	The proposed system doesn't work on the duty cycling algorithm, instead it uses an d sleep/wake-up algorithm for more optimized network
2	Green heterogeneous networks via an intelligent sleep/wake-up mechanism and D2D Communications	F. H. Panahi	Fuzzy Q-learning (FQL) and device-to-device (D2D) communications	The results are more optimized for small area network
3	Investigations of graph properties in terms of wireless sensor network optimization	G. Kovásznai	Optimization modulo theories (OMT) and satisfiability modulo theories (SMT)	With the use of this OMT solver, more graphical optimizes criteria of WSN are gathered
4	Green heterogeneous networks via an intelligent power control strategy and D2D communications	F. H. Panahi	Fuzzy Q-learning (FQL)	Result of their proposed method leads them to achieve an operative energy-optimizing sleep/wake-up system
5	Channel-aware polling-based MAC protocol for body area networks: design and analysis	C. H. Lin	Channel-aware polling-based MAC protocol CPMAC	The result shows that improvement in polling periods improves energy efficiency adaptively
6	Improved scheduling algorithm using dynamic tree Construction for wireless sensor networks	M. P. Vaiyshnavi	(LECSA) load and energy-consumption-based scheduling algorithm	The results obtained are more efficient as compared with other sleep/wake-up protocols

References

1. Deepa C et al (2014) HHCS: hybrid hierarchical cluster based secure routing protocol for wireless sensor networks, In: ICICES
2. Ye D et al (2017) A self-adaptive sleep/wake-up scheduling approach for wireless sensor networks. IEEE Trans Cybern
3. Latif S et al (2013) A greener MAC layer protocol for smart home wireless sensor networks. In: IEEE online conference on green communications, pp 169–174
4. Amjad M et al (2017) QoS-aware and heterogeneously clustered routing protocol for wireless sensor networks. IEEE Access 5:10250–10262
5. Kang B et al (2017) A Distributed delay-efficient data aggregation scheduling for duty-cycled WSNs. IEEE Sens J 17:3422–3437
6. Zhou Y et al (2017) Clustering hierarchy protocol in wireless sensor networks using an improved PSO algorithm. IEEE Access 5:2241–2253
7. Wang K et al (2014) A Two-layered clustering-based MultiHop routing protocol. In: Fifth international conference on intelligent systems, modelling and simulation, pp 573–578
8. Sreevidya B et al (2017) Enhanced energy optimized cluster based on demand routing protocol for wireless sensor networks. IEEE, pp 2016–2019
9. Gnanambigai J et al (2014) A clustering based hybrid routing protocol for enhancing network lifetime of wireless sensor network. In: 2nd international conference on devices, circuits and systems (ICDCS), pp 1–4
10. Behera TM et al (2017) Work-in-progress: DEEC-VD: a hybrid energy utilization cluster-based routing protocol for WSN for application in IoT. In: International conference on information technology, pp 97–100
11. Xiao X et al (2017) 6LoWPAN hierarchical cluster routing protocol. In: International conference on cyber-enabled distributed computing and knowledge discovery, pp 80–83
12. Shaha SAN et al (2017) Cluster based routing protocol using rendezvous agent. In: International conference on energy, communication, data Analytics and soft computing (ICECDS), pp 1537–1542
13. Acharjee T et al (2016) An improved hierarchical cluster based routing approach for wireless mesh network. In: International conference on computer communication and informatics (ICCCI)
14. Misra S et al (2016) A literature survey on various clustering approaches in wireless sensor network. In: IEEE 2nd international conference on communication, control and intelligent systems (CCIS), pp 18–22
15. Lenka RK et al (2017) Cluster-based rendezvous routing protocol for wireless sensor network. In: International conference on computing, communication and automation (ICCCA), pp 748–752
16. Pant P et al (2015) A Multihop routing protocol for wireless sensor network based on grid clustering. IEEE, pp 137–140
17. Panahi FH et al (2018) Green heterogeneous networks via an intelligent sleep/wake-up mechanism and D2D communications. IEEE Trans Green Commun Netw
18. Kovásznai G et al (2018) Investigations of graph properties in terms of wireless sensor network optimization. Institute of Mathematics and Informatics Eszterházy Károly University, Eger, Hungary
19. Panahi FH et al (2017) Green heterogeneous networks via an intelligent power control strategy and D2D communications. IEEE
20. Lin C-H et al (2016) Channel-aware polling-based MAC protocol for body area networks: design and analysis. IEEE Sens J
21. Alhalaf A et al (2016) "gTBS: a green task-based sensing for energy efficient wireless sensor networks. In: IEEE conference on computer communications workshops
22. Vaiyshnavi MP et al (2015) Improved scheduling algorithm using dynamic tree construction for wireless sensor networks. In: IEEE ICCSP conference, pp 0846–0849

23. Kuo M-S et al (2012) Joint design of asynchronous sleep-wake scheduling and opportunistic routing in wireless sensor networks. IEEE
24. Zheng R et al (2003) Asynchronous wakeup for ad hoc networks
25. Kumar S et al (2007) Optimal sleep-wake up algorithms for barriers of wireless sensors. The Ohio State University
26. Zhang Y et al (2018) An efficient EH-WSN energy management mechanism, vol 23, no 4, pp 407–418

Journey of Wireless Communication

Vignesh Parameswaran and M. Shanmugasundaram

Abstract Development of mobile communication is rapid, with different methods and techniques being introduced in wireless communications. The next few pages will deal with the detailed study of wireless cellular technologies—first, second, third, and fourth generations eventually leading to the fifth generation as well. This will visualize the evolution from analog system transmissions to digital transmissions which brought the usage of audio, graphics, video, etc. The evolution also gave rise to Internet on the cellular mobile phones which were once realizable only in computers through broadband connections. With improved technologies, we saw the development of fourth-generation cell phones which harnessed the use of LTE. The world is moving very fast, and the corporates involved in mobile communications are in a strong tussle to achieve the fifth generation of mobile networks which will shift the world's entire way of functioning from autonomous vehicles to IoT and many other things which could be seen only as part of sci-fi movies.

1 Introduction

The exchange of data which can be in any form between points that are not connected physically is wireless communication. It helps us avoid the recurring cost incurred in setting up physical means of communication such as cables. It is the fastest developing field in the world today. This development has been triggered by the need of employing the major use case of wireless communication—voice transmission, to be accompanied by video, packet, and data transmission on the air. There was a time when there used to be research conducted to increase the capacity of wired lines. This has reached a point wherein the world is researching on increasing the capacity

V. Parameswaran (✉)
M. Tech. Embedded Systems, VIT, Vellore, India
e-mail: viguinuniverse@gmail.com

M. Shanmugasundaram
School of Electronics Engineering, VIT, Vellore, India
e-mail: phdsundaram@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_28

of the wireless modes [1] of communication to accommodate the fifth generation of wireless communication so-called 5G. As there are limitations in increasing the bandwidth and maintaining power requirements, research is widely carried out on the types of signal transmission and the signal processing methods used in receiver. Due to rapid increase in the number of mobile subscribers, many issues such as congestion, low speed, and low bandwidth are faced. But above all this there are many advantages of wireless communication as well which include saving cost of installation of cables, saving time of installing the same, and at the time, instance creating mobility of devices connected to a network. But wireless communication is not only restricted to the cellular communication part. It also includes radio satellites which are used to communicate across the world as well as the networks which work inter-continentally. Even though we have come this far in the evolvement, there is still scope for perfection. The journey of coming to the fifth generation of networks is very long, and many researchers and companies have had to give in to the needs of the present world. Those who could not adapt were left back. For instance, Nippon Telegraph and Telephone (NTT) were the first to start a commercial cellular network which was automated in 1979 creating huge popularity which went to become the first nationwide 1G network in Japan. NTT is still at the forefront in the world in revenue terms. Nordic Mobile Telephone (NMT) was an early 1G network mostly used in Nordic countries. As the NMT specifications were free and open, many companies tried their recipes and companies like Nokia, Ericsson, and Motorola [2] came to the fore in manufacturing communication equipment. Some of these companies, however, could not survive the retail market beyond the 2G networks because they could not adapt to the changing needs of the people in cellular phones. And then came many other mobile operating systems which were all outclassed by Android and IOS. Chip manufacturing companies like Qualcomm, MediaTek, Broadcom, etc. have had their share of successes till date. As 2G evolved into 3G, people started expecting more and eventually came 4G which changed the outline of the cellular market. The corporates involved in the development of 4G dished out all companies surviving on 2G and 3G, and it has come to a stage where service providers like AT&T, Verizon, Jio, etc. have either completely shut down the GSM network-related infrastructure or are in the process of phasing it out soon. As companies started cashing on the success of 4G, a survey claims that more than 54% of the companies involved in technology and as service providers have started developing technologies for 5G with 16% already partially deployed.

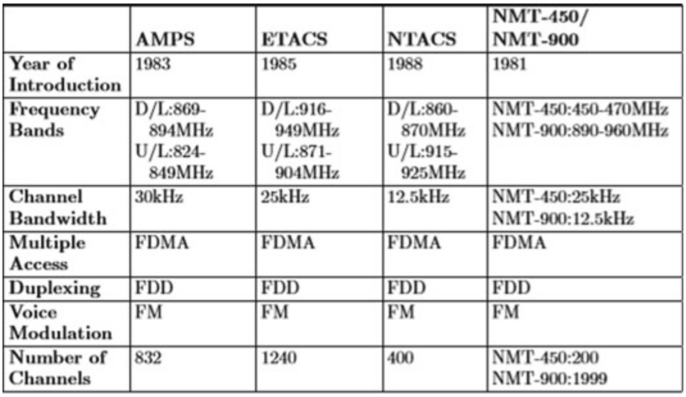
2 Evolution of Mobile Cellular Networks

Wired communication using landlines and setting up public switched telephone network (PSTN) is considered the most reliable source of communication wherein we see very good speech quality and high-speed broadband services. Cable television providers still use wired systems from their control room because of the quality and reliability in spite of being costly. The evolution of the mobile cellular networks has been phenomenal, and lots of scene changing episode have made this field evergreen. It was presumed that satellite phones first used for communication between boats will become a sensation, but this vision was proved wrong by the upcoming discoveries in the wireless ocean.

2.1 First Generation

This generation of wireless mobile communications supported communication which was only analogue in nature. They were used predominantly for voice. They improved on earlier systems by providing automatic switching, handover of calls to different cells thus using the cellular concept. Japan's NTT paved way to different adaptations by different operators in various countries. NMT was the first system to support automated handover and international roaming. This was used in most parts of Europe. AMPS from USA and total access communication system (TACS) from Europe (ETACS) and Japan (NTACS) were more successful. These systems had only a major difference in channel bandwidth with AMPS deploying a 30 kHz channel whereas NTACS deployed 12.5 kHz and ETACS used 25 kHz [3]. A quick summary can be seen in Fig. 1.

AMPS used frequency division multiple access (FDMA). Subscribers were assigned a pair of voice channels (forward and reverse) for the duration of their call. AMPS had a coverage of 2100 square miles. It had only ten base stations. Each of them had height of antenna tower around 150–550 ft. They mostly deployed a frequency reuse pattern of 7 cells with 3 sectors for each cell. The Federal Communications Commission (FCC) allocated the spectrum to two operators per market in USA. Each operator supported a total of 416 AMPS channels and assigned 20 MHz of spectrum, in each market. Of the 416 channels, control information was sent in 21 channels and the remaining 395 channels for voice traffic. Control information was



	AMPS	ETACS	NTACS	NMT-450/ NMT-900
Year of Introduction	1983	1985	1988	1981
Frequency Bands	D/L:869-894MHz U/L:824-849MHz	D/L:916-949MHz U/L:871-904MHz	D/L:860-870MHz U/L:915-925MHz	NMT-450:450-470MHz NMT-900:890-960MHz
Channel Bandwidth	30kHz	25kHz	12.5kHz	NMT-450:25kHz NMT-900:12.5kHz
Multiple Access	FDMA	FDMA	FDMA	FDMA
Duplexing	FDD	FDD	FDD	FDD
Voice Modulation	FM	FM	FM	FM
Number of Channels	832	1240	400	NMT-450:200 NMT-900:1999

Fig. 1 Major first generation cellular systems

sent using frequency-shift keying (FSK) and frequency modulation (FM) at higher frequencies typically 150 MHz and above was used for the transmission of analog voice. Such typical systems had a lifetime of a decade from 1980 to 1990. The rate at which data was sent was around 2.4 Kbps. When such 1G phones started getting popular, the number of people who started using it rose to 20 million by 1990 which meant an astonishing growth rate of around 40%. It has bad voice links, less capacity, more noise interference, not so reliable handoff, and susceptibility to eaves dropping by hackers. Also the phones were big in size and had a poor battery life. Even after 2G came into picture, such systems were used as a fallback network by service providers and also for providing roaming between different operators with incompatible 2G systems.

2.2 Second Generation

This generation evolved mainly due to hardware platforms depicting increased processing abilities. It also aimed toward efficient voice communication only but adapted digital modulation in contrast to 1G systems. This shift also increased the system capacity through use of digital speech codes which were efficient spectrally, thus deploying time or code division multiple access to multiplex many users on the same frequency channel. It could also realize frequency reuse due to better digital modulation, coding, and equalization techniques. Better speech codecs and signal-level processing also improved voice quality. Security was also worked upon in 2G to prevent eavesdropping through simple encryption techniques which differed for every channel access and known only to mobile station and the infrastructure.

Global System for Mobile Communications (GSM), IS-136 TDMA, and IS-95 CDMA systems were the prominent cellular systems in this generation among many others. IS-95 was used mostly in some parts of Asia and North America. IS-136, touted as a digital improvement over AMPS using 30 kHz channels, was a TDMA-based system. However, GSM was the most used technique and widely adapted which went on to become a standard. GSM is also based on TDMA, and one 200 kHz channel is time shared between 8 users in different time slots [4]. It used Gaussian minimum-shift keying (GMSK) for modulation because of its ability to provide constant envelope and providing efficient use of the spectrum along with good power characteristics [5]. GSM did not stop here and went on to provide numerous services. Short messaging service (SMS) was one of them, and this does not describe at all. Besides voice and SMS, circuit-switched properties started to get imbibed. Around middle of the 1990s, European Telecommunications Standards Institute (ETSI) that had taken charge of the GSM standard introduced GSM Packet Radio Systems (GPRS) as a stepping stone toward increasing the data rates. The architecture for GSM and GPRS was almost the same in the signaling links and also usage of the same bands as well as slots in time. GPRS could garner average data rate of 30 kbps. GSM also got a further push during the early part of 1997 in the data domain with the innovation of Enhanced Data Rate for GSM Evolution (EDGE). EDGE could increase the data rate to around 59 kbps per slot by addition of the 8 PSK scheme of modulation. This was almost 3 times as that of GPRS. Practically EDGE could provide average user rates around 100 Kbps.

CDMA was claimed by Qualcomm in 1989 as a more efficient and higher quality technology. The unique property which it provided was the usage of same frequency at same time by many users. It used a 12.5 MHz bandwidth to transmit a voice signal at around 9.2 Kbps. Other advantages include every cell using same frequency channel in turn simplifying the planning for frequency and increasing the capacity. It was also instrumental in the innovation of a mobile station able to connect to a new base station before the disconnection from the previous one which was referred to as soft handoff [6]. It also was able to provide one dedicated channel for data at 9.6 kbps which went on to become around 14.4 kbps later on. CDMA was instrumental in the fast transition to 3G through newer versions like CDMA2000-1X and EV-DO thus challenging GSM which was undertaking a subtle evolution through GPRS and EDGE to 3G.

2.3 *Third Generation*

The second generation improved voice capacity and quality and began data support for Internet. But the circuit-switched way was inefficient for data providing low data rate. Hence, the need for third-generation systems to provide increased data rate and advanced services and applications was felt thus triggering the International Telecommunications Union (ITU) to invite proposals for such systems. It laid out criteria such as 2 Mbps in fixed, 384 Kbps in pedestrian, and 144 Kbps in wide area vehicular environments. There were parallel evolutions going on in the GSM and CDMA track which were carried out by consortium bodies for standards called Third-Generation Partnership Project (3GPP) and 3GPP2 (spearheaded by Qualcomm), respectively [7].

CDMA2000-1X was 3GPP2's first bet (here 1X implied that it uses same bandwidth as IS-95). As it provided specifications less than the standards set, it was referred to as 2.5G. CDMA-1X increased capacity by doubling the number of forward channels as compared to previous 64. In contrast, 3GPP was created as a consortium of 6 regional standards in telecommunication. The 3G system based on the evolution of GSM was Universal Mobile Telephone Service (UMTS), indigenously developed by ETSI. The characteristics of UMTS were a core network (CN) which provided routing, user management in addition to switching. It also comprised of UMTS Terrestrial Radio Access Network (UTRAN) and the User Equipment (UE). UMTS was consistent with the architecture used for GSM/GPRS. It is described in Fig. 2. The air interface used was Wide-band CDMA (W-CDMA) inspired by IS-95. The system supported 100 voice calls at the same time and maximum data rates from 384 to 2048 kbps due to bandwidth of 5 MHz.

Further additions to 3G family included EV-DO which was the first system to deliver speeds comparable to broadband developed by Qualcomm (the 3GPP2 group)

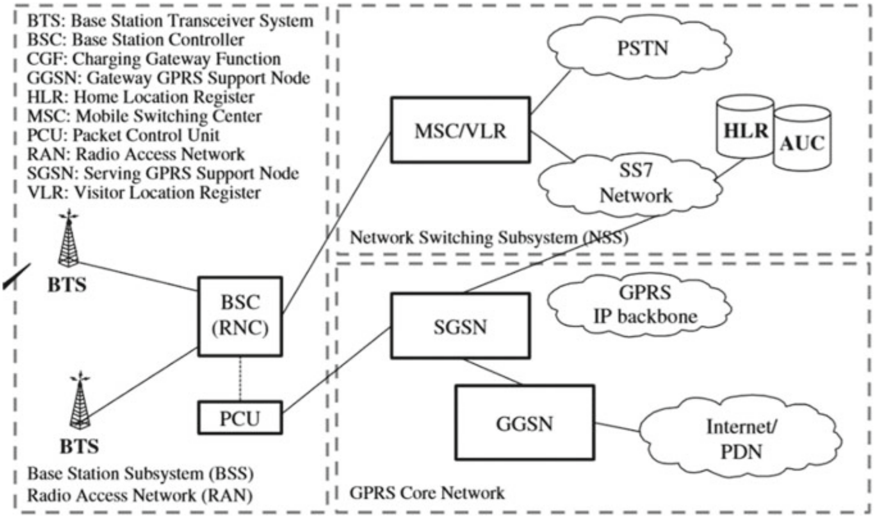

BTS: Base Station Transceiver System
BSC: Base Station Controller
CGF: Charging Gateway Function
GGSN: Gateway GPRS Support Node
HLR: Home Location Register
MSC: Mobile Switching Center
PCU: Packet Control Unit
RAN: Radio Access Network
SGSN: Serving GPRS Support Node
VLR: Visitor Location Register
PSTN
MSC/VLR
HLR
AUC
SS7 Network
Network Switching Subsystem (NSS)
BTS
BSC (RNC)
GPRS IP backbone
SGSN
PCU
GGSN
Internet/ PDN
BTS
Base Station Subsystem (BSS)
Radio Access Network (RAN)
GPRS Core Network

Fig. 2 GSM network architecture

in 2002, 3 years ahead of HSDPA deployed by GSM. It provided up to 2.4 Mbps downstream and up to 153 kbps upstream. The modulation and coding could be dynamically adapted according to conditions by EV-DO. High-Speed Data Access (HSPA), a combination of HSDPA and HSUPA (downlink and uplink), was additional enhancement to the 3GPP standard. It introduced new advanced techniques such as adapting modulation and coding according to channel conditions, fast dynamic scheduling of packets, and hybrid automatic repeat request (H-ARQ), an improved retransmission technique, to soft-combine multiple erroneous retransmissions to recover from errors more quickly. Various other additions occurred to the family which are considered as part of 4G or 3G by different explanations which will be seen further as part of 4G here.

2.4 Fourth Generation

This generation has lots of arguments of technologies not meeting the standards set by ITU for 4G. HSPA+, WiMAX, and LTE are some of the most prominent ones. HSPA+ uses higher order modulation such as 64QAM and 16QAM, in addition to multiple-input multiple-output (MIMO) wherein two transmit and receive antennas each are used to enhance diversity, beamforming, and spatial multiplexing. It uses dual-carrier downlink operation for doubling data rates and could enhance capacity in addition to data rates. It also gave attention to the draining batteries of the devices using discontinuous transmission and reception. WiMAX has many features adapted by LTE, the most prominent one being orthogonal frequency division multiplexing

(OFDM) [8]. OFDM can operate even when not in line of sight and can resist multipath. Its peak data rate is 74 Mbps. Support for advanced antenna techniques and dynamic allocation of resource to a user are other characteristics of OFDM.

LTE, referred to as Long-Term Evolution, has many features inherited from HSPA+ and WiMAX. When 3G was at its peak, the world was moving rapidly to high bandwidth applications such as music downloads, video streaming, and IPTV. It was the time when smart devices started proliferating. We started using laptops, netbook computers, large screen devices, devices for gaming, camcorders and projectors with built-in wireless interfaces, portable media players, cameras, and other machine-to-machine communication devices. Also service providers and device manufacturers started cashing in on this and the need was felt for bringing the performance on wireless devices on par with broadband in addition to lowering the cost per megabyte of data for the users to make the market competitive. But this had to be done using the already existing spectrum taken up by 2G and 3G. OFDM had many advantages. It had reduced computational complexity due to use of known FFT/IFFT techniques, frequency diversity, was robust against narrowband interference, and had graceful degradation of performance under excess delay. Advanced multi-antenna solutions [9] such as beamforming, spatial multiplexing, and transmit diversity in addition to MIMO that made the spectrum efficient, increased capacity, and made a robust link were provided by the LTE standard. The core design to support LTE is called Evolved Packet Core (EPC) which can be seen in Fig. 3. LTE has a capability of data rate up to 150 Mbps. LTE-Advanced has been targeted to obtain 1 Gbps downlink and 500 Mbps uplink [10]. With such capability, the existing 2G and 3G systems are being planned to be phased out to free the spectrum which is captured by them. But it is not an easy task because LTE alone cannot guarantee service in every nook

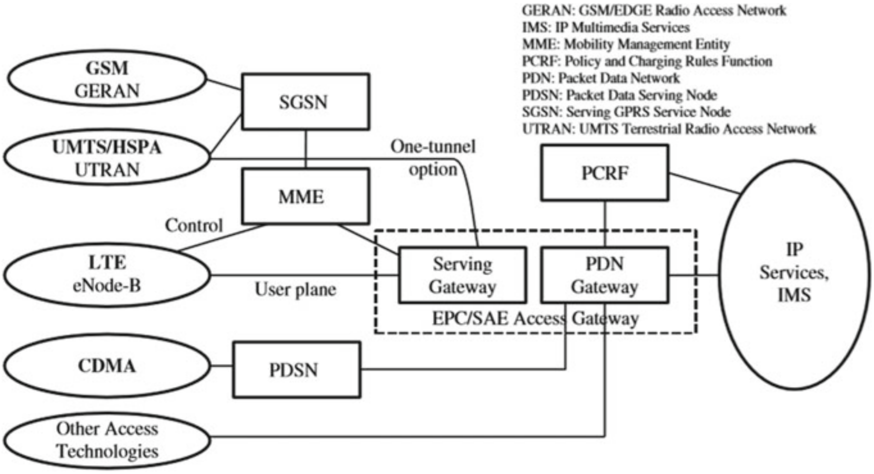

GERAN: GSM/EDGE Radio Access Network
IMS: IP Multimedia Services
MME: Mobility Management Entity
PCRF: Policy and Charging Rules Function
PDN: Packet Data Network
PDSN: Packet Data Serving Node
SGSN: Serving GPRS Service Node
UTRAN: UMTS Terrestrial Radio Access Network
GSM GERAN
UMTS/HSPA UTRAN
SGSN
One-tunnel option
MME
Control
LTE eNode-B
User plane
Serving Gateway
PDN Gateway
EPC/SAE Access Gateway
PCRF
IP Services, IMS
CDMA
PDSN
Other Access Technologies

Fig. 3 Evolved packet core architecture

and corner of the world. 2G is the best fall back network option available in this fast-evolving industry of wireless networks.

2.5 Fifth Generation

The world has started becoming greedy. From the smart handheld devices to more advanced use cases such as online gaming, virtual reality, artificial intelligence, 3D 4K–8K cloud and video streaming, autonomous cars, big data [11], and the most important one which will drive all the previous, Internet of Things (IoT), the vision forward has been just like some sci-fi movie. The extent of people realizing technology to aid in surgery and medical tracking proves the fact that we humans have progressed to unimaginable levels. To envisage this vision, IUT has aimed for a standard peak data rate of 20 Gbps and latency of 1 ms for 5G systems. Basically, IUT has defined 3 categories of service. They are enhanced Mobile Broadband (eMBB) or handsets, Ultra-Reliable Low-Latency Communications (URLLC) including industrial applications and autonomous vehicles, and Massive Machine Type Communications (MMTC) or sensors. As the throughput requirements have increased enormously, a large number of new spectrum called the 5G NR frequency bands have been allocated which work in the GHz range and some particularly in millimeter wave bands. In addition to this, multiple access schemes, modulation methods, Future PHY/MAC, flexible duplexing methods, and massive MIMO have all been under research for 5G [12]. Corporates like Qualcomm, Intel, and Huawei are actively involved in modem technology while Nokia, Cisco, ZTE, Samsung, and Ericsson are involved in infrastructure of 5G. Companies have left no stone unturned to safeguard their architecture or design for the 5G systems due to which details on the architecture are only an imagination.

3 Conclusion

Every generation of wireless mobile communication intended to raise the bars set for that particular decade. 2020 is seen as a revolutionary year in this field where we will be able to experience some technologies which were imagined only in movies. The journey so far has been fantabulous and will continue to be. No generation can be considered as a winner as all of them satisfied the needs of that decade very well in their own way and own limitations.

References

1. Raychaudhuri D, Mandayam NB (2012) Frontiers of wireless and mobile communications. Proc IEEE 100(4):824–840
2. Escher JS (1997) Wireless portable communications trends and challenges. In: 1997 IEEE radio frequency integrated circuits (RFIC) symposium. Digest of Technical Papers, Denver, CO, USA, pp 1–3
3. Hughes CJ, Appleby MS (1985) Definition of a cellular mobile radio system. IEE Proc F—Commun Radar Signal Process 132(5):416–424
4. Eberspächer J (2009) GSM—architecture, protocols and services. Wiley, Chichester
5. Heine G (1999) GSM networks: protocols, terminology, and implementation. Artech House, Boston, MA
6. Orlik PV, Rappaport SS (1999) On the hand-off arrival process in cellular communications. In: WCNC. 1999 IEEE wireless communications and networking conference (Cat. No. 99TH8466), New Orleans, LA, USA, vol 2, pp 545–549
7. Hoy J (2015) 3GPP network types. In: Forensic radio survey techniques for cell site analysis. Wiley. https://doi.org/10.1002/9781118925768.ch5
8. Chia S (2007) Mobile network evolution beyond 3G. In: 2007 IEEE radio and wireless symposium, Long Beach, CA, pp 269–272
9. Ghosh A, Zhang J, Andrews J, Muhamed R (2011) Fundamentals of LTE. Prentice Hall
10. Abeta S (2010) Toward LTE commercial launch and future plan for LTE enhancements (LTE-Advanced). In: 2010 IEEE international conference on communication systems, Singapore, pp 146–150
11. Huang J et al, A big data enabled channel model for 5G wireless communication systems. IEEE Trans Big Data
12. Vannithamby R, Talwar S (2017) Massive MIMO communications. In: Towards 5G: applications, requirements and candidate technologies. Wiley

A Survey on K-Means Clustering for Analyzing Variation in Data

Pratik Patil and A. Karthikeyan

Abstract Most of the times data for certain task seems to be varying due constant changes made to method of data collection as well as due to inclusion of new parameters related to the task. This may result in false conclusion derived from data generated and might lead to failure in task or degradation in the standard of activity related to that task which is being monitored from that data. Clustering is basically the grouping of similar kind of data wherein each cluster consist of data with some similarities. Whereas most of the data is unstructured or semi-structured, and that's where unsupervised K-means Clustering method plays role to convert the data into structured one's for clustering. This paper consist of K-means clustering method which is being used to keep an eye on such variations which are occurring in data generated for a task when certain changes are incorporated in technique to track this data.

Keywords K-means · Clustering · Machine learning · Dataset · Variation · Analysis · Data mining · Iterations · Parameters · Eucledian · Structure

1 Introduction

Data analysis and its mining are basically related to data science field of computer science which are the major part of nowadays technique to understand the pattern, structure and hidden specifications of large data that is being generated by user activities on daily basis. This Data analysis plays a major role in keeping track of this huge amount of data and improving the application whose data is being monitored.

Clustering is the machine learning method which involves grouping of data according to their characteristic, behaviors, and features. These data points are

P. Patil (✉)
M.Tech Embedded Systems, VIT, Vellore, Tamil Nadu, India
e-mail: priyanshuagri@gmail.com

A. Karthikeyan
School of Electronics Engg, VIT, Vellore, Tamil Nadu, India
e-mail: karthikeyan.anbu@vit.ac.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_29

grouped such that, each data point in a particular group differs from other group data point and shows some similarity with the other points in its own group. Clustering technique is an unsupervised ML method wherein input data points are clustered into groups without any reference data about its features. These clustered data can then be utilized to understand the behavior, pattern in these groups for better understanding of the problem. The clustering method of ML follows unsupervised learning procedure for training.

Unsupervised learning is the method of training an artificial intelligence algorithm with data that is neither labeled nor classified so as making the algorithm to work through it without any help or guide. There are two types of clustering technique hard clustering and soft clustering. In hard clustering, every data point in the group either belongs to its cluster completely or partially. Whereas in soft clustering, the likelihood of each data point to be in a particular group is assigned instead of putting it in separate group.

Based on the task of clustering, there are different methods which can be used to define the likelihood between the data points viz. connectivity model, centroid model, distribution model, and density model. Connectivity model takes into account the data space exhibited by the data points and the points which are closer, are clustered in one group. Centroid model considers the centroids defined by user and according to data points distance from centroids they are grouped in particular group. Distribution model works on basis of similarity of data point probable distribution (Normal, Gaussian), whereas density model search for areas of varied density of data points in data space.

2 K-Means Clustering

K-means clustering is an iterative technique which involves finding local maxima during each iteration so that data points are grouped properly. For processing the data points, first it works with formation of groups for randomly selected centroids. Then it performs the optimization through iterative method. Whereas the groups are formed through calculating closest distance to the centroid using Eucledian distance.

Let say there are two points,

$$L = (x1(L), x2(L), \ldots) \text{ and}$$
$$M = (x1(M), x2(\mathrm{M}), \ldots)$$

Then its Eucledian distance will be,

$$d(L, M) = \mathrm{sqrt}((x1(L) - x1(M))2 + (x2(L) - x2(M))2 + \cdots)$$

The centroids mentioned are basically the means of the points that are assigned to it in the cluster, which can be calculated by either random initialization method or through selection of centroid in range of dataset values.

The Algorithm is as follows:

- First we select the number of clusters *k* (using different methods).
- Then select random *k* points which are the centroids (not necessarily from your dataset).
- Assign each data point to the closest centroid according to distance from the centroids, this forms K clusters.
- Now compute and place the new centroid after recalculation.
- Reassign each data point to the new closest centroid. If any reassignment took place again repeat the step four, otherwise stop as final clusters are formed.

3 Procedure for Finding Clusters

If we use the random initialization method, then we face the issue of random initialization trap wherein the clusters formed after the iterations are unexpected and results in improper data analysis. So to solve this issue we are using the K means Elbow method or K-means ++ method (Figs. 1 and 2).

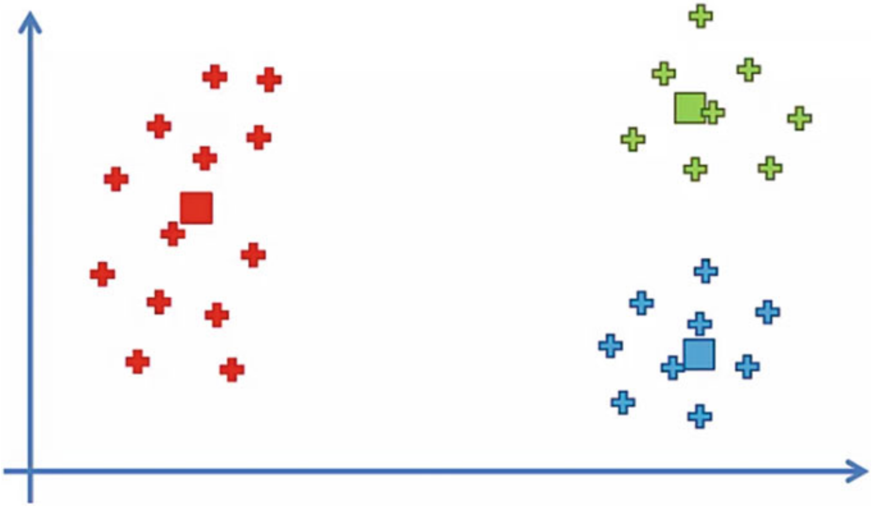


Fig. 1 Actual clusters expected

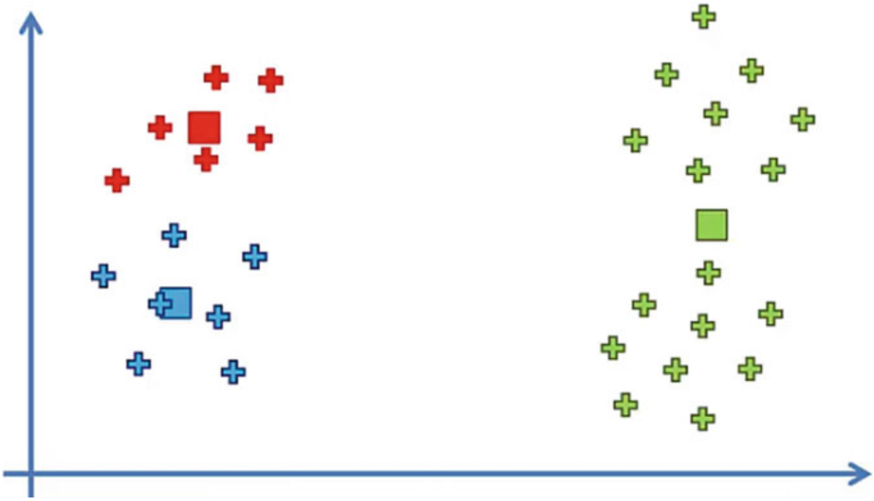


Fig. 2 Cluster obtained (Random initialization trap)

Steps for K-means Elbow method to find number of clusters,

- So first start with number of clusters to be as $k = 1, 2, 3\ldots$ (Fig. 3).
- Calculate for each k value the Within cluster sum of squares WCSS given by equation,

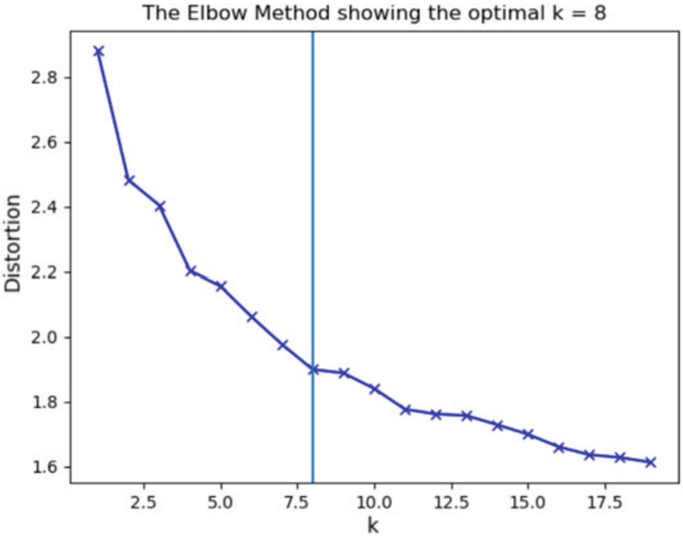


Fig. 3 Elbow method plot

$$\text{WCSS} = \sum \text{distance}(\text{Pi}, C1)^2 + \sum \text{distance}(\text{Pi}, C2)^2 + \sum \text{distance}(\text{Pi}, C3)^2 + \cdots$$

Pi are the distance of points in dataset

This is the distance of all points in cluster from centroid which are squared and summed.

- Now use these WCSS values for each value of *k* to make the WCSS plot as shown in fig.
- Lastly, find the optimized value of *k* where we have almost unvarying distortion i.e. WCSS (check the point where there is no steep descent).

4 Analysis of Data Variation Using K-Means

Many of research fields are utilizing K-means for keeping the track of data variation happening in the data generated by particular field, wherein the number *K* is decided for the expected variation understanding. The data points from previous version of task and its further changed version are compared to get complex clustering plot for the task.

This data can be used to keep a complete understanding of changes incurred over a period of time and then accordingly act to handle the errors or further improvements in the system. From Fig. 4, we can see that the plot formed show variation in terms of cluster with respect to some parameter related to the system under analysis. Wherein the data points are grouped into eight clusters each with varying density. Data points in each cluster indicates the variation, for example from cluster 6 it is clear that the data points present in it are collected from system with different versions whose properties are related whereas in some case the variation is unique to itself example cluster 2 and 5 wherein it has less data points from few version of changes system and may indicate a major change in system or some serious bugs in system. This gives researcher's a good understanding of the system behaviors and can utilize it to overcome the issue.

5 Advantages and Disadvantages

5.1 Advantages

Easy implementation and being unsupervised it doesn't require any reference output for training, i.e., based on input it finds patterns and forms cluster. For large number of variable, it require high computational power compared to other clustering algorithms. It can change clusters with each iteration thus generating new centroid for

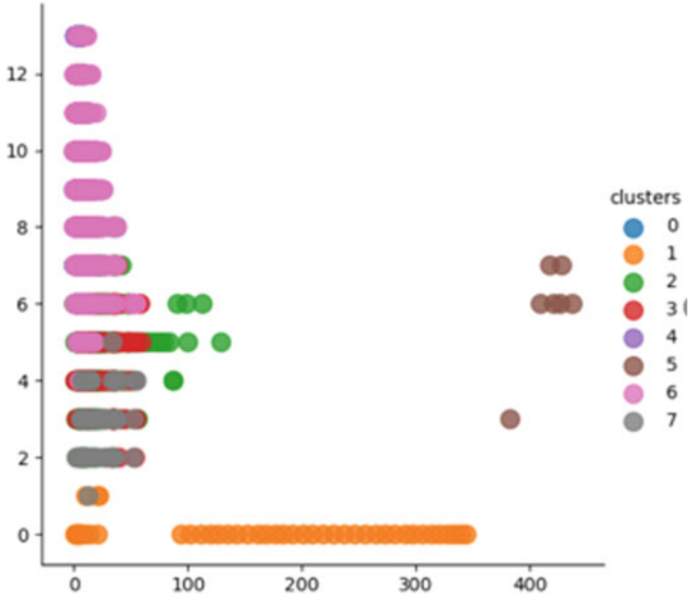


Fig. 4 Clustering data for variation in data points

perfect optimization. Clusters produced by K-means are almost accurate for each data points. This method reduces the noise and spatial course.

5.2 *Disadvantages*

There is no unique solution for this method, as for different k value we get different result being sensitive to local optima and initial values. Also for the K value as it is not known properly for accurate results. Generates same size clusters mostly even if input belongs to different size cluster. Rescaling the data can change the result in other way. The way in which data is feed to K-means model also decides the results.

6 Conclusion

Clustering methods are the best one when something related to analyzing large unstructured data comes up. But since it requires large amount of dataset for learning the pattern it has its drawbacks for small database systems. In this paper, we mostly talked regarding K-means clustering method which involves lots of iterations and try to get optimal results but this is not efficient solution. Hence K-means elbow method can be utilized which again requires some computation power. K-means clustering being unsupervised learning doesn't require any reference output data for analysis as is not easily available in most system. This clustering method can further be improved by using multiple iteration for optimized value or by utilizing K ++ method which uses elbow criteria to find optimized *k*. For variation analysis of data K-means seems to be perfect method as it is simple, easy to implement and moreover it catches the changes in system at very cheap cost compared to other algorithms. Also being simple in clustering mechanism it ignores the too small detail which is good for some system with some exceptions where only certain issue leads to problem.

Bibliography

1. Kodinariya TM (2013) Review on determining number of Cluster in k-means. 1(6)
2. Pattern recognition and machine learning book by Christopher Bishop
3. Gondaliya B (2014) Review paper on clustering techniques. 2(7). ISSN 2349-4476
4. Koundinya AK, Srinath NK, Anchalia PP (2013) Mapreduce design of K-means clustering algorithm
5. Santini M (2016) Machine learning for language technology ML4LT
6. http://www.datascience.com/
7. http://www.geeksforgeeks.org/k-means-clustering-introduction/
8. Theodoridis S Koutroumbas K (2003) Pattern Recognition. Elsevier Science
9. Kleinberg, J (2003) An impossibility theorem for clustering. In: Advances in neural information processing systems. pp 463–470
10. Han J, Kamber M (2001) Data mining: concepts and techniques. Morgan Kaufmann
11. Kaufman L, Rousseuw P (1990) Finding groups in data—an introduction to cluster analysis. In: Wiley series in probability and mathematical statistics
12. Machine Learning For Dummies Book by John Mueller and Luca Massaron
13. Ester M, Kriegel H-P, Sander J, Xiaowei X (1996) A density-based algorithm for discovering clusters in large spatial databases with noise. Kdd 96(34):226–231

A Review on Mobile Cloud Computing Interoperability Issues and Challenges

Tribid Debbarma and K. Chandrasekaran

Abstract Mobile cloud computing (MCC) is the convergence of two recent technologies namely "*Cloud Computing*" and "*Mobile Computing*" with wireless networks as a communication backbone. There are mainly three paradigms that use the concepts of MCC, viz. edge computing, fog computing and cloudlets. Due to the presence of various heterogeneous hardware and software platforms in MCC, there are many interoperability issues which create vendor/services lock-in problems, it also makes data and application portability difficult. This paper studies the different paradigms of MCC and the challenges in making them interoperable in heterogeneous hardware and software platforms. We have summarized some of the MCC-based research papers and their findings. Contribution of this paper is the summary of challenges and research scopes in the field of MCC where it needs to be addressed to mitigate the *interoperability* issues.

Keywords Mobile cloud computing · Interoperability · Portability · MCC

1 Introduction

Cloud computing (CC) and mobile computing (MC) are the two most happening technologies in the recent information and communication technology (ICT) and computing world. Cloud computing has changed the ICT infrastructure in a great way. The days of companies/organizations handling their own ICT infrastructure is replaced with cloud data centres and cloud storage services. On the one hand, mobile device technology is growing by leaps and bounds. Still, these technologies are not

T. Debbarma (✉)
Department of Computer Science and Engineering, National Institute of Technology Agartala, Agartala, India
e-mail: tribid@ieee.org

K. Chandrasekaran
Department of Computer Science and Engineering, National Institute of Technology Karnataka, Surathkal, Mangalore, India
e-mail: kchnitk@ieee.org

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_30

without its own limitations; e.g., CC does provide distributed services accessible from anywhere in the world, but it has limited or no mobility. On the other hand, mobile computing devices are having limited battery, storage, processing power and data storage capability due to its small form factor.

MCC merges two technologies and makes cloud computing services mobile. Further, mobile devices are augmented with large cloud storage and unlimited computing power of servers by accessing data centre infrastructure. The access to cloud server systems can help mobile devices to save the energy consumption by different techniques, e.g. by using computational offloading techniques [1, 2] and partitioning of mobile applications at the runtime to execute the application in the mobile device and cloud servers with dynamic/static context awareness.

Despite having many advantages, MCC has certain challenges, viz. interoperability and portability of the cloud services in the vastly heterogeneous mobile operating system (OS) and hardware platform, different wireless communication technology, offloading overheads, security, privacy, etc.

This paper summarizes different MCC and cloud computing-based research works findings and highlights the research scopes in MCC, present scenario, and challenges that need to be addressed. Specifically, the aspects of interoperability and portability of the MCC services with data portability to the end-users are highlighted for further work.

The rest of the paper is organized in different sections as follows: Sect. 2 discusses the background of MCC and motivation behind this work. Section 3 discusses CC- and MCC-related works. Section 4 discusses the challenges in MCC, Sect. 5 discusses the research scopes in MCC field including interoperability issues, and in Sect. 6, conclusions of this review and future work are discussed.

2 Background and Motivation

MCC is the convergence of mobile computing and cloud computing. Mobile cloud computing leverages cloud computing and mobile computing for a pay-as-you-use manner.

According to Sanaei et al. [3] "*Mobile Cloud Computing is a rich mobile computing technology that leverages unified elastic resources of varied clouds and network technologies toward unrestricted functionality, storage, and mobility to serve a multitude of mobile devices anywhere, anytime through the channel of Ethernet or Internet regardless of heterogeneous environments and platforms based on the pay-as-you-use principle*".

There are different paradigms that are based on MCC concepts. Below, we discussed some of the extended MCC concepts that are being studied and implemented at a different level in the industry and academia.

Edge Computing (EC): This architecture primarily transfers the processing, data analysis, communication and other tasks from the edge gateway or the source devices to the programmable automation controllers (PACs) instead of sending it to the cloud data centres. Only the large data and processing jobs are sent to the cloud systems. This approach reduces the latency of different operations where it does not need the service of large cloud systems [4].

Cloudlets: Computing systems connected at the edge of the Internet, which can act as local cloud computing data centre and access point to the mobile devices covering a small area and provides low latency computing services with a limited area of mobility [5].

Fog Computing (FC): This term was first introduced by Cisco Systems [6]. The concept of fog computing has been coined after edge computing. In FC, the cloud computing is extended to the edge of the Internet. The mobile devices and IoT devices transfer the data processing tasks into IoT gateway or fog nodes instead of directly connecting to the cloud data centres. The availability of local gateway and fog nodes can greatly reduce access latency of different services. The IoT gateways and fog nodes can access centralized cloud data centres as and when additional resources are required. OpenFog Consortium [7] formed by academic and industrial organizations are supporting, and developing guidelines for fog computing-based systems.

2.1 Motivation

Though there are different studies which have emphasized different issues related to cloud computing and MCC such as security, scalability, VM migration [1], portability and interoperability [8, 9] issues. Still, there is no common industry standard till date for MCC services interoperability and portability. The industry is yet to adapt standard interoperable application and service frameworks. Interoperability is nontrivial in the MCC as the hardware and application software's of mobile devices are vastly heterogeneous in nature. Moreover, different wireless network technologies on which the mobile devices are connected to the cloud systems make the interoperability issues more challenging and also makes it vulnerable to security and difficult to maintain QoS.

Presently, some of the cloud services that are extended to MCC services, e.g. Dropbox, Google Drive, etc., support storage services across different mobile OS and device categories which end-users can access without any device/OS lock-in. On the other hand, service like iCloud Drive mobile app-based service is not supported outside Apple products. Voice assistant service Siri (by Apple) is supported only in an Apple-developed operating system; this creates a lock-in situation where the users of other devices from non-Apple products cannot access such services. Here, the service and device lock-in create a situation where the end-user may have to compromise in his/her requirements. MCC with interoperable applications and services is the need of the hour.

3 Related Works

There are various studies on CC and MCC. Some of the studies' findings have been summarized in Table 1.

Haile and Altmann [8] studied the impacts of portability and interoperability on the value of cloud computing platforms and their users. Their findings give us an idea of how closed platform lock-in is counterproductive for the cloud service providers and can be dissatisfying to the end-users.

Table 1 Summary of different MCC studies

Studies/proposed systems	Proposed solutions
CloneCloud [1]	Migrates application into the computational cloud with dynamic profiling and static analysis to optimize energy and execution time. It is designed to offload the tasks of android-based systems to the cloudlets
MAUI [10]	Computation offloading with context awareness for decision-making
Marmalade [11]	Is a cross-platform toolkit that converts the application code to the target platform-supported format automatically
SAMI [3]	SOA-based system to facilitate application portability prevents energy losses by using nearest resources and provides interoperability by using MNO
Cloudlet [5]	It uses virtualization techniques to mitigate the heterogeneity problems of mobile devices. It is a small cloud data centre that provides low latency compute-intensive services to nearby mobile users
MOMCC [12]	MNOs are used to authorize and govern mobile users to enhance computing capabilities in the cloud platform
Mirage [13]	A cloud OS that runs on top of a hypervisor. Different portable cross-platform and applications can be produced in the normal OS, and they can be compiled to run in the mobile devices
Aneka [14]	Architecture and platform for distributed application development in the cloud computing. This allows to develop cloud applications for different cloud infrastructures
Akherfi et al. [9]	A middleware to adapt cloud Web services by transforming SOAP to REST and XML to JSON
Green Cloudlet Network (GCN) [15]	A private virtual machine executes the offloaded tasks of user equipment. The cloudlets are run by green and with grid power as a backup
Manjunatha et al. [16]	A cloud mobile hybrid application development systems using domain-specific language (DSL) for auto-generation of a communication link between mobile systems and target cloud platforms

Sanaei et al. [3] proposed a three-tier architecture based on service-oriented architecture (SOA) for MCC that provides interoperability by using mobile network operators (MNOs) and portability by utilizing SOA concepts. But the use of MNOs for arbitration process in a continuous manner adds processing overheads. CloneCloud [1] concept tries to resolve the energy consumption and execution time issues of mobile devices by offloading the process into the mobile device's clone, i.e. running in a cloud system.

Aneka [14] is a development environment for the CC that allows to develop cloud applications which can be deployed in various cloud infrastructures.

By providing portability and interoperability, cloud service providers can give better leverage to the users of different mobile platforms which are very much present in the MCC scenario.

The summary of some of the MCC studies, their proposed solutions are given in Table (1).

4 Challenges of MCC

The challenges of MCC are inherent to cloud computing and mobile computing. Many of the issues overlap with cloud computing and mobile computing. The augmentation of mobile computing systems into the cloud computing adds additional challenges in the existing CC issues. Table 2 provides summary of different MCC survey studies. The major issues and challenges in MCC are listed below.

Privacy and Security: Privacy is one of the most pertinent issues in MCC, where there is a thin line between personal/private data and data which is to be shared. So when a mobile device is connected to the CC service, its application which is keeping the private data and shareable data within the same application's accessibility is a major concern of accidental and unwanted breach of those private data.

Table 2 Summary of different MCC survey studies

Studies	Discussed open issues and challenges
Sanaei et al. [17]	Context awareness, live VM migration, trust, security, privacy, mobile communication congestion
Abolfazli et al. [18]	Lightweight techniques, portability, interoperability, seamless connectivity, live VM migration
Han Qi [19]	Data delivery, task division, better service
Dinh et al. [23]	Low bandwidth, network access management, quality of service, standard interface, service convergence
Chang et al. [20]	Privacy, SaaS design for mobile, green computing and energy saving, mobility, architecture and infrastructure for mobile cloud
Fernando et al. [21]	Mobility, mobile cloud security, incentives for surrogates
Roman et al. [22]	Security issues for the edge computing

Privacy issues of MCC [20] have been discussed as a requirement for MCC in their review study. Fernando et al. [21] discussed the mobile security issues as challenges in the MCC. Roman et al. [22] in their study highlighted the security challenges in the edge computing platforms.

The underlying security issues of cloud computing are also omnipresent in MCC. In addition to this, the use of wireless networks introduces the security vulnerabilities of wireless communications.

Portability: Portability issues are very much inherent in different mobile cloud services; e.g., songs purchased through iTunes service are not compatible or portable to other players. This service is application's platform-dependent. They do not support outside of other players out of the box. Portability of different mobile services among different OS vendors and hardware is still a prevalent issue which is not addressed fully.

Interoperability: The underlying technologies of MCC are heterogeneous in many ways. The major components of MCC are MC devices with different OS vendors and versions, wired and wireless networking technologies (3G, GSM, WAN, 4G, etc.) and different cloud service vendors with proprietary architectures. Interoperability is of major concern to the customers of MCC as the changes in MC technologies happen very rapidly and the end customers might fall in a vendor/service lock-in situations which are not desirable. There are some open standards and APIs and middleware's to support the issues. But there is still a gap in the adaptability of any common standard by different cloud service providers.

The interoperability and portability issues and challenges have been discussed in [21, 18].

Limitation in the interoperability among cloud services is a major issue which creates cloud vendor/services lock-in situations where the end-users/clients are compelled to accept compromises. The interoperability among different cloud infrastructure and services are to be resolved in many dimensions.

5 Research Scopes

The interoperability challenges need to be studied in more detail at the academia and industry. Primarily, interoperability issue is mainly concerned to developers and service providers for management of IaaS, PaaS, and SaaS layers of the cloud computing. But the growing interest of MCC services among end-users who are non-developers has increased the importance to extend the benefits of the interoperability and portability of services and data towards them also. In [24], it interpreted the interoperability and portability with five different scenarios. In this guide, scenarios 1–3 give guidelines on how to achieve the interoperability and address the issues related to it. The scenario becomes more complex when these cloud services are to be augmented with mobile devices. Vertical and horizontal heterogeneity [17] nature of MCC needs to be considered on different aspects to achieve an MCC system that supports the interoperability.

Survey studies [17] discussed the taxonomy and open challenges issues of heterogeneous MCC. In their study, they have pointed out some open issues which need to be addressed, e.g. context awareness, live VM migration, trust and security issues.

ReSTful models have been used in CC systems for achieving interoperability in the industry and in academic studies. The ReSTful model can be integrated with SOA into the MCC platform to achieve interoperability and data portability.

5.1 Summary

There are many studies and development of middleware and application programming interface (API) taking place to provide interoperability among the services for the management of PaaS as well as IaaS and SaaS layers, but fewer works have been carried out for interoperable MCC applications that serve end-users of MCC services. End-users need mobile applications that are interoperable across various mobile platforms, and the ability to port the data has to be incorporated in the new architectures. Further research works need to be carried out for the development of frameworks with ReSTful Web services and service-oriented architecture for seamless interoperability and portability among various MCC services.

6 Conclusions

Many research activities addressed different challenges pertaining to MCC. Still, there is a need to develop standards and frameworks to handle the interoperability and portability issues of MCC.

This paper discussed about the findings of different review studies and MCC related sources. Many studies have proposed application migration techniques using with static/dynamic profiling for optimized decision to reduce energy consumption and augment the processing power of cloud systems. Some studies discussed on the security and privacy issues as major challenges. But few studies have emphasized on the portability and interoperability issues of MCC applications and services at the end-user level. As there is still no standard industry-accepted architecture and many cloud services vendors run homegrown platform with little interoperability and portability to others, it has opened an opportunity for researchers to develop semantic architectures and standards with interoperability and portability among heterogeneous MCC technologies.

In our future work, we will develop an interoperable MCC services architecture based on a combination of RESTful and SOA architecture that will support an interoperable MCC application, irrespective of software and hardware platform.

References

1. Chun B, Ihm S, Maniatis P, Naik M, Patti A (2011) CloneCloud: elastic execution between mobile device and cloud. In: Proceedings ACM the European professional society on computer systems (EuroSys'11). Salzburg pp 301–314
2. Kristensen MD (2010) Scavenger: transparent development of efficient cyber foraging applications. In: Proceedings IEEE eighth annual international conference on pervasive computing and communications (PerCom). Mannheim pp 217–226
3. Sanaei Z, Abolfazli S, Gani A, Shiraz M (2012) SAMI: service based arbitrated multi-tier infrastructure for mobile cloud computing. In: Proceedings of IEEE 1st international conference on communications in China workshops (ICCC). Beijing, pp 14–19
4. Mobile Edge Computing: https://en.wikipedia.org/wiki/Mobile_edge_computing
5. Satyanarayanan M, Bahl P, Caceres R, Davies N (2009) The case for VM-Based cloudlets in mobile computing. IEEE Pervasive Comput 8(4):14–23
6. Fog Computing: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf
7. OpenFog Consortium: https://www.openfogconsortium.org/
8. Haile N, Altmann J (2017) Evaluating investments in portability and interoperability between software service platforms. Future Gener Comput Syst
9. Akherfi K, Harroud H, Gerndt M (2016) A mobile cloud middleware to support mobility and cloud interoperability. Int J Adapt Resilient Auton Syst (IJARAS)
10. Cuervo E, Balasubramanian A, Cho D, Wolman A, Saroiu S, Chandra R, Bahl P (2010) MAUI: making smartphones last longer with code offload. In: Proceedings of ACM 8th annual international conference on mobile systems, applications and services (MobiSys'10). San Francisco, pp. 49–62
11. Marmalade: http://madewithmarmalade.com/
12. Abolfazli S, Sanaei Z, Shiraz M, Gani A (2012) MOMCC: market-oriented mobile cloud computing based on service oriented architecture. In: Proceedings of IEEE 1st international conference on communications in China workshops (ICCC). Beijing, pp. 8–13
13. Madhavapeddy A (2010) Mirage, a cloud operating system: http://www.openmirage.org (2010)
14. Vecchiola C, Chu X, Buyya R (2009) Aneka: a software platform for .NET-based cloud computing. In: Gentzsch W, Grandinetti L, Joubert G (eds.) High speed and large scale scientific computing. pp 267–295
15. Xiang S, Ansari N (2017) Green cloudlet network: a sustainable platform for mobile cloud computing. IEEE Trans Cloud Comput
16. Manjunatha A, Ranabahu A, Sheth A, Thirunarayan K (2010) Power of clouds in your pocket: an efficient approach for cloud mobile hybrid application development. In: IEEE 2nd international conference on cloud computing technology and science (CloudCom'10). Dayton, OH, pp 496–503
17. Sanaei Z, Abolfazli S, Gani A, Buyya R Heterogeneity in mobile cloud computing: taxonomy and open challenges. IEEE Commun Surv Tutorials
18. Abolfazli S, Sanaei Z, Sanaei MH, Shojafar, M., and Gani, A.,: Mobile Cloud Computing: The State-of-the-art, Challenges, and future research. Encyclopedia of Cloud Computing, wiley (2015)
19. Qi H, Gani A research on mobile cloud computing: review. Trend and Perspectives
20. Chang RS, Gao J, Gruhn V, He J, Roussos G, Tsai WT (2013) Mobile cloud computing research—issues, challenges and needs. Serv Oriented Syst Eng (SOSE)
21. Fernando N, Loke S, Rahayu W (2012) Mobile cloud computing: A survey. Future Gener Comput Syst 29(1):84–106
22. Roman R, Lopez J, Mambo M Mobile edge computing. In: Fog et al (eds) A survey and analysis of security threats and challenges. Future generation computer systems

23. Dinh H, Lee C, Niyato D, Wang P (2011) A survey of mobile cloud computing: architecture, applications, and approaches. Wireless Communications Mobile Computing
24. http://www.cloud-council.org/deliverables/CSCC-Interoperability-and-Portability-forCloud-Computing-A-Guide.pdf

Filter Bank Modulation in Massive MIMO Scenario

S. Sruthi and J. Dhoulath Beegum

Abstract Advancement in the field of wireless communication technologies emerges as a research area of increased interest due to the recent developments in 5G and Internet of things. Newer and better methodologies of modulation will help to achieve efficiency in energy and judicious use of spectrum. Filter bank multi-carrier modulation scheme in the context of 5G is a better alternative to any of the currently deployed schemes. This promises better intersymbol interference and inter-carrier -interference factors, and hence, it is ideal for massive MIMO scenarios. A comparative study of FBMC system with the presently deployed OFDM scheme is also analysed.

Keywords Massive MIMO · FBMC · OFDM · MU-MIMO · Impulse response · 5G

1 Introduction

As per the Cooper's law, the amount of wireless voice and data communication is increasing at an exponential pace. The Ericsson Mobility Report forecasts a 42% rise in mobile data traffic from 2016 to 2022. So we need to meet the continuously increasing demand and satisfy the rising expectations of service quality. Researchers need to turn every stone unturned to design new revolutionary wireless network technologies.

Massive multi-input multi-output (MIMO) wireless communication refers to the idea of equipping the cellular base stations with a very large number of antennas. Massive MIMO is a potential technology which allows for orders of improvement in parameters like spectral and energy efficiencies. Hence, better and efficient modulation schemes are the need of the hour. The commonly used modulation scheme

S. Sruthi (✉) · J. Dhoulath Beegum
Department of ECE, TKM College of Engineering, Kollam, Kerala, India
e-mail: sruthisree11@gmail.com

J. Dhoulath Beegum
e-mail: jdhoulathf@tkmce.ac.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_31

is Orthogonal Frequency-Division Multiplexing (OFDM). But it has some inherent disadvantages like need of a cyclic prefix code, problem of spectral leakage, etc.

Filter bank multi-carrier (FBMC) is a multi-carrier transmission approach. It possesses advantages over OFDM. FBMC does pulse shaping on each sub-carrier, and each sub-channel is then filtered. It does not require a cyclic prefix code which increases bandwidth efficiency [1]. It also promises good spectral efficiency and better data rate. So the large number of users can simultaneously use the data or voice service with minimal interference.

2 Related Work

MIMO scheme is still a widely researched arena of technology which needs advancements in various aspects of performance, security and efficiency to be met. Introduction of MIMO as a wireless service scheme can drastically enhance the capacity and reliability of wireless systems. The acceptance to Internet of Things (IoT), which is a network of networks, brought in the need for better and efficient wireless connectivity schemes.

In recent years, the focus has been shifted to a newer version of MIMO with enhanced capabilities. Multi-User MIMO (MU-MIMO) systems employ multiple antennas at the base station. The expensive communication components are needed only at the base station, and the user terminals can use relatively cheap single-antenna devices [2]. Also, the performance of MU-MIMO system is less sensitive to propagation environment than that in the case of point-to-point MIMO.

This paper focuses on filter bank multi-carrier (FBMC) modulation. Basically, filter bank technique is an improvement over direct FFT mechanism [3]. OFDM and its different variants require the property of orthogonality to be satisfied among all the carriers, whereas FBMC needs the property of orthogonality only for adjacent sub-channels. Also, OFDM makes use of a particular bandwidth of frequency with other carriers, whereas FBMC uses the transmission channel associated with a particular bandwidth to different sub-channels [4]. To put the channel bandwidth to complete use, sub-channels are to be modulated in such a way as to adapt with the orthogonality constraint of the neighbours and offset quadrature amplitude modulation.

3 System Model

Massive Multiple-Input Multiple-Output (MIMO) is a promising technological advancement that is under consideration for the fifth generation (5G) of mobile systems. But this technology requires improvement in parameters like data rate, energy efficiency and latency in comparison with the presently deployed LTE scheme [5]. In particular, due to the effect of considerable side-lobe interference due of sub-carriers in OFDM, it suffers from a high spectral leakage which results in higher out-of-band emissions (Fig. 1).

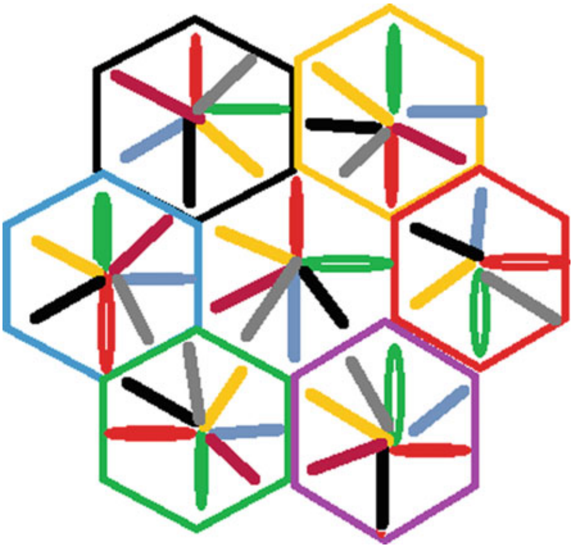


Fig. 1 Massive MIMO scenario

Filter bank multi-carrier (FBMC) is a 5G candidate waveform which has better spectral properties. The requirement of synchronization in uplinks can be relaxed, and imbibing carrier aggregation into the system becomes easy. Due to these advantages, the technique of FBMC is being actively studied to deduct the efficiency of the technique in practical scenarios.

In the proposed design, $d_{m,n}$ denotes the discrete time data symbol transmitted over the mth sub-carrier and nth time instant. The total number of sub-carriers is taken as M. To nullify the possible interference between data symbols and to maintain the orthogonality, the data $d_{m,n}$ is corrected in phase with the term $e^{j\theta}_{m,n}$, where $\theta_{m,n} = (\pi/2)*(m + n)$. Thus, each symbol will have a $(\pm\pi/2)$ difference in phase with its nearby neighbours in both time and frequency by means of which orthogonality is ensured. The output is upsampled and then given as input to the filter Fig. 2. Finally,

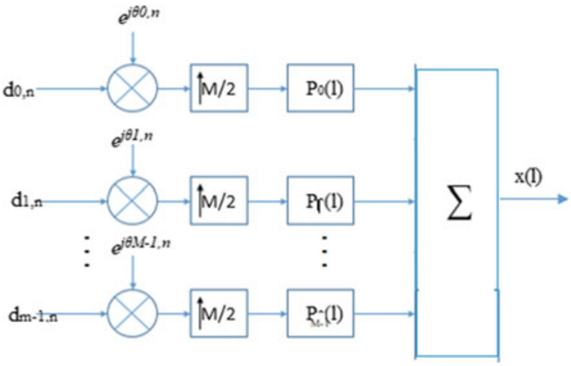


Fig. 2 Block diagram of the filter design

Table 1 Frequency domain filter coefficients

K	H_0	H_1	H_2	H_3
2	1	$\sqrt{2/2}$	–	–
3	1	0.911438	0.411438	–
4	1	0.971960	$\sqrt{2/2}$	0.235147

the pulses are shaped using the filter p(l), which has designed to be a Nyquist pulse which has zero crossings at every Mth intervals [6–10]. Mathematically, the technique that is described can be depicted as follows:

$$x(l) = \sum_{n=-\infty}^{+\infty} \sum_{m=0}^{M-1} d\mathrm{m}, n\, \mathrm{a}_{m,n}\ (l) \tag{1}$$

where

$$\mathrm{a_{m,n}}(l) = p_m\left(l - \frac{nM}{2}\right)\mathrm{e}^\wedge\, j\theta_{m,n} \tag{2}$$

Half-Nyquist filters are used at the transmitter and receiver ends [3]. The half-Nyquist filter with the corresponding frequency coefficients for $K = 2$, 3 and 4, respectively, is as in Table 1.

The equation which gives impulse response $h(t)$ of the filter is given by

$$h(t) = 1 + 2\sum_{k=1}^{K-1} Hk\left(\cos\frac{2\pi kt}{KT}\right) \tag{3}$$

where H_k indicates the various frequency coefficients for different number of sub-carriers [11–13].

4 Results and Discussions

The FBMC modulation technique is implemented in the massive MIMO scenario. The OFDM technique is also carried out. A comparative study between the modulation techniques of FBMC and OFDM is done on the basis of spectral leakage, and the subsequent results are obtained as follows.

The impulse response will help to get an idea about the behaviour of the system to various inputs. The impulse response for the given filter is obtained as in Fig. 3.

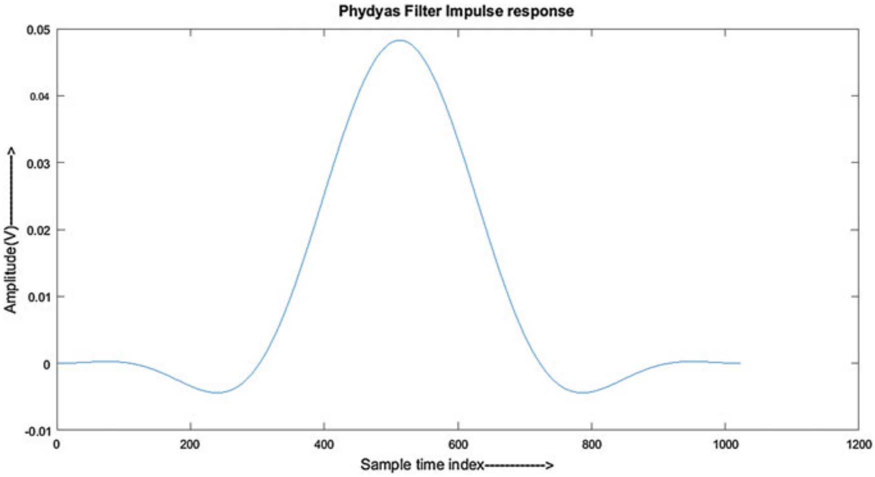


Fig. 3 Impulse response of the filter

It is pretty evident from the frequency response of the system Fig. 4 that the FBMC system offers a lower spectral leakage in comparison with the OFDM system. The OFDM plot shows a persistent intrusion of sub-bands in the required output band, whereas FBMC plot shows a gradual drop in the influence of sub-bands on the main output.

As frequency component increases, it can be observed that the spectral leakage drastically falls off in FBMC whereas it is not so in the case of OFDM. So FBMC is a reasonable approach for 5G systems where a large number of users and large

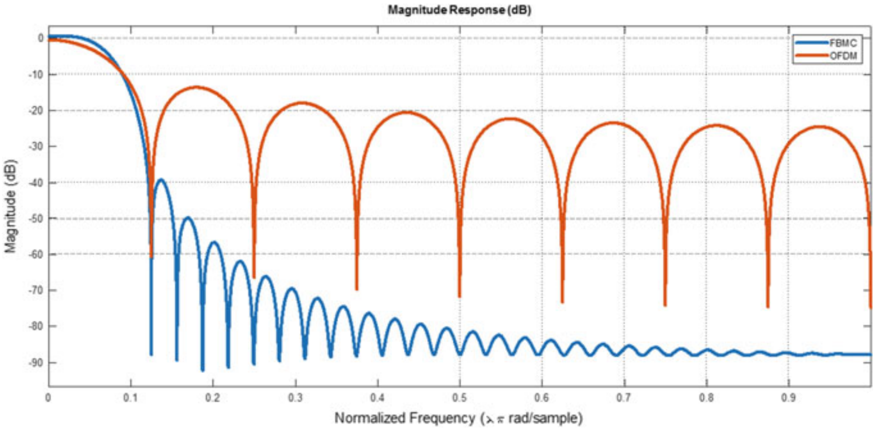


Fig. 4 Frequency response of the proposed system

number of devices are to be supported. Figure 5 depicts the frequency responses of the proposed FBMC system for varying number of sub-carriers (Fig. 6).

The response of the system for different number of sub-carriers is as plotted above. It can be observed that when $K = 2$, even though the spectral leakage is poor, the unwanted sub-bands have considerable strength. When $K = 3$, there is a drastic reduction in the strength of sub-bands, which can be filtered-off with a moderate filter. But when $K = 4$, it shows a very good response with minimal influence of

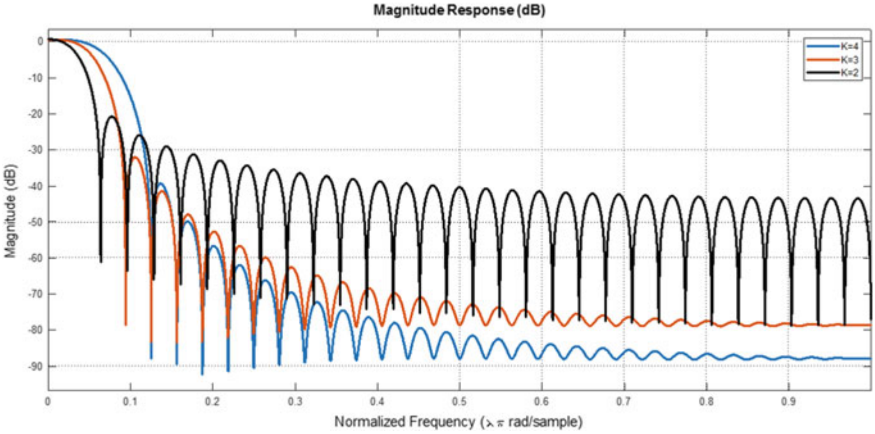


Fig. 5 Comparative study of FBMC with varying number of sub-carriers

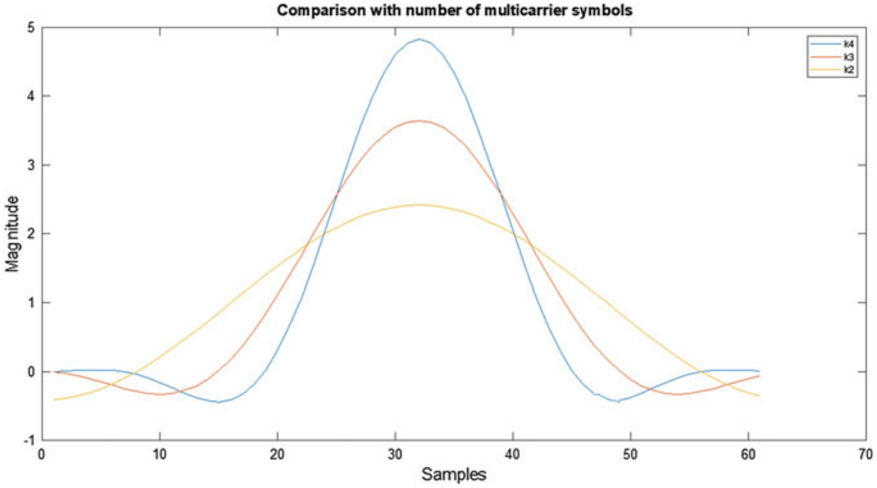


Fig. 6 Comparison of system with different number of sub-carriers

sub-bands. Therefore, it can be observed that, as the number of sub-carriers increase, the output is getting narrower (Table 2).

It can be easily observed that, though there is a minimal difference between the leakage values of OFDM and FBMC systems in the initial samples, but as the succeeding samples are analysed, it becomes clear that the leakage values are very low for FBMC in comparison with OFDM. The truncation of the required frequency band is a demerit in case of OFDM (Fig. 7).

Table 2 Comparative study of spectral leakage values at different sample instants for OFDM and FBMC systems

Samples	OFDM	FBMC
0.0307	0.99	0.9891
0.0368	0.9857	0.984
0.043	0.9805	0.9777
0.0491	0.9746	0.9703
0.0552	0.9679	0.9614
0.0614	0.9605	0.9512
0.0675	0.9523	0.9395
0.0736	0.9434	0.9261
0.0798	0.9337	0.9111
0.0859	0.9234	0.8943
0.092	0.9124	0.8758
0.0982	0.9007	0.8555
0.1043	0.8883	0.8335
0.1104	0.8753	0.8097
0.1166	0.8617	0.7843
0.1227	0.8475	0.7574
0.1289	0.8326	0.729
0.135	0.8173	0.6993
0.1411	0.8014	0.6685
0.1473	0.7849	0.6367
0.1534	0.768	0.6042
0.1595	0.7506	0.5712
0.1657	0.7327	0.538
0.1718	0.7145	0.5047
0.1779	0.6958	0.4715
0.1841	0.6767	0.4388

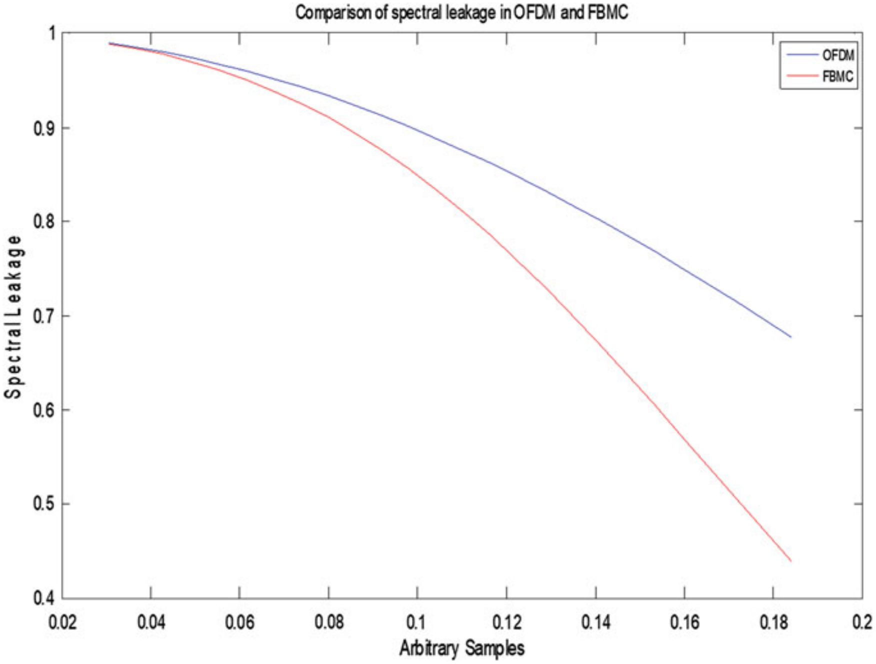


Fig. 7 Spectral leakage comparison for OFDM system versus FBMC system

5 Conclusions

The performance of filter bank multi-carrier (FBMC) modulation in massive MIMO scenario is studied and analysed. FBMC system is found to be advantageous since it does not require a cyclic prefix code before transmission. The impulse response of the filter and the frequency response of the system are plotted to compare with the presently deployed OFDM system. Influence of sub-bands on the required frequency component can be easily observed from the plot. The comparison of FBMC system with varying number of sub-carriers is also plotted. As frequency component increases, spectral leakage drastically falls off, and hence, inter-symbol interference is minimal. So FBMC is a potential candidate for 5G systems. A comparative study of FBMC and OFDM systems was carried out, and the parameters of spectral leakage of both systems were compared and it is concluded that FBMC system is better in all respects over OFDM scheme. Hence, efficiency of the system in terms of energy, spectrum, hardware, cost and resource utilization is better.

6 Future Scope

FBMC implementation in massive MIMO is a leading research topic in the international communication research arena. One of the future works on the topic will be to develop a scheme to combat the imminent problem of pilot contamination in the system so as to deploy it to incorporate dense heterogeneous networks. In the near future, the need for distributed massive MIMO will become more demanding, and hence, a study on the same can be carried out due to the integration of Internet of things, visible light communication and related technologies. FBMC promises to support carrier aggregation scheme.

References

1. Farhang A, Marchetti N, Figueiredo F, Miranda JP (2014) Massive MIMO and waveform design for 5th generation wireless communication systems. In: IEEE 5GU
2. Machrouh Z, Najid A (2018) High efficiency IEEE 802.11ax MU-MIMO and frame aggregation analysis. In: 2nd international conference on recent advances in signal processing, telecommunications & computing (SigTelCom). pp 107–110
3. Farhang-Boroujeny B (2014) OFDM versus filter bank multicarrier. IEEE Signal Process Mag 28(3):92–112
4. Farhang-Boroujeny B (2014) Filter bank multicarrier modulation: a waveform candidate for 5G and beyond. Adv Electri Eng
5. Ott D, Himayat N, Talwar S (2017) 5G: transforming the user wireless experience. In: Towards 5G: applications, requirements and candidate technologies. pp 34–51
6. Aminjavaheri A, Farhang A, Doyle LE, Farhang-Boroujeny B (2017) Prototype filter design for FBMC in massive MIMO channels. In: IEEE ICC signal processing for communications
7. Marzetta TL (2015) Massive MIMO: an introduction. Bell Labs Tech J 11–22
8. Abuibaid MA, Colak SA (2017) Energy-efficient massive MIMO system: Exploiting user location distribution variation. AEU Int J Electron Commun72:17–25
9. Farhang A, Marchetti N, Doyle LE, Farhang-Boroujeny B (2014) Filter bank multicarrier for massive MIMO. In: 2014 IEEE 80th vehicular technology conference (VTC2014-Fall)
10. Bellanger M, Le Ruyet D, Roviras D, Terr´e M, Nossek J, Baltar L, Bai Q, Waldhauser D, Renfors M, Ihalainen T et al (2010) FBMC physical layer: a primer. PHYDYAS
11. Elijah O et al (2015) A comprehensive survey of pilot contamination in massive MIMO—5G System. IEEE Commun Surv Tutorials 18(2)
12. Zafar A, Zhang L (2018) Spectrum efficient MIMO-FBMC system using filter output truncation. IEEE Trans Veh Technol 67(3)
13. Banelli P, Buzzi S, Colavolpe G, Modenini A, Rusek F, Ugolini A (2014) Modulation formats and waveforms for 5G networks: who will be the heir of OFDM?: An overview of alternative modulation schemes for improved spectral efficiency. IEEE Signal Process Mag 31(6):80–93

Autonomous Farming—Visualization of Image Processing in Agriculture

Shivam Thakur, Sushant Bawiskar, Sachin Kumar Singh and M. Shanmugasundaram

Abstract Nowadays, it is important to automate the processes in farming. For efficient farming, we can use embedded systems and IoT by which farming could become like a video game. Robots in control are more than a simple case study. We are demonstrating a simple example of Ploughing in which Tractor has its own vision, through which it can identify the boundary of the field and can plough the field without any driver. A farmer can easily operate various farming operations on his smartphone in just one tap. The vision is able to detect the poles on the boundary of farm, and using image processing, camera on tractor is able to detect the colour flag on a pole, and by detecting the colour of the pole, it is able to turn by its own and plough the field completely and stop. We can use this concept to automate the seeding, irrigation, weeding, harvesting, delivery, etc., depending upon the crop.

Keywords Raspberry Pi · IoT · Image processing

1 Introduction

India is growing day by day in every sector such as manufacturing and IT sector [6]. But India is still lagging somewhere in the agricultural sector. Although the government is doing a lot of efforts to improve productivity and so to help farmers, they are launching new schemes, but still, somewhere we have an option to use technology that brings us a better future. It can boost the agriculture sector by not

S. Thakur (✉) · S. Bawiskar · S. K. Singh · M. Shanmugasundaram
Department of Embedded Technology, VIT, Vellore, India
e-mail: shivam.thakur2018@vitstudent.ac.in

S. Bawiskar
e-mail: sushant.ravindra2018@vitstudent.ac.in

S. K. Singh
e-mail: sachinkumar.singh2018@vitstudent.ac.in

M. Shanmugasundaram
e-mail: phdsundaram@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_32

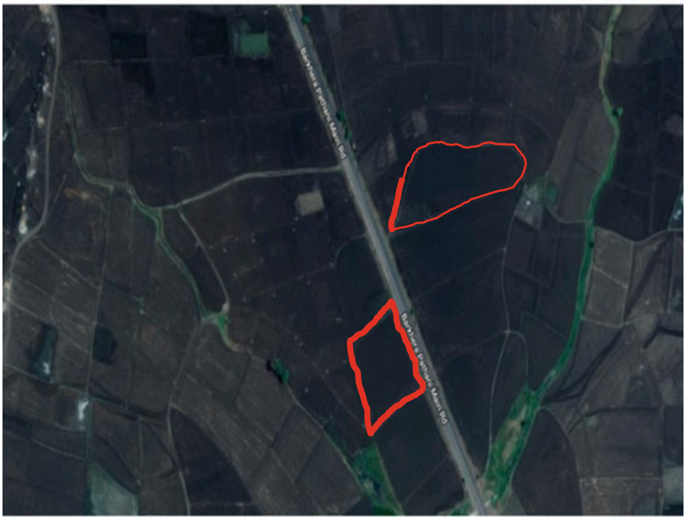


Fig. 1 Different variation in lands

only making convenient to farmers, but also the agriculture department can easily monitor productivity and can suggest the farmer in real time.

Robots represent a natural source of inspiration and a great pedagogical tool for research and teaching in control theory [5]. Here, we have introduced with the concept of autonomous ploughing technique in which a camera on a tractor can be able to detect the boundary of the land and can plough the land completely without any driver using IoT. Since lands can be of any shape, it can have variations in level as shown in Fig. 1.

The farmer just needs to keep some poles with colour in his farm boundaries, and then, he has to just press one button on his mobile and he can sit back and relax. His field will be ploughed automatically by using image processing and IoT [4]. We made a prototype which works on the same principle by interfacing Raspberry pi [9] and IoT as shown in Fig. 3.

We can also automate next steps in farming such as seeding, irrigation, and harvesting [2]. Automation in farming can increase the productivity of agricultural sector, and we can actually save a lot of fuel by making electric tractor and install multiple sensors which can monitor the production rate in real time and using IoT. This real-time data can be accessed by Agriculture Department using cloud computing [3]. A farmer can get the real-time suggestions on mobile app and can work accordingly. Humidity variations and temperature variations can cause a severe reduction in the growth of a crop [8]; thus, it is important to know that when and what a crop needs actually. In summer, field dries very quickly; thus, it is important to irrigate the field more frequently, whereas, in winter and rainy season, it needs water less frequently. So, in this way, we can achieve automation in irrigation and can develop various automated techniques in farming.

Similarly, IoT can play a major role in connecting everything to a cloud, and in this way, we can get the efficiency of seeds by calculating at the time of harvesting. Also, by knowing the environmental conditions, we can improve productivity by implementing solutions for location-based challenges [11].

An improved version of modern agriculture is with the seeding machine the ground it covers is faster than human [10]. Best chance seeds have to rooter and grow now the farming comes in the digital arena with the IoT-based system which gives data to the farmers. The whole farming land is planted by a single human monitoring process over a control dashboard laptop or tablet which gives us proper output with the desired accuracy, which is in the favour of the farmer. Basically, the proper planting depends on two parameters: proper depth of seeds and spacing between plants. In the early stage, these two problems come in front of farmers; by autonomous farming, we can control these two parameters.

2 Related Work

Today's farmers are using traditional methods for farming which is the main reason for less productivity and wastage of electricity; some methods are introduced to overcome these problems; automated farming robot is also a big concept in which attempt is done to connect robotics and automation with agriculture. The main intention is to reduce the effort of farmers encountered in the field. The main reason for using electric vehicles is to reduce greenhouse gasses and carbon footprints.

The robots [12] are used to assist farmers in the agriculture field; the technology used to control the system is Raspberry Pi which provides manual controlling of the system. The system proposed is used for ploughing, dispensing, and fruit picking [7].

3 Proposed Method

Here, we have made a prototype which has a ploughing mechanism and also a Raspberry Pi and USB camera. As shown in Fig. 2 using OpenCV and NumPy, we were able to differentiate between colours, and thus, we can program the tractor such that it ploughs the complete field in a zigzag manner by detection colours on the poles. If it detects the red colour, then it has to turn 180° right and plough the side lane, and if it detects the blue colour, then it has to turn 180° from the left side and again plough the side lane and so on; it completes the complete land irrespective of field size and shape. Farmer has to just set poles on boundaries before starting operation. And rest the autonomous tractor will do [1].

As shown in Fig. 3 if the camera detects the yellow colour, then the vehicle needs to stop. The farmer needs to get connected with cloud server MQTT, and then, he can turn off the ploughing in between whenever he wants. It is completely user-friendly

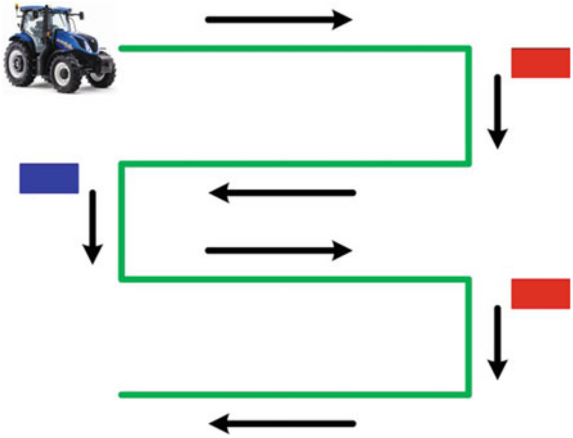


Fig. 2 Ploughing path

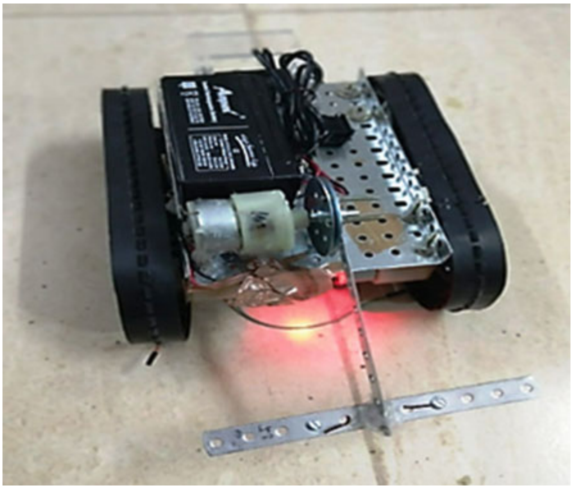


Fig. 3 Prototype

and like a social media platform where farmer is able to interact with the need of its crops by getting information from a bunch of sensors installed on the field.

3.1 Flowchart

Here, we have demonstrated the connection of MQTT server in which if farmer turns on the ploughing through tractor, then it will start and take input from the camera. The camera tells it, where to go. As shown in Fig. 4 if tractor detects yellow colour, then it needs to stop. Colour detection: Where the camera is used to capture and also to provide input to code. Image captured by the camera is in BGR format, i.e.

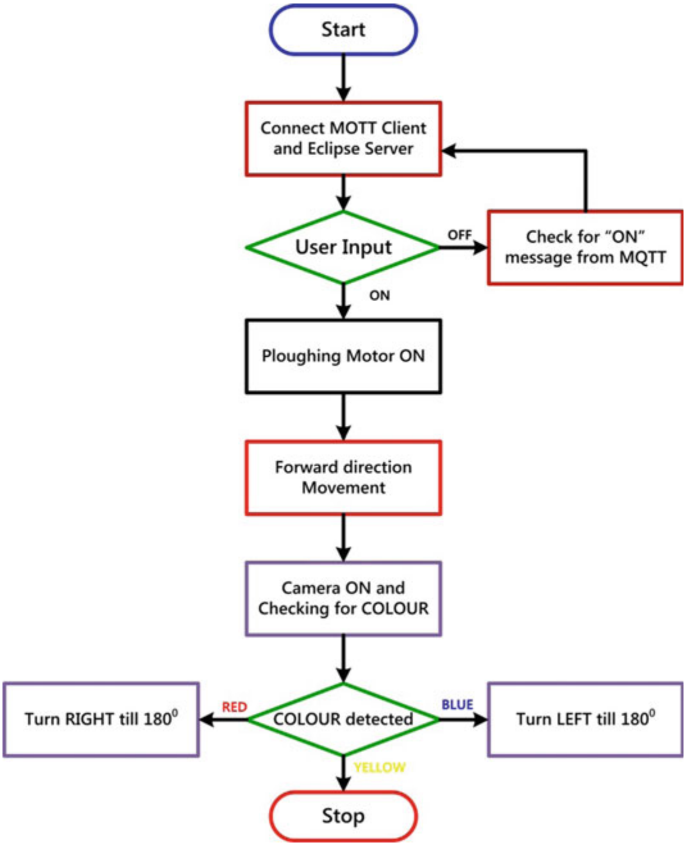

Start
Connect MQTT Client and Eclipse Server
User Input
OFF
Check for "ON" message from MQTT
ON
Ploughing Motor ON
Forward direction Movement
Camera ON and Checking for COLOUR
COLOUR detected
RED
Turn RIGHT till 180^0
BLUE
Turn LEFT till 180^0
YELLOW
Stop

Fig. 4 Flowchart

red, green, and blue. All digital devices use this type of input, but for proper colour detection, we are using HSV format.

HSV means hue, saturation, and value where hue is colour, saturation is greyness, ad value means the brightness of the pixel. Saturation value near means it is dull or grey looking.

The red colour in OpenCV has hue value approximately in the range of 0–10 and 160–180. In OpenCV, value range for three matrices is 0–179(Hue), 0–255(Saturation), 0–5(Value) or (colour), (Saturation), (Brightness).

Saturation: Saturation value represents the amount to which that colour is mixed with white.

Value: Value represents the amount to which that colour is mixed with black.

Figure 5 shows a flowchart for image processing in which morphological transformation is done to remove small noises in the image. Morphological transformations are some operation which is based on the shape of images; for this, we need two inputs: one is original image and another input is the kernel. Kernel decides the nature

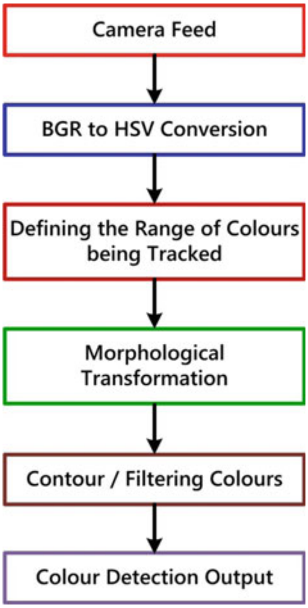

Camera Feed
BGR to HSV Conversion
Defining the Range of Colours being Tracked
Morphological Transformation
Contour / Filtering Colours
Colour Detection Output

Fig. 5 Image processing flowchart

of the operation be performed on the image. Two very basic morphological operators are dilation and erosion. In this, we use dilation and a 5*5 kernel matrix. If at least one pixel under kernel is one, it will simply increase colour region and reduce noise in the image. Dilation adds a layer of a pixel to both inner and outer boundaries of the region.

Now, contour the image previously described means differentiating each colour with the rectangular bounded line which is called a-a contour. A simple line connects continuous points, having the same colour or intensity. Contour is a tool mainly used for shape detection and analysis and object detection and recognition.

4 Conclusion and Future Scope

The prototype is able to plough the field without any human effort. It is also designed in such a way that it follows a specific predefined path by using colour detection. Advance enhancements can be done by installing a drone in the prototype which can fly on the field and can time to time monitor the status of crops. The drone can provide a real-time video feed to the farmer. This can also be used to monitor land. These drones can also be used for theft protection.

References

1. Canudas de Wit C, Siciliano B, Bastin G (eds) (1996) Theory of robot control. Springer-Verlag, New York
2. Liu JJ, Wu L (2014) The study on autonomous agricultural machinery. Modelling and control method. Sens Transducers
3. Goldberg K (ed) (2000) The robot in the garden: telerobotics and telepistemology in the age of the internet. MIT Press, Cambridge, MA
4. Ulrich I, Nourbakhsh I, Appearance-based obstacle. Detection with monocular color vision. In: The proceedings of the AAAI national conference on artificial intelligence. Austin, TX
5. Canudas de Wit C, Siciliano B, Bastin G (eds) (1996) Theory of robot control. Spinger-Verlag, New York
6. Thankachan S, Kirubakaran S (2014) E-agriculture information management system. Int J Comput Sci Mobile Comput 3(5)
7. Umbaugh SE (2016) Digital image processing and analysis: human and computer vision applications. With CVIP tools. CRC Press
8. Tillett ND, Hague T, Merchant JA (1998) A robotic system for plant scale husbandry. J Agric Eng Res 69:169–178
9. Senthilkumar G, Gopalakrishnan K, Sathish Kumar V (2014) Embedded image capturing system using raspberry Pi system. 3(2):213
10. Srivastava UK (1989) Agro-processing industries: potential, constraints and tasks ahead. Indian J Agric Econ 44(3):42–256
11. Dwivedy N (2011) Challenges faced by the agriculture sector in developing countries with special reference to India. Int J Rural Stud 18(2)
12. Siegwart R (2004) Introduction to autonomous mobile robots. MIT.Press, Cambridge, MA

Design and Development of End Effector for Domestic Robots

V. Indu, Putchala Vinay, Narjala Rohith, Kuppili Puneeth and S. Pramod

Abstract The aim of this work is to design and develop efficient and low-cost end effector for holding and handling of fragile objects, which is to be used in the industrial automation and mainly for the purpose of domestic robots. The design consists of three systems: the sensor system, the control module, and the robotic end effector. Different objects have different stress-handling capabilities, when pressure is applied on the object goes beyond the yield point, and then object either deforms or breaks. So, the aim of this work is to utilize that strain being applied to the object for holding the object and handling it carefully. This end effector works with a single degree of freedom. The end effector is designed to have three grasping fingers out of which one is stable with the sensor on it and other two fingers are attached to a single joint with common motion to both fingers.

Keywords Robotic gripper · End effector · Manipulation · Strain sensor

V. Indu · P. Vinay (✉) · N. Rohith · K. Puneeth
Department of Electrical and Electronics Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India
e-mail: vinayputchala@am.students.amrita.edu

V. Indu
e-mail: induv@am.amrita.edu

N. Rohith
e-mail: rohith@am.students.amrita.edu

K. Puneeth
e-mail: puneeth@am.students.amrita.edu

S. Pramod
Department of Mechanical Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India
e-mail: pramods@am.amrita.edu

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_33

1 Introduction

Robots are used to ease human processes; they are widely used in the field of industries and also used for domestic purposes. Household robots can perform many tasks such as cleaning your house, mowing your lawn, and many more. Nowadays we can see the increasing importance in industrial automation where the robotic processes form the crux of this evolution.

End effector is designed to handle various objects of varying shapes and sizes. While designing the end effector, object handling should be taken into primary focus as there is a chance of contortion of the object. With this, we also need to take proper discretion in checking its domestic and industrial needs.

The usage of mechanical grippers is the most common method of making end effectors. Here, perpetual usage of force on the object by the end effector is used to retain the object [1]. But these may not handle fragile objects without contorting them as mechanical grippers are not touch sensitive as our human hands [2]. The usage of programming to hold and release various objects of different shapes and sizes with disparate touch sensitivities is a strenuous task [3]. A five-finger robot gripper with wire, five fingers of the robot using ultrasonic motors, and various other robot hands are being researched. These types of end effectors are tough to build because of the intricate structure and due to the lack of assurance in safe handling [4]. The task of handling fragile household objects such as eggs and vegetables intact is still a challenge in today's world. As mentioned above, the most common end effectors are made up of mechanical linkages which follow a very rough approach in handling but they are not very precise. The gripper is inspired from the most efficient end effector which is the human hand [5]. The usage of polymer strings with servo motors can be a great help in handling delicate objects but its high cost makes it unlikely for utilizing in domestic robots [6]. The usage of depth sensor for finding the end effector data points through the angle and position of the end effector is set [7].

The motto of this work is to develop a flexible, cost-efficient gripper that can handle fragile objects without deformation. So the most important design objective in our work is to utilize the strain, as it varies from object to object.

2 Working of the Gripper

The end effector developed works on a closed-loop control system, where the measured stress value from the stress sensor acts as the loop. Initially, reference stress, i.e., stress where an object can be manipulated, is fed to the microcontroller. Now the microcontroller generates the required PWM pulses with respect to error which is calculated using the difference in measured stress and the reference stress. Then the servo motor which is the actuator converts the PWM signals to the motion, where the motion occurs in angular motion in angles (degree). As the servo is connected to gripper, gripper moves and applies force on the object. The force is being applied in

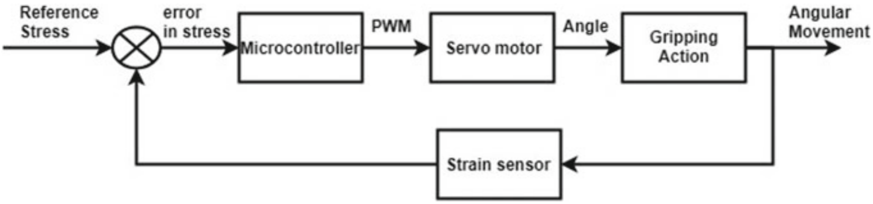


Fig. 1 Block diagram

the form of stress, so stress is being applied on the object, and the stress is perpetually being cross-checked with the reference value. Every time when the reference value is greater than the stress, that difference is given to microcontroller as shown in Fig. 1.

The microcontroller then feeds the pertinent PWM pulse to produce angle through servo and which in the process is converted to stress as described above. Once reference value is equal to the stress value applied, then the microcontroller stops giving PWM input to the servo motor which in return emulates the same zero output due to no input and maintains the stable position where the object can be manipulated for pick and place actions.

3 Algorithm

Initialize the control pins in the microcontroller, which is used to send or receive the data. Calibrate the sensor to reduce the error while obtaining the measured stress value. The reference stress value of the object that is to be handled by the gripper is initially fed to the microcontroller.

Now as mentioned in the working of the gripper, the PWM generated is converted into angular motion, then the gripper applies force on the object. The stress that is being applied on the object is perpetually being cross-checked with the reference value. Every time when the reference value or the threshold is greater than the stress, that difference is given to microcontroller.

Microcontroller unit generates the PWM pulses so that it can increment the angular motion of servo with the angle of one degree. And the loop continues till the error in the stress becomes zero; i.e., both the measured value and the reference stress values are the same (Fig 2).

4 Threshold Measurement and Tabulation

Stress values where the object can be held and manipulated are measured multiple times and are tabulated. Using the tabulated values, the average is calculated to take that value as the reference threshold value for each object (Table 1).

Fig. 2 Algorithm flow chart

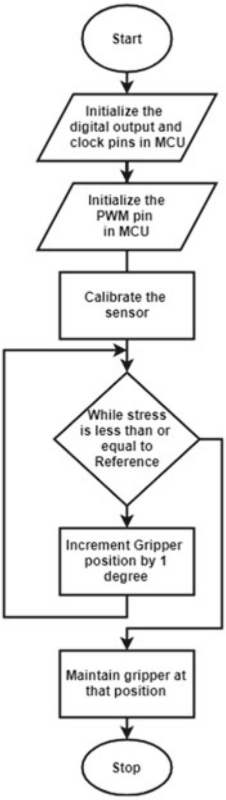

Start
Initialize the digital output and clock pins in MCU
Initialize the PWM pin in MCU
Calibrate the sensor
While stress is less than or equal to Reference
Increment Gripper position by 1 degree
Maintain gripper at that position
Stop

Table 1 Reference threshold

Object	Stress (lbs)
Plastic jar	4.23
Small plastic container	4.81
Steel glass	4.7
Plastic water bottle	2.62

5 Experimental Results

Different objects have different manipulated stress, so to check the stable position for holding the object the measurement was in angle (degree). So, we checked the angular position of object with respect to stress being applied on the object. Plot of angle versus stress is shown in Fig. 3 for plastic jar, Fig. 5 for plastic container, Fig. 7 for Steel glass, and Fig. 9 for plastic water bottle. The experiment had been repeated multiple times to check if the stress being applied is stable. Plot of time versus stress

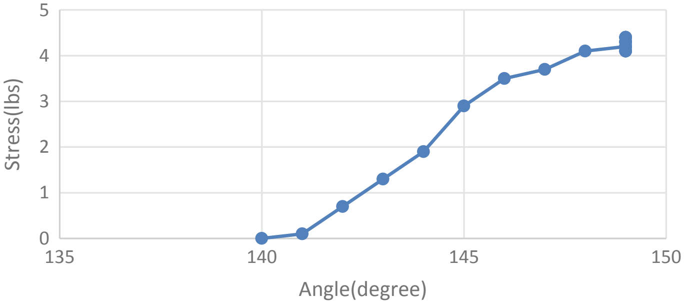


Fig. 3 Angle versus stress plot for plastic jar

is shown in Fig. 4 for plastic jar, Fig. 6 for plastic container, Fig. 8 for Steel glass, and Fig. 10 for plastic water bottle.

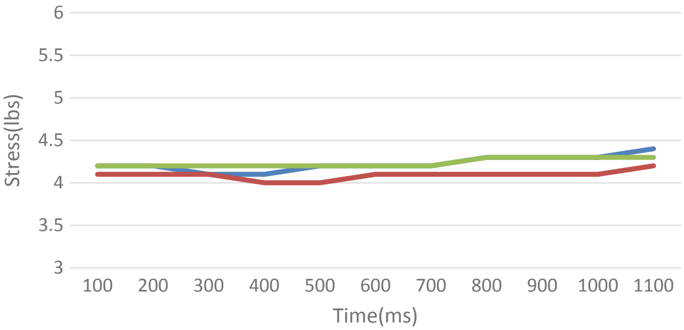


Fig. 4 Stress versus time during multiple manipulation periods for plastic jar

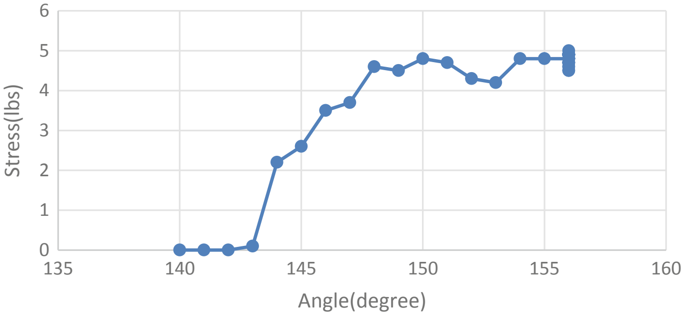


Fig. 5 Angle versus stress plot for small plastic container

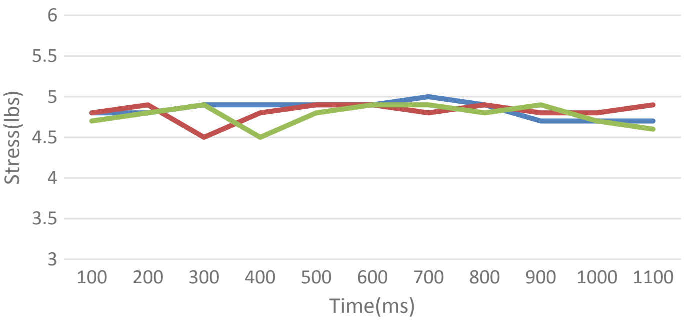


Fig. 6 Stress versus time during multiple manipulation periods for the small plastic container

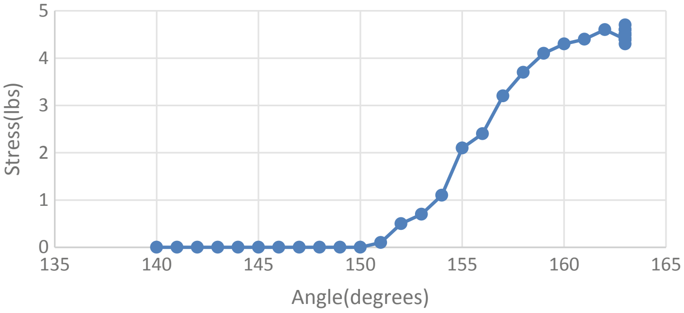


Fig. 7 Angle versus stress plot for steel glass

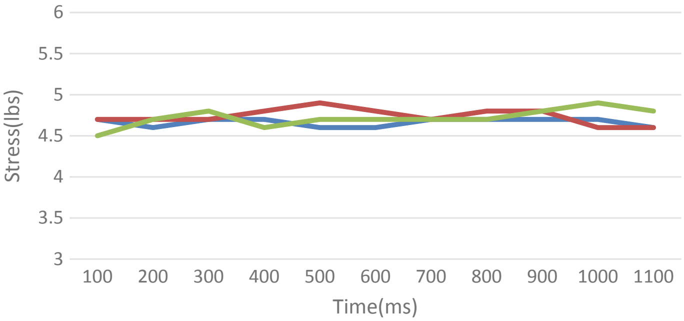


Fig. 8 Stress versus time during multiple manipulation periods for steel glass

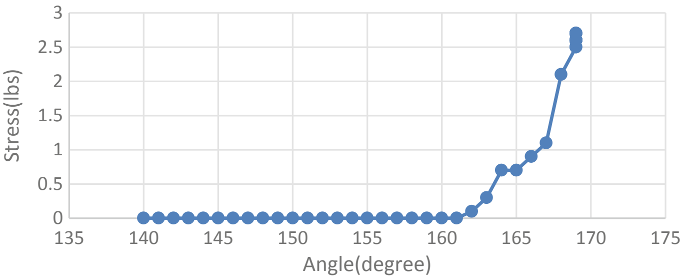


Fig. 9 Angle versus stress plot for plastic water bottle

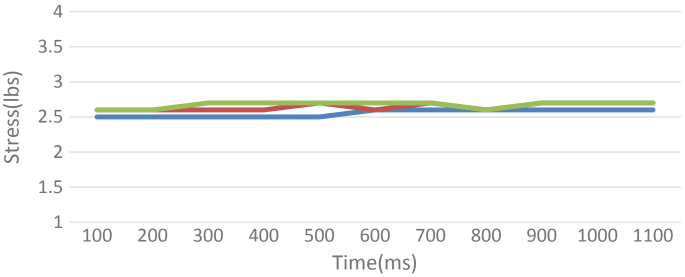


Fig. 10 Stress versus time during multiple manipulation periods for plastic water bottle

6 Conclusion

In this paper, we introduced a simple and easy method to handle fragile objects using their stress values. Using the reference stress values, the objects can be easily manipulated to move from one position to another without deformation, and algorithm implementation procedure has been discussed in this paper.

References

1. Sushmit AS, Haque FM, Shahriar Md, Bhuiyan SAM, Sarkar MAR (2017) Design of a gesture-controlled robotic gripper arm using neural networks. In: IEEE international conference on power, control, signals, and instrumentation engineering
2. Haque FM, Sushmit AS, Sarkar MAR (2017) Design of a voice-controlled robotic gripper arm using neural network. In: International conference on energy, communication, data analytics, and soft computing
3. Venter D, Dirven S (2017) Self morphing soft-robotic gripper for handling and manipulation of delicate produce in horticultural applications. In: 24th international conference on mechatronics and machine vision in practice (M2VIP)
4. Lee YC, Lim SJ, Hwang SW, Han CS (2009) Development of the robot gripper for a home service robot. In: ICROS-SICE international joint conference 2009

5. Choi MS, Lee DH, Park H, Kim YJ, Jang GR, Shin YD, Park JH, Baeg MH, Bae JH (2017) Development of multi-purpose universal gripper. In: Proceedings of the SICE annual conference (2017)
6. Pai UJ, Sarath NP, Sidharth R, Kumar AP, Pramod S, Udupa G (2016) Design and manufacture of 3D printec myoelectric multi-fingered hand for prosthetic application. In: International conference on robotics and automation for humanitarian applications (RAHA)
7. Megalingam RK, Vivek GV, Bandyopadhyay S, Rahi MJ (2017) Robotic arm design, development and control for agriculture applications. In: 4th international conference on advanced computing and communication systems (ICACCS)

Total Variation and Alternate Direction Method for Deblurring of Digital Images

S. Rinesh, C. Prajitha, V. Karthick and S. Palaniappan

Abstract Images captured using smartphones and video cameras are recorded and can be used anywhere and at any time. While taking a quick shot or while capturing the moving objects, it may lead to the motion blurred images. In order to recover the sharp images from motion blurred images, blind motion deblurring can be used. Motion deblurring can be done by knowing both edge and non-edge of motion blurred images. Edge and non-edge are the two methods used in total variation and alternate direction method for deblurring of digital images. Step edges can be predicted and detected by using edge-specific method. In non-edge method, it explores various image statistics, such as the prior distributions and it is sensitive to statistical variation over different images. Both methods are used in large dataset images, but it fails extremely in simple images. To overcome this problem, total variation (TV) based regularization method is used which is followed by an iteratively reweighted algorithm based on alternating direction method. To get higher results, LSED prediction—based technique is employed, which first of all restores sharp edges and then uses them to estimate initial kernel that traps the optimization of local minimum corresponding to sharp images.

Keywords Image restoration · Total variation · Alternating direction method · LSED prediction based method

S. Rinesh (✉) · V. Karthick · S. Palaniappan
Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India
e-mail: rin.iimmba@gmail.com

V. Karthick
e-mail: vkarthick86@gmail.com

S. Palaniappan
e-mail: s.palani.in@gmail.com

C. Prajitha
Department of Biomedical Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India
e-mail: praji.devi@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_34

1 Introduction and Related Work

The vital challenge of blind motion deblurring is that, the amount of unknown is far larger than the amount of accessible measurements. Given a blurred image, we would like it to figure out its sharp version and also the blur kernel.

Molina et al. [1] projected dirichlet distribution to model the blurring operate with smoothness constraints on the improved pictures to resolve blind deconvolution downside. MAP calculator is employed in modeling the original image [1]. Samson et al. [2] proposed the method for image classification that is mainly based on edge preserving regularization process. Variational model is predicted on regularization theory and mechanical action theory [2]. Likas and Galatsanos [3] proposed the expectation maximization (EM) algorithm reaps all the benefits of a full Bayesian model. This algorithm provides better improvement when compared to BID algorithm. Due to computational complexity and convergence assessment of markov chain it is difficult to implement BID algorithm [3]. Koschan and Abidi [4] proposed, Vector-valued techniques, which are used in detecting the edges in color images. Fergus et al. [5] proposed, conventional blind deconvolution and frequency-domain constraints on images. This is mainly focused on kernel estimation. But in non-blind deconvolution method, there will be some artifacts; this can also be improved [5]. Joshi et al. [6] projected sharp edge formula, which will be more useful to measure blur in the restricted device resolution by estimating a sub-pixel, super-resolved PSF even for in-focus images. If there is multi peak kernel it fails to sight edges [6]. Cho and Lee projected quick motion deblurring. Latent image estimation and kernel estimation are mainly used in prediction of step edges [7]. Xu and Jiaya [8] iterative support detection (ISD) kernel refinement, TV deconvolution model is used to handle narrow structure exist in latent images. The edge-specific theme depends on the economical detection or prediction of large-scale step edges (LSEDs), detection-based strategies [9], assume that sharp explanations is favored by the distributed previous for LSEDs. The detection of LSEDs will cause the generation of a pointy version of the input blurred image, this assumption holds only tiny windows around LSEDs. Prediction—based ways adopt sharpening filters [9] inverse random model to revive LSEDs.

LSED detection-based strategies assume that sharp explanations area unit favored by around step edges. LSED prediction—based way first of all restore sharp step edges and so use them to estimate a decent initial kernel, that traps the improvement into local minimum corresponding to sharp resolution. The most usually used approach to revive step edges is that the shock filter. LSED work well for images with straight forward textures and infrequently fail to handle extremely rough texture pictures. The performance of edge-specific theme is greatly restricted by its inability to recover large kind of image edges.

The non-edge-specific theme on the other hand is not designed to hold out deblurring based on detection or prediction of LSEDs. Adopting image measurements to favor sharp explanations [10], however such measurements work just only for little variety of natural images. Marginalizing the thin previous distribution [5, 11] proved that this approach results in actually handling the condition that the image size is far larger than the kernel size.

To address the matter of each edge specific and non-edge-specific scheme, a unique non-edge specific adaptive scheme [NEAS] is projected. NEAS is combination of marginalization and LSED method. NEAS work just for large dataset images, it fails to handle simple images, each of those strategies is unable to supply higher results because of lack of edges, so this makes the kernel estimation unreliable. NEAS produces top quality of results for large dataset images. To overcome such problem, total variation (TV) and an iteratively reweighted algorithm supported by alternating direction method (ADM) is employed.

TV has proven to be a valuable construct in reference to the recovery of pictures that include piecewise smooth elements. TV regularization is standard in image restoration and reconstruction because of its ability to preserve image edges.

2 Proposed Scheme

Blind motion deblurring is an important subject to image processing community. Image deblurring could be a well-known ill-posed inverse drawback, increasing attention from several sectors. Image degradation process can be modeled as:

$$y = k \otimes x + n$$

where,

y observed blurred image,
k blur kernel,
x is the latent sharp image,
n is the image noise and
$\otimes$ denotes the convolution operator

To cope with such deblurring problem, many regularization techniques are used.

Total variation (TV) based regularization method uses [14], non convex first and second–order regularization is used in this proposed method and it is given by,

$$\min\left\{\frac{\mu}{2}\|Hf - g\|_2^2 + \varsigma\|Df\|_1^{v_1} + (1-\varsigma)\left\|D^2 f\right\|_1^{v_2}\right.$$

$\mu > 0$ is a regularization parameter. $v_1 v_2$ are hyper–laplacian distribution of first and second order derivatives. D, D^2 are the finite difference operator of first and second order. ς is the function which is used to preserve the image details in texture and edge region which should be close to 1. ς is achieved based on eigenvalues of the hessian matrix. Hessian matrix is used for kernel estimation.

$$J_{\sigma(f_k)=}\begin{bmatrix} D_{xx}(G_\sigma * f_k) & D_{xy}(G_\sigma * f_k) \\ D_{yx}(G_\sigma * f_k) & D_{yy}(G_\sigma * f_k) \end{bmatrix}$$

f_k is the image with motion blur, G_σ denotes Gaussian distribution function, D_{xx} is the first order derivative with respect to x, D_{xy} is the first order derivative with respect to xy, D_{yx} is the first order derivative with respect to yx, D_{yy} is the first order derivative with respect to y.

An iteratively reweighted algorithm based on alternating direction method is followed by large-scale step edge detection method, which uses shock filter to restore step edges in the blurred image.

2.1 Algorithm

INPUT

Blurred image g,
Hessian matrix,
Parameters µ, β_1, β_2, β_3, v_1, v_2,

INITIALIZATION

$$f_0 = u_0 = \text{g},\ V_0 = Df_0,\ \ W_0 = D^2 f_0,\ \ \omega_0 = 0,\ \ \lambda_0 = 0,\ \ \xi = 0$$

While stopping criterion is not satisfied do

(1) Compute $V_{k+1} = \max\left\{\left\| Df_k + \frac{\omega_k}{\beta_1}\right\|_2 - \frac{\varsigma_k \Psi_1}{\beta_k}\right\}$

Df_k is the first order derivative of blurred image, ω_k is the initialization according to iteration β_1 is the parameter, ς_k denotes the kernel estimation for first order derivative, Ψ_1 is the first order derivative of blurred image.

(2) Compute $w_{k+1} = \max\left\{\left\| Df_k + \frac{\omega_k}{\beta_1}\right\|_2 \frac{(1-\varsigma_k)}{\beta_2}\right\}$

$(1 - \varsigma_k)$ is the kernel estimation for first order derivative, Ψ_2 denotes second order derivative of blurred image

(3) Compute $u_{k+1} = \left(f_k + \frac{\xi_k}{\beta_3}\right)$

End while.

LARGE-SCALE STEP EDGE DETECTION METHOD
The LSED of x_m is sharpened using the shock filter, $x_m = x_m - \text{sign}(\Delta x_m) \sum \gamma \| f_\gamma(x_m) \| \text{d}t$.

Here Δ is laplacian operator $\text{d}t = 0.8$ [7, 15].x_m denotes the convolution of Gaussian point spread function with blurred image. $\| f_\gamma(x_m) \|$ is the normalization of gradient operation with respect to x, y.

3 Experimental Results

The experiments on the large dataset are shown in Fig. 1. Total variation and alternate direction method handles both large dataset and simple images. We used four images from large dataset. In the commencement, in the first step the original image is motion

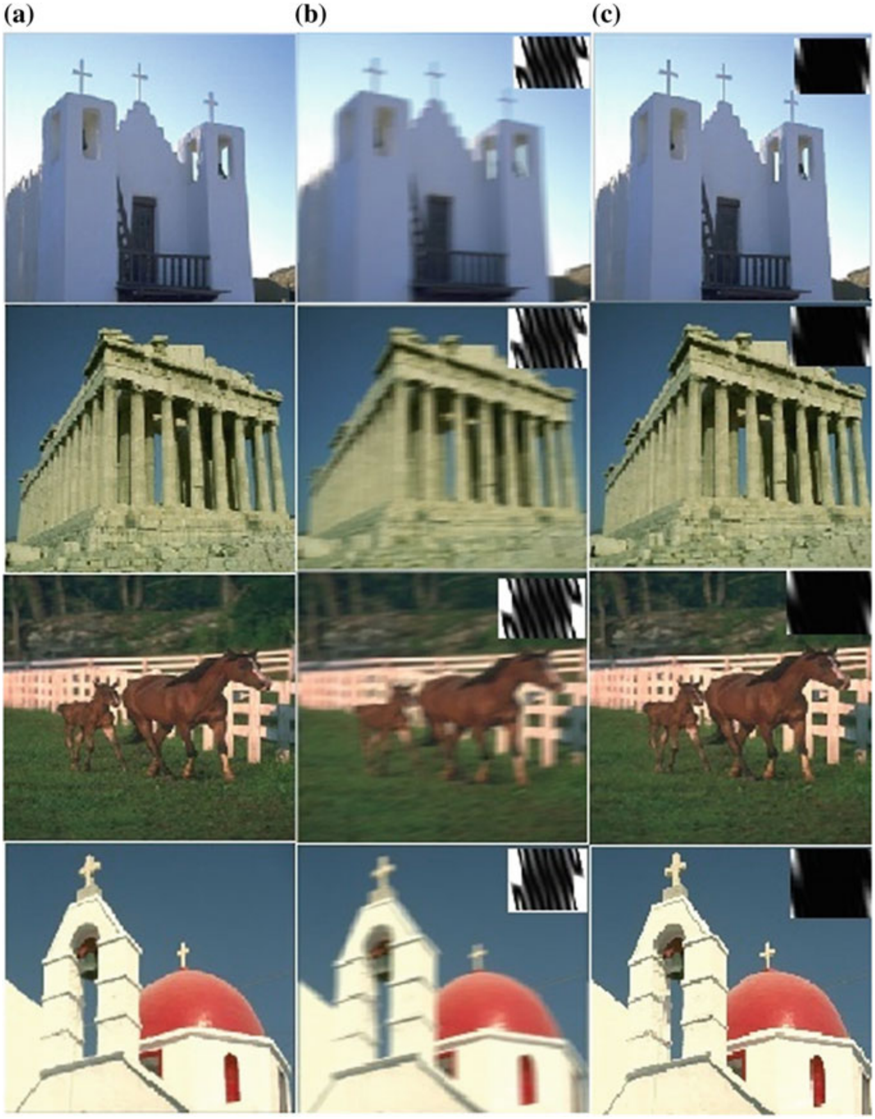


Fig. 1 In large dataset, four images are compared. From left to right are **a** the sharp images, **b** motion blurred images (30,20), kernel estimation and **c** the output produced by our method TV and ADM

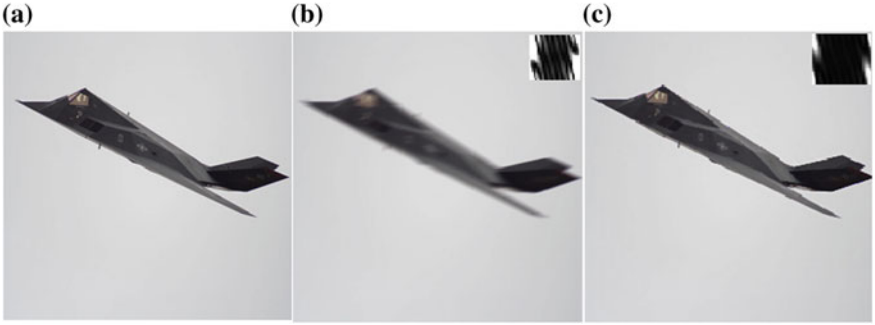


Fig. 2 Results produced for simple image 1. From left to right are **a** the sharp images **b** motion blurred images (30,20), kernel estimation and **c** the output produced by our method TV and ADM

blurred, and blurred image was restored using total variation and alternate direction method (Figs. 2, 3, Tables 1, 2).

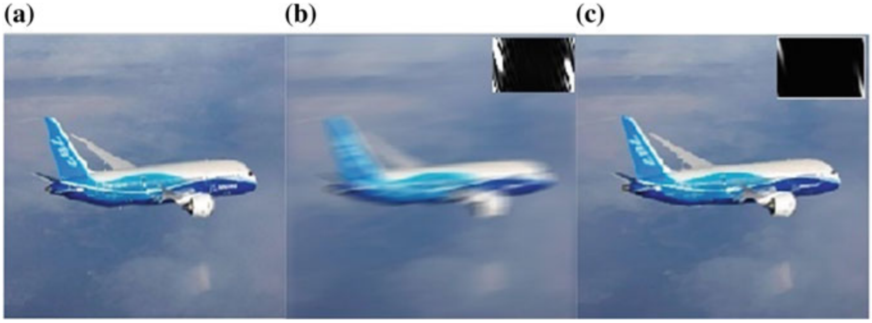


Fig. 3 Results produced for simple image 2. From left to right are **a** the sharp images **b** motion blurred images (30,20), kernel estimation and **c** the output produced by our method TV and ADM

Table 1 Parameter analysis for images in large dataset

Images in large dataset	Size	PSNR (dB)	PSNR (dB) [15]
Image 1	256 × 256	31.6	24
Image 2	256 × 256	26.5	24.2
Image 3	512 × 512	28.5	25
Image 4	512 × 512	30.2	26.2

Table 2 Parameter analysis for simple images

Simple images	Size	PSNR (dB)	PSNR (dB) [15]
Image 1	256 × 256	33.3	24
Image 2	256 × 256	31.3	24.1

4 Conclusion

In this proposed work, total variation (TV) based regularization method was proposed, which could preserve edges and the kernel estimation for motion blurred images is done. TV method is followed by an iteratively reweighted algorithm based on alternate direction method. TV and alternate direction method is used to handle the images in large dataset and also on extremely simple images.

References

1. Molina R, Katsaggelos AK, Abad J, Mateos J (1997) A Bayesian approach to blind deconvolution based on Dirichlet distributions. In: Proceedings of international conference on acoustics, speech and signal processing, pp 2809–2812
2. Samson C, Blanc-Feraud L, Aubert G, Zerubia J (2000) A variational model for image classification and restoration. IEEE Trans Pattern Anal Mach intell 22(2):460–472
3. Likas AC, Galatsanos NP (2004) A variational approach for Bayesian blind image deconvolution. IEEE Trans Signal Process 52(8):2222–2233
4. Koschan A, Abidi M (2005) Detection and classification of edges in color images. IEEE Signal Process Mag 22(1):64–73
5. Fergus R, Singh B, Hertzmann A, Roweis ST, and Freeman WT (2006) Removing camera shake from a single photograph. ACM Trans Gr 25(3):787–794
6. Joshi N, Szeliski R, Kriegman D (2008) PSF estimation using sharp edge prediction. In: Proceedings of IEEE conference on computational vision pattern recognition, pp 1–8
7. Cho S, Lee S (2009) Fast motion deblurring. In: Proceedings SIGGRAPH Asia, pp 1–8
8. Xu L, Jiaya J (2010) Two-phase kernel estimation for robust motion deblurring. In: Proceedings of 11th European conference on computer vision, pp 1–14
9. Harmeling S, Hirsch M, Scholkopf B (2010) Space-variant single-image blind deconvolution for removing camera shake. In: Advances in neural information processing systems. Cambridge
10. Krishnan D, Tay T, Fergus R (2011) Blind deconvolution using a normalized sparsity measure. In: Proceedings of IEEE conference on computer vision and pattern recognition, pp 233–240
11. Levin A, Weiss Y, Durand F, Freeman WT, (2011) Efficient marginal likelihood optimization in blind deconvolution. In: Proceedings of IEEE conference on computer vision and pattern recognition, pp 2657–2664
12. Levin A, Weiss Y, Durand F, Freeman WT, (2009) Understanding and evaluating blind deconvolution algorithms. In: Proceedings of IEEE international conference on computer vision, pp 1–8
13. Kundur D, Hatzinakos D (1996) Blind image deconvolution. IEEE Signal Process Mag 13(3):43–64
14. Liu RW, Xu T (2013) A robust alternating direction method for constrained hybrid variational deblurring model. In: Proceedings of computer vision and pattern recognition, pp 1–8
15. Wang C, Yue Y (2013) Non edge-specific adaptive scheme for highly robust blind motion deblurring of natural images. IEEE Trans Image process 22(3):884–893

16. Krishnan D, Fergus R (2009) Fast image deconvolution using hyper-Laplacian priors. In: Advances in neural information processing systems. MIT Press, Cambridge, MA
17. Whyte O, Sivic J, Zisserman A, Ponce J (2010) Non-uniform deblurring for shaken images. In: Proceedings of IEEE conference on computer vision pattern recognition, pp 491–498
18. Roth S, Black MJ (2007) Steerable random fields. In: Proceedings of IEEE international conference on computer vision, pp 1–8
19. Ayers GR, Dainty JC (1988) Interative blind deconvolution method and its applications. Opt Lett 13(7) pp 547–549
20. Ankit G, Neel J, Larry Z, Michael C, Brian C (2010) Single image deblurring using motion density functions. In: Proceedings of 11th European conference on computer vision, pp 171–184

Design of MIMO Triangular Microstrip Patch Antenna for IEEE 802.11a Application

M. Arulaalan, K. Mahendran, P. Prabakaran and G. Manikannan

Abstract A compact multiple-input-multiple-output (MIMO) antenna for wireless local area network (WLAN) applications with dual-band characteristics is presented. The proposed antenna is composed of two microstrip line-fed fractal triangular microstrip antenna. To achieve good return and high isolation, a Z-shaped stub is added in the ground plane. To reduce the mutual coupling and ECC, a Z-shaped stub is added to the ground plane. The proposed antenna covers the bandwidths of WLAN 5.2 GHz (5.11–5.23 GHz) and 5.8 GHz (5.72–5.92 GHz). A high isolation over −25 dB is achieved for both the IEEE 802.11a bands. The MIMO antenna return loss, envelope correlation coefficient, gain and radiation characteristics are also investigated. The results indicate that the MIMO antenna is suitable for WLAN applications. The geometry of the proposed dual-band WLAN MIMO antenna has an overall size of 68 × 26 × 1.6 mm^3.

Keywords Multiple-input-multiple-output (MIMO) · Envelope correlation coefficient (ECC) · Triangular microstrip antenna (TMSA)

1 Introduction

The wireless communication medium is very complicated. The signal from the transmitting antenna over a wireless communication channel undergoes severe fluctuations by fading the signal level, path loss, co-channel interference, etc. The bandwidth

M. Arulaalan · K. Mahendran (✉) · P. Prabakaran · G. Manikannan
CK College of Engineering & Technology, Cuddalore, India
e-mail: srimahendrancs@gmail.com

M. Arulaalan
e-mail: arulaalan@gmail.com

P. Prabakaran
e-mail: 1984.praba@gmail.com

G. Manikannan
e-mail: kannan.gr18@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_35

limitation is a major challenge to a designer in designing a system with high quality and high spectral efficiency at low cost in single-input-single-output (SISO) system. The two factors, improved spectral efficiency and high quality, can be achieved by an MIMO system which is not possible in SISO system. To achieve spatial diversity and spatial multiplexing in a MIMO system, multiple antennas are required at the transmitting and receiving ends to improve the reliability and data rate [1]. MIMO antennas increase the data rate and range compared to SISO using the same radio transmits power.

MIMO can improve all forms of wireless communication system, but the design of MIMO system is more complicated than SISO. Antennas designed for MIMO systems require high decoupling between antenna elements, i.e., very low mutual coupling and low correlation coefficient. In a MIMO system, antenna is an integral part of the system.

The return loss, gain and radiation pattern are considered for the single antenna element, but in the design of MIMO antenna, mutual coupling and ECC are the important factors. Lower mutual coupling between antennas ensures that reliability and data rate of the system are improved. ECC gives the information of how radiation pattern of two antennas differs. The ECC value is zero if one antenna is horizontally polarized and the other one vertically polarized, and similarly, one antenna radiates toward the sky, and the other antenna radiates in ground surface. The ECC value given in Equation can be calculated by using S parameter [1–5] without considering radiation pattern.

$$\mathrm{ECC} = \frac{\left|S_{11}^{*}S_{12} + S_{21}^{*}S_{22}\right|^{2}}{\left|\left(1 - |S_{11}|^{2} - |S_{21}|^{2}\right)\left(1 - |S_{22}|^{2} - |S_{12}|^{2}\right)\right|}.$$

There are various methods proposed to reduce the mutual coupling. The simplest method of reducing the mutual coupling is increasing the separation between the antennas, but the drawback is the size of the antenna increases. The various methods used for reducing mutual coupling are to add single negative magnetic metamaterials between antenna elements [6–8] and adding stub in the ground plane [9–11], using slot and stub technique [12] and placing antenna elements orthogonally.

Microstrip antenna has its radiating patch with different shapes namely rectangular, triangular, circular, square, elliptical, annular ring, etc. The TMSA consists of a triangular-shaped radiating patch on the top of the dielectric material and the ground plane at the bottom of the dielectric material. The triangular radiating patch can be equilateral, right-angled triangle, etc.. Helszajn and James initially introduced triangular patch antenna structures. The TMSA structures have less radiation loss, and radiation pattern of equilateral triangular microstrip antenna (ETMSA) is relatively broad.

The TMSA has the advantage of being smaller and occupies half of the metalized area of the patch at a fixed frequency compared to rectangular, square or circular microstrip antenna. TMSA has the advantage of reduced mutual coupling between adjacent antenna elements in an array. Size compactness with high value of directivity can be achieved in ETMSA. Of the different patch shapes, triangular is the best suited for space and place problem. The partial Koch is added to enhance the performance of the ETMSA. The details of antenna design, simulated and measured results are discussed in the following section.

2 Antenna Design

2.1 Antenna Configuration

The geometry of the proposed dual-band WLAN MIMO antenna, with an overall size of only 68 × 26 × 1.6 mm^3, is shown in Fig. 1. It is designed on an FR4 substrate, with a thickness of 1.6 mm and relative permittivity of 4.4. The antenna consists of two triangular antenna elements with Koch fractal as shown in Fig. 1, with microstrip, fed through ports 1 and 2, respectively. The two triangular antenna elements are printed parallel to each other with Z-shaped stub on the ground plane to provide good isolation between the two antenna ports. The two antenna elements with Koch fractal have identical dimensions with the side length $a = 15.4$ mm. The two antennas are fed by a microstrip line with an impedance of 50 Ω. The ground plane of the antenna is printed on the other side of the FR4 substrate. To enhance isolation and return loss, a Z-shaped stub is added in between the ground plane of the antenna as shown in Fig. 1. The simulation of the MIMO antenna is carried out using ADS for optimization of return loss, gain, −10 dB impedance bandwidth, mutual coupling and radiation pattern. The optimized dimension of SISO for dual-band IEEE 802.11a application is extended for MIMO capability [13].

Fig. 1 Proposed layout of WLAN MIMO antenna with Z-shaped stub

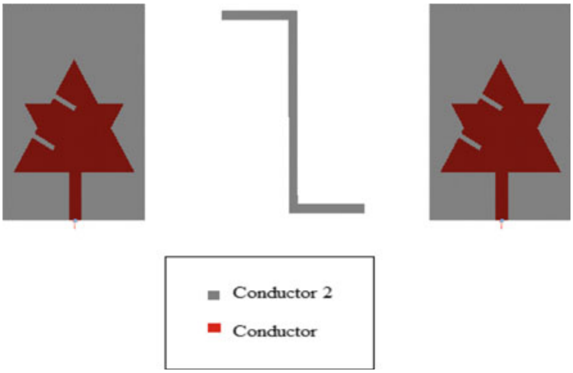
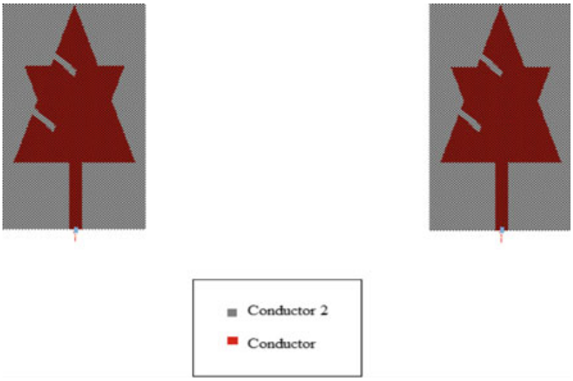


Fig. 2 Layout of WLAN MIMO antenna without stub



2.2 WLAN MIMO Antennas

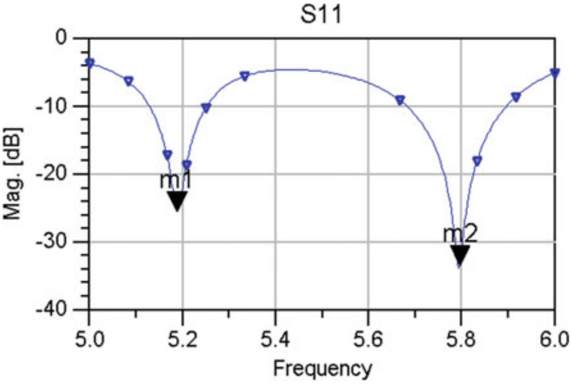
The dual-band antenna for IEEE 802.11a is extended for MIMO configuration as shown in Fig. 2. The performance of the MIMO antenna is improved by placing the antenna elements side by side separated by a small distance without stub.

3 Results and Discussion

3.1 Simulated Results

The two dual-band antenna elements are symmetric and have the same optimized parameters obtained for the dual-band antenna. When port 1 is excited, the MIMO antenna resonated at 5.191 GHz and 5.794 GHz with S_{11} value of −25.42 dB and −33.950 dB, respectively, as shown in Fig. 3. The simulated dual-band −10 dB

Fig. 3 Simulated S_{11} parameter when port 1 is excited without stub



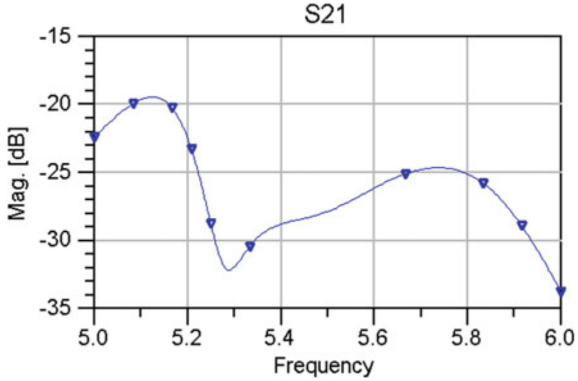


Fig. 4 Simulated isolation coefficient S_{21} parameter when port 1 is excited without stub

impedance bandwidth is 160 MHz (5.08 GHz–5.24 GHz) and 20 MHz (5.72–5.92 GHz) for IEEE 802.11a application. The simulated gains of the antenna for two resonant frequencies are 8.7 dB and 8.2 dB, respectively. The other important parameter in measurement of MIMO antennas is the isolation or mutual coupling between the input ports. When port 1 is excited, the isolation value S_{21} is −22.38 dB and −25.30 dB for the two resonant frequencies which are shown in Fig. 4. The isolation value is greater than −19 dB for two bands and for the entire −10 dB bandwidth.

The ECC plays an important role in evaluating the diversity characteristics of MIMO system. The simulated value of ECC is 0.6. The antenna has good diversity performance if ECC is <0.7. The simulated 2D radiation pattern for the MIMO antenna for frequencies 5.2 and 5.8 GHz is shown in Fig. 5 which is nearly omnidirectional.

3.2 WLAN MIMO Antenna with Stub

To enhance the isolation between the ports, Z-shaped stub is introduced in the ground plane. The significance of the stub is compared with the MIMO antenna without stub. There are many types of stub used for isolation, three stubs Y shaped stub, two long protruding ground stubs and short ground strip are used for UWB application to enhance isolation. For MIMO capability Z-shaped stub is added to the ground plane in between the ground plane of the two antennas to further enhance isolation. The layout of the antenna with Z-shaped stub is shown in Fig. 6. The return loss of the antenna improved for both the bands with the help of the stub. The fabricated WLAN MIMO antenna front and back view is shown in Figs. 6, 7, respectively.

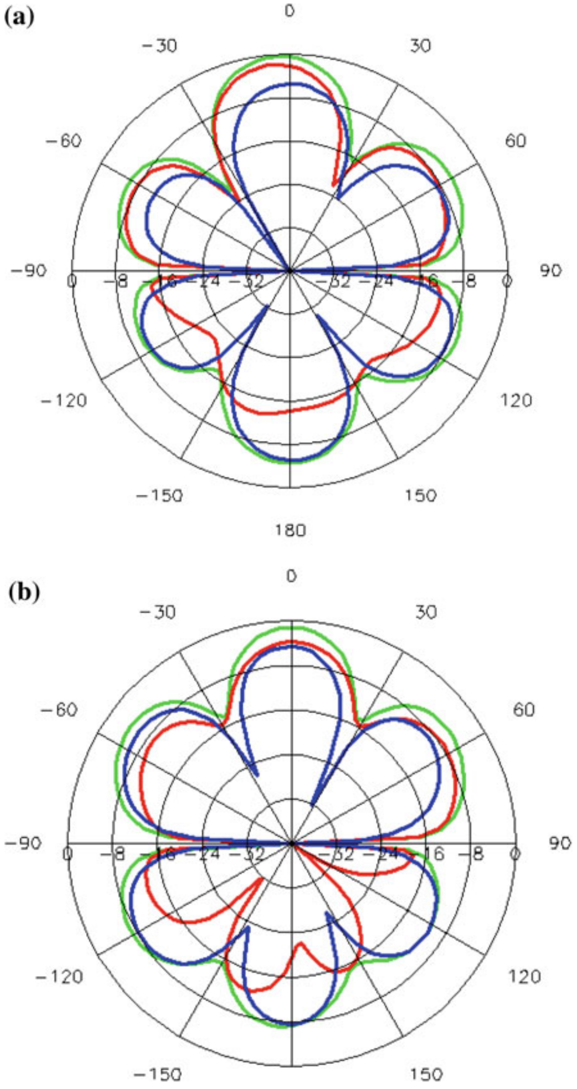


Fig. 5 2D radiation pattern **a** 5.2 GHz. **b** 5.8 GHz

3.3 Measured Results

The antenna measurements are carried by using vector network analyzer (VNA Agilent N9917A). The measured value of S_{11} is −34 and −30 dB at 5.19 and 5.8 GHz. The measured −10 dB bandwidth for the two bands is 120 MHz (5.11–5.23 GHz) and 200 MHz (5.72–5.92 GHz) as shown in Fig. 8.

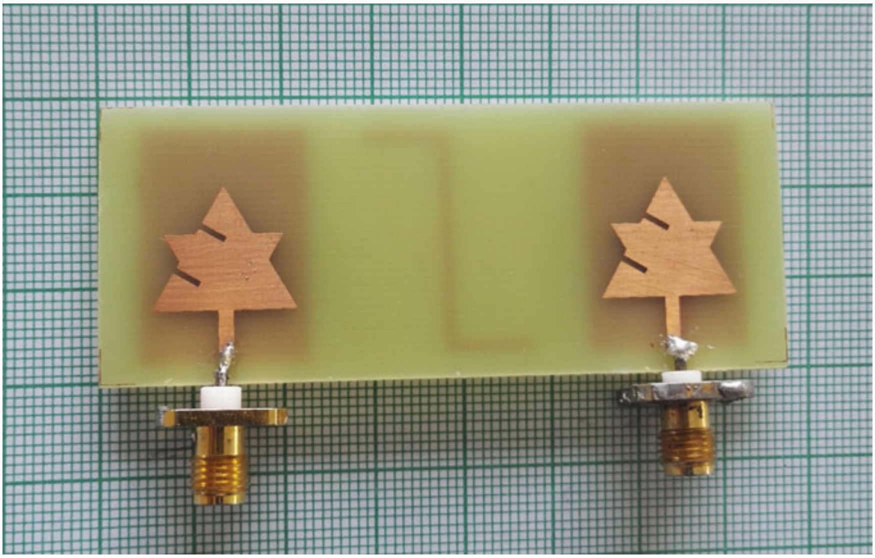


Fig. 6 Photograph of the fabricated WLAN MIMO antenna—front view

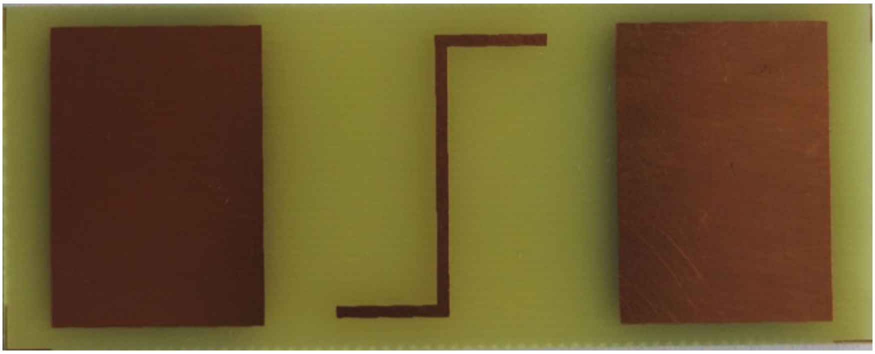


Fig. 7 Photograph of the fabricated WLAN MIMO antenna—back view

Using this Z-stub technique, the measured S_{21} is −34, and −32 dB is achieved for the two operating bands of 5.11–5.23 GHz and 5.72–5.92 GHz with center frequencies of 5.18 GHz and 5.81 GHz, respectively, refer to Fig. 9. The measured values with stub are −22.38 and −25 dB for the two bands as shown in Fig. 9. The increase in isolation value is due to the fact that current is absorbed by the Z-shaped stub, and thus, it enhances the port isolation between the antenna elements. The simulated gain of the antenna with stub is 8.23 and 8.10 dB. The value of ECC is 0.4 due to reduced mutual coupling. The 2D radiation pattern shown in Fig. 10 is nearly an omnidirectional pattern. Table 1 gives the comparison of WLAN MIMO antenna without using stub.

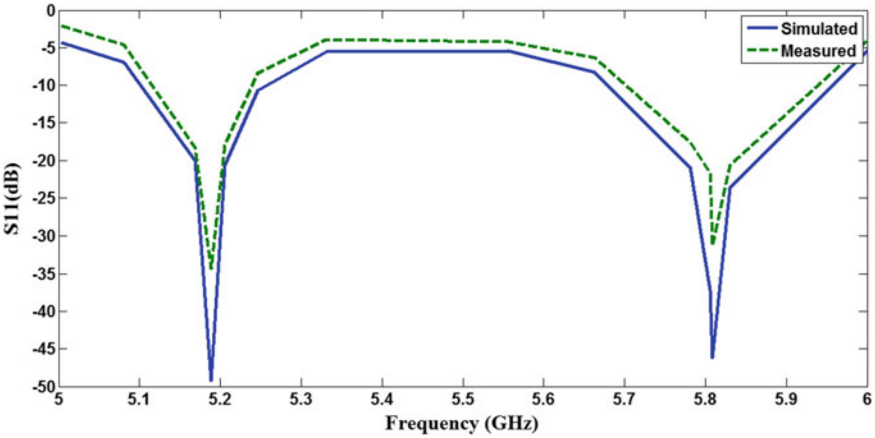


Fig. 8 Simulated and measured S_{11} parameter when port 1 is excited with stub

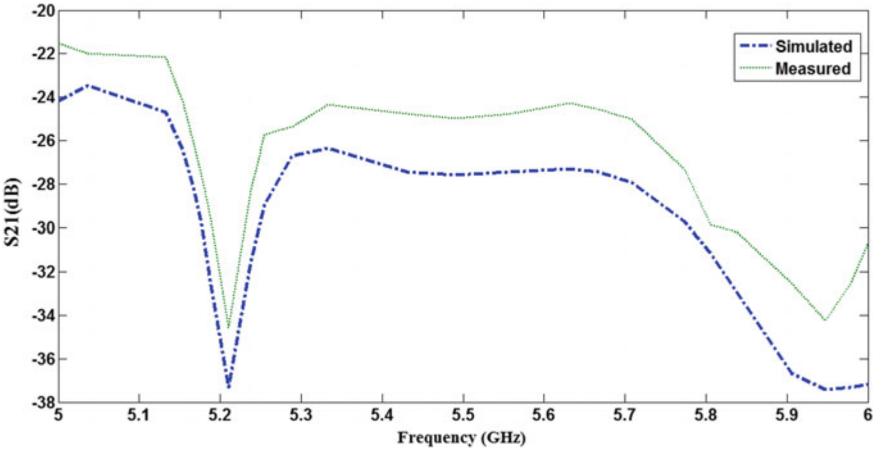


Fig. 9 Simulated and measured isolation coefficient S_{21} parameter when port 1 is excited with stub

3.4 Summary

A printed MIMO antenna for WLAN applications is designed and developed. The antenna consists of two identical fractal-based triangular microstrip antenna etched on the top of the substrate. The isolation between the antenna elements is enhanced by adding a Z-shaped stub on the ground plane. The proposed arrangement results in high isolation with values better than 20 dB. The factors such as return loss, gain and ECC indicate good performance for MIMO system.

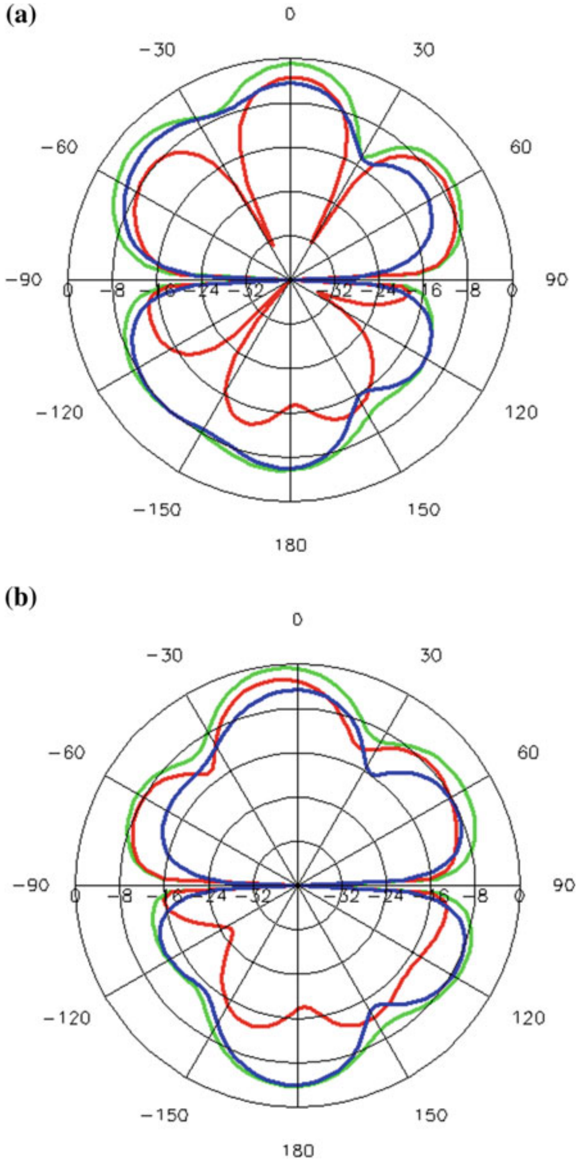
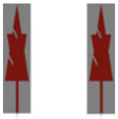
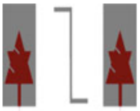


Fig. 10 Simulated 2D radiation pattern of the proposed WLAN MIMO antenna **a** 5.2 GHz. **b** 5.8 GHz

Table 1 Comparison of WLAN MIMO antenna with and without stub

Parameters	MIMO antenna without stub	MIMO antenna with stub (simulated)	MIMO antenna with stub (fabricated)
Layout			
−10 dB impedance bandwidth (MHz)	129 & 215	128 & 205	120 & 200
Resonant frequency (GHz)	5.191 & 5.794	5.188 & 5.807	5.18 & 5.81
S_{11} (dB)	−25.421 & −33.950	−48.352 & −46.879	−34 & −30
S_{21}(dB)	−27.52 & −29.48	−31.041 & −36.086	−22.38 & −25
ECC	0.6	0.4	–
Gain (dB)	8.44 & 8.66	8.23 & 8.10	–

References

1. Oestgates C, Clerckx B (2007) MIMO wireless communications: from real world propagation to space-time code design. Academic Press Ltd
2. Balanis CA, Ioannides PI (2007) Introduction to smart antennas. Morgan & Claypool Publishers
3. Blanch S, Romeu J, Corbella I (2003) Exact representation of antenna system diversity performance from input parameter description. Electron Lett 39(9):705–707
4. Manteghi M, Rahmat-Samii Y (2005) Multiport characteristics of a wide-band cavity backed annular patch antenna for Multipolarization operations. IEEE Trans Antennas Propag 53(1):466–474
5. Chae SH, Oh S-K, Park S-O (2007) Analysis of mutual coupling, correlations and TARC in WiBro MIMO array antenna. IEEE Antennas Wirel Propag Lett 6:122–125
6. Karaboikis M, Soras C, Tsachtsiris G, Makios V (2004) Compact dual-printed inverted-F antenna diversity systems for portable wireless devices. IEEE Antennas Wirel Propag Lett 3(1):9–14
7. Mavridis GA, Sahalos JN, Chryssomallis MT (2006) Spatial diversity two-branch antenna for wireless devices. Electron Lett 42(5):266–268
8. Shin YS, Park SO (2007) Spatial diversity antenna for WLAN application. Microw Opt Technol Lett 49(6):1290–1294
9. Wu TY, Fang ST, Wong KL (2002) Printed diversity monopole antenna for WLAN operation. Electron Lett 38(25):1625–1626
10. Chi G, Binhong L, Qi D (2005) Dual-band printed diversity antenna for 2.4/5.2-GHz WLAN application. Microw Opt Technol Lett 45(6):561–563
11. Wang X, Du Z, Gong K (2008) A compact wideband planar diversity antenna covering UMTS and 2.4 GHz WLAN bands. IEEE Antennas Wirel Propag Lett 7:588–591

12. Ding Y, Du Z, Gong K Feng Z (2007) A novel dual-band printed diversity antenna for mobile terminals. IEEE Trans Antennas Propag 55(7):2088–2096
13. Arulaalan M, Nithyanandan L (2017) Development of triangular shaped dual band 802.11a WLAN application. Asian J Inf Technol 1(16):212–217

A Hollow Core Bragg Fiber with Multilayered Random Defect for Refractive Index Sensing

K. Ben Franklin, R. Kumar and C. Nayak

Abstract In this paper, we present the theoretical analysis of Bragg waveguide containing a random multilayer defect. Transmittance spectrum of the proposed multilayered cylindrical waveguide is obtained by employing transfer-matrix method. Presence of random defect structure shows multiple defect peaks in the photonic band gap of a defect-free Bragg structure. The probability of occurrence of defect peaks around 660–690 nm is found to be very good, and these peaks may be chosen as a sensing element. Result shows that the transmittance of the defect peak has a good agreement with the change in the refractive index of the core.

Keywords Bragg fiber · Photonic band gap · Gaussian distribution · Defect peak · Transfer-matrix method

1 Introduction

Currently, there is a great interest in the fabrication of Bragg fiber waveguides due to its application in high-power laser systems, sensing, telecommunication, medicine, surgery, etc. The idea of Bragg fiber was first demonstrated by Yeh and Yariv in 1976 [1]. Thereafter, feasibility study of cylindrical Bragg fibers was theoretically as well as experimentally presented for different optoelectronics applications. Such studies show that, the hollow core Bragg fiber waveguide structure can be a suitable candidate for chemical gas sensors [2], strain sensors [3], biosensors [4, 5], narrowband transmission filter [6], optical de-multiplexer [7], etc.

Bragg fiber is a multilayered waveguide which consists of a low-index core and a periodic arrangement of alternating high and low refractive index [8]. The electromagnetic wave (EM wave) propagation in the core of a Bragg fiber is done through Bragg reflection produced by the alternating arrangement of high and low refractive index, whereas the conventional fiber uses total internal reflection for propagation

K. B. Franklin · R. Kumar · C. Nayak (✉)
Department of Electronics and Communication Engineering, SRMIST, Kattankulathur, Chennai 603203, India
e-mail: 83chittaranjan@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_36

through the core. Optical properties of the Bragg fiber are characterized by several parameters such as core size, refractive indices, and thickness of the cladding layers, and hence offer a wide choice to tailor their propagation characteristics. Recently, a design of Bragg fiber was reported, in which a liquid core Bragg waveguide showed a photonic band gap in the transmittance spectrum, due to its alternate cladding layers [9]. This photonic band gap is nothing but a band of wavelengths that are not allowed to propagate through the waveguide. This band gap can be used as a sensing element because the position of band gap and transmitted intensity depends on the core refractive index. Further studies were done by introducing a defect layer in the alternate cladding arrangement, and a defect mode (narrow transmission band) appeared in the band gap region [10]. Analysis shows that the transmittance of this defect mode is more sensitive to change in core refractive index than the transmittance of band gap. Usually, defects (randomness) in photonic structure are regarded as undesirable features that spoil optical quality and performances. However, they can also be viewed as an enriching factor since, when controlled, they can be used to build up good waveguides. In disordered structures, the wavelength region corresponding to photonic band gap is filled with localized states (such as Anderson localization) [11], and for such states, the magnitude of the electric field is very high. Such localized states act as a Fabry–Perot resonator and lead to increasing transmission through the structure.

In this work, we propose a hollow core photonic structure, where the cladding is made by embedding multilayered random defect in the alternating cladding region. Multilayer defects (randomness) are introduced in the cladding region by making use of the Gaussian distribution function. The transmittance spectrum is obtained by employing the transfer-matrix method (TMM) which was developed by Kaliteevski et al. [12].

2 Theoretical Model

As can be seen in Fig. 1, the proposed Bragg waveguide consists of a hollow core and the core is assumed to be filled with a liquid under observation having refractive index, n_C. The cladding region of the waveguide is mainly divided into three parts, i.e., a random cylindrical structure sandwiched between two hollow cylindrical Bragg dielectric structures. The first cylindrical Bragg dielectric structure, around the core region, has N layers of unit cell. The unit cell consists of two different materials A, higher refractive index layer (n_H) with thickness (d_H) and B, lower refractive index layer (n_L) with thickness (d_L). Whereas, the second cylindrical Bragg dielectric structure is similar to that of the first one, but it has M layers of unit cell. Layer width of the sandwiched random cylindrical structure is assumed to be Gaussian distributed with O number of layers of alternating high refractive index layer (nd_H) and low refractive index layer (nd_L).

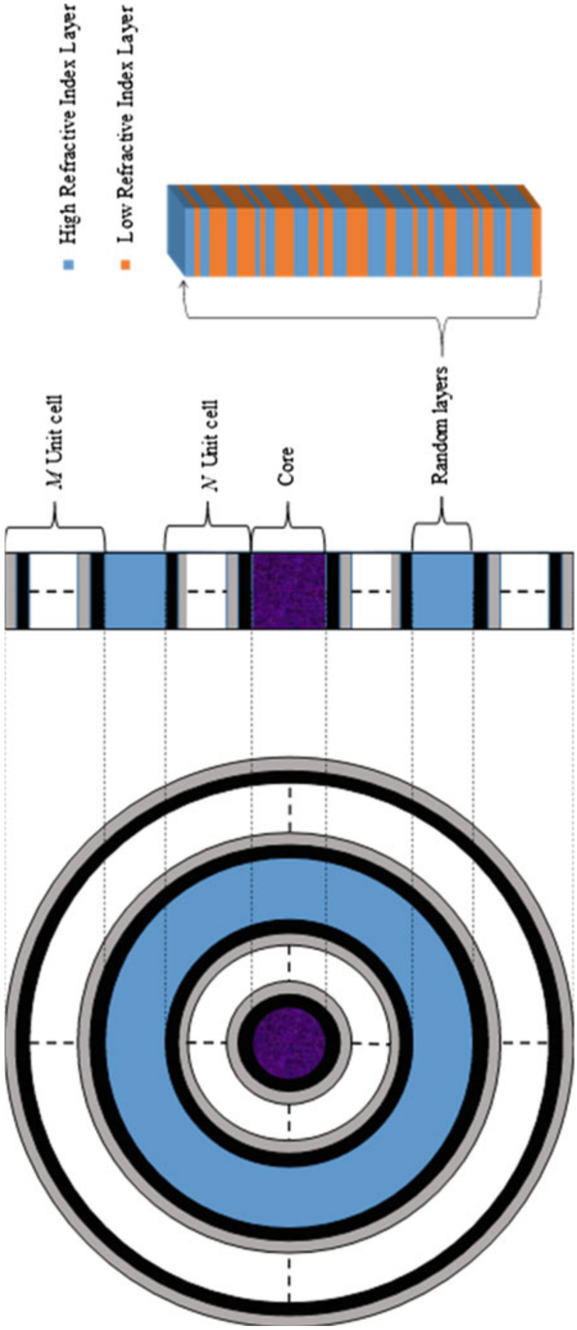


Fig. 1 Cross-sectional schematic representation of the photonic band gap waveguide having a random multilayer defect

The performance analysis of such structure can be done by employing many numerical techniques. But, one of the most popular techniques is the transfer-matrix method (TMM) [13].

Using the Abeles theory, the transfer matrix for the first high refractive index layer of the first cylindrical Bragg dielectric structure with initial position y_0 (inner radius) to other point y_1 (outer radius) is given by

$$\begin{bmatrix} V(y_1) \\ U(y_1) \end{bmatrix} = A \begin{bmatrix} V(y_0) \\ U(y_0) \end{bmatrix} \tag{1}$$

where A is the transfer matrix of the dielectric cylinder and is given by

$$A = \begin{bmatrix} a11 & a12 \\ a21 & a22 \end{bmatrix} \tag{2}$$

The individual matrix elements of the same are given by

$$a11 = \frac{\pi}{2} k y_0 \left[\acute{Y}_m(ky_0) J_m(ky_1) - \acute{J}_m(ky_0) Y_m(ky_1) \right], \tag{3a}$$

$$a21 = j\frac{\pi}{2} k y_0 P \left[\acute{Y}_m(ky_0) J_m(ky_1) - \acute{J}_m(ky_0) \acute{Y}_m(ky_1) \right], \tag{3b}$$

$$a22 = \frac{\pi}{2} k y_0 \left[J_m(ky_0) \acute{Y}_m(ky_1) - Y_m(ky_0) \acute{J}_m(ky_1) \right], \tag{3c}$$

$$a12 = -j\frac{\pi}{2} \frac{k y_0}{P} \left[J_m(ky_0) Y_m(ky_1) - Y_m(ky_0) J_m(ky_1) \right]. \tag{3d}$$

where J_m is a Bessel function, Y_m is a Neumann function, $k = \left(\frac{\omega}{c}\right)n$ is the wave vector in a medium, c is the speed of light in free space, $P = \sqrt{\frac{\varepsilon}{\mu}}$ is the characteristic impedance, and n is the refractive index of that medium.

The final transfer matrix of the proposed Bragg structure is given by

$$\begin{bmatrix} V(y_f) \\ U(y_f) \end{bmatrix} = \left(AB^N\right)(D_1 \ldots\ldots D_O)\left(AB^M\right) \begin{bmatrix} V(y_0) \\ U(y_0) \end{bmatrix} \tag{4}$$

B, the second element of the unit cell, represents the transfer matrix of the lower refractive index material. D_{xx} represents the transfer matrix of Gaussian distributed random layers, where $xx = 1, 2, \ldots\ldots.., O-1,\ O$.

$$\begin{bmatrix} V(y_f) \\ U(y_f) \end{bmatrix} = (F) \begin{bmatrix} V(y_0) \\ U(y_0) \end{bmatrix} \tag{5}$$

The coefficient of reflection for the proposed waveguide can be calculated with the help of the final transfer matrix, F.

$$r_d = \frac{\left(\acute{F}_{21} - JP_0 C^{(2)}_{m0} \acute{F}_{11}\right) + JP_f C^{(2)}_{mf}\left(\acute{F}_{22} - JP_0 C^{(2)}_{m0} \acute{F}_{12}\right)}{\left(-\acute{F}_{21} + JP_0 C^{(1)}_{m0} \acute{F}_{11}\right) + JP_f C^{(2)}_{mf}\left(-\acute{F}_{22} + JP_0 C^{(2)}_{m0} \acute{F}_{12}\right)} \tag{6}$$

$\acute{F}_{11}$,$\acute{F}_{12}$,$\acute{F}_{21}$,$\acute{F}_{22}$ are the matrix elements of the inverse final transfer matrix $\acute{F}$ and

$$C^{(1,2)}_{mx} = \frac{H_m^{\left(1',2\right)}(k_1 y_1)}{H_m^{(1,2)}(k_1 y_1)}, \quad x = 0, f \tag{7}$$

where $H_m^{(1)}$ and $H_m^{(2)}$ are the Hankel function of the first and second kind. Using Eq. (6), the reflectance is calculated as $R = |r_d|^2$, and the value of transmittance, $T = (1 - R)$.

3 Results and Discussions

Let us now present the transmittance spectra for the proposed waveguide in 600–725 nm region. We shall focus on the case of 0th azimuthal mode. Figure 2 shows the calculated transmittance spectra for ten possible 32-layer Gaussian distributed random annular defects (i.e, $O = 32$), whose thickness values are calculated for mean = 250 nm and sigma = 60 nm and are listed in Table 1. Here, we have chosen, $N = M = 32$, $n_H = 1.8$, $n_L = 1.5$, $d_H = 100\,\text{nm}$, $d_L = 100\,\text{nm}$, $\text{nd}_H = 3.2$, and $\text{nd}_L = 1.5$.

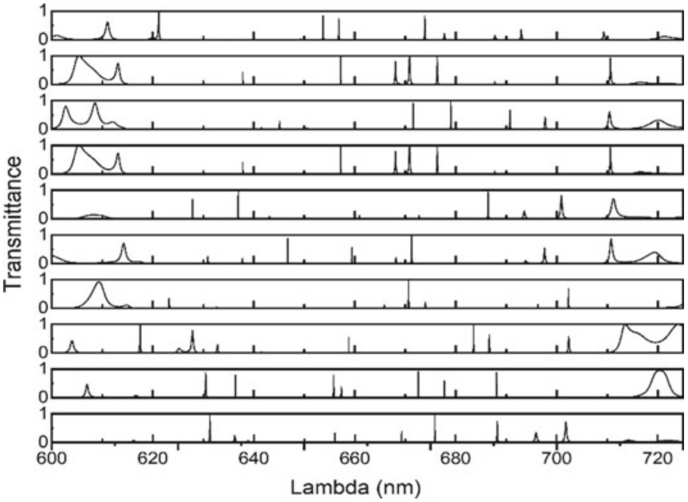


Fig. 2 Transmittance spectrum for 10 different permutations with random defects

Table 1 Thickness of random multilayer (32) defect for 10 different permutations

S. No.	Defect layers thickness (nm)										
	1	2	3	4	5	6	7	8	9	10	11
1	223	269	208	217	254	293	175	321	214	275	291
2	327	240	267	217	261	268	250	263	298	193	258
3	218	177	324	225	254	272	254	213	231	245	309
4	351	137	361	266	300	166	220	236	271	166	273
5	277	172	239	225	269	270	270	231	220	220	292
6	282	234	338	325	258	235	307	192	283	216	229
7	185	204	733	336	269	204	332	147	243	235	269
8	245	134	223	142	300	196	256	217	268	213	279
9	185	201	733	336	269	204	332	147	243	235	269
10	232	217	231	184	220	239	252	246	286	256	358
S. No.	Defect layers thickness (nm)										
	12	13	14	15	16	17	18	19	20	21	22
1	302	293	250	243	225	260	264	235	255	356	249
2	170	251	327	287	249	236	271	292	250	314	217
3	215	281	262	240	207	238	246	191	257	217	246
4	189	253	282	266	304	300	217	262	202	183	296
5	157	239	263	217	273	246	203	258	236	295	214
6	216	278	211	196	277	228	268	232	263	121	273
7	268	198	248	240	287	315	316	198	254	177	183
8	294	352	238	121	199	331	185	307	257	336	132

(continued)

Table 1 (continued)

S. No.	Defect layers thickness (nm)										
	12	13	14	15	16	17	18	19	20	21	22
9	268	198	248	240	287	315	316	198	254	177	183
10	268	358	206	281	234	286	285	118	170	163	274

S. No.	Defect layers thickness (nm)									
	23	24	25	26	27	28	29	30	31	32
1	278	231	228	236	272	217	175	252	232	261
2	170	220	242	235	216	303	185	230	211	231
3	263	213	238	264	176	291	346	288	237	267
4	250	247	295	279	267	312	296	261	215	217
5	253	157	230	222	204	282	213	277	298	242
6	342	301	295	238	259	262	254	208	232	241
7	249	341	203	272	236	317	184	251	283	316
8	238	177	424	299	332	186	221	233	315	233
9	249	341	203	272	236	317	184	251	283	316
10	338	230	298	282	186	273	204	340	248	348

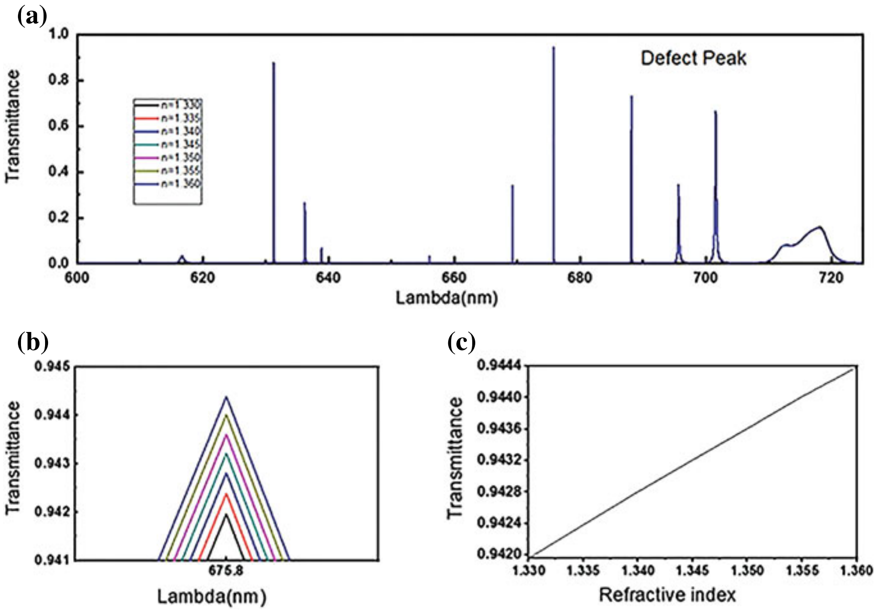


Fig. 3 Transmittance spectra as function of n_C **a** between 600−725 nm **b** around 675.8 nm **c** relation between n_C and transmittance at 675.8 nm

One can see from Fig. 2, that a large number of defect peaks, or so-called localization of light, appear within the photonic band gap of a defect-free structure. The localization of light is obvious and it is caused due to the presence of random layers. Moreover, the probability of occurrence and transmittance of defect peak around the region 660−690 nm is found to be very high. Therefore, these defect peaks can be employed as a sensing element.

To find the effect of change in core refractive index, we examine the transmittance spectra of the first defective structure in Table 1 and is depicted in Fig. 3. It is interesting to see from Fig. 3a that, for different core refractive index, a narrow defect peak having different transmittance appear around 675.85 nm.The defect peak intensity increases with increase in the core refractive index, shown in Fig. 3b. The change in core refractive index and the transmittance of defect peak have a linear relation, Fig. 3c. Due to good agreement between the transmittance and the core refractive index, the proposed waveguide can be a good candidature for sensing application.

4 Conclusion

Looking for alternatives to set up a fiber sensing device, we have investigated in this work the transmission characteristic for a hollow core Bragg fiber with multilayered defects. The obtained result is very interesting; therefore, this proposal may be a good material for sensing industry.

References

1. Yeh P, Yariv A (1976) Bragg reflection waveguides. Opt Commun 19:427–430
2. Shi L, Zhang W, Jin J, Huang YD, Peng JD (2010) Hollow core Bragg fiber and its application in trace gas sensing. In: Communications and photonics conference and exhibition (ACP), IEEE Xplore, Asia, pp 477–478
3. Hang Q, Brastaviceanu T, Bergeron F, Olesik J, Pavlov I, Ishigure T, Skorobogatiy M (2013) Photonic bandgap Bragg fiber sensors for bending/displacement detection. Appl Opt 52:6344–6349
4. Rowland KJ, Afshar VS, Stolyarov A, Fink Y, Monro TM (2011) Bragg waveguides with low-index liquid cores. Opt Express 20:48–62
5. Hang Q, Skorobogatiy M (2012) Resonant bio-and chemical sensors using low refractive-index-contrast liquid-core Bragg fibers. Sens Actuators B 161:261–268
6. Chen MS, Wu CJ, Yang TJ (2012) Narrowband reflection and transmission filter in an annular defective photonic crystal containing an ultra-thin metallic film. Opt Commun 285:3143–3149
7. Sharma G, Kumar S, Prasad S, Singh V (2015) Theoretical modelling of one dimensional photonic crystal based optical DE multiplexer. J Mod Opt 995–999
8. Prajapati Y, Saini JP, Chauhan DS, Singh V (2014) Effect of plasma on modal dispersion characteristic of elliptical Bragg waveguide. Opt-Electron Rev 22(1):13–20
9. Schmidt H, Hawkins A (2008) Optofluidic waveguides: II. Fabrication and structures. Microfluid Nanofluid 4:17–32
10. Chourasia RK, Prasad S, Singh V (2017) Opto-Electron Rev 25:215–221
11. Anderson PW (1958) Absence of diffusion in certain random lattices. Phys Rev 109:1492
12. Kaliteevski MA, Abram RA, Nikolaev VV, Sokolovski GS (1999) Bragg reflectors for cylindrical waves. J Mod Opt 46(5):875–890
13. Born M, Wolf E (1999) Principles of optics. Cambridge, London

Generation of Multiple Key Based on Monitoring the User Behavior

S. Palaniappan, Steward Kirubakaran, V. Parthipan and S. Rinesh

Abstract Cloud computing is the recent technology used to share and store the computer resources rather than having resources in local server to maintain the application. Though cloud is used for a large amount of storage, there is no security in cloud. In general, all the groups have data owners and data members each should have user name, key, and group key. If a user shifts from one group to another, they can easily access the information from another group. It leads to a security problem. In order to increase security and confidentiality, author generates the new group key via Email using Diffie-Hellman algorithm. In case of a new user is added or an existing user leaves themselves from the group. The data members have to get permission from the data owners in case of any data updation. If the user misbehaves, i.e., (DDOS) attack, data owner or cloud terminates the user from the group. The updated key is sent to the users through Email. This mechanism significantly improves security in cloud computing.

Keywords Cloud computing · Group key · DDOS attack

1 Introduction

Cloud computing has a large amount of storage such as (Drop Box, Google Drive) [1–3] and sharing resources. But there is no security in the cloud is enforced. The main goal of the author is to improve security in cloud. It is all about generating

S. Palaniappan (✉) · S. Kirubakaran · V. Parthipan · S. Rinesh
Department of Computer Science and Engineering, KCG College of Technology, Karapakkam, Chennai, India
e-mail: s.palani.in@gmail.com

S. Kirubakaran
e-mail: stewartkirubakaran@gmail.com

V. Parthipan
e-mail: parthipansp@gmail.com

S. Rinesh
e-mail: rin.iimmba@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_37

dynamic and flexible group keys based on user behavior. In general, each group has data owners and data members. For instance, an institute might have several departments. Each department has a separate group key and users have their user key for login purpose. Each data members have to enter user name, key, and group key for login. Due to modification from different users, different blocks are signed by different users. For security reasons, when a user leaves the group or misbehaves, this user must be revoked from the group [4]. This will provide confidentiality and reliability. As a result, this revoked user should no longer be able to access and modify shared data, and the signature generated by this revoked user is no longer valid to the group [5]. In this case, new group key is sent to the corresponding data members via Email. This can be done once the data members shift from the group or a new data member is added to the group obviously this will improve security of the cloud. On each updation, data members need to get approved from the data owners. In case of any mischievous activities (DDOS) attack, the data owners or cloud itself terminates that particular data members from that group and the updated key is sent to the corresponding group through Email.

2 Methodology

In this article, the author categories the improvement of security into three ways.

(1) **Automatic Key Generation**—Data members have their user name, key, group key for login purpose. If a new member is added to the group or an existing member leaves from the group, the updated group key is sent automatically through Email. This will improve the privacy of the data.

For Example: Consider a department, and it consists of various members. If a member of that department shifts from one group to another, the group key will be automatically changed and sent to the department through Email for confidentiality of data.

(2) **Mischievous Activity**—In general, each group has data owners and data members. Data owners have authority to update the data to the cloud server for accessing data. Data owners appoint the data member for data utility and data updation. In the case of any mischievous activity, a data owner has their privilege to terminate the data members from that group and generates the new group key. Obviously, this will improve the reliability and confidentiality.

For Example: If a data member had a privilege only to access the data, in case if a user tries to attempt for data updation, it will be considered as mischievous activity, then data owners had an authority to terminate that particular data member from that group and group key is updated automatically.

(3) **DDOS Attack**—If a data members attempt to upload the same file for N number of times, then data owner or cloud itself terminates the data members and updated key is sent to that corresponding group through Email.

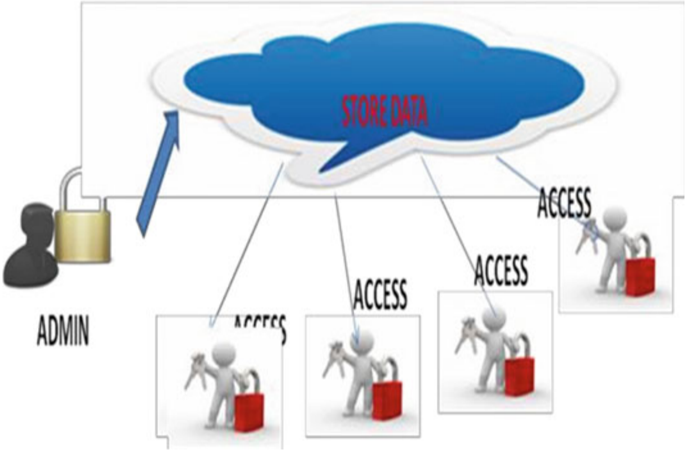


Fig. 1 Dynamic key generation architecture

> **For Example**: If a data members attempt to login to for more than particular number of times, the data owners automatically terminate the data members from the group and group key is updated.

These three ways contribute security and privacy to the cloud server. And also increase the efficiency and integrity of data. User termination will improve the high efficiency because the terminated user is no longer to the group; hence, accessing data from the group is impossible. Termination can be done by data owners of the group. Once the user is terminated, resigning is impossible (Fig. 1).

However, the above architecture is mainly focused on dynamic and flexible group key generation. Security is the big challenge in cloud computing server other than networking and communication. This article updates the group key in case of any activities in the group.

3 Implementation

A user interface is implemented using Java technology or C#. Database is created using My SQL. Here, drop box is used for cloud for sharing resource. Diffie-Hellman algorithm is used for generating a new key in case of any updation takes place among the group for security purpose. This will make the group secured and efficient.

4 Diffie-Hellman Algorithm for Dynamic Key Generation

The Diffie-Hellman key agreement protocol (1976) was the first practical method for establishing a shared secret over an unsecured communication channel [6]. The main goal of this algorithm is to generate the new group key in case of any changes in the group. It shares the secret key among the groups. Every piece of information that shares among the groups is noticed by the data owners of the group. This algorithm is used to share the random secret key in case of any changes in the group. Diffie-Hellman key exchange shares the key randomly for security purpose among the groups. Although RSA algorithm is the first algorithm used to share the new key. Secret key will be generated if an existing user shifts or a new user is added to the group and also if a user misbehaves, the group key will be updated using the above mechanism. By this way, data in the group will be secured. Diffie-Hellman key exchange algorithm solves the following problem. For instance, john and mark are belong to same group; they can share and access the data of same group. If a new user wants to access, the information from john and mark is highly impossible, because Diffie-Hellman generates the group key. If a user wants to access, the data group key is mandatory. Even if john and mark went under any mischievous activity, the group key will be updated by using above algorithm and shared in cloud server which will share the current group key for the corresponding data members. Even when john and mark share the group key, they may use a password-authenticate key agreement (pk) form of Diffie-Hellman to prevent man in the middle attack [6] (Fig. 2).

5 Secure and Efficient User Termination

In this article, we argued about the user termination; this will make data more secure and efficient. The cloud can resign blocks that were previously signed by the revoked user with a resigning key, while an existing user does not have to download those blocks, recompute signatures on those blocks, and upload new signature to the cloud [4]. User termination is secured because an existing user can access the data stored in the group. Once the user is revoked from the group, he/she is no longer in the user list. The resigning performed by the cloud improves the efficiency of user revocation and saves communication and computation resources for existing users [7].

6 Module Description

To perform effective resource allocation and to achieve security in cloud, five different modules are used. These modules are discussed below.

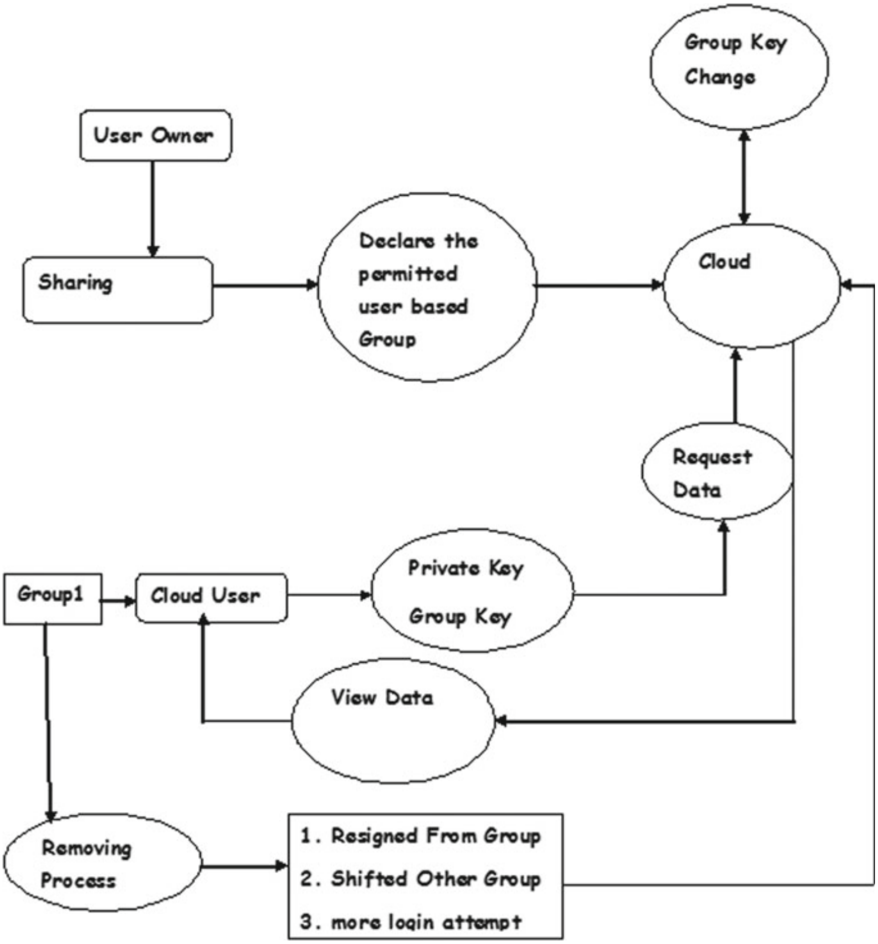


Fig. 2 Data flow diagram

Network Construction—In this module, dynamic network is created. Nodes are interconnected with particular group, used to share the information among them. The network should be controlled and handled for successful transmission of data. Network is constructed using interconnection of various nodes.

Server—All the group information and details are maintained by the server. It will distribute the data to the client of a group. In case of any data issue, server is responsible. It will instruct the data owners to change the group key in case of any changes in the group and the updated key is sent to the data members through Email.

User Status—All the user status is to be maintained here. User can shift from one group to another, and also they can participate in more than one group. The information can be shared depending upon user status. For authentication purpose, all the information about the user is to be maintained here.

Group Key Generation—In this module, group key as well as individual key is created and then shared among the group via Email. Group key is updated in case of any changes in the group. This can be done whenever any changes take place in the group.
Data Access—The user can able to access the information of any user of same group that can be done using group key and user key. Accessing the information of a user of a different group is impossible. Information of a user of different groups can be accessed only with the help of that particular group key.

7 Advantages

This paper has been framed to improve security of the cloud server. The paper has the following advantage.

- It improves high security
- It provides integrity and confidentiality
- Dynamic and flexible key generation.

8 Conclusion

In this article, we have discussed and implemented a new mechanism for improving security and efficiency of data. It is all about maintaining secured data among the groups. Each group has separate group key for login purpose. If a user in the group leaves or shifts to another group, the updation of group key will take place. Since the user from another group can not access the data. If a new user is added to the group, the key will be updated and sent to the corresponding data members of that group. Group key will be changed in case of any mischievous activity in the group and that particular user will be terminated from that group. Generation of new group key takes place in case of any (DDOS) attack in the group. These three ways of group key generation help us to increase the security. This will improve the confidentiality and efficiency of data. And also this will increase security in the cloud server. In further, any other research will produce more security in the cloud.

References

1. Drop Box (2007) On the impact of virtualization on drop box like cloud file storage/synchronization services
2. Mozy (2007) A study on cloud backup technology and its development
3. Bitcasa (2011) Proof of ownership in duplicated cloud storage with mobile device efficiency

4. Wang B, Li B, Li H (2013) Panda: public auditing for shared data with efficient user revocation in the cloud. IEEE Trans Serv Comput 8(1):92–106
5. Wang B, Li B, Li, H (2012) Knox: privacy-preserving auditing for shared data with large groups in the cloud. In: Proceedings of 10th international conference on applied cryptography and network security (ACNS'12), pp 507–525
6. https://en.wikipedia.org/org/wiki/Diffie%E2%80%93Hellman key exchange Password-authenticated_key_agreement
7. https://www.cs.utexas.edu/~byoung/cs361/lecture52.pdf
8. Memopal (2007) Memopal
9. Gantz JF, et al. (2006) The expanding digital universe: a forecast worldwide information growth through 2010
10. Bowers AJ, Oprea A (2009) Proofs of retrievability: theory and implementation. In: Proceedings of the first ACM cloud computing security workshop (CCSW 2009), USA
11. Wang Q, Wang C, Li J, Ren K, Lou W (2009) Proofs of retrievability via hardness amplification. Saint-Malo, France, pp 355–370
12. Saikumar K, Rais MdZ, Palaniappan S (2015) Smart id card with NFC tags using elliptical curve digital certificate authentication. Int J Appl Eng Res 10(4):3077–3079
13. Yuan J, Yu S, Proofs of retrievability with public verifiability and constant communication cost in cloud. In: Proceedings of international workshop on security in cloud computing, Hangzhou, China
14. Shi E, Stefanov E, Papamanthou C (2013) Practical dynamic proofs of retrievability. In: Proceedings of ACM CCS, Berlin, Germany
15. eXo Cloud IDE (2002) https://codenvy.com/
16. Albert MJ, Yovan FA, Chintalapudi M, Balaji R, Vigneshwaran R (2015) Fault-open minded resource allocation rescheduling algorithm and expense minimization for cloud systems. Glob J Pure Appl Math 11(6):4111–4117
17. Erway C, Kupcu A, Papamanthou C, Dynamic provable data possession. In: Proceedings of ACM CCS, Illinois, pp 213–222
18. Kumar B, Palaniappan, Jashwanthreddy, An hybrid of RSA token and iterated hash algorithm for secured data transfer. Int J Pharm Technol 19417–19423. ISSN: 0975-766X

Towards Convolution Neural Networks (CNNs): A Brief Overview of AI and Deep Learning

Preetjot Kaur and Roopali Garg

Abstract Today's era is of cutting edge of innovations as well as technologies. One of the major problems, researchers often face is an issue looking for an appropriate research area. For instance, there are numerous fields these days on which research is being carried out and to pick one out of those topics is itself a challenging task. The major objective of this review paper is to embark upon Artificial Intelligence (AI) that prompted the emergence of deep learning (DL) and further to convolution neural networks (CNNs). Limitations of CNNs that led to the development of Capsule Neural Networks (CapsNets) have been included. The significant goal of this review paper is to discuss the latest trends in which research is on-going and is still in progress. Also, the key challenges faced by past researchers are highlighted.

Keywords Artificial intelligence (AI) · Current research trends · Convolution neural networks (CNNs) · Capsule Neural Networks (CapsNet) · Deep learning techniques

1 Introduction

There are many trends in the field of computer science engineering. However, out of these, only a few patterns are ruling this century and stand out as truly newsworthy. Since the acquaintance of Artificial Intelligence (AI) with the market, it has become a reason for speedy changes in the technology and business worlds. AI is the ability of machines to do tasks in such a way as humans do in any situation. The growing trends of computer science community are of special importance as they provide future researchers with all the tools and equipments that they need to make progress into this field [1]. It is very necessary to build connection with new technologies, as it

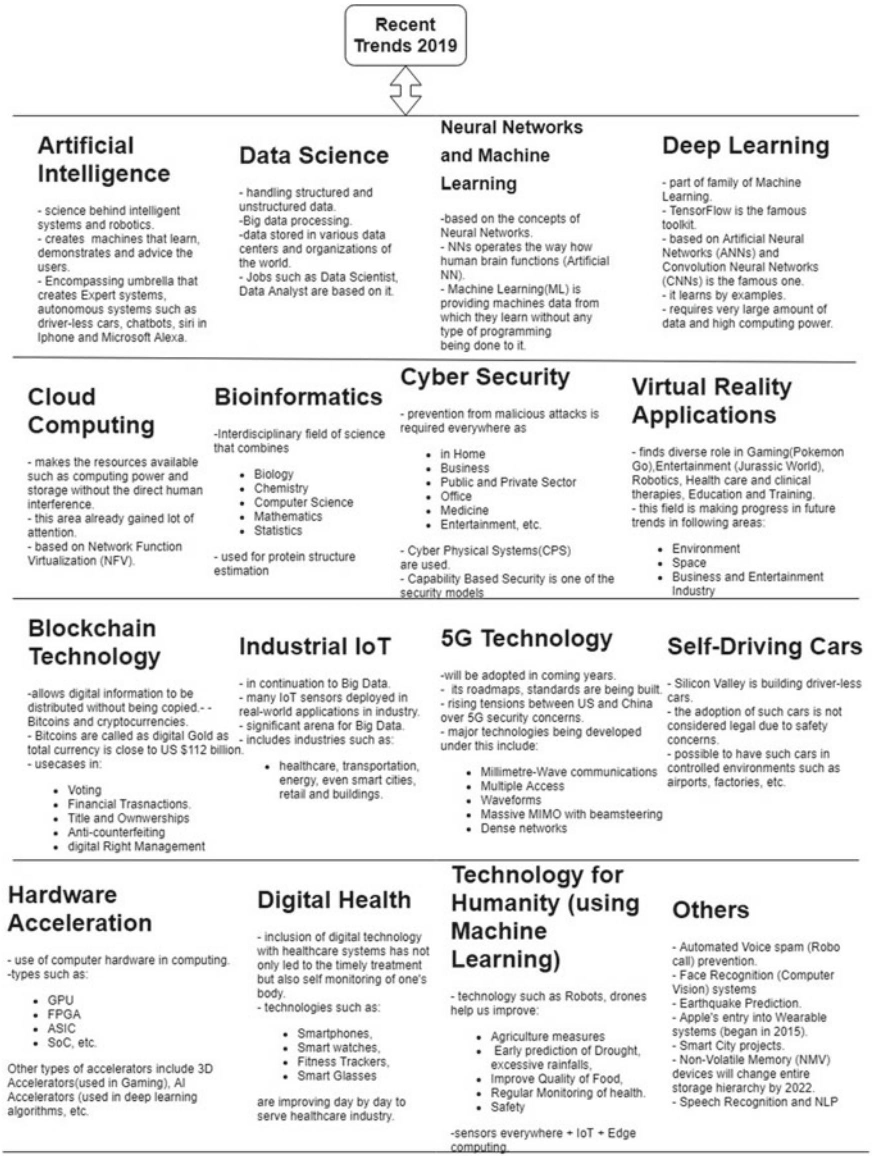
P. Kaur (✉)
PhD Research Scholar, UIET, Panjab University, Chandigarh 160014, India
e-mail: preetjotkaur20@gmail.com

R. Garg
Associate Professor, UIET, Panjab University, Chandigarh 160014, India
e-mail: roopali.garg@pu.ac.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_38

leads to the discovery of an abundance of future developments. Today's era is of the cutting edge of issues in innovations and technology and wide range of opportunities are available [2] as shown in Fig. 1.

Multidisciplinary and interdisciplinary research is trending these days. For instance, detecting facial expressions is a major concern among researchers in AI



Recent Trends 2019

Artificial Intelligence

- science behind intelligent systems and robotics.
- creates machines that learn, demonstrates and advice the users.
- Encompassing umbrella that creates Expert systems, autonomous systems such as driver-less cars, chatbots, siri in Iphone and Microsoft Alexa.

Data Science

- handling structured and unstructured data.
-Big data processing.
-data stored in various data centers and organizations of the world.
- Jobs such as Data Scientist, Data Analyst are based on it.

Neural Networks and Machine Learning

-based on the concepts of Neural Networks.
- NNs operates the way how human brain functions (Artificial NN).
- Machine Learning(ML) is providing machines data from which they learn without any type of programming being done to it.

Deep Learning

- part of family of Machine Learning.
- TensorFlow is the famous toolkit.
- based on Artificial Neural Networks (ANNs) and Convolution Neural Networks (CNNs) is the famous one.
- it learns by examples.
- requires very large amount of data and high computing power.

Cloud Computing

- makes the resources available such as computing power and storage without the direct human interference.
- this area already gained lot of attention.
- based on Network Function Virtualization (NFV).

Bioinformatics

-Interdisciplinary field of science that combines

- Biology
- Chemistry
- Computer Science
- Mathematics
- Statistics

- used for protein structure estimation

Cyber Security

- prevention from malicious attacks is required everywhere as

- in Home
- Business
- Public and Private Sector
- Office
- Medicine
- Entertainment, etc.

- Cyber Physical Systems(CPS) are used.
- Capability Based Security is one of the security models

Virtual Reality Applications

- finds diverse role in Gaming(Pokemon Go),Entertainment (Jurassic World), Robotics, Health care and clinical therapies, Education and Training.
- this field is making progress in future trends in following areas:

- Environment
- Space
- Business and Entertainment Industry

Blockchain Technology

-allows digital information to be distributed without being copied.- - Bitcoins and cryptocurrencies.
- Bitcoins are called as digital Gold as total currency is close to US $112 billion.
- usecases in:

- Voting
- Financial Trasnactions.
- Title and Ownwerships
- Anti-counterfeiting
- digital Right Management

Industrial IoT

- in continuation to Big Data.
- many IoT sensors deployed in real-world applications in industry.
- significant arena for Big Data.
- includes industries such as:

- healthcare, transportation, energy, even smart cities, retail and buildings.

5G Technology

-will be adopted in coming years.
- its roadmaps, standards are being built.
- rising tensions between US and China over 5G security concerns.
- major technologies being developed under this include:

- Millimetre-Wave communications
- Multiple Access
- Waveforms
- Massive MIMO with beamsteering
- Dense networks

Self-Driving Cars

- Silicon Valley is building driver-less cars.
- the adoption of such cars is not considered legal due to safety concerns.
- possible to have such cars in controlled environments such as airports, factories, etc.

Hardware Acceleration

- use of computer hardware in computing.
-types such as:

- GPU
- FPGA
- ASIC
- SoC, etc.

Other types of accelerators include 3D Accelerators(used in Gaming), AI Accelerators (used in deep learning algorithms, etc.

Digital Health

- inclusion of digital technology with healthcare systems has not only led to the timely treatment but also self monitoring of one's body.
- technologies such as:

- Smartphones,
- Smart watches,
- Fitness Trackers,
- Smart Glasses

are improving day by day to serve healthcare industry.

Technology for Humanity (using Machine Learning)

- technology such as Robots, drones help us improve:

- Agriculture measures
- Early prediction of Drought, excessive rainfalls,
- Improve Quality of Food,
- Regular Monitoring of health.
- Safety

-sensors everywhere + IoT + Edge computing

Others

- Automated Voice spam (Robo call) prevention.
- Face Recognition (Computer Vision) systems
- Earthquake Prediction.
- Apple's entry into Wearable systems (began in 2015).
- Smart City projects.
- Non-Volatile Memory (NMV) devices will change entire storage hierarchy by 2022.
- Speech Recognition and NLP

Fig. 1 Latest research trends in computer science (CS)

and the combination of LBP with CNN yields desirable results [3]. Computer vision has been in trend since the 90s and is a vast grown field now. Despite having much work done in this field, there is a need of robust device, which could help vehicles in becoming autonomous and help blind persons in independent outdoor navigation. Detecting interesting video game clips is an important task in computer vision. Many algorithms, for example, feature extraction along with deep convolution networks provide interesting results [4].

In healthcare industry, the computerised tests such as electrocardiogram (ECG), electroencephalogram (EEG), EKG, etc. have proved to be very beneficial for the patients and are tremendously growing research fields. These are important to analyse the emotional behaviour of the patients so as to prevent them from depression [5]. The technology has risen to levels that it can now defeat human experts in games and many other such fields. In almost all the games, AI machines have won, and recently, AlphaStar, the DeepMind's project, has successfully defeated top professional StarCraft's player and set a benchmark record [6]. Most of the developed algorithms are actually inspired from natural phenomenon of biological things, for example, ant colony optimisation algorithm and techniques such as sailfish optimiser [7].

This review paper intends to help researchers who are in the beginning phase of framing research problem. It is organised as Sect. 2 introduces Artificial Intelligence and its history. Section 3 mentions the timeline of deep learning and CNNs. Section 4 discusses the challenges faced by early researchers. Section 5 presents the conclusion and is appended with references.

2 Artificial Intelligence

AI is an encompassing umbrella that intends to make such computer programs that are able to think, behave and take decisions just like humans. Since the acquaintance of AI with market, it has become a reason for speedy changes in the technology and business worlds. Ever since the development of powerful digital computers, the capability of machines to perform various tasks have grown tremendously [8]. A part of computer science named AI seeks in making machines that are as astute as people. The two ultimate goals of AI are creating self-learning expert systems and embedding human intelligence into machines. Today, AI has reached the unexpected levels of development and almost all the major developments are being made under it.

Neural networks (NN) are the set of algorithms that copy the way by which human brain operates. The first model of NN was developed by McCulloch and Pitts in 1943 [9]. By the prediction of machine learning (in 1947) and development of Allan's Turing test (in 1950), first, machine learning (ML) program was developed. At the same time, several self-learning programs to play the games such as checkers were built [10]. ML teaches machines on how to learn, by providing them with data and without programming of any type.

2.1 Story of Birth of Artificial Intelligence with Chronological Order

Getting into the roots of any field is important, before beginning research in it. Table 1 shows the inception of AI and how has it grown over the years.

3 Deep Learning

Deep learning (DL) is a part of machine learning, which is further a subset of AI. It is based on learning data representation method, i.e. an algorithm learns by itself from large amount of data. The objective of DL is to enhance technologies such as driverless vehicles, Siri in Apple's iPhone, Amazon's Alexa, etc.

3.1 Deep Learning History

Frank Rosenblatt set up the foundation of deep neural networks in the theory developed for perceptron in 1957 [11]. Around the same time, two types of cells—simple and complex—were discovered in the primary virtual cortex. Most of the artificial neural networks (ANNs) are inspired from them. The ideas of control theory, as published by Henry J. Kelly in 1960 [12], were utilised in making ANNs. Ivakhneko, known as father of modern deep learning, developed a famous method of inductive statistical learning—group method of data handling (GMDH) [13]. Using GMDH, he created an eight-layer deep network known as ALPHA in 1971. In the 1980s, K. Fukushima proposed Necognitron that led to the development of first convolution neural networks (CNNs) [14].

Hopfield networks are recurrent neural networks. They have become famous tool for DL these days. An AI-based program called NETtalk was written by Terrence Sejnowski and Charles Rosenberg around 1985 [15]. It was used to pronounce English words just like a child and learns by its own. Geoffrey Hinton, the Godfather of DL, suggested many improvements in NN for word prediction, object shape recognition, etc. By 1989, deep learning's CNN was combined with backpropagation algorithm to make the machines read handwritten notes [16]. Supervised deep learning algorithms started to develop by the early 1990s.

In order to retain information for longer period of time, long short-term memory was proposed in 1997. The integration of backpropagation algorithm with gradient-based learning became popular technique for deep learning [17]. The ImageNet database was launched in 2009 [18]. It was used to build high level features by using large-scale unsupervised learning [19]. Today deep learning has reached exceptional levels [20].

Table 1 History of artificial intelligence

Timeline of history of AI						
1940	1943	1950	1951	1955	1956	1958
Possibility of creating artificial brain discussed	Artificial neurons proposed	Alan Turing test introduced	• SNARC introduced • First, chess-playing program	Logic theorist	• Dartmouth conference • Birth of AI	Perceptron and logic introduced
1963	1965	1970	1972	1974	1975	1980
Grant of 2.2 million dollars given to AI by DARPA	Dendral expert system produced	Prologue created	• WABOT-1, intelligent robot • MYCIN (expert system)	First AI Winter	Frames created and scripts made	XCON (an expert system) formed
1982	1985	1987	1988	1997	2003	2005
Hopfield nets and backpropagation introduced	Funding began	Second AI Winter till 1993	• HiTech won a match • Deep thought won	Deep blue defeated world champion	AI became rigorous scientific field	Stanford robot won DARPA grand challenge
2007	2011	2016	2018	2019		
Self-driving SUV-boss won the DARPA grand challenge	Watson—an IBM's question answering system defeated	AI products marketed	AI machine painted canvas sold in October 2018 for $432,500	(1) chatbots selling insurance (2) drawing robot-Ai-Da		

3.2 Convolution Neural Networks (CNN)

CNNs—the algorithms of deep artificial neural networks (ANNs)—are used to categorise images based on the low-level features such as edges as shown in Fig. 2. CNNs include large number of neurons in their layers, which help them in recognising new images based on their learning from previous dataset.

Today, CNNs find numerous applications in almost all the vision imaging areas such as human facial expression recognition [21], classifying social-network events [22], brain tumour detection [23], age and gender recognition [24], community question answering [25], etc. The architecture of CNN is originated from Neocognitron [14], which is inspired from cat's visual system [26]. The layers of CNN are discussed below.

Convolution Layer: It is the core layer of the CNNs that do most of the computational work. It takes an image matrix and a filter as input and performs the following computation as shown in Eq. (1).

$$\text{Activation map (Output)} = \text{(image matrix)} \cdot \text{(Filter matrix)} \tag{1}$$

ReLU: The output of the above layer is passed through nonlinear activation function-rectified linear unit (ReLU), to make network as nonlinear. The obtained output is shown in Eq. (2).

$$f(x) = \max(0, x) \tag{2}$$

Pooling Layer: It is also referred to as downsampling layer as it reduces the number of excessive parameters and redundancy in an image. To reduce the amount of memory consumed by the network, spatial pooling is applied. There are different ways of doing so, such as max pooling, average pooling and sum pooling.

Fully Connected Layer: After many convolution and pooling layers, the output is flattened into a vector and fed into a fully connected layer. This layer actually categorise the image by matching the detected features with several classes of the objects and the class that most correlate to those features are detected.

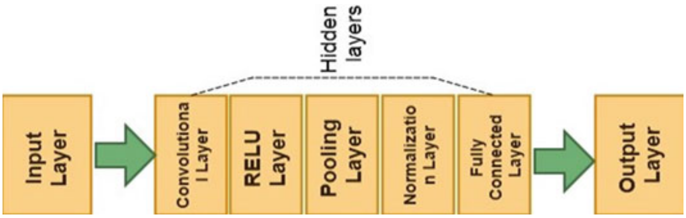


Fig. 2 Architecture of convolution neural networks (CNNs)

3.3 Capsule Neural Networks (CapsNet)

Due to some limitations observed while using CNNs, structures such as capsules are added to them, called CapsNet [27]. These are listed below.

- CapsNets are invariant to viewpoint as they recognise objects even from different angles and provide less error rate as compared to CNNs.
- CapsNet is composed of many capsules and each capsule represents a group of neurons. Due to this, lesser parameters are required for connections between layers.
- CNN breaks on applying transformations such as rotation, scaling, etc. Also, same viewpoint is shown even after different rotations, while CapsNet prevents this and shows better viewpoints.
- CNN requires a large amount of data while training in contrast to CapsNet.
- CNNs suffer more loss by adversarial attacks such as fast gradient sign method (FGSM) in contrast to CapsNet [28].

4 Problems Faced by Previous Researchers in Artificial Intelligence

There were certain risks involved in the development of AI in the past years and due to this, it took a long time to develop and grow. Availability of *Limited Computer Resources* was one such reason. The simplest AI applications require at least 1000 MIPS to execute properly. But in 1976, even the Cray-1 (fastest supercomputer) was able to achieve only 80–130 MIPS. Today, the fastest supercomputer-Sunway Taihulight (China) delivers maximum sustained performance of 93.01 petaflops (a quadrillion floating-point operations per second). *Cost* of the hardware was the second issue that researchers faced. An average desktop computer had a cost of 3000$ approx. in the 1976s, making it a huge factor. Due to the unavailability of experimental labs, time was another crucial factor. According to Tim Cook, certain problems demanded an *exponential time* to get solved [29]. ML and DL algorithms required a gigantic amount of *datasets*, which were unavailable at that time. Accomplishing complex tasks such as face recognition, etc. were very tough for very simple AI systems developed in earlier times. Certain scientists (such as Dreyfus) *criticized* that artificial thinking is based on logical deduction and humans rarely used logics when they solve problems. Therefore, *funding* became major problem for AI researchers [30, 31]. AI has become a highly emerging field now with very innovative technologies.

5 Conclusion

This paper gives an insight to the researchers, about the spectrum of the field of computer science. There are several trends in which research is on-going these days and choosing one, out of them is a challenging task. The characteristics of all areas have been discussed with major stress on AI's deep learning and CNNs. The limitations of CNN and how CapsNet has improved those limitations have also been highlighted. The key challenges faced by researchers working in AI have also been identified. This review paper endeavours to guide the researchers to frame their research problem in the chosen research area.

References

1. Catania BK (Dü.) (2019) Theory and practice of computer science. In: 45th international conference on current trends in theory and practice of computer science. Springer International Publishing, Nový Smokovec, Slovakia
2. IEEE Computer Society predicts the future of tech: top 10 technology trends for 2019, 18 Dec 2018. IEEE Computer Society. https://www.computer.org/web/pressroom/ieee-cs-top-technology-trends-2019
3. Kennedy Chengeta SV (2018) Facial expression recognition using local directional pattern variants and deep learning, ACAI 2018. In: International conference on algorithms, computing and artificial intelligence. ACM, China, NY, USA
4. Chao Huang LZ (2018) RGVCD: a new real-time game video clip detection system, ISB-DAI'18. In: International symposium on big data and artificial intelligence. ACM, Hong Kong, NY, USA, pp 172–177
5. Yu X, Qi W (2018) A user study of wearable EEG headset products for emotion analysis, ACAI 2018. In: International conference on algorithms, computing and artificial intelligence. ACM, Sanya, China, NY, USA
6. Vinyals OA (2019) Mastering the real-time strategy game StarCraft II
7. Shadravan S, Naji HR (2019) The sailfish optimizer: a novel nature-inspired metaheuristic algorithm for solving constrained engineering optimization problems. Eng Appl Artif Intell 80:20–34. Elsevier Ltd.
8. Birrer FAJ (1986) Artificial intelligence. In: Emerging technologies and military doctrine. Palgrave Macmillan, UK, pp 44–52
9. McCulloch WS, Pitts W (1943) A logical calculus of the ideas immanent in nervous activity. Bulletin Math Biophys 5(4):115–133
10. Samuel AL (1959) Some studies in machine learning using the game of checkers. IBM J Res Dev 3:210–229
11. Rosenblatt F (1958) The perceptron: a probabilistic model for information storage and organization in the brain. Psychol Rev 65:386–408
12. Kelley HJ (1960) Gradient theory of optimal flight paths. ARS J 30:947–954
13. Ivakhnenko AG, Lapa VG, Nikolic ZJ (1966) Cybernetic predicting devices. Purdue University School of Electrical Engineering, Lafayette, Indiana
14. Fukushima K (1980) Neocognitron: a self-organizing neural network model for a mechanism of pattern recognition unaffected by shift in position. Biol Cybern 36:193–202
15. Bien B (1988) The promise of neural networks. Am Sci 76:561–564
16. LeCun Y, Boser B (1989) Backpropagation applied to handwritten zip code recognition. Neural Comput 1:541–551

17. LeCun Y, Boser B (1998) Gradient-based learning applied to document recognition. IEEE 86:2278–2324
18. Deng J, Dong W, Li LJ, Fei-Fei L (2009) ImageNet: a large-scale hierarchical image database. In: IEEE conference on computer vision and pattern recognition. IEEE, FL, USA
19. Le QV (2013) Building high-level features using large scale unsupervised learning. In: IEEE international conference on acoustics, speech and signal processing. IEEE, Vancouver, BC, Canada
20. Dhabaleswar K, Panda DK, Awan A (2019) High performance distributed deep learning: a beginner's guide. PPoPP'19. In: 24th symposium on principles and practice of parallel programming. ACM, Washington, District of Columbia, NY, USA, pp 452–454
21. Nikolaos Christou NK (2018) Human facial expression recognition with convolution neural networks. In: Third international congress on information and communication technology. Springer, Singapore, pp 539–545
22. Hussain A, Keshavamurthy BN, Wazarkar S (2019) An efficient approach for classifying social network events using convolution neural networks. In: Advances in data and information sciences, vol0 39. Springer, Singapore, pp 177–184
23. Havaei M, Davy A, Warde-Farley D, Biard A, Courville A, Bengio Y, Larochelle H (2017) Brain tumor segmentation with deep neural networks. Med Image Anal 35:18–31
24. Kharchevnikova AS, Savchenko AV (2018) The video-based age and gender recognition with convolution neural networks. International conference on network analysis, NET 2016: computational aspects and applications in large-scale networks. Springer, Cham, pp 37–46
25. Wang J, Sun J, Lin H, Dong H, Zhang S (2016) Predicting best answerers for new questions: an approach leveraging convolution neural networks in community question answering. In: Chinese national conference on social media processing, SMP 2016, pp 29–41
26. Hubel DH, Wiesel TN (1962) Receptive fields, binocular interaction and functional architecture in the cat's visual cortex. J Physiol 160:106–154
27. Sabour S, Frosst N, Hinton GE (2017) Dynamic routing between capsules. In: 31st conference on neural information processing systems (NIPS 2017). CA, USA
28. Yuan X, He P, Zhu Q, Li X (2017) Adversarial examples: attacks and defenses for deep learning
29. Cook S (1971) The complexity of theorem proving procedures. ACM Digital Library
30. Feng Z, Xiaofeng H, Lin W, Xiaoyuan H, Shengming G (2016) Inspiration for battlefield situation cognition from AI military programs launched by DARPA of USA and development of AI technology. In: Theory, methodology, tools and applications for modeling and simulation of complex systems, pp 566–577
31. Mitchell JR (1987) Workshop on research directions and opportunities II: current funding programs. In: Empirical foundations of information and software science IV. Springer, Boston, MA, US, pp 507–517

Populating Indian GST Details into Java Apache Derby Database Powered by Glassfish Server

R. Sridevi and S. Srimathi

Abstract In simple words, data is the real specifics associated with any objective for consideration. Data, in the perspective of databases, corresponds to all particular items that are stored in a database, moreover separately or as a set. Data in a database in general is preserved in database tables, which are ordained into columns with the intention to enforce the data types retained therein. Database is a staged collection of data and elaborates them as information; more exclusively, a database depicts an electronic framework which eases data to be modestly accessed, manipulated and updated. In other words, whenever an organisation having database it embodies method of storing, managing and retrieving information and they are governed by database management system (DBMS) to make it flexible. Generally, databases encompass multiple tables with numerous different fields suitable to the data stored in the table. Database management system (DBMS) let its users to retrieve information in the database and operate data. In addition, it controls the access to the database. This paper deals with Indian GST rates for various categorical products into the Derby DB using NetBeans as IDE and Glassfish application server. This system can be manipulated and enhanced with the simple SQL queries. This system proves to be a smart way for creating a secure, standardised and transactional Derby DB.

Keywords Indian GST system · Oracle populating · DBMS manipulation · Derby DB · NetBeans

R. Sridevi (✉) · S. Srimathi
Department of Computer Science and Engineering, K Ramakrishnan College of Engineering
Samayapuram, Trichy 621112, India
e-mail: sridevivelon@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_39

1 Categories of DBMS

There were four categories of database management systems available which are listed below:

- Relational database management systems.
- Hierarchical database management systems.
- Network database management systems.
- Object-oriented database management systems.

1.1 Hierarchical DBMS

This category implies the hierarchical if the relations present in the database are with the purpose of having one data that seems as the sub of another data, which indicates the "parent–child" links with them. This category is appropriate for keeping data items depicting attributes features and so on.

1.2 Network DBMS

A network information model could be an information model that enables multiple records to be joined to a similar owner file. The multiple linkages make sure that this permits the network information model to be terribly versatile. Moreover, the data in network model has many-to-many relationship, so one owner file is often joined to several member files and vice versa.

1.3 Object-Oriented DBMS

Object-oriented DBMS has significant advancement when compared to the remaining DBMS. An Object-oriented DBMS acquire data from numerous dissimilar sources like text, photographs and frame output in a multimedia.

1.4 Relational DBMS

In relational DBMS, the database relations are represented by table with the relations that the data related with other in the same or with other tables which can be exactly handled by means of merging one or more tables and processed with the help of structured query language.

2 Uses of Database

Uses of database systems include:

- Accumulate data for effectual and proficient management.
- Simple to know and user-friendly.
- Security and integrity of data.
- Better access to accurate data.
- Handle query processing and management in an excellent way.
- Enhanced decision-making done with the support of database.
- Data sharing and storage for additional handing made.
- Database guarantees error-free information.

3 Oracle Database

When the company develops and complaisance policy varies, it necessitates the flexibility to manage data economically. Oracle affords a principally absolute, incorporated and protected database and data management solution for any exploitation. The organisation necessitates data to stay on premises, managed in data centre or deployed in the cloud; Oracle facilitates access to the same database technology. An Oracle database gathers data ordered by type with associations preserved amongst the different categories. An Oracle database is an aggregation of information perceived as unit which is used for large business processing because of its flexibility and realistic nature to handle data and software applications. Oracle has abundant uses everywhere around the globe in various fields with options like quicker access and speedy recovery, and it makes management and processing of knowledge in a truthful way.

Oracle database reacts extraordinarily well for requesting situations, and the execution is performed in an extremely well mannered. It is a reliable database, and with further highlights, those are tested through the ACID test, which is essential in ensuring the propriety of information. This is necessary because information is the centre of every structure in the association.

Oracle is the most reliable and highly used relational database found today. Its common usage includes:

- Pre-defined data stored for future processing.
- Keeping the standard query language (SQL).
- Administration and handling the data.
- Storing needed information and massive data.
- Providing security options.
- Recovering database.

Oracle is utilised in most applications and one amongst is in banking. It offers powerful combination of technology with wide range of integrating business applications, together with practicality engineered completely in banks. Most of the databases similar to Sybase and SQL include conveniences intended for using conditional loops, arrays, therefore an exceeding program and in addition, services like cursors and employee tables. However, all this can be readily used in a fancy approach that is implausibly easy and resource-intense functions. Usually, new versions releases serve better than earlier versions that exist in Oracle new version which also comprise several features existing compared with prior versions, and it maintains improvement and liberates novel products, and thus, the performance is improved to a great extent. The advantages of newer version led to additional options and with advanced features like this, one could run Java in the Oracle 8i itself. In its next version, 9i Oracle overcame the drawbacks existing in 8i and added new features to assist the DBA in handling changes. In the recent times, Oracle 10 versions have many features together with recycle bin which enhance operations of users just like Windows recycle bin.

Information is the heart of each application or organisation that demands careful maintenance. However, often, application disruption happens, and principally, DBA maintains the explanations for this like hardware collapse, and the reasons may include human-made errors like unintentional removal of valuable information, removing the incorrect information or inappropriate usage of the table. By using recent flash technology, it provides streamline management and administration processes in an efficient manner and provides many features used for providing protection, security, maintenance, dependability and performance in a user-friendly way.

4 Different Ways of Populating Oracle Database

SQL loader uses three different strategies to load information: conventional path, direct path and external tables.

4.1 Conventional Path

The default loading method available in Oracle is the conventional path load. The SQL INSERT statements were used to execute and populate tables in Oracle.

4.2 Direct Path

In this method, the Oracle data blocks were written directly on the database files, which are much faster than the previous method and eliminates a lot of the Oracle database overhead by means of data formatting.

4.3 External Tables

In this, external table is created for data which is enclosed in a data file, and the INSERT statements allow modification of the data and use SQL*loader to carry out the tasks like loading data in network, handling multiple data files, multiple tables, selectively load, manipulate and generating key values and loading data from disk and tape.

5 Indian GST System

In earlier taxation, before GST, there have been several indirect taxes charged by each state and central government. States naturally raise taxes as value-added (VAT). In India, all state had a various set of policy. In the pre-GST system, each buyer as well as the ultimate client paid tax on tax. The sale of products amongst interstate was taxed by the Centre's CST central state tax, was relevant for interstate sale of products, and many other all possible taxes like duty taxes for travel, movie, tips and other local taxes were the put by the respective state and the central government. There were several indirect taxes put in the pre-GST like central excise duty, duties of excise, additional duties of excise, additional duties of customs, special additional duty of customs, cess, state VAT, central sales tax, purchase tax, luxury tax, entertainment tax, entry tax, taxes on advertisements and taxes on lotteries, betting and gambling, and all these extra taxes are currently included in CGST, SGST and IGST.

GST replaced many indirect taxes for the entire country. On 29 March 2017, the Goods and Service Tax Act was passed in the Parliament and came into effect on 1 July 2017. The GST law came into effect on 1 July 2017 in both the Lok Sabha and Rajya Sabha.

5.1 Elements of GST

In GST, there are three different elements of taxes enforced such as: CGST, SGST and IGST.

- CGST: The tax which was charged by the central government for intra-state sale.
- SGST: The tax which was charged by the state government for intrastate sale.
- IGST: The tax which was charged by the central government on an interstate sale.

5.2 Benefits of GST

The introduction of GST mainly removes the barriers in the taxation process by eliminating the tax on tax, so the cost of product reduced. Usually, the GST is principally a technological-based one, and in this, all the product-related deeds starting from registration of product to the filing of return and application processing everything is done only in online GST Portal.

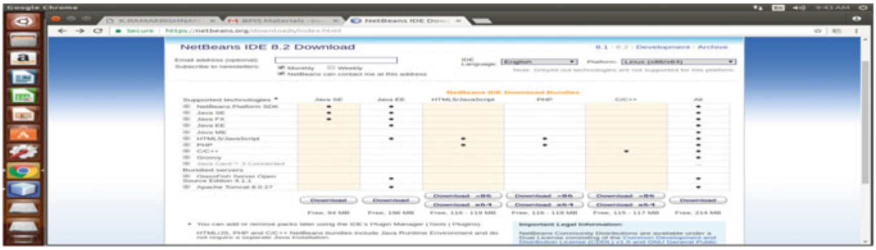
5.3 Experimental Setup

The experiment of populating Indian GST rate for a specific product is carried out using Java DB in NetBeans IDE. The secure and transactional Apache Derby DB running on Glassfish application server is used to implement the system. Here, various operations like creation, populating DB, updating DB and deleting items were performed using the create table command or using SQL queries. After creating Derby DB, the details of various commonly used items along with Indian GST rates are populated into the database. The software requirements include NetBeans version 7.2 along with Java development kit 6.0 and bundled with Glassfish application server. The following steps were involved in populating Indian GST rates into the Derby DB.

1. Installing NetBeans IDE version 7.2 and above.
2. Configuring and adding Glassfish server into the environmental setup.
3. Starting server and establishing connection with the Derby DB.
4. Creating table under Derby DB.
5. Adding and updating Derby DB.
6. Deleting entries if necessary under Derby DB.

5.4 Results and Discussions

The details of Indian GST rates for various categorical products are added into the Derby DB using NetBeans as IDE and Glassfish application server. This system proves to be a smart way of creating a secure, standardised and transactional Derby DB. This system can be manipulated and enhanced with the simple SQL queries. The following snapshots illustrate the implementation of populating Indian GST rates into our system designed using Derby DB. Figure 1 shows the usage of NetBeans IDE 8.2 for various versions of Java. According to the version of Java and the compatibility of operating system, the NetBeans IDE 8.2 can be downloaded. Figure 2 shows the

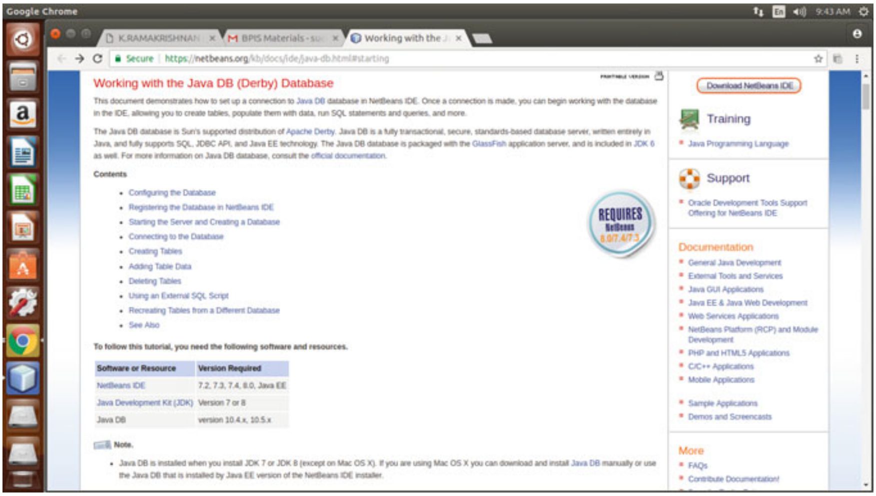


NetBeans IDE 8.2 Download

Supported technologies *	Java SE	Java EE	HTML5/JavaScript	PHP	C/C++	All
NetBeans Platform SDK	●	●				●
Java SE	●	●				●
Java FX	●	●				●
Java EE		●				●
Java ME						●
HTML5/JavaScript		●	●	●		●
PHP			●	●		●
C/C++					●	●
Groovy						●
Java Card™ 3 Connected						
Bundled servers						
GlassFish Server Open Source Edition 4.1.1		●				●
Apache Tomcat 8.0.27		●				●
	Download	Download	Download x86 Download x64	Download x86 Download x64	Download x86 Download x64	Download

Important Legal Information:

Fig. 1 Snapshot of NetBeans IDE 8.2



Working with the Java DB (Derby) Database

This document demonstrates how to set up a connection to Java DB database in NetBeans IDE. Once a connection is made, you can begin working with the database in the IDE, allowing you to create tables, populate them with data, run SQL statements and queries, and more.

The Java DB database is Sun's supported distribution of Apache Derby. Java DB is a fully transactional, secure, standards-based database server, written entirely in Java, and fully supports SQL, JDBC API, and Java EE technology. The Java DB database is packaged with the GlassFish application server, and is included in JDK 6 as well. For more information on Java DB database, consult the official documentation.

Contents

- Configuring the Database
- Registering the Database in NetBeans IDE
- Starting the Server and Creating a Database
- Connecting to the Database
- Creating Tables
- Adding Table Data
- Deleting Tables
- Using an External SQL Script
- Recreating Tables from a Different Database
- See Also

To follow this tutorial, you need the following software and resources.

Software or Resource	Version Required
NetBeans IDE	7.2, 7.3, 7.4, 8.0, Java EE
Java Development Kit (JDK)	Version 7 or 8
Java DB	version 10.4.x, 10.5.x

Note.

- Java DB is installed when you install JDK 7 or JDK 8 (except on Mac OS X). If you are using Mac OS X you can download and install Java DB manually or use the Java DB that is installed by Java EE version of the NetBeans IDE installer.

Download NetBeans IDE

Training

- Java Programming Language

Support

- Oracle Development Tools Support Offering for NetBeans IDE

Documentation

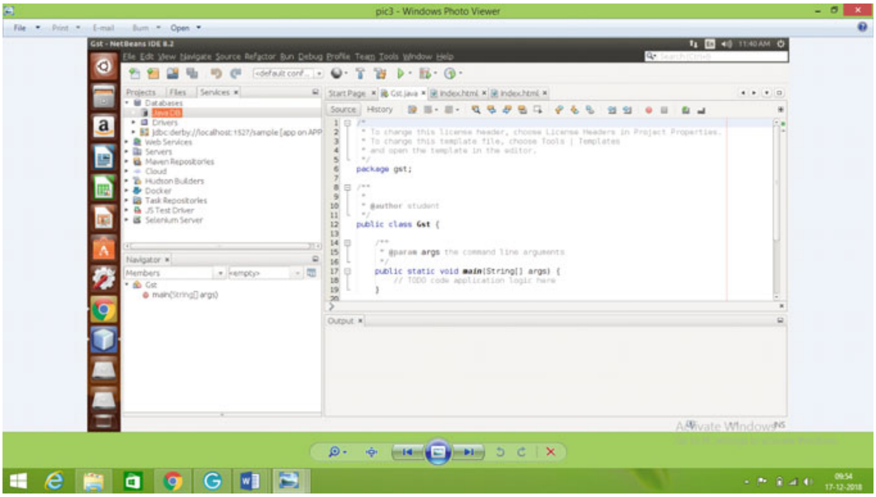
- General Java Development
- External Tools and Services
- Java GUI Applications
- Java EE & Java Web Development
- Web Services Applications
- NetBeans Platform (RCP) and Module Development
- PHP and HTML5 Applications
- C/C++ Applications
- Mobile Applications
- Sample Applications
- Demos and Screencasts

More

- FAQs
- Contribute Documentation!

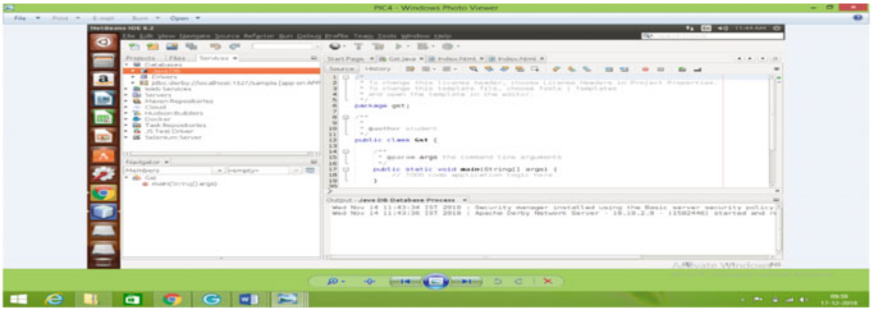
Fig. 2 Snapshot of Java DB (Derby) database

features to download and install Java DB Derby database. Figure 3 shows about how to create Java DB database in NetBeans IDE. Figure 4 shows enabling Apache Derby



```
/*
 * To change this license header, choose License Headers in Project Properties.
 * To change this template file, choose Tools | Templates
 * and open the template in the editor.
 */
package gst;

/**
 *
 * @author student
 */
public class Gst {

    /**
     * @param args the command line arguments
     */
    public static void main(String[] args) {
        // TODO code application logic here
    }
```

Fig. 3 Snapshot of creation of Java DB

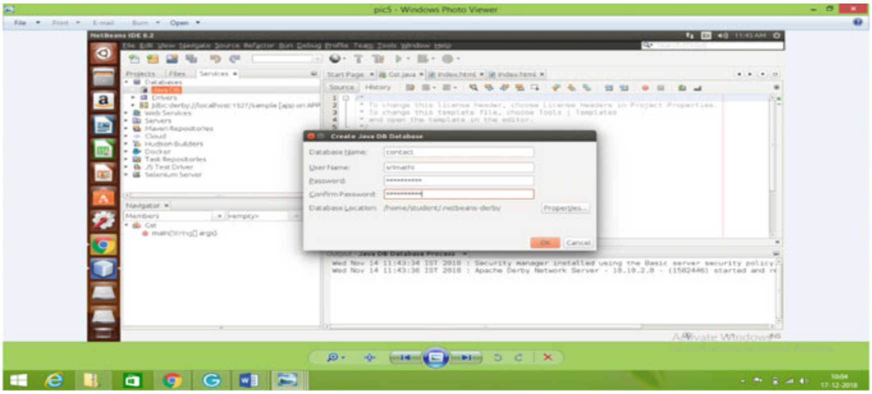


```
/*
 * To change this license header, choose License Headers in Project Properties.
 * To change this template file, choose Tools | Templates
 * and open the template in the editor.
 */
package gst;

/**
 *
 * @author student
 */
public class Gst {

    /**
     * @param args the command line arguments
     */
    public static void main(String[] args) {
        // TODO code application logic here
    }
```

```
Wed Nov 14 11:43:34 IST 2018 : Security manager installed using the Basic server security policy.
Wed Nov 14 11:43:36 IST 2018 : Apache Derby Network Server - 10.10.2.0 - (1582446) started and r
```

Fig. 4 Snapshot of enabling Apache Derby network server

network server. Figure 5 shows creating Java Derby DB and assigning username and password for the created database. Figure 6 shows the way to establish connection in Java Derby DB. After the connection establishment, Fig. 7 shows the way to rename the DB. Figure 8 shows that Glass Fish server is made as a default application server whilst establishing connection with Java Derby DB. Also, Fig. 9 shows the creation of GST Table, and Fig. 10 shows how to create the columns of GST Table like SNO, ITEMS and GST PER CENT. Finally, Figs. 11 and 12 show the way the details of various products are added into the table and final populated GST Table for Indian GST System.



Create Java DB Database

Database Name: contact

User Name: srimathi

Password: ***********

Confirm Password: ***********

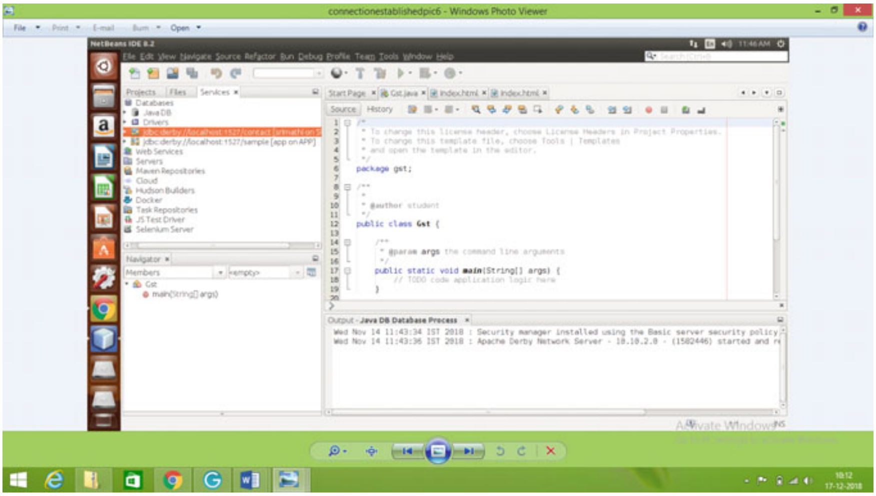
Database Location: /home/student/.netbeans-derby

```
/*
 * To change this license header, choose License Headers in Project Properties.
 * To change this template file, choose Tools | Templates
 * and open the template in the editor.
 */
```

Output - Java DB Database Process

```
Wed Nov 14 11:43:34 IST 2018 : Security manager installed using the Basic server security policy
Wed Nov 14 11:43:36 IST 2018 : Apache Derby Network Server - 10.10.2.0 - (1582446) started and re
```

Fig. 5 Snapshot of creating Java Derby DB

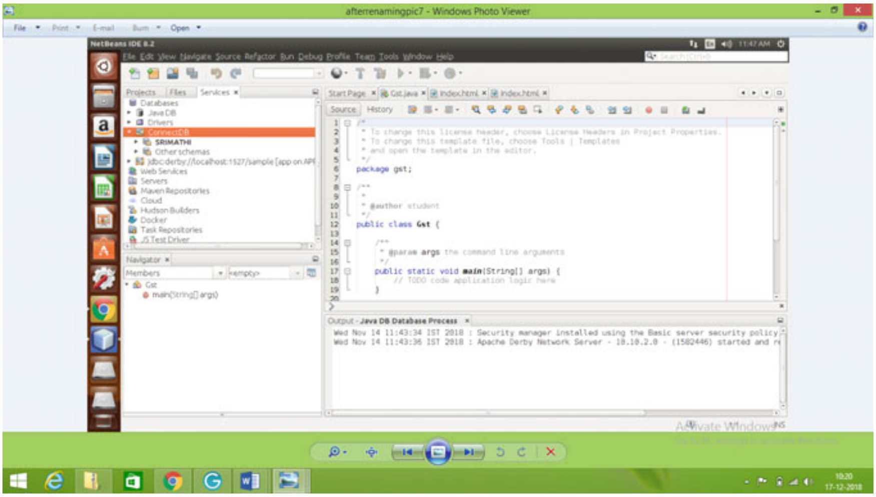


```
/*
 * To change this license header, choose License Headers in Project Properties.
 * To change this template file, choose Tools | Templates
 * and open the template in the editor.
 */
package gst;

/**
 *
 * @author student
 */
public class Gst {

    /**
     * @param args the command line arguments
     */
    public static void main(String[] args) {
        // TODO code application logic here
    }
```

Output - Java DB Database Process

```
Wed Nov 14 11:43:34 IST 2018 : Security manager installed using the Basic server security policy
Wed Nov 14 11:43:36 IST 2018 : Apache Derby Network Server - 10.10.2.0 - (1582446) started and re
```

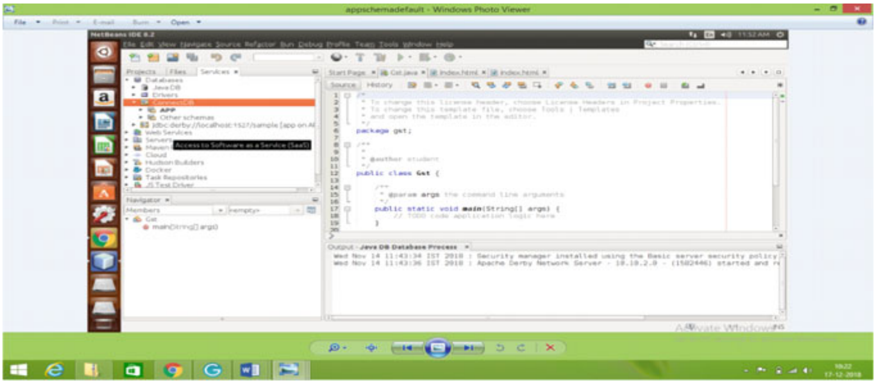
Fig. 6 Snapshot of connection establishment in Java Derby DB



```
/*
 * To change this license header, choose License Headers in Project Properties.
 * To change this template file, choose Tools | Templates
 * and open the template in the editor.
 */
package gst;

/**
 *
 * @author student
 */
public class Gst {

    /**
     * @param args the command line arguments
     */
    public static void main(String[] args) {
        // TODO code application logic here
    }
```

```
Wed Nov 14 11:43:34 IST 2018 : Security manager installed using the Basic server security policy
Wed Nov 14 11:43:36 IST 2018 : Apache Derby Network Server - 10.10.2.0 - (1582446) started and re
```

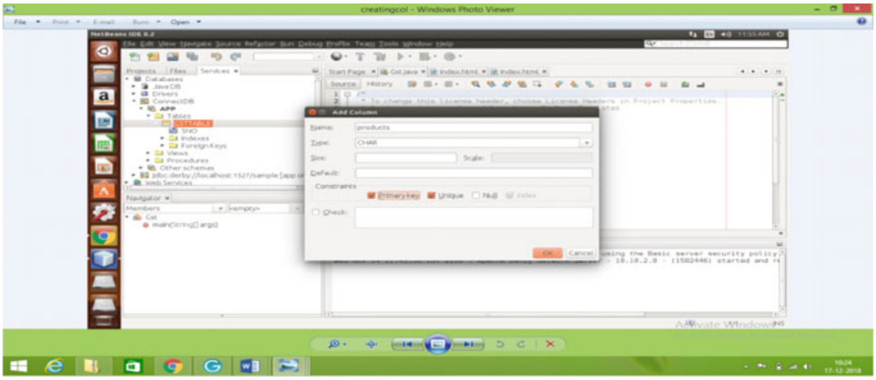
Fig. 7 Snapshot of renaming DB after connection establishment



```
/*
 * To change this license header, choose License Headers in Project Properties.
 * To change this template file, choose Tools | Templates
 * and open the template in the editor.
 */
package gst;

/**
 *
 * @author student
 */
public class Gst {

    /**
     * @param args the command line arguments
     */
    public static void main(String[] args) {
        // TODO code application logic here
    }
```

```
Wed Nov 14 11:43:34 IST 2018 : Security manager installed using the Basic server security policy
Wed Nov 14 11:43:36 IST 2018 : Apache Derby Network Server - 10.10.2.0 - (1582446) started and re
```

Fig. 8 Snapshot of application server made default


Add Column

Name: products

Type: CHAR

Size: Scale:

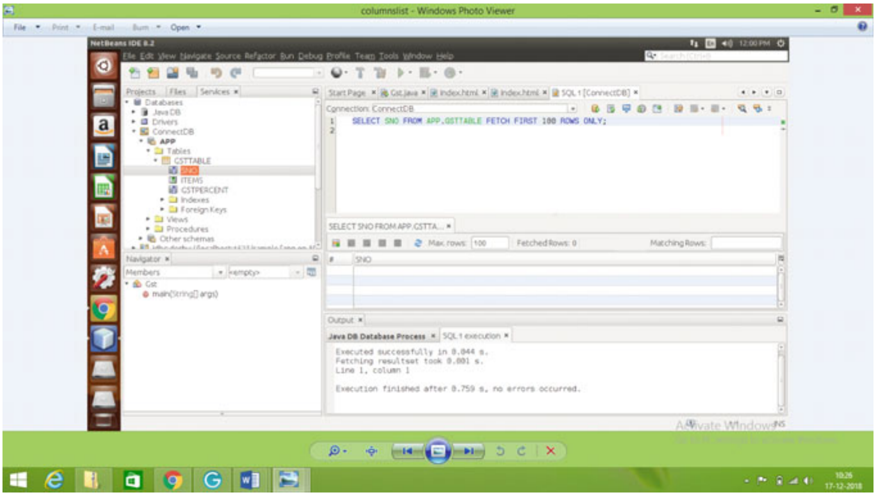
Default:

Constraints ☑ Primary key ☑ Unique □ Null ☑ Index

□ Check:

OK Cancel

Fig. 9 Snapshot of creating column list after creating GST table


Connection: ConnectDB

```
SELECT SNO FROM APP.GSTTABLE FETCH FIRST 100 ROWS ONLY;
```

SELECT SNO FROM APP.GSTTA...

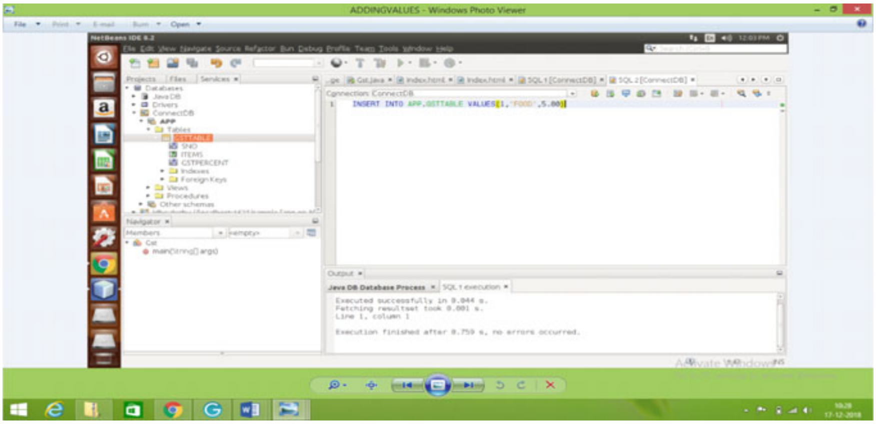
Max. rows: 100 Fetched Rows: 0 Matching Rows:

#	SNO

Output — SQL 1 execution

```
Executed successfully in 0.044 s.
Fetching resultset took 0.001 s.
Line 1, column 1

Execution finished after 0.759 s, no errors occurred.
```

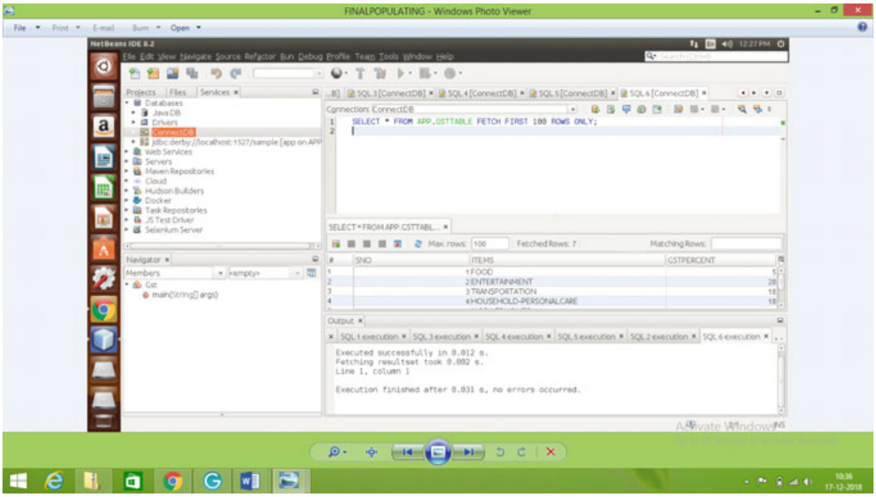
Fig. 10 Snapshot of creating columns like SNO, ITEMS and GST PER CENT



```
INSERT INTO APP.GSTTABLE VALUES(1,'FOOD',5.00)
```

```
Executed successfully in 0.044 s.
Fetching resultset took 0.001 s.
Line 1, column 1

Execution finished after 0.759 s, no errors occurred.
```

Fig. 11 Snapshot of ADDING VALUES into the columns



```
SELECT * FROM APP.GSTTABLE FETCH FIRST 100 ROWS ONLY;
```

Max. rows: 100 Fetched Rows: 7

#	SNO	ITEMS	GSTPERCENT
1	1	FOOD	5
2	2	ENTERTAINMENT	28
3	3	TRANSPORTATION	18
4	4	HOUSEHOLD-PERSONALCARE	18

```
Executed successfully in 0.012 s.
Fetching resultset took 0.002 s.
Line 1, column 1

Execution finished after 0.031 s, no errors occurred.
```

Fig. 12 Snapshot of final populated table

6 Conclusion

This paper deals with Indian GST rates for various categorical products into the Derby DB using NetBeans as IDE and Glassfish application server. This system can be manipulated and enhanced with the simple SQL queries. This system proves to be a smart way of creating a secure, standardised and transactional Derby DB. In future, the system can be enhanced by depicting the operations and accessing permissibility and can be used as a back-end database system whilst designing a website for Indian GST System.

Bibliography

1. Viswanathan B (2016) Goods and services tax (GST) in India. New Century Publications, New Delhi
2. Gupta SS (2019) GST how to meet your obligations, 7th edn. Taxmann Tax & corporate laws of India
3. Taxmann (2018) GST manual with GST law guide & GST practice referencer, 2 volumes, 10th edn
4. Laddha V, Saxena S, Patwari P (2019) GST audit manual, 2nd edn.
5. Amutha D (2018) Economic consequences of GST in India, SSRN's eLibrary
6. Nayyar A, Singh I (2018) A comprehensive analysis of goods and services tax (GST) in India. Indian J Fin 12
7. Mehra G (2017) GST as major reform in taxation system of India. Int J Sci Res (IJSR) 6(9):497–501
8. Jatin (2016) Awareness towards goods and services tax in India. Int J Inform Futuristic Res 4:5891–5896
9. Madesh HR, Kavya Dechamma KM Impact of good and service tax on various sectors in India. IOSR J Bus Manage (IOSR-JBM)
10. Mahender P (2017) GST effect on manufacturing industry—India. Int J Manag Stud Res (IJMSR) 5(1):28–30
11. Cnossen S (2013) Preparing the way for a modern GST in India. In: International tax and public finance. Springer Science & Business Media, New York
12. Dash BB, Raja Angara V (2013) Intergovernmental transfers and tax collection in India: does the composition of transfers matter? In: Public budgeting & finance, Blackwell Publishing Ltd., Maiden
13. Satish Kumar R (2018) Indian textile industry: opportunities, challenges and suggestions. Trends Textile Eng Fashion Technol CRIMSON PUBLISHERS 2(3)

Web References

14. https://www.oracle.com/technetwork/java/javadb/overview/index.html
15. https://www.paisabazaar.com/tax/gst-rates/
16. https://cleartax.in/

Intrusion Detection System Using WoSAD Method

R. Sridevi and N. Nithya

Abstract The network services are reducing the secure communication through preventive detection of intrusion services. Besides, different types of network transmission host the intrusion detection services by data centres that vary of server organisation mechanism. Network security topology is afflicted of one application service by a different communication reciprocal that assume poor performance through application services. Further, work factors that can affect the communication packets performance by including network infrastructure component failure, configuration issues, or damage cost of informal distinct components. The intrusion detection services are the community around time for servicing a request of main user. This work has been proposed to Whole of Service Anomaly Detection (WoSAD) methods, which remain more effective than the alternative route transmission and to the whole of service models.

Keywords Total cost of ownership · Whole of service · Anomaly detection · Intrusion detection

1 Introduction

The network intrusion services are generally a major problem of market distributors, individuals, and disruptors of current firm models. The costs of network service failure stages or delay communications are important drawbacks for customer services and emerging new marketing services. Information Technology Security Manager (ITSM) in vast organisations is a complexity of energetic and highly solid firm condition in service operations. Various manufacturing standards for, e.g. ISO/IEC 20000, COBIT substantiate possibility (e.g. Information Technology Infrastructure Library

R. Sridevi (✉) · N. Nithya
Department of Computer Science and Engineering, K. Ramakrishnan College of Engineering, Trichy, India
e-mail: sridevivelon@gmail.com

N. Nithya
e-mail: nithyasrichithra@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_40

(ITIL), Microsoft MOF, HP ITSM, and IBM ITPM) which naturally slowdowns the services. Intrusion said to be the process of accessing data and computer resources without authenticity thus causing hazard to security breach [1]. Intrusion detection is like a weapon which monitors and analyse the activities going on in a computer or network and to identify security breaches. Intrusion detection system (IDS) assess the activities of servers, file systems, firewall, routers, and also tests the network traffic activities that deviate from the security policy [2] and alerts the system or network about the threat. These events should be avoided detection for security abilities. Moreover, a number of firm multitudes their information services data centres that feature varying degrees of information processing service centre streamlining. The reasons for low performance is based on infrastructure or component failure, design issues, or accidental cost of actualising distinct components. The principal measure used to define user experience purely based on time taken for completing the request, so require a robust communication to control any process corruption.

The effectiveness of detecting the network data inconsistency or abnormalities from usual behaviour developed the system with time distribution known as grade of service (GoS). This paper investigates the behaviour incompatibilities by sensing abnormal events in complex real-world systems and summarising them with consistent service authorisation frameworks like Information Technology Security Manager (ITSM) and also it distinguishes ITSM frameworks such as ITIL.

Threshold alert set as a key for identifying delay in applications which compute and observe performance activities and generate alerts every time when things move beyond defined limits. The problem with the threshold-based notification system is which can cause technical improvement assets become unsusceptible and the alarms become too noisy and how it is rectified is a big question which can be addressed by event filtering ability that reduces noise by multiple orders of magnitude but categorises actual problems. Operationally, it can generate prohibitive storage details and security on system presentation for huge data and ensures the monitoring systems to be sensible to manage, balance size.

The challenge of real-time anomaly detection technique earlier than primary source diagnostic detail is lost and/or rollup happen. This is effectively achieved community process and problem management ITSM process with modify process detection, the characterisation of event symptoms, formulation, and testing assumptions and root cause justification.

The rest of the paper comprises of the proposed method, methodology, and conclusion part.

2 Proposed Method

The Whole of Service Anomaly Detection (WoSAD) proposes to be extra efficiency than another operations and whole of service models.

The WoSAD methodology is mainly used to detect, characterise, support root cause identification, and determine tortuous systems operation anomaly problems.

1. Whole of Service Measurement Method (WoSMM)
    - Application portfolio monitoring points,
    - Application architecture sampling points.
2. Whole of Service Profiling (WoSP)
    - Application identification,
    - Transaction load identification,
    - Traffic mix identification.
3. Whole of service measurement used in system profile WoSP

    The WoSAD based on data-driven model through which data behaviour represents the application presentation signature concept with time capture the WoSMM data contour. Figure 1 depicts the WBAN connectivity diagram.

    - AA scheme for WBANs scheme proven to be vulnerable securing and validating the result the system performed with the computation costs at a client side.
    - Our proposed scheme reduces the computation time and not only solves the existing approach drawbacks, but also reduces the computation trouble on the users.
    - The lightweight cryptographic approach is verification of device collocation and authentication scheme for WBANs.

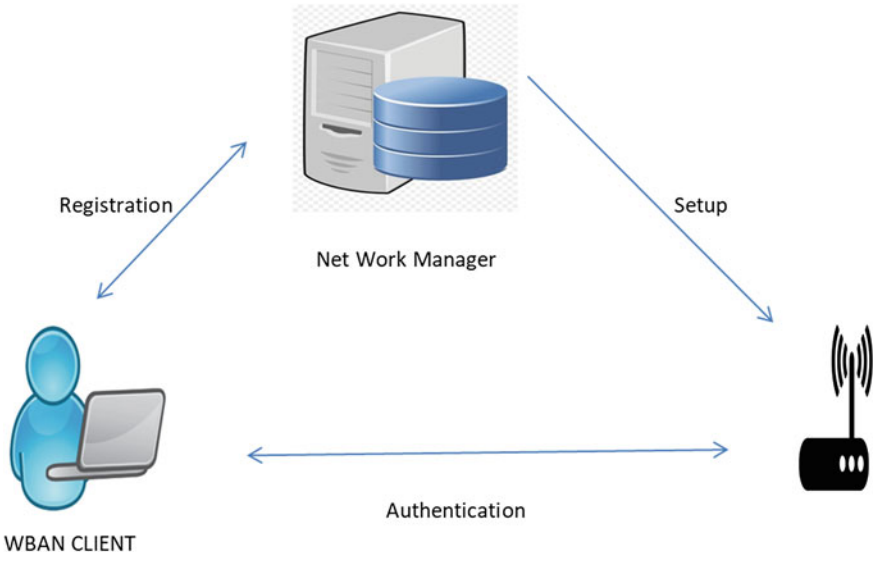


Fig. 1 WBAN connectivity

3 Methodology

3.1 Security Requirements

The scheme of WBAN mechanism performs a client and the service provider communicates independently. Accordingly, the scheme of authentication for WBANs technology is vulnerable to different type of attacks. The agreement of secure communication in WBANs schemes, the authentications are able to solve various types of attacks. According to previous works, the authentication arrangement for WBANs scarifies the following security supplies.

(1) **Shared Substantiation**:

It is important that the authentication schemes for WBANs services which can provide mutual authentication among the client and the application service provider and limited the number of clients in accessing information.

(2) **Obscurity**:

To protect the client's collective details it is mandatory that no one including or modify the application service provider and network manager with client's identity.

(3) **Non-traceability**:

The application service provider and the network manager were not capable to outline the client's action priory and not sufficient for maintaining the client's privacy location to know necessary for authentication scheme.

(4) **No Verification Table**:

Usually, the verification table performs secure authentication systems. Lot of trouble to manage the service provider has to report when connect to a new client or existing client revoke from the system so as a result of requirement that no verification table used by the system.

(5) **Session Key Agreement**:

To authenticate the confidentiality, integrity, and non-repudiation of secure data transmission in WBANs scheme with session key management between the client and server.

(6) **Perfect Forward Secrecy**:

The communication established between the client and the service provider in WBANs scheme by using shared key while the adversary becomes their secret keys by decrypting the received messages. To protect the client's information, it is essential WBANs scheme supports forward secure communication and ensure network user cannot receive the session key authentication level if the secret keys for client and the application service provider are gain.

(7) **Attack Resistance**:

In open network position, the secure validation for WBANs exposed to different attacks like reply attack, impersonation attack, modification attack, stolen verifier table attack, and includes man-in-the-middle attack. The safeguard security mechanism is highly required for authentication schemes.

(8) **Data Encryption**:

The recommendation of a lightweight encryption algorithm as the use of secure IoT (SIT) method which is depicted in Fig. 5. It performs a 64-bit block-cipher mechanism and requires 64-bit key to encrypt the data for security. The algorithm is a combination of feistel and identical substitution–permutation network architecture. It used to advance secure IoT (ASIT) approach. The 1024-bit block cipher needs to be 10,254-bit key computation to encryption of the secure data.

For the experimental purpose, the KDDCUP'99, especially meant for intrusion detection data set used which can hold tcp dump portions. The data set contains a total of 24 attack types that fall into four major categories: Denial of service (Dos), probe, user to root (U2R), and remote to user (R2L). Each record is labelled either as normal, or as an attack, with exactly one specific attack type. In this work, all the UDP packets and their relevant attacks were taken and analysed with java platform. Figure 2 indicates the process of training and test set selection, Fig. 3 mentioned about the hybrid learning process used, and Fig. 4 shows the result which was detected as anomaly (Fig. 5).

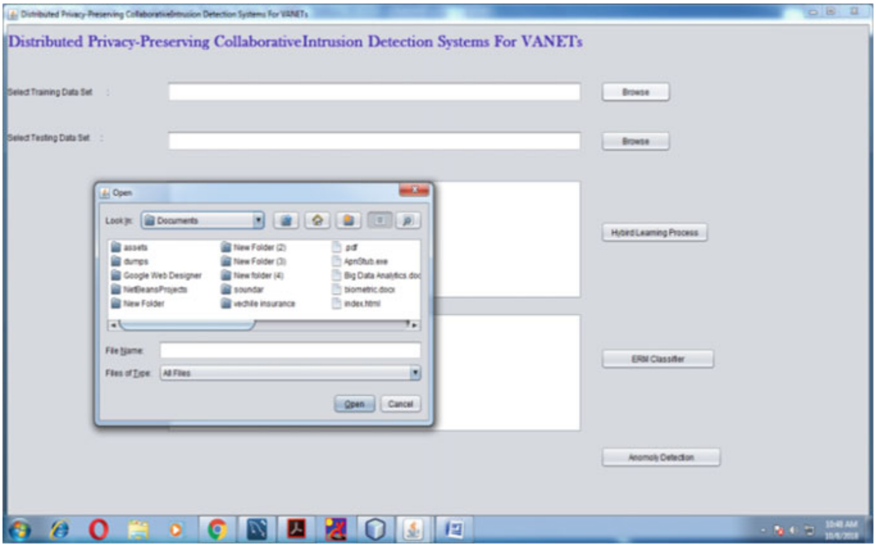
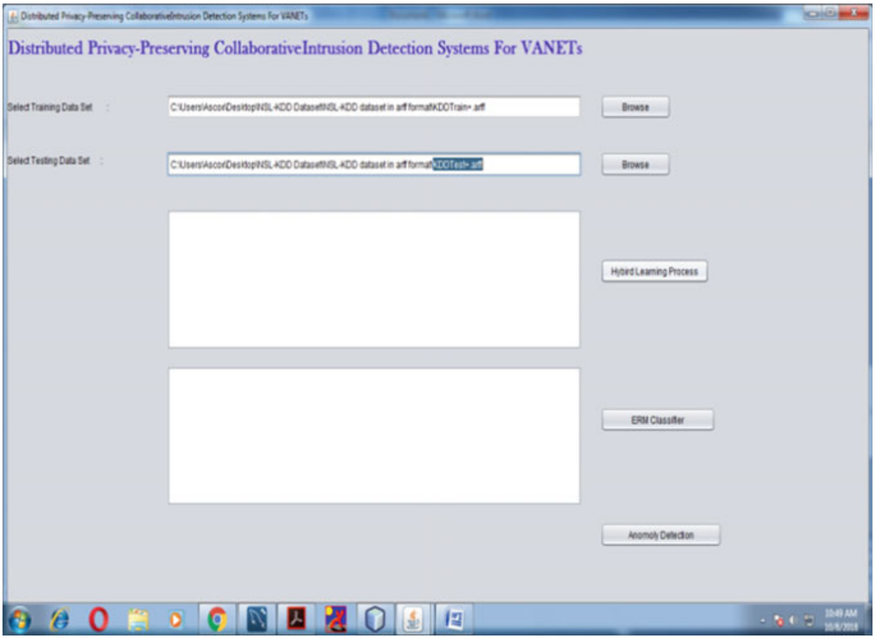


Fig. 2 Training data set selection

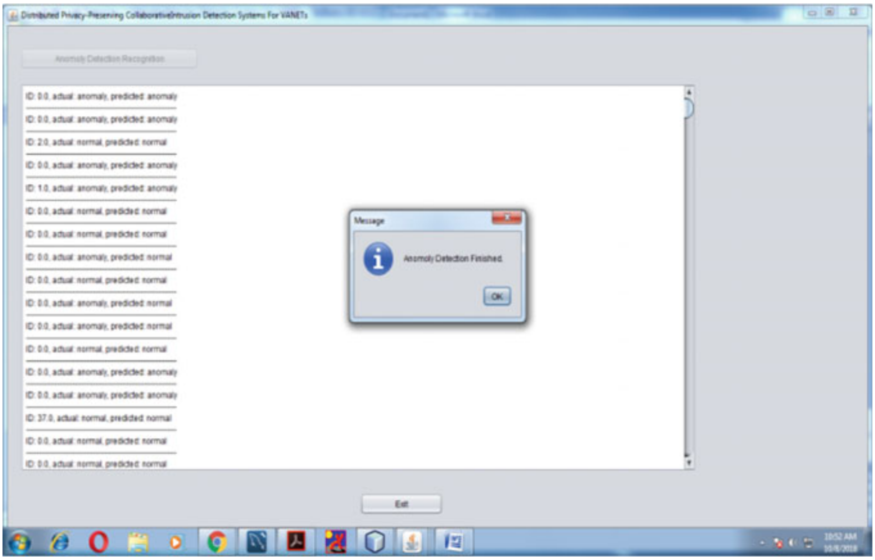


Distributed Privacy-Preserving CollaborativeIntrusion Detection Systems For VANETs

Select Training Data Set : C:\Users\Ascor\Desktop\NSL-KDD Dataset\NSL-KDD dataset in arff format\KDDTrain+.arff

Select Testing Data Set : C:\Users\Ascor\Desktop\NSL-KDD Dataset\NSL-KDD dataset in arff format\KDDTest+.arff

Fig. 3 Hybrid learning process


Distributed Privacy-Preserving CollaborativeIntrusion Detection Systems For VANETs
Anomaly Detection Recognition
Message
OK
Exit
10:52 AM
10/6/2018

```
ID: 0.0, actual: anomaly, predicted: anomaly
ID: 0.0, actual: anomaly, predicted: anomaly
ID: 2.0, actual: normal, predicted: normal
ID: 0.0, actual: anomaly, predicted: anomaly
ID: 1.0, actual: anomaly, predicted: anomaly
ID: 0.0, actual: normal, predicted: normal
ID: 0.0, actual: normal, predicted: normal
ID: 0.0, actual: anomaly, predicted: normal
ID: 0.0, actual: normal, predicted: normal
ID: 0.0, actual: anomaly, predicted: normal
ID: 0.0, actual: anomaly, predicted: normal
ID: 0.0, actual: normal, predicted: normal
ID: 0.0, actual: anomaly, predicted: anomaly
ID: 0.0, actual: anomaly, predicted: anomaly
ID: 37.0, actual: normal, predicted: normal
ID: 0.0, actual: normal, predicted: normal
ID: 0.0, actual: normal, predicted: normal
```

Anomoly Detection Finished.

Fig. 4 Anomaly detection

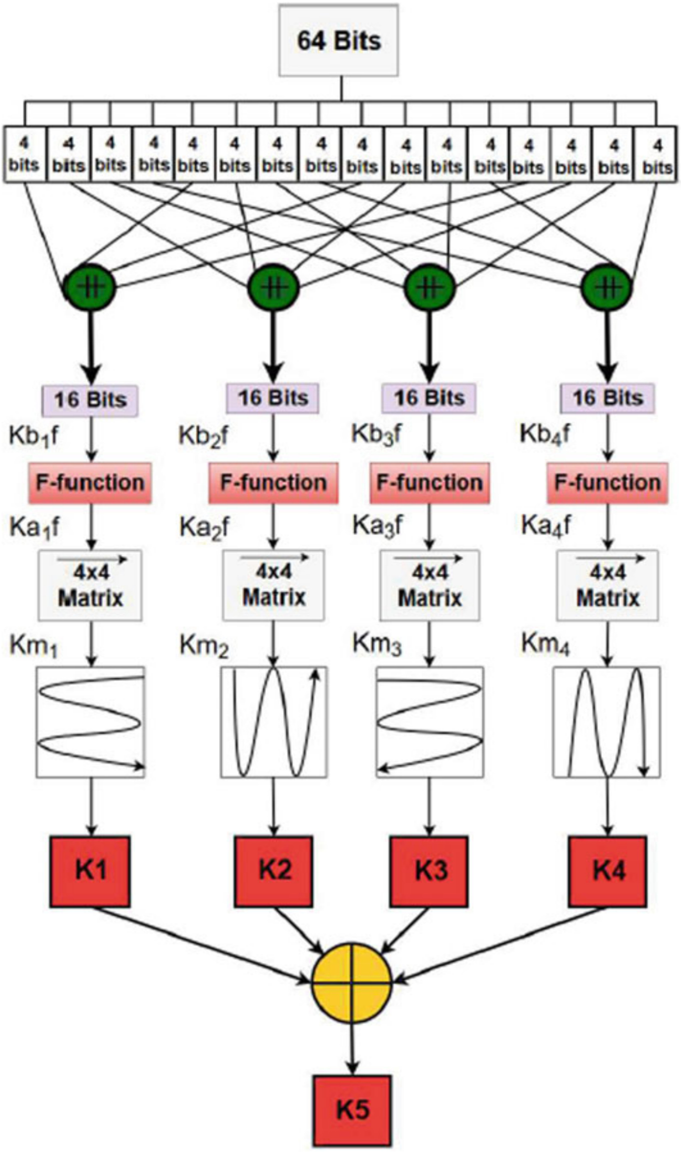


Fig. 5 SIT algorithm

(9) **Whole of Service Measurement Method**:

The Whole of service measurement takes “black box” as key characteristic, begins the measurement of application component reaction from time-to-time in end-to-end manner that captures the reaction time and makes summary about complexity either "inductive" or "reductive" with the approach of component by component; top-to-bottom down approach. The simple terms of these metrics are related to assignment towards the system with the number of users participated in activity, and the responsible time of result system.

4 Conclusion

In this paper, proposed to WoSAD methodology is proposed to combination of data communication model. The performance of application signature is behavioural data-driven denotes existent time attack of the WoSMM data profile. The GoS process proxy service the model of data-driven associated with online performance distribution patterns captured in queue models such as M/M/1 model. The GoS-based WoSAD performance communication proxy "k" found efficient detection model; here, substitutions are used to every transaction in acceptable score boundaries. The issue of key with the least expeditious individual business models needs to de-sensitise them to incomprehensibility from separate transference inconsistency.

This communication device has noise seems to be spontaneously reasonable payable for inconsistency calculations across the many individual communication transaction types are involved. The entire service of mean plus standard deviation response time detection models are less efficiency. This scheme relies on statistical metrics that clarify symmetrical distributions. These metrics were not describing any online transaction time behaviour which is asymmetrical in setting of response. The WoSAD techniques at entire surrounds such as all positions ends are not dependent on specific system mechanism. This work proposed to Whole of Service Anomaly Detection (WoSAD) methods are established to be effective than alternative route transmission and whole of service models.

References

1. Gow R, Rabhi FA, Venugopal S (2018) Anomaly detection in complex real world application systems. IEEE Trans Netw Serv Manage
2. Zhang T, Zhu Q (2018) Distributed privacy—preserving collaborative intrusion detection systems for VANETs. IEEE

Blackhole Attack Implementation and Its Performance Evaluation Using AODV Routing in MANET

Anshu Kumari, Madhvi Singhal and Nishi Yadav

Abstract Mobile Ad hoc Network (MANET) is a self-sorted out remote system, comprising of independent nodes. The correspondence in the MANET is of multihop in nature because of non-attendance of any settled foundation or centralized base. An assailant, it may encroach effectively into MANET by acting like authentic middle of the road hub and present different kinds of security assaults on information exchange occurring among source and goal. In this paper, we have simulated the blackhole assault in AODV reactive routing protocol of MANET and investigated its viability by considering various performance metrics.

Keywords MANET · Blackhole · Performance · PDR · Throughput

1 Introduction

MANET is a remote system where a gathering of mobile nodes can progressively change the topological structure [1]. It is a self-arranging and self-designing system. A hub can discuss specifically with its nearby hubs just which are available inside its transmission go. The hubs communicate with one another by means of radio waves. The hub goes about as both sender and receiver. MANETs do not utilize any type of settled foundation or unified organization that we see by and large if there should be an occurrence of all the more broadly utilized mobile node systems. MANETs are anything but difficult to convey and design which results in their prevalence in contrast with wired systems. The principle highlight of MANET is its moment organized setup. In any case, routing in MANET is a test because of its dynamic topology in the system as portable hubs can move toward any path in the MANET

A. Kumari · M. Singhal (✉) · N. Yadav (✉)
Department of Computer Science & Engineering, Guru Ghasidas University, Bilaspur, India
e-mail: madhvisinghal4@gmail.com

N. Yadav
e-mail: nishidv@gmail.com

A. Kumari
e-mail: anshu1997kri@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_41

[2]. MANET is useful in spots that does not have any correspondences foundation or once that framework is extremely broken [2]. These sorts of systems have the resulting striking qualities: dynamic topologies, data transfer capacity compelled variable limit joins, restricted physical security and vitality-obliged activities.

There are mainly three types of routing algorithms available namely proactive, reactive and hybrid (mixture of reactive/proactive) routing algorithms. Proactive is a table-driven routing protocol. In this, each node keeps up the rundowns of all conceivable goal hubs in a table. To keep the data in the routing table updated, each node intermittently exchanges routing messages [3]. A change in the routing table is informed to all other nodes in the framework through flooding technique. Distributed Sequenced Distance Vector (DSDV) is a proactive protocol [4]. Ad hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) are reactive routing protocols [4] which follow on-demand routing where the routes are found only just when required. When route is required, a type of route discovery system is utilized which results in large control message traffic. Since these conventions expect participation between two hubs for packet sending, a noxious hub may prompt routing assault in the system that disturbs the ordinary routing tasks of MANET [3]. Therefore, decentralized and dynamic nature of MANET may prompt different assaults in the system that can degrade the working of the system [3].

The MANET is prone to various types of attacks which can be classified into two broad categories, one is passive attacks and other is active attacks. A passive attacker monitors the correspondence channel and snoops the data being exchanged in the network without altering it. Thus, a passive attacker does not disrupt proper operation of the system but it is very difficult to be detected. While an active attacker attempts to alter the principal data being exchanged and disrupts the normal working of the system which makes it easy to detect as compared to passive attacker. Because of immaterial structure and quick course of action, MANETs are fitting for emergency conditions like natural calamities rescue activity, medical clinics, war zone, meetings and military applications. Thusly, data trade between two center points must require security. In any case, the extremely basic assaults in MANET are blackhole attack [5–8], wormhole attack which have stunning effect on the efficiency of the framework.

Blackhole assault is a remarkable kind of attack that generally occurs in the reactive algorithms. A blackhole hub is the dangerous node that pulls in the packets by incorrectly attesting that it has most short and fresh way to reach the goal, by then drops the packets. These blackhole hubs may perform distinctive damaging exercises on the framework. For instance, it may carry on as a source node by distorting the route request packet, may go about as a destination center point by twisting the route reply packet, or may lessen the quantity of hop counts, when sending route request packet.

2 Related Work

In past, there have been various attempts for countering the blackhole attacks. Some of them that we overviewed are as follows: In [9], the author has proposed a technique to locate the blackhole attack on AODV protocol in MANET. This technique considers that the first route reply packet that it has received is the reaction from malicious node and, therefore, removes that node from the network. And when the second route reply packet it receives, is considered for the route reply saving mechanism as it originates from the goal hub. He has named this technique as blackhole detection system. The modified AODV with this BDS arrangement against blackhole node has high packet delivery ratio when contrasted with the already existing AODV protocol under blackhole attack. In [10], the proposed method handles with the multiple blackhole nodes assault in MANET. To deal with the numerous blackhole nodes assault, the source hub utilizes the sequence number idea to distinguish the various blackhole nodes in MANET. The source sequence number is utilized by the source hub to detect the blackhole assault. In [8], the authors proposed a technique that uses the fake route request packets to detect and isolate blackhole attack in MANET. The fundamental plan to distinguish and confine noxious hubs is which the utilization of fake messages. Whenever the source hub needs route to goal, it will flood counterfeit route request packets in the system. These route request packets are made counterfeit by including the IP address of the hub which is not present in the system. So when the hub answers with the route reply packet, it will be identified as the malevolent node and can be segregated from the system. In [3], the authors have proposed a clustering approach to identify the blackhole nodes in AODV routing protocol of MANETs. In order to identify the impossible to miss contrast between the number of information packets got and sent by the hub, each individual from the cluster will ping once to the cluster head. On the off chance that anomalousness is seen, every one of the hubs will obscure the malicious hubs from the system.

3 Proposed Work

In this paper, we have considered the implementation and effect of blackhole attack on AODV routing protocol. Softwares that we have used for this are NS-2.35, NSG2.1 and gawk. NS-2.35 is a network simulator. NSG2.1 is a network simulator generator which has been used to create.tr file which is run on NS-2.35. GAWK has been used to read the trace (.tr) file for analyzing the performance of the network. AODV protocol is already present in NS-2.35. For better analysis of the result, we have considered changing number of nodes (100, 200, 300, 400 and 500). After simulation, packet delivery ratio and throughput have been calculated considering the following definition.

Packet Delivery Ratio (PDR): The ratio of the number of packets received by TCP sink to the number of packets delivered by the TCP source.

Throughput: Throughput of the network is defined as the number of bits of data that are received by the goal node per unit time. It is the ratio of number of bits received by the goal node to the total time taken.
Packet Drop Ratio: Packet drop ratio tells about the network performance in terms of packets that have been dropped by the nodes. It has been calculated as:

$$\begin{aligned}\text{Packet Drop Ratio} = {} & (\text{Number of packets received by node} - \text{Number of packets} \\ & \text{forwarded by node})/\text{Number of packets received by node}\end{aligned}$$

The Simulation environment is as follows (Fig. 1; Table 1):

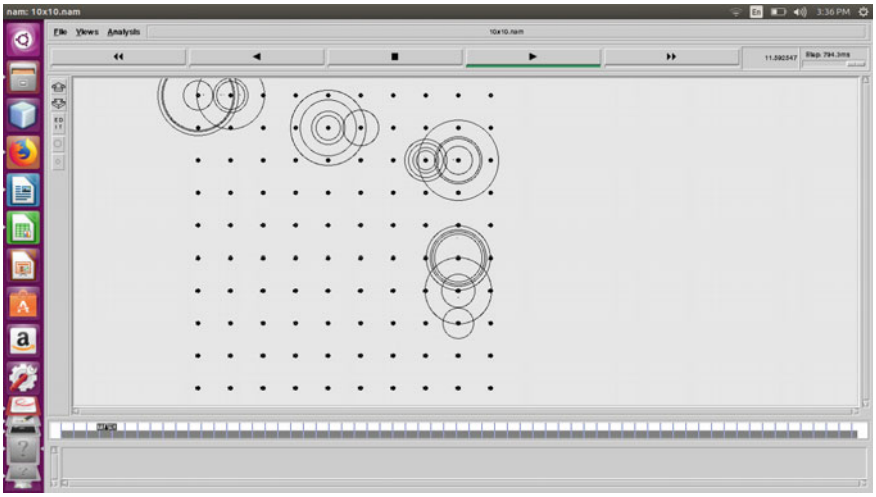
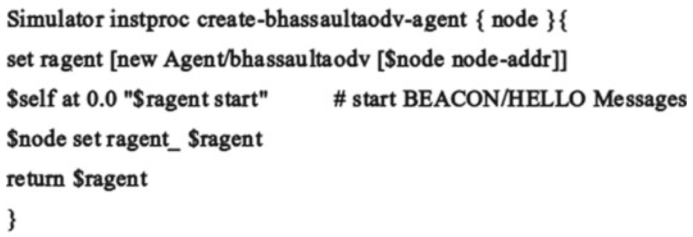


Fig. 1 Simulation of AODV protocol in NS-2.35

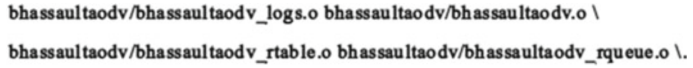
Table 1 Simulation environment parameters

Parameters	Values
Simulator	NS-2.35
Protocols	AODV
No. of nodes	100, 200, 300, 400, 500
Topology	Grid
Simulation time	200 s
Traffic type	FTP
Propagation model	Two ray ground
Max packet in queue	20
Number of blackhole node	1
Packet size	500 bytes



```
Simulator instproc create-bhassaultaodv-agent { node }{
set ragent [new Agent/bhassaultaodv [$node node-addr]]
$self at 0.0 "$ragent start"        # start BEACON/HELLO Messages
$node set ragent_ $ragent
return $ragent
}
```

Fig. 2 Addition of the “bhassaultaodv” protocol agent in the “\tcl\lib\ns-lib.tcl” file



```
bhassaultaodv/bhassaultaodv_logs.o bhassaultaodv/bhassaultaodv.o \
bhassaultaodv/bhassaultaodv_rtable.o bhassaultaodv/bhassaultaodv_rqueue.o \.
```

Fig. 3 Addition in the “\makefile” at the NS-2.35 directory

First of all, we analyzed the performance of already existing AODV protocol utilizing system parameters packet delivery ratio, throughput and packet drop ratio for each node. Then, we implemented blackhole node behavior by modifying the existing AODV. For this, we renamed the file aodv.cc as bhassaultaodv.cc and then modified its content as per our need. To set a routing agent to the node, we included the following lines of code in “\tcl\lib\ns-lib.tcl” file (Fig. 2).

Then, compile the NS2 to create object files. Then, the “/makefile/” is added with following lines in the root directory NS-2.35 (Fig. 3).

Then, we make a node as a blackhole node. We have made node 21 as a blackhole node in our simulation. When a packet utilizing AODV protocol is received, recv() is called which processes the packet according to its type. If it is an RREQ, RREP or RERR packet, then recvAODV() is called and if it is a data packet, then it is routed to the destination. When the data packet reaches a blackhole node, it is dropped there and hence, does not reach to its goal.

In order to incorporate these changes in the required files, open the terminal and run “make” command inside “ns-allinone-2.35/ns-2.35/” directory. If it run successfully, then our new AODV protocol is included successfully. A new tcl file is created with one blackhole node in the system to simulate the new protocol and run into the terminal. Its performance is analyzed utilizing system parameters packet delivery ratio, throughput and packet drop ratio for each node.

4 Simulation Result

From Fig. 4, we can conclude that in case of blackhole attack, the PDR value of network decreases irrespective of the number of nodes. Drop in PDR value can be seen in small as well as large network. Figure 5 reveals that throughput is not much affected by the size of network. It remains almost same on increasing or decreasing

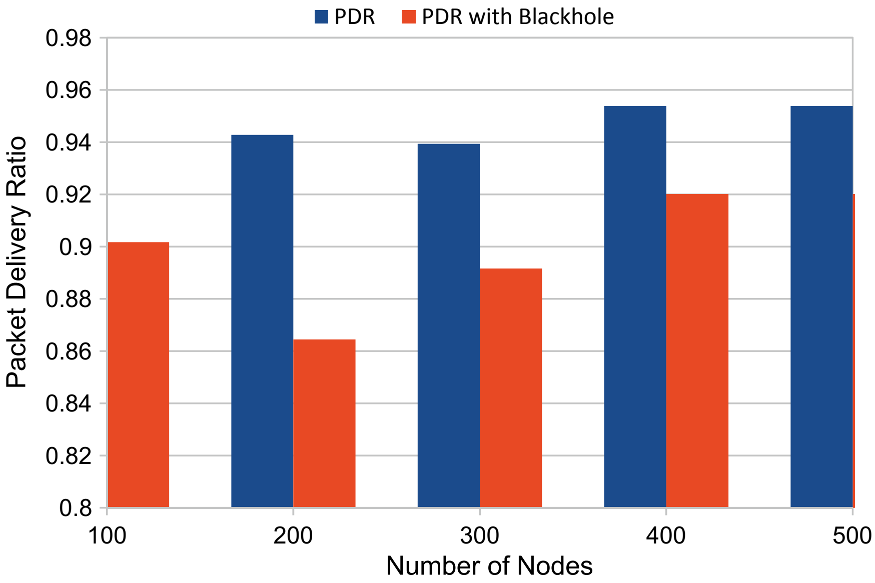


Fig. 4 Packet delivery ratio versus number of nodes

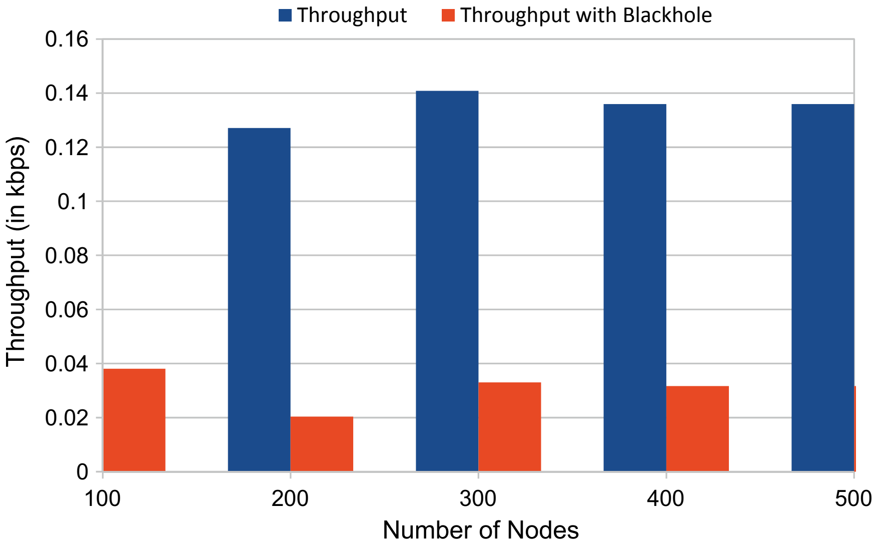


Fig. 5 Throughput versus number of nodes

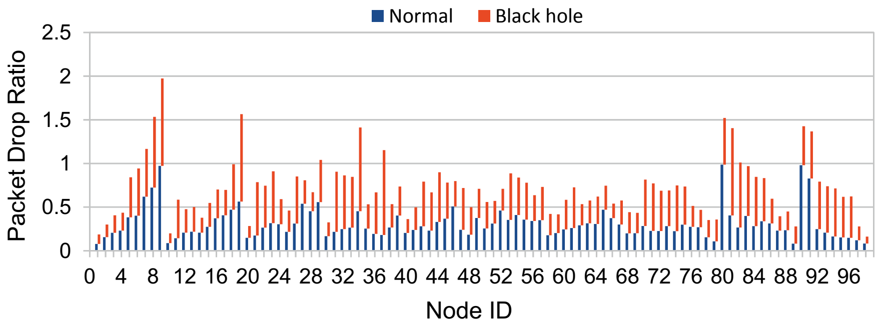


Fig. 6 Packet drop ratio versus node ID

Table 2 PDR and throughput with and without attack

No. of nodes	PDR	PDR with blackhole	Throughput	Throughput with blackhole
100	0.939671	0.901709	0.130594	0.038083
200	0.942738	0.864469	0.12708	0.02037
300	0.939394	0.891626	0.140837	0.032999
400	0.953842	0.920188	0.13592	0.031706
500	0.953842	0.920188	0.13592	0.031706

number of nodes in the network. But it gets affected by blackhole attack, and its value is dropped to large extent on adding malicious node. Figure 6 presents the packet drop ratio of each node in the network. From the graph, it can be seen that drop ratio of packet has increased after adding malicious node. Its effect can be seen in whole network (Table 2).

5 Conclusions

In this paper, we presume that because of self-configuring nature of the MANET much kind of inside and outside assaults are conceivable which debases the system performance. Among all the security assaults, blackhole attack is the most widely recognized and denial of service attack. We have simulated the blackhole attack in NS2 by modifying the current AODV protocol and results are analyzed graphically by taking different system parameters like throughput, packet delivery ratio and packet drop ratio of each node. We have additionally analyzed these parameters on differing number of nodes in the system. In the wake of analyzing the result, we found that because of single blackhole node present in the system, packet drop ratio for almost every hub is increased which debases the PDR value and throughput of the entire system.

Acknowledgements Working on this project on "Blackhole Attack Implementation and its Performance Evaluation using AODV Routing in MANET" was a source of immense knowledge to us. We would like to express our sincere gratitude to our guide Mrs. Nishi Yadav for her guidance and valuable support throughout the course of this project work. We acknowledge with a deep sense of gratitude, the encouragement and inspiration received from our faculty members and classmates.

References

1. Mirza S, Bakshi SZ (2018) Introduction to MANET. Int Res J Eng Technol 5(1)
2. Desai Piyusha P (2013) A study of secure routing in mobile ad-hoc networks. Int J Adv Res Comput Eng Technol 2(5)
3. Rashmi AS (2014) Detection and prevention of black-hole attack in MANETS. Int J Comput Sci Trends Technol 2(4)
4. Banwari DS, Upadhyay D (2013) Routing algorithms for MANET: a comparative study. Int J Eng Technol 2(9)
5. Kaur G, Kaur N (2014) Review of attacks on MANETS. Int J Innov Res Comput Commun Eng 2(6)
6. Madhuri K, Kasi Viswanath N, Usha Gayatri P (2016) Performance evaluation of AODV under black hole attack in MANET using NS2. In: International conference on ICT in business industry & government. IEEE. https://doi.org/10.1109/ictbig.2016.7892661
7. Ghonge M, Nimbhorkar SU (2012) Simulation of AODV under blackhole attack in MANET. Int J Adv Res Comput Sci Softw Eng. ISSN: 2277 128X
8. Kaur J, Singh B (2014) Detect and isolate black hole attack in MANET using AODV protocol. Int J Adv Res Comput Eng Technol 3(2)
9. Koujalagi A (2018) Considerable detection of black hole attack and analyzing its performance on AODV routing protocol in MANET (Mobile Ad Hoc Network). Am J Comput Sci Inf Technol 6(2)
10. Kalia N, Sharma H (2016) Detection of multiple black hole nodes attack in MANET by modifying AODV protocol. Int J Comput Sci Eng 8(5)

Enhancement of Security Using B-RSA Algorithm

Aman Gupta, Saurabh Gupta and Nishi Yadav

Abstract Cryptography is a scientific art which deals with the methods for changing over messages, data and information in some dynamically and haphazardly planned language of characters which are mixed up and not understandable for people or notwithstanding for a machine. While doing this, it is guaranteed that authorized frameworks and humans can recuperate the original message by validating their authentication. There are different calculations and strategies are proposed for cryptography purposes. This paper focuses on examination of two individual cryptographic calculation RSA and Blowfish, how they work and what will be the impact on security and speed if these two are converged into one hybrid calculation with appropriate modification. This paper presents the comparative analysis in terms of encryption and decryption time for individual as well as hybrid algorithm.

Keywords Cryptography · RSA · Blowfish · Encryption · Decryption · Symmetric and asymmetric key

1 Introduction

Technical innovations are getting advanced and spreading its wide region so fastly that at present we find ourselves doing each kind of the works by technical means. We are utilizing web not only for surfing the website pages but also for various daily to daily life works and needs like online shopping, cash exchange, secret military administrations, correspondence over social web media, and so forth. That is the reason there is have to utilize our own personal information for finishing undertakings like check card subtleties while online transactional exchanges. Consequently, we

A. Gupta (✉) · S. Gupta · N. Yadav
Department of C.S.E, Guru Ghasidas Central University, Bilaspur, India
e-mail: ag4cse@gmail.com

S. Gupta
e-mail: mohitsaurav12u@gmail.com

N. Yadav
e-mail: nishidv@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_42

need such security component which can guarantee that our information is secure and is spreading over web in an incomprehensible structure so that regardless of whether interloper gain admittance to the information by, in any case, it won't most likely comprehend the real data or information. Web itself don't represent accessing our data for utilization of danger, however, a few interlopers with expectations of mischief go over our information by unapproved implies. At this situation idea of system or network security in terms of cryptographic art come into the action. Cryptographic algorithms are not just in charge of changing over message into confused structure yet a decent and secure algorithm additionally gives the confirmation to essential objectives of system security. Essential objectives of network security are:

(i) Confidentiality, which guarantees getting to information just by approved elements means maintaining secrecy
(ii) Integrity, it manages the exactness part of the information and
(iii) Availability, which guarantees non-renouncement to the authentic clients.

Cryptography process revolves around certain terminologies. Original data which is intended to be send is called plain-text given as an input to the algorithm of cryptography. The yield of the calculation which is ambiguous coded structure information is called cipher-text. Conversion procedure of the plain-text into cipher-text is called encryption and switch is called as decryption. Cryptography algorithms can be further divided on basis of principles of processing data and keys also known as cipher keys.

Cryptographic strategies depend on two principles. On the off chance that each littlest individual unit of plaintext is mapped with another unit, at that point, it is called substitution and on the off chance that the units of plaintext are reordered, at that point, it is known as standard of transposition.

For encryption and decryption algorithms uses cipher keys which are the soul for any algorithm because methods are publicly known to everyone. The only thing that is meant to be secret is keys which drives the whole algorithm. When both sender and receiver use the same key for respective encryption and decryption process, it is called symmetric or private key cryptography and when two different keys are used by either side for encryption and decryption is known as asymmetric or public-key cryptography. Blowfish is one of the examples of symmetric type and RSA is asymmetric type of algorithm.

1.1 RSA

RSA is one of the broadly used asymmetric key kinds of cryptography algorithm. RSA remains as an abbreviation for the surname initials of the makers of this algorithm—Rivest, Shamir, and Adleman. RSA calculation utilizes the idea of considering factoring issue in number system as it finds as one of the basically troublesome problem. As indicated by this problem factorization of result of two huge prime numbers is by one way or another isn't a bread and butter case. And thus, this algorithm takes advantage of this problem to make itself much secure.

Steps involving in encryption and decryption of RSA algorithm are as follows.

1.1.1 Key Generation

(1) Choose any two dissimilar large random prime numbers say *i* and *j*.

(2) Calculate the value of *n* as product of *i* and *j*.

$$n = i * j$$

modulus operation of this algorithm will use the value of *n*.

(3) Totient function Φ "phi".

$$\Phi(n) = \Phi(i) * \Phi(j)$$
$$\Phi(n) = (i - 1) * (j - 1) \quad // \quad \Phi(k) = k - 1; \text{ if } k \text{ is prime.}$$
$$\Phi(n) = n - (i + j - 1)$$

(4) Select the value of public key (*e*) in such a way so that *e* is relative prime to Φ (*n*).

$$\gcd(e, \Phi(n)) = 1\{1 < e < \Phi(n)\}$$

Here ***e*** is our public key and pair (*e*, *n*) will use at encryption side.

(5) Compute the value of private key (*d*) such that congruence relation does exist.

$$d * e \equiv 1(\bmod \Phi(n))$$

Here ***d*** is our private key and pair (*d*, *n*) will use at decryption side.

(6) Encryption: Let plain-text at sender side is *M*. Receiver side public key (*n*, *e*) is known to everyone thus sender also knows. Private key *d* remains only up to receiver side. It is not meant to be shared.

(7) First, convert *M* into a number *m* (*m* < *n*) by using any pre-defined standards but is ensured that both sender and receiver is aware with that standard or protocol. And then finally cipher-text *c* is computed as.

$$c = m^{\mathrm{e}} \bmod n$$

Now, this cipher-text *c* is sent to receiver side.

(8) Decryption: To recuperate original message from ciphertext at receiver side it requires the private key of receiver *d*. Original message *m* is recovered as

$$m = c^{\mathrm{d}} \bmod n$$

For increasing the security of RSA one new approach was given in which four prime numbers were used and modulus operation was performed twice unlike conventional RSA. This method was named as D-RSA [1].

1.1.2 Key Generation in D-RSA [1]

(1) Modulus keys:

$$\mathrm{n1} = \mathrm{q1} * \mathrm{q2}\,\mathrm{and}\,\mathrm{n2} = \mathrm{r1} * \mathrm{r2}$$

(2) Totient function:

$$\Phi(\mathrm{n1}) = (\mathrm{q1} - 1) * (\mathrm{q2} - 1)$$
$$\Phi(\mathrm{n2}) = (\mathrm{r1} - 1) * (\mathrm{r2} - 1)$$

(3) Public keys (e1, e2):

$$\gcd(\mathrm{e1}, \Phi(\mathrm{n1})) = 1$$
$$\gcd(\mathrm{e2}, \Phi(\mathrm{n2})) = 1$$

(4) Private keys (d1, d2):

$$\mathrm{d1} * \mathrm{e1} \equiv 1\,(\mathrm{mod}\,\Phi(\mathrm{n1}))$$
$$\mathrm{d2} * \mathrm{e2} \equiv 1\,(\mathrm{mod}\,\Phi(\mathrm{n2}))$$

(5) D-RSA encryption:

$$c = \left(\left(m^{\mathrm{e1}} \bmod \mathrm{n1}\right)^{\mathrm{e2}} \bmod \mathrm{n2}\right)$$

(6) D-RSA decryption:

$$m = \left(\left(c^{\mathrm{d2}} \bmod \mathrm{n2}\right)^{\mathrm{d1}} \bmod \mathrm{n1}\right)$$

1.2 Blowfish

Blowfish is a kind of symmetric-key algorithm which finds its place as one of the very fast algorithms as well as it is very compact. Blowfish is structured by the

Bruce Schneier in year of 1993. This algorithm is openly accessible and unpatented algorithm. It is a sort of block cipher algorithm which encrypts plain-message as in 64-bit square sizes. One important feature of this algorithm is that it utilizes variable-length key up to 448 bits beginning from 32 bits. The soul of this algorithm is use of substitution boxes also called *S*-Boxes.

Steps involved in cryptography process of Blowfish algorithm:

This algorithm works in two sections; one that deals with key expansion phase and other one handles the main encryption process.

In key expansion phase subkeys are generated. For subkey generation steps:-

(1) First of all, keys are stored in 14 K—arrays (K1–K14) each of size 32 bit. In this way, variable-length key will have upper bound to 448 bits (14*32).
(2) Initialize *P*-array and *S*-boxes.
(3) Both are initialized with the hexadecimal values of "pi".
(4) There are 18 *P*-arrays each of 32 bit (P1–P18) and four *S*-Boxes each containing 256 entries of 32 bits.
(5) Now bitwise XOR operation is performed between *P*-arrays and 32-bit keys.

$$\mathrm{P1} = \mathrm{P1\,XOR\,K1}$$
$$\mathrm{P2} = \mathrm{P2\,XOR\,K2}$$
$$\mathrm{P14} = \mathrm{P14\,XOR\,K14}$$
$$\mathrm{P15} = \mathrm{P15\,XOR\,K1}$$
$$\mathrm{P18} = \mathrm{P18\,XOR\,K4}$$

(6) In this way, 64-bit plain text when passed through Blowfish encryption process, subkeys are generated by using above method. Subkeys are generated only when all the *P*-arrays and *S*-Boxes are replaced.

1.2.1 Encryption Phase

For encryption, plain-text is divided into block of 64 bits. Let one such block is named as *B*. Further, these 64 bits are divided into two equal blocks size of 32 bits and named as B_{L} and B_{R}.

First, 32 bits that is B_{L} are bitwise XORed with 32-bit P1 array. The output let *X* is now given to the *F*-function of Blowfish algorithm and the output of this function let *Y* is now again XORed with 32 bits of B_{R}. Now this output becomes the left part of the algorithm which will continue its XOR with next P2 array and the output of first XOR that is *X* now becomes the right part of the algorithm. This process continues 18 times as we have to XORed with all 18 *P*-arrays. After 18 rounds we get the ciphertext which will be of 64 bits in size equal to the input plain-text one block size (Figs. 1 and 2).

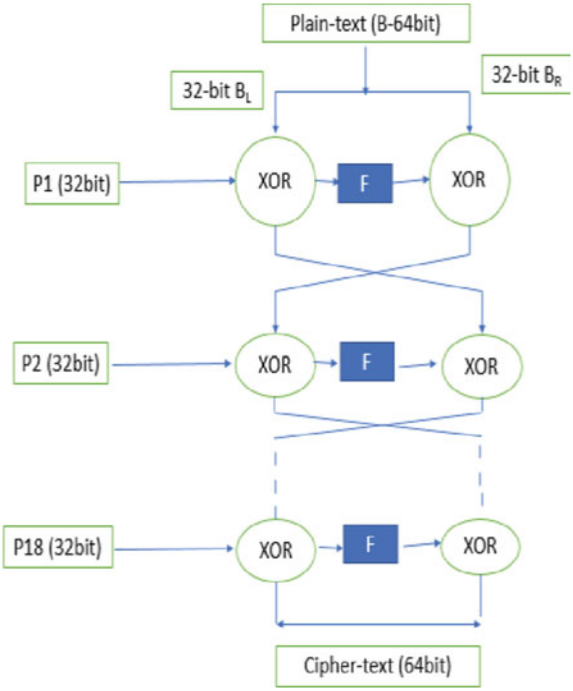


Fig. 1 Blowfish encryption

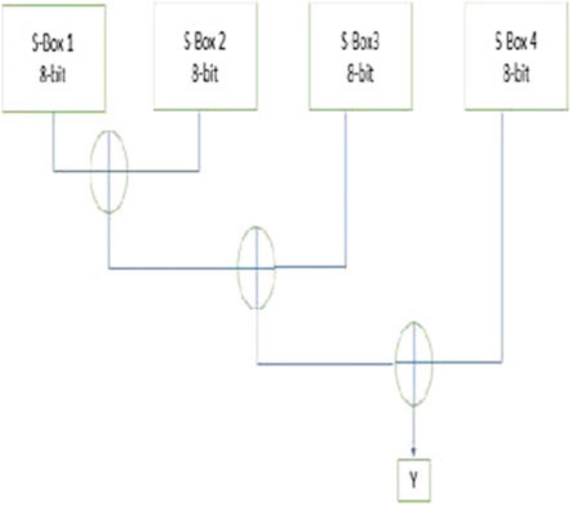


Fig. 2 *F*-function working

1.2.2 Working of *F*-Function

The output of B_L and P1 that is *X* which is first XOR now works as input to the *F* function. This *X* is now split into 4 equal parts of each 8 bits now given as input to the four *S*-boxes. Each *S*-box gets 8 bits and produces the output of 32 bit by using its substitution process. Output of *S*-box S1 is XORed now with S2 and output is again XORed now with S3 and finally their output is XORed with S4 and we get output as *Y* which will become the input to the XORed with B_R.

1.2.3 Decryption

For decryption phase, the reverse approach of encryption phase is applied. We start with the cipher-text and go up to plain-text while processing the 18 steps of XOR's with *P* arrays. And finally, 64-bit ciphertext is now converted into 64 bit of plain-text.

2 Literature Survey

In this paper [1] Ekka et al. proposed a hybrid algorithm of AES and RSA pursued by EX-OR activities. By doing this they reasoned that proposed plan takes lesser time in encryption stage than decoding stage, so security increments.

In this paper [2] Quilala et al. utilizes the Modified Blowfish algorithm for providing security to the Electronic Medical records. Authors did appropriate modification in original Blowfish algorithm to make EMR system more secure.

In this paper [3] Kaur and Singh utilizes the Blowfish algorithm for image encryption. Authors takes advantage of Random selective block encryption for Image encryption. Authors compared the encryption and decryption time of their algorithm with standard methods and find that results are better as compared to the previous.

In this paper [4] Manu and Goel used the RSA algorithm utilizing twofold encryption and twofold decoding utilizing twofold open and private keys to give security against Brute Force assault. This paper beats the shortcoming of customary RSA that is on the off chance that we can figure modulus its prime numbers, at that point private key will be in risk.

In this paper [5] Vasantha and Prasad proposed a half and half security algorithm for RSA cryptosystem. Here they processed public and private keys by utilizing four prime numbers. After that they looked at the different procedure times and speed with customary RSA.

In this paper [6] Panda and Chattopadhyay did their work on investigating and planning of upgraded RSA for enhancing the security by including the element of check at both sender and beneficiary side. They improved their work by utilizing K-NN calculation just as numerous public keys.

In this paper [7] Mathur et al. used the Blowfish algorithm for providing security aspects in internet of things. Authors slightly modified the original algorithm by changing in F-function of the algorithm and found that in terms of throughput and speed this algorithm significantly proved fruitful.

In this paper [8] Suresh and Neema used a hybrid algorithm for cloud computing. They selected RSA and Blowfish algorithm for this work. For implementation purpose, they used FPGA device. In this way authors provides one algorithm for data security at cloud computing level.

In this paper [9] Bansal and Singh performed the analysis part on basis of implementations of various symmetric key-based cryptography like Blowfish. Their basis for comparison involves three parameters what is the execution speed, size of block for processing and size of cipher keys.

3 Proposed Work

RSA algorithm which is public key algorithm on one side have favorable position of high security in view of complex factorization issue yet on other hand it gets moderate down in calculation with regards to the matter of encryption of bigger information. While Blowfish algorithm has preferred standpoint of one it is unpatented openly accessible to utilize algorithm and second it is one of the quickest block cipher algorithms in symmetric key algorithm.

Presently this paper introduces a half and half algorithm which is made by consolidating such two calculations with the goal that recently planned calculation will have forces of RSA as far as mind-boggling security and on other side quickness and unwavering quality of Blowfish calculation. This new algorithm is named as B-RSA.

3.1 B-RSA Encryption

This algorithm first takes plain-text as M. Then this message is first encrypted by blowfish algorithm using symmetric key process of this algorithm. All the intermediate process of these algorithms is applied starting from subkey generation and then splitting plaintext in 64-bit blocks and then all 18 rounds of XORed along with use of S-Boxes in F-function. And finally, message M is now in encrypted form that is ciphertext let C1. Now this ciphertext is used as a plain text for RSA algorithm. Here we use RSA algorithm of 4 prime numbers and dual modulus operation. Now this algorithm converts C1 into another ciphertext C2. And finally, original plaintext M is now in encrypted form as C2 by B-RSA algorithm.

3.2 B-RSA Decryption

For decryption phase at receiver side, the reverse approach of encryption phase is done. Ciphertext C2 is decrypted using dual modulus RSA algorithm. As a result of this we get the output as C1 which is still not our original plaintext. Now this Ciphertext C1 is decrypted by Blowfish algorithm decryption phase. After completing all the 18 rounds of XOR's in order of P18–P1 array we get the original plaintext as M by B-RSA algorithm.

3.3 Example

Let us take plain-text as "hello" which is meant to be encrypted. Let denote this message as *M*. first of all *M* is given as input to Blowfish algorithm phase of B-RSA.

Blowfish Symmetric key = ??6|(??6???¿ßÉ Cipher text C1 = z]ñz?H?+

Now, this C1 is becomes input to RSA algorithm with dual modulus. Ciphertext C1 in bytes = 12293-15122-104726343

Encrypted bytes by RSA phase = 76-16-23127-747-2121-51-71-96-45-52115-67-96-12329-139-71-101-10-101-5918-72-442-26-3123-1185911084-28-22-43109-646-77-2314-6995106-24108-10443-123-80-25-50-100-7248-71-120-476-31123-1210511132-994604279-10-54-7614-33-1124-731-10399109-8420-502359-10-12-96-3065-32-126-123-67-22313416704194-108-30-50-32-8-5-119126-22-72-399-10165-34-9764-120-105-7342-121-84-2-112-49-29-67-29-21-341-702-43-125-10 287619973541259111-1171-5229-42100-74119749-838111469591-9-19-126-110-23926-93-12083-86116-104-40-10910635653-42-8612537-100-62857-48-2648113-58-96-8127-96-49-99-3286-49-71-3654-12512-56-948-60119-10782-187815-30-37137-61113-9110192-9382-94-75-13126-149711973-54-7-664783 599109-79-10070-36

Now decryption phase starts. These encrypted bytes are now decrypted using RSA-decryption phase.

Decrypted string C1 = z]ñz?H?+

Now this C1 is gives as input to blowfish-decryption phase and we get our original plaintext as *M*.

M = "hello"

4 Simulation Work

In this paper, we discussed a new algorithm B-RSA which is hybrid of one symmetric and one asymmetric algorithm Blowfish and RSA respectively. Here we are comparing the Encryption and Decryption time of Blowfish algorithm with proposed B-RSA algorithm. We implemented these algorithms in java language and measured the execution time of these algorithm's encryption and decryption phase.

From Figs. 3 and 4 we can see that decoding time of B-RSA algorithm increments as contrast with the first blowfish calculation. It demonstrates that increase in decoding time will make B-RSA calculation substantially more secure towards assaults

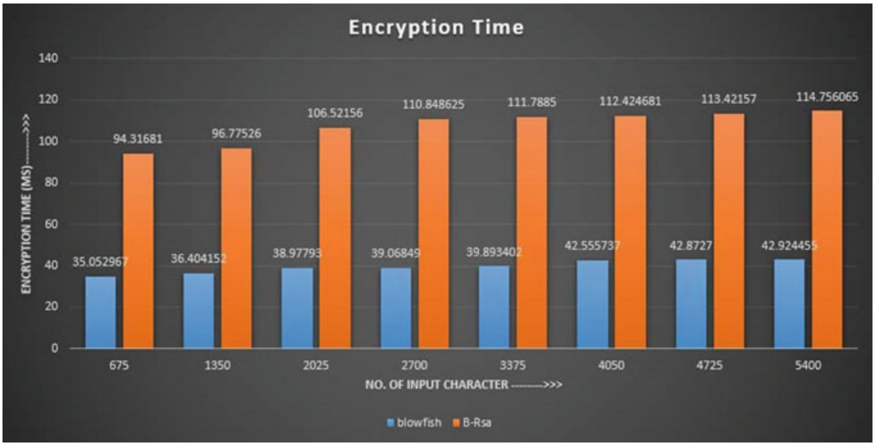


Fig. 3 Encryption time versus number of input character

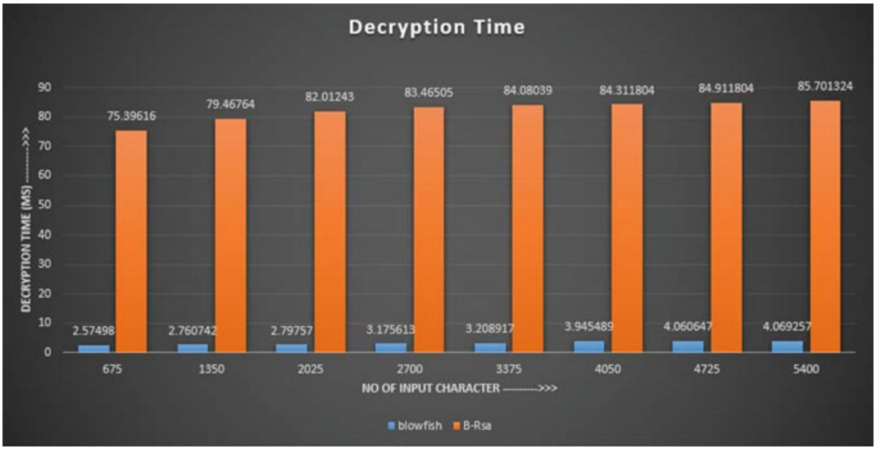


Fig. 4 Decryption time versus number of input character

on the system on the grounds that such mind-boggling and difficult to unscramble result upgrades the security as contrasted with blowfish algorithm. In same way we find that encryption time likewise expanded when contrasted with original blowfish algorithm. It is a direct result of the extra periods of RSA which are included into blowfish algorithm. On the off chance that there is need of making an increasingly secure system at expense of high handling time of encryption and decoding then parameters of RSA algorithm can be expanded like we can go to 6 prime numbers with triple modulus task. In this paper we utilized RSA of double modulus. Making triple modulus in action will make framework or system significantly more secure.

5 Conclusion

From the overall estimations, we presume that proposed B-RSA algorithm have the abilities of both RSA and Blowfish algorithm. Regardless of having perplexing and secure mechanism like double modulus RSA calculation, B-RSA is additionally quick block cipher calculation. Here we can say utilizing of B-RSA algorithm will be by one way or another different and significantly more difficult for gatecrashers to break the component of calculation of B-RSA algorithm. In this way we infer that B-RSA algorithm is such calculation which full-fill the prerequisites of a decent cryptographic algorithm having secure mechanism just as quick execution.

References

1. Ekka D, Kumari M Yadav N (2019) Enrichment of security using hybrid algorithm. In: International conference on computer networks and communication technologies, Springer, Singapore
2. Quilala TFG, Sison AM, Medina RP (2018) Securing electronic medical records using modified blowfish algorithm. Indonesian J Electr Eng Inf (IJEEI) 6(3):309–316
3. Kaur A, Singh G (2018) A random selective block encryption technique for secure image cryptography using blowfish algorithm. In: Proceedings of the 2nd international conference on inventive communication and computational technologies (ICICCT 2018)
4. Manu and Goel A (2017) In: 3rd IEEE international conference on computational intelligence and communication technology (IEEE-CICT 2017), ABES engineering college Ghaziabad, India
5. Vasantha R, Prasad RS (2017) An advanced security analysis by using blowfish algorithm. Int J Sci Res Comput Sci Eng Inf Technol 2017
6. Panda PK, Chattopadhyay S (2017) A hybrid security algorithm for RSA cryptosystem. In: International conference on advanced computing and communication system (ICACCS-2017), Coimbatore, INDIA, 2017
7. Mathur S, Gupta D, Goar V, Kuri M (2017) Analysis and design of enhanced RSA algorithm to improve the security. In: 3rd IEEE international conference on computational intelligence and communication technology (IEEE-CICT 2017)

8. Suresh M, Neema M (2016) Hardware implementation of blowfish algorithm for the secure data transmission in internet of things. In: Global colloquium in recent advancement and effectual researches in engineering, science and technology (RAEREST 2016)
9. Bansal VP, Singh S (2015) A hybrid data encryption technique using RSA and blowfish for cloud computing on FPGAs. In: Proceedings of 2015 RAECS. UIET Panjab University Chandigarh 21–22nd December 2015

Analyzing Different Multiparty Computation Techniques

Tanmay Borade, Dhananjay Dakhane and Tushar Ghorpade

Abstract Strong encryption provides support to data privacy. Although encryption can make the data secure in data transfer and at rest, at some point this encrypted data definitely needs to be decrypted. Now at this very point, it so happens that the data becomes susceptible to attacks ultimately resulting in compromised data privacy. This is where secure multiparty computation (MPC) comes into picture; thereby, it provides ability to calculate required values from numerous encrypted data sources without any party compromising on their secret data. At ground level, MPC is a very general concept that can be realized using different protocols, such as secret sharing, in which secret data from each party is divided and then distributed randomly, encrypted "shares" among the parties. This distributed data when eventually aggregated would provide the final desired result. If anyone happens to intersect the data at hand of any of the parties, it would prove futile. With this paper, we focus on different algorithms or techniques that work behind the scenes in implementing MPC. These techniques include homomorphic encryption, followed by RSA combined with Paillier's algorithm and lastly the concept of garbled circuits.

Keywords Multiparty computation · Homomorphic encryption · Garbled circuits · Paillier's algorithm

T. Borade (✉) · D. Dakhane · T. Ghorpade
Ramrao Adik Institute of Technology, Navi Mumbai, India
e-mail: tanny.wassup@gmail.com

D. Dakhane
e-mail: ddakhane@gmail.com

T. Ghorpade
e-mail: tushar.ghorpade@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_43

1 Introduction

With the advent of modern world technology, today's world revolves around data. This data is sent over a global-wide network; hence, the network security and analysis have become very prime importance for any large organization or establishment. Computers today are involved in large money transfers between banks, IT industries, stock markets, electronics and telecommunication industries, railway and rail services, schools and colleges, satellites and space research, etc. In such crucial areas, security cannot be compromised. Networks could be susceptible to attacks like Phishing, Eavesdropping, DOS and DDOS attacks, and Man-in-the-middle attack. To prevent all of this, network security is essential. Cryptography essentially means converting just an ordinary plain text into scrambled and clueless text and vice versa.

A. Secure Multiparty Computation

The term "multiparty computation" was coined by Yao [1], arguably regarded as the most fundamental problem in cryptography. Being a powerful abstraction, it can model any cryptographic task. The problem shown in Fig. 1 is defined as follows: We have a set of n distrusting parties {P1,…,Pn}, each with its own private input x1,…, xn. They want to compute some publicly known function *f* on their inputs without disclosing their inputs. The approach used by a generic secure computation

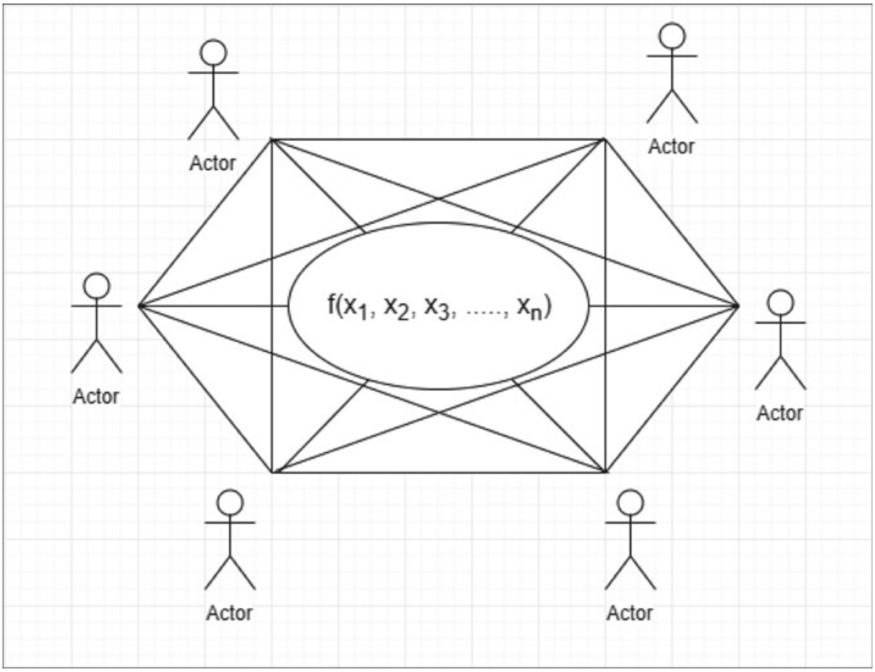


Fig. 1 A generalized scenario of secure MPC

protocol is to "securely" evaluate Boolean circuit (with AND, OR, XOR gates) or arithmetic circuit (with + or * operator) representing the function f to be computed. By "secure circuit evaluation," we mean that the circuit will be evaluated in such a way that nothing other than the circuit output that represents the function output must be revealed during the circuit evaluation.

B. Yao's Millionaire Problem

Yao's millionaires' problem [2] is a secure multiparty computation problem given by Andrew Yao which came into light in 1982. The problem involves two millionaires, say, Alice and Bob, who want to ascertain who is richer. The condition is that they should not reveal their true wealth. This complication is very similar to another problem that has two numbers a and b, and the goal is to solve the inequality $a >= b$ without exposing the definite values of a and b.

2 Related Work

Rani et al. [3] explain the fourth challenge of big data, that is, Veracity, which means how much trustworthy is the data, how securely is the data received, stored, processed, and transmitted. Zhenlin et al. [4] aim at constructing a predicate encryption having multiplicative homomorphic property for the class of inner-product predicates. Yao et al. [5] propose a protocol based on homomorphic encryption which allows function input to be encrypted with various public keys. Based on ECC for SMC problem, Wang et al. [1] present a homomorphic encryption scheme that results in reduced communication and computation cost. Yao [2] in his paper presents a new mechanism for regulating the knowledge transfer process in cryptographic protocol design. Dhakar and Gupta [6] point out the loopholes in RSA cryptosystem: factoring huge numbers by mathematical attack and, with brute force, trying all private keys. Xiang et al. [7] define a new operation—similar modular arithmetic which can be used to achieve algebraic homomorphic encryption scheme on the scope of a rational. Youn et al. [8] put forth an additive HE scheme, used for calculating statistical data such as mean and variance. Naumann [9] in this paper has explained the function of Yao's original algorithm in detail. Snyder [10] in his paper gives a thorough and detailed answer of Yao's original protocol and its security characteristics. Cimato et al. [11] in his paper put forth the technique of using multiple-valued logic for the forming garbled circuits. Ehsanpour [12] in his paper discusses constructing garbled circuit for two parties to securely evaluate a function by means of quantum gates (QG).

3 Multiparty Computation Techniques

3.1 Multiplicative Homomorphic Encryption Along with Secure MPC

Encoding:

1. Padding of the message is done with k1 zeros to be *n*—k0 bits in length.
2. *r* is just any k0-bit string that is randomly generated.
3. *G* expands the k0-bits of *r* to *n*—k0 bits.
4. Evaluate *X* as

$$X = \text{m}000\ldots0 \oplus G(r) \tag{1}$$

5. *H* reduces the *n*—k0 bits of *X* to k0 bits.
6. Calculate *Y* as

$$Y = r \oplus H(X) \tag{2}$$

7. Finally, the result is calculated as *X*||*Y*.

Decoding:

1. First, find *r* as

$$r = Y \oplus H(X) \tag{3}$$

2. Second, recover *m* as

$$\text{m}000\ldots0 = X \oplus G(r) \tag{4}$$

Algorithm for Secure Cloud Computing:

At first, padding of the user's data takes place by Optimal Asymmetric Encryption Padding (OAEP) as shown in Fig. 2, combined with hybrid encryption technique based on RSA algorithm (HE-RSA). Multiple parties wish to work out a function upon their personal inputs without compromising on correctness and secrecy. Encrypted data is homomorphically encrypted. This double encrypted data is not decrypted in cloud. The algorithm [13] incorporates the MPC along with HE that follows evaluations to be done on encrypted data without decrypting it. After combining homomorphic encryption and multiparty computation (HE + MPC), the confidentiality and integrity of the data are preserved without any compromise. The latency is lesser than HE but more than MPC. The algorithm thereby gives medium amount of latency based on the HE and MPC.

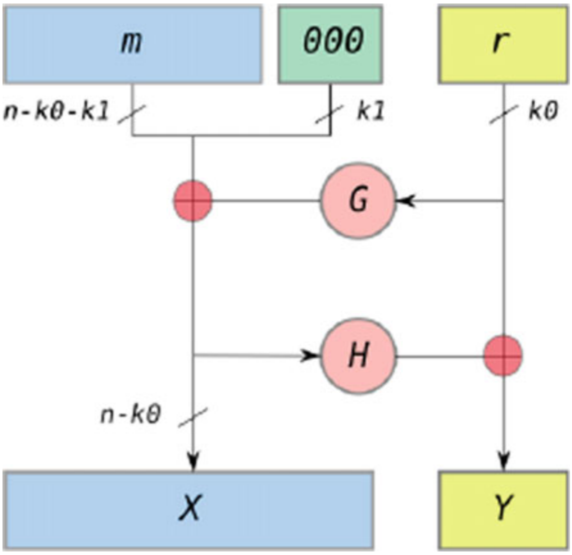


Fig. 2 Optical asymmetric encryption padding

3.2 Additive Homomorphic Encryption with Paillier's Algorithm

Key Generation:

1. Let p and q be any two large primes.
2. Compute the modulus as

$$n = p * q \tag{5}$$

3. Calculate the Carmichael function

$$\lambda = \text{LCM}(p - 1, q - 1) \tag{6}$$

and

$$g = 1 + n \tag{7}$$

4. Calculate

$$L_1 = L(g^{\lambda} \bmod n^2) \tag{8}$$

5. Calculate

$$\mu = 1 + K.\frac{n}{L_1} \tag{9}$$

Thus, public key is (n, g)
private key is (λ, μ)

Encryption:

For any plaintext m, choose a random $r \in \mathrm{Zn}_2^*$, calculate

$$c = g^{\mathrm{m}} * r^{\mathrm{n}} \bmod n^2 \tag{10}$$

Decryption:

1. For ciphertext $c <= n^2$, calculate

$$L_2 = L(c^{\lambda} \bmod n^2) \tag{11}$$

2. Finally, calculate the plaintext from ciphertext as:

$$m = \left[\frac{L_2}{L_1}\right] \bmod n \tag{12}$$

or

$$m = L_2 * \mu \bmod n \tag{13}$$

Actual Implementation:

Suppose a number of hospitals wish to jointly evaluate total number of people suffering from a certain disease without revealing any secretive or private information of the concerned patients. Here, security is the key factor that should definitely be taken into consideration. In fact, information in medical field is mostly secretive kind of data that should be kept confidential. To accomplish this, there is a need of secure framework that will collaborate between various hospitals. The solution to this forms the secure MPC technique.

With that in mind, after successful encryption each hospital sends their secretive data for evaluations. Then the cloud provider does the computation work on encrypted data and forwards the final result back to the hospitals. After this, every hospital then decrypts this newly received encrypted data using their secret key to yield the final result. This way the parties are aware only of the final output but not aware of the individual inputs thus confidentiality prevails. So, this method [14] permits a number of hospitals to together evaluate a function of their secretive inputs without sharing patients' crucial info to third parties.

In this scheme, hospital A and hospital B encrypt patients' secretive data m1 and m2 to yield the ciphertexts $C1$ and $C2$ using public key pk. So,

$$C1 = E(m1, \text{pk})) \tag{14}$$

$$C1 = g^{m}1 * r1^{\text{n}} \bmod n^2 \tag{15}$$

$$C2 = E(m2, \text{pk}) \tag{16}$$

$$C2 = g^{m}2 * r2^{\text{n}} \bmod n^2 \tag{17}$$

Here, cloud provider evaluates the product of the encrypted data just like RSA.

$$C1\,.\,C2 = E(m1, \text{pk})\,.\,E(m2, \text{pk}) \tag{18}$$

$$C1\,.\,C2 = (g^{m1} * r1^{\text{n}})\,.\,(g^{m2} * r2^{\text{n}}) \bmod n^2 \tag{19}$$

$$C1\,.\,C2 = g^{m1+m2} * (r1\,.\,r2)^{\text{n}} \bmod n^2 \tag{20}$$

$$C1\,.\,C2 = E(m1 + m2, \text{pk}) \tag{21}$$

Eventually, every medical asylum uses its secretive key to get last result, which equals the sum of m1 and m2.

$$D(E(\text{m1}, \text{pk})\,.\,E(\text{m2}, \text{pk})(\text{mod}\, n^2)) = \text{m1} + \text{m2}(\text{mod}\, n) \tag{22}$$

Together a number of hospitals perform addition operation on encrypted data. To sum it up as a whole, the solution securely evaluates addition operations. Hence, it is a effective method to assist collaborative systems in healthcare systems.

3.3 Garbled Circuits Using Quantum Gates

In Yao's GBC, the evaluating function is depicted as a Boolean circuit made up of binary gates. Encryption is then done of input and output wires such that the person or machine evaluating the GBC does not find any information regarding inputs. With GBC consisting of simple Boolean circuits, researchers found out that overall OT payload shoots up proportionally with the number of gates and become tremendous for complex GBCs [15]. So researchers were keenly fascinated in making a GBC that would require a meager number of non-EX-OR gates. An idea of increasing the

Table 1 Comparison of gates required

Version	Comparator(4-bit)	Comparator(8-bit)	Adder(32-bit)
Garbled circuit	10	26	127
Quantum garbled circuit	8	16	64

efficiency is incorporating quantum gates in place of Boolean ones thereby forming Q-GBC. The main motive behind is that the Q-GBC technique will increment the number of XOR gates without any communication delay and computation latency and lessen the number of non-XOR gates, thereby demanding meager interaction.

Quantum garbled circuit for comparison function:

With classical Boolean circuits, it is found that for 4-bit comparator circuit, the number of non-XOR gates is 10, whereas in case of 8-bit comparator circuit, the number of non-XOR gates comes out to just 26. According to RevKit result, each TR gate has got 1 CNOT and 1 Toffoli gate [12]. So we conclude that for implementing a 4-bit comparator circuit, we need just 8 non-XOR gates while for 8-bit millionaire problem with QC we need just 16 TR and 16 non-XOR gates.

Quantum garbled circuit for 32-bit adder:

With classical Boolean circuit of adder, a 32-bit adder GC has 127 AND, 187 INV, and 61 XOR gates. Peres FA gates are utilized as quantum full adder which are implemented by two quantum Peres gate. Additionally, a 32-bit adder forms an array of 32 PFAG. Hence, it can be said that a 32-bit adder can be realized as a GC that needs only 64 non-XOR gates (Table 1).

4 Comparative Analysis of Techniques

See Table 2

5 Conclusion

Nowadays secure multiparty computation is the trendy topic in the field of network security and cryptography. With secure MPC, it is no longer needed to trust the third parties. Thus by eliminating the third party, multiple parties can come together to evaluate some common function f over a cloud environment. The idea of having a secure MPC is quite old but the research still continues, and there are still many things yet to be explored in this regard. Thus, we have studied different techniques of multiparty computation. We compared the different algorithms and techniques such as multiplicative HE with OAEP, additive HE with Paillier's scheme, and garbled

Table 2 Comparison of MPC techniques

Parameters	Multiplicative HE + MPC	Additive HE + Paillier's algorithm	Garbled circuits
Confidentiality	Confidentiality is maintained	Confidentiality is maintained	Confidentiality is maintained
Integrity	Integrity is maintained	Integrity is maintained	Integrity is maintained
Overhead	Overhead is moderate	Overhead is less	Overhead is less
Algorithm or technique used	Multiplicative homomorphic encryption and OAEP technique	Additive homomorphic encryption and Paillier's scheme	Using quantum gates in garbled circuits
Advantages	Overhead lies in between only HE and only MPC	Productive technique to do computation even in distributed circumstances	Lesser non-EXOR gates employed which means lesser overhead
Limitations	Not fully homomorphic, only multiplication operations can be performed	Not fully homomorphic, only addition operations can be performed	Difficult to implement with the existing technology

circuits using quantum gates. Comparative analysis of the algorithms states limitation and advantage of individual algorithm. Secure MPC is undisputedly the future and would definitely be prominent among all kinds of organizations.

References

1. Hong MQ, Zhao WB, Wang PY (2016) Homomorphic encryption scheme based on elliptic curve cryptography for privacy protection of cloud computing. In: 2016 IEEE 2nd international conference on big data security on cloud, IEEE international conference on high performance and smart computing, IEEE international conference on intelligent data and security
2. Yao A (1986) How to generate and exchange secrets. In: 27th annual symposium on, foundations of computer science 1986, IEEE, pp 162–167
3. Rani PS, Vigneswari D (2016) Security and privacy in big data analytics. Int J Intell Electron Syst 10(2) July
4. Zhenlin T, Wei Z (2015) A Predicate encryption scheme supporting multiparty cloud computation. In: 2015 international conference on intelligent networking and collaborative systems
5. Yao Y, Wei J, Liu J, Zhang R (2016) Efficiently secure multiparty computation based on homomorphic encryption. In: proceedings of CCIS 2016
6. Dhakar RS, Gupta AK (2012) Modified RSA encryption algorithm (MREA). In: 2012 second international conference on advanced computing & communication technologies
7. Xiang G, Cui Z (2012) The algebra homomorphic encryption scheme based on Fermat's Little Theorem. In: 2012 international conference on communication systems and network technologies

8. Youn TY, Jho NS, Chang KY Practical additive homomorphic encryption for statistical analysis over encrypted data
9. Naumann F (2016) Garbled circuits. In: Seminar Innovative Internet-Technologien und Mobilkommunikation SS2016
10. Snyder P Yao's Garbled circuits: recent directions and implementations
11. Cimato S, Ciriani V, Damiani E, Ehsanpour M A multiple valued logic approach for the synthesis of garbled circuits
12. Ehsanpour M (2017) Toward design of garbled circuits using Quantum gates. In: 2017 IEEE 41st annual computer software and applications conference
13. Das D (2018) Secure cloud computing algorithm using homomorphic encryption and multiparty computation. International Symposium on Networks and Security Systems, Delhi, India
14. Marwan M, Kartit A, Ouahmane H Applying secure multi-party computation to improve collaboration in healthcare cloud
15. Ehsanpour M, Cimato S, Ciriani V, Damiani E (2017) Exploiting Quantum gates in secure computation. In: 2017 Euromicro conference on digital system design

Power and Delay Comparison of 7:3 Compressor Designs Based on Different Architectures of XOR Gate

Rekib Uddin Ahmed and Prabir Saha

Abstract This paper presents the power and delay comparison of 7:3 compressor circuit designed using three different architectures of XOR gate which are based upon mirror circuit, 4-transistor, (4-T) and transmission gate (TG). The compressors have been implemented in transistor level at 180 nm technology and the functionality is verified in Cadence-spectre. Among the 7:3 compressors, the design utilizing the TG-based XOR gate is exhibiting least power consumption and the least delay is exhibited by the design which is based upon mirror circuit-based XOR gate.

Keywords Compressor · Delay · Mirror circuit · Power · Transmission gate

1 Introduction

In microprocessors and digital signal processors, the multipliers are used to perform dedicated operations like convolution, correlation, and filtering. The multiplication process involves formation of partial products followed by addition of partial products in order to generate the final binary result. Among the process involved in multiplication, the addition of partial products is the main cause of the delay, area, and power consumption in the multipliers. Conventionally, addition of partial products was performed by huge numbers of adders that are capable to add two or three bits at a time [1]. One of the methods to minimize the number of adders is the use of compressors. Compressors are the basic circuits which count the number of "ones" present in the input vector. Different types of compressors like 3:2, 4:2, and 5:2 have been reported in literature [2–5] which are suitable for 8 × 8 bit multiplier. Large-sized compressors such as 7:3 and 15:4 compressors are also proposed in order to design 16 × 16 and 32 × 32 bit multiplier [1, 6, 7]. One important component used in the compressors is XOR gate, which is also the building block in various circuits

R. U. Ahmed (✉) · P. Saha
National Institute of Technology Meghalaya, Shillong, India
e-mail: rekib@nitm.ac.in

P. Saha
e-mail: sahaprabir1@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_44

like adder, parity checker, etc. While implementing in XOR gate in CMOS, the main intention is to reduce its transistor count aiming at reducing the overall delay and area of the constituting circuit [8]. Various CMOS architectures of XOR gate have been proposed [9] in order to obtain faster and more compact circuit structures. In this paper, the 7:3 compressor [10] is designed by utilizing three different architectures of XOR gate: (1) mirror circuit-based (2) 4-transistor (4-T)-based, and (3) transmission gate (TG)-based. The compressor circuits are implemented at gate level using the generic process design kit (gpdk) −180 nm technology node. The functionality of the compressors is verified through simulation in Cadence-spectre and the comparison between the designs as the function of power and delay is presented.

2 The 7:3 Compressor

A 7:3 compressor takes seven-bit input vector $X = (x_6, x_5, x_4, x_3, x_2, x_1, x_0)$ and generates three-bit output vector $q = (q_2, q_1, q_0)$. In order to obtain the Boolean expressions for the q, the X is partitioned into two sub-vectors $X_a = (x_2, x_1, x_0)$ and $X_b = (x_6, x_5, x_4, x_3)$. The truth tables for X_a and X_b are given in Tables 1 and 2.

The Boolean expressions for outputs of X_a are given by

$$q_{a1} = x_2x_1 + x_2x_0 + x_1x_0 \tag{1}$$

$$q_{a0} = (x_2 \oplus x_1 \oplus x_0) \tag{2}$$

Similarly, the Boolean expression for outputs of X_b is as follows (The simplification of q_{b1} is given in Appendix)

$$q_{b2} = x_6x_5x_4x_3 \tag{3}$$

Table 1 Truth table for sub-vector X_a

x_2	x_1	x_0	q_{a1}	q_{a0}
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

Table 2 Truth table for sub-vector X_a

x_2	x_2	x_2	x_2	q_{a1}	q_{a1}	q_{a1}
0	0	0	0	0	0	0
0	0	0	1	0	0	1
0	0	1	0	0	0	1
0	0	1	1	0	1	0
0	1	0	0	0	0	1
0	1	0	1	0	1	0
0	1	1	0	0	1	0
0	1	1	1	0	1	1
1	0	0	0	0	0	1
1	0	0	1	0	1	0
1	0	1	0	0	1	0
1	0	1	1	0	1	1
1	1	0	0	0	1	0
1	1	0	1	0	1	1
1	1	1	0	0	1	1
1	1	1	1	1	0	0

$$q_{b1} = [x_6x_5 + x_4x_3 + (x_6 + x_5)(x_4 + x_3)]\overline{q_{b2}} \tag{4}$$

$$q_{b0} = (x_6 \oplus x_5 \oplus x_4 \oplus x_3)$$

The outputs of two sub-vectors are added through a carry-lookahead (CLA) adder in order to obtain the final expression for the outputs of the 7:3 compressor.

$$q_2 = q_{b2} \oplus [q_{a1}q_{b1} + (q_{a1} \oplus q_{b1})(q_{a0}q_{b0})] \tag{5}$$

$$q_1 = q_{a1} \oplus q_{b1} \oplus (q_{a0}q_{b0}) \tag{6}$$

$$q_0 = (q_{a0} \oplus q_{b0}) \tag{7}$$

The gate-level logic diagram of the outputs q_2, q_1, and q_0 is shown in Fig. 1. The XOR operations used in the 7:3 compressor are implemented using three different architectures of XOR gate which are discussed below.

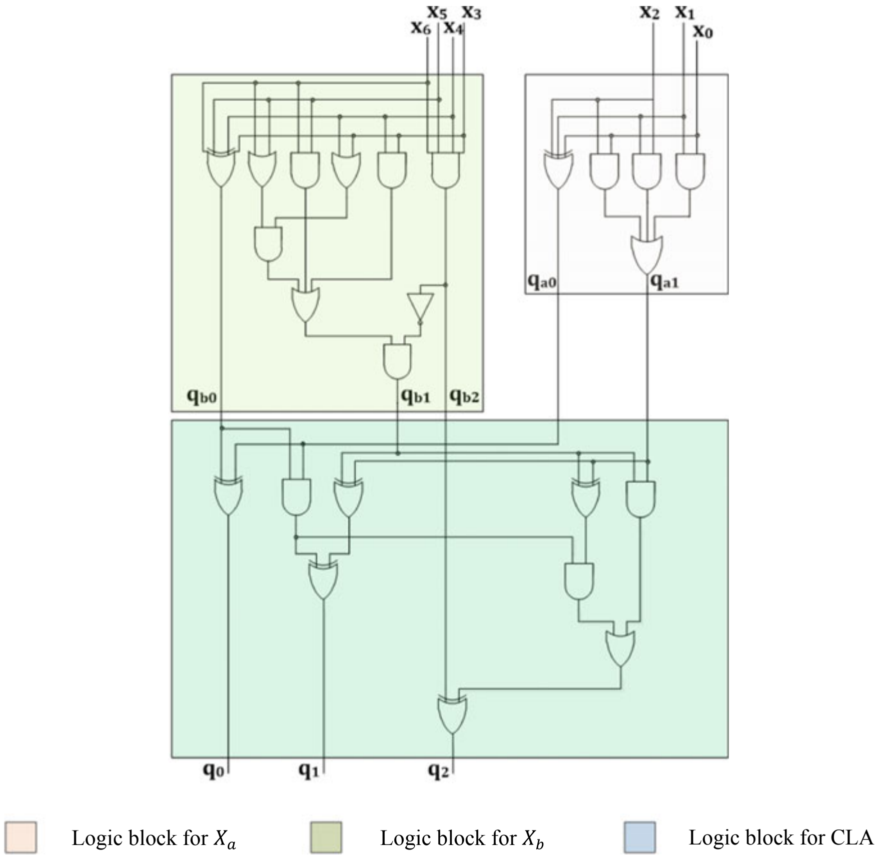


Fig. 1 Logic diagram for the outputs of the 7:3 compressor circuit

2.1 Mirror Circuits-Based XOR Gate (Design 1)

Figure 2a shows the CMOS XOR gate which is based on the concept of mirror circuit. With the two inputs A and B, the possible combinations are: AB, $\overline{\text{A}}$B, A$\overline{\text{B}}$, $\overline{\text{A}}\,\overline{\text{B}}$. The $\overline{\text{A}}$B and A$\overline{\text{B}}$ provide connections from the power supply to Y thereby producing the output high (V_{dd}), while AB and $\overline{\text{A}}\,\overline{\text{B}}$ connect the Y to the ground giving output low (0 V).

2.2 4-Transistor XOR Gate (Design 2)

The 4-T XOR gate consists of two CMOS inverters cascaded together as shown in Fig. 3 with input A applied to the first stage inverter (inverter 1), and connected to

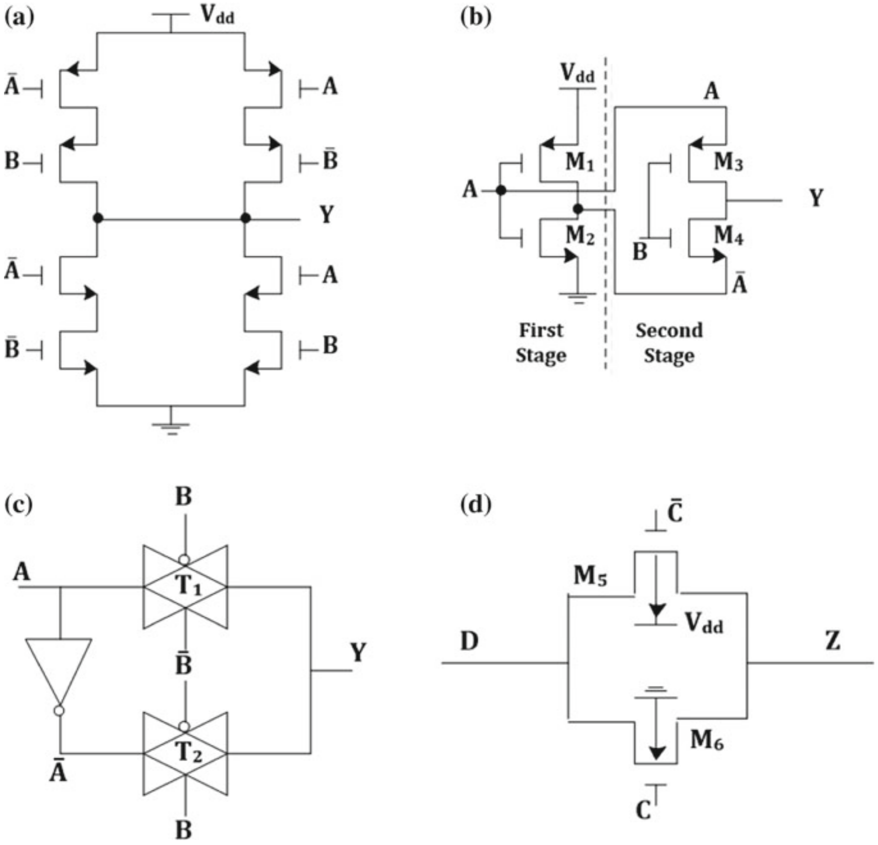


Fig. 2 Different architectures of XOR gate: **a** mirror circuit-based, **b** 4-transistor-based, **c** TG-based, and **d** TG

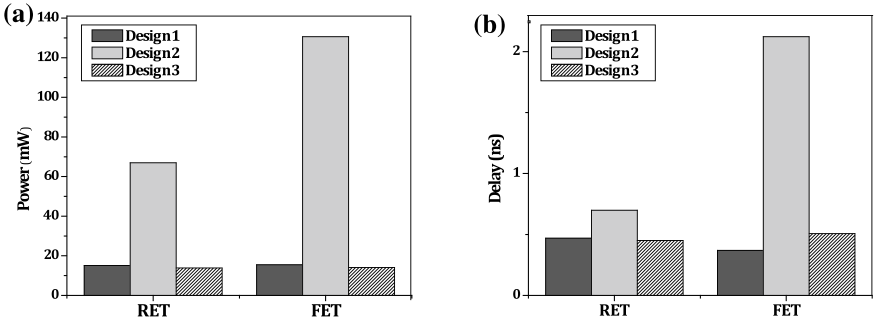


Fig. 3 Bar chart showing comparison between the compressor designs: **a** power analysis, **b** delay analysis

the top of second stage inverter (inverter 2). The $\overline{A}$ from inverter 1 is applied to the bottom of inverter 2. The other input B is used to switch the MOSFET pairs M_3 and M_4. With $B = 0$, M_3 conducts and the logic level at A is transferred to the Y thus producing the term $\mathrm{A\overline{B}}$. If $B = 1$, M_4 conducts thereby connecting $\overline{A}$ to Y, giving $\overline{A}B$. Combining these two gives the function: $\mathrm{A\overline{B}} + \mathrm{\overline{A}B} = A \oplus B$.

2.3 Transmission Gate-Based XOR Gate (Design 3)

The XOR gate can be implemented by using one of the input variables to control the TG. Figure 2c shows the XOR gate implementation using two TGs (T_1 and T_2) where the input B is used to control the TGs with A and $\overline{A}$ as inputs. The transmission gate (TG), sometimes referred as solid-state switch which selectively blocks or passes a logic level from the input to the output. The TG as shown in Fig. 2d is comprised of p-type (M_5) and n-type (M_6) MOSFETs. The gates of M_5 and M_6 are biased in such a manner so that both MOSFETs are either ON or OFF simultaneously. When the voltage at node C is at logic 1, the complementary logic 0 is applied to node $\overline{C}$, allowing both M_5 and M_6 to conduct and pass the logic level at D to Z. When voltage on node $\overline{C}$ is at logic 1 and logic 0 is applied to node C, the both transistors OFF thereby forcing a high impedance condition across D and Z.

3 Results and Discussion

The 7:3 compressor designs are simulated in Cadence-spectre and compiled with gpdk 180 nm technology considering device parameters: channel length $L = 180\text{nm}$, channel width $W = 1.08\,\mu\text{m}$, source and drain (S/D) diffusion area $= 0.972\,\mu\text{m}^2$ and S/D diffusion periphery $= 3.96\,\mu\text{m}$. The compressor designs are simulated under supply voltage of 1.8 V with input pulses of amplitude 1.8 V having rise and fall time $= 10\,\text{ps}$ of time period 20 ns.

The power dissipation and delay of the compressor designs are recorded at rising edge (RET) and falling edge transition (FET) of input pulses. The power and delay observed for some set of selected set of input combinations are given in Tables 3 and 4.

Figure 3 shows the pictorial representation of average power dissipation and delay exhibited by three compressor designs. The least power dissipation is exhibited by the Design 3 which utilized the TG-based XOR gate. As it has been stated earlier that TGs are inherently low power consuming and they are good for designing XOR gate [11, 12], so the Design 3 is exhibiting a minimum power dissipation of 13.84 µW at RET and 14.09 µW at FET. On the other hand, the rise and fall time of mirror circuit-based XOR gate are shorter [9], so the Design 1 is exhibiting a minimum delay of 0.4701 ns at RET and 0.3698 ns at FET. While the 4-T XOR gate is useful in reducing the transistor count but from power dissipation and delay point of view, it

Table 3 Power dissipation (in μW) at different combinations of *X*

X	Design 1		Design 2		Design 3	
	RET	FET	RET	FET	RET	FET
1111111	16.52	17.63	28.38	103.0	12.57	15.29
1111110	13.49	14.65	26.62	45.24	11.69	14.12
1011111	17.73	17.86	85.99	158.5	16.49	16.4
1010111	14.06	13.22	111.2	129.3	16.06	14.31
1010101	11.61	12.44	100.1	159.4	14.57	13.36
1010000	7.553	7.981	21.15	98.13	8.262	7.22
1111101	14.92	16.8	61.03	133.2	12.4	14.56
1111011	15.18	16.75	53.79	133.4	11.53	13.92
1110111	18.02	17.44	82.43	158.7	17.04	16.44
1101111	18.57	17.59	81.43	159.3	16.01	14.73
0111111	18.26	17.97	84.19	159.0	15.63	14.66
Average	15.08	15.48	66.93	130.65	13.84	14.09

Table 4 Delay observed (in ns) at different combinations of *X*

X	Design 1		Design 2		Design 3	
	RET	FET	RET	FET	RET	FET
1111111	0.4018	0.479	0.4081	1.6563	0.3124	0.5381
1111110	0.4747	0.479	0.5041	1.1679	0.4384	0.5324
1011111	0.5268	0.2895	0.6976	2.5549	0.4678	0.4846
1010111	0.3369	0.2668	1.5546	1.6573	0.5419	0.4849
1010101	0.2956	0.2631	1.008	2.4842	0.5492	0.4892
1010000	0.5223	0.4681	0.5437	1.1789	0.4775	0.5191
1111101	0.465	0.4802	1.0076	2.4968	0.4117	0.5373
1111011	0.4542	0.4818	0.4903	2.5196	0.3659	0.5427
1110111	0.5601	0.285	0.4062	2.5176	0.4687	0.4846
1101111	0.5837	0.2858	0.7026	2.537	0.4613	0.485
0111111	0.5502	0.2895	0.7671	2.5844	0.4604	0.4851
Average	0.4701	0.3698	0.6985	2.123	0.4504	0.5075

does not seem to be advantageous. So, Design 2 is showing maximum delay (2.123 ns at FET) and power consumption (130.65 μW at FET) as compared to Design 1 and Design 3.

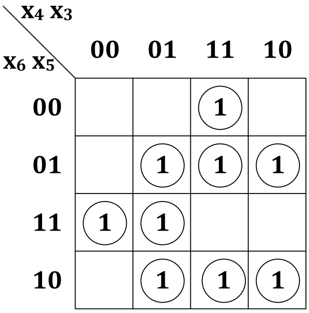
4 Conclusion

In this paper, 7:3 compressor designs have been presented by utilizing the mirror circuit, 4-T, and TG-based XOR gates. The functionality of the designs is verified and comparative study with respect to power and delay have been presented. Maximum average power dissipation and delay is observed in case of 4-T XOR gate-based compressor (Design 2). Least average power dissipation and delay is observed in the compressor utilizing the TG-based XOR gate (Design 3). The performance of Design 3 is found better among the discussed designs of 7:3 compressor.

Acknowledgements This work is supported by Ministry of Electronics and Information Technology, Government of India, under Visvesvaraya Ph.D. Scheme.

Appendix

The Karnaugh map for the output q_{b1} is shown below:



$x_6x_5 \backslash x_4x_3$	00	01	11	10
00			1	
01		1	1	1
11	1	1		
10		1	1	1

Considering the circled minterms:

$$\begin{aligned} q_{b1} &= [x_4x_3 + x_5x_3 + x_5x_4 + x_5x_4x_3 + x_6x_3 + x_6x_4 + x_6x_4x_3 + x_6x_5 + x_6x_5x_3 + x_6x_5x_4]\overline{q_{b2}} \\ &= [x_4x_3 + x_5x_3 + x_5x_4(1 + x_3) + x_6x_3 + x_6x_4(1 + x_3) + x_6x_5(1 + x_3 + x_4)]\overline{q_{b2}} \\ &= [x_4x_3 + x_5x_3 + x_5x_4 + x_6x_3 + x_6x_4 + x_6x_5]\overline{q_{b2}} \\ &= [x_6x_5 + x_4x_3 + x_5(x_3 + x_4) + x_6(x_3 + x_4)]\overline{q_{b2}} \\ &= [x_6x_5 + x_4x_3 + x_5(x_3 + x_4) + x_6(x_3 + x_4)]\overline{q_{b2}} \end{aligned} \tag{8}$$

$$q_{b1} = [x_6x_5 + x_4x_3 + (x_3 + x_4)(x_5 + x_6)]\overline{q_{b2}} \tag{9}$$

References

1. Dandapat A, Goshal S, Sarkar P, Mukhopadhyay D (2010) A 1.2 ns 16 × 16 bit binary multiplier using high speed compressors. Int J Elect Electron Eng 4: 485–490
2. Menon R, Radhakrishnan D (2006) High performance 5:2 compressor architecture. In: IEE Proc. Circuits, Devices, Syst. vol 153, pp 447–452
3. Veeramachaneni S, Krishna KM, Avinash L, Puppala SR, Srinivas MB (2007) Novel architecture for high-speed and low power 3-2, 4-2, and 5-2 compressors. In: IEEE Int. Conf. VLSI Design, pp 324–329
4. Siliveru A, Bharati M (2013) Design of compressor based multiplier using degenerate pass transistor logic. Int J Eng Trends Technol 4:896–900
5. Lakshmi GS, Fatima K, Madhavi BK (2016) Compressor based 8 × 8 bit vedic multiplier using reversible logic. In: Int. Conf. Devices, Circuits, Syst. pp 174–178 (2016)
6. Ravi N, Prasad TJ, Umamahesh M, Rao TS (2010) Performance evaluation of high speed compressors for high speed multipliers using 90 nm technology. In: Recent Adv. Space Technol. Serv. Climate Change. pp 189–193 (2010)
7. Marimuthu R, Rezinold YE, Mallick PS (2017) Design and analysis of multiplier using appropriate 15-4 compressor. IEEE Access 5:1027–1036
8. Kumar S, Kumar M (2014) 4-2 Compressor design with new XOR-XNOR module. In: Int. Conf. Adv. Comput. Comm. Technol. pp 106–111 (2014)
9. Uyemura JP (2002) CMOS logic circuit design. Kluwer Academic Publishers
10. Multiple Operand Addition. https://pubweb.eng.utah.edu/~cs6830/Slides/chap3x2.pdf
11. Navi K, Maeen M, Foroutan V, Timarchi S, Kavehei O (2009) A novel low-power full-adder cell for low voltage. Integration, VLSI J 42:457–467
12. Shams AM, Darwish TK, Bayoumi MA (2002) Performance analysis of low-power 1-bit CMOS full adder cells. IEEE Trans VLSI Syst 10:20–29

Survey of Big Data Warehousing Techniques

Jaspreet Kaur, Rajashree Shedge and Bharti Joshi

Abstract There is a growing need in the industry toward the development of new and sophisticated tools for storing the exponentially growing volume, velocity and variety of data, which is collectively referred to as big data. There has been a paradigm shift from traditional data warehousing techniques to inclusion of NoSQL technology in order to fulfill the requirements of big data. While Hadoop has powerful features, which is not a replacement to Data Warehouse, rather it is a complement. Data Warehouse is already good at processing structured data so when used in conjunction with Hadoop, it becomes a winning combination. Hadoop can be considered as one of the back ends of Data Warehouse for handling unstructured data. Hence there is research on enhancing existing Data Warehouse with new features that have been successful at handling big data, and most popular one among them is MapReduce. We discuss the different tools and techniques used for improving Data Warehouse by adding these features and discuss the limitations associated with them.

Keywords Data warehousing · Hadoop · Unstructured · MapReduce

1 Introduction

Data storage is the recording (storing) of the data in a storage medium. The storage medium could be as diverse as DNA, RNA, phonographic recording, magnetic tape, and optical disks. Organizations typically store their data in a Data Warehouse which is a large store of data collected from heterogeneous sources within the company that allows the management to take informed decisions. With the advent of social platforms and various online portals for consumers to put their views, it becomes

J. Kaur (✉) · R. Shedge · B. Joshi
Ramrao Adik Institute of Technology, Navi Mumbai, India
e-mail: jaspreetseera@gmail.com

R. Shedge
e-mail: rajashree.shedge@gmail.com

B. Joshi
e-mail: bharti.joshi@rait.ac.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_45

crucial for organizations to process such data, which is mostly present in a textual format. Moreover, the volume of data has increased multiple folds and ways to process such huge information is challenging.

The mining of big data produces many interesting results. However, researchers are facing lot of challenges for extracting useful information from such huge chunks of data. Problems arise in the areas of data capture, storage, searching, sharing, analysis, management, and visualization [1]. Moreover, the rate at which the data is growing is exponential and this will surpass the current storage capacity in near future.

Traditional Data Warehouses were built on Online Transactional processing systems by using suitable tools and architecture which is 15–20 years old. Previously, business analysts were satisfied with analyzing the small chunks of data and provide daily, fortnightly or monthly reports to the top management. There was no proper foresight at that point of time on how big data would completely encapsulate and change the data and storage requirements in future. However, we cannot ignore the time and investment spent on building Enterprise Data Warehouse (EDW) and must benefit from new technologies, products and approaches to modernizing the currently inflexible Data Warehouses. Moving toward big data warehousing would require undergoing the following changes [2, 3].

- Offloading the ETL process to a Hadoop cluster that uses inexpensive, industry-standard hardware and processes data quickly.
- Using Parallel processing.
- Capitalizing on in-database analytics.
- Adding unstructured data metrics to existing Data Warehouse.
- Use Data Federation to extend the Data Warehouse.
- Creating Data repository.
- Adopting Lambda architecture.

Section 2 describes the existing research work in the area of big data warehousing techniques. Different techniques are discussed in Sect. 3. An endeavor to compare different techniques briefly in Sect. 4. Section 5 concludes the survey of the different techniques.

2 Related Work

Authors Ramkrushna et al. [4] explained the advantages of Apache Spark over Hadoop MapReduce and analyzed real-time data using time series analysis. Chen et al. [5] discussed Octopus which is a hybrid big data integration engine whose focus is to minimize the data movement by pushing queries to the respective back ends and getting it processed there rather than fetching the table in memory like Spark does. The authors also showed how Octopus [5] performed better than Spark in terms of query running time. Zhou et al. [6] explained that the requirements of real-time processing and large capacity of big data can be fulfilled by hybrid storage. The authors propose a preference model to weight the storage performance imbalance when data is stored on various devices. Based on this calculation, data is distributed on devices by matching the device performance with data access characteristics. Bhat [7] discusses that there is an ever-increasing gap between the volume of digital data being created and the available storage capacity of current devices. The author discusses the working of Optical, DNA and Holographic storage technologies and compares them on the basis of storage density, throughput and lifetime and implications of adoption.

Pticek and Vrdoljak [8] discussed that lack of schema in NoSQL databases makes them less comprehensible and difficult for integration and analysis. Hence the authors suggested that the use of semantics would make the contents more understandable and easy for integration. Dehdouh et al. [9] developed an aggregation operator called Columnar NoSQL Cube which can build data cubes over Data Warehouses stored in column-oriented NoSQL database management system using HBase engine. Having the CN-Cube operator solves the drawback of absence of OLAP operators for column-oriented database. Pticek and Vrdoljak [10] discussed MapReduce research in warehousing of big data wherein they have highlighted that for big data warehousing solution, integrate one or more MR-based technologies like Hadoop and Hive and combine it either NoSQL or traditional Data Warehouse. Herodotus et al. [11] explain about Starfish which is a self-tuning system for big data analytics. It is built on Hadoop while adapting to user needs and system workloads to provide good performance automatically. Abello et al. [12] discuss the possibility of having data in a cloud by using BigTable to store the hierarchical data and using Map Reduce to deploy cubes in ad hoc Data Marts.

3 Big Data Warehousing Techniques

The key requirements of big data storage are its ability to handle large amounts of data, scalability to handle growth and real-time data processing for analysis. The typical approach has been to provide an architecture that spans several storage products in order to provide the required performance and capacity at a reasonable price. A new generation of storage tools has been developed specialized for big data, and efforts have been made to augment these systems with traditional Data Warehouses. In this section, we do an exhaustive study about the recent tools developed for storage of big data and discuss their performance, capabilities and limitations. It investigates the challenge of storing data in a secure and privacy-preserving way.

3.1 Apache Spark

Apache Spark is a cluster computing technology for large scale data processing. It does not use MapReduce as an execution engine, rather it uses its own distributed runtime for executing work on cluster. [4] It is built on top of Hadoop MapReduce and extends the MapReduce framework to incorporate many other computations. The main drawback of Hadoop is that it can be used for batch processing and not real-time computation. But with the growing needs of the industries, having real-time processing is becoming a necessity. Spark is 100x faster than Hadoop for large scale data processing. It provides easy interface for users and is polyglot, i.e., can be programmed in Scala, Python, R and Java. In addition, Spark is flexible in the sense that it can be deployed using Mesos, Hadoop via Yarn or by using its own cluster manager.

Spark creates a Spark Context object, which gives information about accessing the cluster. Using the attributes defined in the Spark Context, it connects to a Cluster Manager whose task is to allocate resources across various applications. The cluster manager is in turn connected to the worker nodes/data nodes where the execution takes place. These worker nodes also have a cache memory which makes Spark fault-tolerant. The executor is space in RAM where all the blocks reside for execution.

Spark also supports streaming data, SQL queries, and complex analytics such as graph algorithms and machine learning using components like Spark SQL, Spark Streaming, GraphX, Spark Core Engine and, MLlib. Resillient Distributed databases (RDD) which is an immutable distributed collection of objects, are the heart of every Spark program. Spark provides two categories of operations on RDDs: transformations and actions. A transformation generates a new RDD from an existing one. An action triggers a computation on an RDD and produces the result into an external storage.

3.2 Octopus

Nowadays, organizations maintain huge amount of data in multiple backend systems which include traditional warehouses and more recently, big data systems. Integrating, querying and analyzing such disparate data become a difficult task. Octopus is a hybrid data processing engine to integrate backend systems. It divides the task into subqueries and pushes them into the respective backend system where it is processed. It comprises of two main components, namely parser and optimizer. Parser generates a logical operator tree based on user programs. Based on the logical operator tree generated by the parser, the optimizer generates optimal query plans for execution in the respective backend [5].

We consider an input query q and S backend systems where S_i $(1 \leq i \leq S)$, D datasets D_j $(1 \leq j \leq D)$ and Q subqueries generated by Octopus where Q_k $(1 \leq k \leq Q)$. Three binary indicators are introduced to understand the relationship among the sets. Given a query task q to access whole data sets D_j, generation of subqueries Q_k that will be pushed down to backend systems S_i with the goal of minimizing the overall query processing time., we measure the running time in the following criteria.

$\mathrm{Tm}_{\mathrm{i,j}}$ of system S_i to move data D_j needed by Q_k
$\mathrm{Tp}_{\mathrm{i,k}}$ of system S_i to process query Q_k.

3.2.1 Dependencies Among Queries

$\mathrm{Tp}_{\mathrm{i,k}}$ depends solely on the processing power of system S_i. $\mathrm{Tm}_{\mathrm{i,j}}$ of system depends on whether the data set D_j required by subquery Q_k is present locally or needs to be fetched from other systems. In the previous case, time $\mathrm{Tm}_{\mathrm{i,j}}$ is dominated by the time required by system *Si* to load *Dj*. In the second case, the time $\mathrm{Tm}_{\mathrm{i,j}}$ is dominated by the time required to fetch dataset *Dj* from remote system. This task of assigning subqueries to backend systems is a job scheduling NP-hard problem; hence, a heuristic solution has been proposed by leveraging the data locality principle which minimizes the data movement.

3.3 Preference Aware Hadoop Distributed File System

Hadoop Distributed File System (HDFS) is the primary data storage used by applications of Hadoop. Due to its distributed storage, scalability, reliability, fault tolerance, high availability and replication, it is a suitable storage medium for big data. However, HDFS also faces certain limitations, one of them being that it distributes data evenly across all storage devices under the assumption that all storage devices have the same I/O performance. Different devices have different I/O performance, asymmetric read/write performance as well as asymmentric read/write access characteristics of data. Hence, a preference model was designed (PAHDFS) to calculate the weight of the storage performance and distribute data based on matching of performance with data access characteristics [6]. Data is divided into blocks. The following equations explain the calculation of preference degree.

$$\mathrm{TR}_{\mathrm{m}}(i) = \frac{S_i}{\mathrm{PR}_{\mathrm{m}}} + \mathrm{TS}_{\mathrm{m}} \tag{1}$$

Read Time of Data Block B_{i} when it is distributed on D_{m} is equal to the sum of read transmission time and seek time.

Similarly, write transmission time of data block B_{i} when it is distributed on D_{m} is equal to the sum of write transmission time and seek time.

$$\mathrm{TW}_{\mathrm{m}}(i) = \frac{S_i}{\mathrm{PW}_{\mathrm{m}}} + \mathrm{TS}_{\mathrm{m}} \tag{2}$$

Hence overall access time for Data Block B_{i} is calculated as

$$C_{\mathrm{m(i)}} = \mathrm{TR}_{\mathrm{m}} * \mathrm{FR}_{\mathrm{i}} + \mathrm{TW}_{\mathrm{m}} * \mathrm{FW}_{\mathrm{i}} \tag{3}$$

Hence, preference degree of block B_{i} to device D_{m} is equivalent to the difference in the access time of B_{i} on device D_{n} and device D_{m}

$$P_{\mathrm{mn}}(i) = C_{\mathrm{n(i)}} - C_{\mathrm{m(i)}} \tag{4}$$

The greater the value of $P_{\mathrm{m,\,n}}(i)$, the more block $\mathrm{B_i}$ prefers to reside in device $D_{\mathrm{m.}}$ Hence deriving the final equation

$$P_{\mathrm{mn}}(i) = S_i * \left[\left(\frac{1}{\mathrm{PR_n}} - \frac{1}{\mathrm{PR_m}}\right) * \mathrm{FR_i} + \left(\frac{1}{\mathrm{PW_n}} - \frac{1}{\mathrm{PW_m}}\right) * \mathrm{FW_i}\right] + (\mathrm{TS_n} - \mathrm{TS_m}) * (\mathrm{FR_i} + \mathrm{Fw_i}) \tag{5}$$

The blocks are sorted in descending order of access frequency. The algorithm traverses the blocks from high frequency to low frequency and determines whether migration is necessary. Higher preference degree of a block in a particular device implies that the particular block will display higher performance if it resides on that device. The algorithm traverses in the Check Device set in descending order of preference degree to ascertain if migration is required. To overcome the problem of excessive migrations, the following conditions are imposed

- The benefit of migration should exceed the overhead incurred.
- Migration should not pull block with higher preference out of the target device.

3.4 Optical Data Storage (ODS)

According to a report published by International Data Corporation, the amount of data is forecasted to reach 44 zettabytes by the year 2020, out of which 13 zettabytes is supposed to be critical data. However, it is estimated that the current storage technologies will be able to hold only 15% of 44 zettabytes resulting in a data capacity gap of 6 ZBs. Optical Data Storage (ODS) [7] which first emerged as CDs and later progressed to DVDs and Blu-ray disks recorded information in diffraction-limited region within a layer beneath the surface of the disk. Due to this, the capacity was limited to few tens of Gigabytes(GBs) The optical spot which records the digital bits is directly proportional to the wavelength of Laser beam and inversely proportional to the numerical aperture of the optical head. The diffraction limit places a limit on the storage capacity to few terabytes per disk which is not enough to overcome the data capacity gap. Nanophotonic approaches have paved the way for increasing the storage capacity by breaking or circumventing the diffraction barrier.

3.5 DNA Data Storage (DDS)

DNA has the potential to have huge storage capacity because it is incredibly dense, is volumetric rather than planar and is fairly stable. DNA strand or Oligonucleotide is a linear sequence of four nucleotides namely Adenine (A), Cytosine (C), Guanine (G) and Thymine (T). Two DNA strands can bind to each other and form a double helix. A in one strand can combine with T in another strand and likewise for C and G. Probability of a nucleotide to bind to the existing partial strand at each step in the process is as high as 99% and is referred to as coupling efficiency. There are four different base pairs namely AT, GC, TA and CG and they are used to encode four Quaternary digits which are 00,01,10 and 11. For reading data stored in DNA, nucleotide pairs are decoded into Quaternary digits and are further translated to binary data. However, the drawback associated with DNA storage is that it is vulnerable to a wide variety of errors during synthesis and sequencing. The error rate could be around 1% per nucleotide. Also, nucleotide sequences degrade when stored leading to data integrity issues [12].

Though DNA, data storage offers huge rewritable storage capacity and sustainability, but still is an expensive proposition because of the cost of sequencing and synthesis. Hence, we look at another technology known as Holographic Data storage in the next section.

3.6 Holographic Data Storage (HDS)

Holographic data storage (HDS) overcomes the limitation of ODS by storing data throughout the volume of the media rather than only on the surface. HDS employs multiplexing for recording multiple holograms in the same volume of data. Light from a laser source is split into two beams. The first is a signal beam which is passed through a Spatial Light Modulator to encode binary data. The second is a reference beam which is recombined with the modulated signal beam before entering the recording media. The pattern produced by the overlapping beams is imprinted as a hologram. The differentiating feature of the hologram is the unique volume address provided by reference beam. For retrieving the data, the reference beam that was used for recording the hologram is used. However, signal beam is independent from the rest of the holograms [7].

3.7 Semantic Web Technologies

NoSQL, which stands for Not Only SQL, is specially designed for large sets of distributed data. It is basically schema-less which allows data of any form to be stored. However, the diversity and lack of clear schema of NoSQL database present integration problems with relational databases. This drawback led to the development of semantic web technologies that can compensate the lack of schema in NoSQL databases and boost the design of the Data Warehouse. NoSQL Databases are classified as document, column, key-value stores and graph. Though they differ in features, they share the schema-less model and have good fault tolerance and consistency. The role of semantics in the semantic-based integration scenario has been discussed under the following heads [8].

- Data Source schema extraction.
- Integration of data source schemas.
- Schema reduction.
- Outlining the multidimensional concepts.

The advantages of having Ontologies are that they can be easily updated, can solve heterogeneity conflicts, can detect multidimensional concepts, can discover hidden semantics and explore large unstructured data sets. Hence using ontologies can help in automating the process to a certain extent.

3.8 Columnar NoSQL Cube

Column-oriented NoSQL systems unfortunately have no OLAP operators. To overcome this limitation, CN-CUBE was developed which is an aggregation operator specially designed for column-oriented NoSQL databases. After identifying the attributes which would form the basis of dimension and facts, a query is formed as a view is created as a result. CN-CUBE uses this view hence reducing disk access. To form all the dimension combinations required to build the cube, it uses value positions and hash tables and extracts data that satisfies the requirements of the query. Because of their suitability for big data, HBase DBMS and Hadoop platform were chosen. Column-oriented databases store data by column rather than rows. Such an approach resulted in faster aggregation, compression and data retrieval and was suitable for big data where the volume of data is very high. The data, which is stored in key-value format, had an additional attribute namely timestamp. This allows us to distinguish the recent data. Hence, the combination of key, column name and time-stamp forms the coordinates of the value. The time-stamp ensures that the most recent version of data is to be taken while retrieving the results of the query.

4 Comparative Analysis of Techniques

Based on the detailed analysis covered in the previous section, we do a comparative analysis of the various techniques based on various performance parameters. This helps us in quickly understanding where we stand presently with respect to these techniques and how they need to mature further (Table 1).

Table 1 Comparative analysis of techniques

Technique	Parameter	Advantages	Limitation
Apache spark [4]	100X times faster than MapReduce	• User-friendly APIs • Capable of near real-time processing • Fault tolerance by the use of RDDs	• No support for real-time processing • Expensive • Lacks a file management system
Octopus [5]	Octopus outperforms spark version 1.4.0 by having a 5.25 times faster running time	• Fully integrate the power of backend systems • Optimizes the amount of data movement	Limited to one module of spark and cannot fully replace it unless other modules of spark such as machine learning are integrated
PAHDFS [6]	Read throughput improves by 87.3%, write throughput improves by 15.6%, mixed throughput by 70.6%	• Unburden name node for scalability • Same interface as HDFS • Devices adequately utilized	• Not suitable for small files • Hadoop security model is complex and disabled by default
Optical data Storage [7]	• Storage density-hundreds of petabytes • Throughput 10GBps(High)	• Reliability under extreme atmospheric conditions • Low maintenance cost • Energy efficient	• Absence of rewritable storage support • Limited to low latency applications
DNA data storage [7]	• Storage density-214 PB per gram of DNA • Low throughput	• Huge and rewritable storage capacity • Sustainability under extreme weather conditions	• Low throughput. And high cost of sequencing and synthesis of DNA strands • Limited to huge volumes of data having high latency
Holographic data storage [7]	• Storage density- tens of terabits percm3 • Throughput 400MBps (Low)	• Better than ODS and DDS in cost/TB basis • Lifetime is best among all devices	• Changes in recording technique may make it incompatible • Intermediate solution till other technologies pick up
Semantic web technologies [8]	Semi automation is possible since the veracity factor of big data requires supervision and hard to automate	• Bridge the gap between traditional and NoSQL databases • Global ontology to derive multidimensional table	• Lack of standardization in ontology • Considers big data warehouse design from scratch
Columnar NoSQL cube [9]	CN-CUBE has lesser computation time than HIVE CUBE operator 15 node cluster records the best time	• Reduces input-output flows by using hash tables • Outperforms the HIVE CUBE operator	Though column-oriented datastores are popularly used for big data, it has no OLAP operators. Limited to only aggregation. Support for new operators to be added

5 Conclusion

For an IT industry which was just getting used to handle terabytes of data in their Data Warehouses, handling unstructured data in petabytes becomes a daunting task. According to a research, the growth of data in the next five years shall be more than data collected in the last fifteen years. Data Warehouse alone is incapable of handling such volume and variety of data. Hence, data storage vendors have been working toward incorporating big data and analytics tool such as Hadoop into their infrastructure. The initial hype of big data storage techniques focussed on only Hadoop and MapReduce but now many other players have entered the market like SAS and SAP HANA. Storage is a necessity but it is not so easy to address. Cloud storage providers such as Azure and Google offer hardware, processing and storage for current and future data growth. Multi-cloud data management solutions are being built which use a mix of services from cloud service providers as well as private clouds.

We analyzed recent research in big data storage technologies and did a comparative study of these technologies. Some of them are in nascent stage and need to mature further in order to satisfy the purpose while other tools such as Hadoop and MapReduce technologies are in developed stage and further improvements are being suggested through the use of add-ons or separate technologies developed using the proven technologies. Hence, there are plenty of solutions in the market but not a single leader which can replace all others.

References

1. Oussus A, Benjelloun FZ et al (2018) Big data technologies: a survey. J King Saud Univ 30(4):431–448
2. Big Data: Five Tactics to Modenize your Data Warehouse. https://www.emc.com/collateral/emc-perspective/h10915-ep-pdf-data-warehouse-modernization.pdf
3. Extract, Transform and Load Big Data with Apache Hadoop. https://pdfs.semanticscholar.org/dcd9/ce3591738b98e2cc9da63ee1fe9932c24500.pdf
4. Maheshwar RC, and Haritha D (2016) Survey on high performance analytics of bigdata with apache spark. In: international conference on advanced communication control and computing technologies, pp 721–725
5. Chen Y, Xu C, Rao W, Min H and Su G (2015) Octopus: hybrid big data integration engine. In: IEEE 7th international conference on cloud computing technology and science, pp 462–465
6. Zhou W, Feng D, Tan Z, Zheng Y (2018) Improving big data storage performance in hybrid environment. J Comput Sci 26:409–418
7. Bhat WA (2018) Bridging data-capacity gap in big data storage. Future Generation Comput Syst 87:538–548
8. Pticek M, Vrdoljak B (2018) Semantic web technologies and big data warehousing. MIPRO 2018:1214–1219
9. Dehdouh K. et al. (2014) Columnar NoSQL CUBE. In: IEEE international conference on systems, man and cybernetics, October 2014, pp 3828–3833
10. Pticek M, Vrdoljak B (2017) MapReduce research on warehousing of big data. MIPRO 2017:1361–1365
11. Herodotou H. et al. (2011) Starfish: a self tuning system for big data analytics. In: 5th biennial conference on innovative data systems research (CIDR2011), 2011, pp 261–272

12. Abello A, Ferrarons J, Romero O (2011) Building cubes with MapReduce. In: proceedings of the ACM 14th international workshop on data warehousing and OLAP(DOLAP11), 2011, pp 17–24
13. Lee S, Jo S, Kim J (2015) MRDataCube: data cube computation using MapReduce. In: international conference on big data and cloud computing, 2015, pp 95–102
14. Sokolov I, Turkin I (2018) Resource efficient data warehouse optimization. In: 9th IEEE international conference on dependable systems, services and technologies, 2018, pp 491–495

Detecting Denial-of-Service Attacks Using sFlow

Shivaraj Hublikar, Vijaya Eligar and Arun Kakhandki

Abstract This paper addresses how to detect denial-of-service attacks using sFlow. Denial-of-service (DoS) attack is a critical security challenge in software-defined network (SDN). In DoS attack, the network bandwidth is acquired by disrupting the services of the server by abruptly increasing the traffic and making the server unavailable for other users. The most challenging problem of DoS attack is to detect the attack almost instantly and in a precise manner. This paper presents the detection of DoS attacks by using sFlow analyzer, a SDNs flow monitoring tool. In the event of any attack, sFlow collects sample packets from network traffic, analyzes suspicious behavior and creates handling rules which are then sent to the controller. Implementation of DoS attack is carried out by emulating a typical network in Mininet and integrating this with sFlow analyzer. Through the simulated results, the potential DoS victims and attackers are quickly found.

Keywords Bandwidth detection · DoS attack · SDN · sFlow

1 Introduction

In a traditional data network, devices are structured into data-plane and control-plane which are local. If there are ten devices in a network, then each device has its own data-plane and control-plane that are having all the relevant information regarding forwarding tables. The data-plane comprises of switches, while the control-plane comprises of controllers of different types. Networking device will get the

S. Hublikar · V. Eligar (✉)
KLE Technological University, Hubballi, India
e-mail: vijayaeligar@bvb.edu

S. Hublikar
e-mail: shivaraj@bvb.edu

A. Kakhandki
KLSs VDRIT, Haliyal, India
e-mail: bvbarun@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_46

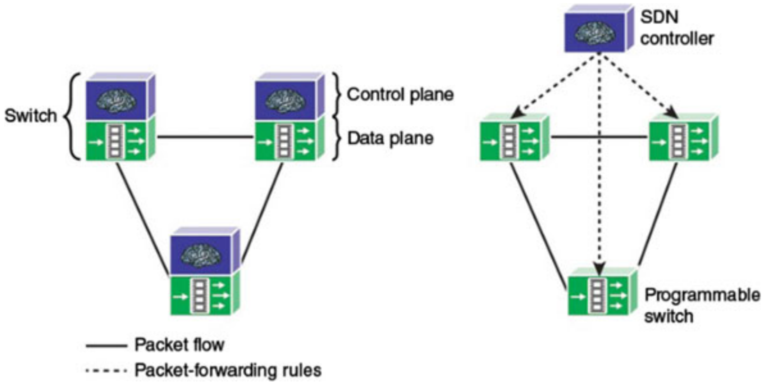


Fig. 1 Traditional network and SDN [11]

packets which are decided by forwarding tables. Since the demand of traditional networks is increasing, working on topology is complex [5]. Even though traditional networks are global and very popular, they have various drawbacks. Firstly, there is no scope to extend the network if a new feature or a protocol is to be added. Secondly, any new command cannot be accepted to improve the functionality of traditional networks since it is not programmable. Thirdly, cost of the network is effectively high since each device contains both data-plane and control-plane. Different topologies of the network are not possible since the traditional network is configured with set of predefined rules during the manufacture. Furthermore, the physical network infrastructure cannot be fully utilized since arranging the traditional network with predefined polices becomes complicated and error prone.

Recent trends such as machine learning, artificial intelligence, cyber security, internet of things (IoT) and mobile traffic have heavy traffic which cannot be managed by the network. SDN manages the overall network programmatically. SDN is very unique from the traditional networks which provide entire central control over the network by separating the control-plane and the data-plane as shown in Fig. 1.

SDN manages the network by centrally controlling the devices which greatly utilize and improve the network management. This network has data-plane within the device for sharing the forwarding data, whereas the control-plane is connected with separate device called controller which handles the information. SDN is categorized into three parts, controllers, southbound application program interfaces (APIs) and northbound (APIs). Controller, which is the programmable central system, controls the entire network which has the information of all the resources (like switches and routers) connected to this network. Switches and routers are the information devices which require southbound APIs as the medium for the controllers to transfer the data packets. OpenFlow is standard protocol used in southbound APIs. SDN uses northbound APIs to manage the traffic which is monitored by the network administrators to communicate with applications shown in Fig. 2.

Fig. 2 SDN controller

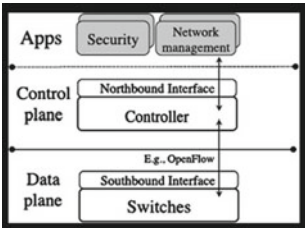
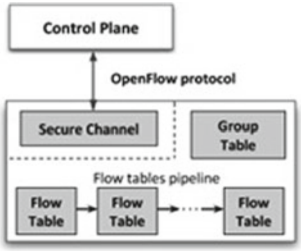


Fig. 3 Open switch architecture



1.1 OpenFlow

OpenFlow is a standard protocol that provides communication and interface between control-plane and data-plane in SDN. The data packets are transferred between devices which have to maintain traffic routing flows that is managed by the OpenFlow protocol. Each SDN device needs to maintain the set of Flow-tables that is controlled by OpenFlow switch. The incoming packets are controlled by the switch which are installed by the control-plane that maintains communication channel and also contains the Flow-table rules [1]. Figure 3 presents the logical structure of an OpenFlow switch. When there is a mismatch in the Flow-tables that does not match with any existing flow rules, the mismatch flows try to trigger forwarding plane to the controller which reduces the bandwidth and memory. The limited communication bandwidth between the control and data-planes could be a bottleneck of the whole network, and lead to security problems. Todays commercial OpenFlow switches only support cable connection to the controller. The practical connection bandwidth is tested to be less than 10 Mbps.

Research in SDN and DoS attacks is predominantly focused on detection of the attack. In July 2001, Internet infrastructure was hit worldwide by DoS attack worms named Code Red and NIMDA. Network scanning was used by Code Red Worm to attack the network at a rapid propagation rate to detect and exploit Internet Information Server (IIS) automatically. This DoS attack consumed huge bandwidth which affected lot of network devices. The attack was complex since the attack came from various sources of IP addresses for which packet analyzing was a big task. In order to mitigate or limit the damage to network resources, content filtering of some type were performed.

In [2], the authors propose a mechanism that avoids the overloading of switch TCAMs along with controller and control channel bandwidth and a solution called SLICOTS, which mitigates a type of flooding attack TCPSYN in SDN. It is built on top of the controller in order to monitor the network traffic related to TCP requests.

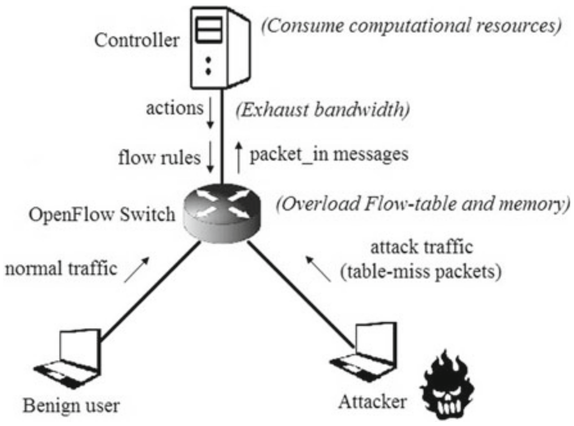
This paper is organized as follows. Section 2 discusses DoS attacks on SDN. Section 3 presents the DoS detection method based on sFlow tool. Section 4 demonstrates the method to detect DoS attacks. The simulation results and discussion are presented in Sect. 5 followed by conclusion in Sect. 6.

2 DoS Attack

DoS attack causes serious impact on the computing system. DoS attacks deny services to valid users by completely consuming the target resources. DoS attacks are usually initiated by an individual or group of individuals exploiting aspects of the Internet Protocol to deny other users from legitimate access to systems and information. The router hosts are disconnected if forwarding packets are stopped by router. The recent applications which are targets to these attacks are Web servers, mail servers and other services [6].

In [9], the authors explain SDN-aimed DoS attacks (data-to-control-plane saturation attacks). The attacker first sends the packets which do not match the packets in the Flow-tables by generating table-miss packets without the order with some or all fields, which does not match with existing flow rules on the target switch as shown in Fig. 4. Then, the attacker launches DoS attacks on the SDN network by flooding with large amount of table-miss packets. These table-miss packets will target massive packet in messages from the switch to the controller, and consume their communication bandwidth, CPU computation and memory in both control- and data-planes [2].

Fig. 4 DoS attack



DoS attacks can be of various types:

- **Destructive**: Attacks which destroy the device to prevent the proper operation of function, such as deleting or changing properties or information and power supply.
- **Resource consumption**: Attacks which try to reduce the ability of the device to perform effectively by opening many simultaneous connections to a single device.
- **Bandwidth consumption**: Attacks which attempt to affect the bandwidth capacity of the network device.

This paper aims to concentrate on bandwidth attack which is done using sFlow tool. When any DoS attack is detected, sFlow generates flow rules by analyzing samples of packets collected from the network traffic to be sent to the controller. In this work, security services are developed to protect networks against different type of network attacks for third parties like servers. A DoS attacker attacks the network by providing enormous flooding traffic in a short time to a server by increasing flow so that the server gets disconnected.

3 sFlow

sFlow helps to monitor the network, that develops various ways of handling the traffic flows, and to improve the performance of the network which consist of switches and routers. sFlow [12] is an open-source sampling tool used for measuring the traffic which is compatible with OpenFlow network. It consists of sFlow agents and collector. The sFlow agent captures traffic statistics from the device which is under observation that uses sampling technology. sFlow datagrams immediately forward the sampled traffic statistics to a sFlow collector for analysis. The main task of the two modules is listed below.

1. **sFlow Collector**: It is a server where sFlow datagrams are collected and stored.
2. **sFlow Analyzer**: It provides real-time overview of the network traffic flow by analyzing the received datagrams by analyzing the irregularities of the network parameters and detailed information. sFlow agents send a stream of sFlow samplings continuously to the collector where they are analyzed to supply a real-time, network-wide view of traffic flows.

3.1 Integration of Mininet and sFlow

Network simulators play an important role by evaluating network topologies of different types over a small scale. Many network simulators like Mininet, GNS3 and EsiNet are available. Mininet is used here which is an open-source network simulator used to generate traffic and analyze its flow.

Mininet [8] is an open-source network emulator and is a command line interface (CLI) and enabled simulator which supports the use of analysis tools like the sFlow, NetFlow and RMON. Mininet creates virtual switch, hosts, links and controllers on a single Linux kernel with a single command. Custom topologies are created using Mininet. It simulates a real machine and can create different hosts. The limitation of Mininet is that it does not have OpenFlow controller and it runs on slower links (10 or 100 Mbps).

According to [7], these simulators provide a platform to set a network topology as a replication to the real-world environment about analysis and detection of the attacks using Mininet and sFlow. The analysis is done in a number of steps in the tool, which are listed here.

1. Start.sh will run the shell script command to run the sFlow application.
2. In another window, Mininet topology will execute. The ping command is run to check the connectivity between the hosts of the topology created. A zero percentage drop depicts the complete connectivity between the hosts.
3. For accessing the sFlow trend GUI, a local host is created using the command: localhost: 8008.
4. A typical command in Mininet for detection of attack is given as: http://localhost:8008/app/mininet-dashboard/html/. It provides an approach to run a SDN Controller along with it.

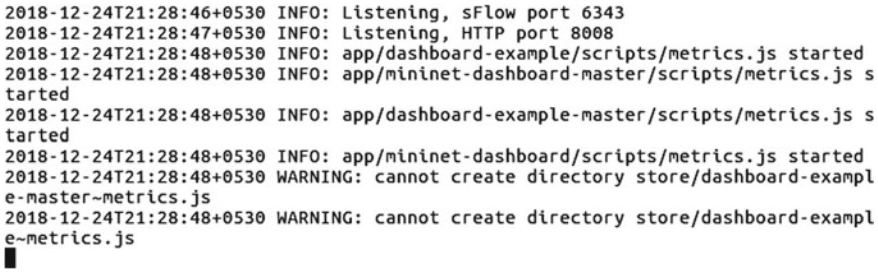
4 Implementation

In this section, the implementation of the network is discussed. Initially, sFlow-RT is created to receive a continuous flow of data that is sent from the network devices and converted into metrics. As soon as the flow reaches certain predefined metric level, it is sent to an analyzer. Next, using the Mininet command, a topology is built with link bandwidths of 10 Mbps. Finally, the output is the link between two hosts.

In order to make it easier to get started, the latest release of sFlow-RT includes a Mininet helper script sflow.py that automates sFlow configuration. The following example shows how to use the script and build a simple application in Python.

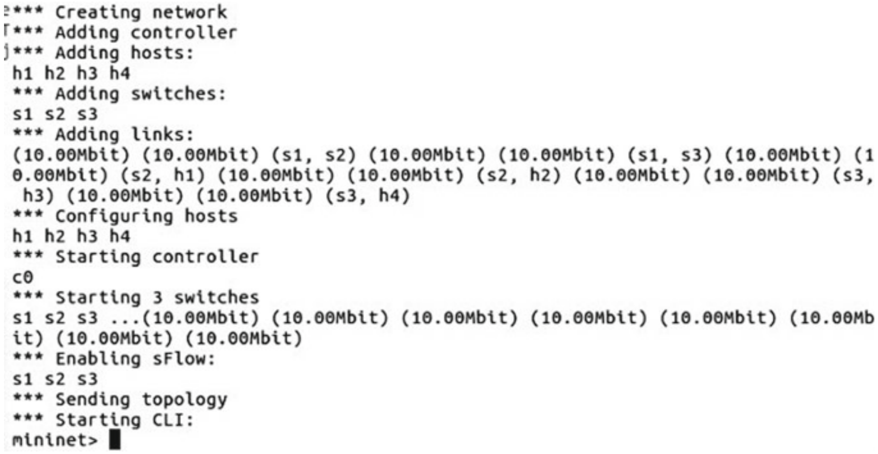
The various steps to detect the flows in a Mininet topology created in Linux environment using sFlow-RT are listed here and shown in Fig. 5.

1. **sFlow-RT**: sFlow-RT is an open-source tool that has an embedded OpenFlow controller, allowing monitoring and flow insertions to OpenFlow supporting switches. It analyzes certain events of interest, raise triggers and apply traffic handling rules to a particular controller. In order to analyze sFlow-RT flows and react on traffic changes, it has to be configured to work together with the existing network.
2. **For Creating Mininet**: In a second terminal, add the—custom argument to the Mininet command line. The following command builds a depth ‘2’ tree topology with link bandwidths of 10 Mbit/s.
   ```
   cd sflow-rt
   sudo mn –custom extras/sflow.py –link tc, bw=10 –topo tree, depth=2, fanout=2.
   ```
   The response of the tool after creating the topology is shown in Fig. 6. The sflow.py



```
2018-12-24T21:28:46+0530 INFO: Listening, sFlow port 6343
2018-12-24T21:28:47+0530 INFO: Listening, HTTP port 8008
2018-12-24T21:28:48+0530 INFO: app/dashboard-example/scripts/metrics.js started
2018-12-24T21:28:48+0530 INFO: app/mininet-dashboard-master/scripts/metrics.js s
tarted
2018-12-24T21:28:48+0530 INFO: app/dashboard-example-master/scripts/metrics.js s
tarted
2018-12-24T21:28:48+0530 INFO: app/mininet-dashboard/scripts/metrics.js started
2018-12-24T21:28:48+0530 WARNING: cannot create directory store/dashboard-exampl
e-master~metrics.js
2018-12-24T21:28:48+0530 WARNING: cannot create directory store/dashboard-exampl
e~metrics.js
█
```

Fig. 5 Starting sFlow



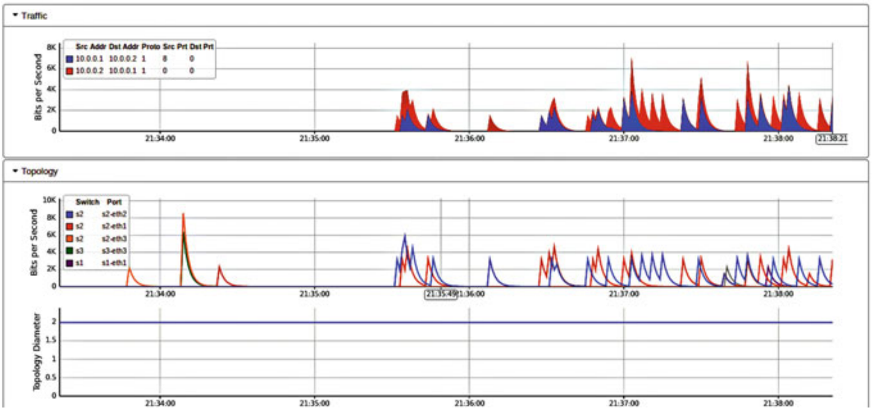
```
*** Creating network
*** Adding controller
*** Adding hosts:
h1 h2 h3 h4
*** Adding switches:
s1 s2 s3
*** Adding links:
(10.00Mbit) (10.00Mbit) (s1, s2) (10.00Mbit) (10.00Mbit) (s1, s3) (10.00Mbit) (1
0.00Mbit) (s2, h1) (10.00Mbit) (10.00Mbit) (s2, h2) (10.00Mbit) (10.00Mbit) (s3,
 h3) (10.00Mbit) (10.00Mbit) (s3, h4)
*** Configuring hosts
h1 h2 h3 h4
*** Starting controller
c0
*** Starting 3 switches
s1 s2 s3 ...(10.00Mbit) (10.00Mbit) (10.00Mbit) (10.00Mbit) (10.00Mbit) (10.00Mb
it) (10.00Mbit) (10.00Mbit)
*** Enabling sFlow:
s1 s2 s3
*** Sending topology
*** Starting CLI:
mininet> █
```

Fig. 6 Creating topology

script extends Mininet, automatically enabling sFlow on each of the switches in the topology, and posting a JSON representation of the Mininet topology using sFlow-RT.

5 Results and Discussion

Whenever the network is simulated without any attack, bandwidth between the two hosts maintained at 9.63 Mbps. When a DOS attack is initiated on the network, the bandwidth falls to 30 kbps. The bandwidth has reduced from Mbits to kbits due to the DoS attack which has increased the datarate. This resulted in the decreased system performance. The GUI output of the DoS detection is shown in Fig. 7. Here, sFlow is initiated in the local host to detect the DoS attack when host h1 pings h2. As more number of packets are sent, DoS attack is detected.



	Src Addr	Dst Addr	Proto	Src Prt	Dst Prt
🟦	10.0.0.1	10.0.0.2	1	8	0
🟥	10.0.0.2	10.0.0.1	1	0	0

	Switch	Port
🟦	s2	s2-eth2
🟥	s2	s2-eth1
🟧	s2	s2-eth3
🟩	s3	s3-eth3
🟪	s1	s1-eth1

Fig. 7 DoS attack detected

6 Conclusion

DoS attack was detected by acquiring network bandwidth and disrupting the services of the server by abruptly increasing the traffic by making the server unavailable for other users. DoS attack was detected using the sFlow tool. In case of any attack, sFlow collects sample packets from network traffic, analyzes suspicious behavior and creates handling rules which are then sent to the controller. Implementation of DoS attack is carried out by emulating a typical network in Mininet and integrating this with sFlow analyzer. The results indicate efficient identification of DoS attack by using sFlow.

References

1. Ambrosin M, Conti M, De Gaspari F, Poovendran R (2017) Lineswitch: tackling control plane saturation attacks in software-defined networking. IEEE/ACM Trans Netw (TON) 25(2):1206–1219
2. Dridi L, Zhani MF (2018) A holistic approach to mitigating DOS attacks in SDN networks. Int J Netw Manag 28(1):e1996
3. Jyothirmai P, Raj JS, Smys S (2017) Secured self organizing network architecture in wireless personal networks. Wirel Pers Commun 96(4):5603–5620
4. Nugraha M, Paramita I, Musa A, Choi D, Cho B (2014) Utilizing OpenFlow and sFlow to detect and mitigate SYN flooding attack, 17(8):988–994
5. Ombase PM et al (2017) Survey on DOS attack challenges in software defined networking. Int J Comput App 975:8887
6. Othman RA (2000) Understanding the various types of denial of service attack. Bus Week Online. Accessed 12 Feb 2000
7. Peter: Mininet flow analytics. https://blog.sflow.com/2016/05/mininet-flow-analytics.html. Accessed 10 Jan 2019
8. Scarlato M. Network monitoring in software defined networking (thesis). Accessed 30 Jul 2014

9. Shang G, Zhe P, Bin X, Aiqun H, Kui R (2017) Flooddefender: protecting data and control plane resources under SDN-aimed DOS attacks. In: INFOCOM 2017-IEEE conference on computer communications. IEEE, pp 1–9
10. Sridhar S, Smys S (2016) A hybrid multilevel authentication scheme for private cloud environment. In: 2016 10th international conference on intelligent systems and control (ISCO). IEEE, pp 1–5
11. Stallings W (2015) Foundations of modern networking: SDN, NFV, QoE, IoT, and Cloud. Addison-Wesley Professional
12. Swapna AI, Reza MRH, Aion MK (2016) Security analysis of software defined wireless network monitoring with sFlow and FlowVisor. In: International conference on communication and electronics systems (ICCES). IEEE, pp 1–7

Area and Power Efficient Multiplier-Less Architecture for FIR Differentiator

Sanjay Eligar and R. M. Banakar

Abstract Digital FIR filters have been used for various signal processing tasks in embedded systems. This paper presents a novel architecture for implementation of an FIR differentiator in FPGA designed for a specific application. The designed component is to estimate the velocity from the suspension displacement in a semi-active suspension controller. The architectures of FIR are modified based on the direct and transposed form, with incremental changes in the manner in which the constant-coefficient multiplication is executed. The recoding of constant FIR filter coefficients using Canonic Signed Digit representation is explored. Three architectures are designed and compared for efficient usage of area of implementation in FPGA. It is observed that the architecture using CSD requires 16% lesser area, and the optimized architecture is an additional 5% more area-efficient and 16% lesser in complexity of design because of sharing of resources. An overall reduction in power consumption by 3% is observed and the computation of the FIR filter convolution sum is faster by 17%.

Keywords FIR differentiator · Constant multiplication · Canonic Signed Digit · Design validation

1 Introduction

Linear phase FIR filters are a category of filters which exploit the property of symmetry or anti-symmetry to reduce the number of multiplications in the computational algorithm. In the FIR convolution, each output sample ($y[n]$) is obtained as a sum of weighted samples of the input signal of finite number and the delayed input samples ($x[n]$, $x[n-1]...x[n-k]$) [6]. A close observation of computation reveals that

S. Eligar (✉) · R. M. Banakar
BVB College of Engineering and Technology, Hubli, India
e-mail: eligar@bvb.edu

R. M. Banakar
e-mail: banakar@bvb.edu

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_47

there is a continuous multiplication of input samples by constants (b_k). This condition which is further explored here, and opens up enormous possibilities to optimize in an FPGA. The convolution sum can be implemented using different types of FIR structures. The most simplest approach is the direct form FIR digital filter structure in which the filter coefficients of the transfer function is nothing but the multiplier coefficients themselves.

In [4] an FIR filter is designed as a differentiator for the specifications of a velocity estimator for semi-active suspension controller. Velocity estimation is one of the primary requirements for the application discussed here, and which is a controller for semi-active suspension system using magneto-rheological dampers fitted to a passenger car. The controller chosen is a variable structure controller of type Sigma-1 and the computation requires estimation of velocity from linear displacement of suspension deflection [3]. An FIR of Type III is chosen for implementation with the specifications as: pass-band frequency ($f_p = 400\,\text{Hz}$), stop-band frequency ($f_{st} = 500\,\text{Hz}$) and sampling frequency ($f_s = 1\,\text{kHz}$). Using equiripple method for design yielded a structure of length M = 7 [4] and the filter coefficients are as shown in Table 1. Because of the anti-symmetric behaviour of the odd length filter designed here, three pairs of filter coefficients are equal in magnitude, but opposite in sign and the centre coefficient (b_3) is 0. The computation of an output sample $y[n]$ needs 6 multiplications and 5 additions apart from the delay elements. This is definitely not an optimal architecture since the anti-symmetry property of the linear phase FIR filter is not exploited. Accordingly, the optimized expression for computation of the convolution sum is shown in Eq. (1).

$$y[n] = b_0(x[n] - x[n-6]) + b_1(x[n-1] - x[n-5]) + b_2(x[n-2] - x[n-4]) \tag{1}$$

As seen the number of product terms is reduced from 6 to 3, but the number of additions remains same at 5. This is a huge savings in computation resources (50%), since multiplication of two 16-bit numbers in Q15 fixed-point format consumes lot of resources. This optimization works very well if the implementation of the system is done using DSPs, which have dedicated multiply-and-accumulate (MAC) units. In

Table 1 FIR filter coefficients for M = 7

b_k	Values	Q15	Non 0's	CSD	Non 0's
b_0	0.15175991026808974	0001001101101101	8		
b_1	−0.41604328754013736	1100101010111111	11		
b_2	0.94234994673082473	0111100010011111	10		
b_3	0	0000000000000000	0		
b_4	−0.94234994673082473	1000011101100001	7	$\bar{1}0001000\bar{1}0\bar{1}00001$	5
b_5	0.41604328754013736	0011010101000001	6	$010\bar{1}010101000001$	6
b_6	−0.15175991026808974	1110110010010011	9	$000\bar{1}0\bar{1}001001010\bar{1}$	6

the application chosen here, the filter coefficients are fixed, and so the multiplier or MAC unit need not be programmable to take different values of coefficients. Thus, the focus of optimization should now be towards multiplication of an input variable by a constant coefficient. This leads to further exploration in optimal multipliers starting from the shift-and-add algorithm which is discussed in the next section.

In Sect. 2, the specific case of multiplication of a constant with a variable is discussed along with the need to use the transposed form architecture of FIR. Section 3 explores the possibility of reducing the number of adders through Canonic Signed Digit representation of the filter coefficients. Section 4 explores the possibilities of using common sub-expressions in multipliers and other techniques to minimize the hardware requirements. In Sect. 5, the top-level architecture of the design is presented along with validation of design and the results of synthesis. Finally, the concluding observations are presented in Sect. 6.

2 Constant-Coefficient Multiplication

Constant-coefficient multiplication optimization is one of the important domains of low power and area-efficient designs of FIR filters. Literature in this domain has extensive research on two types of problems: single constant multiplication (SCM) [9] and multiple constant multiplication (MCM) [10]. In literature related to digital signal processing, the minimization of area and computation time is seen as major criteria. In [1], the authors propose an algorithmic optimization which discovers the common sub-expressions that exist in the computations of various products. In [5], the authors propose a multiplier-less FIR filter using a CSD notation which minimizes the number of non-zero values in the constant coefficient. Apart from the algorithmic changes, some optimizations are also done at the architecture level. In [2], Duraiswamy et al., propose an area-efficient FIR architecture that uses the anti-symmetry property to compute only half of the overall products needed to be computed. The remaining products are evaluated by using NOT gates and setting the carry-in of the remaining tap adders to ‘1’.

In the design problem chosen in this paper, the focus is to arrive at the trade-off in filter architectures in choosing between direct versus transposed form FIR structure, Q15 versus optimal CSD implementation and finally searching for common sub-expressions or/and shifters in the design which can be shared across all the product terms and not just a single multiplication. Since the length of the FIR filter is small, manual sub-expressions with a mix of Q15 and CSD representation are used to discover common sub-expressions.

The most basic form of constant-coefficient multiplier is a shift-and-add multiplier, in which the number of add operations required is one less than the number of non-zero bits in the constant coefficient [6]. The initial design of the FIR filter is implemented using 16-bit adders and shifters. In order to exploit the anti-symmetry property of the design, and use a simple shift-add architecture, an equality of the form $b_0x[n] = -b_6x[n]$ should exist. This is not possible if a direct form of FIR structure is used as in this case the multiplication by anti-symmetric coefficients is with different input samples, $b_0x[n]$ and $b_6x[n-6]$. To summarize, we need to store the original result of $b_0x[n]$ and use it later for computation of $b_6x[n-6] = -b_0x[n]$. This scenario could be avoided if a transposed structure of FIR is used. In this case, the multiplication needed is with the same input sample across the structure at any given point of time. The assignment $b_0x[n] = -b_6x[n]$ in digital logic is easily achieved by means of an inversion and addition by '1', since Q15 notation uses 2's complement notation.

Multiplication by -1 can be simply achieved by using NOT gates for inversion and setting the carry input to '1' in the tap adders wherever needed. The constant-coefficient data is represented using Q15 format and the corresponding values are shown in Table 1 in the third column. In the design option, there is a choice to either use Option 1: $\{b_0, b_1, b_2\}$ or Option 2: $\{b_4, b_5, b_6\}$, to exploit the anti-symmetry property. The choice is then decided based on the total number of non-zero bits in the sets of three coefficients. As seen from the fourth column in Table 1, Option 1 has 29 non-zero bits as compared to Option 2 which has 22 non-zero bits. Also the first adder in Option 1 would need inputs as $\{b_6x[n]$, $b_5x[n]\}$ and an additional adder to add '1' despite using carry-in as '1' for one of the adders. To summarize, Option 1 needs $7 + 10 + 9 + 1 + 5 = 32$ adders while Option 2 needs $6 + 5 + 8 + 5 = 24$ adders, which is a reduction in requirement of adders by 25%.

Thus, multiplication using Q15 notation for filter coefficients requires 13 unique shifters and 20 shifters in all. The transposed form of the FIR differentiator now need not use 6 multipliers but uses only 3 multipliers. The remaining 3 product terms are implemented using 'multiply by 1' logic, which uses NOT gates and the binary '1' is added in the tap adders at next stage as discussed earlier in this section. The entire FIR structure can now be rearranged and is as shown in Fig. 1. This is the most basic architecture which does not optimize the multiplication operation. This architecture is referred to as 'A1' in this paper. It uses Q15 representation of constant coefficients and a shift-and-add architecture for multiplication. All the data lines in the architecture are of 16-bit width, except for the carry-in of the last three tap adders

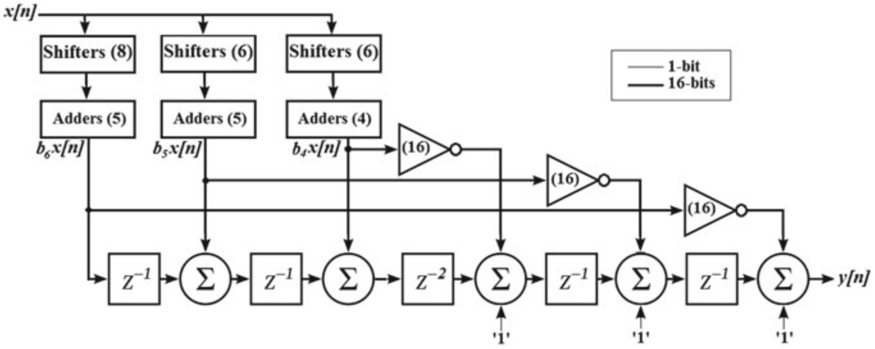


Fig. 1 FIR differentiator using Q15 (A1)

which is 1-bit width. The control lines which are used for clock, reset and enable are not shown in the figure. The next section explores the possibility of further reduction in the number of adders required for computing the convolution sum.

3 Canonic Signed Digit Multiplication

The constant filter coefficients can be recoded such that they contain the fewest number of non-zero bits which can be accomplished using 'Canonic Signed Digit' (CSD) representation. CSD recoding enables the reduction in the number of partial products during multiplications [7, 8]. The filter coefficients in the design discussed here can now be recoded using the 16-bit CSD representation for the three coefficients b_4, b_5 and b_6 as shown in last two columns of Table 1. The architecture which uses optimal CSD representation for constant coefficients and shift-add method for multiplication is referred to as 'A2' in this paper. Architecture 'A2' uses 19 adders, 15 shifters (11 unique shifters) and 48 NOT gates, and is shown in Fig. 2. The number of adders required in 'A2' is now $4 + 5 + 5 + 5 = 19$, which is a reduction of 21% as compared to 'A1'. The architecture presented here is similar to [2] in which Jason Thong et al., demonstrate the usage of NOT gates and tap adders with carry-in set to '1' to implement the negation operation of half of the product terms in anti-symmetric FIR architecture. In this paper, we propose a further optimization of the architecture where in common sub-expressions are explored along with shift operations which can be shared across all the product terms. Once the number of adders required for overall implementation is minimized, the next level of optimization is explored in the shifters used for multipliers. The next section explores various ways of optimizing the shift operation in the CSD multiplier.

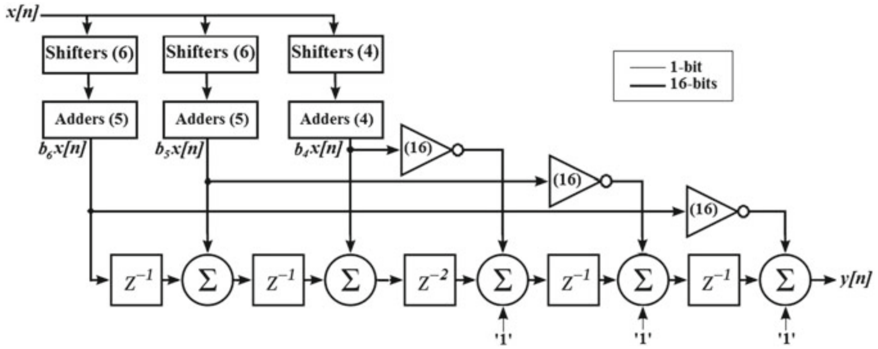


Fig. 2 Optimized architecture of FIR differentiator using CSD (A2)

4 Optimization of CSD Multiplier

The computation of convolution sum involves using 3 multiplications which are executed concurrently, namely $b_4 x[n]$, $b_5 x[n]$ and $b_6 x[n]$. These product terms are implemented using a series of shift-and-add operations. The next process of optimization is to focus on minimizing the overall number of computations. Since in all the multiplication operations one of the inputs is the same input sample $x[n]$, there is a scope to share some of the addition or/and shift operations. This gives rise to possibilities of re-examining the choice of using CSD for all multiplications. The first task is to identify the occurrence of any common sub-expressions which may appear in common across 2 or 3 multiplications in the design. In that case, because of concurrency in the computation, these sub-expressions can be shared across the multipliers, thereby reducing the quantum of resources consumed. There could be a scenario where a direct Q15 representation would yield more common sub-expressions as compared to the CSD format. Another possibility is a combination in which 1 or 2 multiplications are in Q15 and the other/s are in CSD format, may yield more common sub-expressions.

The final selection of the data representations of constant coefficient happens based on that combination which leads to least number of adders. In the design of FIR differentiator used here, and the final choice is CSD implementation of all the three coefficients as there is no common sub-expression. This choice is definitely not a universal choice, since the optimizations are heavily dependent on the number of filter coefficients and their values. The next level of optimization is to choose that option which needs least number of unique shifters and also maximum number of shifters which are shared. In the next part of this section, the possibility of sharing the shifters is explored further.

The logical structure of a shifter if implemented in an FPGA is hard wiring between the bit registers. For example, a $y = (x[n] \gg 1)$ shifter, which is a right shift by 1, would simply connect bit $x[15]$ to $y[14]$, $x[14]$ to $y[13]$ and so on till the connection $x[1]$ to $y[0]$. The most significant bit of $y[15]$ is then cleared to '0'. Thus, there is no need to have any underlying logic like OR/AND gates in between, irrespective of the amount of shifts needed. The only additional logic needed for the shifter would be the control and reset logic which decides when the shifter should be enabled and under what circumstances it should be reset. Since the shift operations are concurrent for all the three multiplications encountered here, the common shift operations can be shared which results in an alternate architecture which uses only 11 shifters as compared to 16 in 'A2', other resources being the same. This architecture is optimal in that it uses minimum number of adders and shifters as compared to 'A1' and 'A2', and is shown in Fig. 3. A seen the last three tap adders in the architecture have an additional carry input of '1', which is needed to implement the negation expression for the coefficient product terms discussed in Sect. 2. All the data lines in the architecture are of 16-bit width except the carry-in bits of last 3 tap adders which are single-bit width. Again the control lines which are used for clock, reset and enable are not shown in this figure.

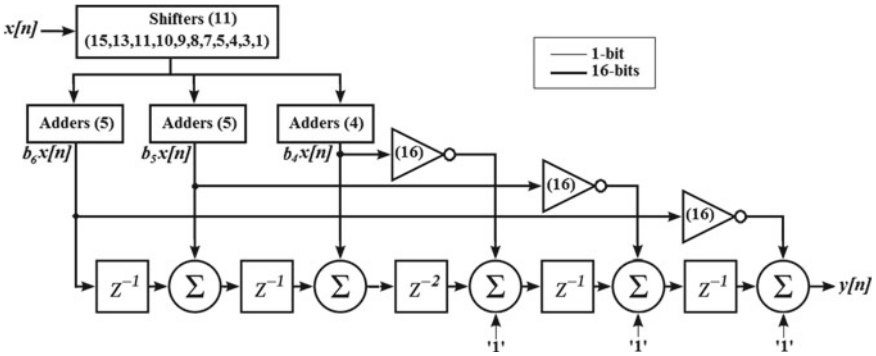


Fig. 3 FIR differentiator using shared CSD shifters (A3)

5 Results and Discussion

The prototyping of the FIR differentiator is done on a FPGA development board using multiple architectures as discussed here. All 3 designs use the multiplier-less architecture in a transposed structure of FIR filter. All 3 designs implement 3 coefficient products, and the remaining 3 product terms are arrived at by using anti-symmetry property of filter coefficients using NOT gates. The design A1 is implemented using Q15 notation for constant coefficients. In design ‘A2’ optimal CSD notation is used, which minimizes the number of adders in the architecture. Finally, in ‘A3’, the shift operations are shared between concurrent multiplications yielding an optimal architecture.

This paper presents the synthesis results for a Spartan6 FPGA device. The results of synthesis of all the 3 architectures ‘A1’, ‘A2’ and ‘A3’ are listed in Table 2. The results of number of ‘adders’ have already been established earlier through the design of FIR architectures. Both ‘A2’ and ‘A3’ have 21% lesser number of adders as compared to ‘A1’. The overall area of the implementation is estimated based on the sum total of slice registers and LUTs used in the design. Based on the synthesis results it is seen that ‘A2’ is 16.2% area-efficient than ‘A1’, while ‘A3’ consumes 21.5% lesser area than ‘A1’. This reduction demonstrates the benefits of using optimal CSD representation of the filter coefficients instead of notation in Q15 format.

The number of latches used in ‘A3’ is the highest at 528, while ‘A3’ is better than ‘A2’ by 16%. This optimization is due to sharing of shifters among all the product terms in the FIR implementation. The reduction in complexity for ‘A3’ is 33.3% when compared to ‘A1’. This proves that the architecture ‘A3’ is the most area-efficient as compared to [2]. The reduction in area obviously reduces the power consumption of the system as seen in Table 2. It is seen that ‘A3’ consumes the least power at 2.4 mW, which is an additional power savings of 1.24 and 2.95% as compared to ‘A2’ and ‘A1’, respectively.

Table 2 Comparison of FIR differentiator architectures

Parameter	A1	A2	A3
Slice registers	511	430	417
Slice LUTs	446	372	334
LUT FF pairs	564	479	463
Adders	24	19	19
Latches	528	419	352
Datapath delay (ns)	13.823	11.273	11.462
Power (Logic+Signal) (mW)	3.4	2.43	2.40

The area and power advantages in ‘A3’ come at the cost of increased data path delay of 11.462 ns, which is 1.7% slower than ’‘A2’. But it is definitely faster than ‘A1’ by 17.1%.

6 Conclusion

The design and implementation of an FIR differentiator to estimate the velocity from suspension displacement are presented. The advantage in optimizing hardware resources by using the transposed form of FIR filter structure is demonstrated. It allows to convert the problem of single constant multiplication to multiple constant multiplication, thereby allowing for sharing of resources by means of common subexpressions and shifters. An alternate representation of Q15 filter coefficients using Canonic Signed Digit is presented, which yields an area optimization of 22% for the chosen design specifications. The number of adders needed for implementation of the FIR convolution sum is also reduced by 21%. The design complexity in terms of latches and multiplexers used reduces by 33% as compare to the standard Q15 representation. The proposed design is also power efficient by 3% and computes the sum faster by 17%. The future work is to explore implementation of the FIR differentiator is VLSI where further optimizations can be done at circuit-level of abstraction.

References

1. Chen MC, Chen TT (2014) Minimizing design costs of an FIR filter using a novel coefficient optimization algorithm. Math Probl Eng 1–9. https://doi.org/10.1155/2014/497471
2. Duraiswamy P, Bauwelinck J, Vandewege J (2011) Efficient implementation of 90 phase shifter in FPGA. EURASIP J Adv Sig Proc 2011(1):32

3. Eligar S, Banakar RM (2014) A model based approach for design of semiactive suspension using variable structure control. Int J Tech Res Appl. e-ISSN 2320–8163
4. Eligar S, Banakar RM (2018) Optimization of control algorithm for semi-active suspension system. In: 2018 proceedings of the international conference on intelligent computing and sustainable system
5. Illa A, Haridas N, Elias E (2016) Design of multiplier-less FIR filters with simultaneously variable bandwidth and fractional delay. Eng Sci Tech Int J 19(3):1160–1165
6. Mitra SK, Kaiser JF (1993) Handbook for digital signal processing. Wiley, New York
7. Parhi KK (2007) VLSI digital signal processing systems: design and implementation. Wiley, New York
8. Proakis JG (2001) Digital signal processing: principles algorithms and applications. Pearson Education, India
9. Thong J, Nicolici N (2010) A novel optimal single constant multiplication algorithm. In: Proceedings of the 47th design automation conference, pp 613–616. ACM
10. Thong J, Nicolici N (2011) An optimal and practical approach to single constant multiplication. IEEE Trans Comput-Aided Des Integr Circ Syst 30(9):1373–1386

Optimized Prediction Model to Diagnose Breast Cancer Risk and Its Management

Athira Vinod and B. R. Manju

Abstract Breast malignancy is the second biggest disease that results in fatal condition for women population. Research endeavors have revealed with expanding affirmation that the support vector machines (SVMs) have more noteworthy precise conclusion capacity. In this paper, breast disease determination is dependent on a SVM-based technique that has been proposed. Investigations have been directed on various preparing test allotments of the Wisconsin breast malignancy dataset (WBCD), which is generally utilized among scientists who use machine learning strategies for breast disease conclusion. The working of the technique is assessed by utilizing characterization precision, particularity positive and negative prescient qualities, collector working trademark bends, and perplexity lattice. The outcomes demonstrate that the most elevated grouping precision (99%) is achieved for the SVM.

Keywords Breast cancer classification · Support vector machine (SVM)

1 Introduction

Breast disease is the most widely recognized harm among women, representing almost 1 of every 3 tumors analyzed among women in the USA, and it is the second driving reason for malignancy demise among women. Breast cancer happens because of anomalous cell developing in the breast tissue, generally alluded to as a tumor. A tumor does not mean disease—tumors can be considerate (not harmful), pre-threatening (pre-dangerous), or dangerous (malignant) [1, 2]. Tests such as MRI,

A. Vinod (✉)
Amrita Center for Wireless Networks & Applications (AWNA), Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Amritapuri 690525, India
e-mail: athiravinodathu@gmail.com

B. R. Manju
Department of Mathematics, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Amritapuri 690525, India
e-mail: manjubr@am.amrita.edu

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_48

mammogram, ultrasound, and biopsy are commonly used to diagnose breast cancer performed.

According to the studies, breast cancer is the most common type of cancer for women regardless of race and ethnicity. Although we may not be aware of all the factors contributing to develop breast cancer, certain attributes such as family history, age, obesity, alcohol, and tobacco use have been identified from research studies on this topic [3]. Like the classification of different features of breast cancer, there are mechanisms to find the faults which occur in variable wind turbine blade using J48 algorithm [4].

The previous research work carried out in the domain of breast cancer: In [5], a method was proposed to work on a set of images which were extracted from MIAS and DDSM databases based on local binary pattern (LBP).

In [6], a method is proposed to detect mammograms, which in turn is used to determine the breast cancer. Here, the algorithms like logistic regression, decision tree, and Hoeffding tree is used and a comparative analysis is done to validate the accuracies. But the method uses, neglecting missing values and working over the remaining dataset, which is not feasible due to the reason that every data is important and must be handled in a way such that no data is lost.

In [7], classification of breast cancer into benign and malignant is done using SVM classifier which produces an accuracy of 92.15%. Hence, the following proposed model is for optimizing the existing SVM classifier and gives a best accurate model.

In [8], discovery of breast malignant growth utilizing (a) marker-controlled level set division of anisotropic dispersion sifted preprocessed picture versus and (b) segmentation utilizing marker-controlled level set on a Gaussian-separated picture. This is reasonable for highlight extraction in PC supported breast malignant growth finding.

In [9], the results show that the level set method and improved edge map are suitable for the accurate segmentation of breast regions from thermal images. The capability of anisotropic filter on breast thermograms is determined and validated by extracting the tissues using level sets.

2 Objective

The marks in the information are discrete, and the expectation falls into two classifications (e.g., dangerous or favorable). In machine learning, this is an arrangement issue. In this way, the objective is to arrange whether the breast disease is amiable or threatening and foresee the repeat and non-repeat of harmful cases after a specific period. To accomplish this, the model utilized machine learning characterization strategies to fit a capacity that can foresee the discrete class of new info.

3 Proposed System

This work focuses on investigating the probability of predicting the type of breast cancer (malignant or benign) from the given characteristics of breast mass computed from digitized images. The cases provided are cases diagnosed with some type of tumor, but only some of them (approximately 37%) are malignant. Here, the available data is examined and attempted to predict the possibility that a breast cancer diagnosis is malignant or benign based on the attributes collected from the breast mass.

The proposed methodology consists of the following steps [10]:

1. Identifying data sources.
2. Data preprocessing.
3. Data visualization (exploratory data analysis).
4. Machine learning prediction.

Proposed methodology of this prediction model is depicted in Fig. 1.

3.1 Identifying data sources

In [11], the dataset is accessible from machine learning store kept up by the University of California, Irvine. The dataset contains 569 examples of harmful and considerate tumor cells.

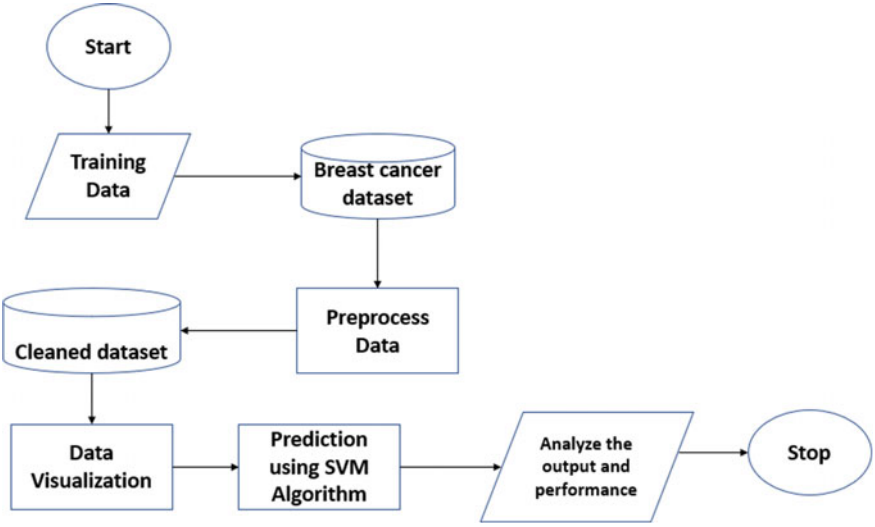


Fig. 1 Proposed methodology

- The initial two sections in the dataset store are one of cancers (M = malignant, B = benign), separately.
- The Sects. 3–3.2 contain 30 genuine esteem includes that have been registered from digitized pictures of the cell cores, which can be utilized to assemble a model to anticipate whether a tumor is amiable or dangerous.

3.2 Data Preprocessing

Data preprocessing [12] is an urgent advance for any information investigation issue. Usually, a smart thought to set up the information in such approach to best uncover the structure of the issue to the machine learning calculations that you expect to utilize. This involves a number of activities such as:

- Assigning numerical values to categorical data;
- Handling missing values; and
- Normalizing the features (so that features on small scales do not dominate when fitting a model to the data).

The objective of the data preprocessing is to locate the most prescient highlights of the information and channel it. Along these lines, it will upgrade the prescient intensity of the examination demonstrate.

In this work, the accompanying advances are taken consideration:

- Allocate highlights to a NumPy cluster X and change the class marks from their unique string portrayal (M and B) into numbers.
- Split data into training and test sets.
- Institutionalize the information.
- Acquire the eigenvectors and eigenvalues from the covariance lattice or connection grid.
- Sort eigenvalues in plunging request and pick the k eigenvectors that relate to the k biggest eigenvalues where k is the quantity of measurements of the new element subspace, $k \le dk \le d$.
- Build the projection lattice W from the chose k eigenvectors.
- Change the first dataset X by means of W to get a k-dimensional component subspace Y.

It is common to select a subset of features that have the largest correlation with the class labels. The effect of feature selection must be assessed within a complete modeling pipeline in order to give you an unbiased estimated of your model's true performance. Hence, in the next section you will first be introduced to cross-validation, before applying the PCA-based feature selection strategy in the model building pipeline.

3.3 Data Visualization

Exploratory data analysis (EDA) is an imperative advance which happens after element designing and obtaining information and it ought to be done before any demonstrating. This is on the grounds that it is essential for an information researcher to almost certainly comprehend the idea of the information without making suspicions. The aftereffects of information investigation can be very helpful in getting a handle on the structure of the information, the appropriation of the qualities, and the nearness of extraordinary qualities and interrelationships inside the informational index.

The purpose of EDA is:

- To utilize rundown measurements and representations to all the more likely comprehend information, discover pieces of information about the inclinations of the information, its quality and to detail suppositions, and the speculation of our hypothesis.
- For data preprocessing to be effective, it is fundamental to have a general image of your information. Basic factual portrayals can be utilized to distinguish properties of the information and features (which features esteems ought to be treated as commotion or exceptions). Next step is to explore the data. There are two approaches used to examine the data using:
- **Descriptive statistics** is the way toward gathering key attributes of the informational index into straightforward numeric measurements. A portion of the regular measurements utilized is mean, standard deviation, and relationship.
- **Visualization** is the way toward anticipating the information, or parts of it, into Cartesian space or into dynamic pictures. In the information mining process, information investigation is utilized in a wide range of steps including preprocessing, modeling, and interpretation of results.

At the end, we get the following conclusions, which are shown in the following Fig. 2:

- Mean estimations of cell span, edge, territory, conservativeness, concavity, and sunken focuses can be utilized in characterization of the malignancy. Bigger estimations of these parameters will in general demonstrate a connection with dangerous tumors.
- Mean estimations of surface, smoothness, and symmetry do not demonstrate an inclination of one conclusion over the other.
- In any of the histograms, there are no recognizable vast anomalies that warrants further cleanup.

3.4 Machine Learning Prediction

Support vector machines (SVMs) [13] learning algorithm will be used to build the predictive model. SVMs are one of the most popular classification algorithms and

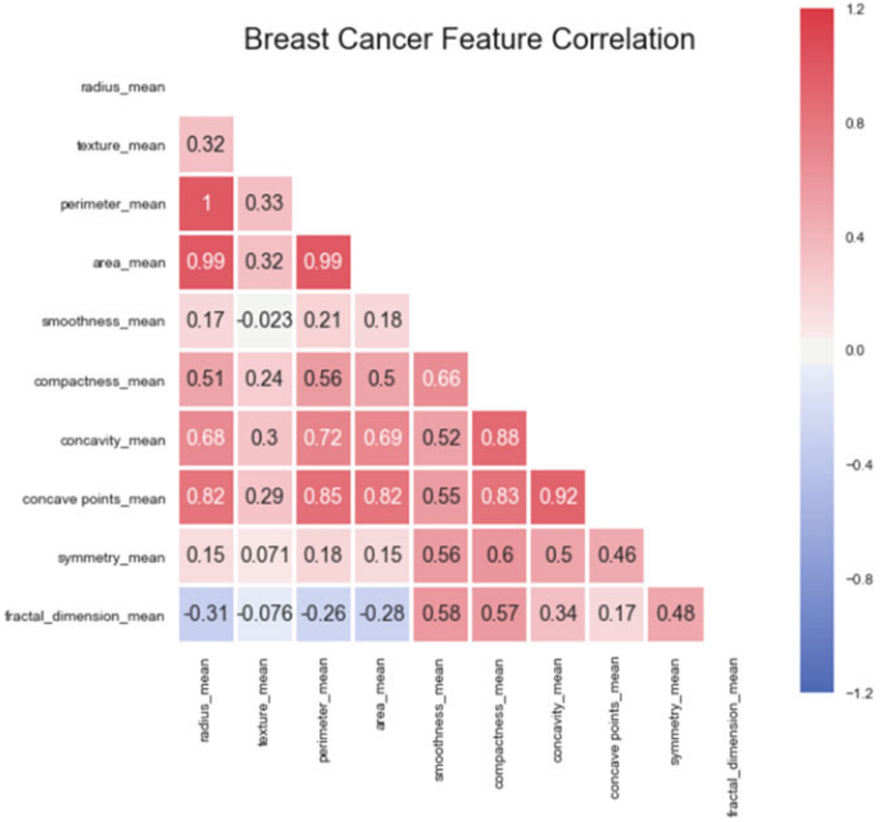


Fig. 2 Breast cancer feature correlation matrix

have an elegant way of transforming nonlinear data, so that one can use a linear algorithm to fit a linear model to the data.

Kernelized support vector machines [14] are ground-breaking models and perform well on an assortment of datasets.

- SVMs take into consideration complex choice limits, regardless of whether the information has just a couple of highlights.
- They function admirably on low-dimensional and high-dimensional information (i.e., few and numerous highlights) and however do not scale great with the quantity of tests.
- Running a SVM on information with up to 10,000 examples may function admirably yet working with datasets of size at least 100,000 can wind up testing regarding runtime and memory use.
- SVMs require cautious preprocessing of the information and tuning of the parameters. In this way, these days the vast majority incline toward tree-based models,

for example, irregular woodlands or angle boosting (which require practically no preprocessing) in numerous applications.

- SVM models are difficult to investigate; it very well may be hard to comprehend why a specific forecast was made, and it may be dubious to disclose the model to a non-expert.

Machine learning prediction has these following steps:

1. Split data into training and test sets.
2. Classification with cross-validation.
3. Model accuracy: receiver operating characteristic (ROC) curve.
4. Optimizing the SVM classifier.

3.4.1 Split Data into Training and Test Sets

This method to compare the performance of a machine learning algorithm is to use different training and testing datasets.

- Divide the available data into a training set and a testing set (70% training, 30% test),
- Train the algorithm on the 70% data,
- Make predictions on the 30% data, and
- Compare the predictions results against the expected results.

The extent of the split can rely upon the size and particulars of your dataset, despite the fact that usually to utilize 67% of the information for preparing and staying 33% for testing.

3.4.2 Classification with Cross-Validation

Split the data into test, and training set is crucial to avoid overfitting. This allows generalization of real, previously unseen data. Cross-validation extends this idea further. Instead of having a single train/test split, we specify so-called folds so that the data is divided into similarly sized folds.

- Training occurs by taking all folds except one—referred to as the holdout sample.
- On the completion of the training, you test the performance of your fitted model using the holdout sample.
- The holdout sample is then thrown back with the rest of the other folds, and a different fold is pulled out as the new holdout sample.
- Training is repeated again with the remaining folds, and we measure performance using the holdout sample. This process is repeated until each fold has had a chance to be a test or holdout sample.
- The expected performance of the classifier, called cross-validation error, is then simply an average of error rates computed on each holdout sample.

This process is demonstrated by first performing a standard train/test split and then computing cross-validation error. The three-fold cross-validation accuracy score for this classifier is 0.97.

3.4.3 Model Accuracy: Receiver Operating Characteristic (ROC) Curve

In statistical modeling and machine learning, a commonly reported performance measure of model accuracy for binary classification problems is area under the curve (AUC). To understand what information the ROC curve conveys, consider the so-called confusion matrix that essentially is a two-dimensional table where the classifier model is on one axis (vertical), and ground truth is on the other (horizontal) axis, as shown below. Either of these axes can take two values (as depicted).

In an ROC curve plotted, "true-positive rate" on the *Y*-axis and "false-positive rate" on the *X*-axis, where the values "true positive," "false negative," "false positive," and "true negative" are events (or their probabilities) as described above. The rates are defined according to the following equations:

- True-positive rate (or sensitivity)}:

$$\mathrm{tpr} = \mathrm{tp}/(\mathrm{tp} + \mathrm{fn}) \tag{1}$$

- False-positive rate:

$$\mathrm{fpr} = \mathrm{fp}/(\mathrm{fp} + \mathrm{tn}) \tag{2}$$

- True-negative rate (or specificity):

$$\mathrm{tnr} = \mathrm{tn}/(\mathrm{fp} + \mathrm{tn}) \tag{3}$$

In all definitions, the denominator is a row margin in the above confusion matrix. Thus, one can express

- The true positive rate (tpr) is defined as the probability that the model says "+" when the real value is indeed "+" (i.e., a conditional probability). However, this does not tell you how likely you are to be correct when calling "+" (i.e., the probability of a true positive, conditioned on the test result being "+").

Figure 3 shows the receiver operating characteristic example.

- To interpret the ROC correctly, consider what the points that lie along the diagonal represent. For these situations, there is an equal chance of "+" and "−" happening. Therefore, this is not that different from making a prediction by tossing an unbiased coin. Put simply, the classification model is random.

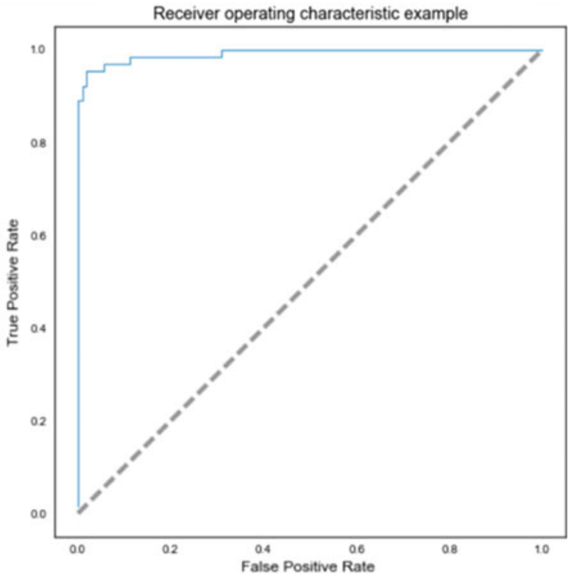


Fig. 3 Receiver operating characteristic example

- For the points above, the diagonal, tpr > fpr, and the model say that you are in a zone where you are performing better than random. For example, assume tpr = 0.99 and fpr = 0.01, Then, the probability of being in the true-positive group is

  $(0.99/(0.99 + 0.01)) = 99\%$.
- Furthermore, holding fpr constant, it is easy to see that the more vertically above the diagonal you are positioned, the better the classification model.

3.4.4 Optimizing the SVM Classifier

Machine learning models are parameterized, so their conduct can be tuned for a given issue. Models can have numerous parameters, and finding the best mix of parameters can be treated as an inquiry issue. In the code built up, the point is to tune parameters of the support vector machine (SVM) classification show utilizing scikit-learn.

We can tune two key parameters of the SVM algorithm:

- The value of *C*
- And the type of kernel.

The default method for SVM (the SVC class) is to use the radial basis function (RBF) kernel with a *C* value set to 1.0. *C* value which indicates range of relaxation of margin. Like with *K*-nearest neighbor (KNN), a grid search using 10-fold cross-validation with a standardized copy of the training dataset is performed. The demonstration of SVC with RBF kernel is shown in Fig. 4. For the RBF kernel, the value of gamma is set to be 0.7 for the optimization. This predictive model used

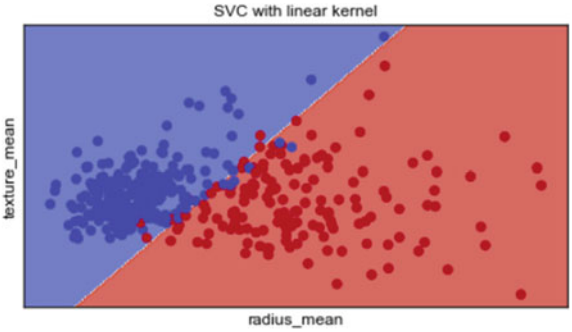


Fig. 4 SVC with linear kernel

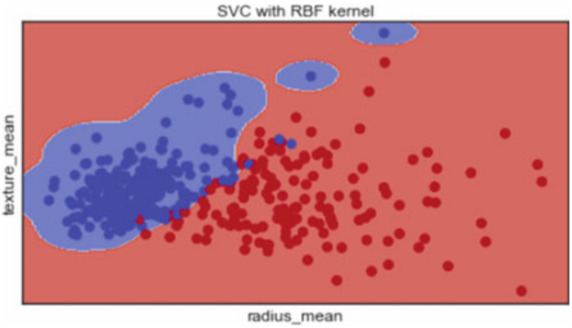


Fig. 5 SVC with RBF kernel

number of simpler kernel types like linear kernel and polynomial kernel, with *C* as regularization parameter (Fig. 5).

- *C* values < 1 indicate less bias.
- *C* values > 1 indicate more bias.

The predictive model with kernel types like linear, polynomial (degree 3), and RBF is creating decision boundaries for the classifiers by considering the mean values of radius and texture.

Python scikit-learn provides two simple methods for algorithm parameter tuning:

- grid search parameter tuning.
- random search parameter tuning.

4 Results

There are two possible predicted classes: “1” and “0.” Malignant = 1 (indicates presence of cancer cells) and benign = 0 (indicates absence).

- The classifier made a total of 174 predictions (i.e., 174 patients were being tested for the presence of breast cancer).

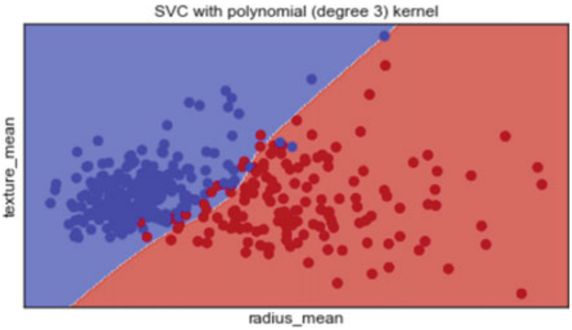


Fig. 6 SVC with polynomial kernel

- Out of those 174 cases, the classifier predicted "yes" 58 times and "no" 113 times.
- In reality, 64 patients in the sample have the disease, and 107 patients do not (Fig. 6).

Rates as computed from the confusion matrix.

1. **Accuracy**: Overall, how often is the classifier correct?
   - (TP + TN)/total = (57 + 106)/171 = 0.95
2. **Misclassification Rate**: Overall, how often is it wrong?
   - (FP + FN)/total = (1 + 7)/171 = 0.05 equivalent to 1 minus Accuracy also known as "**Error Rate**."
3. **True-Positive Rate**: When it is actually yes, how often does it predict 1?
   - TP/actual yes = 57/64 = 0.89 also known as "Sensitivity" or "**Recall**."
4. **False-Positive Rate**: When it is actually 0, how often does it predict 1?
   - FP/actual no = 1/107 = 0.01.
5. **Specificity**: When it is actually 0, how often does it predict 0? Also known as **true-positive rate**.
   - TN/actual no = 106/107 = 0.99 equivalent to 1 minus false-positive rate.
6. **Precision**: When it predicts 1, how often is it correct?
   - TP/predicted yes = 57/58 = 0.98.
7. **Prevalence**: How often does the yes condition actually occur in our sample?
   - actual yes/total = 64/171 = 0.34.

The optimized SVM classifier accuracy is 0.99. The fivefold cross-validation accuracy score for this classifier is 0.97.

Performance measure in terms of precision, recall, f1-score, and support is tabulated in Table 1. The demonstration of predicted versus actual values can be seen in Fig. 7.

Table 1 Performance measure of the classifier

	Precision	Recall	f1-score	Support
0	0.94	0.98	0.96	107
1	0.97	0.89	0.93	64
Avg/total	0.95	0.95	0.95	171

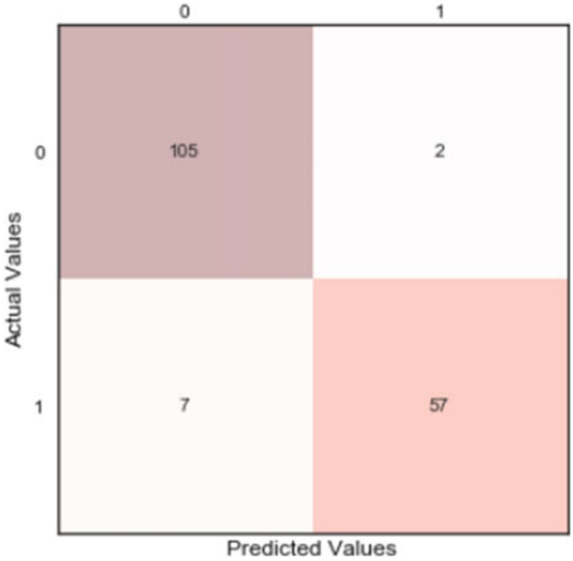


Fig. 7 Predicted values versus actual values

5 Conclusion

This work exhibits the displaying of breast cancer as arrangement assignment utilizing support vector machine joined with highlight choice. The SVM performs better when Wisconsin breast cancer dataset (WBCD) is institutionalized, with the goal that all characteristics have a mean estimation of zero and a standard deviation of one. We can figure this from the whole preparing dataset and apply the equivalent change to the info properties from the approval dataset. The execution of the model is assessed as far as exactness, false-positive rate, false-negative rate, specificity, precision, prevalence, misclassification rate, and ROC. The outcomes demonstrate that the SVM display that contains five highlights is advanced execution for the model.

References

1. Dheeba J, Tamil Selvi S (2011) Classification of malignant and benign microcalcification using SVM classifier. In: 2011 international conference on emerging trends in electrical and computer technology, Nagercoil, 2011. pp 686–690

2. Karahaliou N et al (2008) Breast cancer diagnosis: analyzing texture of tissue surrounding microcalcifications. IEEE Trans Inf Technol Biomed 12(6):731–738
3. Bardou D, Zhang K, Ahmad SM (2018) Classification of breast cancer based on histology images using convolutional neural networks. IEEE Access 6:24680–24693
4. Manju BR, Joshuva A, Sugumaran V A data mining study for condition monitoring on wind turbine blades using Hoeffding tree algorithm through statistical and histogram features. Int J Mech Eng Technol (IJMET) 13(1):102–121
5. Král P, Lenc L (2016) LBP features for breast cancer detection. In: 2016 IEEE international conference on image processing (ICIP), Phoenix, AZ, 2016. pp 2643–2647
6. Manju BR, Amrutha VS (2018) Comparative study of datamining algorithms for diagnostic mammograms using principal component analysis and J48. ARPN J Eng Appl Sci
7. Souza JC et al (2017) Classification of Malignant and Benign tissues in mammography using dental shape descriptors and shape distribution. In: 7th Latin American conference on networked and electronic media (LACNEM 2017)
8. Witten IH, Frank E, Hall MA, Pal CJ (2016) Data mining: practical machine learning tools and techniques. Morgan Kaufmann
9. Gopakumar S, Sruthi K, Krishnamoorthy S (2018) Modified level-set for segmenting breast tumor from thermal images. In: 2018 3rd international conference for convergence in technology (I2CT)
10. https://www.cs.cmu.edu/~ggordon/SVMs/new-svms-and-kernels.pdf
11. UCI machine learning repository, breast cancer Wisconsin (Diagnostic) dataset, https://archive.ics.uci.edu/ml/datasets/Breast+Cancer+Wisconsin+%28Diagnostic%29
12. Data Preprocessing, http://www.cs.ccsu.edu/~markov/ccsu_courses/datamining-3.html
13. Mandhala VN, Sujatha V, Devi BR (2014) Scene classification using support vector machines. In: 2014 IEEE international conference on advanced communications, control and computing technologies, Ramanathapuram, 2014. pp 1807–1810
14. Support Vector Machines and Kernel Methods, 2004

Smart Cane Design for Indoor and Outdoor Navigation: A Cost-Effective Guide

Vandana Mansur and R. Sujatha

Abstract In this paper, the distinction between prototype and product is clearly described. During product design, there are many processes involved which pave a way for an operational product. The discussion on different types of prototypes gives the designer a better insight into the product deployment and testing phase. The in-depth knowledge of the testing involved in different types of prototypes assures that all the technical specifications and product specifications are considered. A questionnaire is developed to design the product that gives the detailed description of the design flow which is to be followed during the development phase. The field testing steps to be followed are known in advance if a proper design flow is adopted. The concept of "Engineering, Design and Process" is discussed in detail for the product design approach.

Keywords Smart cane · Product design · Microcontroller

1 Introduction

The visually challenged are those who are deprived of the ability to visualize the world. They face many difficulties and challenges. According to recent statistics, there are around 217 million people with visual imparity. Statistics also show that 80% of individuals aged over 50 are visually impaired. It is good and of more use, if comfortable and user-friendly assistance is provided in terms of cost-effective devices.

In [1–3], a blind stick model is developed using Arduino Uno, infrared sensor, ultrasonic sensor, LCD display, playback module and voltage regulator. The ultrasonic sensor detects the object ahead of the person by measuring the distance from the object to the stick. To detect the objects in left and right, IR sensors are used.

Vandana Mansur (✉) · R. Sujatha
School of Electronics Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India
e-mail: vandanacmansur@gmail.com

R. Sujatha
e-mail: sujatha.r@vit.ac.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_49

The objects appearing very close are also detected. IR sensor is used in order to avoid calculation problem which may be caused by using many ultrasonic sensors. To assist the blind person to reach the destination, a voice playback module is used and that is controlled through commands generated by microphone. The intention here is to develop a friendly sensing device for the blind. Power bank of 5 V is supplied for the circuit that maintains a constant level of power supply for its working. The software coded is embedded on to the Arduino board and the model works accordingly [4, 5].

In [6], the authors describe modeling of the sensor-assisted stick done by using Pro/E Creo 5.0 software. The PRO/Engineer is 3D CAD/CAM/CAE-integrated software developed by Parametric Technology Corporation (PTC). It is one of the world's leading CAD/CAM/CAE softwares that provide a wide range of integrated solutions for various aspects of product designing and manufacturing. This application was the first to market that provides a feature for solid modeling, drafting and assembly modeling, finite element analysis and NC and tooling function for mechanical engineers.

The microcontroller used here is ATmega8. It is based on AVR RISC architecture which is low-powered CMOS 8-bit microcontroller. The sensor consists of distance measurer comprising of position-sensitive detector, infrared emitting diode (IRED) and signal processing unit. Triangulation method is opted for distance detection, and this works more or less like a proximity sensor. The piezo buzzer used produces sound that is a warning or indication to the user. It works on reverse process of the piezoelectric effect. A playback voice recorder is used which speaks out the voice once there is any obstacle detected. Suppose if the top-side sensor detects an obstacle, then the recorder speaks out as "Top, Top,…". This helps the user to detect obstacle and change his path to reach his destination.

In [7], the authors have developed an intelligent walking stick especially for the blind by using radio-frequency identification (RFID) technology, which tracks the objects using electromagnetic fields that automatically identify the tags attached to the object. This technology also uploads the person's location data which helps the family members of the user to locate the blind person and monitor his or her movements. It is very difficult for the visually impaired people to travel alone in unknown places as they do not have any information regarding their location. In order to make their mobility easier, the different technologies like GSM and GPRS are used for their navigation. This system uses GPS for outdoor navigation and GSM or GPRS to send the information to their family member [8, 9].

The RFID tag is used for indoor navigation. The RFID sensor is installed on the walking stick of the visually impaired. The tags provide a landmark to the blind person. Each tag will be fed with the information of the direction and location so that the current location is determined precisely. For the safety purpose, the RFID tag is covered with a protective shield. The only drawback of using RFID could be the cost-effectiveness. As two technologies are used for both indoor and outdoor navigations, this is an effective solution for the blind [10, 11].

The working of the above solution is as follows. The obstacle is detected by the sensor and distance is calculated; the distance is matched with the code, and then, the buzzer gets activated. The GPS is interfaced with GSM model to locate the person's position; the location is updated in the server and sent to the android application which gives the account of the travel route of the blind [12–15].

2 Prototype and Product: An Overview

Prototype can be called as "original form" of the end vision product. Prototypes are the sample products or model built to replicate a design or test a concept learnt. Generally, a prototype is used to evaluate and enhance the design, accuracy and precision of the product concept used. Prototype serves as a real-time working system providing the specifications rather than a theoretical one. Prototyping can be considered as a bridge or a step between the formation and visualization of an idea or a concept and the evaluation of the same. Thus, the process of prototyping can be called as materialization. Prototype can also be called as the "primitive form" [16, 17].

Prototype is a proof of concept for a new idea or product that proves the viability and illustrates the applications of the new technology. There are many types of prototyping like electronics prototyping, software prototyping, data prototyping and scale modeling [18, 19].

There are two types of prototype: alpha and beta prototypes. Alpha prototype is used to check whether the product works as expected. It is a similar product in size, shape, material and features as the final product will be after production. It is a modeled product. Beta prototype is made to see the reliability of the product to be manufactured. The prototype is checked through remaining bugs and mistakes in the final product. This model product is given to customers for testing in the real environment. Beta prototype is modeled with the actual parts, material and process that are to be followed during production.

A product can be described as a design that is the final produce of a process with proper efforts. It is a physical quantity that can be seen, touched, felt and used. A product is a bundle of objects which consists of different features, benefits, services, style, color, quality, grade and structure that fulfills the consumer needs and requirements. A product has all the characteristics concerned to the customers. Thus, the companies need to keep changing the product design which could be the prototype for the new product that remains competitive in this rising consumerist culture. The two classifications of a product are tangible and intangible. Tangible product is referred as a physical object seen or touched. An intangible product can only be felt like an insurance policy or a service.

A product is offered for sale but a prototype cannot be sold. The prototype is just a basic proof of a design, but a product is added up with many more features and factors such as manufacturing, packing, transportation, power source, external appearance, color, style and also effectiveness. A prototype may fail to prove the idea, but a product should be relevant and have an immediate use . It should functionally perform for what it is designed. Quality also plays an important role in the materials used for the product. Products need to be marketed, wherein advertising and 'brand building' come to entity. The product needs to stand out and a brand name could make this possible.

3 Product Design Steps

Requirement analysis for the product design is done in this work. It is the societal need for the visually challenged to lead a quality life. The basic requirement analysis of a compact power supply, handy device, proper concealing of the controller unit and aesthetics of the device is important.

There are six steps to be followed for the process of product design.

1. Idea generation;
2. Screening ideas;
3. Feasibility study;
4. Preliminary design;
5. Pilot runs and testing;
6. New product launch.

The idea generation is a process that begins with understanding the needs and services of the customers. Ideas evolve from various sources both from inside and outside of the field. It can be the employees, marketing team, research team or sales force and reverse engineering. The external idea generation can be from the consumers, environmental factors, technological strategies and other factors. The product developers need to set a benchmark to find the best in the product that meets the performance required. Reverse engineering is also important in inspecting the competitor's products and can incorporate new design features to improve the product.

Screening of ideas is necessary for eliminating those that do not have high potential, so as to avoid the losses which could be incurred in future stages. The product development committee sets certain criteria that need to be met in the product, and each member gives a proposal supported by sample models, graphics, outline models and technical specifications. This helps to avoid the degree of overlap with the products and services that already exist. For a better progress, each dimension of the idea can be scaled on 0–10 and then proceed further.

Feasibility study is to analyze the market, economic and technical strategies. The market survey gives an analysis whether the proposed product is in demand by the customers so that the product making can be continued. If the demand is met, then economic analysis is to be made which aims to establish a cost-effective product in comparison with the present estimated sales volume. Finally, the technical specification is concerned with technological viability of the product, production and manufacturing, requirement of the chemical materials. If this analysis passes the study, then product making is continued.

In preliminary design, the engineer builds a prototype followed by its testing and retesting till the design meets the expected results. The physical appearance, size, shape, color and style are taken care off. The brand identification, market image, finishing, etc., will also be seen through. Pilot runs and testing before finalizing the design adjustments are made in the product. To check the consumer acceptance of the product, market testing is also carried out, which helps in launching the product in the market.

Consistent production and marketing abilities are required by the company to sell the product. The company should develop the confidence in their ability of production and marketing as the volume increases and should work in a coordinated manner to launch a product successfully.

Figure 1 shows the product design flowchart. In this one notice testing at each stage is an important step. It is testing that ensures the design flow used is correct and optimal. In industry scenario, 70% of the time is spent in testing. Planning the design platform and deploying it play a significant role in achieving a working product. During design planning stage, product specifications need to be arrived at. In this work, an organized approach to obtain the design specifications is presented. This is illustrated below.

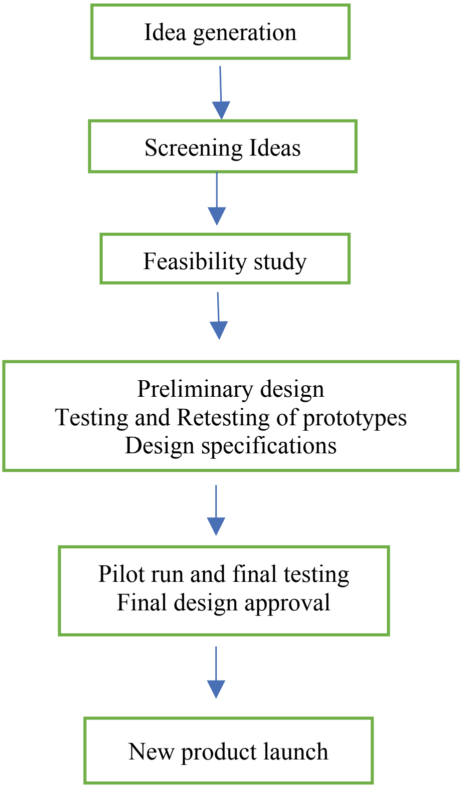


Fig. 1 Product design flowchart

A series of questions assist in arriving at the product specification.

Customer-related questions:
What is the main objective of the product?
What is the user experience that needs to be translated as the product requirement?
What is the risk of the product not being acceptable by the customer?
Are there any device constraints from the user?
What is the voice of the customer?
What is the societal value associated with the product design?
What is the Wish list of the customer?

Hardware-related questions:
What are the hardware models to be developed?
What are the interface design units?
What are the components needed?
From whom should the electronic components be purchased?
To develop a sample design what are the mechanical parts needed?
What is the cost of the spares?
What is the computing unit that has to be used?
Which controller to be used for design deployment?
What is the voltage required for the design implementation?
Should the design have a battery as a power supply unit?
Should the design have 5 V power supply designed or use one which is available in the market?
Should the design have a voltage regulator?
What is the type of the buzzer required for the audio output?
What are the tools like wire cutter, etc., that are needed?
Any specific safety measures to be used during the design and test phase?
Is there any special training needed for the designer to proceed further?

Embedded software questions:
What is the computational model?
Is the software available as open access?
What are the design modules to be developed?
What are the mathematical models to be implemented for proper computation and simulation?
What is the hardware and software requirement together for the design flow?

4 Design Schedule

The design schedule followed for this work is depicted in the form of graphical representation using Gantt chart. This representation helps the designer to work in an organized way. If any task is not done in time, the chart acts as a reminder to complete the task. Table 1 shows the Gantt chart for the work taken up.

Table 1 Gantt chart

Days	10	20	30	40	50	60	70	80
Brain storming	🟩	🟩						
Selection of sensor		🟩						
Component collection		🟩	🟩					
Design Skill learning			🟩	🟨	🟨			
Design development					🟨	🟨		
Interface the Circuit					🟨	🟨	■	
Software development				🟨	🟨	🟨	■	■
Testing					🟨	🟨	■	■

5 Smart Cane Design and Testing

The design commenced with the Wish list of the user.

1. Lightweight;
2. Clear audio output and good proximity response;
3. Less hassles with power/battery.

The product design needs to follow certain distinct approach. There are three key words "Engineering, Design, Process". The key words itself indicate a disciplined approach to be followed when a product needs to be deployed. Dule Savic, Design Engineer [20], Grundfos Company limited, Belgrade, Serbia, has shared his view in FAQ's Quora forum.

Process is a set of tasks to be followed which eventually give the required outcome.

Design is a representation of the appearance and functionality in the form of block diagrams, flowcharts, interfacing features and the software design platform to be implemented.

Engineering indicates that during the design phase the fundamentals of science principles that are to be used in order to achieve the design goals. Science principles may be related to physics, chemistry or mathematics.

From the above Wish list, it is observed that it provides information in a very Layman's way. It is the task of the designer to transform the Wish list into proper design specifications. Analyzing the first Wish list of the designer, a "light weight but yet sturdy cane" is the need of the user.

Coming to the second one, it evidently indicates two design features.

a. Clear audio output

Now mapping this Wish list to a design specification, there can be the following forms of audio output.

- Buzzer;
- Sound card;
- Voice response.

From these, the buzzer is finalized for the design of this work. The reason to choose this is it provides a clear audible response without complicated design interface.

b. Good proximity response

To translate the designers' understanding of this Wish list "Good Proximity Response", it means that what is the design interface that is actually required to achieve this. Here, it is the task of the designer to precisely meet this Wish list and to make sure that the module is exactly as required—no more, no less. The questionnaire will be of immense help to transform the Wish list to technical specification.

From this Wish list, the designer gets insight into two very fundamental technical rules to be investigated. They are the physics of the device to be interfaced and the mathematics involved in computing the response.

"Good Proximity Response" is normally the distance measurement. The word proximity translates to distance in our design approach.

$$\text{Distance} = \text{Speed}^{*}\text{Time}/2$$

The time for the transmission of the signal to the target and receiving it back is taken into consideration.

There are two modes of sending information mainly,

a. Sound wave;
b. Light wave.

If sound wave is chosen, ultrasonic sensor is the choice. If light wave is chosen, IR sensor is the choice. In this work, sound wave transmission is chosen for proximity response. The speed of sound is 340 m/s. This gives the information of the sensor to be used. This is added to the component list. A major review of this gives the design unit needed. One can decide between a microcontroller and a processor. In the present design, Uno ATmega is chosen as the processing unit.

Analyzing the mathematical model needed is extremely important. It assists the designer in developing the software or the algorithm to be developed. In the present design case, there is a clear functionality need to model the design for distance measurement using appropriate software.

Tangential information from this is to freeze the software platform to be used in the design. The mathematical model is used to solve a real-world system of interest. It assists in understanding the system better through the mathematical model.

Building a mathematical model gives an insight into different computing aspects related to the system. Solving a mathematical model and interpreting its solution in the real-world situation are of great importance to simulate and predict the future outcome. Mathematical model simplifies the problem by making certain assumptions and taking them into design consideration. It provides a basis to describe, formulate, simplify and simulate the problem statement. Mathematically describing features can be done in many ways:

- Formulating equations;
- Defining variables;
- Data acquisition;
- Plotting graphs to find the nature of system;
- Probability calculation.

Simulating is a distinct task during product design phase. It is necessary to know what the system output is considered into the decision making.

The mathematical model can be implemented here with the program development in Arduino IDE using Embedded C. The hardware pins of the ultrasonic sensor are invoked by the software commands, and the mathematical formula is implemented in the code.

If the condition given for the buzzer is matched, then the buzzer gives the audio output. Speed of sound is 340 m/s. Then 1/340 = 29.1. This knowledge is needed for the simulation model to work.

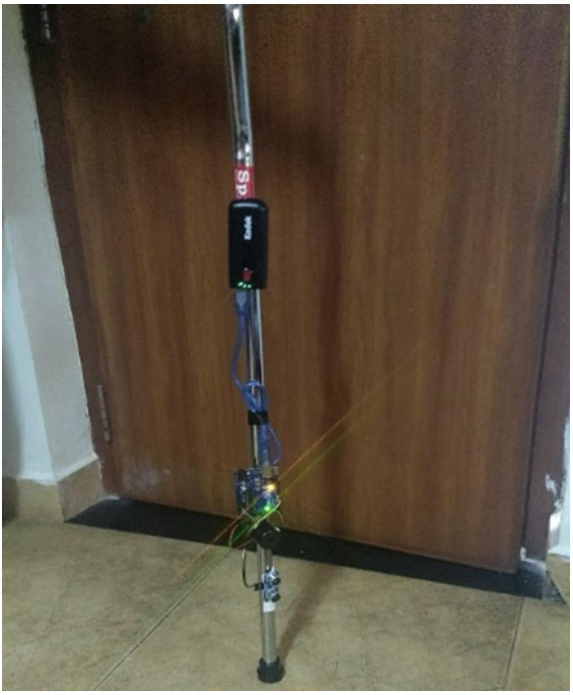
Designing the Smart Cane:

The Arduino Uno microcontroller board is based on microchip ATmega 328P developed by Arduino.cc. This board is very feasible for interfacing as it is based on object-oriented programming in C language for code implementation. There are 14 digital pins and 6 analog pins. The controller is the brain of the system carrying out the functions. The Arduino accepts input voltage 7–20 V, but the operating voltage is 5 V.

This work is an integrated blind stick with ultrasonic sensor, ATmega Uno microcontroller, a power bank for power supply on the stick to function and a buzzer to give an indication of the obstacle. The ultrasonic sensor measures the distance of the obstacle detected as per the range specified in the software code embedded onto the Arduino Uno board. If the given condition of target detection is matched, then the buzzer keeps giving an indication to the blind person. This is a simple mechanism which is easy to handle and also cost-effective. There is a need to make sure that the design provides all the functionalities with right interface and is also cost-effective.

The product is shown in Fig. 2. The basic feature of ultrasonic sensor is to measure the distance of an object using ultrasonic waves. A transducer is used in the sensor to send ultrasonic pulses and receive the echo. Ultrasonic sensor is cost-effective and can be used in both indoor and outdoor environments. This can be referred as a proximity sensor as it is a non-contact sensor. Ultrasonic sensor HC-SR04 is used in this work. The measuring range is 2–400 cm with an accuracy of 3 mm. The voltage and current rating are 5 V and 15 mA, respectively.

Fig. 2 Smart cane



The main objective is to detect the obstacle. The Arduino and the ultrasonic sensor are connected to the pins according to the pins assigned in the software.

The power management unit is a standalone power bank which normally the user may already have. Multipurpose usage of this for the user's mobile and navigation stick saves cost. The cost of the stick can also be saved in the proposed product design, if the user is already having his/her stick. Then, the electronic bay product cost of the gadget will be the minimal cost to be borne by the user.

Another benefit of this product design is the height adjustment ability to detect the obstacles. It can be adjusted to knee height for indoor navigation and above knee height for outdoor navigation. The sound buzzer alert provides a quick reflex to the person who is using this.

6 Conclusion

The smart cane appears as a user-friendly guide for the visually impaired people. The system provides enhanced mobility and also ensures safety. It is a cost-effective and feasible device. This paper throws light on the product design methodology. The difference between product and prototype is discussed which helps the designer to design an efficient product that has all the requirements and provides the expected services. Documentation and questionnaire are important records in designing or developing a product. The designer has to see through this questionnaire and find solutions to these questions during product development.

Preparation of Gantt chart will help the developer to schedule the tasks accordingly and follow up the work in a planned manner in order to complete it in the assigned time frame. Learning the physics concepts involved in the working of the device is required to know the output accuracy.

The knowledge of mathematical modeling is required for formulation and simulation of the software. Thus, this paper leverages an overall view on the product design development, physics and mathematics involved in it.

References

1. Dhanuja R, Farhana F, Savitha G (2018) Smart blind stick using Arduino. Int Res J Eng Technol (IRJET) 5(3):2–6
2. Kumar M, Kabir F, Roy S (2017) Low cost smart stick for blind and partially sighted people. Int J Adv Eng Manag (IJOAEM) 2(3):65–68
3. Tekade A, Sonekar M, Ninave M, Dongre P (2018) Ultrasonic blind stick with GPS tracking system. Int J Sci Eng Res (IJSER) 8(3):3–5
4. Badoni Manoj, Semwal Sunil (2011) Discrete distance and water pit indicator using AVR ATmega8 in electronic travel aid for blind. Int J Disaster Recovery Bus Continuity 2:59–61
5. Gbenga DE, Shani AI, Adekunle AL (2017) Smart walking stick for visually impaired people using ultrasonic sensors and Arduino. Int J Eng Technol (IJET) 9(5):3442–3447
6. Prasanthi G, Tejaswidho P (2016) Sensor assisted stick for the blind people. Trans Eng Sci 3:12–16
7. Kher Chaitrali S, Dabhade Yogita A, Kadam Snehal K, Dhamdhere Swati D, Deshpande Aarti V (2015) An intelligent walking stick for the blind. Int J Eng Res General Sci 3(1)
8. Ambudkar B, Patil P, Bonage K, Gire B (2015) Voice navigation stick for blind. Int J Adv Foundation Res Sci Eng (IJAFRSE) 1(9)
9. Gayathri G, Vishnupriya M, Nandhini R, Banupriya M (2014) Smart walking stick for visually impaired. Int J Eng Comput Sci 3(3):4057–4061
10. Shanmugam M, John V, Gupta M, Saravanakumar K (2017) Smart stick for blind people. Int J Trend Res Develop (IJTRD) 1:30–32
11. Sourab BS, D'souza S (2015) Design and implementation of mobility aid for blind people. Int J Electronic Electr Eng 1:3–5
12. Lin CH, Cheng PH, Shen ST (2014) Real-time dangling objects sensing: a preliminary design of mobile headset ancillary device for visual impaired. Int J Electronic Electr Eng 1:1–3
13. Sukhija Nitish, Taksali Shruti, Jain Mohit, Kumawat Rahul (2014) Smart stick for blind man. Int J Electronic Electr Eng 7(6):631–638
14. Gaikwad D, Baje C, Kapale V, Ladage T (2017) Blind assist system. Int J Adv Res Comput Commun Eng 6(3):442–444
15. Singh R, Succena A, Singh N (2016) PIR based walking stick. Int J Comput Sci Mobile Comput 5(4):486–490
16. Elverum CW, Welo T, Tronvoll S (2016) Prototyping in new product development: Strategy considerations. In: 26th CIRP design conference sciencedirect. Elsevier, pp 117–122
17. Vaziri R, Mohsenzadeh M (2012) A questionaire based data quality methodology. Int J Database Manag Syst (IJDMS). 4(2):28–31
18. Oliva R, Kallenberg R (2003) Managing the transition from products to services. Int J Serv Ind Manag 14(2):1–5

19. Parry G, Newnes L, Huang X (2011) Goods, products and services. Springer J 21–25
20. Savic D (2018) Difference between engineering, design and process. Design Engineer, Grundfoss Company limited, Belegrade, Serbia, Quora forum, pp 1–2

Triclustering of Gene Expression Microarray Data Using Coarse-Grained Parallel Genetic Algorithm

Shubhankar Mohapatra, Moumita Sarkar, Anjali Mohapatra and Bhawani Sankar Biswal

Abstract Microarray data analysis is one of the major area of research in the field computational biology. Numerous techniques like clustering and biclustering are often applied to microarray data to extract meaningful outcomes which play key roles in practical healthcare affairs like disease identification, drug discovery, etc. But these techniques become obsolete when time as an another factor is considered for evaluation in such data. This problem motivates to use triclustering method on gene expression 3D microarray data. In this article, a new methodology based on coarse-grained parallel genetic approach is proposed to locate meaningful triclusters in gene expression data. The outcomes are quite impressive as they are more effective as compared to traditional state-of-the-art genetic approaches previously applied for triclustering of 3D GCT microarray data.

Keywords Triclustering · Parallel genetic algorithms (PGAs) · Coarse-grained PGAs (CgPGAs) · Mean-square residue (MSR) · Gene expression microarray data

1 Introduction

In microarray research, finding groups of genes exhibiting similar expressions, clustering and biclustering techniques are more commonly used in gene expression analysis [9, 14]. However, these techniques become inefficient when the influence of the time as a factor affects the behavior of expression profiles [7]. Now, these types of

S. Mohapatra (✉) · M. Sarkar · A. Mohapatra · B. S. Biswal
DST-FIST Bioinformatics Laboratory, IIIT Bhubaneswar, Bhubaneswar, India
e-mail: B114042@iiit-bh.ac.in

M. Sarkar
e-mail: B114066@iiit-bh.ac.in

A. Mohapatra
e-mail: anjali@iiit-bh.ac.in

B. S. Biswal
e-mail: c114002@iiit-bh.ac.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_50

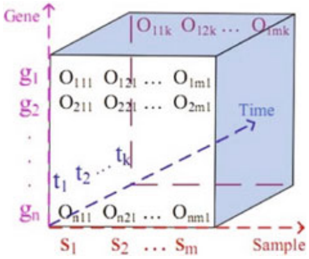

Gene
O_{11k} O_{12k} ... O_{1mk}
g_1
g_2
g_n
O_{111} O_{121} ... O_{1m1}
O_{211} O_{221} ... O_{2m1}
t_1 t_2 ... t_k
O_{n11} O_{n21} ... O_{nm1}
Time
S_1 S_2 ... S_m
Sample

Fig. 1 Illustration of a tricluster

longitudinal experiments are gaining interest in various areas of molecular activities where the evaluation of time is essential. For example, in cell cycles, the evolution of diseases or development at the molecular level is time based as they consider time an important factor of evaluation [1]. Hence, triclustering appears to be a valuable mechanism as it allows evaluation of the expression profiles under a block of conditions along with under a subset of time points.

A coherent tricluster is defined as a set of genes that pursues either coherent values or behaviors. These clusters might have useful information that identify significant phenotypes or potential genes relating to the phenotypes and their regulation relations [17]. The computational complexity of triclustering algorithms is more expensive than the biclustering algorithms (which are already NP hard), so heuristic-based algorithms are an upstanding resemblance for triclustering (Fig. 1).

Genetic algorithms (GAs) are search-specific algorithms and are motivated by the characteristics of genetics and natural selection [10]. GAs usually undergo some important phases like reproduction, mutation, fitness evaluation and selection. Sequential GAs are competent in many applications as well as in different domains. However, there exist some problems in their utilization of problems like triclustering. For example, the fitness evaluation in sequential GAs is usually very time-consuming. Also, sequential GAs may get trapped in a sub-optimal region of the search space thus becoming unable to find better quality solutions. So parallel GAs (PGAs) seem to be a better alternative to the traditional sequential GAs with the adoption of parallelism. The static subpopulations with migration parallel GAs have a key characteristic of applying multiple demes along with the presence of a migration operator. Coarse-grained parallel genetic algorithms (CgPGA) follow the same general terms for a subpopulation model having a fairly small number of demes with many individuals. Very often coarse-grained parallel GAs are treated as distributed GAs as in general, their implementation is carried out on distributed memory MIMD computers. This appeal can also be well configured with heterogeneous networks.

In this paper, an algorithm based on coarse-grained parallel genetic algorithms (CgPGA) approach is proposed. This algorithm finds genus of similar patterns for genes on a three-dimensional space, where genes, conditions and time factor are taken into consideration.

The rest of this paper is organized as follows: A review of the literature is presented in Sect. 2. The proposed methodologies along with the details of the fitness functions and the genetic operators used are described in Sect. 3. The simulation results with their GO term validation are discussed in Sect. 4.4. Finally, Sect. 5 presents the summary and the research findings of the proposed scheme and prospects for the future work.

2 Related Work

Zhao and Zaki introduced tricluster algorithm in 2005 [21]. In this work, the patterns are discovered in three-dimensional (3D) gene expression data along with a set of matrices for the quality measure. A contemporary approach that finds coherent triclusters which contain the regulatory relationships among the genes is stated in [20] and subsequently, extract time-delayed clusters in [18].

LagMiner, in [19] introduced a new technique to detect time-lagged 3D clusters. The evolutionary computation in the form of a multi-objective algorithm has also been employed in the search for triclusters in [13]. Bhar Anirban et al. in 2012 presented δ-TRIMAX algorithm [2]. Again in 2013, the same authors applied the δ-TRIMAX algorithm in estrogen-induced breast cancer cell datasets which provides insights into breast cancer prognosis [3]. David et al. presented a novel tricluster algorithm called as TriGen in 2013 [8]. The novelty of this TriGen algorithm lies upon the use of the genetic approach to mine three-dimensional gene expression microarray data. In 2015, Ayangleima et al. applied coarse-grained parallel genetic algorithm (CgPGA) with migration technique to mine biclusters in gene expression microarray data [12]. In the year 2016, Kakati et al. presented a fast gene expression analysis that uses distributed triclustering and parallel biclustering approach [11]. In her work, the initial bicluster finding is performed by parallel or shared memory approach and then the triclusters are extracted by a distributed or a shared-nothing approach. Premalatha et al. in 2016 presented TrioCuckoo [16] which implemented triclustering using the famous cuckoo search technique.

3 Proposed Methodology

In this section, the reported algorithm has experimented on the standard yeast cell-cycle dataset (Saccharomyces cerevisiae) [15]. Then, the biological validation process is initiated with a tool called GO Term Finder (version 0.83) [4] to get the functional annotations of the genes resulted in the output tricluster.

3.1 Encoding of Individuals

Every individual in the population encodes a tricluster. Triclusters are represented in the form binary strings of G + C + T length, G being the genes (rows), C being the conditions (columns) and T being the times (height) of the 3D expression matrix. If the bit in an individual is 1, it indicates that the respective row, column or height have a place in the tricluster.

3.2 Fitness Function

Here, a fitness function has been implemented to select the best candidates, which is conceptualized up on the three dimensions aspect of the mean square residue measure (MSR) which has been an all-time effective biclustering measure for gene expression analysis [5]. It is named as F_{msr} now onward. As F_{msr} is a minimization function, we expect better results with smaller values.

$$F_{msr}(T_C) = MSR - Weights - Distinction$$

The function is defined for every tricluster (TC). It is minimizing and thus, lower values are favorable.

3.3 Weights

The weights term is defined as:

$$Weights = G_l * w_g + C_l * w_c + T_l * w_t$$

where w_g, w_c and w_t are weights for the number of genes, conditions and times in a tricluster solution, respectively. High values of weights are favorable.

3.4 Distinction

The distinction term is defined as:

$$Distinction = CDN_g/G_l * wd_g + CDN_c/C_l * wd_c + CDN_t/T_l * wd_t.$$

where, CDN_g (Co-ord Distinction no. of g), CDN_c (Co-ord Distinction no. of c) and CDN_t (Co-ord Distinction no. of t) are, respectively, the number of genes, conditions and time coordinates in the tricluster that are absent in the tricluster being evaluated, and wd_t, wd_g and wd_c are the distinction weights of the genes, conditions and times, respectively. Distinction is a measure for the uniqueness of the tricluster being currently evaluated. With increased value of distinction, non-overlapping solutions compared with results previously found can be found. Where,

- G: Tricluster gene coordinates subset.
- C Tricluster condition coordinates subset.
- T: Tricluster time coordinates subset.
- T_l: No. of time co-ord of the tricluster
- C_l: No. of condition co-ord of the tricluster.
- G_l: No. of gene co-ord of the tricluster.
- $TC_v(t, g, c)$: Expression value of gene g under condition c at time t from the expression matrix.

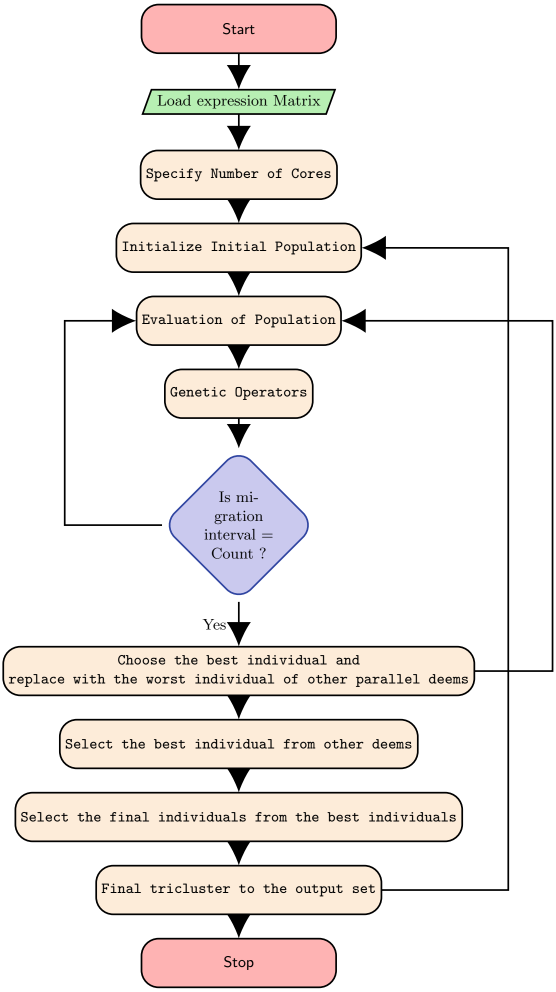
3.5 Tri-CgPGA

Tri-CgPGA is based on coarse-grained genetic algorithms which come under parallel genetic algorithm family. So like coarse-grained algorithms, this evolutionary algorithm takes several steps to execute which are illustrated in the flowchart and pseudo-code below (Fig. 2).

Algorithm 1: Tri-CgPGA Pseudo Code

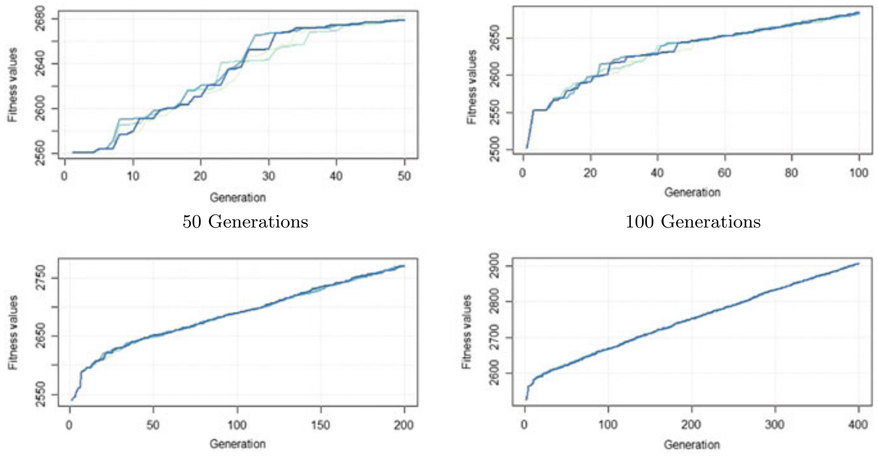
```
Input: Expression Matrix
Output: Coherent Triclusters
Load the expression matrix
Specify the number of cores to be used in parallel
for tricluster number I =1 to maximum_triclusters do
    Initialise the initial population
    Evaluate the population
    for generation number J=1 to maximum_generations do
        selection of parents
        crossover each parent to generate offsprings
        mutation of generated offsprings
        evaluate the new individuals
        select the individuals with better fitness
        if migration_interval =count then
            choose the best individual of the best deem and replace with the
            worst individual of the other parallel deems
    select best individuals from all deems
    select the final individual from best_indiduals
    add final tricluster to output_set
return output_set
```

Fig. 2 Tri-CgPGA algorithm workflow


Start
Load expression Matrix
Specify Number of Cores
Initialize Initial Population
Evaluation of Population
Genetic Operators
Is migration interval = Count ?
Yes
Choose the best individual and replace with the worst individual of other parallel deems
Select the best individual from other deems
Select the final individuals from the best individuals
Final tricluster to the output set
Stop

4 Experimental Results and Discussions

All the computational simulations are performed in general conditions on a multiprocessor machine with four processors Intel Core i7 3.60 GHz with 4 GB RAM and Windows 8.1 64 bit operating system memory. The yeast cell-cycle dataset (Saccharomyces cerevisiae) [15] is used for establishing the efficacy of the proposed algorithm. This dataset contains 6179 genes, 4 conditions and 14 time points. The experiment is performed on the above-mentioned dataset along with its two synthetic versions but only reported for the former.



50 Generations

100 Generations

200 Generations

400 Generations

Fig. 3 Fitness value plots

4.1 List of the Parameters

During execution, some parameters have been set up like the crossover probability P_c, mutation probability P_m, weights: w_g for genes, w_c for conditions and w_t for times, distinction weights: w_{dg}, w_{dc} and w_{dt} for genes, conditions and times, respectively. The details of them are available in Table 1. As the algorithms are designed for gene filtration (to obtain the solution with a minimum number of genes), the value of w_g is set to 0.8 so that maximum number of genes can participate in the solution. While setting up the parameters for the distinction term, a higher value is being provided for the genes to cover up as much space as possible in this dimension.

4.2 Results on Yeast Dataset

The simulation results are analyzed from the perspective of the different generations. Analyzing across different generations, it indicates as the number of generations is increased, the values also increase. So for bigger generations, better homogeneity among the genes is obtained which is presented in the following graphs (Fig. 3)

Table 1 Values of the parameters taken during algorithm execution

P_c	P_m	w_g	w_c	w_t	w_{dg}	w_{dc}	w_{dt}
0.8	0.5	0.8	0.1	0.1	1.0	0.0	0.0

Table 2 Detailed information about triclusters found by Tri-CgPGA algorithm

Gene size	Avg. MSR	Avg. volume	Avg. No. of genes	Avg. No. of conditions	Avg. No. of time
1000	493.35	5124.65	616	1.35	6.5
3000	1322.88	33,889.5	1651.37	3	7
6178	2669.086	67,798.75	3334	2.65	7.65

4.3 Comparitive Study

The results obtained from the execution of the algorithm are quite impressive in terms of time and the volume of the output triclusters. As the fitness function is minimizing, lower the value of MSR the better is the fitness of the tricluster. Further, the results of the Tri-CgPGA algorithm is compared with the results obtained by the trigen algorithm [8]. The comparison has been done on the basis of computational time taken by the proposed algorithm to execute the codes and to derive the output. In the case of Tri-CgPGA algorithm, it took 30 s approximately to run for 1000 genes for 50 generations to deliver the output, whereas the trigen algorithm [8] requires 118 s to do the same. Hence, exploring parallelism with the genetic approach on triclustering of gene expression microarray data is preferable against the traditional GAs as it reduces the computation time for the algorithm execution. Other relevant information regarding the results obtained from the algorithms Tri-CgPGA algorithm is presented in Table 2.

4.4 GO Term Analysis

The validation of the results obtained is carried out with the Gene Ontology project (GO) [6]. This analysis renders the ontology of terms which describes gene product annotation data along with its characteristics. The ontology describes attributes like molecular functions, cellular component and the relevant biological processes. The queries associated with the associated genes are addressed in GO using the GO Term Finder (version 0.83) [4]. The findings of the GO Term analysis are presented in Table 3.

Table 3 GO for yeast cell-cycle results

Cluster ID	Biological process	Molecular function	PI (P-value = < 0.01)
0044699	Single-organism process	Only one organism is being involved	3.02E−10
0016043	Cellular component organization	Assembling or de-assembling of a cellular component constituent parts	4.87E−08
0065007	Biological regulation	Biological process regulation of quality or function	0.00725
0080090	Single-organism cellular process	Cellular-level activity, occurring within a single organism	1.61E−06
0060255	Single-organism process	Only one organism is being involved	1.91E−06
0019222	Single-organism process	Only one organism is being involved	0.00019
0044763	Single-organism cellular process	Cellular-level activity, occurring within a single organism	2.69E−06
0050789	Single-organism process	Only one organism is being involved	4.10E−05
2000112	Single-organism cellular process	Cellular-level activity, occurring within a single organism	4.89E−06
0010556	Single-organism cellular process	Cellular-level activity, occurring within a single organism	0.00315
0071840	Cellular component organization	Biosynthesis of constituent macromolecules, assembly, arrangement of constituent parts, or disassembly of a cellular component	0.00753
0051171	Cellular component organization or biogenesis	Biosynthesis of constituent macromolecules, assembly, arrangement of constituent parts, or disassembly of a cellular component	0.00026
0006996	Organelle organization	Cellular-level assembly, arrangement of constituent parts, or disassembly of an organelle within a cell	6.00541
0010468	Organelle organization	Cellular-level assembly, arrangement of constituent parts, or disassembly of an organelle within a cell	0.00563
0032774	Biological regulation	Biological process regulation of quality or function	0.00939

5 Conclusion

A new framework Tri-CgPGA, based on the coarse-grained parallel genetic approach (CgPGA) to generate the triclusters from gene expression database is proposed in our work. The results of the suggested framework are compared with another state-of-the-art technique called as Trigen algorithm. As the comparison justifies the proposed scheme's efficiency over the existing schemes considering the computation time, hence it is preferable to adopt parallel GAs over traditional GAs in the triclustering of gene expression 3D microarray data. There exist number of future directions which might further improve this framework: (1) The acquisition of large-scale databases from other standard datasets to measure the performance of the frameworks (2) To further improve the coherence and the computation time, other competent evaluation measures with the suggested or other existing versions of PGAs should be investigated to obtain more meaningful triclusters.

References

1. Bar-Joseph Z (2004) Analyzing time series gene expression data. Bioinformatics 20(16):2493–2503
2. Bhar A, Haubrock M, Mukhopadhyay A, Maulik U, Bandyopadhyay S, Wingender E (2012) δ-TRIMAX: extracting triclusters and analysing coregulation in time series gene expression data. In: International workshop on algorithms in bioinformatics. Springer, pp 165–177 (2012)
3. Bhar A, Haubrock M, Mukhopadhyay A, Maulik U, Bandyopadhyay S, Wingender E (2013) Coexpression and coregulation analysis of time-series gene expression data in estrogen-induced breast cancer cell. Algorithms Mol Biol 8(1):9
4. Boyle EI, Weng S, Gollub J, Jin H, Botstein D, Cherry JM, Sherlock G (2004) Go: termfinder-open source software for accessing gene ontology information and finding significantly enriched gene ontology terms associated with a list of genes. Bioinformatics 20(18):3710–3715
5. Cheng Y, Church GM (2000) Biclustering of expression data. ISMB 8:93–103
6. Consortium GO (2004) The gene ontology (GO) database and informatics resource. Nucl Acids Res 32(Suppl 1):D258–D261
7. Gómez-Vela F, Martínez-Álvarez F, Barranco CD, Díaz-Díaz N, Rodríguez-Baena DS, Aguilar-Ruiz JS (2011) Pattern recognition in biological time series. In: Conference of the Spanish association for artificial intelligence. Springer, pp 164–172
8. Gutiérrez-Avilés D, Rubio-Escudero C, Martínez-Álvarez F, Riquelme JC (2014) Trigen: a genetic algorithm to mine triclusters in temporal gene expression data. Neurocomputing 132:42–53
9. Hartigan JA (1972) Direct clustering of a data matrix. J Am Stat Assoc 67(337):123–129
10. Holland J, Goldberg D (1989) Genetic algorithms in search, optimization and machine learning. Addison-Wesley, MA
11. Kakati T, Ahmed HA, Bhattacharyya DK, Kalita JK (2016) A fast gene expression analysis using parallel biclustering and distributed triclustering approach. In: Proceedings of the second international conference on information and communication technology for competitive strategies. ACM, p 122
12. Laishram A, Vipsita S (2015) Bi-clustering of gene expression microarray using coarse grained parallel genetic algorithm (CGPGA) with migration. In: 2015 Annual IEEE India conference (INDICON). IEEE, pp 1–6
13. Liu J, Li Z, Hu X, Chen Y (2008) Multi-objective evolutionary algorithm for mining 3D clusters in gene-sample-time microarray data. In: IEEE international conference on granular computing, 2008. GRC 2008. IEEE, pp 442–447
14. Rubio-Escudero C, Zwir I, et al (2008) Classification of gene expression profiles: comparison of k-means and expectation maximization algorithms. In: Eighth international conference on hybrid intelligent systems. IEEE, pp 831–836
15. Spellman PT, Sherlock G, Zhang MQ, Iyer VR, Anders K, Eisen MB, Brown PO, Botstein D, Futcher B (1998) Comprehensive identification of cell cycle-regulated genes of the yeast saccharomyces cerevisiae by microarray hybridization. Mol Biol Cell 9(12):3273–3297

16. Swathypriyadharsini P, Premalatha K (2018) Triocuckoo: a multi objective cuckoo search algorithm for triclustering microarray gene expression data. J Inf Sci Eng 34(6):1617–1631
17. Tchagang AB, Phan S, Famili F, Shearer H, Fobert P, Huang Y, Zou J, Huang D, Cutler A, Liu Z et al (2012) Mining biological information from 3d short time-series gene expression data: the optricluster algorithm. BMC Bioinform 13(1):54
18. Wang G, Yin L, Zhao Y, Mao K (2010) Efficiently mining time-delayed gene expression patterns. IEEE Trans Syst Man Cybern Part B Cybern 40(2):400–411
19. Xu X, Lu Y, Tan KL, Tung AK (2009) Finding time-lagged 3d clusters. In: IEEE 25th international conference on data engineering, 2009. ICDE'09. IEEE, pp 445–456
20. Yin Y, Zhao Y, Zhang B, Wang G (2007) Mining time-shifting co-regulation patterns from gene expression data. In: Advances in data and web management. Springer, pp 62–73
21. Zhao L, Zaki MJ (2005) Tricluster: an effective algorithm for mining coherent clusters in 3d microarray data. In: Proceedings of the 2005 ACM SIGMOD international conference on Management of data. ACM, pp 694–705

Ensemble Feature Selection to Improve Classification Accuracy in Human Activity Recognition

Nivetha Gopalakrishnan, Venkatalakshmi Krishnan and Vinodhini Gopalakrishnan

Abstract Real-time data with redundant and irrelevant features can degrade the performance of the classifier. Dataset with more number of features also increases the noise of the data and increases the time complexity of the learning algorithm. Feature selection is a solution for such problems where there is a need to reduce the dimensions of the data. In existing feature selection methods, the resultant feature sets can lead to local optima in the space of feature subsets. In this paper, ensemble-based feature selection approach is proposed to reduce size of the dataset and to improve classification accuracy. Results show that the proposed ensemble approach enhances the classifier performance, with reduced number of features.

Keywords Sensor · Feature · Classification · Learning

1 Introduction

Extracting useful knowledge from the raw sensed data, in general, has provided useful information in various domains. Machine learning and data mining techniques are effective than the classical mathematics and statistical techniques in extracting knowledge from data. Data classification is the process of categorizing data into labels or classes. The performance of the classifier model is described by the percentage of

N. Gopalakrishnan (✉)
Department of Electronics and Communication Engineering, University College of Engineering Panruti, Panruti, Tamilnadu, India
e-mail: gtv.evin@gmail.com

V. Krishnan
Department of Electronics and Communication Engineering, University College of Engineering Tindivanam, Tindivanam, Tamilnadu, India
e-mail: venkata_krish@yahoo.com

V. Gopalakrishnan
Department of Computer Science Engineering, Annamalai University, Chidambaram, Tamilnadu, India
e-mail: vinodhini.g.t@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_51

accuracy of correctly predicting the labels or classes. The significant specification of the classifier model depends on the number of training data and the adequacy of the features used in the analysis. Feature selection (FS) is defined as the process of the selection of the features in the analysis in order to maximize the performance of the resulting model. Feature selection is usually performed as a data pre-processing stage before the classification process. Feature selection retains only useful features or attributes via removing irrelevant features [1, 2]. This means that the full information content can be obtained from minimum number of features in the dataset with maximum distinction information about the classes. Hence, by eliminating the irrelevant features, the amount of data can be reduced which will improve the classifier performance [3].

The rest of the paper is organized as follows: Sect. 2 outlines the literature survey and motivation; Sect. 3 explains the proposed methodology and experimental setup; Sect. 4 gives the experimental results obtained, and Sect. 5 concludes the paper with possible future scope.

2 Literature Survey

In recent years, ensemble learning is applied to many data mining tasks such as outlier detection [4], classification [5], and few ensemble-based feature selection methods [6]. A hybrid evolutionary ensemble feature selection method with two variants of genetic algorithms (GA) has been proposed [7]. In the first stage, the features or attributes are selected using GA's. The features selected by a feature selection method are combined together in the second stage through averaging method. Another feature selection method is proposed for breast cancer classification with ensemble size of five feature selection methods such as CHI2 discretization, information gain, 1 rule, relief, and RMean methods, and feature subsets are aggregated using mean function. Another method is proposed with ten feature selection methods such as ReliefF, ReliefF-W, SVM-ONE, and SVM-RFE with three subset aggregators mean, median, and exponential for biomarker discovery from high-dimensional genomic data. Authors Guru et al. in [8] proposed ensemble of three FSM such as chi-square, IG and likelihood ratio and three aggregation methods such as intersection, union, and average-based aggregations for text classification. Another method was proposed using ensemble of five feature selection methods like symmetric uncertainty, gain ratio, information gain, relief and chi-square and rank-based combiner is used to aggregate the feature subset.

3 Proposed Work

In this proposed work, we opt to use ensemble with variants in ensemble size. The proposed ensemble uses different FSM with the same training data as shown in

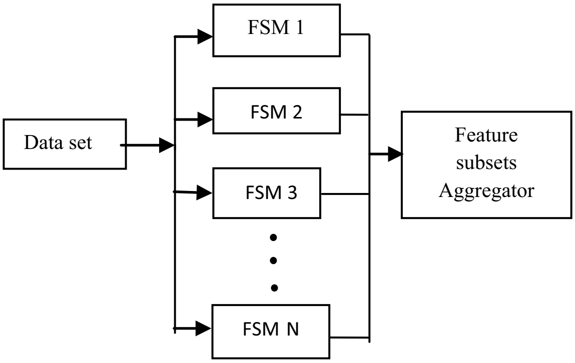


Fig. 1 Ensemble feature selection

Fig. 1. In spite of the extensive number of FSMs available for feature selection, there is no existing work investigating the advantages of the EFSM after outlier detection and removal. With this drawback, in this proposed work, an analytical study of alternative ways of ensemble feature selection methods resulted by multiple FSMs. The proposed ensemble feature selection framework consists of two steps as shown in Fig. 1. The first step is ensemble formation, and the second is the aggregation of ensemble outputs. Moreover, as the main goals of ensemble feature selection is to improve classification accuracy of feature selection. Feature aggregators like intersection lead to very limited number of features sets, even leads to the null set of features, and in practice, it does not tend to produce best results. On the contrary, the union operator consists of combining those features subsets selected by weak feature selectors. In this case, the final set of features subsets contains all the features that had been considered important by any selector, leads to selection of all features in the dataset. This approach tends to produce better results than the intersection, but at the expense of a lower reduction in the number of the features. Statistical aggregators like mean, median can also be used as an aggregation function. In this proposed approach in Fig. 2, outlier-removed HAR dataset is applied to '*M*' feature selection methods (FSM), features selected from '*M*' FSM are FS1, FS2, FS3, … FSM and these subsets are combined using feature aggregator method. In this proposed approach, feature subsets are aggregated using frequency of occurrence (FOO) of features or attributes. Then the aggregated subset is ranked in descending order, top k attributes are labeled as most significant relevant features (MSRF), and last 'K' attributes are labeled as least significant labeled features (LSRF), and LSRF attributes are removed from the dataset. Other than top K features, other features are to be analyzed. As depicted in Fig. 3, divide all intermediate features into blocks of size S, as '$B1$, $B2$, and $B3$ … BS.' Add the attributes of first block $B1$ to MSF and perform classification and find the classification accuracy. Next, add the attributes of block $B2$ with top k attributes and $B1$ attributes and find classification accuracy and repeat this procedure for other blocks. Finally, add attributes of last block BS with top $k + B1 + B2 + B3 + \cdots \mathrm{BS} - 1$ and perform classification. Now, sort all classification accuracies with feature block

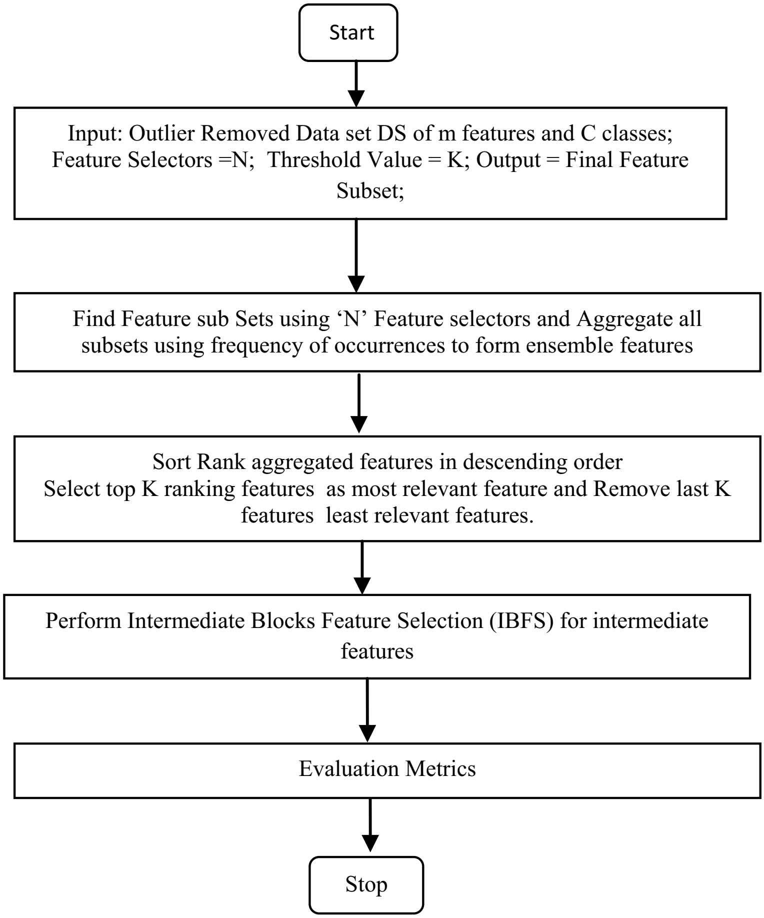

Start
Input: Outlier Removed Data set DS of m features and C classes; Feature Selectors =N; Threshold Value = K; Output = Final Feature Subset;
Find Feature sub Sets using 'N' Feature selectors and Aggregate all subsets using frequency of occurrences to form ensemble features
Sort Rank aggregated features in descending order Select top K ranking features as most relevant feature and Remove last K features least relevant features.
Perform Intermediate Blocks Feature Selection (IBFS) for intermediate features
Evaluation Metrics
Stop

Fig. 2 Workflow of the proposed ensemble feature selection (ENFS) method

Top K features	**Intermediate Features (B1, B2, B3, ….BS)**	**Last K Features**
Select Most Significant features (MSF)	**= Total number of features - Top K features - Last K Features**	**Remove Least Significant Features (LSF)**

Fig. 3 Intermediate blocks feature selection (IBFS)

Table 1 Ensemble combinations

S. no.	Ensemble size (N)	Feature selection methods
1	2	IGR, MRMR
2	3	IGR, MRMR, PCA

sets and find the maximum classification accuracy. The set of blocks with maximum classification accuracy is the final ensemble attributes.

4 Experimental Setup

To evaluate this proposed ENFS method, an experimental evaluation is carried using human activity recognition datasets from offline and online environments. The datasets used for this experimental evaluation are dataset-1 (DS1) collected from offline environment, and the second dataset is the online dataset-2 (DS2). These datasets are preprocessed for outlier detection and then passed to ensemble feature selection (ENFS) for further processing.

1. MRMR: Peng et al. [9] proposed the mutual information-based method called, minimum redundancy maximum relevance (MRMR). It selects features according to the maximal statistical dependency criterion.
2. Information gain: The importance of an attribute relating to the class is evaluated using the information gain measure [10].
3. PCA: This method calculates weight using principle components analysis [11].

We used the implementation of the feature selection algorithms provided by the rapid miner software. The performance of the ensemble approach is evaluated using support vector machine (SVM) classifier. In this study, the SVM classifier used a Gaussian radial-basis-function (RBF) with values $C = 1$ and gamma $= 0.01$ (default values for both parameters in rapid miner). In order to prove the efficiency of ensemble feature selection methods, features selection with various ensemble sizes is taken. First, we choose ensemble size (N) as two and combinations of two standard FS methods IGR and MRMR are used. Feature selection is done individually using IGR and MRMR, and the results obtained are aggregated using the proposed aggregation algorithm. Finally, activity classification is done with ensemble feature subsets using SVM classifier. The same procedure is repeated for ensemble size three using feature selection algorithms as shown in Table 1.

5 Results and Discussion

In this section, we evaluated the performance of this proposed ensemble feature selection (ENFS) with existing three individual feature selection methods such as IGR,

Table 2 Number of features selected

S. no.	Feature selection-methods	Number of features selected	
		DS1 (46)	DS2 (46)
1.	IGR	36	36
2.	MRMR	36	36
3.	PCA	36	35
4.	ENFS2	29	29
5.	ENFS3	29	28

MRMR, and PCA, method in terms of number of features selected and classification accuracy.

5.1 Number of Features Selected

The total number of features selected using ensemble feature selection is shown in Table 2. The total number of features selected by standard existing methods for DS1 are IGR = 36, MRMR = 36, and PCA = 36. Total number of features selected by standard existing methods for DS2 are IGR = 36, MRMR = 36, and PCA = 35. For ENFS = 2, the number of feature subsets obtained from two standard methods IGR = 36 and MRMR = 36 are aggregated using frequency of occurrence, and the final feature subset is selected using aggregation algorithm. The number of features selected by ENFS2 is 29 for DS1 and 29 for DS2, whereas the number of features selected by ensemble methods for DS1 and DS2 are ENFS3 = 29 and ENFS3 = 29. From the results shown in Table 2, the number of features selected by ensemble methods is less when compared to other ten standard feature selection methods.

5.2 Classification Accuracy

In order to prove the efficiency of this proposed ensemble feature selection methods, classification accuracy is typically treated as the main goal. Feature subsets selected using ensemble feature selection are classified using SVM classifier. The classification accuracies to classify six human activities for the datasets DS1 and DS2 with outlier removal (WOR) are calculated. For DS1, the classification accuracy for the three standard feature selection methods, and the five proposed ensemble feature selection methods are shown in Table 3. The proposed ensemble methods ENFS2 and ENFS3 have achieved higher classification accuracies than standard feature selection methods for DS1 and DS2. It is clear that the ensemble methods with reduced number of features or attributes can achieve high-classification accuracies than existing feature selection methods.

Table 3 Classification accuracy of DS1, DS2, and DS3

S. no.	Feature selection-methods	Accuracy	
		DS1	DS2
1	IGR	92.8	92.6
2	MRMR	92.3	91.89
3	PCA	92.04	91.99
4	ENFS2	95.87	95.24
5	ENFS3	96.54	96.32

Thus from the experimental results obtained, the proposed (ENFS) ensemble feature selection methods improve classification accuracy of human activity recognition (HAR).

6 Conclusion

In this paper, to increase the classification accuracy the irrelevant features of the activity datasets are removed using ensemble feature selection method ENFS. Two variants of the proposed ensemble methods such as ENFS2 and ENFS3 are proposed. The ensemble combinations of IGR, MRMR, and PCA are used for analysis. The proposed methods yield an optimal feature subsets. From the results obtained, the number of features selected is less for the proposed ensemble methods. It can be seen that the proposed ENFS methods achieves high-classification accuracy due to elimination of irrelevant features. Therefore, the overall performance of the proposed ENFS has been found to be excellent for the two datasets.

References

1. Chandrashekar G, Sahin F (2014) A survey on feature selection methods. Comput Electr Eng 40:16–28
2. Yaqub M, Javaid MK, Cooper C, Noble JA (2011) Improving the classification accuracy of the classic RF method by intelligent feature selection and weighted voting of trees with application to medical image segmentation. In: Suzuki K, Wang F, Shen D, Yan P (eds) Machine learning in medical imaging. lecture notes in computer science. Springer, Berlin, Heidelberg, 7009
3. Quiroz JC, Banerjee A, Dascalu SM, Lau SL (2017) Feature selection for activity recognition from smartphone accelerometer data feature selection for activity recognition from smartphone accelerometer data. Intell Automation Soft Comput 1–9
4. Zimek A, Campello RJGB, Sander J (2014) Ensembles for unsupervised outlier detection. ACM SIGKDD Explorations Newsletter 15:11–22. http://doi.org/10.1145/2594473.2594476
5. Rokach L (2010) Ensemble based classifiers. Artif Intell Rev 33:1–39. https://doi.org/10.1007/s10462-009-9124-7
6. Pérez RR, Silva AF (2015) Ensemble features selection method as tool for breast cancer classification Isabel Ramos. Int J Image Mining 1:224–244

7. Goh J, Thing VLL (2015) A hybrid evolutionary algorithm for feature and ensemble selection in image tampering detection. Int J Electron Secur Digit Forensics 7:76–104
8. Guru DS, Suhil M, Pavithra SK, Priya GR (2018) Ensemble of feature selection methods for text classification: an analytical study. In: Abraham A, Muhuri P, Muda A, Gandhi N (eds) Intelligent systems design and applications 2017. Advances in Intelligent Systems and Computing. Springer, 736, 337–349
9. Peng H, Long F, Ding C (2005) Feature selection based on mutual information criteria of max-dependency, max-relevance, and min-redundancy. Pattern Anal Mach Intell 27:1226–1238. https://doi.org/10.1109/tpami.2005.159
10. Lee C, Lee GG (2006) Information gain and divergence-based feature selection for machine learning-based text categorization. Info Process Manag 42(1):155–165
11. Song F, Guo X, Mei D (2010) Feature selection using principal component analysis. In: International conference on system science, engineering design and manufacturing informatization, IEEE society, 27–30

An Exploration on Cloud Computing Security Strategies and Issues

Amrita Raj and Rakesh Kumar

Abstract Cloud computing is revolutionizing many ecosystems by providing organization with computing resources that feature easy connectivity, deployment, automation, and scalability. In the recent past, the attractive features of cloud computing fuel the consolidation of cloud environment in the industry, which has been consequently motivating research on the related technologies by both the academia and industry. Regardless of its advantages, computing paradigm raises security concerns in transition phase, which have subjected several studies. Cloud computing tends to offer scalable on-demand services to the consumer with greater flexibility and lesser infrastructure investment. Since cloud services are delivered using classical network protocols and formats over the Internet, implicit vulnerabilities existing in these protocols as well as threats introduced by newer architectures have raised many security and privacy concerns. In this paper, we have focused on the data security issues found in the cloud computing. In addition to this, we discovered an appropriate solution and a private cloud domain.

Keywords Cloud computing on-demand services · Virtualization · Security · Data security · Threads · Attacks

1 Introduction

In the distributed computing framework implementation, the client has the features of high adaptability and quality [1]. The assets on the demand and the client do not know any information about the place of assets. Client can equip their application and information from an unspecified area. The distributed computing is considered as the valuable difference in data industry as well as a more effective improvement of

A. Raj (✉) · R. Kumar
Department of Computer Science and Engineering (CSE), M.M.M. University of Technology, Gorakhpur, U.P. 273010, India
e-mail: amritaraj4501@gmail.com

R. Kumar
e-mail: rkiitr@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_52

data technology for the general society. Most of the cloud computing framework now consists of reliable services which have been sent through information center built on the servers with various levels of virtualization technologies. The cloud computing is the outcome of various factors like conventional computing, communication technology, and business approach [2]. The cloud computing can ensure the information security and client will not secure the information without anyone else's input [3]. So the distributed computing will be the process for storing information in the cloud framework. Numerous organizations support the distributed computing stages, for example, IBM, Amazon, Microsoft, Google, VMware, and EMC which involves its common element that has been done by the cloud computing [4]. In spite of the fact that distributed computing and their advantages are huge, security and protection concerns are the essential obstructions toward their wide appropriation [5].

1.1 Measured Service

Although computing assets are combined and shared by more than one consumer (i.e., multi-tenancy), cloud framework is to utilizing a suitable system for measuring the usage of these assets for required person. The National Institute of Science and Technology (NIST) had defined cloud computing as "Cloud computing is a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." The services given by the cloud are very striking because of there intrinsic feature present in on-demand service. Due to this feature, the client is required to pay to remunerate for service that they have used [6].

1.2 On-Demand Self-service

Consumer can individually calculate computing skills, such as server time and network storage automatically, if needed, without the need for human communication with all the service providers [7].

1.3 Broad Network Access

Capabilities are accessible over the network and access through the standard component that promotes use by heterogeneous stages (e.g., cell phones, laptops, and PDAs).

1.4 Resource Pooling

In the attempt of using multiplex consumers or virtualization, the cloud service provider is pooled with computing resources; models are dynamically assigned with defibrillators, resources and redistributed the need of user demand. In this way, the motivation to establish a pool-based computing design is contained in the two-impact factor.

1.5 Economics of Scale an Expertise

The outcome of a pool-based model is that the physical computing resources become "invisible" to the customers, who do not normally have the information of controller on the place, formation, and ownership of these resources.

Example: Databases, Central Processing Unit etc. It is easy to access the information as it is stored in the cloud.

1.6 Rapid Elasticity

Computing resources for customers develop fast rather than constant: There is no upfront and agreement because they can increase them as much as they want and leave them after scaling them. Apart from this, the resources provision seems to be infinitely mated for them, and consumption can increase rapidly to complete the time-peak imports [9] (Table 1).

Table 1 Comparison of data processing centers

Parameter	Data processing center		
	Traditional	Virtual	Cloud based
On-demand service	No	No	Yes
Wide network access	Yes	Yes	Yes
Elasticity	No	Yes	Yes
Measured pooling	No	Yes	Yes
Resource pooling	Yes	Yes	Yes

2 Cloud Model Provides Three Types of Services

2.1 Software as a Service

The SaaS provides the customer a platform or application to manage a cloud infrastructure continuously. In general, SaaS allows to use software applications as a service to end users. Example: Google Applications.

2.2 Platform as a Service

It is the ability that has been given to a customer to deploy onto the cloud infrastructure his own applications without the need of installing any platform or tools on the local machine. PaaS states towards providing platform layer resources, in addition to it providing the operating system support and software development frameworks that can be deployed to craft higher-level services [10].

2.3 Infrastructure as a Service

It provides the customer with the ability to plan prepare, storage, network, or different basic computing assets, or all pass the customer to deploy and fast arbitrary, which can include software and applications. Furthermore, it enables the customer to send and run subjective programming, which can incorporate working framework and applications. Consumers have limited authorized over operating systems and applications, storage deployment applications, and potentially selected networking components [8]. Be that as it may, client can deal with his information put away on cloud and applications which he has sent. Gmail and Dropbox are a few uses of distributed computing administrations [11].

3 Attacks on Cloud Computing

3.1 Zombie Attacker

On the Internet, the aggressor challenges to increase the victim by transfer demands from the honest host on the system in this way and these hosts are known as zombie. In the cloud, the demand for virtual machines (VMs) is approachable by every client by the Internet. An aggressor zombie may flow largest multiple calls. Such attacker cloud software helps to improve the performance of the cloud.

In order to serve the large number of requests the cloud becomes overloaded and finally becomed exhausted causing the DoS (Denial of Service) or DDoS (Distributed Denial of Service) to the servers. The results of above becomes adverse as the cloud is not able to serve valid user's request due to the flooded attacker's requests. Thus better authentication and authorization & IDS/IPS can give better protection against such attacks. In case of flooding or zombie attack, the cloud provider provides more computing power to serve the huge number of requests (which includes zombie requests too). Attacker Service can become a lead offs insufficiency of the attack you are not able to do so, you cannot use any information about any service that is used in the search result [12]. With the gadgets, these methods enable an aggressor to screen the simple qualities of intensity supply and interface associations; along these lines, they can be utilized to get to the chip surface straightforwardly, so we can watch, control, and meddle with the gadget. Owing to these truths, employers are extra relying on cloud-based information processing to achieve a large information amount. The employers are ignorant of the strength data processing methods of the cloud-based features and want that the existing network is protected and reliable adequate to inhibit any unapproved approach to the information [8]. This type of attack is DDOS attack. Thus the existing network must be protected & reliable enough to prevent any unapproved accessing of the information [8] (Table 2).

3.2 *Man-In-The-Middle Cryptographic Attack*

This attack is complete when places himself between two clients. Whenever attackers put themself in the information way, there is the feasibility that they can interrupt changes information [13].

3.3 *Side-Channel Attack*

These methods enable an aggressor to screen the qualities of intensity supply and interface associations; along these lines, they can be utilized to get to the chip surface straightforwardly, so we can watch, control, and meddle.

3.4 *Service Level Agreement*

In numerous regards, cloud computing speaks to redistributing of calculation and capacity to outside specialists co-op. Such redistribution has been administered service level agreement (SLA) that indicates least dimensions of execution that the client can anticipate. Although, classically there exists 99.99% system availability per year yet SLA have not covered security aspects such as confidentiality and integrity.

Table 2 Analysis on security problem and solutions directive

Synopsis of threads into cloud and solution instruction

Threads	Issues	Causes cloud services	Resolution instruction
Modification into economical class	Decline of modify over cloud database infrastructure framework	IaaS, PaaS, or SaaS	Access control or checking framework on offered administrations
Insulting utilization of Cloud computing	The intruder gives the signup or when due to the strong attackers the absence of approval, benefit minimum	PaaS and SaaS	Strong enrollment and verification of comprehensive monitoring of system traffic
Unsafe interfaces and APIS	Poses threads like clear-content validation, transformation to content: advance verification	SaaS, PaaS or IaaS	Establish secure verification as well as provide modify component among coded communication
Malicious insiders	Insider malicious movement debate from firewall and pass around protection model	PaaS, IaaS, or SaaS	Access clarity as security and management system, usage deference broadcasting as well as breath information
Shared technology problem	Allow one client to interface other client's services by compromise hypervisor	IaaS	For solid certification access control component and for managerial task. Inspection and vulnerability as well as structure
Information damage and leakage	Confidentiality information can be removed and modified	IaaS, PaaS, or SaaS	Uses protected APIs encrypting, keys, apply information detention, or substitute policy
Service hijacking	Customer file and service instances cases could thus make another new base for attacker	PaaS, IaaS, and SaaS	Uses security strategies, solid validation mechanism, or movement monitoring

(continued)

Table 2 (continued)

Synopsis of threads into cloud and solution instruction			
Risk profiling	Interior protection strategies, security compliance, structure, solidifying fixing inspecting or log might be ignored	SaaS, IaaS, or PaaS	Uncover incomplete logs, information and infrastructure detail. Use observing and alerting framework for information breaks

In a cloud computing seller market, it is sensible to expect that not all suppliers will be capable, or willing, to give some level of security to their customers.

Besides, a given cloud supplier may offer administrations with differing dimension of security relying upon how much the client will pay for the administration [14].

In spite of the fact that cloud consumer does not command over the fundamental computing assets, they do need to guarantee the assets when purchasers I have related their center business capacities onto their depended cloud. In other words, it is important for client to get provides on service delivery. Normally, these are given through service level agreement (SLA) consulted between suppliers and purchasers. The first issue is the definition of SLA specifications in such a way that has an appropriate level of granularity is the tradeoffs between expressiveness and complicatedness such that they can cover most of the consumer desires and relatively simple to be verified and evaluated. Also the different cloud offerings (IaaS, PaaS, SaaS & DaaS) will certainly need to define different SLA meta-specifications.

This likewise raises various usage issues for the cloud provider. For instance, assets administrator needs to have exact and restored data on the assets use at specific time inside the cloud. By refreshed data, we mean any adjustment subscribed to by. The assets administrator is in continuous assessment and modification for SLA fulfillment. The assets administrator needs to utilize quick useful choice model and streamlining algorithm to do. SLAs cannot be completed when resource requests may be required to be dismissed. All of these need to be done complete "self- service" in the cloud computing. Apart from this, there is a need to consistently include user feedback and evaluation features in advanced SLA evaluation framework [9].

3.5 Application-Level Security

The application level security refers to the usage of software and hardware resources for providing security to the applications such that the attacker is not able to get the unauthorised access to the application and make the desirable changes to its format. Now, some day the attack begins and it tries to access as the trusted user and it easily allows the full access to the attacker and this makes the client suffer. The major reason behind this is; old network level security policies. With the latest technological progress, it is quite possible to duplicate a trusted user and contaminate the entire data without seeing it. Subsequently, it is important to introduce large amount of security checks to limit these dangers.

Traditional ways to deal with increased security problem have been developed to develop a work-oriented ASIC device that can handle the specific work that provides higher level of security with greater performance. Be that as it may, with application-level dangers being dynamic these shut frameworks have been seen to case back in contrast with the open finished framework.

The abilities of a shut framework and additionally the flexibility of an open finished framework have been consolidated to build up the security stages dependent on Check Point Open Performance Architecture utilizing Quad-Core Intel Xeon processors. Indeed, even in the virtual condition, organizations like VMware and so forth are utilizing Intel Virtualization Technology for better execution and security base. It has been seen that all the more frequently sites are anchored at the system level and have solid safety efforts; however, there might be security provisos at the application level which may permit data access to unapproved clients. The dangers to application-level security incorporate XSS assaults, cookie poisoning, hidden field control, SQL infusion assaults, DoS assaults, backdoor and debug options, CAPTCHA breaking, and so forth coming about because of the unapproved utilization of the applications [12].

3.6 Data Security

Data Security is the prime concern for any technology, but it still remains as a major challenge when SaaS users have to depend upon their providers for proper security [15].

The organisational data is often processed in plaintext & stored in the cloud in SaaS. Moreover the data backup becomes a prime topmost aspect in order to carry out recovery in case of any disaster but this imparts security questions as well [16]. Rotating administration applications & databases having sensitive data about the Cloud Service Provider (CSP) which have no controller of their own information have various weaknesses [17]. Numerous clients have weaknesses in the information security model and this increases an unauthorized access to information. The following valuations validate the security of the enterprise that collects the information at the SaaS vendor [15]:

- Cross-site scripting [XSS].
- Access control weaknesses.
- OS and SQL injection flaws.
- Cross-site request forgery [CSRF].
- Cookie manipulation.
- Hidden field manipulation.
- Insecure storage.

- Insecure configuration.

In SaaS, organizational information is often managed in plaintext and stored in the cloud. The SaaS supplier is responsible for the security of the information in the way it is processed and stored. Additionally, data backup is very important feature for ceasing the recovery cause of disaster; however, it brings security burden as well [16].

3.7 Security Concerns with the Hypervisor

Distributed computing lays essentially on the idea of virtualization. In a virtualized world, the hypervisor is characterized as a controller prominently known as virtual machine director (VMM) that enables various working systems to be kept running on a system at any given moment, giving the assets to each working system to such an extent that they do not meddle with each other. As the digit of operating systems going on the hardware unit increases, however, the problem of security increases, the need to consider the new operating system. Since different working frameworks would keep running on a solitary equipment stage, it is beyond the realm of imagination to expect to monitor all, and consequently, keeping all the working frameworks secure is troublesome. It might happen that a visitor framework attempts to path a malignant encryption on the feaster framework and fetch the framework low or take complete control of the framework and square access to other company working frameworks.

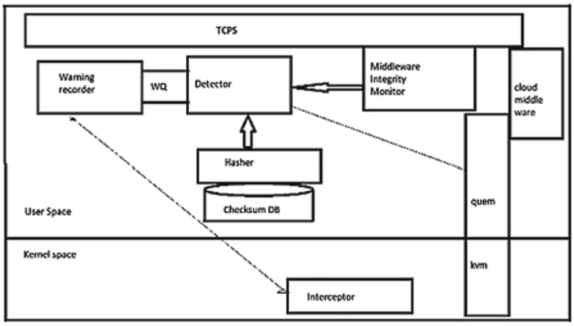
It cannot be denied that there are dangers related with having the equivalent physical foundation among a lot of numerous employers; even one existence vindictive can make dangers the other utilizing the equivalent organization, and consequently, security as for hypervisor is of extraordinary worry as all the visitor frameworks are controlled by it. On the off chance that a programmer can deal with the hypervisor, he can make changes to any of the visitor working frameworks and oversee every one of the information going through the hypervisor.

Different kinds of attacks can be propelled by focusing on various parts of the hypervisor. In the hypervisor architecture, an advanced cloud security system can be developed on the basis of the behavior of different components, which monitors the interval between guest VM activities and various hybrids.

3.8 Virtualization Level Security Issues

Of cloud runs simultaneously on the host computer applying OSs in the virtualized (multi-inhabitant) condition. Actual weaknesses in a VM that are circulated all through the physical and simulated venture assets permit digital attacker, malware, or different dangers to remotely misuse.

Fig. 1 Structure of TCPS



The security danger also increases with the help of VMS. As soon as the amount of visitor operating framework increases in the hypervisor, security concerns with that new visitor OS also increases. Since it is impossible to hope to screen all OSs, keeping up the security of those OSs is troublesome. There can be chances that a visitor framework attempt to execute harmful code upon the host structure as well as cleave lower hold the full control of a framework plus square approach to further visitor OSs. There are dangers related to having equivalent real framework among lot of various clients yet one being malevolent. On the off chance that a hacker can deal with hypervisor is that they can make changes to any of the visitor OSs and deal with every one of the information going through hypervisor. Isolation between two VMs is not completely adequate by current virtual machine monitors (VMMs). By compromising the lower layer hypervisor vulnerabilities, the attacker can get access over installed VMs. Example of some attacks include Blue pill, Subvert & DKSM on the virtual layer. This is still an open challenge to prevent such threats. Latest Generation of rootkits that benefit from the processor technology that allows an attacker to insert an additional hypervisor between the hardware and the software. The hypervisor takes control of the system & transforms the original OS into a virtual guest on the fly. As regards the software based virtualization is considered, this kind of hijacking does not require restart & this makes it all the way more difficult to detect the intrusion [11].

3.9 Sharing of VM images in Cloud Introduces Security Risk

The proprietor of a picture is worried about privacy (e.g., unapproved access to the picture). The client of picture is worried about privacy, for example, a malignant picture that is able to debasing or theft the clients own individual information. For sample, instances working on Amazon's EC2 platform simply compromise by performing different attack, related the mark wrapping attack short scripting (XSS) attack, or DOS attack. This enables attackers to make, modify, and erase VM pictures and change administrative passwords and settings that are put into setting with EC2 for S3 get to. This is a threat of infringement (e.g., working unrestricted software and programming with expired licenses). The manager of cloud is worried about the security and consistency of the cloud all in all and the trustworthiness of the pictures. There is a danger of harms caused by malware contained in any picture put away in the repository.

There ought to be standard machine for finding out integrity of visitor VMs for effective capability or avoid interface of computing, information damage, and abuse of assets.

Figure 1 depicts Manager based clear cloud protection system (TCPS) that screens honesty of cloud parts. TCPS is put among visitor's OS and the virtualization layers, which screens visitor VMs and secures them opposite to interlopers and assaults. It also addresses clear issues in the cloud [11].

4 Cloud Security Problems

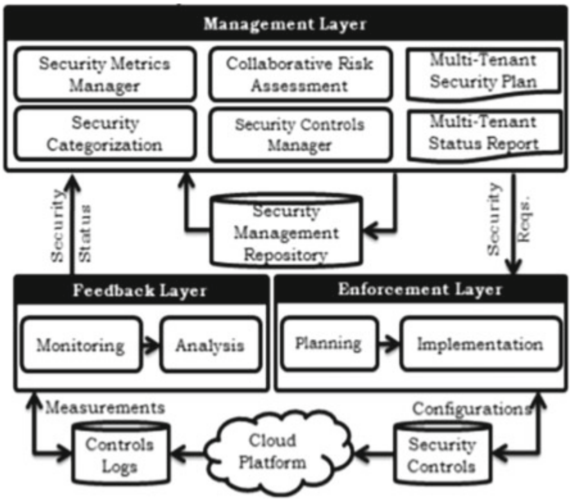
The cloud framework is functioning in online network, and the security issues in online network also can be detected in the cloud classification. The cloud structure is not different from the traditional structure in the PC, and it can fit other important and unique security issues. The large outfit around cloud computing remains security and privacy [18]. The information resources the cloud classification. The cloud requirement provides information control framework for the employer. The information security analysis too may be deployed in the cloud system. The cloud framework can deploy in various cloud bud. The different area has various rules, so the security managing can face the rule problem. Distributed computing service is necessary to enhance permissible security [19]. It has appeared as a major issue for online network clients, and they have to face the problem of managing large multiple of records and identification, which helps the clients using password and identification management scheme that decreases security of their personal information. Besides, Web site-driven web experience issues in managing Internet client record and individual content allocation [18, 19].

For large and fast processing of the information, a CSP may utilize assets that are accessible around the activity. This factor reveals the client information over whole net which may result in major security menace. To fix this problem, an intrusion finding system (IDS) component is mostly in the cloud paradigm [20].

4.1 Trust Chain in Clouds

Trust has a significant influence in pulling in more customer by depending on cloud players, due to loss of control (as discussed earlier) cloud costumers depend upon the cloud providers using trust system as on alternate into giving customers transparent power their information and cloud resources (Fig. 2).

Fig. 2 Management layer



Therefore, the cloud provider assures the client that the operation of the provider is following organizational safety measures and standards.

Concern of identification management includes various measurements; amid others, they consist of clients having to share their characteristics to many service providers, dealing with individual data of the client being conciliated while executing a federated identity. Rodriguez et al. exhibited Federated Identity Architecture (FIA) as a method for resolving weakness and there are three designs for enforcing security problem in FIA including WS-Federation, Shibboleth, and Liberty Alliance [21]. Other than attack, permissible compliance and protection guaranty are other softy matter in federated identity. The recent FIA has no decent way to protect client's data. Stage for Privacy Perform.33 acnes Project or P3P (founded by W3C) has been introduced as a standard and an assignment for developing FIA, by integrating P3P into the FIA [22]. Network to human resources (HR) is hard because HR is the only master source for team identification. Ability to succeed federated identities does not exist in maximum administrations. There are no authoritative data sources to find identities in partner associations. Most associations have no capability to convey with individuals directly in extra institution. These problems and the need of provisioning standards emphasize the importance for decent and comprehensive method to manage how identity properties, accounts, and development management system of all entity-types will take action in the cloud co-framework [23] (Fig. 3).

5 Conclusion Direction

This paper explains the security problem of the cloud computing such as low-cost, platform, independent scalability, elasticity, as well as reliability. The security cloud

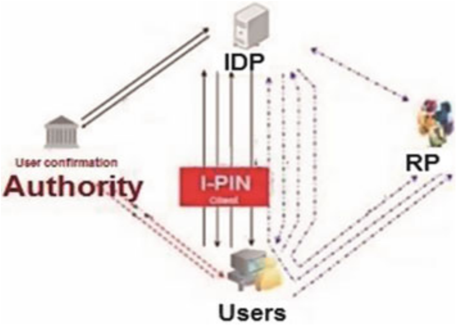


Fig. 3 You and Jun proposed mode [23]

computing manages various field of information management along with its services. The problems included data security in cloud problem also discuss problems in the cloud system are discussed. The cloud computing are on the accelerated pace in their development which have good prospect along with great potential. In this script presented the number of attacks cloud authentication although our main in used to magnified the theft concern because some of the issues are partially solved but identity theft requires further thought. The various customers which degrade mistrust as well as privacy of cloud computing which do not want to move the data into Cloud computing. The various method which are used to protect the security in order to make it effectively or solved this problem are issues are check by the cloud computing provide. Developing the cloud computing as well as security issues is the core problem.

References

1. AmazonElastic Compute Cloud, http://www.amazon.com/ec2/ National Institute of Standards and Technology. The NIST definition of cloud computing; 2011. [retrieved 14.04.11]
2. Google App Engine, http://appengine.google.com Google AppEngine, http://appengine.google.com
3. Microsoft, http://www.microsoft.com/
4. Ren K, Wang C, Wang Q (2012) Security challenges for the public cloud. IEEE Internet Comput 16(1):69–73
5. Vieira K, Schulter A, Westphall C, Westphall C (1989) Intrusion detection techniques for Grid and Cloud computing environment. IT Professional 12(4):38–43. Young M (1989) The technical writer's handbook. University Science, Mill Valley, CA
6. Mell P, Grance T (2011) The NIST definition of cloud computing
7. Zissis D, Lekkas D (2012) Addressing cloud computing security issues. Fut Gener Comput Syst 28(3):583–592
8. Dillon T, Wu C, Chang E (2010) Cloud computing: issues and challenges. In: 2010 24th IEEE international conference on advanced information networking and applications (AINA). IEEE, pp 27–33
9. Hashizume K, Rosado DG, Fernández-Medina, E, Fernandez EB An analysis of security issues for cloud
10. Veeramachaneni VK (2015) Security issues and countermeasures in cloud computing environment. Int J Eng Sci Innovative Technol 4(5)

11. Modi C, Patel D, Borisaniya B, Patel A, Rajarajan M (2013) A survey on security issues and solutions at different layers of Cloud computing. J Super Comput 63(2):561–592
12. Singh A, Shrivastava DM (2012) Overview of attacks on cloud computing. Int J Eng Innovative Technol (IJEIT) 1(4)
13. Rong C, Nguyen ST, Jaatun MG (2013) Beyond lightning: a survey on security challenges in cloud computing. Comput Electr Eng 39(1):47–54
14. Bhadauria R, Chaki R, Chaki N, Sanyal S (2011) A survey on security issues in cloud computing. arXiv preprint arXiv:1109.5388
15. Hashizume K, Rosado DG, Fernández-Medina E, Fernandez EB (2013) An analysis of security issues for cloud computing. J Internet Serv Appl 4(1):5
16. Kumar SN, Vajpayee A (2016) A survey on secure cloud: security and privacy in cloud computing. Am J Syst Software 4(1):14–26
17. Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl 34(1):1–11
18. Cloud Securit Alliance: http://www.cloudsecurityalliance.org/
19. Dean J, Ghemawat S (2008) MapReduce: simplified data processing on large clusters. Commun ACM 51(1):107–113
20. Sun ST, Pospisil E, Muslukhov I, Dindar N, Hawkey K, Beznosov K (2011) What makes users refuse web single sign-on?: an empirical investigation of OpenID, p. 4
21. Gharooni M, Zamani M, Mansourizadeh M, Abdullah S (2011) A confidential RFID model to prevent unauthorized access. pp 1–5
22. Rodriguez UF, Laurent-Maknavicius M, Incera-Dieguez J (2006) Federated identity architectures
23. Archer DCJ, Puhlmann N, Boehme A, Kurtz P, Reavis J (2011) Security guidance for critical areas of focus in cloud computing v3.0. Cloud Secur Alliance

A Hybrid Approach-Based Energy Aware Cluster Head Selection for IOT Application

A. Kannammal and S. Suresh

Abstract Internet of Things environment has collection of communication system of various devices with few heterogeneous and homogeneous characteristics, where each device has unique identification address for activate action over network. The main purpose of gathering information is to process the communications and evolution. IOT applications face several challenges such as energy efficiency, reliable communication, latency awareness, etc. The most emerging requirement in IOT application is to implement an effective energy conscious communication protocols and clustering techniques. These techniques are reducing energy utilization of nodes and increase the network lifetime and scalability. A robust clustering technique is essential for self-organizing sensor networks. Proposed work on this paper is hybrid method of LEACH with firefly technique for optimal cluster head selection. The proposed hybridization methods used for best clustering with cluster head also enhance the energy level of node and improved lifetime of networks. Simulation results have shown the improved performance of proposed task.

Keywords WSNs · IOT · Energy-aware clustering · LEACH · Firefly algorithm · Hybrid approach

1 Introduction

During last decade, the research community focuses on the development of smart sensors networks with small size, less expensive [1]. The current research works revival in WSN and Internet of Things (IOTs). Internet of Things was first proposed for

A. Kannammal (✉)
Department of Computer Science and Engineering, Jayam College of Engineering and Technology, Dharmapuri, TamilNadu, India
e-mail: ravikanna.oct@gmail.com

S. Suresh
Department of Computer Science and Engineering, P.a College of Engineering and Technology, Pollachi, Coimbatore, TamilNadu, India
e-mail: ssuresh.siv.72@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_53

the purpose of automatically recognizing and tracing the flow of goods. Nowadays, IOT can be developed in current Internet environment to connecting wide variety things to interoperate. An IOT integrating the current emerging research technologies such as sensing, communication, networking, and cloud computing. An IOT application faces the many challenges on today research work. An IOT environment offers quick deployable solution with low cost in various applications. All nodes in IOT architecture have the following components such as sensor to sense and monitors the environment, computation unit for processing information, memory unit for data storage, transmission unit for transmitting these data to a base station and a power management unit for managing lifetime of battery.

IOT networks can be categorized with following constraints factors such as a amount of energy consumed; computing and storage capacity; communication range and bandwidth also some problems in networks architectures like security and fault tolerance, etc. [2]. In IOT application, the energy utilization relay in the following criteria such as design management on network and deployed environments. An IOT-network can be adapted in different applications like environment observing, army sector, healthcare system, etc. [3, 4].

The researches in IOT application have several challenges remain open; the challenges are energy level management, area of coverage and synchronization data and security [5]. An energy-conscious communication among all the devices is the main challenge. These articles focus on these challenges by selecting head node using clustering technique. Clustering techniques can group sensors into different subset. In each individual cluster, a CH is chosen as group coordinators for the purpose of producing a transmission schedule, gathering sensors data, and transmitting assembled data to the base station (BS). Cluster head can communicate with the base station directly or through other CHs called intra-cluster routing. The network lifetime is essential in IOT research, lifetime of network can be enhanced with effective energy-aware mechanism [6–8].

This paper reviews the energy-aware technique and dispute factors of clustering in IOT systems. The rest of this work can be described as follows. Section 2 gives overview of some of cluster head selection algorithm. Section 3 describes some of the preliminary work such as protocol and network model, and the proposed works are described in Sect. 3.1. Section 4 shows the simulation results. The proposed work is concluded in Sect. 5.

2 Related Work

Researches in IOT mainly focus on developing clustering protocols for energy-saving purpose. Younis et al. [9] describe hybrid energy efficient distributed (HEED) technique for clustering IOT architecture. This protocol mainly focuses on balancing load among the group. The key parameters to decide on cluster head are residual energy of respective node, degree of node, and distances to neighbors. Heinzelman et al. [10] describe EEDUC protocol gives a way to producing distributed cluster.

In this scheme, the grouping of node done based on distance between node and cluster head, distance within a certain unit of cluster head can be groped in same cluster and node with *m* units of distance from the cluster head may consider other cluster.

Yang et al. [11] implemented most effective optimal cluster head methods by using various hybrid meta-heuristic algorithms. This scheme has to focus global optimum with improved solutions. From literature GA has good global search characteristics, convergence is poor. Representation of weights in PSO is done arbitrarily and hence search is limited to either global or local space. In this work, it is proposed to hybrid the firefly meta-heuristic with LEACH, which finds optimal global solution with fast convergence.

Faisal et al. [12] SEP protocols mainly focus on heterogeneous architectures. SEP selects cluster heads based on the probabilities that is weighted on each node. Zonal-Stable Election Protocol (Z-SEP) which impart zonal heterogeneous, it is more applicable in IOT multi-region real environment.

3 Protocol Description

3.1 Low Energy Adaptive Clustering Hierarchy

The LEACH protocol [13–15] was the most frequently adapted protocol. This protocol mainly focus on homogeneous sensor networks because of all the nodes have equal energy. In this method, the head nodes are selected depend on system-defined probability values. The cluster head then processes the data and communicates it with the base station. This technique includes two-step processes such as setup phase and steady state phase. Main task of setup phase is nominating CH also clusters are formed based on chosen CH. In steady phase information transmission performed. A random number will be chosen in range from 0 to 1 for each node. The node has random number which is below its threshold value can be selected as cluster head, the random value greater than threshold can be consider as normal node

$$t(n) = \left[\frac{\rho}{1 - \rho\left(Rmod\left(\frac{1}{\rho}\right)\right)}\right] \quad , if\ n\epsilon N\ else\ t(n) = 0 \tag{1}$$

where the value of ρ stands for CH probability, *R* describes the current round number and *N* stands group of normal node rather than cluster heads in the last1/ ρ rounds. Clustering can be framed based on energy, the energy of available CH can be matched with other actual node, if any non-CH node has higher value than current CH, then the non-CH node can be chosen as new CH. The transmission energy can be calculated using first order radio model. A new optimal scheme projected as hybridization of LEACH and firefly methods to diminish energy utilization and enhance the network lifetime.

3.2 Firefly Algorithm

Firefly heuristic is based on the light intensity produced by fireflies. The intensity of light produced is mapped to the objective function, and hence, fireflies with low intensity are attracted toward fireflies with higher light intensity. The intensity of the light helps a firefly swarm move to brighter and attractive locations which can be mapped to finding best [16].

Firefly algorithm standardizes based on firefly characteristics and can be listed as follows:

- Each firefly can be attracted to another irrespective of their sex.
- The brightness produced by the firefly is directly proportional to its attractiveness and between two fireflies; the firefly with higher brightness attracts the one which has lower brightness. A firefly moves randomly if it is not able to find a brighter neighboring firefly.
- In the mathematical model, firefly's brightness is based on the objective function. Firefly meta-heuristic is chosen for its capability of providing optimal solutions for multi-objective problems.

3.3 Firefly Procedure

```
1. Define an objective function $g(A), A = (A_1, A_2, \ldots A_D)$
2. Initializes fireflies $A_i$ $(i = 1, 2, \ldots, N)$
3. Calculate light intensity $I_i$ at $A_i$ is using objective function $g(A_i)$
4. Compute light absorption coefficient $\gamma$
5. if $t < M$
     i.   for $x = 1$: $N$
     ii.  for $y = 1$: $i$
     iii. if $(I_y > I_x)$ then
     iv.  Reassign firefly $x$: $y$
             End if
6. Based on distance, the attractive of brightness varies $r$ via $\exp[-\gamma r]$
7. Calculate new solutions then revise light intensity
      Scope of loop $y$ and $x$
8. Pick best rank solution
9. Repeat step from 5 to 8 until the condition becomes false.
```

4 Proposed Hybrid Algorithm

This proposed scheme is used hybrid-based approach of LEACH and firefly search. Enhancing lifetime and reducing energy conception of an IOT node by clustering the network with suitable methods. The clustering process can be done in IOT two steps such as CH election and cluster formation.

i. **CH Election**:

Cluster head is acting as coordinator of cluster, while selecting CH suspicious analysis needs. The CH can be selected using three ways such as deterministic with help of preset fixed location, random scheme based on probability value and adaptive based on energy. The last method is more preparable.

ii. **Cluster Formation**:

Cluster head broadcasting own information to all other sensors, each individual sensor selects its own CH based on hop count, distance, and size of cluster. LEACH protocol gives better result in the initial steps then followed iteration the firefly methods execute, thus enhance the network energy level and lifetime. The evaluation of the proposed work was carried using MATLAB. Simulations were carried out using LEACH, firefly. The proposed hybrid LEACH with firefly algorithm minimized the packet loss rate. The IOT-network performance is measured based on energy and lifetime node.

Figure 1 demonstrates that the result of hybrid scheme with individual protocol such as LEACH and LEACH-Monkey Search algorithm for energy optimization. This hybrid schemes performing better than other schemes because of joins the searching ability of FA with strength of LEACH. This proposed hybrid method increases the lifetime and efficiency of node.

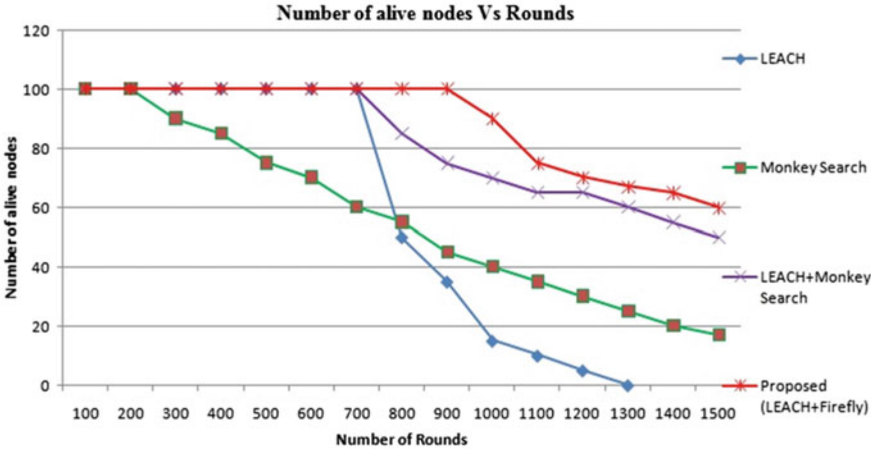


Fig. 1 Network throughput of hybrid schemes

5 Conclusion

Current research widely focus on sensors application like IOT in which clustering process is main issues to saving energy level of sensors node, in concern this, a proposed hybrid scheme of LEACH and firefly search methods performance is offered. The result of hybrid approach for the clustering nodes illustrates enhancement in the performance parameters such as energy level, lifetime of IOT environments.

References

1. Labraoui N, Gueroui M, Aliouat M, Petit J (2011) RAHIM: robust adaptive approach based on hierarchical monitoring providing trust aggregation for wireless sensor networks. J UCS 17(11):1550–1571
2. Arampatzis T, Lygeros J, Manesis S (2005). A survey of applications of wireless sensors and wireless sensor networks. In: Intelligent Control, 2005. Proceedings of the 2005 IEEE international symposium on Mediterrean conference on control and automation. IEEE, pp. 719–724
3. Palumbo F, Ullberg J, Štimec A, Furfari F, Karlsson L, Coradeschi S (2014) Sensor network infrastructure for a home care monitoring system. Sensors 14(3):3833–3860
4. Malinowski J, Geiger EJ (2014) Development of a wireless sensor network for algae cultivation using ISFET pH probes. Algal Res 4:19–22
5. Xu L, Collier R, O'Hare GM (2017) Survey of clustering techniques in WSNs and consideration of the challenges of applying such to 5G IoT scenarios. IEEE Internet of Things J 4(5)
6. Huang J, Meng Y, Gong X, Liu Y, Duan Q (2014) A novel deployment scheme for green Internet of things. IEEE IoT J 1:196e205
7. Jelicic V, Magno M, Brunelli D, Paci G, Benini L (2013) Context-adaptive multimodal wireless sensor network for energy-efficient gas monitoring. IEEE Sens J 13:328e38
8. Sun X, Coyle EJ (2012) Quantization, channel compensation, and optimal energy allocation for estimation in sensor networks. ACM Trans Sens Netw 8:1e25
9. Younis O, Fahmy S (2004) Heed: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. IEEE Trans Mob Comput 3(4):366–379
10. Li C, Ye M, Chen G, Wu J (2005) An energy-efficient unequal clustering mechanism for wireless sensor networks. In: Proceedings of the 2nd IEEE international conference on mobile Adhoc and sensor systems, 597–604
11. Yang X-S, Deb S, Fong S (2014) Metaheuristic algorithms: optimal balance of intensification and diversification. Appl Mathe Inform Sci (AMIS) 8(3):977–983
12. Faisal S, Javaid N, Javaid A, Khan MA, Bouk SH, Khan ZA (2013) Z-SEP: zonal-stable election protocol for wireless sensor networks. J Basic Appl Sci Res 3(5):132e9
13. Tyagi S, Kumar N (2013) A systematic review on clustering and routing techniques based upon LEACH protocol for wireless sensor network. J Netw Comput Appl 36:623e45
14. Heinzelman W, Chandrakasan A, Balakrishnan H (2000) Energy-efficient routing protocols for wireless microsensor networks. In: 33rd Hawaii International conference system sciences
15. John A, Babu KV (2017) Two phase dynamic method for cluster head selection in wireless sensor network for internet of things applications. IEEE WiSPNET 2017 conference
16. Fister Jr I, Yang X-S. Brest J (2013) A comprehensive review of firefly algorithms. Swarm Evol Comput 13:34–46

Modified Dive and Rise Technique Incorporating Enhanced Weighted Centroid Localization Algorithm with Ocean Current Mobility Model in Underwater Acoustic Sensor Networks

R. Bhairavi and Gnanou Florence Sudha

Abstract Underwater Acoustic Sensor Networks (UASN) have a wide variety of applications such as oil platform monitoring, prediction of natural disasters, monitoring the pollution levels, study of aquatic life, etc. The next step after the deployment of sensor nodes in the subsea environment is their localization. Localization is a vital requirement to utilize the sensed data effectively and it is necessary for trailing of nodes and detection of the target. In this paper, drifting of unlocalized nodes caused by changes in ocean currents or other factors that are modelled by using Meandering Current Mobility (MCM) Model and the unlocalized nodes computes their positional coordinates by the Modified Dive and Rise Technique (MDRT) incorporating Enhanced Weighted Centroid Localization (EWCL) algorithm. Simulation results indicate that the proposed MDRT with EWCL algorithm outperforms the existing MDRT with DV Hop localization algorithm in terms of packet delivery ratio, delay, localization ratio, and coverage.

Keywords Localization · Modified dive and rise technique · Enhanced weighted centroid localization · DV hop localization

1 Introduction

In recent times, Underwater Acoustic Sensor Networks is evolving as an emerging technology for the exploration of the underwater aquatic environment. UWASN comprises of ample number of distributed sensor nodes, Autonomous Underwater Vehicle (AUV), surface buoys, base station, and some application-specific devices [1]. In the subsea environment, the propagation of electromagnetic waves is extremely worse. At low frequencies, Radio waves can propagate only brief distances. These

R. Bhairavi (✉) · G. F. Sudha
Department of Electronics and Communication Engineering, Pondicherry Engineering College, Puducherry 605014, India
e-mail: bhairavi@pec.edu

G. F. Sudha
e-mail: gfsudha@pec.edu

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_54

characteristics make the radio waves unsuitable for communication in the aquatic environment.

Optical signals, although utilized in the blue-green region in the range of 500 nm, undergo attenuation. Irrespective of high bandwidths, the propagation of optical signals is not more than 100 m. The acoustic signal travels around 1500 m/s in underwater. This range is approximately a magnitude of five orders lesser than electromagnetic signals. Propagation speed of acoustic signal is a versatile parameter that depends on the following factors temperature, salinity and pressure (due to depth) of water.

Underwater acoustic nodes with sensing, processing and communication capabilities need to locate themselves for various applications since the information about the sensed event without its positional information is of no use. The process of finding the positional coordinates of the underwater nodes localization. Thus, precise localization of sensor nodes is a primary concern in Underwater Acoustic Sensor Network. Underwater Acoustic Communication suffers from high propagation delay, low bandwidth, Doppler shift, high bit error rate. These factors, in turn, makes the localization of nodes in UWASN a challenging task.

The structure of the paper is organized as follows: In Sect. 2, the overview of various localization techniques in Underwater Acoustic Sensor Network is summarized. In Sect. 3, the proposed MDRT with Enhanced Weighted Centroid Localization (EWCL) algorithm for efficient localization of nodes in subsea environment by considering the ocean drift model is described. In Sect. 4, the Aquasim results of the proposed MDRT with EWCL and its comparison with the existing Dive and Rise technique is presented. Finally, the conclusion is made in Sect. 5.

2 Related Works

Several research works related to the computation and estimation of positional coordinates of the underwater acoustic nodes in the subsea environment are discussed in this section. M. TalhaIsik et al. proposed in [2], a Three-Dimensional Underwater Localization (3DUL) scheme. 3DUL comprises of 2 phases, Ranging and projection and dynamic trilateration phase. In the initiative phase, the unlocalized acoustic node computes its distance to the neighbouring anchor nodes. In the Projection and Dynamic Trilateration Phase, each sensor node utilizes the computed distance and the (z coordinate) depth information from the initiative phase and creates a robust virtual quadrilateral plane by projecting any 3 anchor node onto its horizontal level to execute three-dimensional localization.

Erol-Kantarci et al. in [3, 4] studied the design principles, architectural dependencies, pros and cons of various localization techniques. A comprehensive study of centralized and distributed localization techniques along with the two subcategories namely, estimation based and prediction based and their performances are discussed. Zhou et al. in [5] proposed Unit Ball Fitting (UBF) algorithm and Isolated Fragment Filtering (IFF) algorithm for localization and accurate or high fidelity boundary detection in sensor network. Unit Ball Fitting algorithm finds a group of latent boundary nodes, which is succeeded by the refinement IBF algorithm, that is responsible for eradicating the nodes those misconceived as boundary nodes by Unit Ball Fitting technique. For each 3D boundary, a locally planarized triangular mesh surface is constructed.

Anil et al. in [6] made a comparative study of various techniques of localization that are anchor-based and anchor free schemes in underwater acoustic sensor networks. Mukesh Beniwal et al. in [7] proposed an extended version of Dive and Rise scheme incorporating time synchronization free localization technique and gave a detailed analysis of energy efficiency which is a prime concern for UWASN is discussed. In this work, the acoustic nodes whose positional coordinates are unknown are assumed to be static and the speed of propagation of acoustic signal in water is assumed to be constant. In real-time considerations, speed of propagation of acoustic signal in water depends on various parameters like temperature, pressure, salinity, gravity variation, specific volume and other oceanographic forces like tides, water currents etc., To beat out this limitation, in the proposed paper drift of the sensor nodes caused due to oceanographic forces is taken into account by incorporating the Meandering Current Mobility (MCM) Model in the subsea environment.

Anjana Das et al. proposed in [8], a positional estimation algorithm based on a single anchor node. In SAS (single anchor node support) sensor node estimates its location by considering the TOA and AOA (Time and Angle of Arrival) upon the reception of a packet from an anchor node. Location is estimated by using the equi-rectangular approximation method for projecting the latitude and longitude coordinates of sensor node into a Cartesian plane. Simulations and testing of SAS technique is carried out in several locations in Arabian ocean and which depicted that for sensor nodes of short-range, SAS technique exhibited better performance.

HanjiangLuo et al. proposed in [9] localization for double-head maritime sensor networks (LDSN). LDSN has three phases. In the initial phase, self-moored node localization (SML) algorithm is utilized by the supergroup nodes to compute the positional coordinates of the moored subsea nodes. The moored nodes that are localized in the former step turn into anchor nodes which aid the unlocalized underwater moored nodes to compute their locations by USD (underwater sensor localization) algorithm. In the terminating phase, FLA (Floating Node localization Algorithm) is used to compute the positional coordinates of free floating sensor nodes.

ZhuSanfeng et al. proposed in [10] a Dual-Hydrophone Localization (DHL) method with an objective to overcome three main issues and provide high robustness and better performance by reducing the effects of location and angular error in underwater nodes. DHL converts localization problems into half-plane intersection issues. Synchronized Dual-Hydrophone is used to meet the requirement of time synchronization which is required to overcome the long latency in underwater communication.

DV (Distance Vector) Hop algorithm proposed in [11] comprises of three stages. In the initial stage, each anchor node forwards their positional coordinates and their value of hop count to its one hop neighbouring nodes. The nodes upon the reception of these packets will add one to the hop count value and sequentially forwards the packets to its one hop nodes. Thus, almost each and every acoustic node in the entire sensor network will perceive the minimum hop count from each anchor node and the positional information of every anchor node [12]. In the succeeding phase, each and every anchor node computes the average hop distance. Finally, each unlocalized nodes estimates its positional coordinates (x, y) by performing multilateration technique. Underwater nodes are fitted with pressure sensor so the depth (z coordinate) can be calculated.

Kayalvizhi et al. proposed in [13], a node localization technique where the positional coordinates of the underwater nodes are estimated by Dive and Rise (DNR) localization incorporated with DV hop technique. Beacon node dive and rise above the water surface and periodically broadcast its location coordinates to the unlocalized nodes. Upon the reception of DNR messages, each unlocalized node estimates its positional coordinates by performing DV Hop localization. The main disadvantages of DV Hop technique is that the unlocalized nodes utilizes the average hop distance (AHD) estimated by the anchor node as a replacement for the actual distance, which induces localization error. Thus localization accuracy is an indispensable problem in the DV hop technique. The computational complexity of the DV hop algorithm is also comparatively high.

To overcome the disadvantages of existing works, in this paper, Modified Dive and Rise Localization (MDRT) incorporating Enhanced Weighted Centroid Localization (EWCL) algorithm [14] is proposed so that the unlocalized nodes compute their positional coordinates accurately.

3 Proposed Modified Dive and Rise Technique Incorporating Enhanced Weighted Centroid Localization (EWCL) Algorithm

3.1 Drift Model

In most works, the acoustic nodes whose positional coordinates are unknown are assumed to be static and the speed of propagation of acoustic signal in water is assumed to be constant In real-time considerations, speed of propagation of acoustic signal in water depends on various parameters like temperature, pressure, salinity, gravity variation, specific volume and other oceanographic forces like tides, water currents etc., To beatout this limitation, in the proposed paper drift of the sensor nodes caused due to oceanographic forces is taken into account by designing and incorporating the Meandering Current Mobility (MCM) Model in the subsea environment [15].

Meandering Current Mobility Model for oceanology renders a satisfactory degree of accuracy in modelling coastal shallow and deep water ocean currents. MCM validates the drift of the sensor nodes in the subsea environment caused by waves, hydro currents, tides and other oceanographic forces [16]. The mobility of nodes in meandering current mobility model is defined by Eqs. (1) and (2),

$$\varphi(x, y, t) = -\tan h \frac{[y - A(t)\sin(M(x - \mathrm{St}))]}{\sqrt{1 + M^2 A^2(t) \cos^2(M(x - \mathrm{St}))}} \tag{1}$$

$$A(t) = W + \alpha \cos(\Phi t) \tag{2}$$

where W is width of the meanderer, S is phase speed, M is no. of meanders, Φ is the frequency, and α is the amplitude. For this work, the following values have been assumed, $W = 1.2$, $S = 0.2$, $M = 2\pi/7.5$, $\Phi = 0.4$, and $\alpha = 5$. The current field of the ocean is taken as the sum of the net response of the tidal field of ocean and the residual current field. The spatially unvarying oscillating ocean current in an unitary direction is adopted in order to deceive as the tidal field of ocean, while the boundless sequence of clockwise and anticlockwise rotating eddies is the residual current field. The velocity field without any dimension in the kinematical model can be judged tentatively or taken close to

$$\begin{aligned} V_x &= K_1 * ƛ * v * \sin(K_2 * x) * \cos(K_3 * y) + \mathrm{K}_1 * ƛ * \cos(2K_1 t) + K_4 \\ V_y &= -ƛ * v * \cos(K_2 * x) \sin(K_3 * y) + K_5 \end{aligned} \tag{3}$$

where V_x is the speed in x-axis, V_y is the speed in y-axis, K_1, K_2, K_3, K_4, v and $ƛ$ are variables which are closely related to environmental factors, such as tides, etc. These parameters will change in different environments. Using Eqs. (1), (2) and (3), the drift of acoustic sensor nodes by oceanographic forces is modelled. After the implementation of the drift model, the randomly deployed underwater nodes at distinct depth begin to locomote. Hence the node position changes to (x', y', z'). Thus, to compute the geographical coordinates of an unlocalized acoustic node, MDRT with EWCL algorithm is proposed.

3.2 *Dive and Rise Technique*

Dive and Rise Localization method comprises of mobile anchor nodes also known as DNR Beacons with inbuilt GPS to compute their geographic coordinates while floating on the surface. These DNR beacon nodes have a predefined mobility pattern which dive and rise in vertical direction. While diving, these beacon nodes periodically broadcast their location coordinates to the unlocalized nodes that are in the region of coverage. Upon rising after one cycle, the DNR Beacon nodes recompute its geographic coordinates and dives again. Unlocalized nodes upon reception of these messages from the DNR Beacon nodes computes its positional coordinates by enhanced weighted centroid localization algorithm.

3.3 Modified Dive and Rise Technique (MDRT)

Enhanced weighted centroid localization computes weight by taking into account of several factors such as effect of different anchor nodes, radius of communication and the near anchors of the unlocalized node. EWCL algorithm comprises of three phases:

- Computation of minimum hop count (h_{count}) of each node from every anchor node in the network
- Computation of $\text{AHD}_{\text{anchor}(m)}$
- Computation of positional coordinates of unlocalized node.

Computation of minimum hop count (h_{count}) of each node from every anchor node in the network:

In the existing DVHop localization algorithm, to localize a node the vital requirement of large number of anchor nodes leads to higher localization error. The proposed MDRT with DNR localization overcomes this issue by making the anchor node broadcast only within m hops instead of broadcasting to all the nodes in the network. The range of m is 2 to h_{max}.

Initially each anchor node broadcasts $<x_k, y_k, h_{\text{count}}>$ information where $<x_k, y_k>$ represents its two-dimensional positional coordinates and h_{count} its hop count value in the form of packets to the unlocalized nodes within m hops. The value of h_{count} is initially assigned to 0. Each unlocalized node (q) maintains a table containing the following information $<k, x_k, y_k, h_{\text{qk}}>$ for each anchor node k within m hops. Each unlocalized node upon the reception of a packet from an anchor node checks its own table. If the h_{qk} value stored in its own table is less when compared to the received h_{qk} and value of h_{qk} is less then m, then the received h_{qk} value is ignored by the unlocalized node else the value of h_{qk} is incremented by 1 and the new h_{qk} is subsequently stored by the unlocalized node in its table. After the updating the table, it broadcasts the table to its neighbouring unlocalized nodes. Thus at the end of this initiative phase, each unlocalized node computes its minimum h_{qk} value from every anchor node k that are within m hops and maintains an updated hop count table.

Consider a network with 6 Anchor nodes (here nodes 10, 11, 12, 13, 14, 15) and 9 unlocalized nodes (nodes 1, 2, 3, 4, 5, 6, 7, 8, 9) as shown in the Fig. 1. Let the value of m be 2 hops. The 2-dimensional positional coordinates of anchor nodes is specified in the Table 1.

In the initial phase, anchor nodes in the network broadcast its geographic coordinates to all the unlocalized nodes within m hops. In the network depicted in Fig. 1, for the unlocalized node 3, all the anchor nodes within m hops (anchor nodes 10, 11, 12, 13, 14) are considered and anchor node 15 (since its hop count is greater than 2) is ignored. At the end of this phase, the unlocalized node 3 maintains an updated hop count table as shown in Table 2. Similarly, all the other unlocalized node maintain their updated hop count table containing $<x_k, y_k, h_{\text{count}}>$ information of the anchor nodes within m hops.

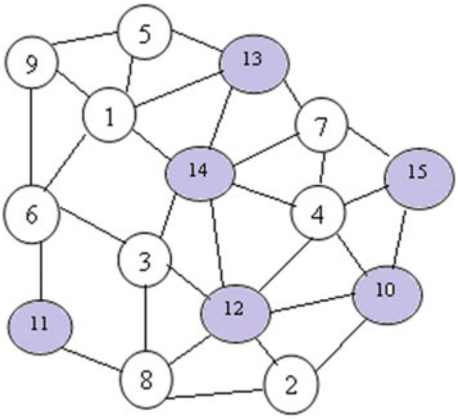


Fig. 1 Deployed anchor and unlocalized nodes

Table 1 Positional coordinates of anchor nodes

Anchor$_k$	x_k	y_k
10	436	287
11	124	237
12	381	264
13	394	605
14	347	412
15	460	407

Table 2 Table maintained by node 3 for each anchor node within m hops

Anchor$_k$	x_k	y_k	h_{k3}
10	436	287	2
11	124	237	1
12	381	264	1
13	394	605	2
14	347	412	1

Computation of AHD$_{\mathbf{anchor}(\boldsymbol{k})}$:

Each anchor node computes its average hop distance AHD$_{\text{anchor}(k)}$ using the following Eq. (7).

$$\text{AHDanchor}_{(k)} = \frac{\sum_{k=0;l=0}^{t} \sqrt{(x_k - x_l)^2 + (y_k - y_l)^2}}{h_k} \tag{4}$$

where t is the aggregate number of anchor nodes in the UWASN, l denotes all other anchors and h_k is the number of hops between anchor node k and anchor node l, (x_k, y_k) and (x_l, y_l) represents coordinates of anchor nodes k and l, respectively.

Each anchor node after estimating its average hop distance AHDanchor$_{(k)}$, sends the computed value to all the unlocalized nodes within m hops. The unlocalized node stores only the packet from the nearest anchor whose packet with information AHDanchor$_{(k)}$ while discards all the other packets. Each unlocalized node estimates its distance from the anchor node A_k using the Eq. (5),

$$d_k = \text{AHDanchor}_{(k)} * h_k \tag{5}$$

Computation of positional coordinates of unlocalized node:

In terminating stage, the unlocalized nodes determine their location coordinates <x_r, y_r> exploiting Eq. (6). Weight used for estimating the coordinates of the unlocalized node is computed using the following Eq. (7)

$$X_r = \frac{\sum_{k=1}^{t} w_k x_k}{\sum_{k=1}^{t} w_k},\ y_r = \frac{\sum_{k=1}^{t} w_k y_k}{\sum_{k=1}^{m} w_k} \tag{6}$$

where $\text{Wi} = \frac{1}{h_{\text{qk}}}$ is the weight of each anchor node i, h_{qk} is minimum hop count value of node q from anchor k and t represents the total number of anchor nodes.

$$\text{wi} = \left(\frac{\sum_{k=1}^{t} h_{\text{qk}}}{t * h_{\text{qk}}}\right)^{\frac{r}{\text{AHDanchor}_l}} \tag{7}$$

where, AHD$_{\text{anchor}(l)}$ is the average hop distance of its nearest anchor node l to the unknown node q and r is the communication radius of node.

The weight factor is inversely proportional to number of hops [14]. This has been used to give more weight age to nearest anchor. The anchor with less number of hops is closer to the given node, thus has more impact in determining the location of given node (Fig. 2).

The computed weight factor relies on the distance between the anchor node and the unlocalized node. The near anchor node to the unlocalized node have higher impact factor than the far anchor nodes.

Depth of Sensor nodes

The z coordinate which represents the depth of the sensor node is computed from the following parameters: Variation of gravity (GR) [15], specific volume (V).

$$Q = \text{Sin}(\text{Lat}/57.29578);$$

The gravity variation and the specific volumes [16, 17] are calculated by,

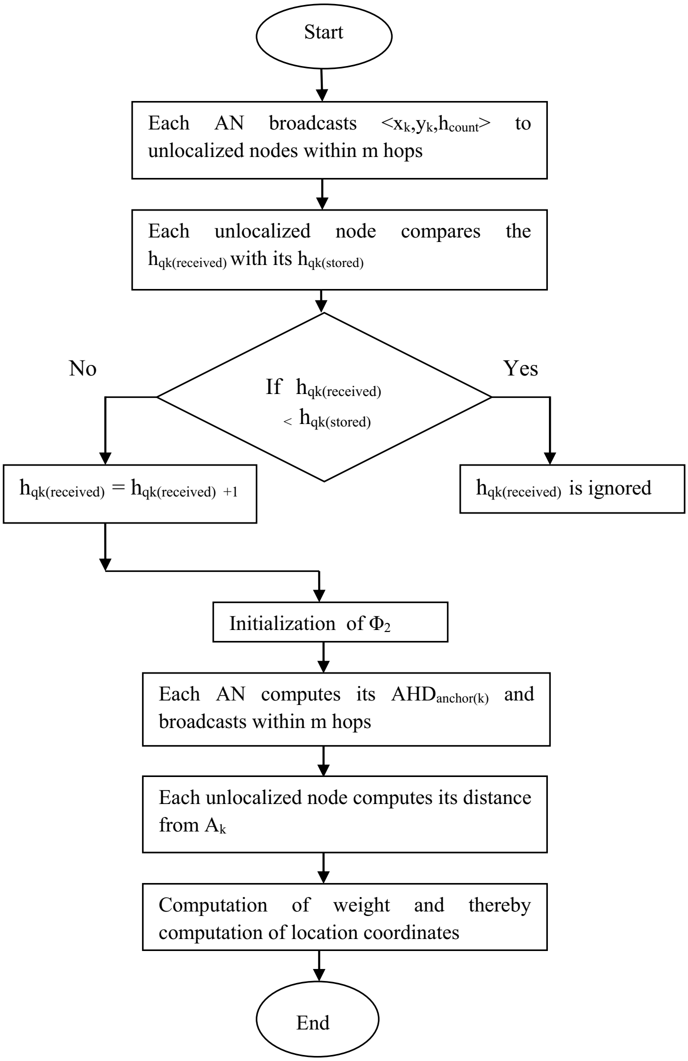

Start
Each AN broadcasts <x_k,y_k,h_count> to unlocalized nodes within m hops
Each unlocalized node compares the h_qk(received) with its h_qk(stored)
No
Yes
If h_qk(received) < h_qk(stored)
h_qk(received) = h_qk(received) +1
h_qk(received) is ignored
Initialization of Φ2
Each AN computes its AHD_anchor(k) and broadcasts within m hops
Each unlocalized node computes its distance from A_k
Computation of weight and thereby computation of location coordinates
End

Fig. 2 Flowchart for EWCL algorithm

$$\mathrm{GR} = 9.780318 * \left(1.0 + \left(5.2788\mathrm{e}^{-3} + 2.36\mathrm{e}^{-5} * Q^2\right) * Q^2\right) + 1.092\mathrm{e}^{-6} * P \tag{8}$$

$$\begin{aligned}\text{specificvolume} = {} & \left(\left(\left(-1.82\mathrm{e}^{-15} * P + 2.279\mathrm{e}^{-10}\right) * P - 2.2512\mathrm{e}^{-5}\right)\right. \\ & * P + 9.72659) * P\end{aligned} \tag{9}$$

where $P = 10{,}000$ decibars

$$\text{Depth}(Z\text{ coordinate}) = \text{specific volume}/\text{GR} \tag{10}$$

By using Eq. (10), depth (Z coordinate) can be calculated. Thus the coordinate of node (x, y, z) can be calculated using Eqs. (6) and (10).

4 Performance Evaluation

In this section, the performance of the proposed Modified Dive and Rise Technique with EWCL algorithm and the existing DV hop localization algorithms were evaluated using Aquasim (NS 2.30). Aquasim can efficiently configure and simulate the Real Underwater Acoustic Channel incorporating the object-oriented design of NS-2. The communication range of the underwater acoustic nodes are 200 m. 50 unlocalized nodes and 7 Dive and Rise Beacon nodes are randomly deployed in 1000 m × 650 m monitored space with varied depth. The mobility of the unlocalized acoustic sensor nodes are restricted within a range of 50 m. Table 3 lists the simulation parameters of NS 2.30.

4.1 Performance Metrics

The performance of the proposed MDRT with EWCL algorithm is evaluated in terms of localization ratio, packet delivery ratio, transmission range versus localization ratio, transmission range versus coverage and error. The proposed technique is studied taking into considerations the drifting of sensor nodes by incorporating MCM. The

Table 3 Aquasim simulation parameters

Parameter	Value
Number of nodes	57
Interface type	Phy/underwater phy
MAC type	802.11
Queue type	Queue/drop tail/pri queue
Antenna type	Omni-antenna
Propagation type	Underwater propagation
Transport agent	UDP
Application agent	CBR
Meandering current mobility model settings	Mean: $A = 1.2, c = 0.2,$ $K = \frac{2\pi}{7.5}, \varepsilon = 5, \omega = 0.4$
Ocean current parameter settings	$K_1, K_2 = \pi,\ K_3 = 2\pi,\ K_4,$ $K_5 = 1, v = 1,$ ƛ $= 0.5$–3.0

existing Dive and Rise technique with DV hop localization technique is compared with the proposed MDRT with EWCL algorithm.

Nodes versus localization ratio

The localization ratio (Loc_Ratio) of the UWASN is the ratio of total number of localized underwater nodes to the total number of deployed underwater nodes. The Loc_Ratio is determined as follows

$$\text{Loc\_Ratio\%} = (N_{\text{Loc}}/N_{\text{Tot})} \times 100\% \tag{11}$$

where N_{Loc} is the number underwater nodes whose positional coordinates are known and N_{Tot} is the total number of deployed underwater nodes.

From Fig. 3, it is perceived that when the number of deployed sensor nodes in the network is 25, the proposed MDRT with EWCL algorithm achieves Loc_Ratio of 96%. As Loc_Ratio is inversely proportional to the total number of deployed sensor nodes in the network, it decreases as the number of nodes increases. When the total number of nodes is increased to 55, the proposed modified MDRT algorithm still maintains a localization ratio of 89%. Thus it is observed that the proposed MDRT with EWCL algorithm has higher Loc_Ratio compared to the existing DVhop irrespective of the increase in the deployed sensor nodes.

The performance of the proposed modified MDRT algorithm is next validated by analyzing the localization ratio while varying the transmission range in steps of 20 m. Initially, the transmission range of sensor nodes is 100 m. From the Fig. 4, it is observed that when the transmission range is increased, the localization ratio of the proposed modified MDRT scheme with EWCL approach also increases when analyzed with the existing localization techniques. Consider the network scenario where the transmission range of sensor node is 150 m, the proposed DNR with EWCL has a localization ratio of 90% whereas it is 88% for existing DV hop localization.

Localization error percentage

The performance of the modified EWCL algorithm is next analyzed in terms of localization error percentage. Localization error percentage is computed using the difference between the real and the estimated coordinates of the node by using the Eq. (11),

Fig. 3 Localization ratio versus number of nodes

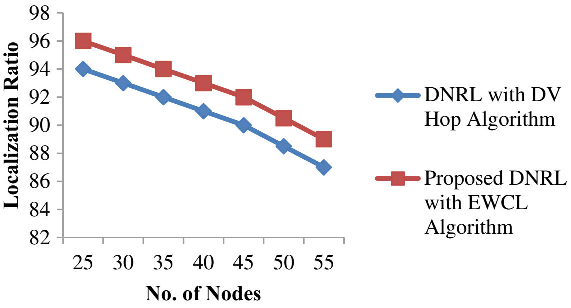
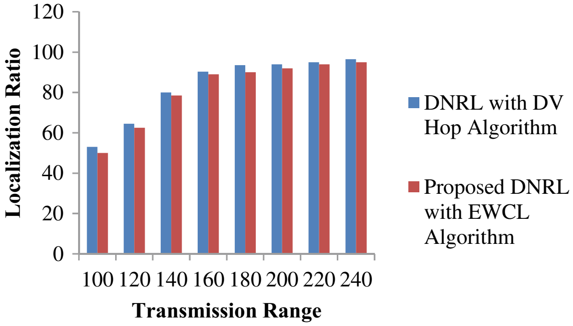


Fig. 4 Localization ratio versus transmission range



$$\%\text{Localization error} = \frac{\sqrt{(X - X')^2 - (Y - Y')^2}}{n * R} * 100 \quad (12)$$

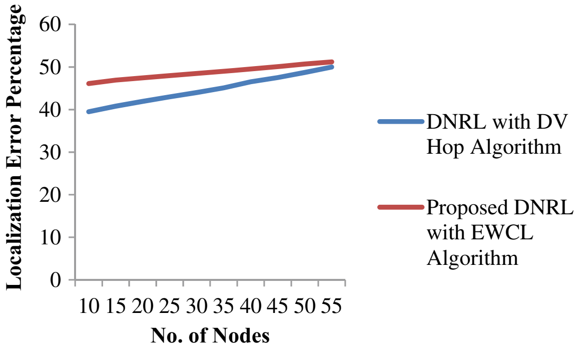
$(X, Y) =$ Actual coordinates of the sensor nodes
$(X', Y') =$ Estimated coordinates of the sensor nodes

As shown in the Fig. 5, initially when the deployed nodes is 10, the modified EWCL algorithm has an error percentage of 39.46% whereas for DV hop it is 46.187%. The proposed modified EWCL algorithm shows considerable reduction in the localization error percentage than that of the existing DV hop localization technique. The localization error percentage for the proposed algorithm is 50.311% and for existing DV hop algorithm is 51.49% when the total number of deployed nodes is 55. Thus, from the Fig. 5, it is inferred that when the deployed nodes increases, the localization error percentage is also increased.

Transmission range versus coverage

Coverage (C_R) is defined as the extent at which each point of the deployed network is under the vigilance of the sensor node. Let T_R be the transmission range of DNR Beacon node. The travelling distance of the DNR Beacon node before broadcasting its geographic coordinates is denoted as D_{beacon}. Then the C_R for the DNR Beacon node is computed from Eq. (12) as,

Fig. 5 Localization error percentage



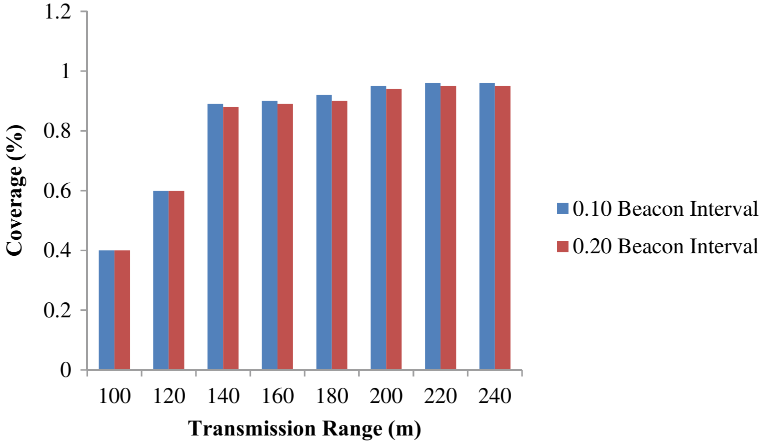


Fig. 6 Transmission range versus coverage

$$C_R = ((22/7)/12)(4T_R + D_{\text{beacon}})(2T_R - D_{\text{beacon}})^2 \tag{13}$$

The performance of the proposed MDRT with EWCL is then validated by varying the beacon interval in two cases initialized as 0.10 and 0.20 s in terms of transmission range versus coverage. Transmission range of underwater nodes is gradually changed from 150 to 250 m with a fixed interval of 20 m. From Fig. (6), it is inferred that when the beaconic message interval is initialized as 0.10, the overall coverage percentage increases when compared with the beacon interval 0.20. It is clearly observed that when the transmission range of the sensor increases, then there is a subsequent increase in the coverage. The reason for achieving coverage to such an extent is that when the beacon interval is set small with higher transmission range of sensor nodes, then many sensor nodes are able to receive multiple messages.

5 Conclusion

In this paper, the Dive and Rise Localization technique is modified using the Enhanced Weighted Centroid localization algorithm for the estimation of node position in subsea environment. EWCL algorithm comprises of three phases: Determining minimum number of hop counts by each node from every anchor, Determining average distance per hop by each anchor, Determining location of unknown node. The results validate that proposed MDRT incorporated with EWCL algorithm shows improvement in the localization performance when compared with the existing DV hop localization algorithm evaluated in terms of localization ratio, localization error percentage, transmission range and coverage.

References

1. Ong KG, Yang X, Mukherjee N, Wang H, Surender S, Grimes CA (2004) A wireless sensor network for long-term monitoring of aquatic environments: design and implementation. Sens Lett 2(1):48–57
2. TalhaIsik M, Akan OB (2009) A three dimensional localization algorithm for underwater acoustic sensor networks. IEEE Trans Wirel Commun 8:4457–4463
3. Erol-Kantarci M, Mouftah HT, Oktug S (2010) Localization techniques for underwater acoustic sensor networks. IEEE Commun Mag:152–158
4. Erol-Kantarci M, Mouftah HT, Oktug S (2011) A survey of architectures and localization techniques for underwater acoustic sensor networks. IEEE Commun Surv Tutorials 13:487–507
5. Zhou H, Xia S, Jin M, Wu H (2014) Localized and precise boundary detection in 3-D wireless sensor networks. IEEE/ACM Trans Netw:1–14
6. Anil CB, Mathew S (2014) A survey and comparison study of localization in underwater sensor networks. Int J Comput Sci Mob Comput 3:23–29
7. Beniwal M, Singh RP, Sangwan A (2016) A localization scheme for underwater sensor networks without time synchronization. Springer Wirel Pers Comm 88:537–552
8. AP Das, SM Thampi (2015) Single anchor node based localization in mobile underwater wireless sensor networks. Springer Int Publ:757–770. Springer, Switzerland
9. Luo H, Wu K, Gong Y-J, Ni LM (2016) Localization for drifting restricted floating ocean sensor networks. IEEE Trans Veh Technol 65:9968–9981
10. Sanfeng Z, Naigao J, Lei W, Xueshu Z, Shuailing Y, Ming Z (2016) A novel dual-hydrophone localization method in underwater sensor networks. IEEE/OES China ocean acoustics symposium
11. Kaur A, Gupta GP, Kumar P (2017) A survey of recent developments in DV-hop localization techniques for wireless sensor network. J Telecommun Electron Comput Eng 9:69–71
12. Khurana M, Payal A (2011) Analysis of DV-hop localization algorithm in wireless sensor networks. In: Proceedings of the 5th national conference, India, pp 1–4
13. Kayalvizhi C, Bhairavi R, Sudha GF (2018) Localization of nodes with ocean current mobility model in underwater acoustic sensor networks. In: Proceedings of international conference on computer networks and inventive communication technologies (ICCNCT 2018). Springer, India
14. Kaur A, Kumar P, Gupta GP (2017) A weighted centroid localization algorithm for randomly deployed wireless sensor networks. J King Saud Univ Comput Inf Sci:1–11
15. Caruso A, Paparella F, Vieira LFM, Erol M, Gerla M (2008) The meandering current mobility (MCM) model and its impact on underwater mobile sensor networks. In: Proceedings of 27th IEEE infocommunication, USA, pp 771–779
16. Che X, Wells I, Dickers G, Kear P, Gong X (2010) Re-evaluation of RF electromagnetic communication in underwater sensor networks. Commun Mag IEEE 48:143–151
17. Grosso VAD (1974) New equations for the speed of sound in natural waters (with comparison to other equations). J Acoust Soc Am 93(4):10841091

Tree-Based Approaches for Improving Energy Efficiency and Life Time of Wireless Sensor Networks (WSN): A Survey and Future Scope for Research

Pranesh and Santhosh L. Deshpande

Abstract Wireless Sensor Networks (WSN) are characterized by highly application-specific nature, stringent resource constraints, self-organizing, spatio-temporal traffic, and large dynamic topology with several contradicting design goals. Of these design goals, network life time and energy efficiency are considered as of paramount importance. Many research works from the past have dedicated themselves in extending the network life time and achieving energy efficiency of WSN through various techniques, including that of the application of Tree as a data structure. This article attempts to present a detailed survey of the existing research works with the application of different variants of Trees. Further, the paper tries to analyze the performance implications of application of variants of trees, advantages, and disadvantages. The paper mentions possible feasibility of the application of Red Black Trees (RBL) in WSN and the potentials for future research while giving algorithmic comparison of RBL with other tree data structures.

Keywords Wireless sensor network · Tree-based approaches · Red black tree · Network life time · Energy efficiency

1 Introduction

A wireless sensor network is constituted of large number of sensor nodes deployed randomly around phenomenon of interest Some important applications of WSN are: home automation, industrial applications, monitoring applications for environment, traffic, & wildlife, health care applications, defence applications involving security & surveillance, and some special research applications like study of sand bar formations

Pranesh (✉)
VTU-RRC, Visvesvaraya Technological University (VTU), Belgaum, Karnataka, India
e-mail: praneshvkallapur@yahoo.co.in

S. L. Deshpande
Department of Post Graduate Studies, Visvesvaraya Technological University (VTU), Belgaum, Karnataka, India
e-mail: sld@vtu.ac.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_55

or related to oceanography, etc. Due to these wide varying applications WSN are evolving as a new paradigm for information processing [1, 2]. Although WSN are similar to Adhoc Networks, there are number of fine differences. Some important differences between WSN and Adhoc network are: the number of sensor nodes in a sensor network will be large, densely deployed, prone to variety of frequent failures, the topology of a sensor network changes very frequently, and have stringent constraints for various resources. In this regard, a novel architecture & design of WSN, its protocol stack, layer-wise open issues have been discussed in detail, along with description of some of the existing WSN specific protocols as solutions to some of the open issues, in [1]. The need for self-organization and some solutions for the same have been presented elaborately in [3]. Thus, with the above general background about WSN, the motivation of this paper is to attempt to present a detailed survey of the various existing works which proposed application of Tree as a data structures and Chain concept from discrete mathematics for achieving energy efficiency and extended the network life time. Further, the organization of this paper is as follows: Sect. 2 presents the detailed literature survey of research works, the implications of application of tree data structures on the overall performance of WSN is analyzed in Sect. 3 and Sect. 3.4 identifies the potentials for application of Red Black Trees, and the paper will be concluded in Sect. 4 mentioning the scope for future research using Red Black trees.

2 Literature Survey

Wendi et al. have proposed a work involving clustering for energy-efficient communication resulting in seven times efficiency in energy [4]. Huang et al. proposed an energy-efficient routing scheme for WSN based on clustering with the use of minimum spanning trees degree constrained (CMST-DC) [5]. Z. Han et al. proposed an efficient routing by constructing routing tree (GSTEB) and mention about achieving increase in life time anywhere in between 100 and 300% depending on various scenarios while comparing with PEDAP [6]. Weighted Spanning Tree variant of LEACH (WST-LEACH) was proposed in [7] and authors claim that it performs better than LEACH. Geographic and Energy Aware Routing (GEAR) algorithm is proposed in [8]. Krishnamachari et al. [9] have discussed in detail about the influence of source-destination placement, communication network density, and the energy costs on each other. Boulis [10] proposed distributed estimation algorithm to explore energy-accuracy subspace for subclass of periodical data collection problems and presents results with five-fold improvement in energy efficiency. Yu et al. [11] explores energy-latency trade off to a great deal. Tan and Korpeoglu [12] proposed a new work consisting of two new algorithms, with power efficiency as their major design goals, called as "Power Efficient Data gathering and Aggregation Protocol (PEDAP)". These two algorithms were relying on the usage of near-optimal minimum spanning trees. A near-optimal chain-based protocol with energy-efficient as its primary design goal, called Power-Efficient Gathering in Sensor Information Systems (PEGASIS), was proposed by [13]. Kulik et al. [14] proposed Sensor Protocols for Information via Negotiation (SPIN) family of protocols, claiming 75% energy efficiency but incur lot meta-data usage. He et al. [15] proposed a research work by using feedback between sensor nodes, and reported 30–50% energy efficiency when compared to non-feedback based fixed scenarios but incurs 2 byte extra overhead for each packet for dealing with feedback. Tabassum et al. [16] proposed a work which is energy-aware version of periodical data collection. Further the same authors present two more improved works in [17, 18] which are based on 'chain' concept and claim to achieve 15–30% extended network life time and 90–95% energy efficiency. Du et al. [19] also present a similar chain-based improved algorithm for data gathering, called 'Chain Oriented SEnsor Network' (COSEN). Heuristics based aggregation tree construction for data gathering had been discussed in detail (called EADAT) in [20]. Kalpakis et al. [21] attempted to propose a novel solution for extending life time of network for data gathering purposes. Another work intending to extend the life time of network for data aggregation is presented by Hong and Prasanna [22]. Sadagopan et al. [23] focused on maximizing the data collected than so far considered parameters. However, Ordonez et al. [24] presented a more interesting work concerning the same maximization of data collection but amidst of energy constraints while providing flexibility to choose trade-off depending upon the design requirements. Another research work intending to extend the life time of the network for data aggregation was presented by Xue et al. [25]. Kim et al. [26] proposed an idea of construction of trees for the purpose of data collection, which was termed by authors as Tree-Based Clustering (TBC). Parthasarathy and Karthickeyan [27] presented a research work to improve the life time of the network for data aggregation purposes. The approach of this work involved both trees and cluster concepts as well. Salam and Ferdous [28] present a detailed survey of Tree-based data aggregation works for WSN in detail. Dreef et al. [29] focused on the application of Tree as a data structure to achieve improved security. Hussain et al. [30] proposed a work for hierarchical clusters operating in distributed fashion.

3 Analysis of Implications of Application of Tree Data Structures on Overall Performance of WSN

It may be observed from the literature survey presented in Sect. 2 that, most of the existing works have considered mainly spanning-tree variant as a data structure, with one or two applying general tree approaches. Also, few works were based on chain concept.

3.1 Disadvantages of Minimum Spanning Trees (MST) and Binary Search Trees (MST)

Main advantage of MST and BST variants of trees is that they are easy and simple to implement. But, at the same time, they have several disadvantages. In case of minimum spanning trees, they have varying path lengths along with many instances being applicable. Most frequently followed algorithms for constructing minimum spanning tree have been shown to run with complexity of $O(m \log n)$ where 'm' is the number of edges in the resultant spanning tree and 'n' is the number of nodes. Any other variants of binary trees are also having varying depths and operational costs (time complexity) depending upon the circumstances. For example, simple binary search tree may often show the performances for best case as $O(\log n)$ and for worst-case can degrade to $O(n)$ when it becomes unbalanced, where 'n' is the number of nodes in the tree. Thus, the time taken to perform operations is less if the height of the search tree is small; but if its height is large, their performance may be no better than with a linked list.

3.2 Disadvantages of Self-balancing Variants of Trees

Now let us consider the case of self-balanced tree variants those could be considered for application in WSN. AVL trees are a kind of self-balancing trees. But they are good only if lookups dominate the insert/delete operations. In the case of frequent insert/delete operations, even though its depth is at most ~1.44 * $\lg(n + 2)$, AVL tree performance will be slower requiring as many as $\Theta(\log n)$ rotations to maintain balance in an n-node tree. Further, AVL trees impose rigid balance on the tree structure leading to slow and costly operations.

3.3 Reasons for Worst-Case Performance of MST, BST, and Self-balancing Variants of Trees When Applied in WSN

But, all the above-discussed variants of tree data structure are not well suited for application in WSN. Major reasons for such infeasibility come from two aspects. First aspect of such infeasibility is that most often applied tree variants in the existing works are going to demonstrate the worst performance in case of frequent insert, delete and lookups in trees with arbitrarily longer depths. Second aspect of such infeasibility stems from some important unique features of WSN like highly dynamic topologies with very large number of sensor nodes. This unique nature may also imply that the length of path/depth/number of levels in WSN with respect to Sink/Base station/Gateway may be a serious concern. Added to these limitations, spatio-temporal nature of traffic in WSN also expects that path discovery and maintenance activities, which are local to a particular part of the WSN at any time, should be attempted in an efficient way in order to achieve the overall better performance and specifically the energy efficiency and extended network life time.

3.4 Red Black Trees (RBL): Feasibility and Potentials for Application in WSN

At first, let us glance through the properties of Red Black Trees(RBL). Red Black Trees are a variant of self-balancing trees. The nodes in RBL are differentiated as red and black nodes. Further, every path in RBL from root to leaf has same number of black links. In RBL at most one red link in-a-row or path from root to leaf is permissible. Height of tree in case of RBL is less than 2 log $(n + 1)$. Additionally, following are the advantages of RBL trees:

- Red-black trees perform insert, delete, and lookup with the Best- and Worst-case complexity guaranteed to be always $O(\log(n))$.
- Particularly useful when inserts and/or deletes are relatively frequent.
- Relatively low constants in a wide variety of scenarios.
- All the advantages of binary search trees are also available.

The only disadvantage is that they are comparatively difficult to be implemented. More details on these Red Black Trees can be found in from references like [31]. The brief summary of implementation costs in case of various tree variants has been described in [31] and repeated in Table 1 for convenient reference.

With the above-mentioned advantages of RBL trees, the potentials for being applied in WSN are very high. With this motivation, the authors of this paper have been progressing in their research work, with a hope, to design algorithm(s) for

Table 1 Summary of implementation costs of various data structures [31]

	Worst case scenario			Average case scenario		
Approach	Search	Insert	Delete	Search	Insert	Delete
Sorted array	log N	N	N	log N	N	N
Unsorted list	N	1	1	N	1	1
Hashing	N	1	N	1^a	1^a	1^a
Binary search tree	N	N	N	log N^b	log N^b	log N^b
Randomized binary search tree	log N^c	log N^c	log N^c	log N	log N	log N
Splay tree	log N^d	log N^d	log N^d	log N^d	log N^d	log N^d
Red-Black tree	log N	log N	log N	log N	log N	log N

Legend [a]based on random hash map for all keys; N^b number of nodes ever inserted; [c]probabilistic guarantee; [d]amortized guarantee applying RBL trees exploiting the previously mentioned properties of WSN and to take the benefit of advantages of RBL tree specifically to improve the energy efficiency and extend the network lifetime. Authors are hoping to publish the outcomes of the same in their future research publications.

4 Conclusions

WSN have found widespread application in different domains. The WSN are also characterized by peculiar features and conflicting design goals making them different from other types of networks. Various techniques like application of data structures etc. have been considered in the earlier research works to improve the overall performance and specifically energy efficiency and network life time. In this regard, this article made an attempt to present, as far as possible, a detailed survey of existing research works which applied tree data structures for improving the energy efficiency and extending the network life time of WSN. Further, an analysis of implications of applying different types of tree data structures on the overall performance and specifically towards the energy efficiency and network life time was also presented. Also, this article presented a brief discussion on the possible potentials for application of Red Black Tree as data structures for improving energy efficiency and network life time while comparing the same with other variants of trees with a hope to establish the feasibility of application of Red Black Trees as a data structure in WSN.

References

1. Akyildiz F, Su W, Sankarasubramaniam Y, Cayirci E (2002) Wireless sensor networks: a survey. Comput Netw 38(4):393–422
2. Zhao F, Guibas LJ (2007) Wireless sensor networks: an information processing approach. Elsevier Publications
3. Sohrabi K, Gao J, Ailawadhi V, Pottie GJ (2000) Protocols for self organization of a wireless sensor network. IEEE Pers Commun 7(5):16–27
4. Heinzelman WR, Chandrakasan A, Balakrishnan H (2000) Energy-efficient communication protocol for wireless micro sensor networks. In: Proceedings of international conference system sciences
5. Huang Y, Lin J, Liang C (2008) An energy efficient routing scheme in wireless sensor networks. In: 22nd international conference on advanced information networking and applications workshops. IEEE, pp 916–921
6. Han Z, Wu J, Zhang J, Liu L, Tian K (2014) A general self-organized tree-based energy-balance routing protocol for wireless sensor network
7. Chen P, Gong S, Zhang H (2010) Weighted spanning tree clustering routing algorithm based on LEACH. In: 2nd international conference on future computer and communication (ICFCC'10). IEEE, pp V2–223–V2-227
8. Yu Y, Govindan R, Estrin D (2001) Geographical and energy aware routing: a recursive data dissemination protocol for wireless sensor networks

9. Krishnamachari B, Estrin D, Wicker S (2002) The impact of data aggregation in wireless sensor networks. In: Proceedings of 22nd international conference on distributed computing systems workshops, pp 575–78, July 2002
10. Boulis A, Ganeriwal S, Srivastava MB (2003) Aggregation in sensor networks: an energy-accuracy tradeoff. In: 1st IEEE international workshop on sensor network protocols and applications, USA, May 2003
11. Yu Y, Krishnamachari B, Prasanna VK (2004) Energy-latency tradeoffs for data gathering in wireless sensor Networks. IEEE INFOCOM
12. Tan HO, Korpeoglu I (2003) Power efficient data gathering and aggregation in wireless sensor networks. SIGMOD Rec 32(4):66–71
13. Lindsey S, Raghavendra C, Sivalingam KM (2002) Data gathering algorithms in sensor networks using energy metrics. IEEE Trans Parallel Distrib Syst 13(9):924–935
14. Kulik J, Rabiner W, Balakrishnan H (1999) Adaptive protocols for information dissemination in wireless sensor networks. In: Proceedings of 5th ACM/IEEE mobicom conference, Seattle, WA, Aug 1999
15. He T, Blum BM, Stankovic JA, Abdelzaher T (2004) AIDA: adaptive application—independent data aggregation in wireless sensor networks. ACM Trans Embed Comput Syst 3(2):426–457
16. Tabassum N, QEK Mamun, Urano Y (2007) An energy aware protocol for periodical data collection in wireless sensor networks
17. Tabassum N, Mamun QEK, Haque AKMA, Urano Y (2006) A chain oriented data collection protocol for energy-aware and delay constrained WSN. Afr J Inf Commun Technol 2(3):126–136
18. Tabassum N, Mamun QEK, Urano Y (2006) COSEN: a chain oriented sensor network for efficient data collection. In: Third international conference on information technology: new generations (ITNG'06)
19. Du K, Wu J, Zhou D (2003) Chain-based protocols for data broadcasting and gathering in sensor networks. In: International parallel and distributed processing symposium, Apr 2003
20. Ding M, Cheng X, Xue G (2003) Aggregation tree construction in sensor networks. 2003 IEEE 58th Veh Technol Conf 4(4):2168–2172
21. Kalpakis K, Dasgupta K, Namjoshi P (2003) Efficient algorithms for maximum lifetime data gathering and aggregation in wireless sensor networks. Comput Netw 42(6):697–716
22. Hong B, Prasanna VK (2004) Optimizing system lifetime for data gathering in networked sensor systems. In: Workshop on algorithms for wireless and ad-hoc networks (A-SWAN), Boston, Aug 2004
23. Sadagopan N (2004) B Krishnamachari (2004) Maximizing data extraction in energy-limited sensor networks. INFOCOM 3:1717–1727
24. Ordonez F, Krishnamachari B (2004) Optimal information extraction in energy-limited wireless sensor networks. IEEE J Sel Areas Commun 22(6):1121–1129
25. Xue Y, Cui Y, Nahrstedt K (2005) Maximizing lifetime for data aggregation in wireless sensor networks. In: ACM/Kluwer mobile networks and applications (MONET) special issue on energy constraints and lifetime performance in wireless sensor networks, Dec 2005, pp 853–864
26. Kim KT, Lyu CH, Moon SS (2010) TBC for energy efficient WSN. In: Proceedings of international conference advanced information networking and application workshop
27. Parthasarathy P, Karthickeyan R (2014) Tree based data aggregation algorithm to increase the lifetime of wireless sensor network. Int J Innovative Res Sci Eng Technol (IJIRSET) 3(1)
28. Salam MA, Ferdous T (2012) Tree-based data aggregation algorithms in wireless sensor networks: a survey. In: Proceedings of the 2012 international conference on industrial engineering and operations management Istanbul, Turkey, 3–6 July 2012
29. Dreef D, Sun B, Xiao Y, Wu K (2006) Secure data aggregation without persistent cryptographic operations in wireless sensor networks. In: 25th IEEE international performance, computing, and communications conference (IPCCC'06), IEEE, pp 635–640
30. Hussain S, Yang L, Gagarin A (2009) Distributed search for balanced energy consumption spanning trees in wireless sensor networks. In: International conference on advanced information networking and applications workshops, IEEE, pp 1037–1042

31. https://www.cs.princeton.edu/courses/archive/fall06/cos226/lectures/balanced.pdf
32. Duarte Melo EJ, Liu M (2003) Data-gathering wireless sensor networks: organization and capacity. Comput Netw Int J Comput Telecommun Netw 43(4)
33. Vaidhyanathan K, Sur S, Narravula S, Sinha P (2004) Data aggregation techniques sensor networks. In: Technical report, OSU-CISRC-11/04-TR60. Ohio State University

Automated Cyber Threat Intelligence Generation from Honeypot Data

Kumar Sanjeev, B. Janet and R. Eswari

Abstract The evolving of advance cyber threats requires the cyber security specialist and system analyst to detect, analyse and timely react against such kind of cyber attacks. In real practical scenario, the timely dissemination of attack information is a challenge and that is not possible without cyber threat intelligence with inclusion of deep analysis of attack features and attack contextual information. In this paper, automated proactive approach for cyber threat intelligence generation is presented integrated with standard data sharing formats that can act as attack indicator for the security defence mechanism put in place in an organization such as SIEM. The strength of Honeypot-based approaches for cyber threat intelligence is proven with well-defined use cases. The capabilities of Honeypots to detect zero-day attacks can be benefited if and only if the attack events are timely digested by the security solutions and that is only possible by sharing the attack events in standard data sharing languages. The developed system is fully automated that include captured attack data is processed by various automated analysis engines, augmenting the contextual information and applying deep learning models for later threat prediction. Finally, we propose a system design incorporating deep learning neural network-based cyber threat intelligence generation for cyber threat prediction. To achieve all these, cluster of VM Honeypots are deployed in a public IP4 network.

Keywords Cyber threat intelligence · Cyber security · Honeypots · Malware · Deep learning

K. Sanjeev (✉)
Centre for Development of Advanced Computing (C-DAC), Mohali, India
e-mail: sanjeev@cdac.in

B. Janet · R. Eswari
National Institute of Technology, Tiruchirappalli, India
e-mail: janet@nitt.edu

R. Eswari
e-mail: eswari@nitt.edu

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_56

1 Introduction

In present technological domain, everybody is connected and utilizing the technology without knowing the advantage and disadvantages of these technologies. The same philosophy is applying in Internet-connected cyber space. The users of the Internet are growing exponentially. In the current technological world where people are virtually connected and sharing information over the Internet, it exposes them to the attackers. In recent time, the attacks performed by the attacker are highly targeted and sophisticated that exploit the vulnerabilities in processes adopted by the peoples connected over the Internet [1].

Recently, cyber criminals are becoming more skilled, and it is seen that complex attacks are being launched by adopting the advanced tactics, techniques and procedures (TTPs) which are becoming very difficult to handle by major defensive security solutions and it is very hard to investigate and remediate [2]. The TTPs adopted by the attacker is becoming less detectable, more persistent and sophisticated. Many organizations being already effected by such category of incidents like attacker used to deploy the ransomware and then demand for the payments to unlock and access the critical data and assets of the organizations. For example, the latest WannaCry ransomware attack targeted over 150 countries and infected millions of the computers [3]. To protect against these latest attacks, organizations and companies are spending huge amount of budget in state of the art security tools such as intrusion detection and prevention systems, firewalls, corporate antivirus solutions, end point protection systems, web application firewall(WAP), unified threat management system, content filtering, etc. But due to limitation in their detection approach, these security tools solutions sooner or later will be failed to provide security against the latest sophisticated and complex attacks.

Cyber threat intelligence has gained popularity and attention by the researchers and security analyst in recent years, and it has been considered as a quick remedial solution to counter the latest complex attacks. Organizations have started to download and incorporate the threat intelligence feed in their security mechanism from open sources intelligence (OSINT) databases as well as commercial partners [4]. One of the definitions of cyber threat intelligence is “evidence-based knowledge, including context, processes, indicators as well as actionable advise about the current state of the cyber connected system” [5].

This paper discusses the current state of art proactive technologies that can lead to generation of threat intelligence. In first section of the paper, the proactive tools helpful to generation of cyber threat intelligence are discussed including technology benefit to cyber security. Then in Sect. 2, the solution is proposed and designed that will lead directly as indicator for various state of art defensive security solutions. Also the experimental results are discussed in subsequent section. The main contribution of this research is highlighted as:

- Capabilities of Honeypot technology are addressed by the researchers to detect zero-day attacks however but most of the time it leads to offline analysis of captured data. In this paper, an automated proactive approach for attack data capturing, collection and processing is presented without loss of the contextual information of attack data.

- In-built attack data classification and labelling mechanism in the system that depicts the unclassified data further require the deeper investigation of attack data to reduce the false alarms. Honeypot is a machine designed by the human analyst, there may be possibility of false alarms. This problem is addressed by machine-based learning models.
- Detection of unknown and latest attack events through regular updating of Honeypots.
- Cyber threat intelligence generation and data sharing in standard data exchanged formats.
- Timely dissemination and integration of threat information to defensive security solutions.

2 Proactive Tools for Cyber Threat Intelligence

2.1 Cyber Threat Intelligence

In recent years, cyber threat intelligence (CTI) is playing a vital role in information security but there is a lack of standardization and literature review on clarifying the standard definition of it, every company is using his own definition of it [6]. Due to lack of standardization, it is a confusion term among many users of it. It is can be defined as threat patterns that as evidences to support that with severity of threat associated with it [7]. The definition of cyber threat intelligence states that the companies can convert their processes into actions at any level of security by considering those evidences and information as contextual records [8].

2.2 State of Art Proactive Technology

Here in this section, the proactive technology is introduced and evolution of proactive technology in cyber security field is highlighted. Lance Spitzner, founder of Honeynet Project, defined Honeypots as "a security resource whose value lies in being probed, attacked or compromised [9]".

Figure 1 depicts the evolution of Honeynet technology started from GenI to GenIII Honeynet. The development of Honeypots began in the year of 1999 [9]. GenI (Generation I) Honeynet technology is introduced that was simple to implement and also considered as proof of concept in Internet security. GenI Honeynet only had basic requirements in the form of data capture and data control. Reverse firewall technique was implemented to control the infection propagation. This firewall was simple to set up as only design criteria is: (i) allow all inbound connection to the Honeypot

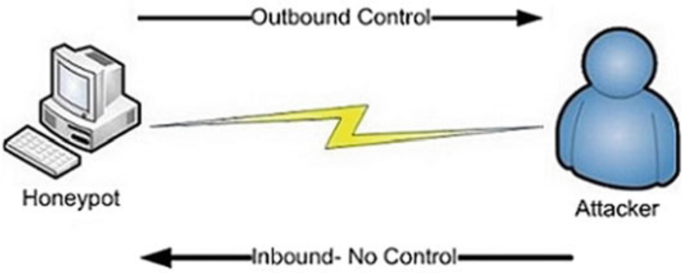


Fig. 1 Data control

and (ii) control outbound connection originating from Honeypot. The data capture mechanism in GenI Honeypot was performed with IDS engine which has to monitor the traffic traversing through the firewall to Honeypot machine.

Then, GenII (Generation II) Honeypot developed was started in the year 2002. The main aim of Gen II Honeynet is to include the real and high-interaction Honeypot to catch the real malwares. As this generation of Honeypots provided the real resources, their risk increased; thereby, the data control was crucial component. This class of system basically consists of inline firewall and an Intrusion Prevention System (IPS).

In Generation III Honeynet, the standards are introduced in the form data capture, data control and data analysis mechanisms. The combinations of Honeypots low- and high-interaction Honeypots are implemented with strong data control, collection and data analysis mechanism provided by Roo-Honeywall. Figure 2 describes the various generation of Honeynet in an abstract form.

Figure 3 depicts the broad overview and evolution of proactive technologies and their detection vector in a general way, and it may not be complete study but to provide the abstract overview of Honeynet technology and their detection attacks indicators over the period of time [10].

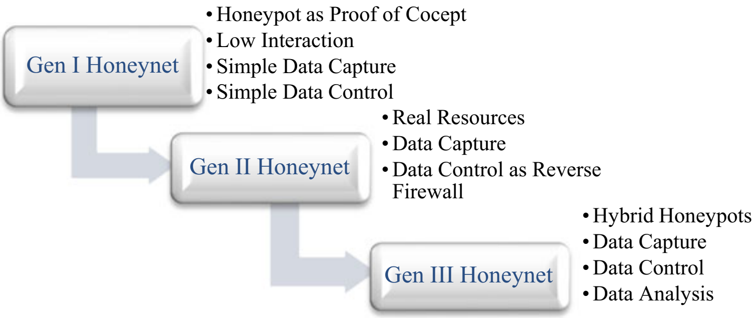


Fig. 2 Generation of Honeynet

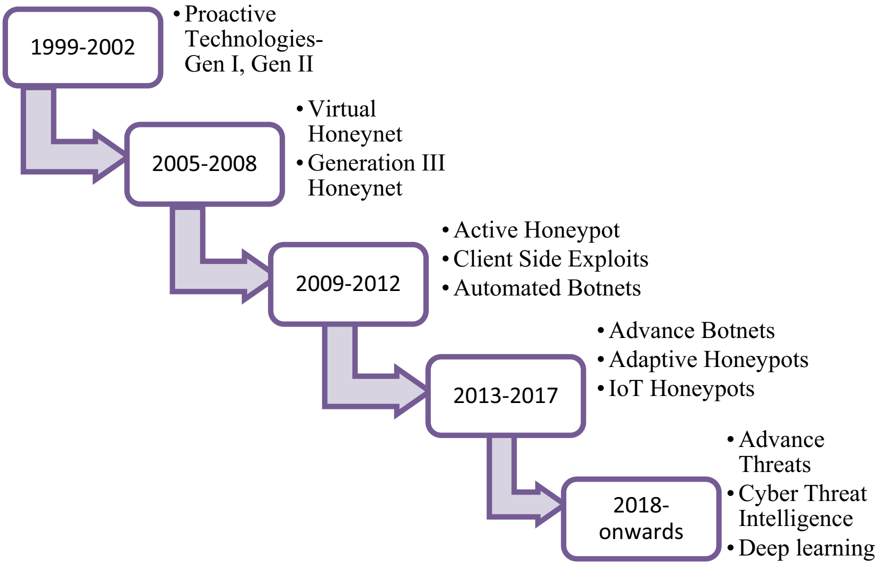


Fig. 3 Evolution of Honeynet and their detection vector

3 Proposed Solution

3.1 Honeypot as Detection Indicators for SIEM

In security field, a new technology is introduced in recent years known as SIEM which stands for Security Information and Event Management [11]. It is a very helpful product having capabilities to digest security event's raw information from multiple sources such as syslog, firewall, IDS/IPS, analyse them and apply correlation mechanism to them and provide the unified picture of threat to security and incident analyst. The broad block diagram of SIEM is depicted in Fig. 4.

One scope to enhance the detection approach of SIEM or other related security defensive solutions is use of Honeypots. Honeypots is an environment where the vulnerabilities are intentionally introduced in order to catch the latest and complex attacks who are trying to attack the asset of the organizations. Moreover, Honeypot had shown the capabilities of zero-day attack detection.

The evidences captured on the Honeypot are treated as attacks infection with low false positive and also these evidences can be used as contexts of the attacks. These information can lead to generation of threat intelligence as detection indicator to SIEM. By deployment of a variety of Honeypots covering different geographical locations, different types of organizations (banking, telecommunications, health, academic, etc.) shall give a real-time visibility of the attack infection life cycle.

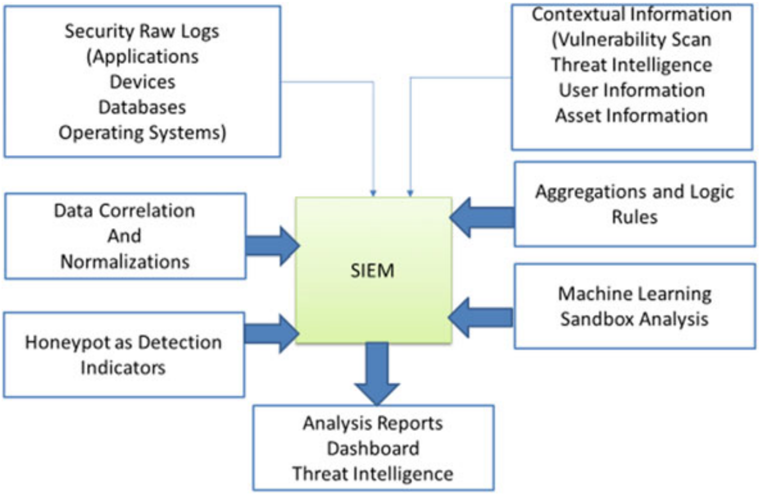


Fig. 4 Honeypot integrated with SIEM

4 Experimental Results

Table 1 describes the first level of identified threat feeds that can be generated and converted into standard formats for data sharing platforms. The first column of the table indicates the parsed and normalized data sets of different attack classes such as (i) Port Scan, (ii) Connections, (iii) Bot CnC IP, (iv) Infection Source IP,

Table 1 Threat feed categories

Parsed threat feed name	Threat feeds from various Honeypots	
	Indicator	Source of feeds
Port scan	IP and geo-details	Passive Honeypots
Connections	IP and geo-details	Passive Honeypots
Bot CnC IP	Command and control IP	Botnet analysis applied on Honeypot data
Infector source	Bot source IP	Processed data of Honeypot
Egg download IP	Secondary infection IP in Bot infection life cycle	Processed data of Honeypots
Exploit	IP and geo-details	Passive Honeypots
Malicious URL	URLs	Active Honeypots
Malware	Malware hash	All Honeypots
Malware domain	Domains	Behaviour analysis
DGA domains	DGA malicious domains	ML unsupervised model for DGA Botnet analysis

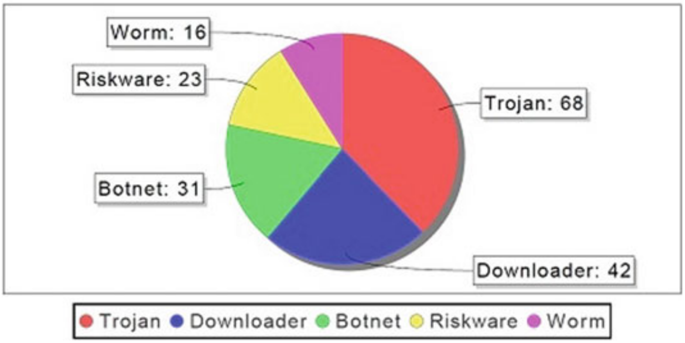


Fig. 5 Malware distribution

Table 2 Honeypot categories

Honeypot class	Types of Honeypots	
	Category of Honeypot	Descriptions
Dionaea	Passive Honeypot	Emulate ports and services
Window 7—home base edition	Passive Honeypot	Real resources

(v) Egg Download IP, (vi) Exploit IP, (vii) Malicious URLs, (viii) Malware, (ix) DGA Domains, (x) Malware Domains and (xi) Indicator of Compromise. The attack classes are in standard data sharing models such as STIX 2.0 [12] formats so that it can be directly given to security solutions such as SIEM.

Figure 5 depicts the distribution of malware attacks that occurred during 01/07/2018 to 04/02/2019. These are the brief categories of malwares hashes labelled by popular antivirus scanners. Table 2 highlights the category of Honeypot sensors deployed during this period. Certain malware hashes have not labelled by popular antivirus engines; hence, they need further deeper investigation to strengthen the scope of cyber threat intelligence.

Table 2 depicts the classes of Honeypot deployed in IPv4 networks including low- and high-interaction Honeypot sensors. First column is the class of Honeypot second is category like passive or active Honeypot and third column depicts the descriptions like what are the ports and services running on that Honeypot sensor.

5 Conclusion and Future Work

In this paper, automated framework for cyber threat intelligence generation using Honeypot Technology is presented. Honeypot is a resource where the vulnerabilities are intentionally configured to catch the latest targeted attacks; hence, there is a low false positives. But we cannot take everything as low hanging fruit because it needs further deeper investigation to avoid any mislead information to the customer, organizations, incident response team, etc. Analytical techniques are applied on both class of attacks (i) labelled attack detected by signature-based and heuristic-based approaches and (ii) unlabelled attacks, i.e. not detected or missed by these techniques. In the end, we propose a research and development of Deep Neural Network-based cyber threat intelligence that will automatically analyse the attack data based on the feature matrix given to them and can be fine-tuned at later stage.

Acknowledgements We would like to thank to Centre for Development of Advanced Computing (C-DAC), Mohali for considering National Institute of Technology (NIT), Tiruchirappalli as a model deployment location under threat intelligence generation project.

References

1. Ernst and Young Global Limited (2014) Cyber threat intelligence—how to get ahead of cybercrime. Insights on Governance, Risk and Compliance
2. Watkins K-F (2017) M-Trends 2017: a view from the front lines, vol 4. Premier Outlook
3. Kaur Sahi Asst S. A Study of WannaCry Ransomware Attack. Int J Eng Res Comput Sci Eng. 2017;4(9):79
4. https://github.com/hslatman/awesome-threat-intelligence
5. https://www.gartner.com/doc/2487216/definition-threat-intelligence
6. Boeke S, van de BDP J (2017) Cyber threat intelligence—from confusion to clarity; an investigation into cyber threat intelligence
7. Qiang L, Zeming Y, Baoxu L, Zhengwei YJJ (2017) Framework of cyber attack attribution based on threat intelligence. ICST Inst Comput Sci Soc Inform Telecommun Eng 190:92103
8. Alsmadi I (2019) Cyber threat analysis. In: The NICE cyber security framework. Springer, Cham
9. Spitzner L (2003) The Honeynet project: trapping the hackers. IEEE Secur Priv Mag 1(2):15–23
10. Kumar Sanjeev et al (2012) Distributed Honeynet system using Gen III virtual Honeynet. Int J Comput Theory Eng 4(4):537–541
11. Ailianos T (2014) SIEM optimization using Honeypots. Master Thesis
12. https://oasis-open.github.io/cti-documentation/stix/gettingstarted.html

Analysis of MPTCP Packet Scheduling, The Need of Data Hungry Applications

Neha Rupesh Thakur and Ashwini S. Kunte

Abstract Multihomed devices are common in today's environment but are underutilized. Uninterrupted application requirements have leap bounds in terms of throughput requirements. Multipath TCP (MPTCP) is a recent and successfully built standard at transport layer, to achieve the above requirement using multipathing. Long-lived flows carry heavy payload and short-lived flows look for quick response. Scheduling algorithm should consider these requirements and accordingly implement varying strategies to fulfill these needs. Long-lived flows need MPTCP, to get maximum throughput. Short-lived flows can perform with TCP or with slow subpath of MPTCP. To distinguish between short- and long-lived flows and distribute their traffic on appropriate subflow of MPTCP, an intelligent packet scheduling algorithm is required. Research is climbing toward building optimum scheduler for MPTCP. Many packet scheduling algorithms are investigated in this paper for proper path selection, increased throughput, energy efficiency, bandwidth aggregation and receiver buffer optimization, by which issues are listed for them to develop better strategy using newer and advanced algorithms.

Keywords Multihomed · Multipath TCP · Packet scheduling · Short- and long-lived flows

1 Introduction

Why multipathing: TCP uses only one interface for single path communication. If it comes across the range of powerful and cheap network-like WI-FI, then it has to break its previous network path (4G/LTE), and it has to establish a new one. Switching between two networks may introduce unnecessary delay and breaks. This degrades

N. R. Thakur (✉) · A. S. Kunte
Department of Electronics and Telecommunication, Thadomal Shahani Engineering College, Bandra, Mumbai, India
e-mail: neha.thakur81@gmail.com

A. S. Kunte
e-mail: askunte@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_57

the ongoing application's performance. This requirement introduces the concept of concurrent multipath communication. Today's multihomed devices, modern radio access technologies and advanced wireless communication technologies are able to provide seamless and fast communication to data hungry applications. Seamless data reception needs multipath transmission rather than single path transmission. This paper is mainly written to focus packet scheduling in multipath TCP. In first section, it gives information about what is MPTCP, its evolution and how it works. This paper gives small description of congestion control in MPTCP also, and finally detailed study of its packet schedulers is given.

1.1 Exploration of MPTCP

Work has been done at various layers on multipath transmission. Application layer protocol XFTP (modified File Transfer Protocol) [1] provides multiple sockets to single path for multipath communication. Microsoft gave virtual WI-FI technology for multipath communication. At transport layer Transmission Control Protocol (TCP) [2], enhancement is done since last decade to give best throughput, resilience and better performance feel in modern applications, requiring fast response. Next to TCP other protocol built is SCTP (Stream Control Transmission Protocol) [3]. SCTP uses TSN (Transmission Sequence Number) for flow control of multipaths. It is IETF (Internet Engineering Task Force) standard. SCTP is UDP protocol and not compatible with TCP. It uses round-robin path scheduling technique. LS-SCTP (Load Sharing SCTP) [4, 5] uses intelligent path scheduling for multipath transmission. PATTHEL (Parallel TCP transfer Helper) [6] gives better feel of multipath transmission but it does not determine total number of paths available between the end hosts. MPTCP [7] is recent and successful work done at transport layer. MPTCP, the standard of IETF is purely built in Linux kernel. MPTCP is always restricted by middleboxes whereas MPLEX [8] is a software architecture used for mobile multipath, which manipulates proxy. It is transparent to server and client application. MPLEX selects multipaths using mobile settings. In this three-way handshake is reduced to one-way handshake thus bandwidth is properly utilized. "Table 1" shows small description of multipath protocols in chronological order.

1.2 MPTCP

TCP uses only one IP address and network interface at the end hosts. Multihomed devices require concurrent paths transmission for good throughput and efficient performance. Multipathing is implemented mostly at transport layer since multipathing protocols do not modify lower layer protocols and these are transparent to upper layers. MPTCP is mainly invented for large network capable data centers. Due to the

Table 1 Exploration of MPTCP

Multipathing protocols	Author	Method/use
TCP/IP [9]	Ramaboli et al.	Packet switching
TCP [10]	Dr. Maxemchuck	Multipathing at transport layer
IETF TCP [11]	Huitems, Christian	TCP multipathing
TCP [12]	Key, Peter et al.	Stable and balance congestion control for multipath TCP
TCP [13]	Shakkottai, Srinivas et al.	Benefit of multipathing for multihomed gaming and good for Internet service providers
SCTP [3]	Stewart, Randall	Multipathing without considering fairness with TCP
W-SCTP [14]	C. Casetti and W. Gaiotto	Bandwidth aggregation for proper traffic allocation
CMT-SCTP [15]	R. Iyengar, Janardhan et al.	Fast and less retransmission using delayed acknowledgment for congestion control
CMT-SCTP [16]	Liu, Jiemii et al.	Avoidance of receiver buffer bloating by using RTX-LCS retransmission policy
LS-SCTP [17]	Abd, Ahmed, Tarek Saadawi et al.	Flow and congestion control using association and path sequence number uses (cwnd/RTT) factor to find weight of each subpath
CMP-SCTP [18]	Liao, Jianxin et al.	Flow and congestion control using association and path sequence number uses bandwidth of each subpath to find weight of each subpath
WIMP-SCTP[19]	Huang, Chung-Ming et al.	Wireless multipath SCTP, increases throughput by using two modes of transmission
PTCP [20]	Hsieh, Hung-Yun et al.	Micropath switching using bandwidth factor
M-TCP [21]	Chai, Jiwei, Kaixin Xu et al.	Sender side multipathing in heterogeneous lossy networks
MELOT [22]	Sharma, Vicky et al.	Multipath loss tolerant protocol heterogeneous lossy networks
TCP-MPTCP [23]	Raiciu, Costin, et al.	Improved throughput, aggregated bandwidth for data center environment
MPTCP [24]	Raiciu, Costin et al.	Fairness to TCP
MPTCP-MA [25]	Lim, Yeon-sup et al.	Improvement in MPTCP for wireless communication

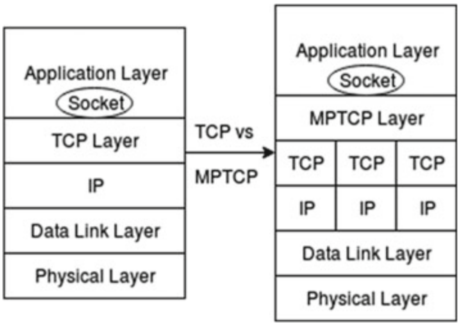


Fig. 1 TCP versus MPTC

multihoming features of devices, MPTCP is further implemented for wired and wireless communications. MPTCP is built on TCP and not on UDP [26]. Figure 1 shows the network layer architecture of [26] TCP versus MPTCP. MPTCP uses many paths with different interfaces having different IPs between two hosts. Each path of MPTCP is single path TCP (SPTCP). Host to host connection of each subpath is formed by three-way handshake as that of TCP. Multipaths combine into a single socket at end host. Number of paths in MPTCP are equal to number of interfaces available at present. To avail multipath facility multihomed devices should be MPTCP capable. “Figure 2” shows environment of MPTCP. Multipaths give high-quality end to end (e2e) performance and throughput as well as it can be used as backup. MPTCP uses two types of sequence numbers subflow and data sequence numbers [27]. Sequence numbers are helpful in two ways, for loss detection, retransmission and reassembly of out of order packets at receiver side. Currently, MPTCP is used in mobile IOS built in applications like SIRI and Korean GIGA LTE which is able to give Gbps throughput for local mobile communication. It is also used in other applications for single

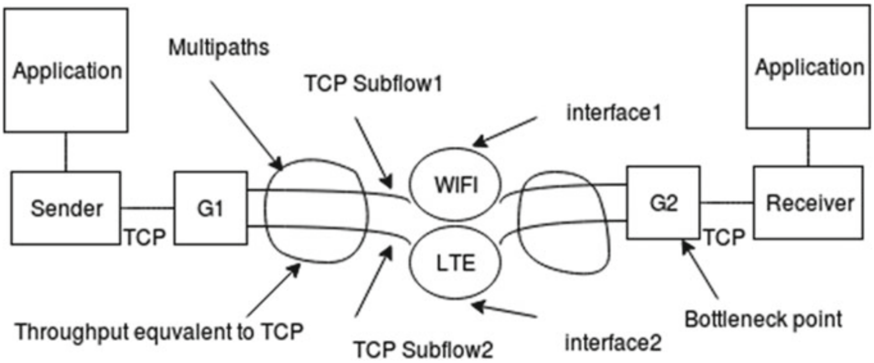


Fig. 2 MPTCP environment

and multifile download. These applications are Voice over IP (Skype, Google Hangout), Web browsing (Google search), Video streaming (YouTube, Netflix) and Instant Messengers (Facebook, Google, Hangout, WhatsApp). MPTCP is built on TCP. TCP header is not changed for MPTCP. Among all subflows of MPTCP, each individual subflow behaves exactly same as SPTCP. MPTCP works with cycle of three things establish connection, maintain connection and end up connection. MPTCP connection establishment is shown in "Fig. 3." It establishes connection like SPTCP. It uses SYN/ACK (request/response) for each subflow connection establishment. If two network interfaces are available, then MPTCP connection can have two subflows between server and user [26]. Considering two subflows as AB and CD. Firstly server sends MP_CAPABLE signal. Saying server is MPTCP capable from end A to end B (user) along with request of connection (SYN) and encrypted key of A. On the other hand, after receiving these information from A, B understands A is requesting connection and if B is free and not MPTCP compatible, it continues as SPTCP; otherwise, it sends MP_CAPABLE, SYN and ACK (acknowledgment) of B and encrypted key of B toward A. On the reception of these information from B, A sends ACK and encrypted keys of A and B. This way AB connection establishes. Additional connection can be added from any side but usually server initiates new connection by ADD_ADDR. Server sends MP_JOIN, nonce (random number to avoid replay attack), IP of C, security key of C and flag to distinguish primary path or backup path for establishing additional path CD. D then sends MP_JOIN, security key of D, authentication message and random number to C. C after receiving these sends ACK and its authentication message to D. Finally, D sends ACK to C and establishes the additional connection of different interface network. While establishing additional connection, user can discard the IP address by using NATs. MPTCP maintains connection by using packet scheduling and congestion control

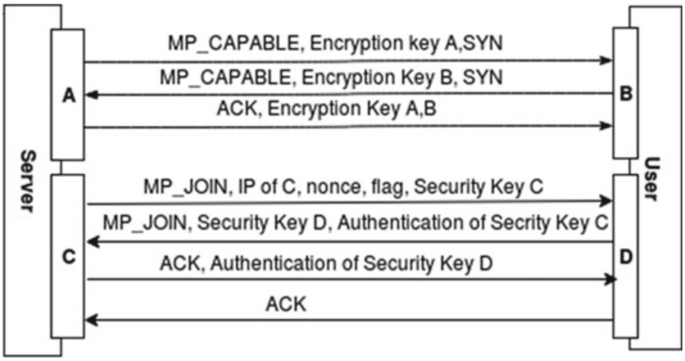

Server
A
MP_CAPABLE, Encryption key A,SYN
MP_CAPABLE, Encryption Key B, SYN
ACK, Encryption Key A,B
B
C
MP_JOIN, IP of C, nonce, flag, Security Key C
MP_JOIN, Security Key D, Authentication of Secrity Key C
ACK, Authentication of Security Key D
ACK
D
User

Fig. 3 MPTCP connection establishment

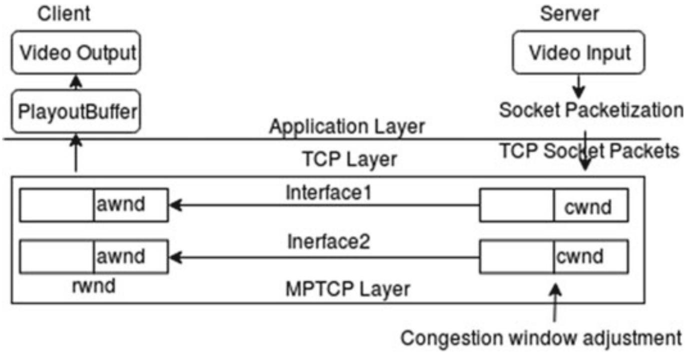


Fig. 4 MPTCP congestion control framework

algorithms. Packet scheduling distributes packets on different subflows. Congestion control diverts packets from congested subflows to less congested or free subflows. MPTCP connection ends with FIN flag, when the entire data transfer on that subflow finishes. It can also be interrupted and ended with RST (reset flag). Cascading buffers are mediators between application and transport layer [28]. These buffers are useful in communication.

1.3 MPTCP's Requirements

Congestion control. Congestion control/load balancing is required in MPTCP to increase the effectiveness of multipathing. MPTCP's sender congestion window (cwnd) size should be less than receiver cwnd size. Process is shown in "Fig. 4." TCP NewReno [29] based, TCP subflow congestion control framework [30] works in three steps, first is Slowstart (ss), in this cwnd size is blindly doubled for each round trip time when TCP just starts building connection. Flow control is not done here. It persists for a very short time. It ends when cwnd size climbs to its maximum limit, slow start threshold (ssthresh) parameter, or when very first packet is lost. In second step, congestion avoidance is done. It starts just after first step. Flow control is done using different congestion control methods. Third step is fast retransmit/immediate recovery. In this step, cwnd size is freezed. New packet insertion is also stopped. Only retransmission of lost packets is carried out.

MPTCP behavior with short-lived and long-lived flows. Short-lived flows carry lightweight data. For long-lived flows, MPTCP is blessing but for short-lived flows it is a curse. Google search (web browsing), WhatsApp messaging, SMS (Short

Messaging System) and other mobile applications generate short-lived flows. Short-lived flows are delay sensitive rather than bandwidth and throughput sensitive thus lowest RTT path is selected. When it is unavailable next lowest RTT, path is chosen but it may not always be accurate. If one connection has two subflows of 10 and 100 ms with congestion window size of 10 but 11 packets are queued at the sender buffer, then 10 packets will be transferred on 10 ms path and others will be sent on 100 ms path. Total delay is 100 ms. Delay can be reduced to 20 ms if we wait for 10 ms subflow instead of using 100 ms path. These two are heterogeneous paths and may generate many out of order packets. Out of order packets require more retransmissions and more receiver buffer. This phenomenon is called as head of line blocking. But after timeout, entire data unit may be discarded due to missing packets and the throughput decreases.

Packet scheduling. MPTCP uses concurrent diverse paths for transmission. These subflows differ in path characteristics like RTT, cwnd, delay and packet loss rate. Due to path diversity, small sequence number packets may reach receiver after high sequence number packets. They lead to many out of order packets at the receiver, many retransmission, many data units rejection and ultimately streaming quality may not be good. Due to delay factor, many packets are discarded with late successful retransmission. Receiver buffer is limited in size, so buffer overflow or head of line blocking may occur at the receiver. To avoid this problem of buffer bloating [31] and head of line blocking, smart and intelligent packet scheduler is required. MPTCP packet scheduling is packet oriented. MPTCP IETF standard uses two packet schedulers, default and round-robin. Default scheduler always opts minimum RTT subflow whereas round-robin scheduler gives data transmission chance to every subflow in round-robin manner. Some of the packet schedulers are surveyed and issues are listed in “Table 2.”

2 Limitations of Existing MPTCP

Long and short flows need to be discriminated properly. Delay should be considered in heterogeneous multipathing and retransmissions. Stringent reliability in video streaming and flexible multimedia MPTCP Architecture is needed and receiver buffer overflow should be managed.

3 Conclusion

MPTCP is capable of providing maximum throughput and uninterrupted transmission for huge data-carrying applications. In huge data-centric applications like video streaming applications, delay as well as performance is crucial. Discrimination of packet types is essential to distribute them on different appropriate subflows for concurrent transmission in MPTCP. Default scheduling methods will not use much

Table 2 Survey of multipath packet scheduling

S. No.	Problem definition	Method	Advantage	Scope
1	Bandwidth aggregation in mobile wireless technology [32]	Mobile IP is used to achieve objective. Equisize packets are scheduled on link until idle link gets packet. Scheduler uses weighted queue striped on channels	Bandwidth optimization and proper packet scheduling on multipaths are achieved. Path overheads and retransmissions are reduced	Path losses are not considered
2	Efficient multipath transmission [14]	Finds scores of paths. Minimum score path is selected for transmission. Multiple send buffers are used	Packet transmission is done considering width of congestion windows and bandwidth of subpath	Lack of intelligence in transmitting specific packet on specific path from queued sender buffers
3	Delay aware throughput optimization [33]	For each subflow, it measures combined delay of sender TCP queue and network delay. From delay, it estimates arrival time of packets at receiver and accordingly schedules new packets at sender	Along with increased throughput, this algorithm can find path failure and do recovery detection. Missing packets are also recovered	It is good for packet scheduling but throughput is below ideal throughput because of heavy packet loss

(continued)

Table 2 (continued)

S. No.	Problem definition	Method	Advantage	Scope
4	Augmentation of SCTP to improve performance in multihoming to serve concurrent multipath situations [15]	Packet reordering is done at sender. It splits fast retransmit. Virtual queues are formed at sender for retransmission queue. Two variables are used one is to save ACK of packet and other is to store destination of packet (sent for first time). Packet sent after for missing packet to same destination is acknowledged newly	Along with increased throughput, this algorithm can do path failure and recovery detection	Although concurrent multipathing is used, it uses only one path for traffic and others are used for backup or retransmission
5	Multipathing using UDP protocol at transport layer [3]	Transport address is IP address and SCTP port number. User data is fragmented and chunks of data are built. Packet validation is done for path management. Two types of sequence numbers one for data and other for subflows are used. Congestion avoidance is done using receiver acknowledgment	Multipathing is achieved using the UDP algorithm	Even if it is multipath protocol, it uses only single path for transmission at a time. It is not compatible with TCP
6	Efficient transfer of data on multipaths using TCP [6]	Data is split into chunks and spread on different TCP channels based on different active channels. Channel is assigned to active interfaces	Without doing any change in the protocol stack, the algorithm is implemented	Losses on wireless links are not considered

(continued)

Table 2 (continued)

S. No.	Problem definition	Method	Advantage	Scope
7	Reduced out of order packets at the receiver with concurrent flows at the transport layer [34]	Predicts how many data packets should be placed on each subpath based on delay	Smart scheduler compared to SCTP and MPTCP	During path selection, actual path quality is not considered
8	Building real-time multimedia environment using TCP [35]	Parallel subpaths are formed between a distributed server replicas and multimedia client. RTT is used to control and schedule multimedia streams on different paths. Coordination module coordinates content and rate. Expected video streaming time is estimated to control real-time traffic	Real-time multimedia traffic has vast bandwidth variations on subpaths, still TCP-ROME increases quality of experience	Real-time competition and rate changes of TCP flows cannot be managed
9	Estimation of RTT by using machine learning [36]	Estimation of RTT is done by many experts. Finally, average RTT is taken and correction in new RTT is done by considering current RTT	Improves multipathing efficiency of TCP by 40% and retransmission also reduces by 30%	This algorithms are applied to TCP but can be implemented for MPTCP also
10	Concurrent transmission on multiple paths (multiple interfaces) to get better throughput [7]	Uses two types of packet schedulers: default: uses lowest RTT path in round-robin fashion. Round-robin: subflows are selected randomly for data transmission in round-robin manner	In multihoming scenario, MPTCP achieves throughput at least that of normal TCP	All path characteristics are not considered for path scheduling

(continued)

Table 2 (continued)

S. No.	Problem definition	Method	Advantage	Scope
11	Improvement of throughput and receiver buffer efficiency in dynamic scenarios like gaming to reduce undesirable delay [37]	Even if congestion window is not available on subflows, subflows are used to schedule the data. Scheduling time is calculated for each path. Scheduled data packet is not sent immediately on path. If congestion window get available, scheduled packet is sent on the path	If packets are not over sent at receiver, then there is improvement in the throughput as compared to MPTCP default scheduler	It is not good for bursty traffic. Receiver buffer needs to be used carefully than default
12	($N + 1$)th packet is estimated for slow, eligible subflow. Decision-making is done for each packet on different available subflows [38]	($N + 1$)th packet is scheduled on under scheduling subflow. Concurrently, N packets are scheduled on other eligible subflows. Loss indication is done by triple duplicate ACKs. Loss rate of packet is different for each packet	Gives more robustness in lossy network	Bursty path losses are not considered
13	Throughput optimization and congestion window matching for all subflows [39]	Adaption of congestion window is done by using path delay, RTT and congestion window of each subflow, expected throughput is calculated for each subflow. If adaption time is exceeding maximum adaption time, the path is blocked for some time. Pull and push method is used	Decrease in out of order packets at the receiver. Receiver buffer size is saved	Recovery of missing and delayed packets is not coordinated. Out of order packets are also decreases

(continued)

Table 2 (continued)

S. No.	Problem definition	Method	Advantage	Scope
14	Feedback SACK (selective acknowledgment) of out of order packet is used for scheduling of current packets [40]	Estimation of N number of packets on faster subflows. Two different situations are handled, N is too small and N is too large	More adaptive in wireless networks	Path losses and bursty traffic are not considered
15	High-quality mobile streaming in heterogeneous network using coding and rate allocation. Forward error correction (FEC) is used for coding [41]	Uses coupled congestion. FEC code adjusts packet size and redundancy at rate allocator. FEC coder checks path status (RTT, delay) for window adaption. FEC packets wrap encoded video packets. Receiver has informative feedback unit, which provides RTT, bandwidth, packet loss of subflows to scheduling algorithm at sender	Arranges out of order packets into order. Multimedia interrupted output is avoided by hiding of frame copy error at application layer. Path loss and delay on subflows are reduced	Energy consumption and retransmission are not considered
16	Improvement of existing scheduler and building scheduler for high performance in multipath applications [42]	Finds maximum RTT path. Checks path as fresh or retransmitted. Retransmission is done on different subflow. Congestion window is checked for each path. Path transmission time and number of packets on subflows will be calculated	Improvement over MPTCP	In scheduler, all path characteristics are not considered

(continued)

Table 2 (continued)

S. No.	Problem definition	Method	Advantage	Scope
17	Serving of short flows within less time by considering delay and bandwidth [27]	If the RTT difference between two subflows is considerably more, then it freezes subflow having large RTT for short-lived flows. This is done regardless of their congestion window	It uses default MPTCP round-robin strategy. Data delivery is always done on fastest path and always gives throughput at least equal to SPTCP	Slow path is unused until congestion window of fast path gets saturated
18	Enhancement of MPTCP for multimedia services in multihomed vehicular networks to get sustained throughput when bandwidth is changing [43]	It considers satellite network is always available. Along with MPTCP default round-robin scheduling, deep packet inspection by group of pictures is also used. Selective discarding and partial reliability of packets are used	Packets are forwarded to application layer after RTO without waiting for missing packets. Efficient handoffs and reduced jitter are achieved	Automotive computing is not used. Slow start and loss of packets cause poor performance
19	MPLEX design for multipath transmission [8]	Middlebox proxy programming is done for multipath selection	Bandwidth is saved. Instead of three-way handshake only one-way handshake is required. 63% improvement over short-lived flows	Every middlebox should be modified

(continued)

Table 2 (continued)

S. No.	Problem definition	Method	Advantage	Scope
20	Maximization of video data received on time at the receiver [25]	Integer Linear Program is executed at scheduler. Four constraints are used. Video block is received only when exact number of different packets are obtained. Packets can send data of same video block. Decoding happens only if video block is received on which it is dependent. Video block is transmitted by packets if it is received before decoding deadline	Algorithm is independent of applications. Uses same MPTCP at transport layer	Not that efficient as optimal schedulers
21	Implementation of solution in wireless heterogeneous radios, using concurrent subpaths, which is throughput aware and energy efficient [44]	Designed by using simple or machine learning algorithms. Keeps track on interface utilization and checks for utilization above threshold. It uses five different algorithms for prediction	The best analysis is done for better understanding and experimentation	Algorithm is implemented using many algorithms thus it is complex
22	When Router's buffer size is small, throughput of MPTCP should not drop at least as that of SPTCP [45]	Routers buffer size, RTT, Ack are analyzed for transmission of new packets on the subflow	Routers buffer consideration for path with other path characteristics	Packet losses and retransmissions are not considered for path

(continued)

Table 2 (continued)

S. No.	Problem definition	Method	Advantage	Scope
23	Implementation of earliest completion first algorithm for packet scheduling using maximum path characteristics and not only RTT [46]	It considers RTT, bandwidth, bit rate, congestion window and buffer size of connection. If the fastest subflow is not available, packet is scheduled on second fastest path	Multimedia transmission is done in less time and with less error at the receiver. Web download and browsing also became fast	Negligible degradation of quality of experience thus algorithm is not 100% perfect
24	Better video streaming by using utilization of network performances measures [29]	Three algorithms are used: (1) short packet delay, (2) largest packet credit and (3) largest estimated throughput	Algorithm works for video streaming over MPTCP. It is rare topic	Scheduler uses dynamic path characteristics. Random losses are not considered
25	Optimization of throughput by using scheduling of application-oriented packets on time at the receiver [47]	Use of quality interpreter and efficient run time environment. API—per packet scheduling is done. Differentiate small and large data requests. Scheduler selection in 100 ns. Load balancing in scheduler by less overheads. One scheduler with different modes with registers. Before stoping path, it is flushed	High-level API is built. Seven novel scheduler objectives are achieved	Scheduler execution time is challenging. At application layer, less number of schedulers are tested

(continued)

Table 2 (continued)

S. No.	Problem definition	Method	Advantage	Scope
26	Efficient multipathing to increase throughput by using learning [48]	Optimum path characteristics are chosen. Optimization of WI-FI path. According to feedback, result path is managed or aborted	Access point interference is reduced. Algorithm is accurate, stable and reduces overfitting. More predictive, uses less overhead	Efficient, adaptive and more realistic scheduling algorithm can be built
27	Packet scheduling in MPTCP considering packet losses and feedback from the receiver [49]	It estimates packet on each concurrent subflows. It considers feedback from the receiver to change the estimation of packets on the master subflow. Dynamic path characteristics are considered. Modeling time of master subflow is estimated. Estimation is improved by error offset	Algorithm considers packet losses and path characteristics (RTT, cwnd). Receiver feedback is considered for proper packet flows	Small probabilities are neglected thus retransmission packets and packets after timeout are not considered

intelligence for packet scheduling on different subflows also they do not consider various path losses and different environmental conditions. Using more intelligence and machine learning module, path scheduling can be studied in more better way.

References

1. Allman M, Kruse H, Ostermann S (1996) An application-level solution to TCP's satellite inefficiencies. In: Proceedings of the first international workshop on satellite-based information services (WOSBIS), (XFTP)
2. Duke M et al (2006) RFC 4614: a roadmap for transmission control protocol (TCP) specification documents. IETF Internet Standard
3. Stewart R (2007) Stream control transmission protocol. No. RFC 4960
4. Abd A, Saadawi T, Lee M (2004) LS-SCTP: a bandwidth aggregation technique for stream control transmission protocol. Comput Commun 27(10):1012–1024
5. Amer PD, Ekiz N, Natarajan P, Becke M, Tuexen M, Dreibholz T, Stewart RR, Iyengar J (2019) Load sharing for the stream control transmission protocol (SCTP)
6. Baldini A, De Carli L, Risso F (2009) Increasing performances of TCP data transfers through multiple parallel connections. In: 2009 ieee symposium on computers and communications. IEEE 2009
7. Bonaventure R et al (2012) An overview of multipath TCP. Login 37(5):17
8. Nikravesh A et al (2016) An in-depth understanding of multipath TCP on mobile devices: measurement and system design. In: Proceedings of the 22nd annual international conference on mobile computing and networking. ACM 2016
9. Ramaboli AL, Olabisi EF et al (2012) Bandwidth aggregation in heterogeneous wireless networks: a survey of current approaches and issues. J Netw Comput Appl 35(6):1674–1690 (TCP/IP packet scheduling)
10. Maxemchuk N (1975) Dispersity Routing in Store-and-Forward Networks
11. Huitema C (1995) Multi-homed TCP. Internet Draft IETF
12. Key P, Massoulié L, Towsley D (2006) Combining multipath routing and congestion control for robustness. In: Conference on information sciences and systems
13. Shakkottai S, Altman E, Kumar A (2006) The case for non-cooperative multihoming of users to access points in IEEE 802.11 WLANs. In: Proceedings IEEE INFOCOM 2006. 25TH IEEE international conference on computer communications. IEEE 2006
14. Casetti C, Gaiotto W (2004) Westwood SCTP: load balancing over multipaths using bandwidth-aware source scheduling. In: IEEE 60th vehicular technology conference 2004. IEEE, vol 4, VTC2004-Fall
15. Iyengar JR, Amer PD, Stewart R (2006) Concurrent multipath transfer using SCTP multihoming over independent end-to-end paths. IEEE/ACM Trans Netw 14(5):951–964
16. Liu J et al (2008) Rethinking retransmission policy in concurrent multipath transfer. In: 2008 International conference on intelligent information hiding and multimedia signal processing, (RTX-LCS), IEEE 2008
17. Abd A, Saadawi T, Lee M (2004) Improving throughput and reliability in mobile wireless networks via transport layer bandwidth aggregation. Comput Netw 46(5):635–649
18. Liao J, Wang J, Zhu X (2008) cmpSCTP: an extension of SCTP to support concurrent multi-path transfer. In: 2008 IEEE international conference on communications. IEEE 2008
19. Huang C-M, Tsai C-H (2007) WiMP-SCTP: multi-path transmission using stream control transmission protocol (SCTP) in wireless networks. In: 21st International conference on advanced information networking and applications workshops (AINAW'07), IEEE, vol 1
20. Hsieh H-Y, Sivakumar R (2002) pTCP: an end-to-end transport layer protocol for striped connections. In: 10th IEEE international conference on network protocols 2002. Proceedings IEEE

21. Chen J, Xu K, Gerla M (2004) Multipath TCP in lossy wireless environment. In: Proceedings of IFIP third annual Mediterranean ad hoc networking workshop (Med-Hoc-Net'04)
22. Sharma V et al (2008) MPLOT: a transport protocol exploiting multipath diversity using erasure codes. In: IEEE INFOCOM 2008-the 27th conference on computer communications. IEEE, 178
23. Raiciu C et al (2010) Data center networking with multipath TCP. In: Proceedings of the 9th ACM SIGCOMM workshop on hot topics in networks. ACM 2010
24. Raiciu C et al (2011) Improving datacenter performance and robustness with multipath TCP. ACM SIGCOMM Comput Commun Rev 41(4)
25. Lim Y-S et al (2014) Cross-layer path management in multi-path transport protocol for mobile devices. In: IEEE INFOCOM 2014-IEEE conference on computer communications. IEEE 2014
26. Van Der Pol R et al. (2012) Multipathing with MPTCP and OpenFlow. In: 2012 SC companion: high performance computing, networking storage and analysis. IEEE 2012
27. Hwang J, Joon Y (2015) Packet scheduling for multipath TCP. In: 2015 Seventh international conference on Ubiquitous and future networks. IEEE 2015
28. Corbillon X et al (2016) Cross-layer scheduler for video streaming over MPTCP. In: Proceedings of the 7th international conference on multimedia systems. ACM 2016
29. Allman M, Paxson V, Stevens W (1999) TCP Congestion control IETF RFC 2581, (TCP NewReno)
30. Matsufuji R et al (2017) Multipath TCP path schedulers for streaming video. In: 2017 IEEE Pacific Rim conference on communications, computers and signal processing (PACRIM). IEEE 2017
31. Polese M et al (2018) A survey on recent advances in transport layer protocols. In: arXiv preprint arXiv:1810.03884
32. Hasegawa Y et al (2005) Improved data distribution for multipath TCP communication. GLOBECOM'05 IEEE Global Telecommun Conf 1:5
33. Mirani FH, Boukhatem N, Tran MA (2010) A data-scheduling mechanism for multi-homed mobile terminals with disparate link latencies. In: 2010 IEEE 72nd vehicular technology conference-fall. IEEE 2010
34. Park J-W, Karrer RP, Kim J (2011) TCP-ROME: a transport-layer parallel streaming protocol for real-time online multimedia environments. J Commun Netw 13(3):277–285
35. Nunes BAA et al (2011) A machine learning approach to end-to-end RTT estimation and its application to tcp. In: 2011 Proceedings of 20th international conference on computer communications and networks (ICCCN). IEEE 2011
36. Yang F, Wang Q, Amer PD (2014) Out-of-order transmission for in-order arrival scheduling for multipath TCP. In: 2014 28th International conference on advanced information networking and applications workshops. IEEE 2014
37. Ni D et al (2014) Fine-grained forward prediction based dynamic packet scheduling mechanism for multipath TCP in lossy networks. In: 2014 23rd International conference on computer communication and networks (ICCCN). IEEE 2014
38. Bhat PA, Talmale G (2014) MPTCP combining congestion window adaptation and packet scheduling for multi-homed device. In: International conference for convergence for technology. IEEE 2014
39. Ni D et al (2015) OCPS: Offset compensation based packet scheduling mechanism for multipath TCP. In: 2015 IEEE international conference on communications (ICC). IEEE 2015
40. Wu J et al (2016) Streaming high-quality mobile video with multipath TCP in heterogeneous wireless networks. IEEE Trans Mob Comput 15(9):2345–2361
41. Popat KJ, Raval JA, Johnson S et al (2015) An efficient scheduling scheme of multipath TCP for MPI. Int J Sci Eng Technol Res (IJSETR) 4(6):2123–2126
42. Rene S et al (2015) Multipath TCP architecture for infotainment multimedia applications in vehicular networks. In: 2015 IEEE 81st vehicular technology conference (VTC Spring). IEEE 2015
43. Saputra Y et al (2017) E-MICE: energy-efficient concurrent exploitation of multiple Wi-Fi radios. IEEE Trans Mob Comput 16(7):1870–1880

44. Kim H, Choi S (2016) The effect of routing path buffer size on throughput of multipath TCP. In: 2016 International conference on information and communication technology convergence (ICTC). IEEE 2016
45. Lim Y-S et al ECF: an MPTCP path scheduler to manage heterogeneous paths. In: Proceedings of the 13th international conference on emerging networking experiments and technologies. ACM 2017
46. Frömmgen A et al (2017) A programming model for application-defined multipath TCP scheduling. In: Proceedings of the 18th ACM/IFIP/USENIX Middleware conference. ACM 2017
47. Chung J et al (2017) Machine learning based path management for mobile devices over MPTCP. In: 2017 IEEE international conference on big data and smart computing (BigComp). IEEE 2017
48. Xue K et al (2018) DPSAF: forward prediction based dynamic packet scheduling and adjusting with feedback for multipath TCP in lossy heterogeneous networks. IEEE Trans Veh Technol 67(2):1521–1534
49. Ferlin S et al (2018) MPTCP Meets FEC: supporting latency-sensitive applications over heterogeneous networks. IEEE/ACM Trans Netw (TON) 26(5):2005–2018

Voice Controlled Home Automation Using Blynk, IFTTT with Live Feedback

M. Rajasekhar Reddy, P. Sai Siddartha Reddy, Suthapalli Akhil Sri Harsha and D. Vishnu Vashista

Abstract As people life becomes easier, people are habituated to the comforts in order to meet their needs. One such invention is home automation. This area has many opportunities which are emerging every day. The proposed technique will give home automation with a cost-effective implementation. We can automate the lights, fans, refrigerator, etc. The requirements are NodeMcu, relay module, smartphone with Blynk and IFTTT apps, and proper Wi-Fi source.

Keywords Home automation · IFTTT · Blynk · IoT · Analog extender · NodeMcu

1 Introduction

IoT is one of the latest technologies emerging in the modern world [1, 2]. The recent development on the Internet creates many opportunities for people to come up with new ideas. One such idea is the home automation. There are several such automation techniques where people require more and easier ways to use it in their day-to-day life. In order to bring comfort to the user, the Google Assistant is used as a translator. Google Assistant is integrated with the circuit by using the If This Then That (IFTTT), and it acts as the intermediate platform.

M. Rajasekhar Reddy (✉) · P. Sai Siddartha Reddy
School of Computing, SASTRA Deemed to Be University, Thanjavur, India
e-mail: rajasekharmanyam04@gmail.com

P. Sai Siddartha Reddy
e-mail: siddusiddartha1999@gmail.com

S. Akhil Sri Harsha · D. Vishnu Vashista
School of Electrical and Electronics Engineering, SASTRA Deemed to Be University, Thanjavur, India
e-mail: akhilsuthapalli@gmail.com

D. Vishnu Vashista
e-mail: vishnuvasista99@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_58

The proposed system will purely come under the Internet of Things (IoT), in which the different modules (such as lights, fans, refrigerators, etc., with the smartphones) can be connected.

The overview of the paper is as follows: Sect. 2 describes the prerequisites. Section 3 describes the past and present existing techniques which are being used. Section 4 explains the proposed method with complete analysis. Section 5 describes the results and analysis. Section 6 concludes this paper.

2 Related Work

2.1 NodeMcu

It is an open-source platform which is mainly used for IoT. It has a Soc ESP8266 manufactured by Espressif Systems [3]. The main features of NodeMcu are it's an open source and Wi-Fi enabled. The term MCU stands for microcontroller unit on a single chip. It has many processors along with memory and several programmable input/output pins. These i/o pins also called as general purpose input/output (GPIO) are used to interface many sensors and other electronic modules to achieve a particular task. The code is created in Arduino IDE with pre-installed libraries. Later that code is compiled and uploaded to the NodeMcu. NodeMcu has the following specifications:

- Maximum output voltage: 3.3 V.
- Wi-Fi Direct (P2P), soft-AP.
- Analog to digital: one input with 1024 step resolution.
- Built-in USB connector (Fig. 1).

2.2 Relay Module

A relay is an electromagnetic switch which can turn ON/OFF a much larger electric current when a relatively small current is applied to its terminals [5]. The main working component of a relay is an electromagnet, which is a coil of wire that excites and creates a temporary magnetic field when current is passed.

The following are the specifications of a relay module in Fig. 2.

- High-voltage side current 10 A and 250 V AC or 30 V DC.
- Source voltage 5–12 V.
- For each channel, the control signal is 3–5 V.
- For each channel 1- normally open, 1-normally closed and 1-common.

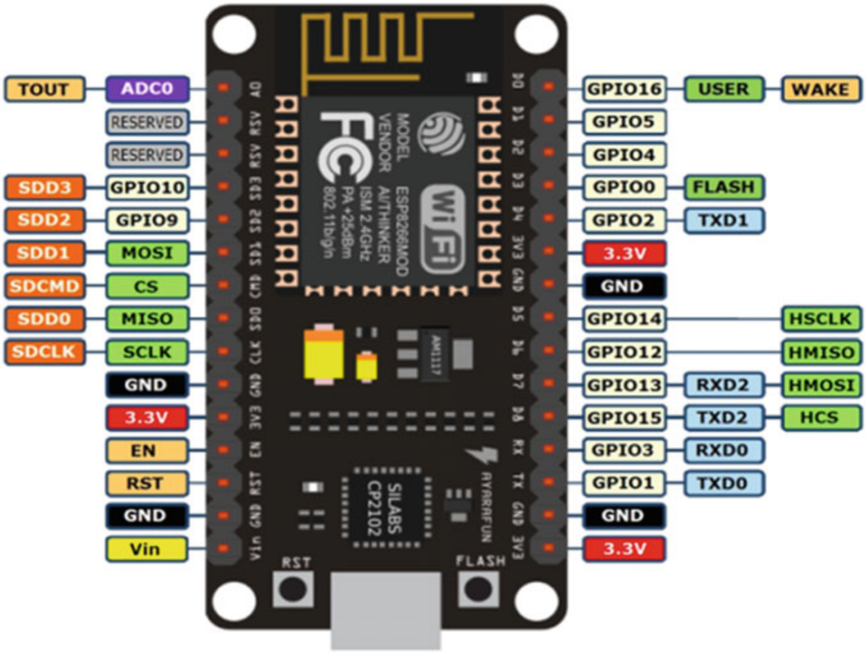
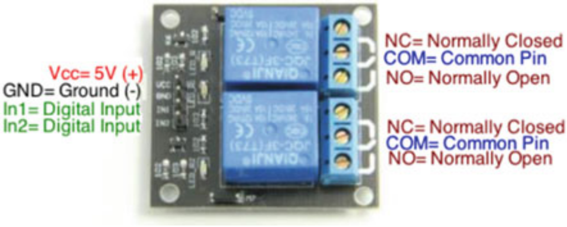


Fig. 1 Pin configuration of NodeMcu [4]

Fig. 2 Relay module [6]

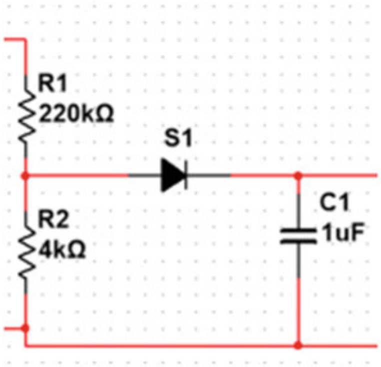


2.3 Sensing Circuit

The sensing circuit works as a feedback circuit wherein the power status of the appliances connected to the relay is detected. The circuit mainly consists of a potential divider along with a diode and a capacitor as shown in Fig. 3.

Working. The input to the circuit is a 230 V AC supply wherein the drop across the 4Kohm is brought nearly to 5 V AC which is passed through a diode and a capacitor so as to generate voltage level of 5 V which is passed to the analog input of NodeMcu. A high-level voltage indicates switch ON condition of the appliance. The NodeMcu is programmed in such a way that the data from analog input is processed and the notification of whether the device is ON or OFF.

Fig. 3 Sensing circuit



2.4 Analog Pin Extender (ADS1115)

The number of analog pins in NodeMcu is only one. In order to connect more devices, an external device must be used. ADS1115 acts as an analog pin extender increasing the number of analog pins on which NodeMcu can work to 4. ADS1115 performs communication with NodeMcu and transfer the data when triggered.

2.5 Blynk

Blynk is a platform with iOS and Android apps to control Arduino, Raspberry Pi, NodeMcu and many other devices over the Internet [7]. It is a digital dashboard where you can build a graphic interface for your project by simply dragging and dropping widgets. For android mobiles, it is available in Google Play Store. The auth_token generated gives the user, protection from others controlling the NodeMcu. In the project window, we are given with a toolbox where we can add several widgets like buttons, terminal, value display, notification, etc. Upon adding the required widgets, the user needs to configure the respective widget as to which pin of NodeMcu is to be controlled using that widget. There is a play button which starts the communication between Blynk and NodeMcu. And the operation can be stopped by clicking a rectangular stop box on top.

2.6 IFTTT

'If This Then That' (IFTTT) is a free web-based service to create chains of simple conditional statements, called *applets* [8]. An applet is triggered by changes that occur within other web services such as Gmail, Facebook, Instagram, Google Assistant, etc. In this paper, Google Assistant accesses the Blynk cloud. Since Blynk has no web service associated with it, webhooks are used with the IP address of Blynk followed with a particular auth_token.

3 Existing Techniques

3.1 Past Techniques

Bluetooth. Android apps are used to send data via Bluetooth, and the received data is analyzed in Arduino which responses accordingly. Those apps could be created using various app development software like MIT app inventor, Android studio, etc. The drawbacks are limited range and sync rate [9].

ZigBee. The above problem is overtaken if we use ZigBee for long range and it has its own limitations as it could not provide access worldwide [10].

DTMF. In 'Dual Tone Multi-Frequency' the numbers can be sent from one device to other over a phone call. On receiving the digit, pressed the decoder detects the frequency of the digit and sends relative signals to control devices.

3.2 Present Techniques

Privatization. Many companies are now developing their own software and controller circuits to control home appliances. This technique is costly.

Blynk. It is a cloud service provided by Blynk. The microcontroller is connected to its server with a unique auth code. It has features like GPS, notification alert, live data transmission, etc. The code needed reduces enormously.

IoT. The data can be trans-received worldwide and can be used in various places which have Internet access using IoT [11]. The rapid growth in IoT is due to the in-hand operation, reliability, extendability, and connecting a range of devices.

4 Proposed Technique

Keeping the circuit ready, this cost-effective technique provides a solution to home appliances control, fetching data from Blynk app as well as from various platforms. To work with those platforms, a service connector known as IFTTT integrates to perform various actions when triggered. IFTTT, Blynk, and Google Assistant are integrated such that IFTTT gets data from Google Assistant and sends to Blynk cloud. The Blynk server transmits data to NodeMcu. Then, microcontroller controls various appliances connected to it via a relay module. A sensing circuit is adopted which

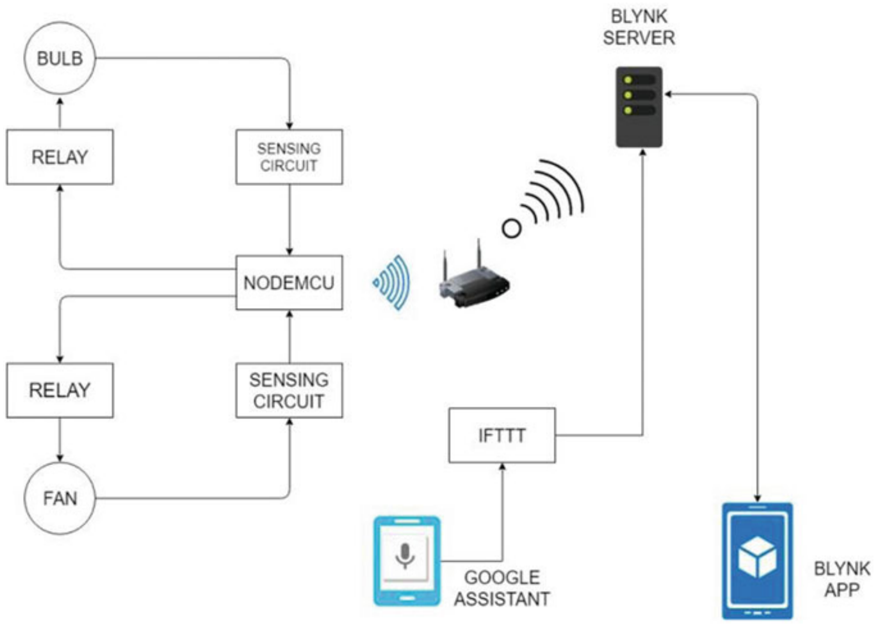


Fig. 4 Overall architecture of the proposed method

basically detects the voltage applied, ensuring perfect feedback on the appliance status. The overall architecture of the proposed method is shown in Fig. 4. The procedure can be written as an algorithm.

Algorithm: Home_Automation()

1. Install Arduino software with NodeMcu, Blynk, ADS1115 libraries in laptop
2. Install Blynk app in the smartphone

    2.1. Select new project and set it to NodeMcu
    2.2. Burn the code (Sect. 4.1) with network credentials and auth_token

3. Create an IFTTT account

    3.1. Create a new applet inside IFTTT as specified.
        3.2. Connect Google Assistant with Blynk server.

4. Connect the relay and sensing circuit as shown in Fig. 4.
5. Place an internet hotspot access point.

    1. Create a new applet inside IFTTT as specified.
    2. Connect Google Assistant with Blynk server.

End Home_Automation

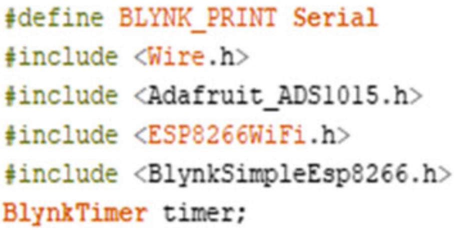
This work is split into five steps to set up the automation. They are as follows:

(a) software code (b) Blynk app configuration (c) IFTTT setup (d) hardware (e) simulation of the sensing circuit.

4.1 Software Code

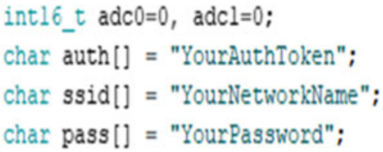
The programming is done in Arduino IDE Software, which is an open-source application. In Fig. 5, the necessary packages which are required for a NodeMcu to connect with the Blynk server [12] and the analog extender ADS1115 are included. The credential details of the internet hotspot device along with the auth_token are declared (as shown in Fig. 6) to connect the NodeMcu to the hotspot. Declare a function called 'powerstatus()' (as shown in Fig. 7), which gives the current status of the device (ON/OFF). In the 'setup(),' serial monitor is used for debugging. Declare D_0, D_1 pins on the NodeMcu board as output pins. D_0, D_1 are referred to 16, 5 which are Arduino equivalent. Set a timer object which runs the block 'myTimerEvent()' for every second and initiate the Blynk connection. Figure 8 gives the setup details. Virtual pins V_1, V_2 are used to control D_0, D_1 respectively as shown in Fig. 9. The 'loop()' block which runs infinitely, starts Blynk as well as a function 'powerstatus()' is called, which senses the present state of the device using the sensing circuit, as shown in Fig. 10.

Fig. 5 Packages

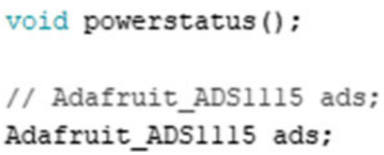


```
#define BLYNK_PRINT Serial
#include <Wire.h>
#include <Adafruit_ADS1015.h>
#include <ESP8266WiFi.h>
#include <BlynkSimpleEsp8266.h>
BlynkTimer timer;
```

Fig. 6 Credential declarations

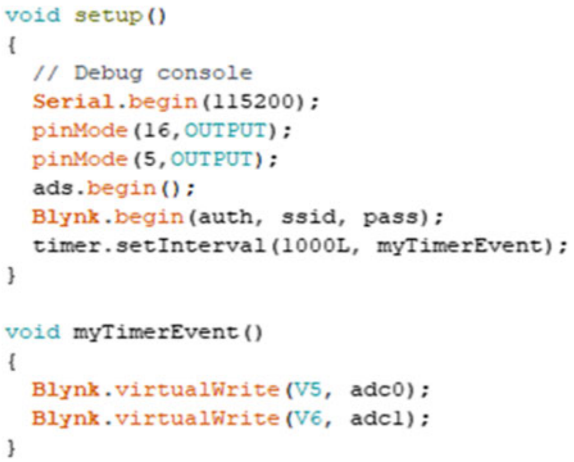


```
int16_t adc0=0, adc1=0;
char auth[] = "YourAuthToken";
char ssid[] = "YourNetworkName";
char pass[] = "YourPassword";
```



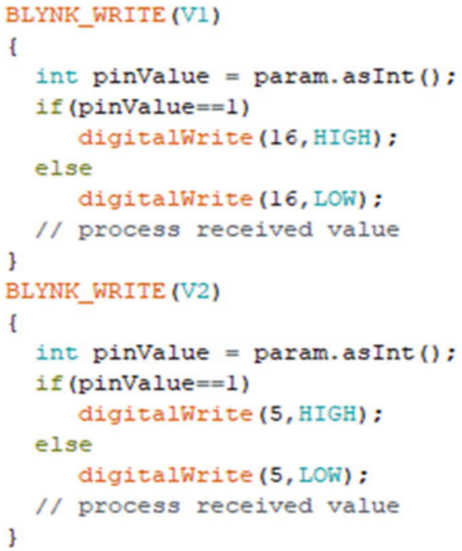
```
void powerstatus();

// Adafruit_ADS1115 ads;
Adafruit_ADS1115 ads;
```

Fig. 7 Power status



```
void setup()
{
  // Debug console
  Serial.begin(115200);
  pinMode(16,OUTPUT);
  pinMode(5,OUTPUT);
  ads.begin();
  Blynk.begin(auth, ssid, pass);
  timer.setInterval(1000L, myTimerEvent);
}

void myTimerEvent()
{
  Blynk.virtualWrite(V5, adc0);
  Blynk.virtualWrite(V6, adc1);
}
```

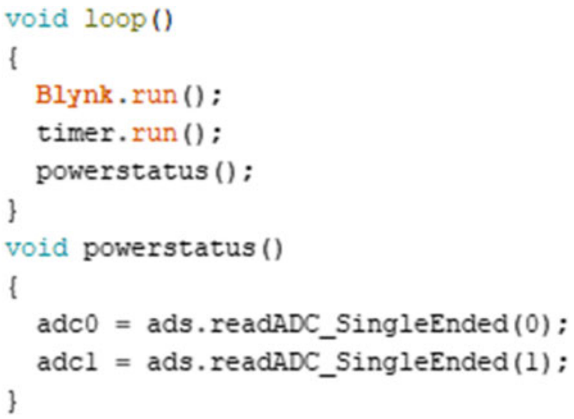
Fig. 8 Setup



```
BLYNK_WRITE(V1)
{
  int pinValue = param.asInt();
  if(pinValue==1)
     digitalWrite(16,HIGH);
  else
     digitalWrite(16,LOW);
  // process received value
}
BLYNK_WRITE(V2)
{
  int pinValue = param.asInt();
  if(pinValue==1)
     digitalWrite(5,HIGH);
  else
     digitalWrite(5,LOW);
  // process received value
}
```

Fig. 9 Assigning virtual pins

Fig. 10 Loop



```
void loop()
{
  Blynk.run();
  timer.run();
  powerstatus();
}
void powerstatus()
{
  adc0 = ads.readADC_SingleEnded(0);
  adc1 = ads.readADC_SingleEnded(1);
}
```

4.2 Blynk Configuration

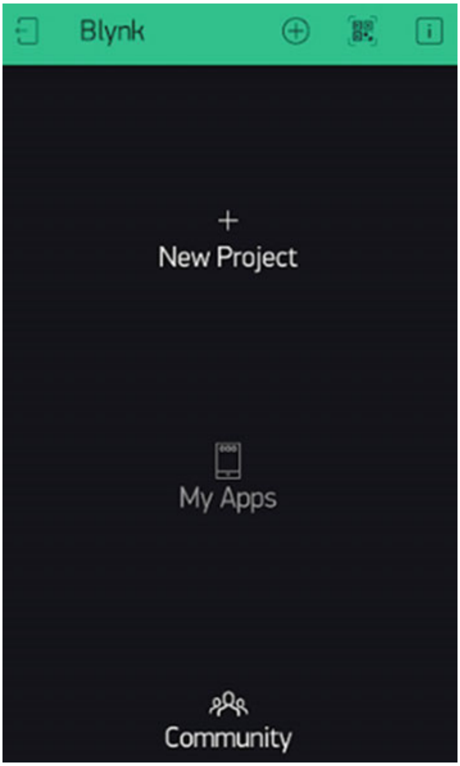
1. Create an account in Blynk using Google or Facebook.
2. Click on NEW PROJECT option as shown in Fig. 11.
3. Given the project title and select the device in the ‘choose device’ option as per requirement. The screenshot is in Fig. 12.
4. Auth token is generated and will be sent to your Gmail.
5. A dashboard having 2000 energy points will be provided.
6. The required components are dragged and dropped on the workspace and are configured as shown in Fig. 13.

4.3 IFTTT Setup

Working Algorithm:

1. Login into the IFTTT using Gmail credentials, and grant access to it.
2. Go to MY APPLET and create a new applet.
3. Click on ‘+this’ button and select the web service as Google Assistant.
4. Choose trigger as ‘say a phrase,’ fill trigger fields as shown in Fig. 14
5. After creating a trigger to turn on a device, click on ‘+that’ button.
6. Select the action service as ‘WEBHOOKS.’
7. Now make a web request as shown in Fig. 15.
8. Fill the URL field as ‘HTTP://188.166.206/Auth_token/update/pin.’
9. Choose the method as ‘PUT’ and content type as ‘application/json.’
10. Fill the body as [“1”] and click on create action.
11. Click on the finish button to finish the applet creation.
12. Create various applets for ON/OFF of different appliances separately.

Fig. 11 Start-up screen



4.4 Hardware

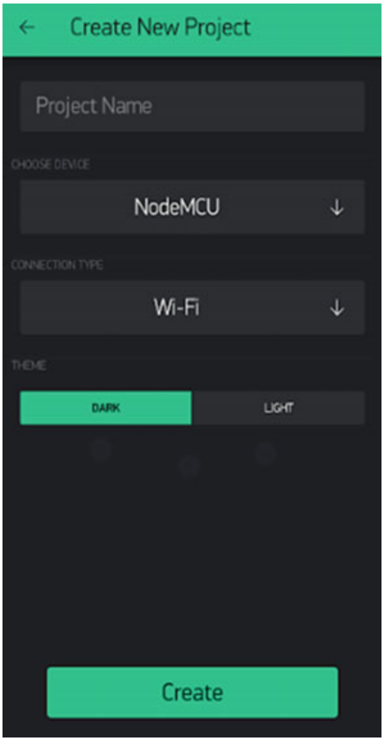
The hardware components, pin configuration, and specifications are explained in Sect. 2. The connections are made to integrate NodeMcu, relay module, sensing circuit. The connections are shown in Fig. 16.

4.5 Simulation of Sensing Circuit

See Fig. 17.

WORKING. Now when we say a particular frame of the sentence to Google Assistant, it will pass on the information to IFTTT and the latter will perform the action of updating the Blynk cloud with specified data. The updated data is received by the NodeMcu and performs the actions.

Fig. 12 New project



CHOOSE DEVICE: NodeMCU

CONNECTION TYPE: Wi-Fi

THEME: DARK

5 Results

Using the proposed method, the accessibility is increased and the person operating this need not be in the specific or region bounded. The proposed method costs very less when compared to other techniques [13]. The cost of components used in the proposed method is listed in Table 1.

6 Conclusion

The proposed method is cost-effective for home automation with easy maintenance and security. Home automation remains as a growing field in twenty-first century. This paper aims at providing people an easier access for operating the devices at home from any part of the world at a very low cost.

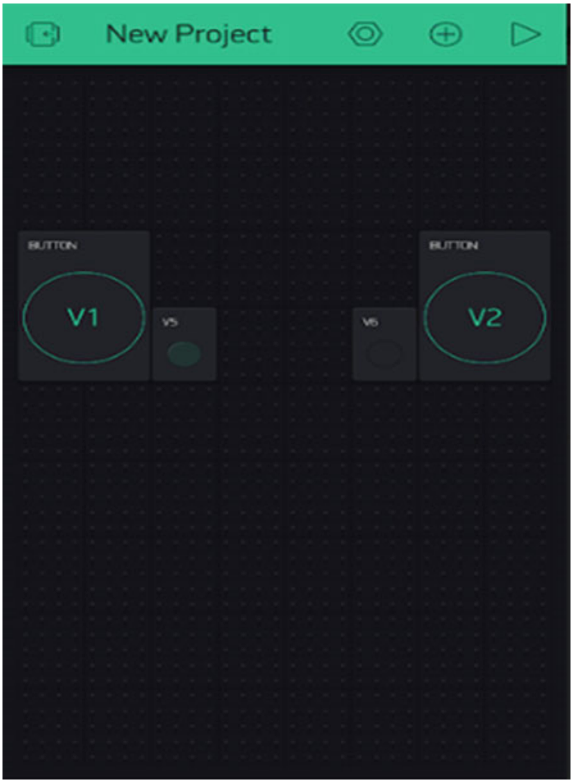
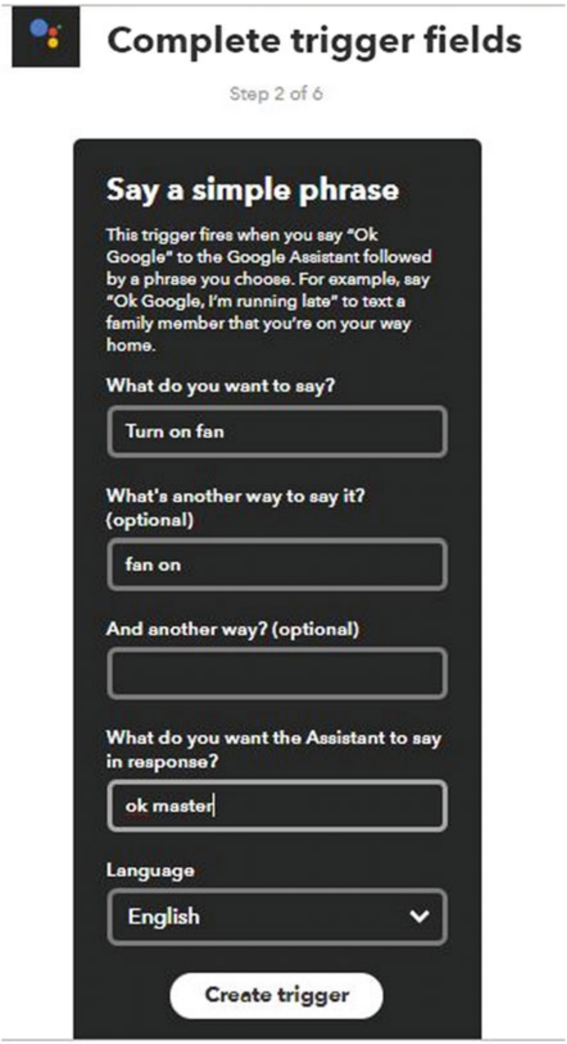


Fig. 13 Workspace

Fig. 14 Trigger creation



Complete trigger fields

Step 2 of 6

Say a simple phrase

This trigger fires when you say "Ok Google" to the Google Assistant followed by a phrase you choose. For example, say "Ok Google, I'm running late" to text a family member that you're on your way home.

What do you want to say?

Turn on fan

What's another way to say it? (optional)

fan on

And another way? (optional)

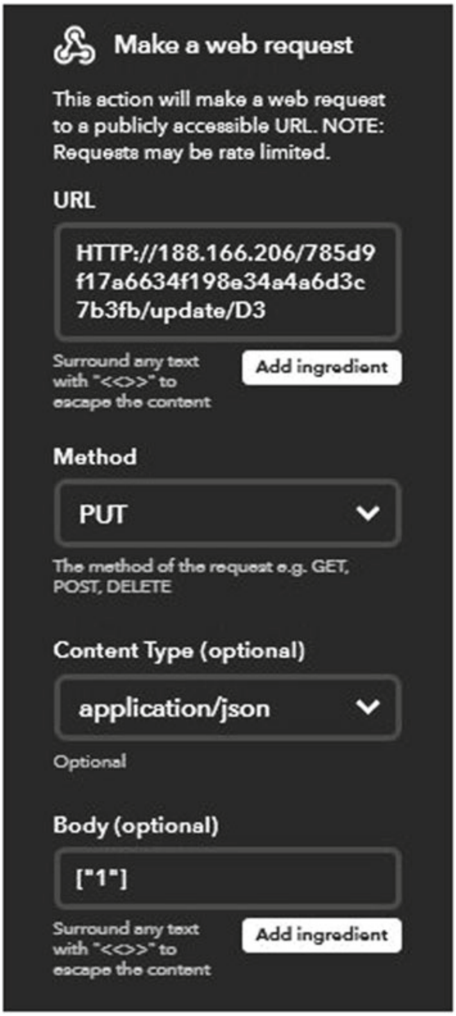
What do you want the Assistant to say in response?

ok master

Language

English

Fig. 15 Making a web request



Make a web request

This action will make a web request to a publicly accessible URL. NOTE: Requests may be rate limited.

URL

HTTP://188.166.206/785d9f17a6634f198e34a4a6d3c7b3fb/update/D3

Surround any text with "<<>>" to escape the content

Method

PUT

The method of the request e.g. GET, POST, DELETE

Content Type (optional)

application/json

Optional

Body (optional)

["1"]

Surround any text with "<<>>" to escape the content

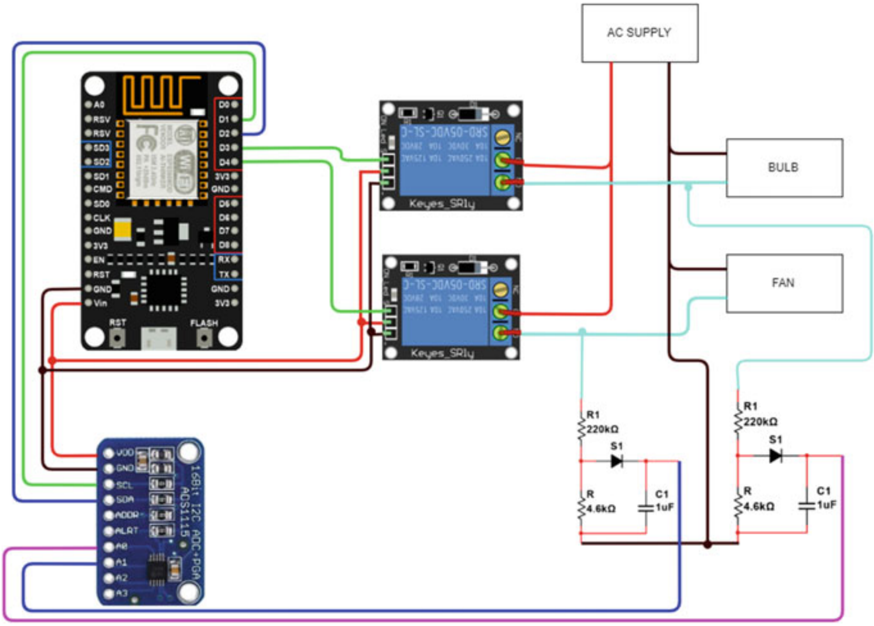
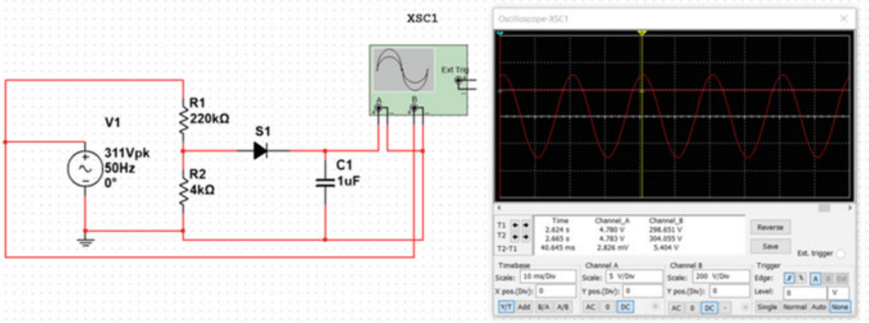


Fig. 16 Circuit



```
      Time        Channel_A    Channel_B
T1    2.624 s     4.780 V      298.651 V
T2    2.665 s     4.783 V      304.055 V
T2-T1 40.645 ms   2.826 mV     5.404 V

Timebase                Channel A               Channel B               Trigger
Scale: 10 ms/Div        Scale: 5 V/Div          Scale: 200 V/Div        Level: 0 V
X pos.(Div): 0          Y pos.(Div): 0          Y pos.(Div): 0
```

Fig. 17 Sensing circuit simulation

Table 1 Cost of components used in the proposed method

S. No.	Components	Cost
1	NodeMcu	Rs. 350
2	Relay	Rs. 180
3	Analog input extender	Rs. 450
4	Blynk and IFTTT apps	Rs. 0
	Total	Rs. 980

References

1. Singh H, Pallagani V, Khandelwal V, Venkanna U (2018) IoT based smart home automation system using sensor node. In: 4th international conference on Recent Advances in Information Technology (RAIT) IEEE
2. Lee Y, Jiang J; Underwood G; Sanders A, Osborne M (2017) Smart power-strip: home automation by bringing outlets into the IoT. IEEE
3. Taştana M, Gökozanb H (2018) An Internet of Things based air conditioning and lighting control system for smart home. Am Sci Res J Eng Technol Sci (ASRJETS) 50(1):181–189
4. https://iotbytes.wordpress.com/nodemcu-pinout/
5. Rout K, Mallick S, Mishra S (2018) Design and implementation of an Internet of Things based prototype for smart home automation system. Researchgate
6. https://sites.google.com/site/summerfuelrobots/arduino-sensor-tutorials
7. Durani H, Sheth M, Vaghasia M, Kotech S (2018) Smart automated home application using IoT with Blynk App. In: Second International Conference on Inventive Communication and Computational Technologies (ICICCT)
8. Vorapojpisut S (2015) A lightweight framework of home automation systems based on the IFTTT model. Researchgate
9. Mandula K, Parupalli R, Murty CHAS, Magesh E, Lunagariya R (2015) Mobile based home automation using Internet of Things (IoT). In: International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT) IEEE
10. Vivek GV, Sunil MP (2015) Enabling IOT services using WIFI—ZigBee gateway for a home automation system. In: IEEE International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)
11. Mohamed Imran M (2016, April) Intelligent home control and monitoring system via Internet. Int J Sci Dev Res (IJSDR). 1(4). ISSN: 2455-2631
12. Altabatabaie KF (2017) Remote automation system control using Arduino board. Researchgate
13. Alvarez J, Arturo A, Gutierrez S, Rodrigo PM, Lay-Ekuakille A (2018) A low-cost presence detection system for smart homes. In: International conference on Research in Intelligent and Computing in Engineering (RICE), IEEE

AD-LIB: Automated Library System

Dattatray Sawant and Rohan Patil

Abstract Automation is increasing rapidly, and intelligence in applications emerges as a new form of automation. The impact of automation is observed in the software, hardware, and machine layer. Due to automation, human intervention is reduced in a number of areas such as manufacturing, transport, utilities, defense, facilities, operations and lately, information technology. With this view in mind, we have developed library system for renewal and submission of books. To develop this system, we have used a microcontroller, a barcode scanner, and conveyor. First, we developed graphical user interface with MATLAB and then with LabVIEW for this system. Developed library system allows students to renew and submit in 24/7 basis.

Keywords Graphical user interface · Virtual instrument · Acquisition · Database · Barcode · Library management

1 Introduction

Robotization and innovation have turned out to be an aid for digital operations. It has made the human to work simpler. The developed system demonstrates the understudy subtitles, the book of the week; it additionally demonstrates the visual history of the understudy; it makes a database of the restoration and accommodation and furthermore contains a criticism area. The procedure begins with client entering one of a kind ID given to every client. When the client enters a substantial ID, the drove on the GUI turns green. On the off chance that the client enters an invalid ID, the drove will turn red. On the off chance that the ID entered is substantial, the photograph of the client will be shown alongside his/her different details shown,

D. Sawant (✉)
Department of Mechatronics Engineering, MPSTME, NMIMS University, Mumbai, India
e-mail: dattatray.sawant@nmims.edu

R. Patil
Automation Department, Jain Irrigation Systems Ltd., Jalgaon, India
e-mail: patil.rohandeepak@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_59

which are name, sexual orientation, degree, stream, year, age, and the name of the last book issued by him/her.

Once signed in, one can look over the numerous activities given and the one he wishes to do. He can check his issual history, present the book, re-establish the book, check the book of the week, or look for any book. On the off chance that the client taps on the issual history catch, he can check the quantity of books which he directly has issued on his name. The issual history demonstrates the quantities of books he has issued. It demonstrates all the book subtitles that are the Book ID, Title of the book, Publication Company, Name of the Author, Genre, and its time of distributing, ISBN no. also, the book version for each issued book. The following choice is present in the book.

On the off chance that the client needs to restore the book they obtained, they should examine the standardized tag given on the book by holding it under the constant standardized tag scanner. Once examined, they should press the submit catch. At the point when the catch is squeezed, the transport line framework turns on, and the belt activates. The book goes to the opposite side and falls into a book holding holder. On the off chance that the client re-establishes the book, they should filter the book by holding it under the standardized tag scanner. When the book is examined snap on the re-establish catch. The date will be reached out by a week or the quantity of days indicated by the library as per its framework. The book of the week catch will show the image of the book of the present week. This book changes each week and should be refreshed by the curator physically.

Usually, librarian has to enter data manually in the system, and then give it back to the user while returning or re-issuing a book. During examination, there are long queues while returning of books. To overcome this problem, we developed library system where submission and re-issual of books are done automatically. The portal is a model of a system which can be introduced in libraries to automize the procedures with the goal that less time is taken for the accommodation and re-issual of books. The developed system primarily consists of three parts, viz. the GUI screen, the conveyor line, and the barcode identification scanner. It comprises of sensors and LEDs to show what activities are going on. With the help of sensor, barcode scanner gets activated. Every user will be issued a unique ID and password to sign in. After user signs in, detailed information about his library transactions will be displayed. The user may choose to either submit or renew the particular book. This procedure will along these lines lessen the time taken for the entire accommodation process. Likewise, supervision is not required for the task of these portals.

2 Related Work

Using pick and place robotic arm, the library management system is developed [1]. Anita et al. created robotization in library for transporting of books in faster manner [2]. Mobile robotics is introduced as a motivating platform in courses with the help of combination of LEGO NXT mobile robots with LabVIEW [3, 4]. By the use of an RGBD sensor, the pose of a known object is detected in the shelf using visual data [5]. Rahul Pol et al. designed and developed a low cost superior four degrees of freedom (DoF) robot ARM [6]. Modern database-driven Web applications are developed by ISIS family member [7]. Author [8] investigated the problems encountered during automation in two Nigerian university libraries. The significant improvement in service and use of library facilities are observed with the help of proposed library information system [9]. The mechanical and technical issues and problems were investigated while designing line follower robot [10]. In the paper [11], the library inventory management system (LIMS) is demonstrated using line following robot (LFR). Based on National Instruments LabVIEW controlled PXI RF hardware, Pavel and Rao [12] developed a UHF radio frequency identification tag test and measurement system.

2.1 Motivation and Scope

In the present scenario, the reader has to physically come to the library specifically to submit or renew the book; the librarian will then manually scan the barcode on the book. Once the computer receives the code on the screen, then the librarian will search for the excel sheet belonging to the SAP ID of the student. Since the information has to be typed by the librarian inside the excel sheet, there is a margin for the human error, as well as it is time-consuming since the supervisor has to check for the librarian's mistakes at the end of the day. Since all students get free from their lectures about the same time, there is a heavy rush, and the staff is under pressure to complete the process as soon as possible, which may lead to further errors. Due to long queue, it is very difficult for physically disabled user.

2.2 Salient Contribution

The idea of automated library is yet to be implemented in India. AD-LIB is an integration of microcontroller, Barcode Scanner, National Instruments LabVIEW.

- Strong acrylic sheet covering to withstand the shocks and simple encasing of the framework inside the wall.
- Black conveyor belt for easy scanning of the barcodes placed on the books.
- Secured Logging via a password-based GUI 24/7 without fail.
- Accessing and printing the database through Microsoft Excel Sheet. Arrangement of enrollment of new user at portal and additionally at the organizational work area.
- Unique barcode assigned to every book and each student. The barcodes are useful in calling out the functions from the spreadsheet database.

- National Instruments LabVIEW GUI for cost sparing and easy to understand user-friendly interactive system, LabVIEW is utilized for interfacing barcode scanner with the GUI.
- National Instruments VISA tool is used to establish the connection between Arduino and the GUI.

3 Methodology

Automation and technology have proven to be a boon for us. It has made human work easier. The portal which we have made aims at reducing the workload on the library staff by automating the renewal and submission process. Figure 1 shows the flow chart of the whole process of renewal and submission of books. It also has additional features, viz. It shows the student details, the book of the week, it also shows the issual history of the student, and it creates a database of the renewal and submission and also contains a feedback section. The process starts with the user entering the unique ID given to each user. Once the user enters a valid ID, the led on the GUI turns green. If the user enters an invalid ID, the led will turn red. If the ID entered is valid, the photo of the user will be displayed along with his/her other details which are name, gender, degree, stream, year, age, and the name of the last book issued by him/her. Once logged in, one can choose from the many actions given, the one he wishes to do. He can check his issual history, submit the book, renew the book, check the book of the week, or search for any book. If the user clicks on the issual history button, he can check the number of books which he presently has issued on his name. The issual history shows the numbers of books he has issued. It shows all the book details that are the Book ID, Title of the book, Publication Company, Name of the Author, Genre, its year of publishing, ISBN no., and the book edition for each issued book. The next option is submit the book.

If the user wants to return the book they borrowed, they will have to scan the barcode given on the book by keeping it under the continuous barcode scanner. Once scanned, they will have to press the submit button. When the button is pressed, the conveyor belt system turns on and the belt actuates. The book goes to the other side and falls into a book holding container. For renewal, user will have to scan the book by barcode scanner. After the successful scan, click on the renew button. The date will be extended by a week or the number of days specified by the library according to its system. The book of the week button will display the picture of the book of the current week. This book changes every week and needs to be updated by the librarian manually.

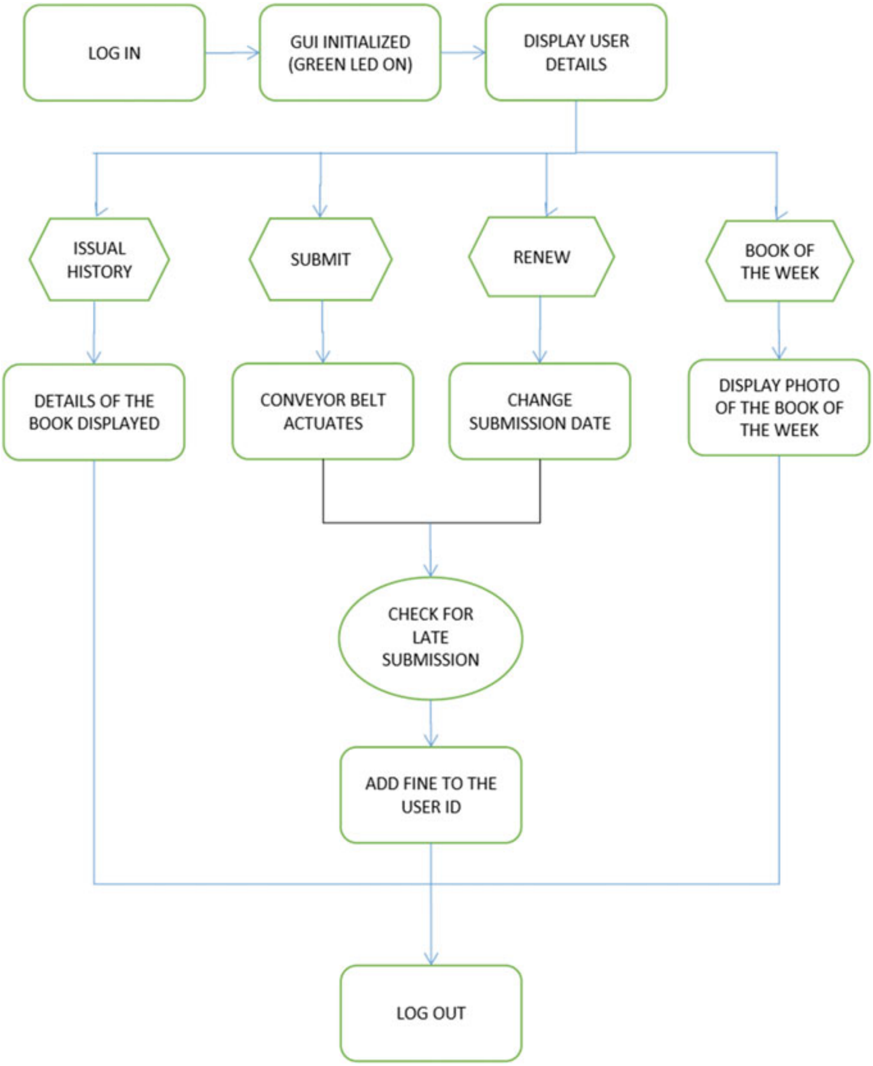


Fig. 1 Flowchart of AD-LIB

4 Softwares

The main purpose of AD-LIB is to carry out the library operations as desired by the user, so we require an intermediate platform that would take the inputs from the end-user, which in our case would be students, and these inputs would give specific commands to the controller. A Graphic User Interface (GUI) functions as the median platform, which has been designed and programmed to perform the functional requirements. The inputs given by the user would be captured via an event structure, initialized during mouse click.

A GUI has been the Centralized Unit of the System; it comes in handy while interfacing microcontroller, barcode scanner, database (spreadsheets), Arduino UNO so that the user can trace back the problem or the run-time errors when the system breaks down. The GUI build up was initially started on MATLAB, but later, it was shifted to LabVIEW as the LabVIEW programming has a specific architecture in the form of state machines. We found the MATLAB programming a little sturdy and rectifying error consumed lot of time.

LabVIEW comes as an alternative for Supervisory Control and Data Acquisition (SCADA), so getting hands on experience on LabVIEW for future aspects was a good start for any Mechatronics Engineer. Whereas, having a little knowledge of MATLAB programming made us aware of the application development protocols. Overall, all the interfacing with the different components made us aware of the real-time working of the subsystems from a single centralized unit that supervises the decision and control of the modules attached to it.

4.1 MATLAB Guide

As we can see in Fig. 2, the initial GUI contained combinations of Push Buttons, a Header Text Box, and an ACTIVE X control developed by the Adobe Reader. You can likewise code the format and conduct of your application total utilizing MATLAB capacities.

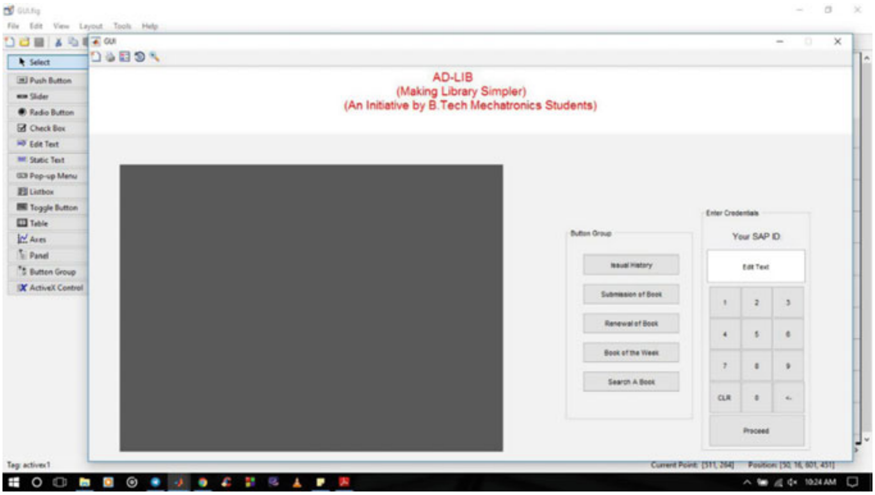
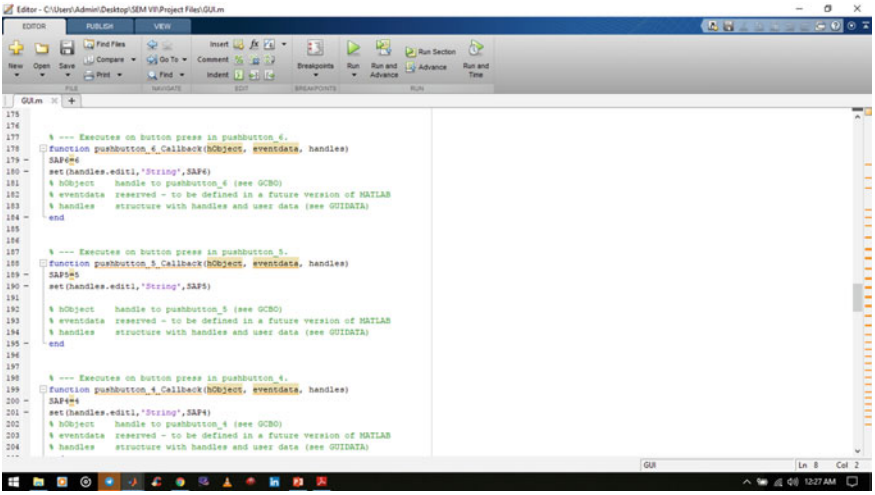


Fig. 2 Initial MATLAB GUIDE screen



```
% --- Executes on button press in pushbutton_6.
function pushbutton_6_Callback(hObject, eventdata, handles)
SAP6=6
set(handles.edit1,'String',SAP6)
% hObject    handle to pushbutton_6 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
end


% --- Executes on button press in pushbutton_5.
function pushbutton_5_Callback(hObject, eventdata, handles)
SAP5=5
set(handles.edit1,'String',SAP5)

% hObject    handle to pushbutton_5 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
end


% --- Executes on button press in pushbutton_4.
function pushbutton_4_Callback(hObject, eventdata, handles)
SAP4=4
set(handles.edit1,'String',SAP4)
% hObject    handle to pushbutton_4 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
```

Fig. 3 MATLAB GUI algorithm

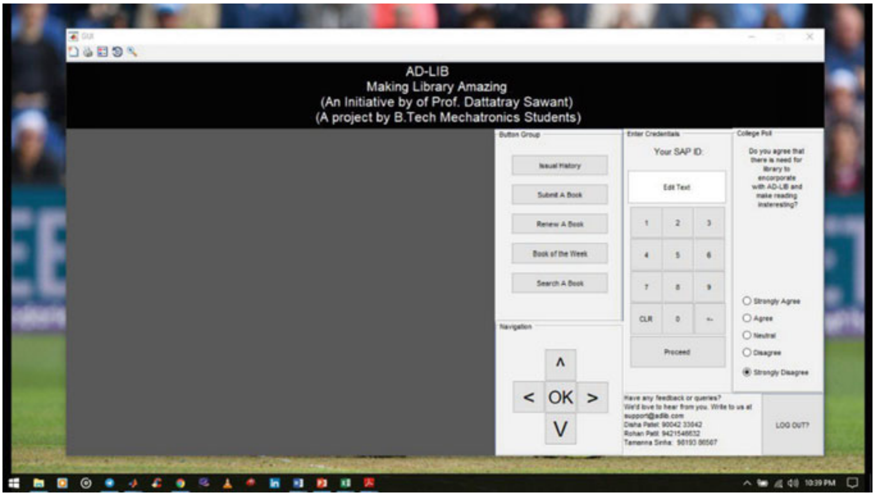
In this approach, you make a customary figure and place intuitive parts in that figure automatically. These applications bolster similar kinds of designs and intelligent parts that GUIDE underpins, and also selected boards. Utilize this way to deal with manufacture complex applications with numerous reliant parts that can show any kind of plot.

Every time there is a mouse click event on any one of the push buttons placed on the GUI screen, it generates a variable value assigned to the function named as event data. Therefore, upon a clicking, an event is called out of particular function name to which the push button has been added. An insight of the working algorithm has been shown in Fig. 3. If a user clicks on push button 4, a function named push button 4 call-back function is called, and its event data is then transfered to the edit text (set (handles.edit1, String, SAP4)) window above to show which push button has been pressed. Radio Buttons, Navigation Panel, and User Feedback had been added to the final GUI on MATLAB GUIDE as shown in Fig. 4.

4.2 National Instruments LabVIEW

LabVIEW structures are called virtual instruments in light of the fact that their appearance and activity mimic physical instruments, for example, oscilloscopes and multimeters. LabVIEW contains an extensive arrangement of devices for securing, breaking down, showing, and putting away information and also devices to enable you to investigate code you compose.

In LabVIEW, you fabricate a VI, or front panel, with controls and markers. Controls are handles, push buttons, dials, and other information systems. Pointers are



AD-LIB
Making Library Amazing
(An Initiative by of Prof. Dattatray Sawant)
(A project by B.Tech Mechatronics Students)

Do you agree that there is need for library to encorporate with AD-LIB and make reading insteresting?

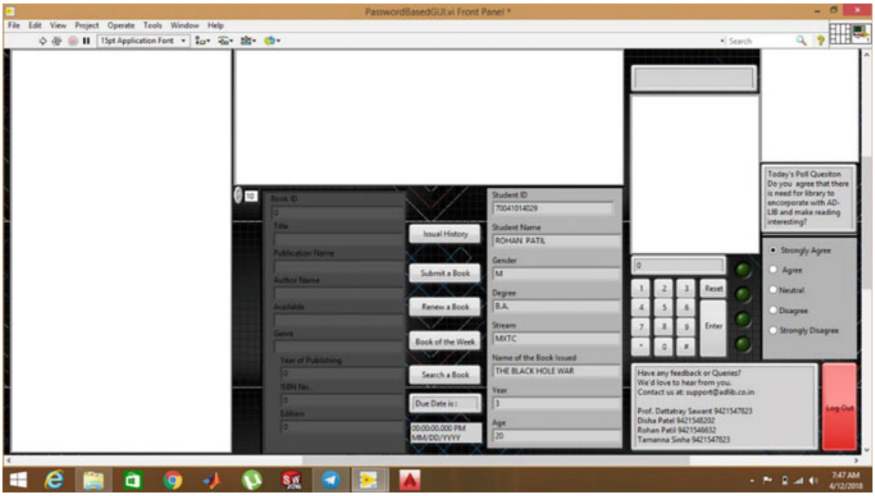
○ Strongly Agree
○ Agree
○ Neutral
○ Disagree
● Strongly Disagree

Have any feedback or queries?
We'd love to hear from you. Write to us at support@adlib.com
Disha Patel: 90042 33042
Rohan Patil: 9421546632
Tamanna Sinha: 98193 86587

Fig. 4 Final MATLAB GUI

charts, LEDs, and other yield shows. After you construct the front pane as shown in Fig. 5, you include code utilizing VIs and structures to control the front panel objects. The square chart contains this code.

One advantage of LabVIEW over other advancement situations is the broad help for getting to instrumentation equipment. Drivers for a wide range of sorts of instruments such as ARDUINO, Barcode Scanners, DAQs, Motors, and LEDs are accessible for consideration. These present themselves as graphical hubs.



Book ID: 0
Title:
Publication Name:
Author Name:
Available:
Genre:
Year of Publishing: 0
ISBN No.: 0
Edition: 0

Student ID: 70041014029
Student Name: ROHAN PATIL
Gender: M
Degree: B.A.
Stream: MXTC
Name of the Book Issued: THE BLACK HOLE WAR
Year: 3
Age: 20

Due Date is :
00:00:00.000 PM
MM/DD/YYYY

Today's Poll Quesiton
Do you agree that there is need for library to encorporate with AD-LIB and make reading interesting?

● Strongly Agree
○ Agree
○ Neutral
○ Disagree
○ Strongly Disagree

Have any feedback or Queries?
We'd love to hear from you.
Contact us at: support@adlib.co.in

Prof. Dattatray Sawant 9421547823
Disha Patel 9421548202
Rohan Patil 9421546632
Tamanna Sinha 9421547823

Fig. 5 Front panel of AD-IB screen in LabVIEW

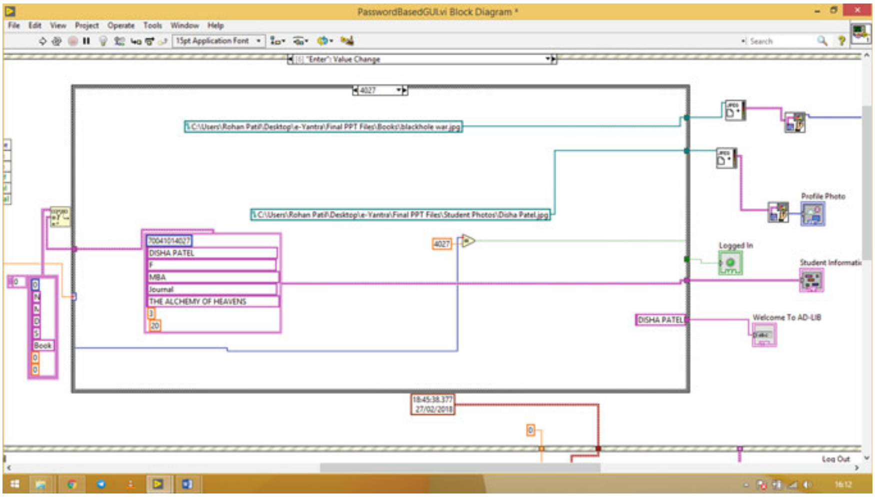

PasswordBasedGUI.vi Block Diagram *
File Edit View Project Operate Tools Window Help
15pt Application Font
Search
[6] "Enter": Value Change
4027
\C:\Users\Rohan Patil\Desktop\e-Yantra\Final PPT Files\Books\blackhole war.jpg
\C:\Users\Rohan Patil\Desktop\e-Yantra\Final PPT Files\Student Photos\Disha Patel.jpg
70041014027
DISHA PATEL
F
MBA
Journal
THE ALCHEMY OF HEAVENS
3
20
4027
0
N
N
O
S
Book
0
0
Profile Photo
Logged In
Student Informati
DISHA PATEL
Welcome To AD-LIB
18:45:38.377
27/02/2018
0
Log Out
16:12

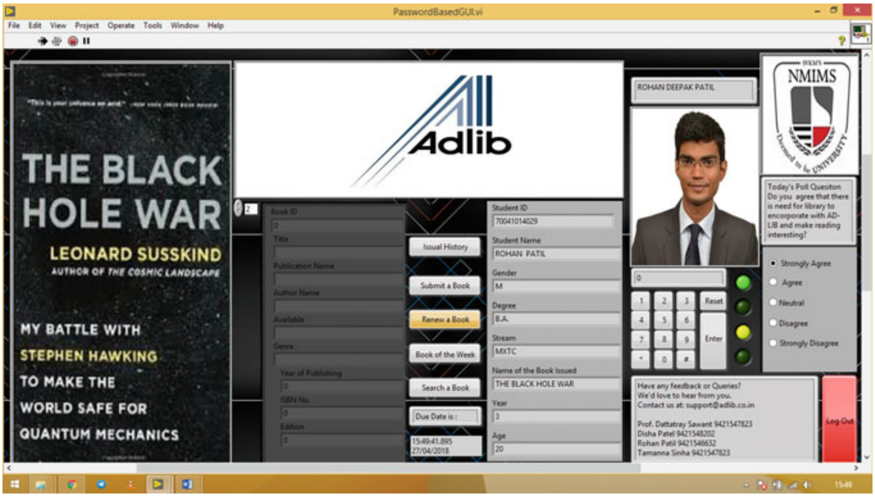
Fig. 6 Block diagram of the GUI in LabVIEW

Once we had created the front panel, we moved on to developing logic of the block diagram as shown in Fig. 6 which consists of the control of the front panel objects. The square outline contains this graphical source code. The terminals provide the information to the control after execution of the VI. The block diagram shows up as symbol or feed information to be written in the database (spreadsheet).

Terminals are passage and communication ports that trade data between the front board and block diagram. Upon initializing the inputs or providing events in the form of mouse clicks, the GUI performs tasks when a VI runs. The use of event structures monitors the execution of functions, .jpeg image reading, writing data to the excel sheets, and a communication channel between Arduino UNO and Front Panel Push Button (Submit a Book) in content-based programming architecture as shown in Fig. 7.

Combination of push buttons and clusters are graphical portrayals in the silver squares, and case structures give selective content-based programming decision to the Front Panel. The output of the clusters purely depends upon the unique passwords of the students and the information saved in the case structures.

Whenever a transaction occurs through the GUI, its information is saved in the excel sheets with the help of the write to measurement file function palettes; the librarian can send a command to print the monthly data as per the administration requirements. This eliminates the data discrepancies and human error during data logging, and thus AD-LIB becomes more reliable and accurate in such scenario.



Book ID: 0
Title:
Publication Name:
Author Name:
Available:
Genre:
Year of Publishing: 0
ISBN No.: 0
Edition: 0

Due Date is :
15:49:41.895
27/04/2018

Student ID: 70041014029
Student Name: ROHAN PATIL
Gender: M
Degree: B.A.
Stream: MXTC
Name of the Book Issued: THE BLACK HOLE WAR
Year: 3
Age: 20

ROHAN DEEPAK PATIL

Today's Poll Quesiton
Do you agree that there is need for library to encorporate with AD-LIB and make reading interesting?

● Strongly Agree
○ Agree
○ Neutral
○ Disagree
○ Strongly Disagree

Have any feedback or Queries?
We'd love to hear from you.
Contact us at: support@adlib.co.in

Prof. Dattatray Sawant 9421547823
Disha Patel 9421548202
Rohan Patil 9421546632
Tamanna Sinha 9421547823

Fig. 7 Final AD-LIB GUI screen in LabVIEW environment

5 Testing

Initially, testing was done in two parts. The conveyor and the GUI were both tested separately. The conveyor was first controlled using PIC microcontroller. There were two sensors attached at the start and the end on the conveyor to sense when the book is kept. When the book was placed, it would get sensed by the sensor, and a red led on the sensor circuit would glow to show that the book has been placed, the conveyor would then actuate in clockwise direction. When the book would reach the sensor 2 it would sense, a red LED on the circuit would glow indicating that the book has passed; this would give the microcontroller instruction that the book has passed and the conveyor has to be stopped.

There were times when the conveyor did not stop even after the book passed from the sensor and fell in the basket. This was because there was a problem in the range of the sensor. The range was adjusted by the POT given on the IR sensor circuit. The conveyor could also be moved counter clockwise by reversing the connections to the microcontroller. There were two switches which were used to start or stop the conveyor manually when the sensor did not pick up the signal accurately. When we bought the barcode scanner (INTEX IN-101), the logic was to have a sensor which gives command to the scanner to actuate the scanning, but at the later part of the stage we realized that the sensor is getting lot of the disturbances from the surrounding and continuous change in the direction of rotation of the motor to pick up the barcode would be difficult task, so the discontinuous scanner was converted to the continuous mode through the barcode command, given in the manual of the INTEX IN-101.

6 Conclusion

There is very little automation in India's library system and a lot of scope to increase the library system efficiency and improve the data-keeping methods. This paper surely helps them in understanding the microcontrollers, actuation system, HMIs, Bio-Metric systems, and data logging to improve their knowledge. The developed system provides effective management of library as well as reduces human intervention. The GUI build up was initially started on MATLAB, but later it was shifted to LabVIEW as the LabVIEW programming has a specific architecture in the form of state machines. We found that LabVIEW software shortens the design cycle and simplifies the design process as compared to MATLAB. Finally, since the complete project will be built in India and will be used for Indian people, the project meets the Make in India Initiative.

Acknowledgements In Fig. 7, we have used the author photo. The authors thankful to the NMIMS Deemed to be University's Mukesh Patel School of Technology Management and Engineering, Mumbai, India for providing the necessary facilities for carrying out this work.

References

1. Gade A, Angal Y (2017) Automation in library management using LabVIEW. In: IEEE international conference on computing communication control and automation, pp 1–5
2. Gade A, Angal Y (2017) Development of library management robotic system. In: IEEE international conference on data management, analytics and innovation, pp 254–258
3. Gomez-de Gabriel JM, Mandow A, Fernandez-Lozano J, Garcia-Cerezo AJ (2011) Using LEGO NXT mobile robots with LabVIEW for undergraduate courses on mechatronics. In: IEEE Trans Educ 54(1):41–47
4. Gomez de Gabriel JM, Mandow A, Fernandez-Lozano J, García-Cerezo A (2015) Mobile robot lab project to introduce engineering students to fault diagnosis in mechatronics systems. IEEE Trans Educ 28(3):187–193
5. Rennie C, Shome R, Bekris KE, De Souza AF (2016) A dataset for improved RGBD-based object detection and pose estimation for warehouse pick and place. IEEE Robot Autom Lett 1(2):1179–1185
6. Pol RS, Giri S, Ravishankar A, Ghode V (2016) LabVIEW based four DoF robotic arm. In: IEEE international conference on advances in computing, communications and informatics, pp 1791–1798
7. De Smet E (2010) Some ISIS-software history and technical background on the new FOSS integrated library system ABCD. Liber Q 324–335
8. Adegbore AM (2010) Automation in two Nigerian university libraries. Libr Philos Pract 1–13
9. Jibia MS, Mubaraka CM, Michael O (2013) Integrating ICT in library management: design and development of an automated library management system for Cavendish University Uganda. In: Innovative systems design and engineering, pp 1–11
10. Pakdaman M, Sanaatiyan MM, Ghahroudi MR (2010) A line follower robot from design to implementation: technical issues and problems. In: 2nd IEEE international conference on computer and automation engineering, pp 5–9

11. Thirumurugan J, Kartheeswaran G, Vinoth M, Vishwanathan M (2010) Line following robot for library inventory management system. In: IEEE international conference on emerging trends in robotics and communication technologies, pp 1–3
12. Nikitin PV, Rao KV (2009) LabVIEW-based UHF RFID tag test and measurement system. In: IEEE Trans Ind Electron 56(7):2374–2381

Design and Integrate IoT Sensors to RO Water Purifiers for Remote Monitoring and Allowing Users to Pay Per Usage on the Rented RO System

H. D. Sundresh and D. Priya

Abstract Internet of Things (IoT) has given promising chances to make better condition for humankind. One of its applications is smart metering. In today over-polluted world drinking water is the most precious and one of the costliest resources. This paper discusses the approach to provide access to clean drinking water for everyone cost effectively, by renting the smart water purifier and allowing the user to pay as per their usage, without worrying about the quality of water and maintenance of the purifier. This approach is win-win situation for the user as well as for the company. This system will be very economical.

Keywords IoT · Water purifier · Billing

1 Introduction

Internet of things (IoT) had made a revolution on how we see the real-world objects. It is essentially empowering the littler frameworks to get associated with the web, giving them the capacity to think and impart without expecting human to human or human to machine connection. IoT is a rising worldwide innovation, in which things can be associated with the web and controlled remotely from anyplace around the world [1] (Fig. 1).

Lately, a wide scope of IoT applications has been created and sent in businesses just as in local territories, for example, robotized observing, control, management, and maintenance [2]. Sensors and actuators are ending up increasingly groundbreaking, less expensive, and littler, which make their utilization unavoidable. The data gathered by sensors are changed into savvy data, therefore engrafting knowledge into our encompassing condition. IoT empowers billions of gadgets to report their area, personality, and history over remote associations. With the utilization of new

H. D. Sundresh (✉)
RV College of Engineering®, Banglore, India
e-mail: sundreshhd@gmail.com

D. Priya
Department of Information Science, RV College of Engineering®, Bangalore, India

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_60

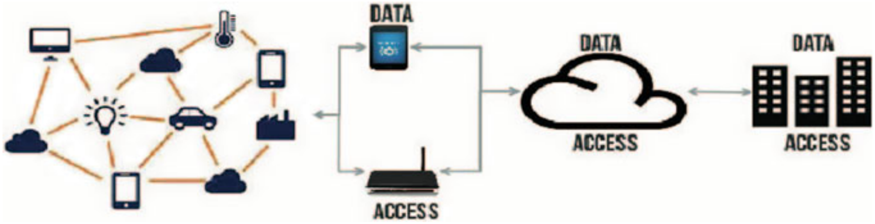


Fig. 1 Overview of IoT

advancements, personal satisfaction is improved just as it lessens the effect of human exercises and utilization designs on condition.

From the urbanization, there has been an exponential increase of demand for clean drinking water [3]. As the population is growing in cities, cost for management of water transmission, storage, and treatment and distribution for consumption are serious issues in underdeveloped and developing countries. With the rapid changes in lifestyle, there is an impact on usage of water and related overheads on sewerage requirements.

In upcoming years, water, the need of life, is conceivably to present the most noteworthy test of its expanded utilization [4, 5] with populace rise, mechanical advance ment, and diminishing supplies because of contamination and over abuse. India is evaluated to end up water focused [6] on the country by 2020.

Brilliant water framework will make clients mindful of their utilization conduct. A wide scope of water sensors is accessible for various modern and residential applications, which measure distinctive substances like water quality, temperature, and spillage location [7, 8].

This paper proposes the implementation of different sensors for water quality control and maintenance of the water purifiers, thus providing access to clean drinking water to the users.

2 Objectives

- Simplifying the safe drinking water challenge.
- Ease of monitoring shelf life of different filters in the RO system for the company that rents it, by integrating IoT-enabled TDS sensor at water inlet and outlet.
- Creating tension-free environment for the user without need for worrying about the quality of water.
- Enabling location tracking with the GPS sensor, thus company can track the device if the user steals it.
- To provide day by day measure of water usage.
- Service provider of water purifier can charge the user based on water usage instead of the amount charged for purifier.

3 Literature Survey

In the present days, there are a lot of water purifiers available in the market with a price tag of around 10,000 INR. Even after buying the purifier the user needs to spend for maintenance, i.e., changing filters time to ensure safe quality drinking water.

If we do a cost-benefit analysis between the proposed system and the regular purifiers, the purifier of an established brand costs around 15,000–35,000 INR and of non-established brands costs around 5000–15,000 INR but in the proposed system the purifier is installed at free of cost in the user space. Also the annual maintenance cost comes around 6000 INR for an established brand's purifier and around 3000 INR for non-established brand's; in the proposed system, it is done free of cost to the user. The water quality and the filters' life are monitored in real-time in the proposed system. So if we consider cost per liter of water, with the established brands it comes around 2.5 INR per liter and non-established brands cost around 1 INR per liter. But with the proposed system, the company can offer a flat rate per month up to certain liters and then it can charge according to the usage of the customer (say 250 INR for the first 250 L then 1 INR per liter). A normal household of four people consumes around 500 L in a month, if they purchase bottled water then that costs around 750 INR (considering 20 L bottle at cost of 30 INR per bottle), or if they install any established brands purifier then that will cost around 1000 INR but in the proposed system it costs around 500 INR which is less than any of the mentioned. Also company can recover its investment within 3 years (Table 1).

Thus, it is a win-win situation for both company and consumer.

4 Methodology

The proposed system will be implemented in different modules.

- One module is where we integrate sensors like TDS sensor, flow rate sensor, and water cut-off valve on the purifier, which are connected to a central server using a GSM module. Periodically, the data from the purifier device is transferred to the

Table 1 Cost-benefit analysis

Comparison	Proposed system	Purifier of established brand	Purifier of non-established brand
Purchasing cost	Zero	15,000–30,000 INR	5,000–15,000 INR
Annual maintenance cost	Zero	Around 6000 INR	Around 3000 INR
Water quality and filter life	Real-time updates from provider	Need to be done by user	Need to be done by user
Cost per liter	Around 1 INR	Around 2.5 INR	Around 1 INR

server. Also, the company can send signals to the purifier to stop the water flow if the bill amount is pending [9–11].

- Another module is where the company can access the data collected on the central server, analyze the data, and update the customer about their usage and billing. The company will keep an eye on the quality of input water and on the output water quality to analyze whether the filters are properly working or not; in case of any abnormality is seen, then it will alert the customer not to use the purifier and will send the service team to check the device and repair it. The customer can also login to the portal and check their usage behavior [12, 13].

5 Conclusion

A novel system for implementing an economic and reliable smart water sensor on the water purifier using IoT-based hardware is discussed. The features of system and the benefits are discussed. The proposed system overcomes the burden of extra costs such as annual maintenance and service charges paid by the user for regular service.

Acknowledgements The authors also acknowledge the help received from the institution—RV College of Engineering, Bangalore.

References

1. Lokhande DG, Mohsin SA (2017) Internet of things for ubiquitous smart home system. In: 2017 1st International Conference on Intelligent Systems and Information Management (ICISIM), 5–6 Oct 2017
2. Atzori L, Iera A, Morabito G (2010) The Internet of Things: a survey. Comput Netw 54(15):2787–2805
3. Mudumbe MJ, Abu-Mahfouz AM (2015) Smart water meter system for user-centric consumption measurement. In: 2015 IEEE 13th International Conference on Industrial Informatics (INDIN), 22–24 July 2015. https://doi.org/10.1109/indin.2015.7281870
4. Smart water metering networks an Intelligent Investment? [Online]. Available http://www.waterworld.com/articles/wwi/print/volume-26/issue-5/regulars/creative-finance/smart-water-metering-networks-an-intelligent-investment.html
5. Tzortzakis G, Katsiri E, Karavokiros G, Makropoulos C, Delis A (2016) Tethys: sensor based aquatic quality monitoring in water ways. In: 2016 at 17th IEEE international conference on mobile data management
6. Gupta N, Shukla D (2016) Design of embedded based automated meter reading system for real time processing. In: IEEE Students Conference on Electrical, Electronics and Computer Science (SCEECS), 5–6 Mar 2016. https://doi.org/10.1109/sceecs.2016.7509328
7. Hsia1 S-C, Hsu S-W, Chang Y-J (2012) Remote monitoring and smart sensing for water quality and leakage detection. IET Wirel Sens Syst 2(4):402–408
8. Suresh M, Muthukumar U, Chandapillai J (2017) A novel smart water-meter based on IoT and smartphone app for city distribution management. In: 2017 IEEE region 10 symposium (TENSYMP), 14–16 July 2017

9. Shingote KS, Shahane P (2016) Microcontroller based flow control system for canal gates in irrigation canal automation. In: 2016 IEEE 6th international conference on advanced computing
10. Mashhadi SKM, Yadollahi H, Mash AM (2016) Design and manufacture of TDS measurement and control system for water purification in reverse osmosis by PID fuzzy logic controller with the ability to Compensate effects of temperature on measurement. Faculty of Electrical Engineering-Iran University of Science and Technology, Tehran, Iran
11. Cloete NA, Malekian R, Nair L (2016) Design of smart sensors for real-time water quality monitoring, published in 19 July 2016
12. Umbaugh HJ (1967, June) Billing frequency and customer relations. J Am Water Works Assoc 59(6):669–674
13. Britton TC, Stewart RA, O'Halloran KR (2013) Smart metering: enabler for rapid and effective post meter leakage identification and water loss management. J Clean Prod 54(1):166–176

MPTCP a Solution Over Crunch in Bandwidth Requirement for Multimedia Application

Vidya Kubde and Sudhir Sawarkar

Abstract Multimedia real-time applications like surveillance systems and video conferencing, where latency plays an important role along with the bandwidth. Today's network advancements are able to resolve bandwidth constraints, but in terms of real-time applications issues related to latency impacts the performance. Multipath TCP (MPTCP) is observed to solve this issues and also able to give the better efficiency in network utilization. In this paper, we have attempted to compare and analyse the growth of MPTCP in multimedia applications and identify the related issues, where by solving these, performance of MPTCP will improve along with the increase in overall efficiency in multihomed or IoT devices and also on real-time multimedia applications.

Keywords Bandwidth aggregation · MPTCP · Multimedia applications · Video streaming

1 Introduction

The use of multimedia has been increasing exponentially over the last decade. Currently the 80% of the bandwidth has been used by the multimedia application on Internet [1]. It is predicted in next decade the requirement of the bandwidth will be multifold as more application areas like education, surveillance, vehicular network and industrial Internet are yet to adopt in full fledge. It has been observed by researchers [2] that bandwidth requirement is growing at the rate of 42% per year. The need of future applications like multimedia applications is saturating the Internet and will drive data rates to levels far beyond the capability of current Internet [3].

V. Kubde (✉)
Department of Information Technology, Datta Meghe College of Engineering, Navi Mumbai, India
e-mail: vidyakubde@gmail.com

S. Sawarkar
Department of Computer Engineering, Datta Meghe College of Engineering, Navi Mumbai, India
e-mail: sudhir_sawarkar@yahoo.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_61

Many researchers have already attempted to meet this huge bandwidth requirement by using aggregation of multiple heterogeneous networks.

MPTCP allows to make them work together and get the benefits of the two at the same time. Multipath TCP allows applications to use all the available interfaces at the same time to improve quality of service (QoS) and quality of experience (QoE). Multipath TCP does not require any additional infrastructure for its implementation.

Understanding the need of future demands and use of existing infrastructure efficiently, we here attempted to study and analyse in depth the issues faced by researchers while implementing the MPTCP which will help to proceed the research on various issues related to MPTCP. This paper describes the basics of MPTCP in Sects. 2 and 3 and further analyse the impact of MPTCP on performance, energy consumptions, and in the case of video streaming applications in Sects. 4 and 5.

2 MPTCP and Related Work

MPTCP is a multipath solution implemented at the transport layer. It is IETF standard; experimental at this stage, MPTCP [4] is designed with goals like, MPTCP should work along with TCP; in case of failure of MPTCP, it should fall back to the TCP, or in case of poor performance then also it should fall back to TCP. Multipath TCP should not harm other flows i.e. it should not take more capacity on any of its path than if it was a single path using only that route.

2.1 MPTCP Working

Application layer access connects to TCP/MPTCP layer by single socket and it appears to the application layer with normal TCP layer. MPTCP establishes connection initially with one of its interface as per the standards of TCP and further it dynamically adds another interface to the existing connection. “Figure 1” describes the details of the establishment of the connection process in MPTCP.

Connection in MPTCP is established with three way handshake signals in “Fig. 1”. At start, M1 confirms that M2 supports MPTCP, when M2 confirms than M1 acknowledges and primary flow is established. The secondary flow is joined to this connection with again three way handshake signals.

3 MPTCP Progress

MPTCP as is a extension of TCP launched in 2011 with the aim of utilizing all the available interfaces concurrently at the same time to improve bandwidth and provide redundant connection with added performance and load balancing strategies as

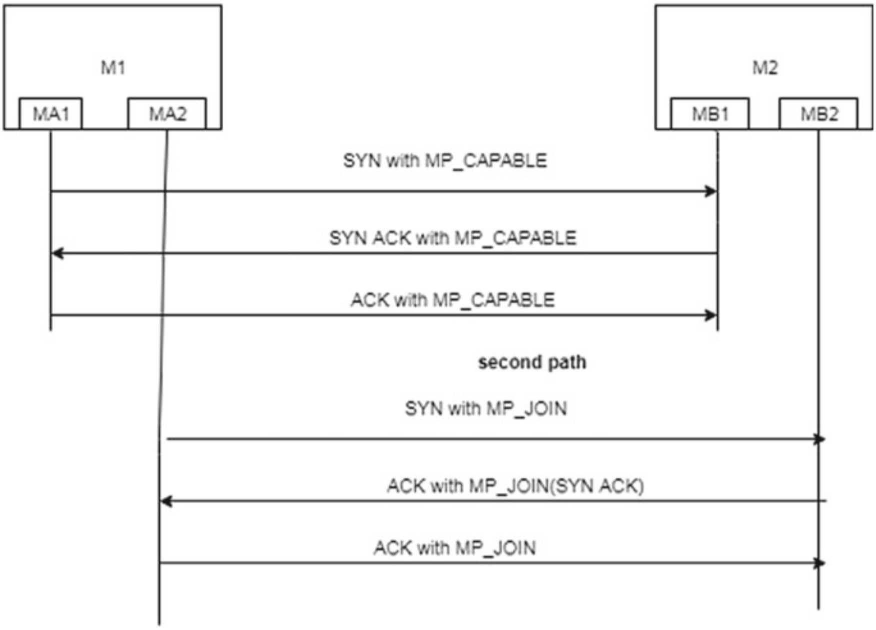


Fig. 1 Connection establishment in MPTCP

shown in Fig. 2. The use cases of MPTCP were smartphones and datacenters. 2012 added the 3G cellular networks to the communication which was not sufficient for multimedia applications, and this deficiency made researchers to use MPTCP for improving quality of service in multimedia applications. Apple, a leading innovative and manufacturer of mobile and desktop, deployed MPTCP in iOS for its siri digital assistant application in 2013. Apple has been using MPTCP since its iOS 7 release understanding the benefit of MPTCP with handover capabilities, where MPTCP has ability to seamlessly handover from one interface to another. In 2014, research was focused on improvement in QoE at the end user side for the multimedia applications like video on demand and high definition (HD) videos over the cellular network and WiFi network through MPTCP. The emphasis was to minimize the delay variation, packet loss, thus enhancing QoE in video streaming applications in heterogeneous networks. In 2015, researchers targeted unsolved issue of bandwidth aggregation for concurrent video transmission in heterogeneous access networks where the problem of mobile video delivery using MPTCP in heterogeneous wireless networks with multihomed terminals was put forth. This issue is addressed by considering path asymmetry in different access networks to achieve the optimal quality of real-time video streaming. From 2016 onward, smartphone vendors have started to deploy Multipath TCP, but its performance with real smart phone applications has to be focused. Multipath TCP is a new TCP extension that has strong potential on smartphones, as shown by its adoption by Apple and Korea Telecom. Apple's deployment

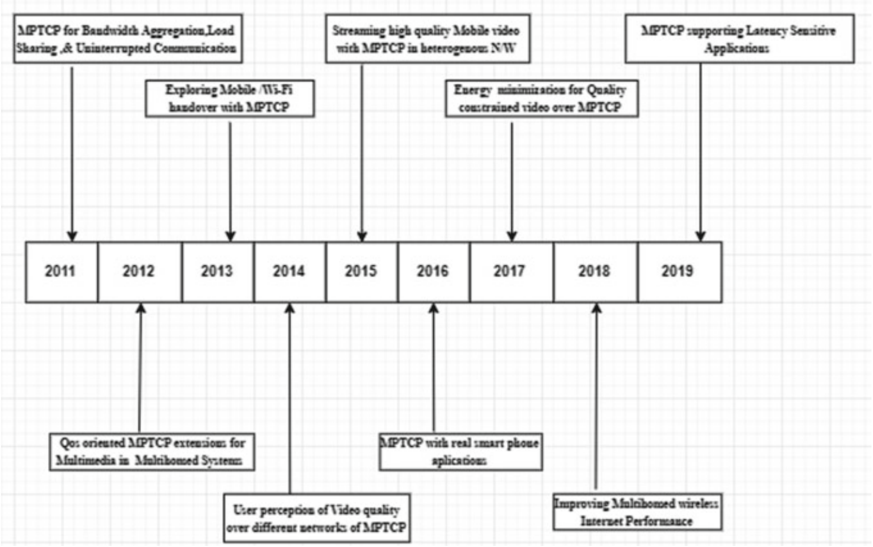

MPTCP for Bandwidth Aggregation,Load Sharing ,& Uninterrupted Communication
Exploring Mobile /Wi-Fi handover with MPTCP
Streaming high quality Mobile video with MPTCP in heterogenous N/W
Energy minimization for Quality constrained video over MPTCP
MPTCP supporting Latency Sensitive Applications
2011
2012
2013
2014
2015
2016
2017
2018
2019
Qos oriented MPTCP extensions for Multimedia in Multihomed Systems
User perception of Video quality over different networks of MPTCP
MPTCP with real smart phone aplications
Improving Multihomed wireless Internet Performance

Fig. 2 Evolution history of MPTCP

focused on a single use case and very little work was done in interactions between real smartphone applications and Multipath TCP.

2017 focused mainly on the energy efficient applications on multihomed devices operated on battery. Several MPTCP schemes for reducing energy consumption and improving user-perceived video quality were developed in this era.

4 Issues and Analysis

In the presents year, bandwidth was not the main concern as cost of the bandwidth decreasing day by day, but many multimedia and video conferencing applications which are latency sensitive applicants, needs less delay path where MPTCP is the only solution. Especially, researchers are focusing on use of MPTCP in all the multihomed devices like smartphones, laptops, tablets or IoT devices based on raspberry pi to improvement in QoS parameters like jitter, delay, energy and latency which will cater the need of the users for multimedia based applications. The architecture components like scheduler, buffer management, congestion control and many more has to be revised with application perspective. "Table 1", is the outcome of our analysis which we have carried doing in-depth survey of the development and research till today. The analysis is carried out keeping the focus on the solving issues and improving performance considering the QoS and QoE.

Considering the MPTCP design goals and solving issues appeared in past we have categorized and identified blocking points of MPTCP as follows.

Table 1 Classifications of issues

Issues	Methodologies	Evaluation metrics
Subflow path scheduling	Comparison of different designs for multipath schedulers ranging from round robin to optimize multipath scheduler [5]	Delay
	Implemented three different schedulers considering sending rate, window space and time/space and compared them with default MPTCP scheduler [6]	Throughput
	In-depth performance analysis considering heavy data transfer and application constraints [7]	(1) Goodput (2) Delay
	Estimating packet receiving time at the receiver and scheduling packet [8]	
	A new scheduling policy considering congestion control and speed as decision metrics [9]	Throughput
	A scheduling scheme that assigns data packets to subflows, by estimating out-of-order packets caused by difference in the subflows [10]	Throughput
	Segregating the data on different links based upon quality requirements or type of data [11]	Throughput
Path heterogeneity	Forward error correction (FEC) coding at transport layer [12]	(1) Throughput
	Forward error correction (FEC) coding [13]	(1) PSNR (2) Delay (3) Goodput
	Context aware and partially reliable, MPTCP extension [14]	PSNR
	A loss-aware disabling mechanism that temporarily switch a lossy wireless interface to a backup mode [15]	Goodput

(continued)

Table 1 (continued)

Issues	Methodologies	Evaluation metrics
	Algorithm, to handle the different path characteristics [16]	Throughput
Congestion control	The different methodologies of congestion control are studied and analysed [17]	Throughput
	Coupled congestion control [18]	–
	An congestion control algorithm is designed considering energy, round trip time and path loss rate [19]	–
	The measurement results for congestion control performance in three multihomed, real world Internet scenarios that are evaluated [20]	–
	Bidimensional multipath congestion control approach to deal with TCP fairly in shared bottleneck [21]	–
	(1) Traffic shaping (2) Traffic offloading [19]	(1) Throughput (2) Energy consumption
	Delay based traffic shifting [22]	Throughput
	Fast coupled retransmission [23]	Queuing delay, TCP timeouts
	A congestion control algorithm for MPTCP, using packet queuing delay as congestion signals [24]	–
	Gentle slow start scheme (GSAM) for which finds the appropriate threshold to smooth the aggressive slow start behaviour [25]	Round trip time
	Algorithm to reduce flappiness across paths [24]	Throughput

(continued)

Table 1 (continued)

Issues	Methodologies	Evaluation metrics
	Adaptive congestion window i.e. minimizing the difference between the subflows and proactive scheduling algorithm to determine the packet sending sequence to each path [26]	Goodput
Energy consumption	Modified MPTCP to minimize the impact on application delay [27]	Goodput, delay
	Designed and implemented a variant of MPTCP, reducing power consumption without affecting download latency [28]	Throughput, energy consumption
	Compared the energy cost of streaming on a device with two interfaces and device with one interface [29]	Energy consumption
	(1) Flow rate allocation algorithm (2) Dropping of less priority frames [30]	(1) PSNR (2) Inter packet delay (3) Jitter
	Flow rate allocation algorithm [31]	(1) Energy (2) PSNR (3) Goodput
Path switching mechanism	MPTCP with path awareness can dynamically shift the traffic to a single path and vice versa [12]	Throughput
	Short flow/long flow [32]	(1) Throughput (2) RTT
	Multi-attribute aware path selection approach for MPTCP [33]	–
Out-of-order packets	Analysis of four solutions for out-of-order packets (1) D-SACK, (duplicate selective acknowledgement) (2) Eifel algorithm (3) TCP-DOOR (detection of out-of-order and response) (4) Forward Retransmission Time Out Recovery (F-RTO) algorithm [34]	(1) Link utilization (2) Throughput
	Scheduling mechanism [35]	(1) Throughput (2) Packet loss rate

(continued)

Table 1 (continued)

Issues	Methodologies	Evaluation metrics
	Network coding [36]	Throughput
MPTCP in video streaming	Challenges of using MPTCP in video streaming [37]	–
	Explored whether MPTCP always benefits video streaming [38]	–
	Survey on existing literatures on QoE of video streaming [39]	–
	User perception Of video quality over LTE network and different protocols [40]	(1) Peak Signal To Noise ratio (PSNR) (2) Packet loss (3) (OWD) One Way Delay (4) Inter Packet Delay (IPD)
	Qos improvement in multimedia applications through partial reliability [41]	(1) Peak Signal to Noise ratio (PSNR) (2) Loss rate (3) End to end delay

It describes the ability to use multiple paths with different characteristics to reach the destination. The difference in the characteristics of different paths like round trip time, packet loss ratio etc. is going to cause variation in the throughput. The difference in delay of the paths will lead to out-of-order packets at the receiver. One of the solutions for this problem is FEC coding [13]. QoE is effected by path heterogeneity; in [14], the author has given a context aware solution for this issue. Loss due to heterogeneous networks can be reduced by switching between full mode and backup mode MPTCP [15]. To use MPTCP in latency sensitive applications, [11] has suggested FEC coding as a solution for heterogeneous paths. The negative aggregation caused by the lossy path can be bypassed, by switching to single path MPTCP [12].

Congestion control in MPTCP switches the traffic from more congested path to less congested path. The TCP fairness design goal states the controlling of sub-window increase on each path as important issue. At start, congestion control of single path TCP was used on each path of MPTCP. This has not satisfied the TCP fairness goal, so later on the control of the sub-window was done collectively at centralized manner. All the subflows congestion windows were coupled together [18]. More deliberate design of multipath congestion control algorithms has used a queuing delay [24] as a congestion signals. The challenging issue of MPTCP congestion control is TCP friendliness. One of the approaches for this problem is to apply the weight [21] to individual congestion control of each subflow, so that a bundle of sub flows can have the same aggressiveness as one TCP flow. In [19] congestion control, algorithm with new approach is proposed, which considers energy consumption, RTT and packet loss rate. Congestion control along with energy efficiency is suggested by [19, 22] where they have focused on the energy consumption at the receiver side.

Throughput of MPTCP is primarily dependent upon the scheduler. In [42] the scheduling of the packet depends upon congestion on that path, RTT of that path and its energy consumption. Estimation-based scheduling is proposed by [8]. The various scheduling strategies are analysed by [5]. Constraint based proactive solution is proposed by [10], where additional path is only used when round trip time is acceptable. The wrong scheduling decision leads out-of-order packets [35] at the receiver. A novel scheduler [11] segregates the data, into control information and the data. The scheduling of this both is done on different paths, depending upon their characteristics.

The multi-interfaces remaining active all the time may result in more energy consumption. However, multipath transfer consumes more energy to maintain all the active interfaces. Analysis of MPTCP energy consumption [27] along with handover mechanism in various operational modes is proposed. In [29], authors have determined the energy cost of using MPTCP. An energy aware variant of MPTCP called as eMPTCP [28] is designed and implemented. To minimize the energy consumption in quality constrained video [30], dropping of less priority frames and flow rate allocation algorithm is used. Congestion control along with energy consumption perspective is analysed [22].

5 Conclusion

MPTCP has been proposed to implement from 2011, to overcome the bandwidth aggregation. Since then the researchers have modified and improved the MPTCP in various stages, but still looking to the future need of bandwidth and multimedia application TCP is not fully replaced by MPTCP. New areas are emerging into the like IoT and tactile Internet where multiple interfaces are available on such devices capable of handling MPTCP, but because of issues like congestion control, path heterogeneity, energy consumption, scheduler stated in the analysis, the efficient utilization of bandwidth and low latency applications are yet to be used with MPTCP.

References

1. Index, Cisco Visual Networking (2015) Cisco visual networking index: forecast and methodology 2015–2020. White paper, CISCO
2. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html
3. https://www.itu.int/en/ITU-T/Workshops-and-seminars/201807/Documents/3_Richard%20Li.pdf

4. Raiciu C et al (2012) How hard can it be? Designing and implementing a deployable multipath {TCP}. In: 9th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 12)
5. Singh A et al (2012) Performance comparison of scheduling algorithms for multipath transfer. In: 2012 IEEE Global Communications Conference (GLOBECOM). IEEE
6. Kimura BYL, Lima DCSF, Loureiro AAF (2017) Alternative scheduling decisions for multipath TCP. IEEE Commun Lett 21.11:2412–2415
7. Paasch C et al (2014) Experimental evaluation of multipath TCP schedulers. In: Proceedings of the 2014 ACM SIGCOMM workshop on capacity sharing workshop. ACM
8. Kim HA, Oh B-H, Lee J (2012) Improvement of MPTCP performance in heterogeneous network using packet scheduling mechanism. In: 2012 18th Asia-Pacific Conference on Communications (APCC). IEEE
9. Yang F, Amer P, Ekiz N (2013) A scheduler for multipath TCP. In: 2013 22nd International Conference on Computer Communication and Networks (ICCCN). IEEE
10. Oh B-H, Lee J (2015) Constraint-based proactive scheduling for MPTCP in wireless networks. Comput Netw 91:548–563
11. Mondal A et al (2018) PPoS: a novel sub-flow scheduler and socket apis for Multipath TCP (MPTCP). In: 2018 Twenty Fourth National Conference on Communications (NCC). IEEE
12. Ferlin S et al (2018) MPTCP meets FEC: supporting latency-sensitive applications over heterogeneous networks. IEEE/ACM Trans Netw (TON) 26.5:2005–2018
13. Wu J et al (2016) Streaming high-quality mobile video with multipath TCP in heterogeneous wireless networks. IEEE Trans Mobile Comput 15.9:2345–2361
14. Cao Y et al (2016) PR-MPTCP+: context-aware QoE-oriented multipath TCP partial reliability extension for real-time multimedia applications. In: 2016 Visual Communications and Image Processing (VCIP). IEEE
15. Nguyen K et al (2016) An enhancement of multipath TCP performance in lossy wireless networks. In: 2016 IEEE 41st conference on Local Computer Networks Workshops (LCN Workshops). IEEE
16. Nguyen SC et al (2011) Evaluation of throughput optimization and load sharing of multipath TCP in heterogeneous networks. In: 2011 Eighth international conference on wireless and optical communications networks. IEEE
17. Xu C, Zhao J, Muntean G-M (2016) Congestion control design for multipath transport protocols: a survey. IEEE Commun Surv Tutorials 18(4):2948–2969
18. Raiciu C, Handley M, Wischik D (2011) Coupled congestion control for multipath transport protocols. No. RFC 6356
19. Wang W, Wang X, Wang D (2018) Energy efficient congestion control for multipath TCP in heterogeneous networks. IEEE Access 6:2889–2898
20. Fu F et al (2015) Performance comparison of congestion control strategies for multi-path TCP in the NORNET testbed. In: 2015 IEEE/CIC International Conference on Communications in China (ICCC). IEEE
21. Honda M et al (2009) Multipath congestion control for shared bottleneck, vol 357. In: Proceedings of PFLDNeT workshop
22. Zhao J, Liu J, Wang H (2017) On energy-efficient congestion control for multipath TCP. In: 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). IEEE
23. Hwang J, Walid A, Yoo J (2018) Fast coupled retransmission for multipath TCP in data center networks. IEEE Syst J 12(1):1056–1059
24. Cao Y, Xu M, Fu X (2012) Delay-based congestion control for multipath TCP. In: 2012 20th IEEE International Conference on Network Protocols (ICNP). IEEE
25. Dong P et al (2019) Tuning the aggressive slow-start behaviour of MPTCP for short flows. IEEE Access 7:6010
26. Zhou D, Wei S, Minghui S (2013) Goodput improvement for multipath TCP by congestion window adaptation in multi-radio devices. In: 2013 IEEE 10th Consumer Communications and Networking Conference (CCNC). IEEE

27. Paasch C et al (2012) Exploring mobile/WiFi handover with multipath TCP. In: Proceedings of the 2012 ACM SIGCOMM workshop on Cellular networks: operations, challenges, and future design. ACM
28. Lim Y-S et al (2015) Design, implementation, and evaluation of energy-aware multi-path TCP. In: Proceedings of the 11th ACM conference on emerging networking experiments and technologies. ACM
29. Kaup F et al (2015) Can multipath TCP save energy? A measuring and modeling study of MPTCP energy consumption. In: 2015 IEEE 40th conference on Local Computer Networks (LCN). IEEE
30. Wu J, Bo C, Ming W (2016) Energy minimization for quality-constrained video with multipath TCP over heterogeneous wireless networks. In: 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS). IEEE
31. Wu J et al (2017) Quality-aware energy optimization in wireless video communication with multipath TCP. IEEE/ACM Transactions on Networking 25.5:2701–2718
32. Deng S et al (2014) Wifi, lte, or both?: measuring multi-homed wireless internet performance. In: Proceedings of the 2014 conference on internet measurement conference. ACM
33. Zeng J et al (2017) Multi-attribute aware path selection approach for efficient MPTCP-based data delivery. J Internet Serv Inf Secur 7.1:28–39
34. Alheid A, Kaleshi D, Doufexi A (2014) Performance evaluation of MPTCP in indoor heterogeneous networks. In: Proceedings of the 2014 first international conference on systems informatics, modelling and simulation. IEEE Computer Society
35. Xue K et al (2018) DPSAF: forward prediction based dynamic packet scheduling and adjusting with feedback for multipath TCP in lossy heterogeneous networks. IEEE Trans Veh Technol 67.2:1521–1534
36. Ageneau P-L, Nadia B, Mario G (2017) Practical random linear coding for MultiPath TCP: MPC-TCP. In: 2017 24th International Conference on Telecommunications (ICT). IEEE
37. Priyadarshini MS, Rekh AS (2016) Streaming video with MultiPath TCP in wireless networks. IEEE Trans Mobile Comput 15.4:2345–2361
38. James C et al (2016) Is multipath TCP (MPTCP) beneficial for video streaming over DASH? In: 2016 IEEE 24th international symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS). IEEE
39. Su G-M et al (2016) QoE in video streaming over wireless networks: perspectives and research challenges. Wireless Netw 22.5:1571–1593
40. Uppu P, Kadimpati S (2013) QoE of video streaming over LTE network
41. Diop C et al (2012) QoS-oriented MPTCP extensions for multimedia multi-homed systems. In: 2012 26th international conference on advanced information networking and applications workshops. IEEE
42. Wu J et al (2017) Quality-aware energy optimization in wireless video communication with multipath TCP. IEEE/ACM Trans Netw 25.5:2701–2718

Design of *AYUSH*: A Blockchain-Based Health Record Management System

A. V. Aswin, K. Y. Basil, Vimal P. Viswan, Basil Reji and Bineeth Kuriakose

Abstract We are living in a world where data is considered to be the next fuel; also, we know how much value the data is. Considering this over the health records on which a patient deals with whenever he/she goes to a hospital, the present scenario lags in securing the patients' health record management system in order to provide more transparency over patients' past health data. If the same was available, then data sharing between hospitals would have been much easier. If the hospital gets to know the past health history like the amount of drugs the patient is consuming as part of medication, then the doctor could make a stern decision over the disease and could also satisfy the patient with a better treatment over his symptoms. The basic problem to be dealt with these would be the privacy consideration of the patient when he/she is sharing the data. In order to tackle that problem, we are using a patient-centric health record management system under the distributed network architecture. In this paper, we are proposing a solution that makes use of the emerging blockchain (permissioned) technology to achieve this goal.

Keywords Blockchain · EHR · Hyperledger Fabric · Health care · Ethereum

A. V. Aswin · K. Y. Basil · V. P. Viswan · B. Reji · B. Kuriakose (✉)
Muthoot Institute of Technology and Science, Ernakulam, India
e-mail: bineethbinz@gmail.com

A. V. Aswin
e-mail: aswinavofficial@gmail.com

K. Y. Basil
e-mail: basilky145@gmail.com

V. P. Viswan
e-mail: vimal974ever@gmail.com

B. Reji
e-mail: basilreji3@gmail.com

B. Kuriakose
Oslo Metropolitan University, Oslo, Norway

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_62

1 Introduction

The advancement and impact of technology can be found in every field of the society. Considering this over the health records which a patient deals with whenever he/she goes to a hospital, the present scenario lacks a secure patient's health record management system to provide more transparency over patients' past health data. Also, there is an absence of a widely accepted digital standard for sharing EHR data. If the hospital gets to know the past health history of a patient like past diseases, the amount of drugs the patient is consuming as part of medication, medical test results, allergies, etc., then the doctor could make a stern decision over the disease and could also satisfy the patient with a better treatment. This can also benefit patient by getting a better treatment at lower cost and reduced time. Unnecessary medical tests can be avoided if the past history of patient is available.

In this paper, we are proposing a solution to these problems in healthcare sector by applying emerging blockchain technology. In the AYUSH network, there will be patients and service providers like hospitals, doctors, and laboratories. Patients can securely create an account on AYUSH, and all the upcoming medical records of the patients will be added to the AYUSH platform. Easier user interface and APIs will be provided by the platform for easier access for participants.

Saving the history of patients in the blockchain can provide many advantages. Since there is no central administrator, patient will have full control over his/her entire health records and he/she can determine for whom permission should be given to access their data. Built-in transparency how the blockchain system works can bring trust between participating entities. Existing symmetric and asymmetric cryptography principles can be used along with the blockchain system to provide privacy control for patients. All the data of patients can be encrypted by their private key, and needed records can be selectively decrypted for sharing. The distributed record keeping nature of blockchain can ensure that patient data is not lost by a single point of failure. Health records in blockchain are series of records logically connected using the hashes of records. This provides easier traceability to health records on blockchain, along with resistance toward tampering of digital records. Immutability of blockchain records can bring easier claim adjudication. The transaction rates of Hyperledger, the blockchain platform we are using, are also higher. Patients can benefit even if they have a long history of records. Researchers are also the beneficiaries of the platform, since they can avail large amount of anonymous health data for finding new insights.

2 Blockchain in Health Care

Blockchain [1] is a distributed and decentralized chain of records or ledgers. The immutability of blockchain records ensures trust between participating entities. This has brought many applications for blockchain including health care.

2.1 Problems in Healthcare Sector

Current healthcare infrastructure lacks proper mechanisms for the exchange of healthcare information. There is no accepted standard for sending, receiving, and managing information between EHR systems. Most of the cases, patient has to carry all of his past medical records to the new hospital or has to do the previous medical tests again. Lack of health history of a patient may lead to improper treatment also. Another problem is the lack of patient-centric longitudinal list of records. Thus, patient data gets scattered across multiple records at multiple hospitals. The current health data keeping systems does not provide any resistance toward tampering and cannot be used for claim adjudications on insurances. Currently, there are chances that healthcare service providers may use the patient's data for analytics, without considering their privacy. The health data is unreliable since it is not stored at multiple locations.

2.2 Advantages of Using Blockchain

Blockchain is perfectly suited for health care because of its distributed, immutable implementation. Blockchain can ensure trust between participating entities. Privacy and security of data can be preserved by using cryptography principles. The transaction speed of blockchain is much faster, and transactions are traceable from beginning. Distributed nature of blockchain ensures data reliability also.

2.3 Challenges in Implementation

Even though there are good reasons behind applying blockchain on healthcare sector, there are many challenges which have to be solved for proper implementation of blockchain over health care. There are limited successful blockchain models and the success of blockchain on health care, and the cost that will incur is uncertain. Health data is huge, and replicated storage of data will create storage capacity problems. The platform should be scalable as more service providers are added, and they should not be considerable delay. Different standards for keeping and sharing EHR are also a major challenge. Various rules like HIPAA and unwillingness to share health data by service providers are also a major problem.

3 Familiarization of Tools

3.1 Hyperledger Fabric

Hyperledger Fabric [2] is an open-source enterprise-grade permissioned distributed ledger technology (DLT) platform designed for use in enterprise contexts that delivers some key differentiating capabilities over other popular distributed ledger or blockchain platforms. Hyperledger Fabric has a highly modular architecture which is configurable. It enables innovation, versatility, and optimization for a broad range of applications including banking, finance, insurance, health care, human resources, supply chain, and even digital music delivery.

The taxonomy of blockchain includes public, private, consortium blockchains, where public blockchain is completely distributed in terms of its architecture, whereas consortium blockchain is considered to be partially decentralized and private blockchain is said to be a centralized one. The Fabric platform provides a permissioned network. In a permissioned network, the resources that are being shared in the network are permissioned; that is, only authorized persons get access to it. This means that while the participants may not fully trust one another (they may, e.g., be competitors in the same industry), a network can be operated under a governance model that is built off of what trust does exist between participants, such as a legal agreement or framework for handling disputes [2].

3.2 InterPlanetary File System (IPFS)

InterPlanetary File System (IPFS) [3] is a new hypermedia distribution protocol addressed by content and identities. IPFS enables the creation of completely distributed applications. It aims to make the Web faster, safer, and more open.

IPFS is a distributed file system that seeks to connect all computing devices with the same system of files. In some ways, this is similar to the original aims of the Web, but IPFS is actually more similar to a single BitTorrent swarm exchanging git objects. After a file is successfully added onto the IPFS, it computes a hash of the file and now other systems will be able to access this file through this calculated hash value. Consider the situation of a PDF file. Let the file be stored on the IPFS network. If you run your own node, the file would only be stored on your node and available for the world to download. If someone else downloads it and sends it, then the file is stored on both your nodes, and so on [3].

4 Proposed Work

In the proposed system, we are applying the emerging blockchain technology in creating transparent health record chain. When the patient goes to a new hospital after similar visit in yet another hospital, he/she opts the data to be shared to the new hospital. If any new health data is produced at the new hospital, they first add the information (clinical reports or other scan reports) into the IPFS file system. The hash of this file is added to the blockchain.

The proposed solution is a patient-centric one; that is, the patient has got the power to give access to his data. Hyperledger Fabric is used since the system requires a permissioned network.

4.1 Architecture

This section will discuss the architecture of the proposed system, AYUSH.

4.1.1 API Module

API module acts as an interface between AYUSH platform and end users (patients, hospitals, and doctors). It abstracts implementation details of AYUSH platform, and users can interact using simple UI and HTTP requests (Fig. 1).

4.1.2 AYUSH Platform

AYUSH platform abstracts implementation details of Hyperledger Fabric and IPFS and provides services to API module. Various modules present in AYUSH network are:

1. Fabric client;
2. IPFS interface;
3. Auth module;
4. Membership module;
5. Application logic and database.

IPFS Interface

InterPlanetary File System (IPFS) [3] interface is used to communicate with IPFS to upload or fetch from IPFS network.

Auth Module

Auth module is used to recognize a user’s identity, allowing only legitimate users to interact with the platform.

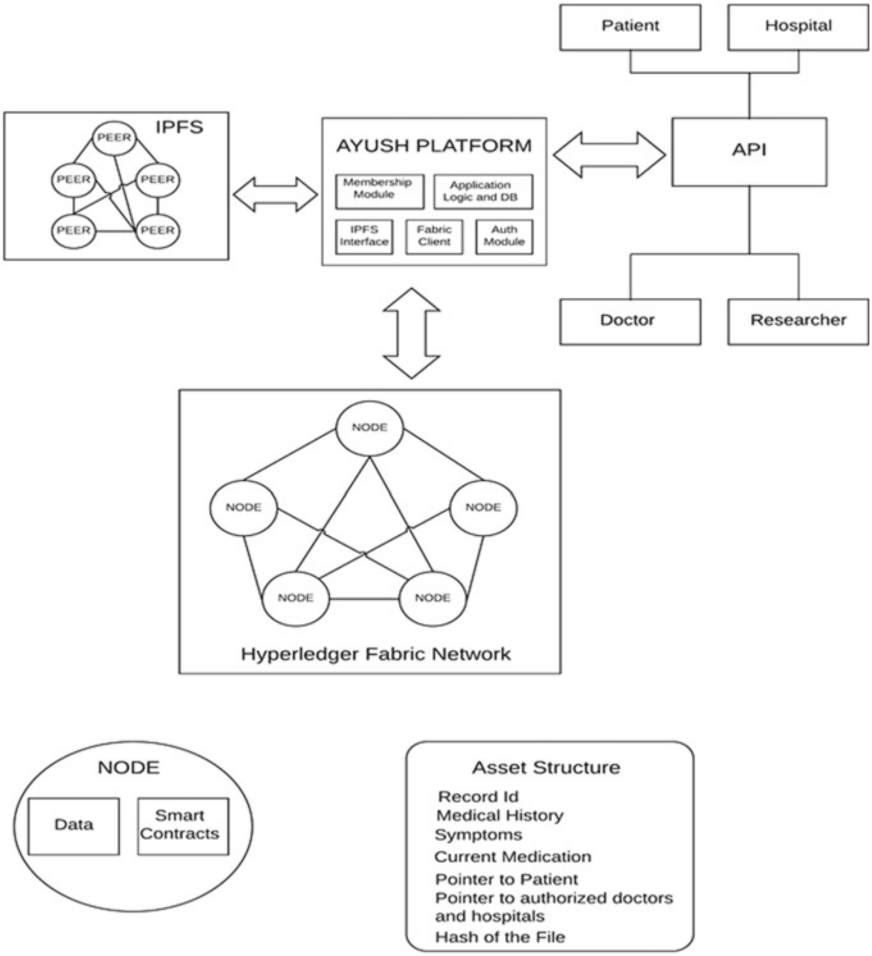


Fig. 1 AYUSH architecture

Membership Module

Membership module is a component that aims to offer an abstraction of a membership operation architecture. In particular, it abstracts away all cryptographic mechanisms and protocols behind issuing and validating certificates and user authentication. It issues certificates which are used by peers to join the Hyperledger Fabric network.

Application Logic and Database

This module will be responsible for overall operation of the platform, and it has a local database also.

5 Methodology

Every patient in the AYUSH network will have a public key and a private key, which are created at the time of registration. All the data of patients are encrypted using their private key. To share the data, decryption is needed using their private key, which is encrypted using their passwords. So, patient decrypts his private key and selects the health records which have to be shared. Then, the selected data is decrypted at client side. The decrypted data is again encrypted using the public key of service provider, to provide additional security to ensure that only required service provider receives the data. The integrity of the shared file can be verified at the receiver end just by re-calculating the hash of the file and comparing it with the original hash which is on the AYUSH blockchain network. After receiving the shared files at service provider, they analyze the past data to give better treatment for the patient. After necessary observation, the textual details like symptoms are added to the blockchain. The treatment records of the patient may be of huge size, which is difficult to put in the blockchain since it will increase the time required to calculate the hashes. This might also cause reduced transaction rates. To avoid this, the heavy records are stored on the IPFS, after encrypting the records with public key of the patient. The hash of the original field is added to the blockchain to later check the integrity of the file, if it gets shared with any other service provider. The hash of the encrypted file is generated by IPFS, after uploading the file into IPFS. This helps to uniquely identify files in the IPFS system and to prevent duplicate upload of files. The record is now spread to all the nodes in the network from the node on which it was uploaded. This makes the data reliable and immutable to the IPFS system. No one other than patient can decrypt this data, since only he has the matching private key pair. The newly added record becomes a part of the personal health records of the patient. He/she can later share these files with other service providers by following the similar process. All the encryption, decryption, and key generation process are performed at the client side for improving the security.

6 Conclusion

We are now able to witness the revolutionary changes that technologies have brought to various sectors in the society which makes human life much more simpler. Even though we have achieved a lot in various sectors, the healthcare sector decades back in terms of technological advancements. The blockchain is considered to be one of the promising technologies with its application over many sectors. Bringing blockchain into healthcare sector could enhance the trust between participating entities which contributes to the betterment of healthcare record management system while considering the privacy of patients' data. We hope the proposed design of AYUSH which can solve the data sharing and privacy issues faced by health industry today.

References

1. Blockchain: The Chain of Trust and its Potential to Transform Healthcare—Our Point of View, IBM Global Business Services Public Sector Team 6710, 8 Aug 2016
2. Chen Y, Li H, Li K, Zhang J (2017) An improved P2P file system scheme based on IPFS and blockchain. 2017 IEEE Int Conf Big Data (Big Data). https://doi.org/10.10007/1234567890
3. Ekblaw A, Azaria A, Halamka JD, Andrew Lippman MD (2016) A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data, MIT Media Lab

Support Vector Machine-Based Focused Crawler

Vanshita R. Baweja, Rajesh Bhatia and Manish Kumar

Abstract The Internet is an immense source of information. People use search engines to find desired web pages. All these web pages are gathered from the search engine by using web crawler. In traditional crawler, the information retrieval was based on the occurrence of keywords in a document due to which many irrelevant web pages were also retrieved. For the effective classification of web pages, support vector machine (SVM)-based crawler model is proposed in this paper. Various features of URL and web page are used for effective classification. SVM is trained by using these features and further tested. The proposed model is analyzed using precision and recall metrics. The experimental results exhibit optimized results by using this proposed approach.

Keywords Support vector machine · Focused crawler · Feature extraction · Web page classification · Uniform resource locator

1 Introduction

Web pages are the source of information exchange in today's world. For example, many firms can publicize their stocks and sales through web pages. If any person has interest in football match, they can watch matches live on web pages. All the web pages are gathered by the help of web crawler [1]. It is a tool that searches for a specific subset of the web rather than exploiting all regions of the web.

There are many search engines provided to users for searching the set of keywords like Google. The search engine serves as a tool that provides many desired web pages. Typical search engines use only keyword searching for web page classification. They

V. R. Baweja (✉) · R. Bhatia · M. Kumar
Computer Science, PEC University of Technology, Chandigarh, India
e-mail: vanshitarbaweja@gmail.com

R. Bhatia
e-mail: rbhatiapatiala@gmail.com

M. Kumar
e-mail: manishkamboj3@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_63

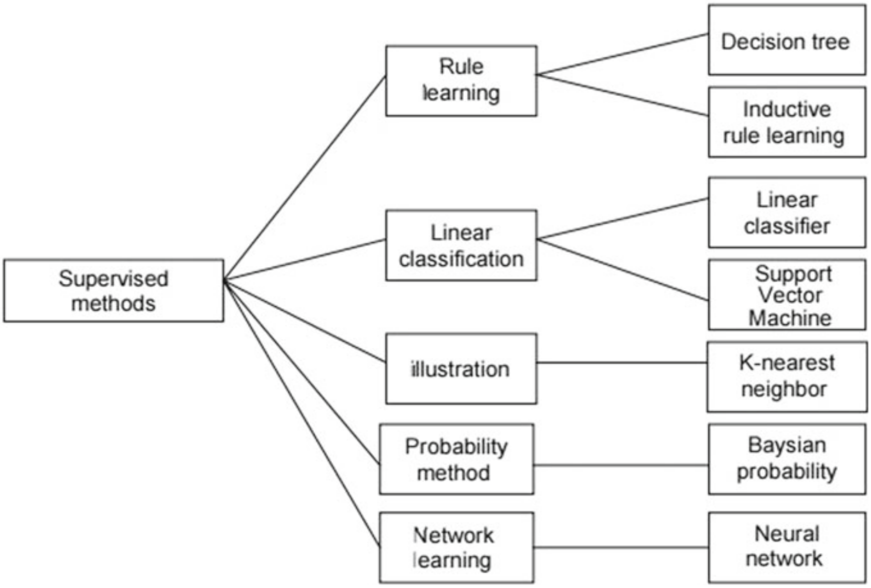


Fig. 1 Taxonomy of supervised classification methods [2]

may give irrelevant web pages and unrelated links. Many machine learning methods, supervised and unsupervised exist in literature. Supervised algorithms are used to train machine learning task for every input with corresponding outputs, whereas unsupervised algorithms are performed over machine learning task with a set of inputs which in turn gives relationships between different inputs. Figure 1 represents the classification of supervised learning algorithms.

This paper presents a novel web page classification framework that uses SVM as a classifier. SVM classifies the samples using an optimal hyperplane. An optimal hyperplane is determined by the samples closet to it and not bothering any other sample called support vectors.

The rest of this paper is organized in the following manner. Section 2, presents an overview of SVM framework and its types. Section 3 presents the literature survey. Section 4 explains the proposed model of SVM web page classification model. The SVM classification method is explained in Sect. 5. In Sect. 6, experimental results are presented. Then, conclusions are explained in Sect. 7.

2 Support Vector Machine

2.1 Overview

Support vector machine is a supervised machine learning algorithm and can be used as classification and regression model. SVM was introduced by Vapnik and Chervonenkis [3] in 1963. In 1992, Vapnik suggested nonlinear classification with the help of kernel trick [3].

SVM can be used for classification or regression by forming a hyperplane or a set of hyperplanes. During the training of SVM quadratic problem arises, this problem can be solved by sequential minimal optimization (SMO). Therefore, SMO is used for training of SVM.

2.2 SVM Working

In learning a classifier for binary classification, given a set of training samples in the form

$$(p_1, q_1), \ldots, (p_n, q_n)$$

The input features $p_i \in \mathrm{R}$ are usually d-dimensional vectors describing the properties of the input example, q_i are either -1 or 1 each of them are indicating a class which belongs to p_i. Equation (1) represents the hyperplane that can be used to distinguish the sample sets in SVM where w is the optimum weight and b is the excursion.

$$w * p + b = 0 \tag{1}$$

Figure 2 demonstrates the linearly separable case where samples of one category are portrayed as "∘" and samples of other category is portrayed as "•" [4]. These data points are separated by a hyperplane. There is the number of possibilities of drawing a hyperplane but according to SVM methodology, only one optimal hyperplane is selected. An optimal hyperplane lies between maximum margin, i.e. $d_1 + d_2$ and determined by the samples closest to it and not bothering any other sample. As support vectors determine the optimal hyperplane, the maximal margin can be found by minimizing $\frac{1}{2}\|w\|^2$, as shown in Eq. (2)

$$\min\left\{\frac{1}{2}\|w\|^2\right\} \tag{2}$$

An optimal hyperplane can be configured by minimizing (2) under the constraint of (3)

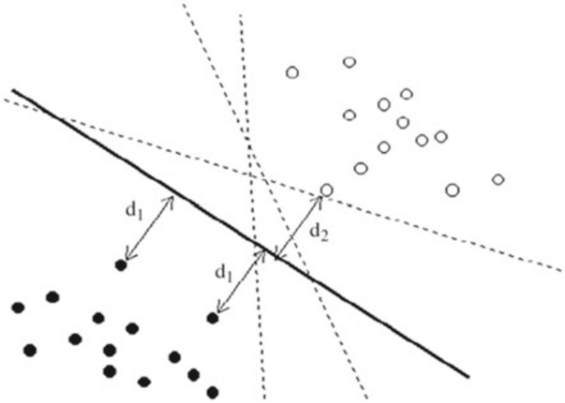


Fig. 2 Optimal separating hyperplane [4]

$$q_i * (w * p_i + b) \geq 1, \forall i \tag{3}$$

By the use of kernel functions, hyperplane can be optimized for nonlinear cases too. SVM can be used for nonlinear cases, by implementing the kernel functions. The implicit mapping ($\phi(.)$) of the input samples (p_i, p_j) to high-dimensional feature spaces by the use of kernel function is illustrated in Fig. 3. Hence, the kernel function is given by Eq. (4):

$$K(p_i, p_j) = \left\langle \phi(p_i).\phi(p_j) \right\rangle \tag{4}$$

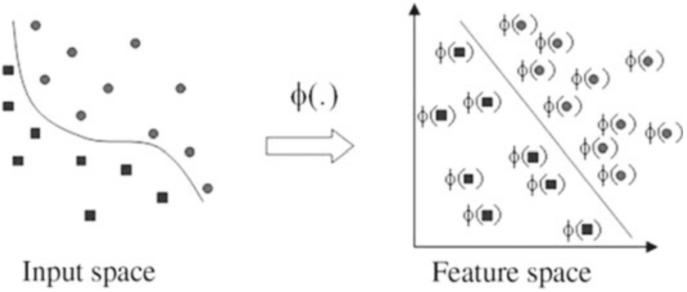


Fig. 3 Mapping of input space to high-dimensional feature space [4]

3 Related Work

There are many machine learning methods for classification purpose and SVM is popularly used for different kinds of classification and documented as the best classification algorithm [2, 5, 6]. The best training characteristic of SVM is implemented by SMO that helps in finding an optimal hyperplane and hence results in highly accurate classification in most applications. In this paper, SVM is used for web page classification and features are extracted from the content of web page.

Joachims [5] used the technique in which documents are transformed to strings of characters. Information gain is the criterion used to select subsets of features. It analyses the properties of learning with text. SVM attains the considerable enhancements over the best-performing methods and results in a vigorous manner over a variety of many learning tasks.

Basu et al. [6] compared different algorithms used as text classifiers, classifying news items and identifying a reduction in feature set that helps to improve the results. It is observed that artificial neural network is more complex in terms of computation than SVM algorithm.

Kan et al. [7] used URL features like length, orthographic features, sequential Bi-, Tri-, 4-grams, URI components, entropy reduction for web page classification. Resulting feature is used in supervised maximum entropy modelling. The research says that lower the entropy more meaningful URL will be found.

Chen et al. [2] proposed a web page classification model which consists of two methods, i.e. latent semantic analysis (LSA) and web page feature selection. These methods are used to extract semantic and text features. To improve the performance factor, they have used feature selection criteria and a similarity measure and its evaluation. It works for both small and large data sets. The problem of linear inseparability can be resolved by selecting an appropriate kernel function.

Wang et al. [8] proposed a focused crawler based on naïve Bayes to find the relevant pages according to the research. They use reinforcement learning to train the crawler and naïve Bayes classifier is used for evaluating the class of new web page. The importance of the word in link context is calculated using TF-IDF vectorization. It is observed that it has better performance than PageRank crawler. But this focused crawler can only be applied on the small datasets.

Lee et al. [4] proposed a text document classification framework that uses SVM in training phase and Euclidean distance function in the classification phase. This framework has a very low impact on the implementation of different kernel functions and parameter c. C is the parameter that controls the influence of each support vector. The classification decision is based on the category that has the lowest average distance (Euclidean distance) between support vectors and unknown data point. Parameter C does not have a great impact on SVM because each feature is unique.

Selvakumar et al. [9] proposed technique that increases the efficiency of the crawler by using the anchor text of links and by checking the revisit policy. This technique is able to manage large spaces of features and high generalization ability.

In result, this makes the SVM more complex that in turn demand for high time and memory ability.

Shafiabady et al. [10] describe a methodology that uses self-organizing maps (SOM) and alternatively does the clustering by using the correlation coefficient (CorrCoef). They are eliminating the effect of curse of dimensionality. SOM and CorrCoef are used for organizing and labelling the unlabelled data. The proposed clustering technique is able to match the actual human data with a high degree for accuracy.

Several research gaps observations have been made through the literature review, few of them are discussed here. Traditional crawling methods require huge amounts of time and cost. In web page classification, to reduce the dimensionality of feature space, there is always a need to select best feature subsets. Most of the researchers have worked on small datasets. The classified model should work in such a way that it categorizes the entailed web pages in an effective manner such that the desired web pages can be extracted time efficiently. This optimizes the existing models and classifies web pages effectively. Therefore, the main objective of this paper is to propose a framework for web page classification that uses SVM-based focused crawler model.

4 Proposed SVM Web Page Classification Model

Various Indian universities associate with Indian academicians working for universities across the globe. Generally, when searching for the names of these Indian academicians from a domain, users are engrossed in particular web pages/topics within that domain, such as Harvard University domain has web pages of faculty, Ph.D., or alumni, events, curriculum and student details [11]. The users are mostly interested in faculty, Ph.D. and alumni web pages. However, searching specific names from aforementioned web pages takes a lot of time. Thus, to lessen the time, proposed approach classifies the desired topics/web pages in a particular domain.

The proposed approach aims the web page classification using SVM-based focused crawler. The workflow of the proposed approach is shown in Fig. 4. It is divided into two modules:

4.1 URLs Screening

Crawled URLs of particular university are taken as input. All the URLs are being preprocessed and learned under the algorithm. Features are extracted from URLs' text by finding TF-IDF values and treated as training input for SVM classification system. Then, the classification decision-making modules classify the URL into two categories, i.e. relevant URLs and irrelevant URLs. Relevant URLs are related to

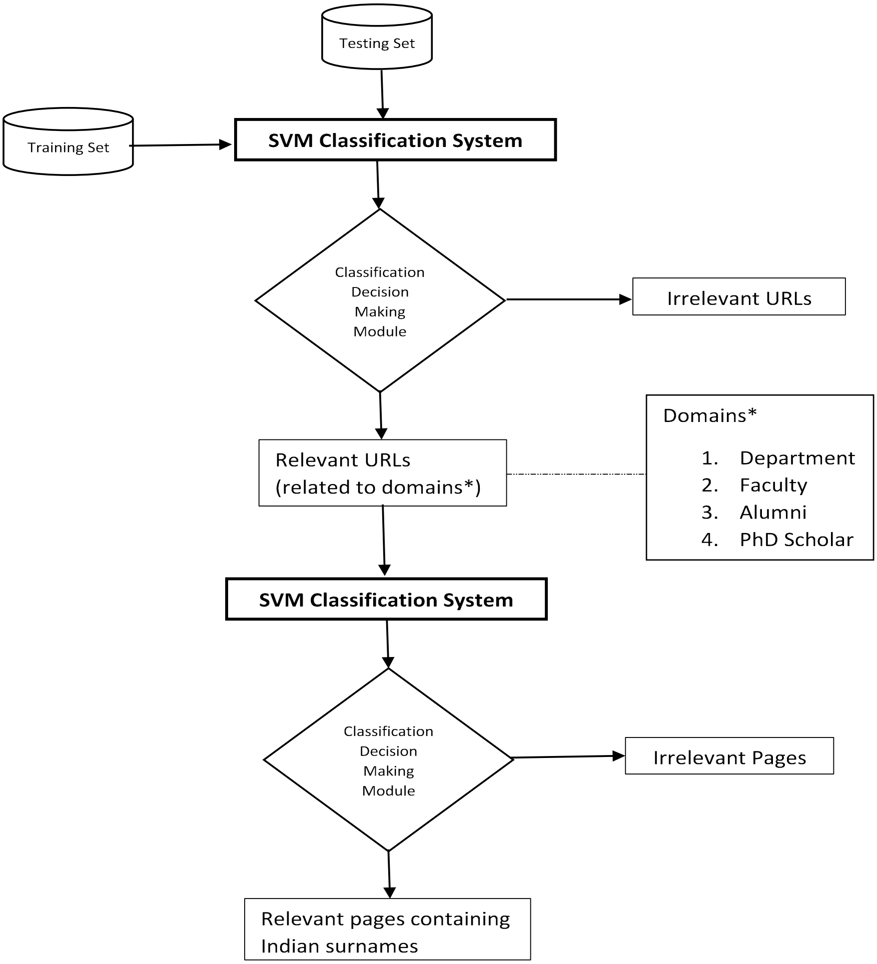

Testing Set
Training Set
SVM Classification System
Classification Decision Making Module
Irrelevant URLs
Domains*
1. Department
2. Faculty
3. Alumni
4. PhD Scholar
Relevant URLs (related to domains*)
SVM Classification System
Classification Decision Making Module
Irrelevant Pages
Relevant pages containing Indian surnames

Fig. 4 Workflow for the proposed model

certain domains like department, faculty, alumni, Ph.D. scholars, whereas irrelevant URLs are the remaining ones. Algorithm 1 illustrates the algorithm of the URL screening approach.

Algorithm1. Algorithm for URL Screening

```
Input: URLs list of university u, Labelled data lb
Output: list of URLs related to faculty
for each URL u in the given list do   //Preprocessing Phase
        Tokenize (u);
        Stemming (u);
        Final_token = Remove_stopwords (u);
If (final_token in Bag_of_words) do  //Labeling
        Label_URL = 1
Else do
        Label_URL = 0
For each Labelled data ld in the list of URLs do  //Learning Phase
        Apply filtered classifier (ld)
        Apply SVM classifier (ld)
          X_train, X_test, y_train, y_test = cross_validation.train_test_split(X, y, test_size=0.2)
          Classifier = SMO
          Classifier.build (ld)
          Classifier.fit(X_train, y_train)
        Train_URLs(ld)
for each new URL u in the given list do   //Prediction Phase
       Repeat the preprocessing phase for u
       Use the saved model for the prediction.
```

Algorithm 2. Algorithm for Web page classification

```
Input: list of filtered URLs u, list of names fetched_names, cross validation data
Output: list of URLs containing Indian names
for each URL u in the given list do  // Preprocessing Phase
        Tokenize (u);
        final_token = Tagging (u);
if (final_token == "PERSON") do
                create list as fetched_names
for each fetched_names in list do
        if (fetched_names NOT in dictionary) do
                create list as modified_names
for each modified_names in surnames_list do     // Labelling
        if (modified_names in surnames_list) do
                Label_URL = 1
        Else do
                Label_URL = 0
For each Labelled data ld in the list of URLs do  // Learning Phase
        Apply filtered classifier (ld)
        Apply SVM classifier (ld)
          X_train, X_test, y_train, y_test = cross_validation.train_test_split(X, y, test_size=0.2)
          Classifier = SMO
          Classifier.build (ld)
          Classifier.fit(X_train, y_train)
          accuracy = clf.score(X_test, y_test)
        Train_URLs(ld)
for each new URL u in the given list do  // Prediction Phase
       Repeat the preprocessing phase for u
       Use the saved model for the prediction.
       Use the saved model for the prediction.
```

4.2 Web Page Classification

All the screened URLs are considered as seed URLs for further module. Now, seed URLs are being preprocessed and learned under the SVM algorithm. Firstly, web page content is extracted and this content is tagged so as to find names from the web page. Then, extracted names are matched with list of Indian surnames. All these filtered names are processed and converted into numeric by finding each TF-IDF values. Then, these are considered as features and they are trained under SVM classification system. Afterwards, the classification decision-making modules classify the URL into two categories, i.e. relevant pages and irrelevant pages. Relevancy of a page is considered when Indian name is found in a web page. Algorithm 2 illustrates the algorithm of the web page classification approach.

The proposed approach involves SVM classification system that consists of three phases: preprocessing phase, learning phase and prediction phase. These phases are described in further section. Section 5 elaborates the working of all phases in brief.

5 SVM Classification System

The proposed workflow of SVM classification is shown in Fig. 5. It is divided into three phases:

5.1 Preprocessing Phase

Before extracting features of webpage, preprocessing of web page should be performed. Preprocessing phase consists of removal of HTML tags, tokenizing of words and stemming.

Removal of HTML tags. Mostly, web pages are formulated in HTML. HTML has open and closed tags represented by '<' and '/>'. They create the hindrance in analysis. Therefore, HTML tags were removed to prevent interference and text is retained where needed.

Tokenization. Tokenization of words is done over the text extracted from webpage content. After tokenizing, the following operations are performed:

- Some of the repetitive words are considered as stop words. Stop words like a, an, the, of, is, am, are and many more. They increase the data size and increase the processing time. To avoid this, stop words are removed where required.
- It reduces the inflected words as many of them have the same meaning and are repeated and increases the data set size. To avoid this, stemming of words are performed where and when required. For example, graduates, graduating reduces to graduate, and applies, applying, apply, applied all reduces to apply.

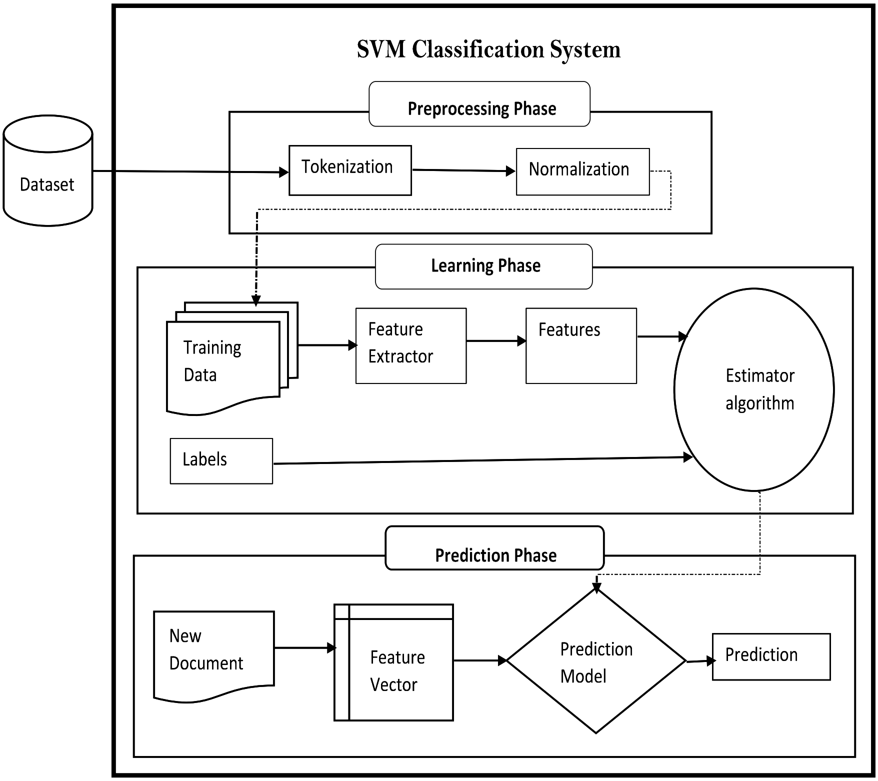


Fig. 5 SVM classification system framework

Tagging. After tokenizing, all words are tagged as proper noun, singular (NNP), predeterminer (PDT), adverb (RB), verb (VB) and many more. Tagging is performed to find names easily which comes under person tag.

5.2 *Learning Phase*

After processing of data, these tokens are used for labelling. Labelling is done by comparing them with some bag of words. Bag of words contains important words related to department, faculty, alumni, post-graduates and many more. Then, system gathers web pages' content for features. These features include number of keywords, frequency of a word in a document, TF-IDF vector of these words. This processed data is given to filtered classifier as input. Under filtered classifier, SVM classifier is applied to train the processed data.

5.3 Prediction Phase

When a new document has to be predicted, again its features are extracted accordingly. Using the prediction model (estimator algorithm), prediction is performed.

6 Result Analysis

This section narrates the design experiment of the model to test the performance of SVM web page classification. The experiments are reported below:

6.1 Experiment Environment

The experiment uses Core i5 2.50 GHz computer with 4 GB RAM. Input is generated using python language on Windows 8.1 Professional operating system. The lexicon is stored in text format. A tool, Weka, is used for classification. Waikato Environment for knowledge Analysis (Weka) has a group of machine learning algorithms. SVM is implemented using this tool.

6.2 Dataset

Crawled URLs are classified as relevant and irrelevant. These URLs are of foreign universities, i.e. Harvard and Lancaster. The University domain has different interlinked domains like faculty, student, alumni or events related. There is need to classify them according to the need of domains. For the cross validation, there is a random selection of training set and testing set from samples.

6.3 Performance Evaluation

In the experiment, dataset is having four possible outcomes as shown in Table 1. Precision and recall values are analyzed to evaluate the performance of the experiment.

Table 1 Four possible outcomes of classification

	Predicted class		
		System does not classify to correct category	System classify to correct category
Actual class	Does not belong to category	True negative	False positive
	Belongs to category	False negative	True positive

6.4 Result

The foreign university URLs are treated as dataset and used for training and testing purpose. The datasets are processed through the vectorization step that transforms each URL or URL content into numerical format. This representation of dataset in numerical form fulfil the requirement of SVM, since all the machine learning methods require the vector space model and accept only numerical data to perform their tasks. Apart from data transformation, preprocessing steps also reduces the dimensionality of the dataset. The output details of URL screening process is mentioned in Table 2. Although, the final goal is to minimize the intervention of humans in training and classification process. After the screening of some URLs, all the relevant URLs of this classification are the input of next classification module, i.e. web page classification. In this experiment, cross validation is performed using SVM with ten-folds. Confusion matrices are obtained during the web classification process and shown in Table 3 with respect to their datasets. Confusion matrix illustrates the performance of a classification model on the dataset.

At last, web page classification is performed to find URLs containing Indian names or not. The results are shown in Table 4.

Table 2 Four possible outcomes of classification

Dataset	Samples	Class	
	Train	Relevant URLs	Irrelevant URLs
Harvard	10,000	1766	8234
Lancater	10,000	5337	4663

Table 3 Details of cross validation

Dataset	Folds	Confusion matrix
Harvard	10	$\begin{bmatrix} 2628 & 34 \\ 7 & 7336 \end{bmatrix}$
Lancaster	10	$\begin{bmatrix} 1347 & 242 \\ 58 & 3434 \end{bmatrix}$

Table 4 Details of web page classification

Dataset	URLs	Relevant URLs (Indian names found)	Irrelevant URLs (Indian names not found)
Harvard	1766	361	1404
Lancaster	5337	1309	4028

Table 5 Comparison analysis

Dataset	Machine learning	Precision	Recall
Harvard	SVM	0.938	0.846
	Naïve Bayes	0.862	0.828
Lancaster	SVM	0.94	0.94
	Naïve Bayes	0.82	0.78

6.5 Comparative Analysis

Comparative analysis is done over different supervised machine learning algorithms. The best-supervised algorithm is SVM for classification purpose. SVM gives better results compared to naïve Bayes for two datasets as shown in Table 5.

7 Conclusion

This paper discusses the need for creating a database of Indian academicians extracted from foreign universities. For this, SVM classification approach is reported to have good accuracy compared to others. In web page classification, there is a need to select best subsets of features to reduce dimensionality of feature space that will improve the time and efficiency of the classifier. To solve this issue SMO has been implemented on dataset using weka. This gives a fair binary classification in finding web pages having Indian names. The experiments show, this classification approach gives a satisfying precision value. To have more accuracy in the results, there is a need to give large training data set to the algorithm.

References

1. Rungsawang A, Angkawattanawit N (2005) Learnable topic-specific web crawler. J Netw Comput Appl 28(2):97–114
2. Chen RC, Hsieh CH (2006) Web page classification based on a support vector machine using a weighted vote schema. Expert Syst Appl 31(2):427–435
3. Wikipedia, Support Vector Machine. https://en.wikipedia.org/wiki/Support_vector_machine

4. Lee LH, Wan CH, Rajkumar R, Isa D (2012) An enhanced support vector machine classification framework by using euclidean distance function for text document categorization. Appl Intell 37(1):80–99
5. Joachims T (1998) Text categorization with support vector machines: learning with many relevant features. Mach Learn ECML 98:137–142
6. Basu A, Walters C, Shepherd M (2003) Support vector machines for text categorization. In: Proceedings of the 36th annual hawaii international conference on system sciences. IEEE (2003)
7. Kan MY, Thi HON (2005) Fast webpage classification using URL features. In: Proceedings of the 14th ACM international conference on Information and knowledge management. ACM (2005)
8. Wang W, Chen X, Zou Y, Wang H, Dai Z (2010) a focused crawler based on naive bayes classifier. In: Third international symposium on intelligent information technology and security informatics. Jinggangshan, IEEE 2010, pp517–521
9. Selvakumar M, Vijaya A (2014) Design and development of a domain specific focused crawler using support vector learning strategy. Int J Innov Res Comput Commun Eng 2(5)
10. Shafiabady N, Lee LH, Rajkumar R, Kallimani V, Akram NA, Isa D (2016) Using unsupervised clustering approach to train the support vector machine for text classification. Neurocomputing 211:4–10
11. Kumar M, Bhatia R, Ohri A, Kohli A (2016) Design of focused crawler for information retrieval of Indian origin academicians. In: 2016 international conference on advances in computing, communication, and automation (ICACCA) (Spring), IEEE 2016, pp 1–6

Indoor Object Tracking Using Wi-Fi Access Points

Vinit Asher, Hardik Thakkar, Suyog Tambe and Prasenjit Bhavathankar

Abstract With the rise of new analytical methods to track and predict various aspects of our lives, gathering data is as important as ever. The way an object moves indoors is an important aspect in terms of crowd flow management, retail marketing, and security fields. Wi-Fi has become a ubiquitous standard with almost every indoor space having some form of Wi-Fi device. This existing infrastructure is put into service to track an object based on received signal strength values. Received signal strength values from different access points form a unique fingerprint which can be used to recognize a location on the map. In order to make the system adaptive to change and drift in fingerprints, deep learning methods are used to convert the system from a static to a dynamic system. The proposed neural network model has the error of 1.3 m for predicting the x-coordinate and 1.8 m for the y-coordinate in the given experimental setup.

1 Introduction

Global positioning system (GPS) has become the de facto standard for providing navigation and tracking services. GPS works well when there is a direct line of sight between sender and receiver. The accuracy of GPS increases as the number of satellites, it gets its signal from, increases. The ultra-high frequency (UHF) signals used by GPS also face disturbances due to other UHF sources. Also, GPS struggles indoors due to the construction materials like concrete not being conducive to transmission

V. Asher (✉) · H. Thakkar · S. Tambe · P. Bhavathankar
Sardar Patel Institute of Technology, Mumbai, India
e-mail: vinitasher1997@gmail.com

H. Thakkar
e-mail: hthakkar8@gmail.com

S. Tambe
e-mail: suyog.tambe52@gmail.com

P. Bhavathankar
e-mail: p_bhavathankar@spit.ac.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_64

of radio signals. Hence, to get a viable solution indoors, alternatives such as cell towers, Bluetooth beacons, ZigBee, and radio frequency identifier (RFID) have been proposed for indoor tracking. But, they each have their own drawbacks and have not managed to find a uniform and consistent way of implementation. However, Wi-Fi is an exciting prospect to fill this gap, as it is already present in most places and characteristics of various Wi-Fi bands are standardized and well defined.

With the advent of data analysis, various insights about object movement inside buildings can be analyzed. More the data is collected about movement patterns inside building, the more improvement can be brought in how the building is designed. Especially, commercial spaces can have huge advantages from a system to track people indoors. Navigation inside commercial spaces has potential of giving better visibility to all shops regardless of their location. How people move inside building can also give a better idea on which shop locations are more lucrative, and which advertising locations can get most exposure. As an attempt to make the surroundings more inclusive to differently abled people, an indoor positioning system can help them navigate easily inside large buildings. Assets can also be tracked inside the building, to prevent their theft and easy location of the asset. Home automation is also a use case for indoor tracking system.

The amount of variation in type of indoor environments which can be encountered is one of the hurdles in designing such a system. Indoor environments are always changing, density of crowd changes depending on time of the day; similarly, the layout of the floor can be changed over time too. Since behavior of Wi-Fi signals varies in different environments, with signal attenuation and multi-path fading playing a major role in defining the signal strength at a particular location, it is difficult to predict how these changes will affect the signal received at a indoor location.

Along with accuracy of the indoor tracking system, effort must also be taken to make it as unobtrusive as possible and as intuitive as possible.

Machine learning has been applied to areas where an inherent pattern can be explored and used in efficiently solving a problem. A case can be made for using machine learning techniques to classify current location of object from the signal values reported or to use a neural network to predict the current location.

This paper is divided into sections as follows, Sect. 2 gives a concise idea about related research which has been performed for indoor object tracking. Section 3 contains the proposed system where the problem at hand is formulated. Section 4 contains the results and Sect. 5 concludes the paper.

2 Related Work

Object tracking problem has been approached in many different ways, with methods differing in terms of how they approach the three major components of any tracking system, technology used for tracking, representing the environment in the system, and calculating current location.

Choice of technology depends on environment as well as cost factors. LANDMARC proposed in [1] used active RFID tags as reference points while calculating current location. It tries to overcome the problems of traditional RFID reader by performing scans at eight power levels. However, the latency is traded for accuracy with the system requiring more time to detect the accurate location. Also, RFID suffers from high disturbances in case of environments with large quantities of metal. Bluetooth is another choice due to its popularity in consumer electronics. In [2, 3], authors have made a case for low-energy Bluetooth beacons to be used for indoor location tracking given their popularity and low-energy needs. Bluetooth requires lower power than Wi-Fi at the mobile node. However, Bluetooth requires dedicated beacons which only serve one purpose. It is a trade-off between power and versatility. [4–6] show the variety in which Wi-Fi-based indoor localization system can be made. Not only are the aforementioned systems accurate, they do so while utilizing the existing hardware. Wi-Fi has a higher range than most other alternatives. [7] formulates the number of reference points required for a stable RSS reading depending on obstructions which are expected to be present in environment. Among findings in [8], it is shown that multiple APs working on same frequency do not have a negative effect on the reading. Hence, having a dense network of APs is possible. The existing infrastructure availability is the major advantage Wi-Fi has over competing techniques.

Generally, to represent the environment, two categories of solution can be used either a fingerprint-aided system or a purely model-based system. Fingerprinting, a process by which a unique value is associated with a location on a map, has been widely used in indoor tracking systems. The location fingerprints are collected by performing a site survey of the received signal strength (RSS) from multiple access points (APs). The entire area is covered by a rectangular grid of points. The RSS is measured with enough statistics to create a database or a table of predetermined RSS values on the points of the grid. The vector of RSS values at a point on the grid is called the location fingerprint of that point [9]. In [10], authors have surveyed a collection of various mathematical models which can be used to track an object. Features of received signal like angle of arrival, time of flight, and time difference of arrival help determine where the object is currently.

K-nearest neighbors (KNN) is a popular algorithm which relies on the online RSSI to obtain the ‘k’ nearest matches (on the basis of off-line RSSI measurements stored in a database) of the known locations using root mean square error (RMSE) [10]. But the good performance of KNN is highly dependent on the metric used for computing pair ware distances between data points [11]. Trilateration determines the position of node from intersection of 3 circles of 3 anchor points that are formed based on distance measurements between its neighbors [12]. However, trilateration requires more than 3 anchors for getting a confident prediction. More recently, 802.11mc Wi-Fi standard has added round trip time (RTT) support which is based on finding distance from APs based on time required for a packet to complete one trip between AP and mobile. Artificial neural networks (ANN) are also fit for this task as shown in [13, 14]. With availability of deep learning libraries for deployment on mobile devices, neural networks have potential of providing high accuracy in dynamic environments.

3 Proposed System

In the following section, the proposed object tracking system to find the location of user based on the RSSI values from the available access points is described.

3.1 System Block Diagram

Figure 1 shows the block diagram of proposed system. A Wi-Fi enabled object is at the core of the system. The object collects the RSSI values from various APs. The object is connected to either Intranet or Internet from where it can fetch the map data. For the initial call, to select the map, current RSSI readings are sent to the server. Once the map is downloaded with the pre-trained model of the floor, the object itself can calculate its current position. Current position is calculated by passing the current RSSI readings into the neural network model.

3.2 Off-line Fingerprinting and Database Description

The off-line phase is very crucial step of the process as it is required to collect the data for training the system to predict the actual location of the user in real time. In the off-line fingerprinting phase, the system has to be calibrated with respect to a single AP considering it as an origin. The RSSI values from different AP's are recorded automatically and the coordinates (x, y, z) are stored with respect to the point which is calibrated as origin. This process of taking reading has to done continuously till the complete area of interest is covered at least once. This process is very tedious and to amplify the performance, the readings at a certain point are taken multiple times by taking the readings from the AP's automatically. These extra scans for RSSI values at the same point help in training the model well and reduce the error in predicting the position of object accurately. The Dataset is created by all these RSSI values which

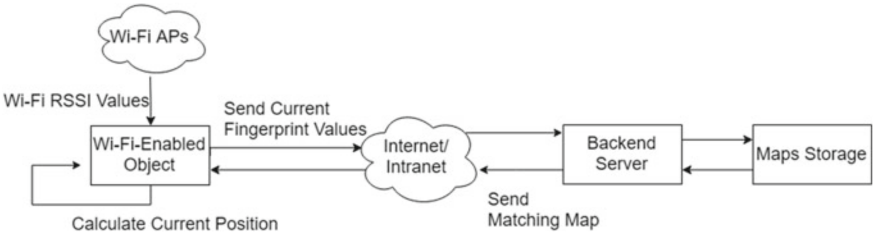


Fig. 1 System block diagram

are collected by fingerprinting this dataset is then used to predict the coordinates of the receiver in real time. The dataset has the following attributes—

X—The x-coordinate based on the grid

Y—The y-coordinate based on the grid

Z—The z-coordinate (basically the floor number)

AP's—RSSI from different access points.

The data from all the AP's is saved in separate columns.

Some preprocessing is required on this dataset as there are various factors which affect the RSSI values. One common issue which is faced is the RSSI values are negative values which converge toward 0 as the distance between the AP and the receiver decreases. Also, during fingerprinting, if the AP is far away or signal strength is reduced due to obstacle between the receiver and AP it is possible that the receiver saves 0 for such values. This causes problem if no preprocessing is done. Ideally, even if the Euclidean distance between the AP and the receiver is 0 the RSSI never becomes 0 it is always negative. Thus, to clean the dataset, zeros in the dataset are replaced by 100. This value is arbitrary and signifies that no signal was received at that location from a particular AP [15]. These steps have to be completed before proceeding to feed the neural network with the RSSI values from all the AP's.

3.3 Regression Using Deep Neural Network

The main idea is to implement regression on the data and predict the actual position of the user with respect to the grid at given point of time. The received RSSI values at any location are used to predict the x, y, and z coordinates based on the grid in real time. After the data is preprocessed, the RSSI values from the access points are feeded to the neural network as shown in Fig. 2. The neural network shown gives the coordinate value as the output and thus there are three similar networks for all

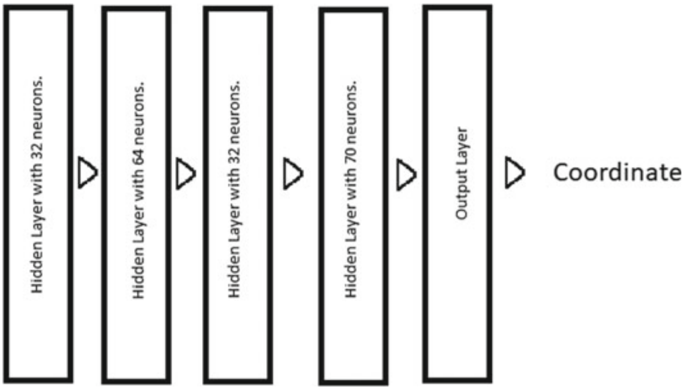

Hidden Layer with 32 neurons.
Hidden Layer with 64 neurons.
Hidden Layer with 32 neurons.
Hidden Layer with 70 neurons.
Output Layer
Coordinate

Fig. 2 Neural network used in the model

the axes. All the axes are trained separately with the RSSI values and thus it is the network with 1 input layer, 5 hidden layers, and 1 output layer for each axis. The deep neural network used for regression has variable number of input layers. This number is dependent on number of access points used to design the system (This varies from system to system based on requirement). The output layer consists of the 1 output neuron with linear function. This structure is same for all the axes. Each hidden layer is a dense layer and thus all the neurons in the layer get the input from all the previous layers. There are a total of 5 hidden layers with 32 and 64 neurons alternatively. The final hidden layer has 70 neurons. The output layer has a linear activation (as regression is done) and a single neuron to predict the value of the coordinates.

All the hidden dense layers have the advanced leaky rectifier linear unit (‘LeakyReLU’) as the activation function which helps in mapping between the input and the output variables.

3.3.1 Mathematical Analysis Deep Neural Network

Activation function—LeakyReLU or leaky rectified linear unit is used for the system. It is the advanced version of the rectifier linear unit. Both these functions are explained in detail later in the section. The primary purpose of the activation function is to add nonlinearity to the model and learn from previous results. The process of backpropagation [15] is possible because activation functions update the weight and the bias depending on the output of the previous losses.

Mathematically, rectified linear unit (Fig. 3) is given by—

$$F(a) = max(0, a) \tag{1}$$

Fig. 3 Rectifier linear unit (RELU)

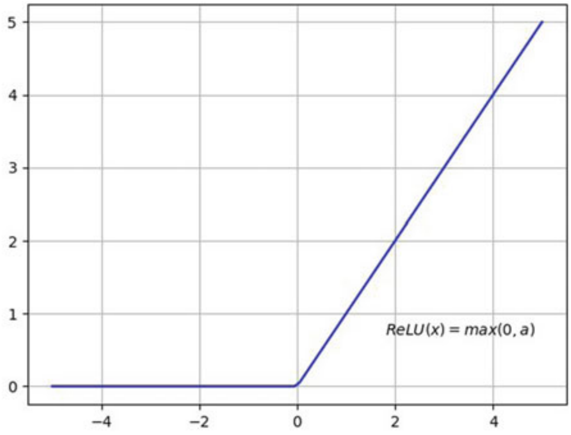
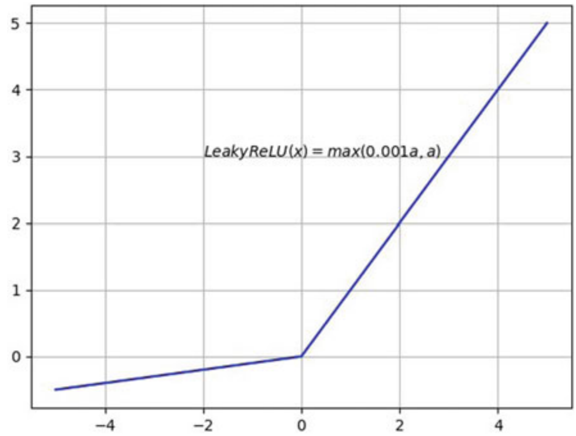


Fig. 4 Leaky rectifier linear unit (LeakyReLU)



$$F(a) = \begin{cases} 0, & \text{if } a < 0. \\ a, & \text{otherwise.} \end{cases} \tag{2}$$

$$\text{Range:}[0 \quad \text{to} \quad \infty)$$

$F(a)$ is the RELU Function.

Along with the simplicity, there is also a drawback of this function—it may sometime render a neuron dead. There could be a certain weight update that could possibly cause the neuron to deactivate forever and thus a better version of RELU, that is, the LeakyReLU is used in the system. Figure 4 represents the LeakyReLU.

Mathematically, Leaky rectified linear unit is given by—

$$F(a) = max(\delta a, a) \tag{3}$$

$$F(a) = \begin{cases} \delta a, & \text{if } a < 0. \\ a, & \text{otherwise.} \end{cases} \tag{4}$$

$F(a)$ is the LeakyReLU function

Delta (δ) here is a small constant (0.001). This small value increases the range for rectified linear unit to

$$\text{Range} : (-\infty \quad \text{to} \quad \infty).$$

LeakyReLU has proved to be much reliable in recent times. Also, RELU or its variants are used because they generally converge faster [15].

Optimization function—This function generally help to minimize or maximize the error function which is a function that depends on the models parameter use to fit the training data to receive the line of best fit (considering the regression problem in this system). The proposed system uses the 'RMSprop' optimizer, this is very similar to the gradient descent with momentum but the calculation of the gradient varies in the two approaches. The RMSprop reduces the vertical fluctuations, which helps us to reach the global minima faster.

The updates done by RMSprop for each parameter are done by the following equations.

$$v_t = \lambda v_{t-1} + (1 + \lambda) * G_t^2 \tag{5}$$

$$\Delta w_t = -\frac{\gamma}{\sqrt{v_t + \epsilon}} * G_t \tag{6}$$

$$w_{t+1} = w_t + \Delta w_t \tag{7}$$

λ is hyperparameter generally set to 0.9, It has to be tuned as needed.

γ is the initial learning rate.

w_t is the weights at time t.

G_t is gradient at time t.

v_t is exponential average of square of gradients. The epsilon (ϵ) is used so that the equation is never accidentally divided by zero. Also, as seen RMSprop indirectly works like simulated annealing.

The loss or error function—In case of regression the error function generally used is 'MSE' which stands for mean squared error. A quality of a machine learning model is determined by the value returned by the loss function. If the value is high means there is a lot of deviation in the predicted value when compared to actual value. There are many types of loss functions which can be used. The proposed system uses mean squared error (MSE) and mean absolute error (MAE).

As the name suggests the mean squared error is the mean of squares of difference between actual value and predicted value.

The mean absolute error is the mean of absolute values of the difference between the predicted values and actual values.

4 Results

The regression algorithm used in system for predicting the position and metrics like MSE and MAE were used to check the validity of the model the results of which are tabulated in Tables 1 and 2.

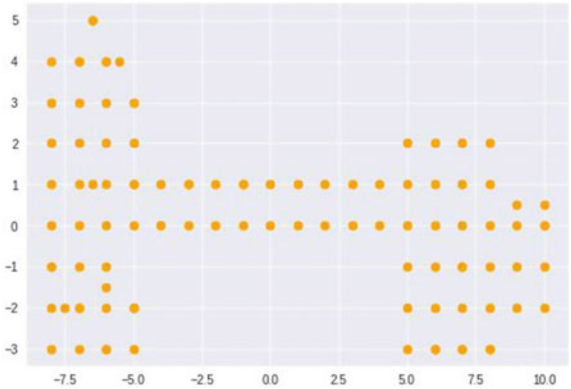
Table 1 Mean square error

–	Validation loss	Training loss
X-coordinate	1.3 m	0.82 m
Y-coordinate	1.8 m	1.85 m

Table 2 Mean absolute error

–	Validation loss	Training loss
X-coordinate	0.96 m	0.67 m
Y-coordinate	1 m	0.922 m

Fig. 5 Floor plan

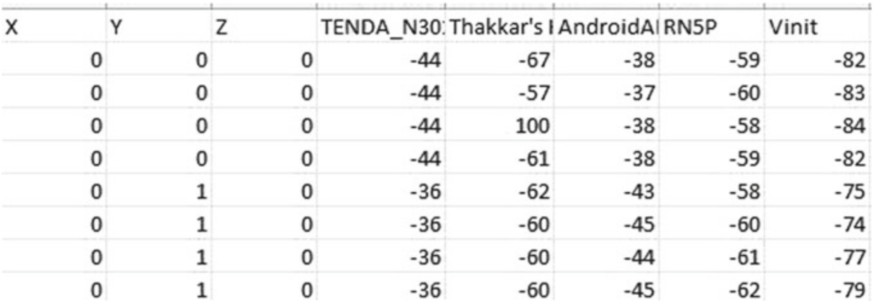


These results are based on readings taken in Sardar Patel Institute of Technology, Mumbai. The complete details of the experiment are further explained.

The RSSI values were collected by using an android device with a personalized application which had the features of scanning for access point and storing the basic service set identifier (BSSID) for getting the RSSI values from it at the different locations. The experiment was done with a total of five access points. One access point was considered as the origin and all the values for the position of the user were taken with respect to the origin. The floor was divided into the grid of 0.5 m x 0.5 m squares and fingerprints from these five access points were recorded at several different locations within the area of concern. Figure 5 illustrates the example of the floor plan (Area of concern).

The data was then collected manually by going to different coordinates of the grid (yellow dots in Fig. 5) and take readings for RSSI values at those points. The final dataset generated had a total of eight columns—X, Y, Z*, AP1, AP2, AP3 and about 400 tuples. The number of columns is generally variable as it is based on the number of access points that are configured to determine the location of the user. Here, five APs were used to find the position, this number is arbitrary and may vary depending on the size of the area to be covered and accuracy expected for determining the position of the device in space.

Initially, dataset contained many null RSSI values due to weak signal strength and also due to the incapacity of the receiver to continuously scan for the access points. Both these issues were solved to some extent by the idea of automatically taking a number of readings at the same location and preprocessing the dataset as explained previously in 3.2. Figure 6 shows the structure of the dataset. In the final step of the preprocessing stage, the data is split into train and test set in the ratio of 8.5:1.



X	Y	Z	TENDA_N30:	Thakkar's I	AndroidAI	RN5P	Vinit
0	0	0	-44	-67	-38	-59	-82
0	0	0	-44	-57	-37	-60	-83
0	0	0	-44	100	-38	-58	-84
0	0	0	-44	-61	-38	-59	-82
0	1	0	-36	-62	-43	-58	-75
0	1	0	-36	-60	-45	-60	-74
0	1	0	-36	-60	-44	-61	-77
0	1	0	-36	-60	-45	-62	-79

Fig. 6 Dataset

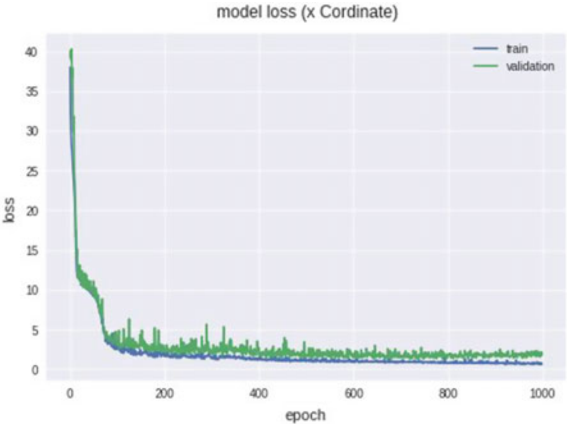


Fig. 7 Loss function (x-coordinate)

***Note**—z was kept constant throughout the experiment as it signifies the floor number and experiment was performed on a single floor. And thus, all the values of column z are 0. The model was not trained for z-coordinate in the experiment.

After the split, the model was compiled and fitted to get the best curve to predict the location. In the training process, hyperparameter tuning resulted in different parameters for training the neural network for x- and y-coordinate. The training of x-coordinate was done with 1000 epochs and batch size of 21 to get the best loss value for the testing and the training dataset. Figure 7 shows the error reaching to 0 for both test and train set at 1000 epoch.

For the y-coordinates, the parameter is different only 195 epochs with batch size 18 were needed to reach the least error value. Figure 8 shows the error function.

The testing data along with the predicted data is plotted in Fig. 9. The orange dots are the points where data was collected. Green points are the testing data and the blue points are the points predicted by the model.

The MSE and MAE which were calculated using this network are being used as evaluation metrics. The validation loss is the equivalent loss obtained on the test set when the best loss value is calculated on the train set. Whereas, loss on the training

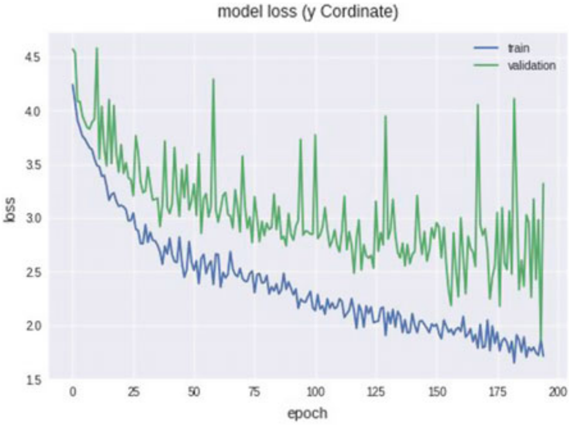


Fig. 8 Loss function (y-coordinate)

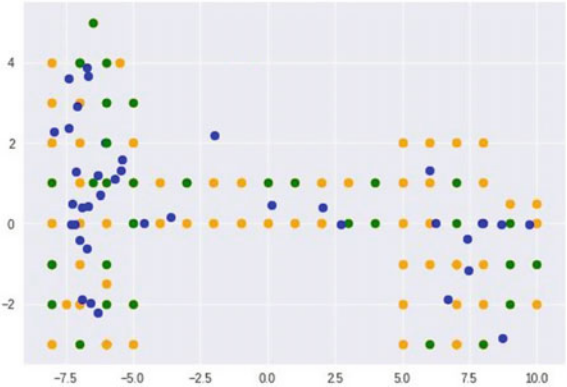


Fig. 9 Actual versus predicted location

set is also mentioned in the table these are the losses found when the best weights are found for the network.

5 Conclusion

As described in the table above, this model can be used to predict the location. The co-relation between the number of AP, their position, and accuracy is still uncertain and can be found in the future experiments. The system can be modified for various use cases blind navigation, crowd flow management, warehouse management, etc. The system further will be updated to have a grid-based agent trained by reinforcement learning.

References

1. Ni L, Liu Y, Lau YC, Patil A (2003) LANDMARC: indoor location sensing using active RFID. In: Proceedings of the first IEEE international conference on pervasive computing and communications. (PerCom 2003). IEEE Computer Society
2. Faragher R, Harle R (2015) Location fingerprinting with bluetooth low energy beacons. IEEE J Sel Areas Commun 33(11):2418–2428
3. Noertjahyana A, Wijayanto IA, Andjarwirawan J (2017) Development of mobile indoor positioning system application using android and bluetooth low energy with trilateration method. In: 2017 international conference on soft computing, intelligent system and information technology (ICSIIT). IEEE
4. Kumar S, Gil S, Katabi D, Rus D (2014) Accurate indoor localization with zero start-up cost. In: Proceedings of the 20th annual international conference on mobile computing and networking - MobiCom '14. ACM Press
5. Vasisht D, Kumar S, Katabi D (2016) Decimeter-level localization with a single wifi access point. In: 13th USENIX symposium on networked systems design and implementation (NSDI 16). USENIX Association, Santa Clara, CA, pp 165–178
6. Xiong J, Jamieson K (2013) Arraytrack: a fine-grained indoor location system. In: Presented as part of the 10th USENIX symposium on networked systems design and implementation (NSDI 13). USENIX, Lombard, IL, pp 71–84
7. Husen MN, Lee S (2016) Design guideline of wi-fi fingerprinting in indoor localization using invariant received signal strength. In: 2016 international conference on information and communication technology (ICICTM). IEEE
8. Kaemarungsi K, Krishnamurthy P (2004) Properties of indoor received signal strength for WLAN location fingerprinting. In: The first annual international conference on mobile and ubiquitous systems: networking and services. MOBIQUITOUS 2004. IEEE
9. Kaemarungsi K, Krishnamurthy P (2004) Modeling of indoor positioning systems based on location fingerprinting. In: IEEE INFOCOM 2004. IEEE
10. Zafari F, Gkelias A, Leung KK (2017) A survey of indoor localization systems and technologies. CoRR
11. Liang X, Gou X, Liu Y (2012) Fingerprint-based location positioning using improved knn. In: 2012 3rd IEEE international conference on network infrastructure and digital content, pp 57–61
12. Asmaa L, Hatim KA, Abdelaaziz M (2014) Localization algorithms research in wireless sensor network based on multilateration and trilateration techniques. In: 2014 third IEEE international colloquium in information science and technology (CIST), pp 415–419
13. Hwang R, Hsu P, Cheng J, Chen C, Chang C, Huang H (2011) The indoor positioning technique based on neural networks. In: 2011 IEEE international conference on signal processing, communications and computing (ICSPCC), pp 1–4 (2011)
14. Tuncer S, Tuncer T (2015) Indoor localization with bluetooth technology using artificial neural networks. In: 2015 IEEE 19th international conference on intelligent engineering systems (INES), pp 213–217
15. Torres-Sospedra J, Mendoza-Silva GM, Montoliu R, Belmonte O, Benitez F, Huerta J (2016) Ensembles of indoor positioning systems based on fingerprinting: simplifying parameter selection and obtaining robust systems. In: 2016 international conference on indoor positioning and indoor navigation (IPIN). IEEE

Crime Analysis and Prediction Using Graph Mining

A. G. Sreejith, Alan Lansy, K. S. Ananth Krishna, V. J. Haran and M. Rakhee

Abstract Crime investigation and counteractive action is a deliberate methodology for distinguishing and examining examples and patterns in crime. Our framework can foresee regions which have a high likelihood for crime event and can predict crime-prone regions. With the expanding approach of mechanized frameworks, crime information investigators can help the law authorization officers to accelerate the way toward identifying violations. Utilizing the idea of information mining, we can extract beforehand, uncertain valuable data from unstructured information. Crimes are a social aggravation and cost our general public beyond all doubt in a few different ways. Any study that can help in explaining crime quicker will pay for itself. About 10 percent of the criminals carry out about half of the violations. Here we utilize graph mining techniques for gathering information to distinguish the crime instances and accelerate the way toward enlightening crime. Graph mining is done with the help of identifying the structure of the graph to obtain frequent patterns of information. With the help of graph database, we could store the past criminal records and infer important information from it. Our project aims to store the data in a graph database and try to determine the important patterns on the graph which can be used to predict the regions which have a high probability of crime occurrence and can help the law enforcement officers to enhance the speed of the process of solving crimes.

Keywords Graph mining · Crime analysis · Graph database · Neo4j

1 Introduction

Graph mining is employed to find helpful patterns from a piece of graph-structured information. The graph contains a set of nodes interconnected using edges which might be used to show the relation between the information and entities. Graphical illustration of any information provides an additional convenient and effective way

A. G. Sreejith · A. Lansy · K. S. A. Krishna · V. J. Haran (✉) · M. Rakhee
Muthoot Institute of Technology and Science, Kochi, India
e-mail: haranvj1997@gmail.com
URL: http://www.mgmits.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_65

to analyze the relationship between the data and entities using graph mining. We extract patterns from the graph through which we can analyze the contents and get useful data from it. For performing the graph mining, we first need to create a graph database of existing records. For creating the graph database, we can use many graph database platforms. We are using Neo4j as it is easy to use and provide drivers for many languages and have very good cypher query language. After creating the graph database, we need to extract the data from it using the API of the database to perform the analysis. Here, we are using R programming language for graph analysis as it is simple and easy to use and have many predefined packages for graph analysis like igraph in which we can find out frequent patterns and perform different centrality measurements for finding frequent crimes, crime-prone areas, and major people influencing in the crimes.

2 Crime Analysis and Graph Mining

Graph mining is the process of finding out frequent subgraphs present in the input graphs and finding useful information from it. Graphs are easy to understand, and mining using graphs is more efficient and faster than normal data normal statistical mining methods. Analysis is done by finding the frequent patterns and by analyzing different centrality measurements. Crime data is best suited to be represented as a graph as it contains different relationships among the data entities like people, incidents, vehicles, etc., and relations are there in the data which forms a complex graph patterns when represented as a graph, and we can perform analysis on it easily for getting the useful data out of it.

2.1 Advantages of Using Graph Mining

The techniques based on graph mining are effective and efficient in comparison with the other statistical data applications. It has a wide range of applications in the regions of law requirement, e-advertising, health and medical industry, educational training, bio-informatics, agriculture, and so on.

2.2 Disadvantages of Using Graph Mining

With greater advantages of graph mining, it also have some disadvantages like as the data grows, the mining algorithms should be as efficient as to quickly process the data, graph mining is in its early stages and the algorithms developed needs more refinement for it to be used with large data, and with datasets with very less number of relationships, graph mining is not very efficient.

3 Familiarization of Tools

3.1 Neo4j

Neo4j is a graph database management system developed by Neo4j, Inc. It is the most popular graph database according to DB-Engines ranking and is the 22nd most popular database overall. [12] In Neo4j, data is stored as nodes and relations between the data as an edge. Each edge and node can be given as many numbers of attributes as needed. Both edges and nodes can be labeled. These labels help to reduce the number of searches. The graph data of Neo4j is stored as record files on the disk. To increase the retrieval speed, it uses the two-layer mechanism of caching, namely file system cache and object cache. Every node holds only their first reference to the relationships. Transaction modules contain a transaction log and transaction management which ensures that transactions are ACID. The system clustering capabilities are characterized by a module called HA module [12].

3.2 R Programming Language

R is a programming language and environment used for statistical computing and graphics. It provides a variety of statistical (linear and nonlinear modeling, classical statistical tests, time-series analysis, classification, clustering) and graphical techniques and is very much extensible. It is a free software. The RStudio IDE is used for R [13].

4 Related Work

Crime data mining uses graph mining techniques for crime analysis. Crimes can be subdivided into many types based on different principles. There are eight crime categories like traffic violations, sex crimes, theft, fraud, arson, drug offenses, cyber crimes, and violent crimes [10].

Various crime data mining techniques are available currently. Some of the most commonly used techniques include entity extraction, clustering techniques, association rule mining, and sequential pattern mining and classification [10].

Criminal analysis methods like hot-spot detection, crime comparison, and visualization of crime patterns are important [10]. A time-series is drawn between the crime frequency and the time in crime pattern visualization, and some interesting crime trends were identified from this. In addition to these steps, some other analysis steps such as crime clock, outbreaks detection, and nearest police station detection were also used [10].

An intelligent crime detection system can be used to predict likely suspects for a given crime. Five types of agents, namely message space agent, gateway agent, prisoner agent, criminal agent, and evidence agent, were used for the same [10]. In countries like England, the Police Department of Cambridge has performed a similar one named Series Finder for determining the patterns in crimes [11].

4.1 Overview of Popular Graph Database

Talking about the graph databases in recent years, there has been a large number of the high-performance graph database environment, such as Neo4j, Infinite, Graph, DEX, InfoGrid, HyperGraphDB, and Trinity. Among all of them, Neo4j is the considered mainstream of a Java-based open-source software. Its kernel is a very fast graphics engine. It supports the recovery, provides two phases of the submission, and supports for XA transactions and other database product features. Neo4j is a network-oriented database, that is, an embedded, disk-based, fully transactional Java persistence engine which stores data structured in networks rather than in tables [12].

5 Proposed Work

Graphs can be used to effectively analyze the data, and we intend to use the graph database to store the criminal data and analyze it to check for different patterns in the graph to show the regions having the high chance of occurrence of crime and visualize the areas having a high crime rate. The first step would be to create a graph database using the existing crime records and then analyze it to show the relevant details. Our system could be used to easily visualize the entire database, identify regions having a high crime rate, identify major criminals or gangs and also, the crime patterns and similar crimes. Finally, we can generate a community graph of criminals and identify their network.

5.1 Architecture Diagram

Figure 1 shows the system architecture, in which the user gives the crime data or queries which then processed by the modules makes the graph database. A graph database is used for further graph mining processes which then yield the necessary output which is then processed by the output processing unit which produces the output which the user needs, which can be shown as graphs or charts.

User inputs the data to the system as a CSV file of the records and can create a database also users can give queries the system to get useful information, data conversation system is used to convert the data to the form which is optimized for

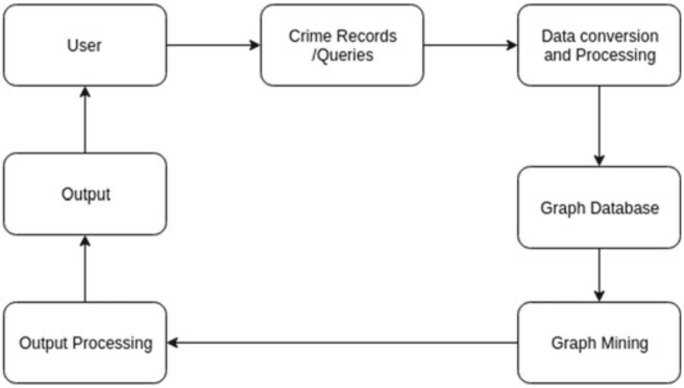


Fig. 1 System architecture

graph analysis. A graph database is used to store the data and to support the graph mining module by supplying data through its API. Graph mining modules are used to analyze the created graph database. Graph mining module will provide the inputs to the output modules which will show the outputs to the user in the form of graphs, charts, or the output to the user query.

5.2 Methodology

A graph database can be created using an open-source platform like Neo4j which is very powerful and has its own query language called cipher to query graph database. Figure 2 shows the data flow diagram of the system in which the input module accepts the input in CSV format which should be processed by the input module to make it to format which can be accepted by the Neo4j for creating the database. With the help of the Neo4j API, we can directly load the data to create the graph database. Here the query from input module is taken by query management unit which converts the normal query to Neo4j's cipher query, queries the graph database, and gets the pattern graph which is then given to subgraph mining unit, which mines the subgraph with pattern matching approach which shows the crimes with the given pattern from the database. Here Neo4j platform is the main module which is used to generate, query, and control the graph database. Clustering is done with the help of R programming language. With the help of clustering, the connection between the crimes and criminal communities can be identified. Centrality measurements consist of mainly two types, namely node centrality and betweenness centrality, which will tell the major type of crimes and who are the major criminals in the area. The result processing unit processes the results and generates the result according to the user query, and output is shown. Graph mining techniques like centrality measurements which include the degree centrality measures can be used to find out the node with maximum direct

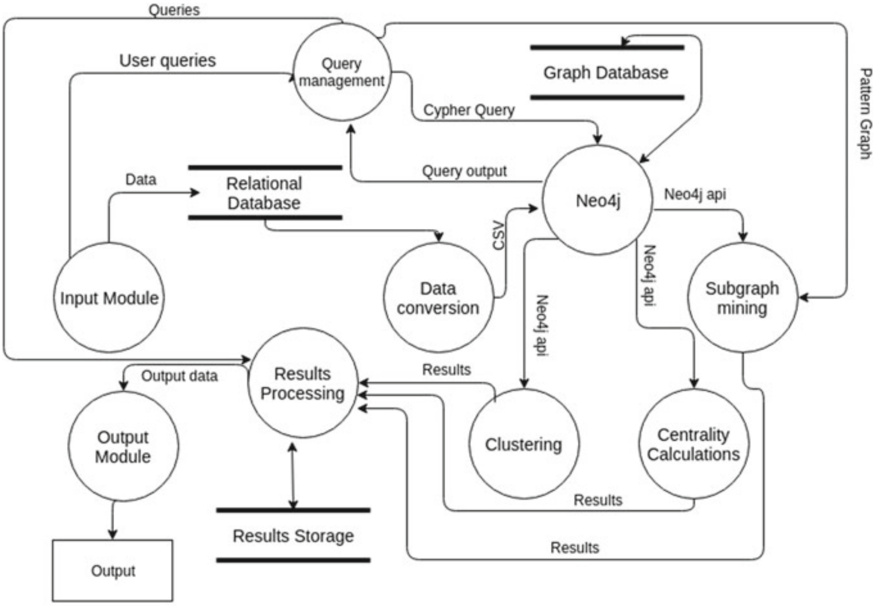


Fig. 2 Data flow diagram

links. Betweenness centrality is the number of times a node occurs on the shortest path between a pair of nodes. In closeness centrality measure, the center of attention is on the closeness of a node in the graph to all the other nodes in the graph. These centrality measurements can be used accordingly to find out the major criminals or gangs. Clustering techniques can be used to cluster the data and show criminal community graph and networks. Subgraph mining can be used to identify the pattern of a crime and find out similar crimes in the database.

6 Conclusion

The number of crimes is increasing day by day, and at the moment, we do not have a mechanism to predict the most possible crimes happening in an area. Each crime has a pattern. Mining patterns from the graph show the foremost possible crime in a region. The techniques used for the processing as well as the prediction of data can improve the performance, speed, and accuracy in the crime prediction process. These procedures will successfully decide regularities in the crimes by breaking down present and past criminal data and foresee future violations.

7 Future Scope

To increase the quality of crime prediction system, one of the enhancements that may be created is to develop the system as a mobile application. This might enable the user to report the crime remotely as shortly as he observes one and eliminates the requirement for a desktop system to report a crime. In future, system can enable the user to register complaints online. Users will read the progress of their criticism online. By the long-run technology, the user will read the case details and progress of the complaints on their mobile phones. Techniques belonging to the information mining and computing field might be incorporated into the system to build the statement method even more practical and economical.

References

1. Kang H-W, Kang H-B (2017) Prediction of crime occurrence from multi-modal data using deep learning
2. Shrivastava S, Pal SN (2009) Graph mining framework for finding and visualizing substructures using graph database. In: 2009 IEEE international conference on advances in social network analysis and mining
3. Tang D, Tan Y (2011) Graph-based bioinformatics mining research and application. In: 2011 IEEE fourth international symposium on knowledge acquisition and modeling
4. Sarvari H, Abozinadah E, Mbaziira A, McCoy George D (2014) Constructing and analyzing criminal networks. 2014 IEEE security and privacy workshops
5. Bogahawatte K, Adikari S (2013) Intelligent criminal identification system. 2013 IEEE 8th international conference on computer science education
6. Xu Y, Mingyang L, Ningning A, Xinchao Z (2012) Criminal detection based on social network analysis. In: 2012 IEEE eighth international conference on semantics, knowledge and grids
7. Ho L-Y, W J-J, Liu P (2012) Distributed graph database for large-scale social computing. In: 2012 IEEE fifth international conference on cloud computing
8. Lu H, Hong Z, Shi M (2017) Analysis of film data based on Neo4j. In: IEEE/ACIS 16th international conference on computer and information science (ICIS)
9. Jain R, Iyengar S, Arora A (2013) Overview of popular graph databases. 2013 IEEE fourth international conference on computing, communications and networking technologies (ICCCNT)
10. Jayaweera I, Sajeewa C, Liyanage S (2015) Crime analytics: analysis of crimes through newspaper articles. Available: 2015 Moratuwa Engineering Research Conference (MERCon)
11. Sathyadevan S, Devan MS, Gangadharan SS (2014) Crime analysis and prediction using data mining. Available: 2014 first international conference on networks soft computing (ICNSC 2014)
12. Huang H, Dong Z (2013) Research on architecture and query performance based on distributed graph database Neo4j. Chongqing University of Posts and Telecommunications
13. R programming [Online]. Available https://en.wikipedia.org/wiki/R

A Semi-supervised Approach to Detect Malicious Nodes in OBS Network Dataset Using Gaussian Mixture Model

Md. Kamrul Hossain and Md. Mokammel Haque

Abstract In this study, we have followed a semi-supervised approach for the classification of optical burst switching (OBS) network traffics generated by the network's edge nodes. We used expectation maximization (EM) technique for Gaussian mixture model (GMM) to obtain a probabilistic classification of the OBS nodes. For this purpose, we used a trustworthy OBS network dataset from UCI machine learning repository. Preprocessing and principal component analysis were applied to the dataset for arranging the data so that GMM can play its role fairly. Only 1% (10 samples) of labeled data from OBS dataset was used to initialize the parameters of GMM and the rest 99% was used for testing performance of the model. We found a maximum accuracy of 69.7% on the test data using just 1% labeled data with the tied covariance type of the constructed GMM. The significance of this result is that it shows the GMM can be used in classification of OBS networks and other similar networks in semi-supervised way when one has very few labeled data and when labeling a huge dataset is not feasible.

Keywords Gaussian mixture model (GMM) · Optical burst switching (OBS) network · Clustering · Semi-supervised learning · Principal component analysis

The original version of this chapter was revised: The corresponding author of this Chapter "Muhammad Kamrul Hossain Patwary" (informal name) has been corrected to "Md. Kamrul Hossain" (official name). The correction to this chapter is available at https://doi.org/10.1007/978-981-15-0146-3_137

Md. Kamrul Hossain (✉) · Md. Mokammel Haque
Department of Computer Science and Engineering, Chittagong University of Engineering and Technology, Raozan, Chittagong, Bangladesh
e-mail: muhammadkamrulhossain@gmail.com

Md. Mokammel Haque
e-mail: mokammel@cuet.ac.bd

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_66

1 Introduction

Optical burst switching (OBS) network [1] is a relatively new networking technology. It combines the optical circuit switching and optical packet switching in one system of data transportation. In summary, in an OBS network, a sending terminal sends a control packet ahead of the actual data packet. The control packet travels through the network and allocates necessary resources for the upcoming data. Once the process is complete, the data packet follows the path reserved by the control packet and reaches to the destination. This system of all optical WDM data transportation, that has opened a new door of multi-gigabit bandwidth utilization is prone to various attacks. One notable attack is burst header packet (BHP) flooding attack. It is a kind of denial of service attack. It happens when an edge node of an OBS network maliciously transmits numerous control packets without sending any associated data packet (also called data burst). As a result, the control packets (also called burst header packets) reserve significant amount of resources which causes a denial of service for other nodes of the network. That is why it is important to detect those malicious nodes who are sending BHP without any associated data burst. Detecting a malicious node in a network by analyzing network traffic is a very rich field of research. Machine learning has been used to classify the traffic of various networks [2]. Since the concept of OBS network is relatively new and it is not widely deployed infrastructure, very few notable works exist regarding classification of OBS network nodes/traffic using machine learning approaches.

Machine learning procedures can be divided into three types: supervised, semi-supervised and unsupervised. In supervised machine learning, a large set of labeled data is used to train and predict the classes. In unsupervised machine learning, unlabeled dataset is trained and distinct clusters/groups are discovered. In semi-supervised machine learning, a relatively small amount of labeled data and a large amount of unlabeled data is used to train and predict the classes/groups of data. Clustering is a type of unsupervised machine learning. Among the available clustering algorithms, Gaussian mixture model [3] is one. In many cases, the distribution of the data in a dataset cannot be represented using a single Gaussian distribution. Rather, a mixture of several Gaussian can be used to represent such distribution. Gaussian mixture model(GMM) is a probabilistic model that attempts to find a mixture of finite number of Gaussian distributions that can model an input dataset. The parameters of that mixture are unknown. GMM uses the expectation maximization algorithm [4] for finding the model's parameters. After learning from train data, it can assign each test sample to the most probable Gaussian it belongs to. GMM has various covariance type, for example, diagonal, tied, spherical, full covariance etc. A Gaussian distribution's covariance matrix and mean determines the length and direction of the axes of its ellipsoid density contours. Four covariance types of mixture model are illustrated in Fig. 1 using a 2D example. In these contour plots of Fig. 1, two components (or clusters) are located at coordinate (0, 0) and (5, 6) with different weights. The diagram shows different covariance types: full, diagonal, tied

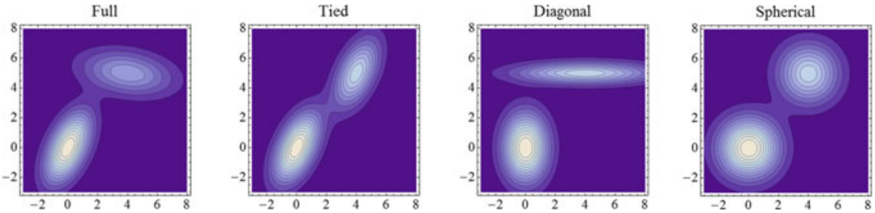


Fig. 1 Plots of the mixture of Gaussians using GMM for different covariance types [5]

and spherical. 'Full' means the components are free to adopt any shape and position independently. 'Tied' means that components may have similar shape where the shape is not predefined. The 'Diagonal' means that the axes of contour are along the coordinate axes. 'Spherical' is like diagonal type but with circular contours.

The reason for choosing GMM for this work is that it is one of the fastest method for learning mixture models. Besides, GMM maximizes only the likelihood, hence chances are negligible that it will bias the means towards zero. Also it is less prone to bias the clusters to have specific structures.

In this study, we used an OBS network dataset, available at UCI machine learning repository [6] for classification using GMM. This dataset was build by some researchers using a simulation environment. Network expert assigned the class labels for each node's traffic. There are four different types of nodes in the dataset. The 'Class' attribute is the target attribute which holds four possible labels for the corresponding node, namely: Block, No-Block, NB-No-Block, and NB-Wait. We took the dataset, performed necessary cleaning and feature selection task. Then we did principal component analysis [7] to make the dataset fit for GMM. A semi-supervised approach was taken by using very few labeled data to precompute mean and covariance for the GMM. After that GMM was trained based on few training samples. Then the model predicted the class label for test data. Finally we computed the accuracy of the model for different GMM covariance types.

2 Related Work

Very few studies exist on the malicious behavior of optical burst switching (OBS) network and fewer on the application of machine learning to classify OBS nodes.

In [8], authors endeavored to filter misbehaving burst header packets (BHP) at the optical layer. They made use of optical codewords to verify whether a BHP came from a legitimate source or not by comparing bit pattern which represents a sequence of pulses that decide the authenticity of source nodes.

In [9], authors demonstrated a firewall to prevent BHP flooding attack. It made use of offset time included in the BHP. The offset time is the time difference between a BHP arrival and its associated data burst arrival. So the firewall detects malicious behavior by comparing the specified delay in the BHP and actual delay of related data burst.

In [10] authors developed a method to classify an OBS network traffic into three distinct categories: Trusted, Suspicious and blocked, by analyzing various parameters related to resource utilization by the nodes. The authors set some rules and thresholds to decide between the classes.

In [11], authors discussed about data burst loss in OBS network. Loss can occur due to contention which does not necessarily mean that there is a congestion in the network. To differentiate between loss due to contention and due to actual congestion, the authors employed both supervised and unsupervised methods. The authors found that the measure of observed losses derived from the number of bursts between failures follow a Gaussian distribution which has different characteristics for different types of losses.

In [12], authors used exactly the same dataset as we have done in this work. The target attribute of the dataset has four probable labels for each row: Behaving-No-Block, Misbehaving-Block, Misbehaving-No-Block and Misbehaving-Wait. The authors followed supervised classification approach using decision tree algorithm to predict four labels of data. The decision tree is an effective classifier which can produce simple if-then rules that classifies the data. In that study, some if-then rules were generated using decision tree algorithm that can fit any new input to the appropriate label. The model showed high accuracy when trained with sufficiently large labeled dataset.

In [13], authors used K-means clustering algorithm to classify an OBS network nodes using a semi-supervised training method. A tiny amount of labeled data from an OBS dataset was chosen as training samples and then an initial clustering was done with those samples to find the probable cluster centers. With these assumed labels and cluster centers, the test dataset was clustered. The accuracy on the test dataset was 41.61% and 53.72% with 1% and 2% training data respectively.

In this study we are using EM based GMM in a semi-supervised approach to classify the OBS network dataset which, we believe, to the best of our knowledge, is among the earliest to be proposed and implemented.

3 Proposed Work

Semi-supervised learning (SSL) [14] is a kind of machine learning method which is useful when we have a large quantity of unlabeled data as compared to the labeled data. Practically it is difficult to find labeled dataset for a particular problem because labeling is usually done by a human hand. Going to an expert to label a large dataset is difficult, costly and time consuming task. In such situation, SSL methods help to label the unknown classes. Usually a SSL algorithm starts with the available labeled data and adjusts its parameters using them. Then using sophisticated probabilistic or other mathematical models it labels the unlabeled data. SSL models also make use of the unlabeled data's information to update its parameters for a better prediction.

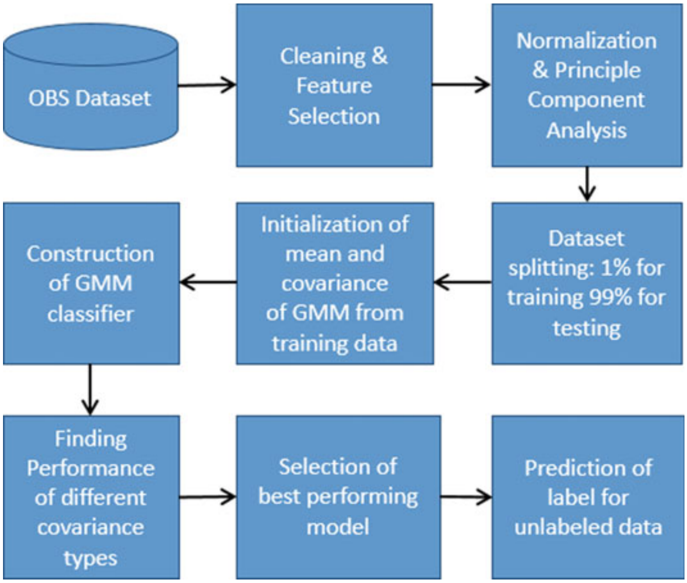

OBS Dataset
Cleaning & Feature Selection
Normalization & Principle Component Analysis
Dataset splitting: 1% for training 99% for testing
Initialization of mean and covariance of GMM from training data
Construction of GMM classifier
Finding Performance of different covariance types
Selection of best performing model
Prediction of label for unlabeled data

Fig. 2 Steps of SSL approach using GMM on OBS data

In this work, after performing necessary dataset preprocessing, we took few samples (1%) from the OBS dataset as training set to initialize the parameters of GMM. The reason for choosing 1% data for training is that, labeled data are hard to find. The OBS dataset has 1075 records, so taking 1% yields just 10 samples. We condition that those 10 sample will have members from all the four classes that we want to find. It can be stated without exaggeration, that it is easier to find 10 labeled data, or to get 10 sample data labeled than to label thousands of data.

After the split, mean and covariance of the Gaussians to be discovered were initialized using the sample data from the training set. Then the model was trained and tested against four of GMM covariance types. The process is illustrated in Fig. 2.

3.1 Dataset Cleaning and Feature Selection

The chosen dataset has 22 attributes [6]. The names are as follows: Node, Utilised_Bandwith_Rate, Packet_Drop_Rate, Full_Bandwidth, Average_Delay_Time_Per_Sec, Percentage_Of_Lost_Pcaket_Rate, Percentage_Of_Lost_Byte_Rate, Packet_Received__Rate, Amount_of_Used_Bandwidth, Lost_Bandwidth, Packet_Size_Byte, Packet_Transmitted, Packet_Received, Packet_lost, Transmitted_Byte, Received_Byte, 10-Run-AVG-Drop-Rate, 10-Run-AVG-Bandwith-Use, 10-Run-Delay, Node_Status, Flood_Status, Class. The last attribute, ‘Class’ is our target attribute. It has four distinct labels/classes. There are some missing or empty values which need to be processed. The missing values, or empty values were replaced by the mean of the corresponding attribute values. Also there are some attributes that can be ignored, like ‘Packet_Size_Byte’ attribute which has constant packet size value. Also the ‘Node’ attribute can be removed as it symbolizes node ID. The ‘Node_Status’ attribute can also be removed as it is a target attribute which we are not considering in this work. The OBS dataset has very irregular shape when plotted in a graph. This makes the task of clustering harder. Clustering algorithms can find the clusters easily when they are well separated from each other and have a regular pattern/shape. A scatter plot of a few pairs of attribute from the OBS dataset is shown in Fig. 3. Four colors symbolizes four distinct classes. And in Fig. 4, distribution of a few attributes of OBS dataset is plotted. We can see that the clusters are not spherical/circular in shape. They are irregular and non-spherical. So the clustering algorithms will find it difficult to do a clear grouping of the classes.

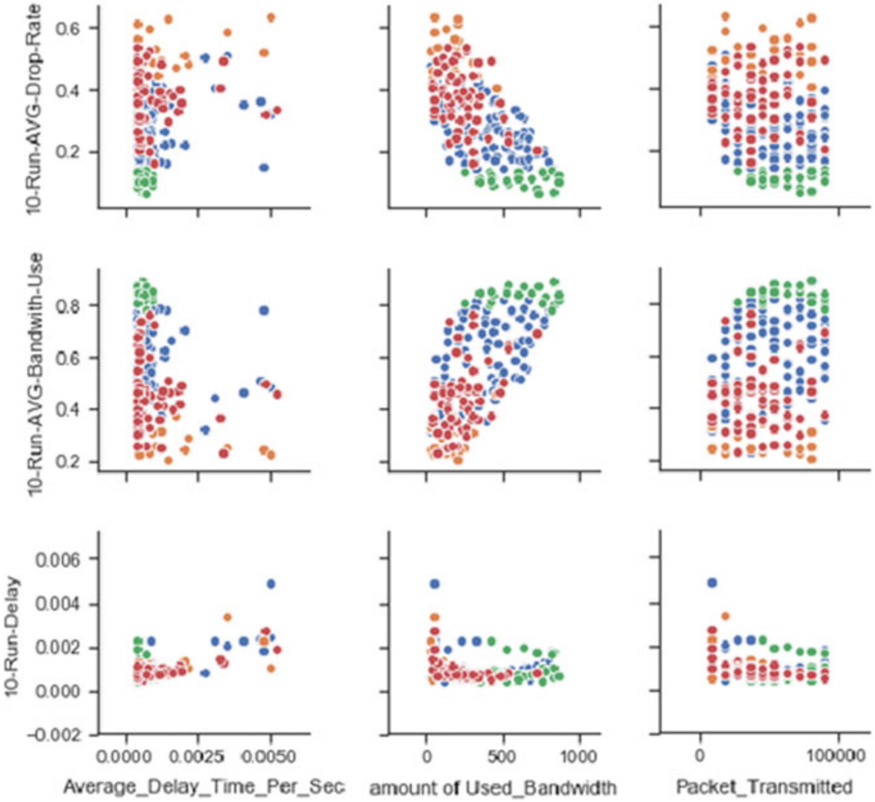


Fig. 3 Scatter plot of three attributes against other three from OBS dataset

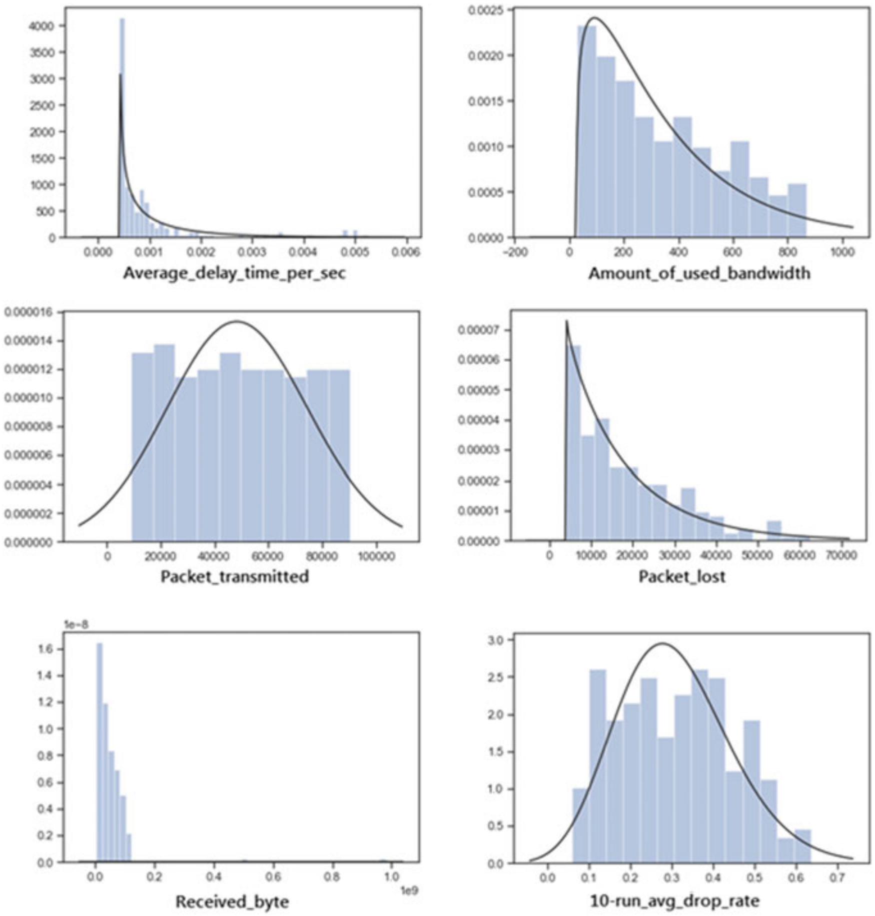


Fig. 4 Distribution plot of six attributes from OBS dataset

3.2 Normalization

We performed normalization [15] on the OBS dataset so that each individual sample will have unit norm. Each row of the dataset was rescaled using L2 norm so that the data points come closer and make a finer grouping of different labels.

3.3 Principal Component Analysis

We performed principal component analysis (PCA) [7] to reduce the number of attribute down to only two. After plotting the two dimensions in a scatter plot we found that the four groups are more clearly separable than before. Figure 5 shows the scatter plot and Fig. 6 illustrates their distribution.

In Fig. 5, the four different colors represent four class labels of the target attribute 'Class'. We can see the outliers in each group. The green is the leftmost color in the plot, which has some blue as outliers. Then the blue group which crosses its boundary and falls into the red group as outlier. The rightmost group is yellow color which touches the red group in the boundary.

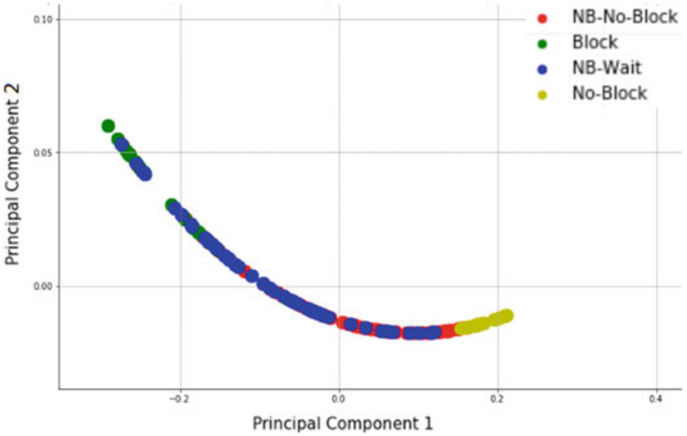


Fig. 5 Scatter plot of two components from PCA showing four groups of data in colors

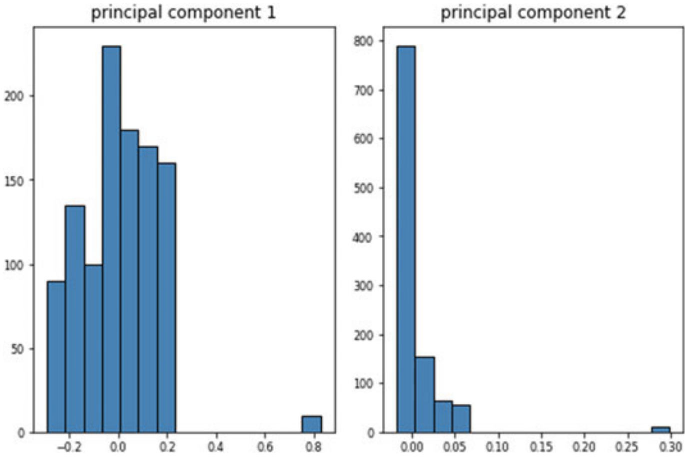


Fig. 6 Histogram of two components given by PCA on OBS dataset

Table 1 Dataset split into train and test set

OBS data	%	Amount of labeled samples	Amount of block, NB-no-block, no-block, NB-wait
Total	100	1075	120, 500, 155, 300
Train	1	10	3, 3, 2, 2
Test	99	1065	117, 497, 153, 298

3.4 Selection of 1% Data from OBS Dataset

We worked with the OBS dataset which has a target attribute called ‘Class’ having four likely sub-classes, i.e. No-Block, Block, NB-No-Block, and NB-Wait. Their meaning is as follows: Misbehaving node and will be blocked (Block), Behaving node and will not be blocked (No-Block), Misbehaving node but will not be blocked instead will be in waiting state (NB-Wait), and Misbehaving node but will not be blocked (NB-No-Block). We separated 1% data randomly from OBS dataset where samples from all four classes appears. As the selection is random, the number of sample from each class varies in every experiment. We found that the result is stable even with fluctuations in the sample frequency of each class. In Table 1, a selection is shown in detail.

3.5 Gaussian Mixture Model

Gaussian mixture model is a probabilistic model that considers a distribution consists more than one Gaussian. It calculates the joint probability for a data point to determine the most probable cluster (i.e. component). GMM employs the expectation maximization (EM) algorithm to maximize the likelihood function for a data point to be a member of a cluster. EM works in two step. In first step, called E step, the expectation or the responsibility of a data point for every component is calculated. Then in second step, called M step, the maximization of likelihood function is done by re-estimating the parameters using existing responsibilities.

Algorithm of EM for GMM

Step 1 Initialization step

Using the labeled training data, initialize the means μ_k, variances Σ_k for each of four components.

$$\mu_k = \frac{1}{N_k}\sum_{i=1}^{n} w_{ik}x_i$$

$$\Sigma_k = \frac{1}{N_k}\sum_{i=1}^{n} w_{ik}(x_i - \mu_k)x_i(x_i - \mu_k)^{\mathrm{T}}$$

where,

μ_k	means of k-th gaussian
Σ_k	variances of k-th gaussian
x	data point for dataset X, i.e. ($x \in X$)
n	total data points in dataset X
k	mixture components
w_{ik}	probability that point x_i is generated by the k-th Gaussian
N_k	$\sum_{i=1}^{n} w_{ik}$ i.e. the effective number of data points assigned to k-th Gaussian

Then initialize the mixing coefficients π, and evaluate the initial value of the log likelihood $L(\Theta)$ which is given by:

$$L(\Theta) = \sum_{i=1}^{n} \ln\left\{\sum_{k=1}^{K} \pi_k F(x_i|\Theta_k)\right\}$$

where,

Θ_k	(μ_k, Σ_k)
π_k	prior probability (weight) of k-th gaussian
$F(x_i \vert \Theta_k)$	probability distribution of observation x_i, parameterized on Θ

Step 2 Expectation step

Evaluate weights:

$$w_{ik} = \frac{\pi_k F(x_i|\Theta_k)}{\sum_{j=1}^{K} \pi_j F(x_i|\Theta_j)}$$

Where, w_{ik} is the probability that point x_i is generated by the k-th Gaussian

Step 3 Maximization step

Re-evaluate parameters:

$$\mu_k^{\text{new}} = \frac{1}{N_k}\sum_{i=1}^{n} w_{ik}x_i$$

$$\Sigma_k^{\text{new}} = \frac{1}{N_k}\sum_{i=1}^{n} w_{ik}\left(x_i - \mu_k^{\text{new}}\right)x_i\left(x_i - \mu_k^{\text{new}}\right)^{\mathrm{T}}$$

$$\pi_k^{new} = \frac{N_k}{N}$$

Then, evaluate $L(\Theta^{\text{new}})$ and stop if converged.

The algorithm is repeated for each of four different covariance types, i.e. full, diagonal, tied and spherical.

4 Result Analysis

We choose Python [16] programming language environment (version 3) for implementing the classification model. We used EM based GMM implementation from Scikit learn machine learning library [17]. After necessary cleaning and preprocessing of the OBS dataset, the EM for GMM algorithm was implemented for four covariance types. The accuracy of the model was tested against the testing data (99%). It was found that each of four covariance types had different accuracy as shown in Fig. 7a–b. The maximum performance on the test data was given by tied covariance, that is 69.7% accuracy.

From the above figures we see that the model best performs with 'tied' covariance type, i.e. gives 69.7% accuracy. This output is significant. It clearly shows how semi-supervised approach helped gain a good accuracy with just 1% (10 samples) of data. The results also showed that 'tied' covariance suits best to the distribution of the OBS dataset. The accuracy of the model can be improved by increasing samples in the training dataset.

It should be noted that, we found far better performance when we used 1% labeled data for the initialization of GMM's mean and covariance, and then fitted the GMM

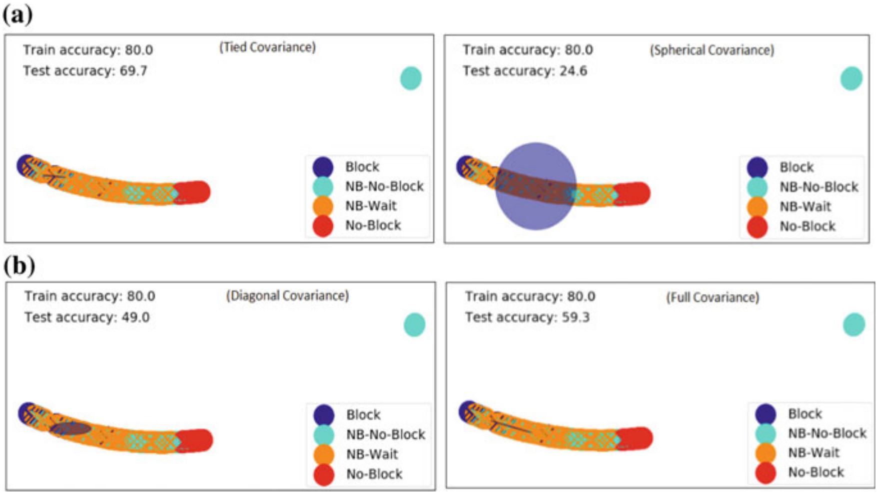


Fig. 7 **a** Performance of GMM with tied (left) and spherical (right) covariance type on test data, accuracy 69.7% and 24.6% respectively. **b** Performance of GMM with diagonal (left) and full (right) covariance type on test data, accuracy 49% and 59.3% respectively

on the rest 99% unlabeled data. This approach is valid because SSL allows using any unlabeled data to gain a better insight. We tested the fitted GMM and found that the performance was more stable than the previous one. So, we suggest to use this approach.

5 Conclusion

In this work, we constructed a Gaussian mixture model (GMM) classifier to predict the behavior of traffics of an Optical burst switching (OBS) network. For this we used an OBS network dataset from UCI machine learning repository. The dataset consists 22 attributes and the target attribute has four distinct classes of traffic that indicates the behavior of the corresponding node, i.e. the source of the traffic. We followed a step-by-step procedure to clean and preprocess the dataset to make it suitable for the GMM classifier. As the distribution of the data is very irregular and nor-spherical, we performed some scaling and transformation on the dataset to fit the data for our classifier. A semi-supervised approach was followed, that is, we considered very few (1%) labeled data samples from the dataset for training and initializing the classifier. The rest (99%) of the data was used to test the performance of the classifier. Experiments showed that the built model displays very good performance (almost 70% accuracy) in predicting the class label of unlabeled data, even when trained with tiny amount of training samples. The accuracy of the model can be increased further by introducing new method of choosing samples for initializing the GMM because GMM is very sensitive to that. Besides, if available unlabeled data can be used to find some insights to the distribution of the Gaussian components, it can help further improve the performance of the model.

Acknowledgements The dataset used in this work was collected from UCI Machine Learning Repository, Irvine, CA: University of California. Originally by Adel Rajab, Department of Computer Science and Engineering, University of South Carolina SC, USA. We used the python implementation of Ron Weiss (ronweiss@gmail.com) and Gael Varoquaux for the graphical representation of different covariance types.

References

1. Qiao C, Yoo M (1999) Optical burst switching (OBS)–a new paradigm for an optical networks. J High Speed Netw 8(1):69–84
2. Wang M, Cui Y, Wang X, Xiao S, Jiang J (2018) Machine learning for networking: workflow, advances and opportunities. IEEE Netw 32(2):92–99
3. Reynolds D (2015) Gaussian mixture models. Encycl Biometr 827–832
4. Moon TK (1996) The expectation-maximization algorithm. IEEE Sign Process Mag 13(6):47–60
5. Plots of the actual mixtures. https://i.stack.imgur.com/0zLpe.png

6. BHP flooding attack on OBS Network Data Set. https://archive.ics.uci.edu/ml/datasets/Burst+Header+Packet+%28BHP%29+flooding+attack+on+Optical+Burst+Switching+%28OBS%29+Network%23
7. Olive DJ (2017) Principal component analysis. In: Robust multivariate analysis. Springer, Cham, pp 189–217
8. Sliti M, Boudriga N (2015) BHP flooding vulnerability and countermeasure. Photon Netw Commun 29(2):198–213
9. Sliti M, Hamdi M, Boudriga N (2010) A novel optical firewall architecture for burst switched networks. In: 12th international conference on transparent optical networks, pp. 1–5
10. Rajab A, Huang CT, Al-Shargabi M, Cobb J (2016) Countering burst header packet flooding attack in optical burst switching network. In: International conference on information security practice and experience. Springer, Cham, pp 315–329
11. Jayaraj A, Venkatesh T, Murthy CSR (2008) Loss classification in optical burst switching networks using machine learning techniques: improving the performance of tcp. IEEE J Sel Areas Commun 26(6):45–54
12. Rajab A, Huang CT, Al-Shargabi M (2018) Decision tree rule learning approach to counter burst header packet flooding attack in optical burst switching network. Opt Switch Netw 29:15–26
13. Patwary MKH, Haque MM (2019) A semi-supervised machine learning approach using *K*-means algorithm to prevent BHP flooding attack in optical burst switching network. Unpublished (2019)
14. Chapelle O, Scholkopf B, Zien A (2009) Semi-supervised learning. IEEE Trans Neural Netw 20(3):542
15. Perronnin F, Sánchez J, Mensink T (2010) Improving the fisher kernel for large-scale image classification. In: European conference on computer vision. Springer, Berlin, Heidelberg, pp 143–156
16. Python programming language. https://www.python.org/
17. Pedregosa F, Varoquaux G, Gramfort A, Michel V, Thirion B, Grisel O, Vanderplas J (2011) Scikit-learn: machine learning in Python. J Mach Learn Res 12:2825–2830

Apache Spark Methods and Techniques in Big Data—A Review

H. P. Sahana, M. S. Sanjana, N. Mohammed Muddasir and K. P. Vidyashree

Abstract Major online sites such as Amazon, eBay, and Yahoo are now adopting Spark. Many organizations run Spark in thousands of nodes available in the clusters. Spark is a "rapid cluster computing" and a broader data processing platform. It has a thirsty and active open-source community. Spark core is the Apache Spark kernel. We discuss in this paper the use and applications of Apache Spark, the mainstream of popular organization. These organizations extract, collect event data from the users' daily use, and engage in real-time interactions with such data. As a result, Apache Spark is a big data next-generation tool. It offers both batch and streaming capabilities to process data more quickly.

Keywords Apache Spark · Big data · Data processing

1 Introduction

Apache Spark [1] has stolen the focus on iterative learning jobs for machines, interactive, and batch data analysis. It is based on Hadoop MapReduce and extends the MapReduce model to more computing types, including interactive queries and stream processing, efficiently. Description of a scheme not only measures water consumption per second but also generates enough electricity (~4 W) to run on the Apache Spark data aggregation network. Apache Kafka is a distributed LinkedIn publication subscribe message system. Both Spark and Kafka have a distributed processing environment [2]. JA-BE-JA is a distributed k-way solving problem algorithm. A balanced graph partitioning has many relevant applications, including biological networks, parallel programming, and online analysis of social networks, and can be used to reduce communication costs and balance workload. The abstraction of the resilient distributed data set is the key concept behind the Spark calculations [3]. Apache Spark is a novel solution for processing large-scale production data

H. P. Sahana (✉) · M. S. Sanjana · N. Mohammed Muddasir · K. P. Vidyashree
Department of Information Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India
e-mail: hpsahana98@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_67

to solve the disadvantages of Hadoop. Evolutionary undersampling was developed with special attention to the class imbalance problem as an extension of evolutionary prototype selection algorithms. Spark's flexibility enabled the proposed model to be implemented easily and fully automatically [4].

SAC is built on Spark to increase the performance using the computer in-memory model. Spark itself provides a Web user for monitoring the resource use of the entire cluster, the status of the task, and detailed information for each stage of the task, which emphasizes the application profile and the time of execution [5].

Apache Spark is an open-source computer cluster with APIs in Scala, Java, Python, and R. Spark can cache working data or intermediate data in memory to minimize data latency so that Spark performs much better than Hadoop in iterative workload types such as machine learning algorithms and interactive data mining [6]. Deep learning offers solid models of learning for MBD analysis. Apache Spark is an open-source cluster computing platform for scalable MapReduce. Spark program RDDS natively supports fault-tolerant executions and recovers worker node program operations [7]. The Halvade framework is the solution to the scalability challenge of the GATK pipeline. GATK is a commonly used tool: Intel Realignment, Haplotype Caller, and Base Recalibration. The output of this tool set is a VCF (variant format) file with sequenced DNA variations [8].

APRACK is designed to calculate some of the user-specified features, such as those of the largest real part of the largest magnitude, with k own values. It gives the calling program control by multiplying the matrix-vector request. TFOCS is a state-of-the-art numeric solver, formally, a convex solver of the first order [9]. Big data analysis converges with HPC in order to unleash big data's full potential. The RDMA shuffle engine is designed to bypass JVM to prevent the overhead of JAVA communication sockets [1].

Apache Spark and Apache Storm are designed to perform high-speed heterogeneous traffic data analysis in real time [10]. Clustering algorithms on static GPS data have been evaluated using the Apache Spark processing architecture. SPARQLGX is a direct assessment. After preprocessing RDF data, it evaluates SPARQL queries using Apache Spark [11]. It depends on a compiler of a conjunctive SPARQLX query that generates Scala code executed by the Spark infrastructure. Spark enables stream processing with large input data and handles only a small amount of flying data [12]. Clustering of k-means is a nonhierarchical approach of grouping items into different groups [12].

2 Comparison of Different Methods in Apache Spark

Table 1 gives us the idea of how the different methods and techniques used in Apache Spark help to increase the result in the big data for the organization.

Table 1 Comparison of different Apache Spark methods and techniques in big data

Reference No.	Approach	Method	Parameter	Result	Advantage
1	Detailed design for high-performance RDMA-based Apache Spark on high-performance networks	Systematic performance evolutionary on chameleon SDSA comet and an in-house cluster with cutting-edge InfiniBand technologies	Spark APIs, Intel HiBench sort and Terasort	RDMA-based Spark design is implemented as a pluggable model	A combined version of RDMA Spark+ "RDMA-HDFS" achieved the best performance with up to 82% improvement on SDSC comet cluster
2	Description of a smart city, a self-powered water monitoring solution that uses low-cost water turbines	Stand-alone remote Apache Spark streaming as a distributed alternative to the conventional hierarchical smart grid	Domestic water pressure levels, utility electric power	Generation of 4 W electric power as UK domestic water pressure levels	A future smart city will have innovative features as high-frequency monitoring of water flows and automated leak detection
3	An adaptation to the JA-BE-JA algorithm to make it efficiently computed by BSP	Implementation of JA-BE-JA over a modified version of peers to comply with the BSP model	BSP abstraction, the second version of Apache Spark, Spark version of BSP	An experiment conducted is similar to the ones effectively achievable using Spark	Spark version adopting the relaxed consistency models runs significantly faster
4	Provide a new big data scheme based on new emerging technology Apache Spark to tackle highly imbalance data	Multiple parallel operations, in-memory operations provided by Apache Spark	Divide and conquer based on MapReduce paradigm by dividing data into multiple subsets	Spark used as parallelization technology helped in the goodness of evolutionary undersampling model	It enabled the softening of lack of density issue presented in the extremely imbalanced problems
5	To answer if Apache is scalable to process seismic data with its in-memory computation and data locality features	Typical seismic data processing algorithms used for the study of performance and productivity	Traditional HPC, big data analytics platform	Customized seismic data distribution in Spark, extraction of templates for seismic data processing algorithms	Performance analysis of several typical seismic processing algorithms
6	TCP-H benchmark as optimization with perspective logs	JVM log such as GC and JIT, system utilization, hardware events from PMO, SMT technology	Java heaps, Java virtual machine, operating systems	Achieves 30–40% speedup on average and up to 5x faster than the naive configuration	Improve Spark core runtime, to develop a more advanced algorithm about JVM

(continued)

Table 1 (continued)

Reference No.	Approach	Method	Parameter	Result	Advantage
7	A context-aware activity recognition application with a real-world data-out containing millions of samples to validate the framework	MapReduce computing on many Spark works, master deep models	MBD analytics, scalable learning framework over Apache Spark	Enables tuning of deep models with many hidden layers and millions of parameters on a cloud cluster	This approach is 63% faster than Hadoop MapReduce-based solutions
8	A framework used for implementation of an in-memory distributed version of GATK	Apache Spark, GATK, DNA analysis pipeline	Harvard, a Hadoop MapReduce solution, Churchill, an HPC cluster-based solutions	Reduction of execution by keeping data active in memory between MapReduce steps	This approach is 63% faster than Hadoop MapReduce-based solutions
9	Description of the distributed and local matrix computations available in Apache Spark	Separating matrix operations from vector operations for single node usage, JVM	Spectral and convex optimization problems	Provides a comprehensive set benchmark on accessing hardware level optimizations for matrix computation from JVM	This has been commercially supported by a slew of companies that provide further services
10	Big data platform for low-latency traffic flow analysis based on real-time and high-velocity data	Apache Flume is used for ingesting real-time data to Spark-streaming analysis	Virtualization, data aggregation, and lightweight protocols such as COAP and MQTT	Load balancing for all Spark executors leads to uneven results	Flume-integrated message brokers such as active MQ or Kafka for more advanced message routing
11	Implementation of a distributed RDF datastore based on SPARQLGX	SPARQL queries on distributed RDF (resource description framework) data sets	Spark executable code, RDF data, SDE	SPARQLGX outperforms several state-of-the-art Hadoop-reliant systems	SPARQLGX represents an interesting alternative in several scenarios
12	Comparison of Hadoop MapReduce and Apache for analysis big data	A standard machine learning algorithm for clustering (k-means)	Performance analysis using the k-means algorithm	Spark is a very strong contender and would bring a change	Spark will be the de facto framework for a large number of use cases involving big data processing

3 Conclusion

This paper outlines the main features and the importance of Apache Spark. Apache Spark is a cluster computing platform that is designed to be fast and extends the popular MapReduce model to support more computing types, including interactive queries and stream processing. It includes the full functionality of the successful hydrogen generation scheme demonstration with a power of ~4 W. The experiment was carried out on the BSP version of peers by using a distributed framework such as Spark. Apache Spark offers multiple parallel operations that benefits in-memory operations. Profiling Spark applications include deep data partition analysis memory and network usage. The in-memory function of Spark and the generation of immutable objects significantly reduce GC overhead from 30 to 10% and by optimizing JVM counts. The Spark-based learning framework for mobile big data analysis offers a promising learning tool to add value from raw mobile big data.

Apache Spark uses the multi-node cluster efficiently, increasing the efficiency and flexibility of the framework. By separating matrix operations from vector operations, a large number of traditional algorithms intended for single node use can be distributed. The default IP Spark over Infiniband (IpoIB) achieves a performance improvement of up to 79%. Spark streaming and Spark batch involve high performance in experiments with the Spark executor, which helps to set RDF data specifically. Spark helps to simplify the computer-intensive and challenging tasks of processing high volumes of real-time or achieved data, both structured and unstructured, integrating relevant complex capabilities such as machine learning and graph algorithms. Spark brings mass processing of big data.

Acknowledgements The authors express gratitude toward the assistance provided by Accendere Knowledge Management Services Pvt. Ltd., in preparing the manuscripts. We also thank our mentors and faculty members who guided us throughout the research and helped us in achieving the desired results.

References

1. Lu X, Shankar D, Gugnani S, Panda DKDK (2016) High-performance design of Apache Spark with RDMA and its benefits on various workloads. In: Proceedings of 2016 IEEE international conference on big data, Big Data 2016, pp 253–262
2. Domoney WF, Ramli N, Alarefi S, Walker SD (2016) Smart city solutions to water management using self-powered, low-cost, water sensors and Apache Spark data aggregation. In: Proceedings of 2015 IEEE international renewable and sustainable energy conference, IRSEC 2015
3. Carlini E, Dazzi P, Esposito A, Lulli A, Ricci L (2014) Balanced graph partitioning with Apache Spark. In: Euro-Par 2014: parallel Processing workshop, pp 129–140
4. Triguero I, Galar M, Merino D, Maillo J, Bustince H, Herrera F (2016) Evolutionary undersampling for extremely imbalanced big data classification under Apache Spark. In: 2016 IEEE congress on evolutionary computation, CEC 2016, pp 640–647

5. Yan Y, Huang L, Yi L (2015) Is Apache Spark scalable to seismic data analytics and computations? In: Proceedings of 2015 IEEE international conference on big data, IEEE Big Data 2015, pp 2036–2045 (2015)
6. Chiba T, Onodera T (2015) Workload characterization and optimization of TPC-H queries on Apache Spark. IBM Research—Tokyo, Japan, pp 1–12 (2015)
7. Alsheikh MA, Niyato D, Lin S, Tan H-P, Han Z (2016) Mobile Big data analytics using deep learning and Apache Spark. IEEE Netw 31:21–29
8. Mushtaq H, Al-Ars Z (2015) Cluster-based Apache Spark implementation of the GATK DNA analysis pipeline. Proceedings of 2015 IEEE international conference on bioinformatics and biomedicine, BIBM 2015, pp 1471–1477
9. Zadeh RB, Meng X, Staple A, Yavuz B, Pu L, Venkataraman S, Sparks E, Ulanov A, Zaharia M (2016) Matrix computations and optimization in Apache Spark. In: KDD' 16, pp 31–38
10. Maarala AI, Rautiainen M, Salmi M, Pirttikangas S, Riekki J (2015) Low latency analytics for streaming traffic data with Apache Spark. In: Proceedings of 2015 IEEE international conference on big data, IEEE Big Data 2015, pp 2855–2858
11. Graux D, Jachiet L, Genev P, Graux D, Jachiet L, Genev P, Graux D, Jachiet L, Genevès P, Layaïda N (2016) SPARQLGX in action: efficient distributed evaluation of SPARQL with Apache Spark. In: 15th international semantic web conference
12. Gopalani S, Arora R (2015) Comparing Apache Spark and Map Reduce with performance analysis using K-means. Int J Comput Appl 113:8887

Artificial Intelligence Applications in Defense

C. Sinchana, K. Sinchana, Shahid Afridi and M. R. Pooja

Abstract Artificial intelligence (AI) is a rapidly growing field of computer science, which involves computer programming and offers tremendous advantages in the military expert system, human intelligence development, and support. This paper describes the use of artificial intelligence in the military field. It shows how the natural language of processing, ontology, and a system based on knowledge is used to create a unified military system. It also shares an insight into the use of AI in the military field for autonomous weapons, land analysis, and aircraft carrier landing.

Keywords Artificial intelligence (AI) · Military · Ontology · Knowledge-based system · Autonomous weapons · Terrain analysis · Aircraft carrier landing

1 Introduction

Artificial intelligence is part of informatics that is booming wildly in the field of the military system. Advances in artificial intelligence (AI), i.e., the natural language of processing, ontology, knowledge-based system, land analysis, and improved aircraft carrier landing performance enable new military capabilities that have a significant impact on military strategies. In this paper, artificial intelligence mainly talks about intelligence, surveillance, recognition of the balance of offense/defense, and, most importantly, about the autonomous arms system. Autonomous weapons are those that have the ability to make their own decisions based on programming constraints, and artificial intelligence incorporates these weapons.

Many military programs, including systems that help combat management in real time, predict and defeat enemy war plans, plan air strikes, fly hazardous pursuits, eliminate operations, and implement AI systems. Military engagement, promises on private industry resources, creates discussion platforms, publishes newsletters

C. Sinchana (✉) · K. Sinchana · S. Afridi · M. R. Pooja
Department of Computer Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India
e-mail: sinchanachandan24@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_68

dedicated to military AI systems, thus creates online databases for AI information, and creates a multi-command committee.

2 Ease of Use

2.1 Ontology

Ontology can be defined as the data model that represents knowledge and the relationship between these concepts as assets of concepts within a domain [1–4]. Today, people have access to more data than people have had in the last decade in a single day. It is therefore important to represent the relationship between the data, as the data are available in many ways. The two standards governing ontology construction are:

(1) web ontology language
(2) resource description framework.

Ontology components are classes and relationships. The main benefit of ontology is that new relationships can easily be added to the existing model. Ontology is now used in many fields, such as knowledge representation, knowledge sharing, integration of knowledge, reuse of knowledge, and information retrieval. With ontology, it is possible to accurately represent a certain military domain, for example, operations, intelligence, logistics, etc.

In certain military domains, we can identify and define entities and events. Relationships between entities and events can be identified and defined. This improves the ability to reason over a particular domain. It contributes to the development of tactics, techniques, and processes. All of these improve efficiency. The ontological methods used by the war planners lead to situational awareness, understanding of the situation, and a common operational picture. These are all necessary for decision-making. The ontology is having good scalability and can be next enriched and improved.

2.2 Knowledge-Based System and AI Supportability

Artificial intelligence is a rapidly growing military field that offers tremendous advantages in the development and support of weapons systems. The study area generally accepted for the artificial intelligence field includes problem-solving, logical reasoning, language, programming, learning, robotics, and vision, system, and language [5].

The knowledge-based system is a computer program that uses methods of determination and knowledge to solve problems that require important human expertise to solve them. Knowledge based on the knowledge of the system comprises truths, heuristics, and patterns. The air force can provide each technician with the expertise

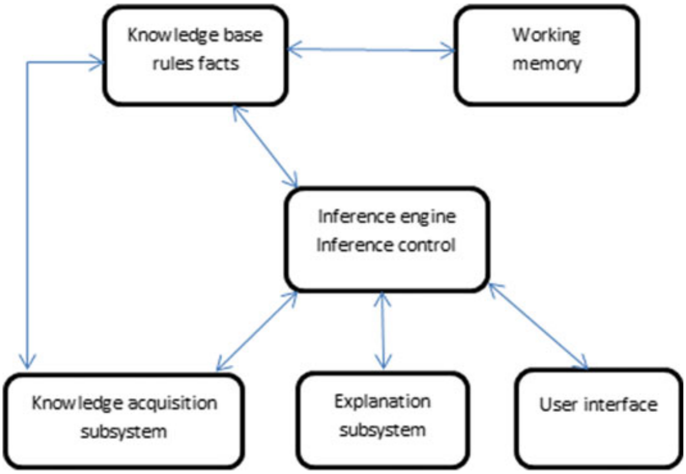


Fig. 1 Structure of a knowledge-based system [6]

of the best air force maintainers through the use of knowledge-based systems. It helps to avoid delays in the need for expertise, retains knowledge of decisions and actions taken in times of crisis, and ultimately helps to retain corporate knowledge by trapping and coding knowledge.

By making the knowledge base more accessible, greater flexibility should be achieved, uniform knowledge should be used to minimize the number of mechanisms required to handle knowledge leading to a more transparent system, and these are the ways in which we can offer greater support through the use of AI.

Figure 1 is a diagram of the two-part knowledge system, the inference engine, and the knowledge base.

2.3 Autonomous Weapon

Autonomous weapons are able to make their own decisions on the basis of programming limitations. These arms contain "AI" This includes a drone or a UAV (unmanned aerial vehicle) usually refers to a pilotless aircraft operating through a combination of technologies, including computer vision, AI, object prevention technology, and others. However, drones can also be autonomous ground or sea vehicles. Autonomous and automated guns' difference: Automatic weapons are those that do not have the ability to learn and cannot change their objectives, and they can be referred to as anti-material weapons, because they could cause civil damage. In this type of weapon, the output is always the same for each input. There is no ability to reason in automated weapons. However, autonomous weapons have the ability to determine the best results possible for a set of inputs. It can modify its objective or deploy sub-goals. Once activated, this weapon does not require further intervention of the operator. It can have many capabilities, such as target identification, tracking, and firing, all of which have different levels of human interaction and input.

Working:

These weapons use technologies such as light detection and ranging (LIDAR). Radars and other devices are used to create a map or "world" around the gun using light pulses. Once the device is complete, it can navigate independently. In practice, these weapons can encounter many obstacles. The programmer or an engineer cannot write code for each obstacle to rely on "machine learning."

Knowledge based on Reasoning:

Logical action based on knowledge occurs if the rule of the established rules does not require the current situation. The skill-based tasks are easier to automate, for example, in self-driven car navigation, the goal is the destination, and the best route can be determined by applying traffic rules and vehicle dynamics. But the uncertainty is much higher in the case of knowledge-based reasoning. It is possible to approximate human intelligence using the concepts of natural language processing, image processing, machine learning, and profound learning, but there are many drawbacks since machine learning is data-driven, and it will not be possible to recognize scenarios or patterns that are slightly different from data. Autonomous military weapons: Several military experts considered autonomous arms to be morally acceptable and ethically better.

Lieutenant Colonel Douglas A. states that, on behalf of robots, moral benefits may be to remove people from high-pressure combat zones. Prairie USR: It focuses on neurological research, referring to the nerve circuits that cause self-control when stressed [7]. There are currently no autonomous arms matching human intelligence. However, AI will have a huge impact on the military in the future.

2.4 Terrain Analysis for the Development of the Mission Plan

Here, we see how the hybrid expert system analyzes the terrain, which develops mission plans that are part of the logical part of the computer-generated force automation system. Figure 2 shows an analysis of the terrain. Land analysis plays an important role in most military operations and applications. It is an integral part of preparing the battlefield intelligence (IPB) [8]. Terrain analysts built many databases in the early days for all important areas of operation. They form a basic basis for tactical decisions, intelligence, and tactical operations. They also help to plan and carry out most other battlefield functions. Since terrain features are constantly changing on the surface of the earth, databases need to be constantly revised and updated. The entity behaviors resulting from the above system are efficient enough to provide an acceptable training value in a distributed interactive simulation for living human opponents. It examines the problem of 3D representation of high-resolution terrain in simulations and offers suggestions and advice for polygons to maintain a high

Fig. 2 Terrain analysis [9]

degree of obedience in significant terrain in the military while reducing the number of terrains used to represent no use.

The investigation of current developments in the automated target recognition is carried out. This technology is relatively new in the field of tactical intelligence and can be used in military simulations. Installation of knowledge-based systems (KBS) is finally carried out for testing imitation material development systems. An ongoing debate is being conducted on the virtual testing ground, which captures test expertise and provides a test analysis function that helps the army fulfill the promise of using simulation technology to facilitate the procurement process.

2.5 Multiple Artificial Intelligence Techniques Used in an Aircraft Carrier Landing Decision Support Tool

An aircraft carrier is a warship that operates as a coastal airfield with a full aircraft deck and aircraft transport, arming, deployment, and recovery facilities. Balloons were used in the early twentieth century to deploy nuclear warships from wooden vessels carrying many fighters, helicopters, strike planes, and other aircraft. A heavier aircraft such as fixed-wing gunships and bombers was launched by aircraft carriers but cannot land at the moment. Aircraft carriers focus on modern action vessels with their tactical and diplomatic power, their autonomy, their mobility, and their many methods. This has shifted strategically to the main role of a fleet. One of the best advantages of navigating international waters is that it does not interfere with regional sovereignty and increases the power of airlines from third countries, reducing flight time and distance of transport and thus increasing time. Availability in the zone of action. Some of the recently completed projects that improve the decision of landing signal officers (LSOs) under the guidance of aircraft landing in aircraft carriers have been discussed here. Using multiple artificial intelligence (AI) techniques, auxiliary solutions have been developed. The project developed pilot trends and also flight prediction techniques and improved the user interface of LSO by applying cognitive psychology decision-centered design methods.

Researchers have identified the parameters of important flight modes and developed the future of the neuro-fuzzy aircraft system [10–12]. Researchers used pilot trend techniques and logical and obscure logic based on case studies. In addition to many LSOs, they decided on the best performance options and had the correct performance logic of the information provided by the pilot trending module, which resulted in the design and implementation of the LOSO interface. Two specific areas of the AI application, the data fusion part of the pilot trend system and the flight path, are presented in Fig. 3.

Fig. 3 Landing signal officers at work [9]

Table 1 Comparative analysis of various fields in defense

AI in different fields of defense	Definition/meaning	Uses in defense
1. Ontology	The data model used for knowledge representation and representation of relationships between various concepts in a domain	• To represent operations, intelligence, logistics, etc. • To define entities and events • To define tactics, techniques, and processes
2. Knowledge-based system and AI supportability	Computer program that uses methods of determination and knowledge to solve problems	• Used by air force to provide expertise in air force maintainers for the technicians
3. Autonomous weapons	Weapon system which once activated can select and act on targets without the further intervention of a human operator	• Various drones, advanced robots, shooters, etc. are designed and used in order to act in specific situations during a war
4. Terrain analysis	Analysis of land, terrain before conducting any military operation	• Forms the basis for any tactical decisions, operations, and intelligence
5. Aircraft carrier landing	A warship which is provided with full aircraft deck and aircraft transport, arming used during wars	• New pilot trends, flight prediction techniques, and improved user interface in an aircraft carrier

3 Conclusion

In Table 1, we have shown the subject of AI and some of its applications in the military, as it is very important for the improvement of defense technology performances. In this paper, we see how ontology works and how AI has improved the performance of land analysis and the use of multiple AI techniques in aircraft carrier landing. There is a long way to apply AI in the military field.

Acknowledgements The authors express gratitude toward the assistance provided by Accendere Knowledge Management Services Pvt. Ltd. in preparing the manuscripts. We also thank our mentors and faculty members who guided us throughout the research and helped us in achieving desired results.

References

1. Jia M, Yang B, Zheng D, Sun W, Liu L, Yang J (2009) Automatic ontology construction approaches and its application on military intelligence. In: 2009 Asia-Pacific conference on information processing, pp 348–351

2. Jia M, Bing-Ru Y, De-Quan Z, Wei-Cong S (2009) Research on domain ontology construction in military intelligence. In: 2009 third international symposium on intelligent information technology Application, pp 116–119
3. Neches R, Fikes R, Finin T, Gruber T, Patil R, Senator T, Swartout WR (1991) Enabling technology for knowledge sharing. AI Mag 12:36–56
4. Gómez Pérez A, Benjamins VR (1999) Overview of knowledge sharing and reuse components: ontologies and problem-solving methods. In: Proceedings of the IJCAI-99 workshop on ontologies and problem-solving methods (KRR5), pp 1–15, Stockholm, Sweden
5. Carlton KA (1988) Artificial intelligence supportability (Air Force application). IEEE Aerosp Electron Syst Mag 3:25–32
6. Max Tegmark, Open letter on autonomous weapons—future of life institute. https://futureoflife.org/open-letter-autonomous-weapons/
7. Cummings ML (2017) Artificial intelligence and the future of warfare. International Security Department and US and the America's Programme, pp 1–18
8. Campbell L, Lotmin A, DeRico MMG, Ray C (1997) The use of artificial intelligence in military simulations. In: 1997 IEEE international conference on systems, man, and cybernetics. Computational cybernetics and simulation, vol 3, pp 2607–2612
9. Richards RA (2002) Application of multiple artificial intelligence techniques for an aircraft carrier landing decision support tool. In: 2002 IEEE world congress on computational intelligence. 2002 IEEE international conference on fuzzy systems. FUZZ-IEEE'02. Proceedings (Cat. No. 02CH37291), vol 1, pp 7–11
10. Zhihong D, Shiwei T, Dongqing Y (2001) An intra-algebra in ontology. J Comput Eng Appl 37:7–8
11. Pao Y-H (1989) Adaptive pattern recognition and neural networks. Addison-Wesley
12. Weiss NA (2012) Introductory statistics. Pearson Addison-Wesley

Hybrid Approach to Enhance Data Security on Cloud

Pratishtha Saxena, Samarjeet Yadav and Neelam Dayal

Abstract Cloud computing is a label for the delivery of hosted services on the Internet. The first challenge in the cloud computing is security, and the second challenge is the large size of the file stored on the cloud. Today, cloud is in young age and used too much for storing the data. So, security is a major concern. Security endures a primary concern for businesses regarding cloud selection, usually public cloud selection. Public cloud service providers share their hardware infrastructure among the numerous customers, as the public cloud has an environment of multi-tenant. Multi-tenancy is an important feature of the cloud computing but also is prone to several vulnerabilities. From the end-user aspect, cloud computing looks very insecure from the perspective of privacy. In this paper, a technique REM (RSA algorithm, Elgamal algorithm, MD5 technique) is proposed by which we can provide better security to our data over the cloud. Unlike the previous techniques, which maintained only one pillar of security, this paper maintains two pillars of security, i.e., confidentiality and integrity along with reducing the size of the file.

Keywords Cloud computing · Data security · RSA algorithm · MD5

1 Introduction

Various definitions of cloud computing are available in which one of the squares is, "a network solution for providing inexpensive, reliable, easy, and simple access to computing resources [1]." Cloud computing relies on sharing of resources often over the Internet to achieve consistency. Cloud computing is a service-based framework

P. Saxena (✉) · S. Yadav · N. Dayal
Department of Computer Science & Engineering, Centre for Advanced Studies, AKTU,
Lucknow, India
e-mail: 17mcs010@gmail.com

S. Yadav
e-mail: 17mcs11@gmail.com

N. Dayal
e-mail: neelamdayal@cas.res.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_69

which pursues at providing everything as a service. The cloud is a storehouse of services and resources that are provided by cloud service providers. Based on the user demand, cloud computing emphasizes on service model and a trade model based on pay as per your use. The main concern in cloud computing is data security. The purpose of security architecture is to maintain the system's policy, confidentiality, availability, and integrity. In the systematic way to understand the fundamentals of cloud computing and securing the stored data over the cloud, a number of resources have been considered. For the user, it is not possible to get control of his data and computing applications until a strong security measure and privacy guarantee are not in place. So, the user never gives priority to flexibility and economic availability over its privacy and the security of his personal data. Nowadays, the users of the cloud are in the incremental phase. Consumers of the cloud are growing enormously. So, there is a need to increase the security level of cloud. Security of the data is the main concern for the cloud storage. This paper proposes a technique to improve confidentiality and integrity of user's data on cloud by combining RSA, Elgamal, and MD5 techniques. To improve the security of data, this paper proposed a technique by which the confidentiality and the integrity of user's data are improved.

The remaining sections of the paper are arranged as follows: Sect. 2 presents related work which provides a detailed study on the essential data security. Section 3 gives a brief overview of cloud architecture which describes the cloud service and deployment models. Section 4 represents the methodology of the proposed technique. Section 5 represents the results. Finally, Sect. 6 represents the future work and concludes the paper.

2 Related Work

Somani et al. [2] presented the challenges of cloud security and also presented the method to access cloud security. They presented the methodology for data security in the cloud by the implementation of the digital signature with the RSA algorithm.

Subhashini and Kavitha [3] in 2010 presented a survey of different security issues that have emerged due to the nature of service delivery models of cloud computing. They present different security issues, threats to the cloud which is already presented in the cloud, they discuss specific security threats of the different service delivery models of cloud.

Albugmi et al. [1] in 2016 presented the data protection method. They proposed an approach which is used throughout the world to ensure high data security by reducing risk and threats. It discussed the threats to data in the cloud and their solution adopted by several service providers' protection for data.

Mishra et al. [4] in 2017 presented the security model for cloud computing. Authors present some approaches to ensure data integrity and security of customers' data which is stored on the cloud by using cryptography techniques. In this paper, they show the economic impact of data loss and proposed the cryptographic algorithms.

Jayalekshmi M. B. and Krishnaveni S. H. [5] in 2018 discussed the different techniques to secure the data on the cloud, and also, they presented different issues of data storage on cloud.

Negi et al. [6] in 2018 discussed the fully homomorphic encryption (FHE) scheme in the optimized form in which the encryption algorithm is applied to improve the performance of FHE schemes and Diffie–Hellman algorithms applied to secure channel establishment in the fully homomorphic encryption.

Rohini and Sharma [7] in 2018 enrapt cloud computing security issues in their paper. In this paper, for securing data over cloud, the author used the cryptographic algorithm encryption of the data, and to maintain the integrity of the data, they use hash code.

Gupta et al. [8] in 2018 analyzed existing encryption methods such as RSA, KP-ABE, CP-ABE, and AED. The comparisons among them were on the basis of computational cost and storage cost. The author also proposed an improvement scheme to increase the speed of RSA algorithm using multi-threading concept on the latest multi-core CPU.

3 Cloud Architecture

Cloud computing has three different services and deployment models in which cloud service providers provide services and resources to its users from an assorted set of models. Cloud computing elevates its users by enabling them to reduce infrastructure cost and helps in small business to scale faster without sinking money in infrastructure and services. Cloud architecture has different delivery models for the cloud service providers and different deployment models for the users.

3.1 Delivery Model

The cloud delivery model delineates a discrete, pre-packaged combination of information technology resources, which are presented by any cloud service provider. There are three different cloud delivery models, which are as follows

- Platform-as-a-service (PaaS)
- Infrastructure-as-a-service (IaaS)
- Software-as-a-service (SaaS).

Infrastructure-as-a-Service (IaaS)

This is the lowermost layer of the cloud stack. This model provides various hardware facilities to the consumers [9]. It provides an infrastructure of cloud-like storage space, network and server capacity, etc., to the end user on a rental basis for increasing organization capabilities [10]. The resources are easily scaled up depending on the demand from the user and the service provider charge for the service on a pay per use basis [11].

Platform-as-a-Service (PaaS)

In the cloud stack, architecture platform as a service layer is the middle and above layer of IaaS. This model provides the development option to the customers. It is a model in which the user can deploy own applications on a platform like a system software, middleware, operating system, or database, etc., provided by cloud [11].

Software-as-a-Service (SaaS)

This is the uppermost layer of the cloud computing stack. At this layer, complete software or applications are hosted that user or consumers can use. SaaS provides the services to the end user. SaaS can provide business applications like clientele relationship management, accounting, and corporation resource planning [12].

3.2 Deployment Model of Cloud Computing

The cloud deployment model delineates a particular environment of cloud which is primarily differentiated by ownership, access, and size. Delivery model of the cloud is narrated as below:

- Private cloud
- Public cloud
- Community cloud
- Hybrid cloud.

Public Cloud

A Public cloud is subordinate or dependent on the cloud service provider such as Google, Amazon, Microsoft etc. In other words, we can say that its services are open to all users. The user can use these resources on rent basis and can generally scale their resource consumption up to their requirements. Rackspace, Google, Microsoft, Amazon, and Salesforce are examples of the public cloud providers. Public clouds are built on the norm of the standard model of cloud computing. In the standard model, cloud service provider fabricates resources such as applications delivered, data storage, and servers to the client by the Internet [4].

Private Cloud

Private clouds are built on the norm of standard cloud computing model. In this deployment model of cloud, it offers resources such as applications, servers, and data storage, but in this deployment method, these services are proprietary and mostly customized for single user [4]. The aim of the public cloud regarding organization is to deliver services to various corporations. Private cloud is mainly used for small group of organizations. It has the same computing model like a public cloud in terms that it provides resources to users, but the only difference is that public cloud is open for all, which means many organizations can use public cloud, but the private cloud is framed for a specific corporation.

Table 1 Cloud service deployment model

Deployment model	Infrastructure management	Infrastructure ownership	Infrastructure location	Access and consumption
Public cloud	Third-party provider	Third-party provider	Off-premise	Untrusted
Private/community cloud	Corporation or a third-party provider	Corporation or a third-party provider	On-premise or off-premise	Trusted
Hybrid cloud	Both corporation and third-party provider	Both corporation and third-party provider	Both on-premise and off-premise	Trusted and untrusted

Hybrid Cloud

The third deployment model is a hybrid cloud. It is a combination of two or more clouds such as public and private cloud, public cloud and community cloud, and so on. They work separately, but they are bounded together to provide services for a common purpose [4].

Community Cloud

Community cloud is the last deployment model. It has an infrastructure service which is shared by different corporations that serve a specific community. It has common agitates like medical, military, etc. [4] (Table 1).

4 Methodology

In this paper, we proposed the methodology of REM technique. In this technique, there are three modules as shown in Fig. 1. The first module describes the process before sending the data over cloud. In this module, the input data (user data) is encrypted by Elgamal cryptosystem. After that, the encrypted data is again encrypted by the RSA algorithm for securing data and improving the confidentiality of data. We calculate the hash of again encrypted data using MD5 hashing technique. In the second module, the encrypted data and hash are stored on cloud. The third and last modules of technique are to retrieve the data over cloud.

To provide data security over cloud, we are using REM (RSA algorithm, Elgamal algorithm, MD5 technique) technique. We are using the combination of these technologies to design an algorithm in which the Elgamal algorithm will be used for key sharing and encryption between the user and cloud server securely. It uses the asymmetric key encryption technique for communication between the server and the client. Elgamal is more secure because it is based on discrete logarithm. Security

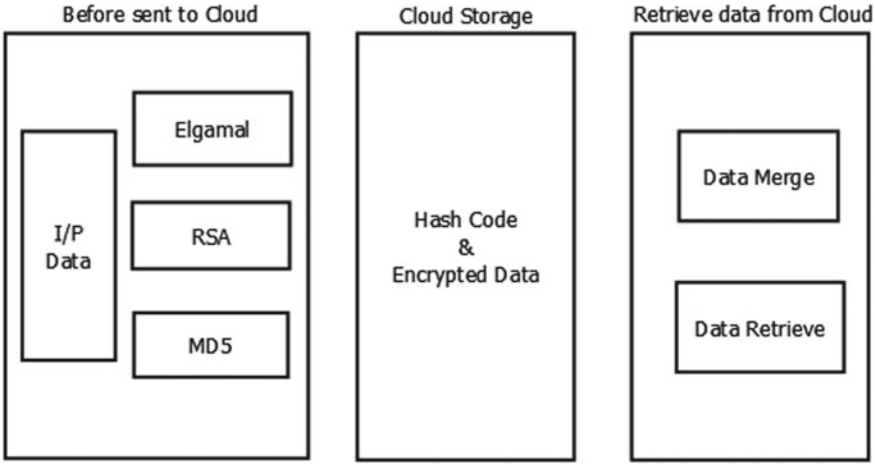


Fig. 1 Methodology of REM technique

of Elgamal depends on the difficulty of computing discrete logs in a large prime modulus. For enhancing data security, we are using double encryption technique. Thereafter, RSA algorithm will be used for the encrypting the data second time. RSA is also the asymmetric key encryption technique. Security of the RSA depends on the difficulty of factoring large integers. Both the encryption techniques are used to maintain the confidentiality of the data. Further, we will generate the hash value of encrypted data by using the MD5 technique. A cryptographic algorithm MD5 is used that takes an input and produces a 128-bit-long message digest. This message digest is called "hash code" or "fingerprint" of the input. Lastly, the encrypted data and hash code combined together are stored over the cloud storage. The flow diagram shown in Fig. 2 represents the data flow diagram of REM technique.

Further, we discuss encryption and decryption processes of our techniques.

Algorithm 1: Encryption Algorithm

Step 1: User uploads the data to the cloud, and a unique data ID will be generated in correspondence to every data item uploaded.
Step 2: Sharing key is generated by Elgamal algorithm.
Step 3: Data will be encrypted using asymmetric encryption algorithm, i.e., Elgamal algorithm.
Step 4: The encrypted data is again encrypted using an asymmetric algorithm such as the RSA encryption algorithm.
Step 5: The hash code of the encrypted data is generated using the MD5 technique which is stored on the local user.
Step 6: The encrypted data and the hash code are stored on the cloud.

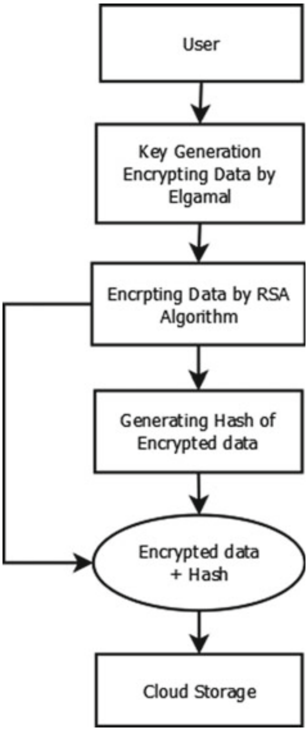

User
Key Generation Encrypting Data by Elgamal
Encrpting Data by RSA Algorithm
Generating Hash of Encrypted data
Encrypted data + Hash
Cloud Storage

Fig. 2 Data flow diagram of REM technique

Algorithm 2: Decryption Algorithm

Step 1: Received data is stored in the cloud to begin decryption.
Step 2: Decrypt the data to ensure the confidentiality of the data using RSA.
Step 3: Generate the hash code of decrypted data to ensure the integrity of the data.
Step 4: Check the hash code of the data with the stored hash code on the local system.
Step 5: Decrypt again the encrypted data using the Elgamal algorithm.

5 Result

This technique improves the security of cloud storage. In this paper, we used different parameters to analyze the performance of REM technique, which are as follows:

I. **Execution time**: Execution time refers to the total time taken for the execution of algorithm.

$$Execution\, time = end\ of\ time - the\ start\ of\ time$$

Table 2 Execution time of RSA and MD5 algorithm

Data size (bytes)	Execution time (s)	Hash generation time (s)
1024	0.532	0.024
5120	2.109	0.041
10240	3.821	0.096

Table 3 Used space of encrypted file and hash

Data size (bytes)	Space used (bytes)	Hash space used (bytes)
1024	759	40
5120	738	40
10240	903	40

II. **Space used**: Space utilization refers to the size of the file used by the algorithm.

$$\textit{Space used} = \textit{time} * \textit{buffer used per unit time}$$

III. **The probability of attacks**: It is measured by how many numbers of vulnerabilities are there in the algorithm.

The implementation of the algorithm is done, and it is tested for different size of files as given in Tables 2 and 3. Table 2 represents the execution time of encrypting the data files and the execution time of the hash code generation. We tested this on different data size sets. Table 3 represents the space used. We test this on different sizes of data, i.e., 1024 bytes, 5120 bytes, and 102400 bytes. This large file size space is reduced which is represented in Table 3. The RSA encryption technique gives a result with less execution time and takes very much less space size for storing the data. As this result is checked on hashing technique MD5 which is taking very less time in generating the hash of big data file and takes less space as given in Table 2.

6 Future Work and Conclusions

This paper proposed the methodology to improve the security of data over the cloud. In cloud computing, security plays a very important role because it stores the user's confidential data and provides the confidentiality of data, which is our prime concern. This paper proposed a hybrid approach to alleviate security challenges. We did this work at the storage level and security authentication level. The implementation of this approach will be done over the CloudSim simulator.

References

1. Albugmi A, Alassafi MO, Walters R, Wills G (2016) Data security in cloud computing. In: Fifth international conference on future communication technology, October 2017, pp 55–59
2. Somani U, Lakhani K, Mundra M (2010) Implementing digital signature with RSA encryption algorithm to enhance the data security of cloud in cloud computing. In: 1st international conference on parallel, distributed and grid computing, pp 211–216
3. Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl 34(1):1–11
4. Mishra N, Sharma TK, Sharma V, Vimal V (2018) Secure framework for data security in cloud computing. Adv Intell Syst Comput 583:61–71
5. Jayalekshmi MB, Krishnaven SH (2015) A study on data storage security issues in cloud computing. Indian J Sci Technol 8(24):128–135
6. Negi A, Goyal A (2018) Optimizing fully homomorphic encryption algorithm using RSA and Diffie-Hellman approach in cloud computing. Int J Comput Sci Eng 6(5):215–220
7. Rohini, Sharma T (2018) Proposed hybrid RSA algorithm for cloud computing. In: 2nd international conference on inventive systems and control, ICISC, pp 60–64
8. Gupta P, Verma DK, Singh AK (2018) Improving RSA algorithm using multi-threading model for outsourced data security in cloud storage. In: 8th international conference on cloud computing, data science & engineering, pp 163–169
9. Kaur J, Garg S (2015) Survey paper on security in cloud. Int J Appl Stud Prod Manag 1(3):27–32
10. Gill RD, Kapur N, Singh H (2018) Increase security of data with respect to both confidentiality and integrity over cloud. Int J Appl Eng Res 13(10):7388–7391
11. Bhadauria R et al (2014) A Survey on security issues in cloud computing. Acta Tehnica Corviniensis—Bull Eng
12. Rong C, Nguyen ST, Gilje M (2012) Beyond lightning : a survey on security challenges in cloud computing q. Comput Electr Eng

Security Threats of Embedded Systems in IoT Environment

Sreeja Rajendran and R Mary Lourde

Abstract The Internet of things (IoT) technology has reached great heights with the integration of efficient networking strategies, application protocols and VLSI. With the unlimited number of devices connected to the IoT, security has become a major concern. Mainly security is ensured by network and application protocols. But with rising threats, there is a need to lay emphasis on security from a hardware design point of view. Smart devices such as sensors and actuators are connected at the node of IoT and work on an embedded processing platform. Hence, embedded processors become an integral constituent of an IoT network. Selection of processors and identification of critical modules in the processor architecture play a key role in developing a secure design. Memory design will play a pivotal role in embedded system security. Memory attack accounts for loss or alteration of information which can impair the growth of IoT. This paper attempts to highlight security from a hardware perspective along with the potential threats likely to affect the critical modules.

Keywords Hardware security · Denial of service · Processor architecture · Memory authentication · IoT

1 Introduction

The Internet of things opens up a new realm of technology which provides connectivity to any device irrespective of its location. With advancements in VLSI and network technology along with application requirements, IoT has been able to expand its reach to intelligent control, intelligent transportation, precision agriculture, etc. [1]. Evolution of micro-electro-mechanical systems, wireless communication and digital electronics has led to the development of miniature devices called nodes [2]. These devices which can sense, compute and communicate wirelessly over short

S. Rajendran · R. Mary Lourde (✉)
Department of EEE, BITS Pilani, Dubai Campus, Dubai, UAE
e-mail: marylr@dubai.bits-pilani.ac.in

S. Rajendran
e-mail: sreejamanojnair@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_70

distances are interconnected to form wireless sensor networks. These sensor nodes play a crucial role in IoT [3].

As interesting as it may sound, the implementation of IoT also brings along with it many challenge**s.** The most important among these is security. Through IoT, small networks will be connected to larger ones which make it even harder to ensure security. The security requirements of an IoT network can be broadly classified into security tasks and security design metrics. Security tasks include authentication and tracking, data and information integrity, etc. Design metrics include cost, size, energy requirements, etc. which places constraints on security solutions [4].

The behavior of IoT depends on the data and information it collects. The more the information shared and stored, greater will be the chances of security breaches. Processing and storing of information on smart devices are handled by embedded systems. Embedded system is the integration of hardware with software that is usually designed for a specific application. It consists of processor, memory, memory controller, communication buses, etc. Embedded systems are an inevitable segment of IoT since they are present in most of the devices connected at the nodes of the IoT. Therefore, the potential growth and implementation of IoT rely on the development of efficient embedded systems. An embedded system mainly consists of a processor on which the software runs. The performance of embedded systems is greatly enhanced by on-chip features like data and instruction caches, programmable bus interfaces and higher clock frequencies.

Security of a system is broadly classified into data security and physical security. Data security can be ensured through cryptographic algorithms and also through more robust design of hardware. Since an adversary can obtain the secure key and the information through timing analysis, power analysis, etc. it is high time that focus be laid on security through hardware design. When dealing with security from a hardware perspective, emphasis needs to be devoted to the embedded system design. There is an urgent need to bring about modifications in the design so that it becomes tamper resistant. Physical security requires ensuring that only authorized users can access the device and the services. Physical separation between entities becomes an unresolvable issue due to resource sharing. The physical hardware components in an IoT working device are illustrated in Fig. 1. The intentional change in hardware inflicted by an adversary is generally referred to as a hardware Trojan. These hardware Trojans can cause the circuit to fail under critical conditions. Hardware Trojan is extremely difficult to detect since they are generally dormant and are designed to get activated under very rare conditions. This paper tries to elaborate the potential threats associated with the hardware connected to IoT.

2 IoT Security

Development of IoT would require strong security features at every level. There is a need for information security, physical security and network security. The more we increase the applications of the Internet of things, more will be the requirement

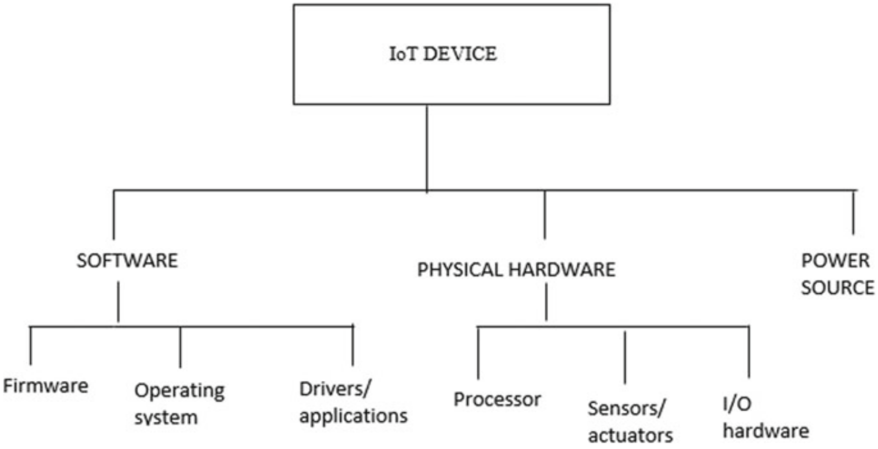


Fig. 1 Components of an IoT device

for stringent security measures. The threats on an IoT network can be on software or hardware. Hardware attacks generally involve hardware Trojans tampering the processor. For any device linked to the IoT, data will be stored in memory, and unused memory space is ideal site for malicious attack. For example, in an embedded processor flash ROMs are in common usage. Flash memory is usually embedded on the chip. It finds widespread use in electronic and computer devices since it is fast and efficient as compared to EEPROM. The main drawback of flash memory is the limit on the number of times data can be written on it. Flash ROMs are predominantly used in embedded systems storing large amount of data in non-volatile memory like digital cameras, cell phones, etc. These ROMs are rarely fully utilized. If an attacker is able to place the Trojan on the unused memory space, it can have access to the entire bus.

Network security is guaranteed through network protocols and standards. In spite of having strong network security features, the network layer is still susceptible to attacks like denial of service (DoS). This type of attack can arise due to lack of sufficiently high bandwidth communication networks, which can result in data congestion. Application layer is highly vulnerable to attacks due to its open-ended nature. A major threat is poor security design of the basic function of an application. Also, applications with no access control are targets for unauthorized use. Undesirable network traffic is generally detected by intrusion detection systems (IDS). Network security and applications security threats are kept at bay by communication, transfer control and Internet protocols and intrusion detection systems. Security measures can be taken to the next level by laying emphasis on hardware security. The first step in designing for security involves the identification of the attacks which need to be prevented. Design for hardware security should be done keeping in mind that any additional circuitry added to prevent hardware attacks should itself be resistant to attacks especially DoS. The architecture of embedded system is shown in Fig. 2.

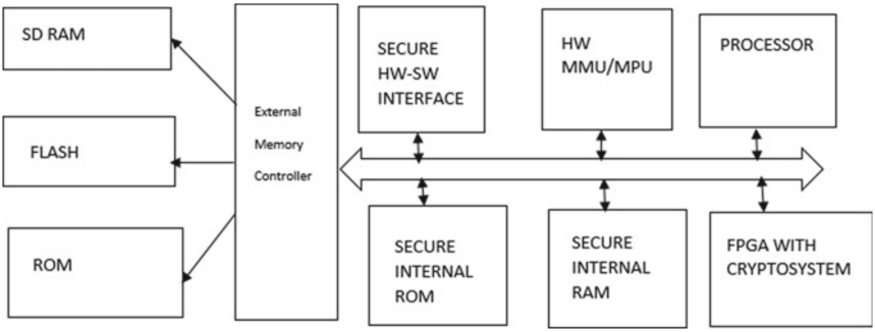


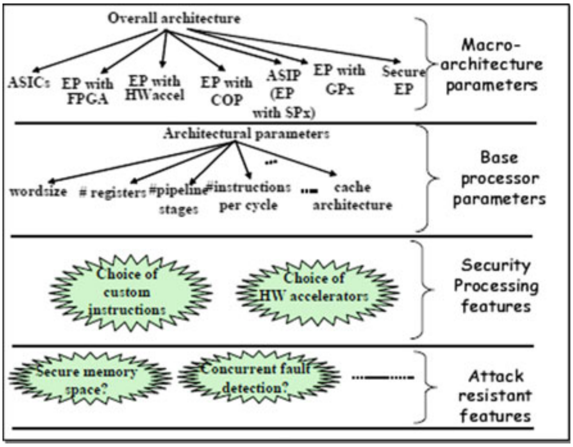
Fig. 2 Architecture of embedded systems in IoT

3 Processor

The processor forms an integral part of any application linked to the IoT. It is very much necessary to have a secure processor in an IoT environment. The security of the processor is dependent on the architecture it is built upon. There has always been a constant effort made by the designers to make the system completely secure. A result of these efforts is shown in the different architectures that have been developed in order to provide more security to the system. The design space available to the designers provides a brief idea about the different parameters and features that need to be addressed. The architectural design space of a processor is represented as shown in Fig. 3.

The first row provides the different architecture that can be implemented such as an ASIC or an embedded general-purpose processor with FPGA or an embedded processor with graphic processing capabilities or a secure embedded processor. The second row provides an idea about the different architectural parameters that need to

Fig. 3 Architectural design space



be considered such as the instruction cycle and word size. The third row articulates security processing features that should be considered for design. The fourth row involves selection of attack resistant features in the embedded system design [5].

Many designs have been implemented which try to focus on each of the parameters and features suggested by this architectural design space. A modern-day embedded application such as secure integrated cards commonly referred to as smart cards employs a bi- processor architecture. In general, the first CPU is configured to perform tasks that do not require utilization of sensitive information. A second CPU which can be referred to as a master CPU is configured to perform tasks that involve manipulation of sensitive information. Both CPUs communicate through a secure interface. Though this architecture provides an enhanced overall security of the embedded system, it does have some disadvantages. Primarily, the overall power consumption of the system will be very high, and as a result, the cost of the application also increases [6].

Internet of things requires the embedded systems to be miniaturized. As a result, architectures employed need to be smaller, efficient and more secure. The Aegis processor [7] provides an increased efficiency and reduction in power consumption as it makes use of a single processor only. The Aegis processor architecture helps build computing systems that are secure against both software and physical attacks with minimum performance overhead for typical embedded applications. However, there is a scope for improvement in this architecture. Firstly, the performance overhead can be reduced for applications which do not require more memory which will help in employing efficient encryption and system verification. Secondly, the architecture is prone to physical attacks. Protecting the IC from side-channel analysis and other hardware Trojans is required. Figure 4 shows the architecture of an Aegis processor. The state of the art processors employed in IoT is mostly RISC processors due to its simple architecture and low power consumption. RISC processors help to accelerate the execution of simplified instructions. As against CISC architecture,

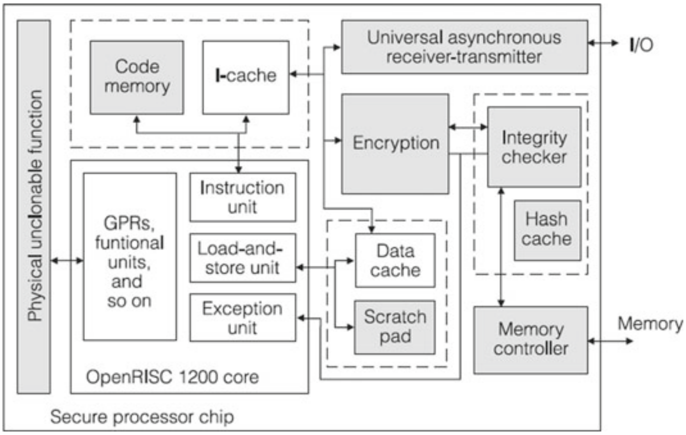


Fig. 4 Aegis processor architecture [7]

RISC methodology utilizes a complex instruction set to achieve high code density and save costly memories. In IoT network, there is a limitation on the memory space due to area and power constraints. In such cases, CISC processor is an advisable solution. The scalable and reconfigurable micro-coded multi-core processor is a proposed architecture for a CISC processor. The main advantage of this architecture is its increased efficiency [8].

The recent trends in processor architecture for embedded systems are a generalized architecture which requires lesser programming, high energy efficiency and enhanced security aspects. There are few processors available today which do provide the required security along with low power consumption and high performance. The most widely used processor is the ARM processor. Figure 5 shows the architecture of ARM Cortex M4 processor. However, this processor is also not completely secure. Researches show that the information in such processors can be leaked through radio frequency, optical, power and timing side channels and by interfaces such as JTAG and RS232. The most prominent locations for hardware Trojans are memory units and clocking units. In order to ensure hardware security of a processor, it is necessary to identify the critical components that could fall prey to such malicious intrusions at the design stage. In a processor, the vital information is always stored in the memory. So an attacker would always attempt to obtain access to the memory. Hence, memory and communication buses are the most critical components to be taken into account while designing for security and memory authentication plays a crucial role in safeguarding against threats.

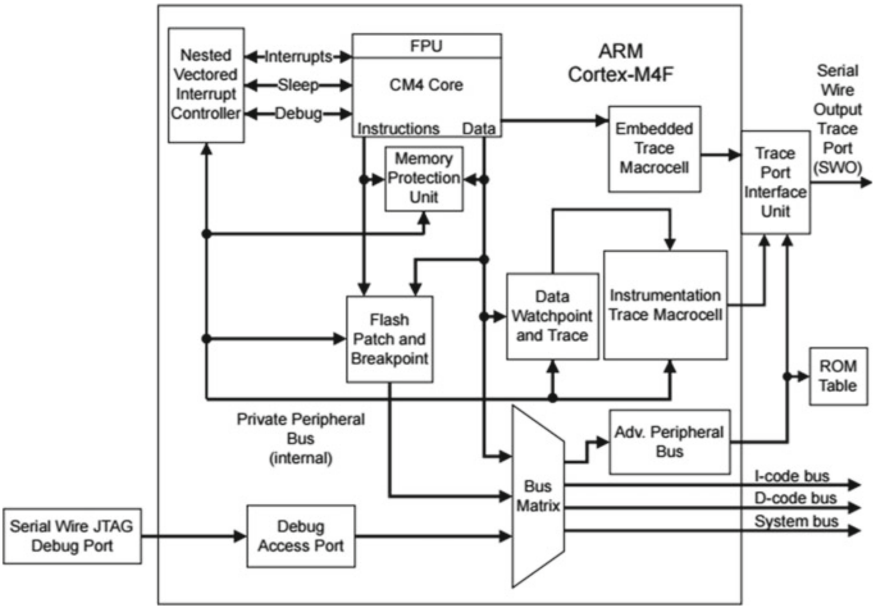

Nested Vectored Interrupt Controller
Interrupts
Sleep
Debug
FPU
CM4 Core
Instructions
Data
ARM Cortex-M4F
Embedded Trace Macrocell
Memory Protection Unit
Serial Wire Output Trace Port (SWO)
Trace Port Interface Unit
Data Watchpoint and Trace
Instrumentation Trace Macrocell
Flash Patch and Breakpoint
ROM Table
Private Peripheral Bus (internal)
Adv. Peripheral Bus
Bus Matrix
I-code bus
D-code bus
System bus
Serial Wire JTAG Debug Port
Debug Access Port

Fig. 5 ARM Cortex M4 processor [9]

4 Secure Embedded Processor Design Challenges

Since embedded systems need to fulfill the security requirements for the application they are designed for, a number of challenges are faced at the design stage. These include processing gap, flexibility, battery limitation, tamper resistance and cost [5].

- Complexity of security protocols and increased data rates make it difficult for the embedded processor to keep up with computational demands involved.
- The embedded systems need to be flexible to support multiple security mechanisms and protocols.
- Battery operated systems face a limitation of power available for performing computations.
- The only mechanism that can guarantee foolproof security is through resistance implementation into the hardware design.
- Implementation of security at the hardware level results in a sharp rise in cost due to the additional circuitry involved. Therefore, there always exists a tradeoff between security and cost.
- There also arises the need for designers to be well informed of the security implications of the design so that the design cycle can be modified to evaluate security at the different stages.

When linked to the IoT, there is a huge amount of data storage and transfer operations involved. Hence, safeguarding memory from potential attacks is a prime challenge. Establishing security between endpoints in a network can only be carried out after taking into account the cryptographic schemes, networking protocols and communication standards.

5 Memory Attacks

Ability to verify that the data read from a specific memory location by a processor is the same as the one it stored at the location during last write is referred to as memory authentication [10]. The main assumption in past works was that the processor chip alone is trusted. One technique involves storing the cryptographic digest of external memory on a trusted area of chip and comparing the data read from the external memory with the digest each time a read is performed. This is a tedious method as all data from external memory should be fetched to perform integrity checking for every read. For every write operation, the data needs to be updated as well. Another solution suggested involves keeping separate cryptographic digests for various memory blocks. This helps to bring down the memory bandwidth problem in the previous method but increases the cost due to requirement for additional hardware. An optimal solution using tree-based structures has also been proposed. In this approach, the leaves are the memory blocks to be shielded from attacks, and the root node computes the current state of the memory block by applying an authentication primitive to tree nodes starting from leaves.

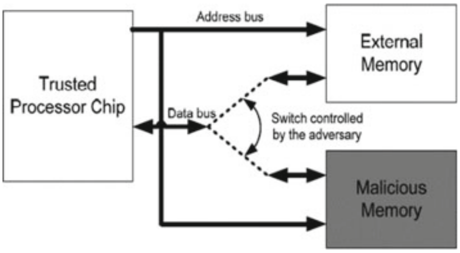


Fig. 6 An attack model of the memory [10]

Prevention of attacks to the memory is the primary goal of memory authentication. Spoofing attacks, splicing attacks and replay attacks are the three main categories of active attacks that an adversary resorts to. Figure 6 shows a model of a memory attack. In spoofing attacks, adversary replaces a memory block with a malicious one by obtaining access to the data bus by means of a control switch. In splicing attacks, the adversary keeps a copy of the original data in a malicious memory. The activation of the switch command by the adversary forces the processor to read data from the malicious location. Replay attacks involve the replacement of memory content with a previous data stored there. The adversary copies data from an address location to the malicious memory to be used later to alter the contents of the same address location.

Multiprocessor technology is widely used in high-end computing platforms. In multiprocessor systems, we require to include security aspects of shared memory also. In symmetric multiprocessors in order to ensure cache coherence, a processor sends the same data to all the cores along with the intended core. An attack that comes into play in this context is message dropping where one of the cores may be temporarily cut off from the bus. So the need arises for bus transaction authentication on cache to cache transfers. Figure 7 depicts message dropping attack on symmetric multiprocessor platform (SMP).

Elbaz et al. [10] discuss a technique for data encryption and authentication on processor-memory bus wherein after adding cipher to the data, a data integrity check is also performed to confirm the authenticity of information. This technique is applied to guarantee secure data communication between the System on Chip (SoC) and external memory. External memory usually holds sensitive information, and an adversary would try to attack the data bus to acquire it. In order to prevent central processing unit (CPU) modification, hardware security measures are inserted between

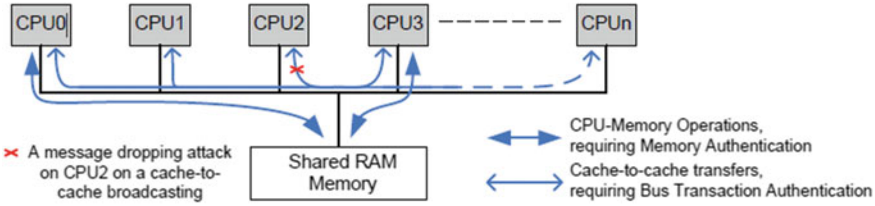

CPU0
CPU1
CPU2
CPU3
CPUn
A message dropping attack on CPU2 on a cache-to-cache broadcasting
Shared RAM Memory
CPU-Memory Operations, requiring Memory Authentication
Cache-to-cache transfers, requiring Bus Transaction Authentication

Fig. 7 Message dropping attack on SMP

the cache memory and memory controller. An additional tag is appended to the plaintext before encryption. The CPU processes read-only and read/write data. The tag used for each of these is different. Since a read-only data stored once in external memory is not modified during program execution and also since the encryption key is the most significant address bits of the encrypted block as tag (T). In the event of a splicing attack, the address used by processor to fetch the data block from the external memory and the address used by the integrity checker to generate tag (T') will not match the stored tag (T). Figures 8 and 9 show the diagrammatic representation of the process.

From a broader angle, malicious attacks on the smart grid could impact devices and users across continents since IoT technology is involved. Data from the smart meter could be used by an adversary as an information side-channel to study customer behavior or habits. Smart grid technology is one of the many applications in IoT which highlights the vulnerabilities involved in the system. These vulnerabilities and challenges arise as a result of the integration of cyber and physical systems [11–13]. It draws our attention to the other side of the coin where the challenges like privacy and security of the users, as well as data, need to be safeguarded through effective hardware design and analysis [14].

The need for development of hardware security also stems from the fact that most of the existing security solutions were developed keeping software concerns in mind. These solutions as described in the paper by Babar et al. [15] reveal that the software attacks are well taken care of while most of the hardware attacks are unguarded. In order that an entirely secure system be developed, both the hardware and software needs to be immune to attacks.

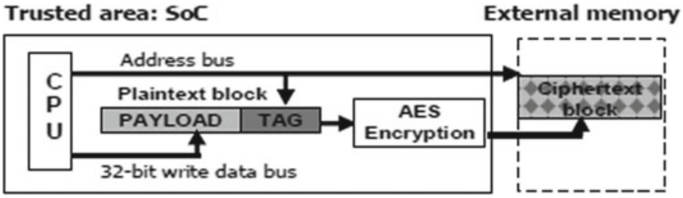


Fig. 8 Tag insertion and encryption during write

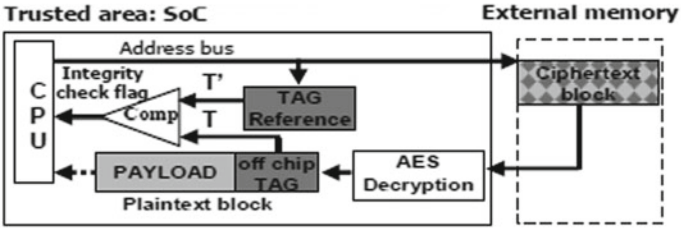


Fig. 9 Decryption and tag matching during read

6 Conclusion

High level of security in an IoT system can be achieved by addressing all possible threats that can affect both hardware and software of the system. The design of embedded systems, which are an essential building block of IoT, will help safeguard the system against hardware attacks. Memory unit of a general-purpose embedded processor needs a secure design to thwart malicious attacks as they are programmed as per user applications. Developing algorithms for memory protection and Trojan detection will prove as a milestone in secure design of embedded systems for IoT applications.

References

1. Zhao K, Ge L (2013) A survey on the internet of things security. In: 9th international conference on computational intelligence and security (CIS). IEEE, pp 663–667
2. Gubbi J, Buyya R, Marusic S, Palaniswami M (2013) Internet of Things (IoT): a vision, architectural elements, and future directions. Future Gener Comput Syst 29(7):1645–1660
3. Atzori L, Iera A, Morabito G (2010) The internet of things: a survey. Comput Netw 54(15):2787–2805
4. Xu T, Wendt JB, Potkonjak M (2014) Security of IoT systems: design challenges and opportunities. In: Proceedings of the 2014 IEEE/ACM international conference on computer-aided design. IEEE Press, pp 417–423
5. Kocher P et al (2014) Security as a new dimension in embedded system design. In: Proceedings of the 41st annual design automation conference. ACM
6. Kaabouch M, Le Cocquen E (2011) Bi-processor architecture for secure systems. U.S. Patent No. 7,984,301. 19 July 2011
7. Suh GE, O'Donnell CW, Devadas S (2005) AEGIS: a single-chip secure processor. Inf Secur Tech Rep 10(2):63–73
8. Ma N et al (2014) A hierarchical reconfigurable micro-coded multi-core processor for IoT applications. In: 9th international symposium on reconfigurable and communication-centric systems-on-chip (ReCoSoC). IEEE
9. ARM Processors, www.ti.com/lit/er/spmz637/spmz637.pdf
10. Elbaz R et al (2009) Hardware mechanisms for memory authentication: a survey of existing techniques and engines. In: Transactions on computational science IV. Springer Berlin Heidelberg, pp 1–22
11. Khurana H, Hadley M, Lu N, Frincke DA (2010) Smart-grid security issues. IEEE Secur Priv 8(1):81–85
12. Liu J, Xiao Y, Li S, Liang W, Chen CP (2012) Cyber security and privacy issues in smart grids. IEEE Commun Surv Tutor 14(4):981–997
13. Simmhan Y, Kumbhare AG, Cao B, Prasanna V (2011) An analysis of security and privacy issues in smart grid software architectures on clouds. In: IEEE 4th international conference on cloud computing. IEEE, pp 582–589
14. McDaniel P, McLaughlin S (2009) Security and privacy challenges in the smart grid. IEEE Secur Priv 1(3):75–77
15. Babar S et al (2011) Proposed embedded security framework for internet of things (IoT). In: 2nd IEEE international conference on wireless communication, vehicular technology, information theory and aerospace & electronic systems technology (Wireless VITAE), Feb 28. IEEE, pp 1–5

Decentralized Bagged Stacking Ensemble Mechanism (DBSEM) for Anomaly Detection

S. L. Sanjith and E. George Dharma Prakash Raj

Abstract Intrusion detection has become a major need for the current networked environment due to the high usage levels and the mandatory security that is needed, as sensitive information are being shared in the network. However, there exist several intrinsic issues in the network data that complicates the detection process. Further, real-time detection is also required due to the high velocity of data flow that can be expected in the domain. This paper presents an ensemble-based intrusion detection model to handle data imbalance and noise. Further, the entire approach has been decentralized to enable parallelized detection. The proposed model utilizes a BAgged Stacking Ensemble (BASE) as the detection model. The ensemble architecture initially creates data bags, enabling distributed processing. The bags are processed by multiple heterogeneous base learners. Prediction results from the base learners are passed to a stacked classifier for final predictions. This ensemble model is distributed over the network to enable decentralized processing. Experiments were performed on the NSL-KDD data and the results were compared with recent models. Comparisons with state-of-the-art models indicate the effectiveness of the proposed model.

Keywords Intrusion detection · Ensemble · Stacking · Bagging · Decentralization

1 Introduction

A huge development in the computing and networking environments have been witnessed in the current decade. However, awareness in terms of technology and threats to technology are still uncalled for. Further, even the improvements in protection technologies are still remaining to be enhanced for want of better protection schemes. This has resulted in the network intrusion domain moving towards evolving security

S. L. Sanjith (✉)
Indian Institute of Management Tiruchirappalli, Tiruchirappalli, Tamilnadu, India
e-mail: sanjithsl@gmail.com

E. George Dharma Prakash Raj
Bharathidasan University, Tiruchirappalli, Tamilnadu, India
e-mail: george.prakashraj@yahoo.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_71

based mechanisms [1]. This is assumed to provide better detection of the security threats.

Although several intrusion detection mechanisms such as malware prevention modules, firewalls, authentication mechanisms, and data encryption schemes are available, they are still not sufficient for the intrusion detection process [2]. The current network models seems to mandate additional defense mechanisms for want of additional security.

Artificial intelligence and artificial intelligence-based systems have become most used approaches for detection of intrusions in networks [3, 4]. The improvements in artificial intelligence-based models has made this domain one of the sought out domains in the network intrusion detection scenario. Further, artificial intelligence-based technologies can also work well with legacy intrusion detection models. Hence they are used in conjunction with existing mechanisms for providing better security for the user.

Intrusion detection models are generally classified into two categories [5]. First is the misuse based detection models, where packet signatures are analyzed and the model specifically concentrates on handling anomalous signatures. Second is the anomaly-based detection models that aims to learn the signatures of normal packets to identify the records that exhibits deviations when analyzed from the perspective of normal packets are to be flagged as anomalous.

Domain analysis further reveals that the intrusion detection domain suffers from the issue of data imbalance and noisy data [6]. Data imbalance refers to the existence of a large number of instances in one class usually termed as the majority class and relatively less number of instances of another class usually referred to as the minority class [7]. This results in the majority classes getting overtrained, while the minority classes remain undertrained. An example for data imbalance is presented in Fig. 1.

This work presents a Decentralized Bagged Stacking Ensemble (DBSEM) based model that can effectively enable faster and more accurate predictions. Bagging was observed to effectively reduce the issue of data imbalance to a large extent. Further, it was also observed that stacking the ensemble was able to reduce the effects of noise. Experimental results and comparisons indicate demonstrates the effectiveness and efficiency of the proposed model.

2 Literature Review

Intrusion detection has gained significance due to the increased reliance on networks and network-based communication. Though there is a huge amount of literature corresponding to this domain, there is still a need for a decentralized, flexible and reliable intrusion detection model. This section discusses some of the most recent and most prominent works in the domain of intrusion detection.

An intrusion detection model using lazy learning methodology was provided by Chellam et al. [8]. Lazy learning was observed to exhibit high computational complexity levels. This model proposes a weighted indexing technique, to reduce the

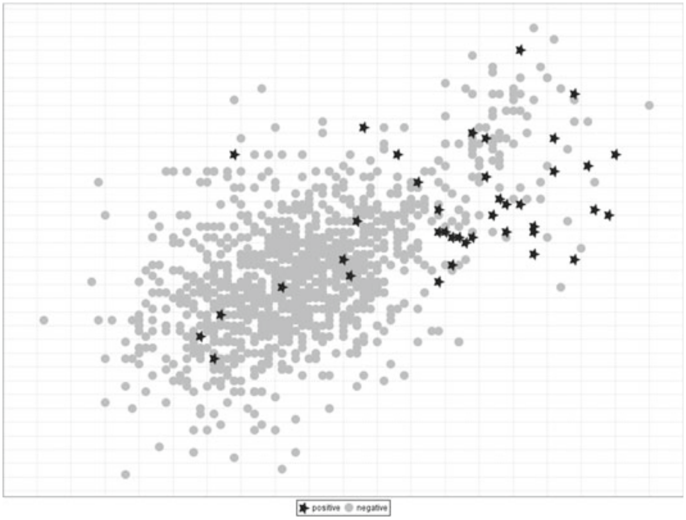


Fig. 1 Data imbalance—a graphical view

computational capacity of last learning models. An imbalance handling model that is a variant of the RIPPER algorithm was presented by Cieslak et al. [9]. This is a clustering-based approach that handles data imbalance by artificial generation of minority classes. An anomaly-based intrusion detection model was presented by Wang et al. [10]. This method trains on regular network behavior data and can effectively predict anomalous behaviors. The model is based on Principal Component Analysis (PCA) as the initial preprocessing technique. A J48 based intrusion detection model specifically designed for high dimensional data was presented by Shahbaz et al. [11]. This technique is based on feature extraction and feature selection for highly improved detection of intrusions.

A real-time model for intrusion detection in high-speed networks was presented by Rathore et al. [12]. This is a Hadoop-based model that operates on REPTree and J48 algorithms. The model selects nine best parameters for the processing architecture enabling highly effective predictions. The research directions have further moved forward from Hadoop and has now started using spark-based models for prediction. A spark-based technique for network intrusion detection on streaming data was presented by Dahiya et al. [13]. This technique is based on two feature reduction algorithms; Canonical Correlation Analysis (CCA) and the Linear Discriminant Analysis (LDA). These algorithms enable faster and more accurate predictions on the streaming network data. A parallelized anomaly detection model using Spark was presented by Yafei et al. [14]. This model is based on HOTSAX intrusion detection algorithms. The HOTSAX algorithm has been parallelized using the Spark architecture to enable faster processing. Other similar streaming data-based intrusion detection models includes Big Data-based model by Juliette et al. [15], sensor data-based model by Michael et al. [16], loss based model by Bamakan et al. [17] and metaheuristic based model by Tamer et al. [18].

Although metaheuristic models were employed for their speed and effective predictability levels, several applications involve metaheuristic models only for the preprocessing phase. A Firefly algorithm based intrusion detection model was presented by Selvakumar et al. [19]. This technique uses Firefly algorithm for the process of Feature Selection on network data. A similar PCA based network intrusion detection model was presented by Salo et al. [20]. Artificial neural network-based intrusion detection model was presented by Shenfield et al. [21]. This technique is based on fine-tuning the artificial neural network for effective prediction of network data. Although the model proves to be effective with high prediction accuracy levels, the computational complexity of neural networks is high, hence making the model less suitable for real-time data analysis. Extreme learning machines have been gaining prominence in the current periods due to the flexibility they provide. An extreme learning machine based model was presented by Wang et al. [22]. This model utilizes the equality constrained optimization technique to improve the detection levels. The model has also been designed as an adaptive technique to enable effective results. Other prominent ELM based models include approximation based model [23], random search based model [24] and error minimized ELM [25].

3 Decentralized Stacked Ensemble Model for Anomaly Detection

Anomaly detection in network environments is usually centralized. All the generated network transactions are initially passed to the centralized server. The anomaly detection model is usually deployed in the centralized server. The model performs predictions to identify if the particular transaction is normal or anomalous. The decision-making process is always performed on the centralized server. Hence the server usually handles higher loads, hence the prediction process is usually slow. A decentralized architecture that can handle distributed workloads can provide faster predictions. This work proposes a decentralized ensemble architecture for handling distributed workloads in the network.

3.1 Decentralization of Architecture

Decentralization in the architecture is achieved by deploying the anomaly detection model on multiple models. Network transmission data is analyzed by these nodes and anomalies are detected. The major advantage is that every node analyses its own data, hence prediction is faster and is closer to the source, making the predictions real-time effective.

3.2 Decentralized Bagged Stacking Ensemble (DBSEM) for Anomaly Detection

Every node in the network is embedded with an intrusion detection model. The intrusion detection model is composed of the data preparation phase, the process of bag creation, creation, and training of the heterogeneous base learners and finally the stacked meta-model for final prediction. The architecture for DBSEM model is shown in Fig. 2. The algorithm for the proposed model is shown below.

Algorithm

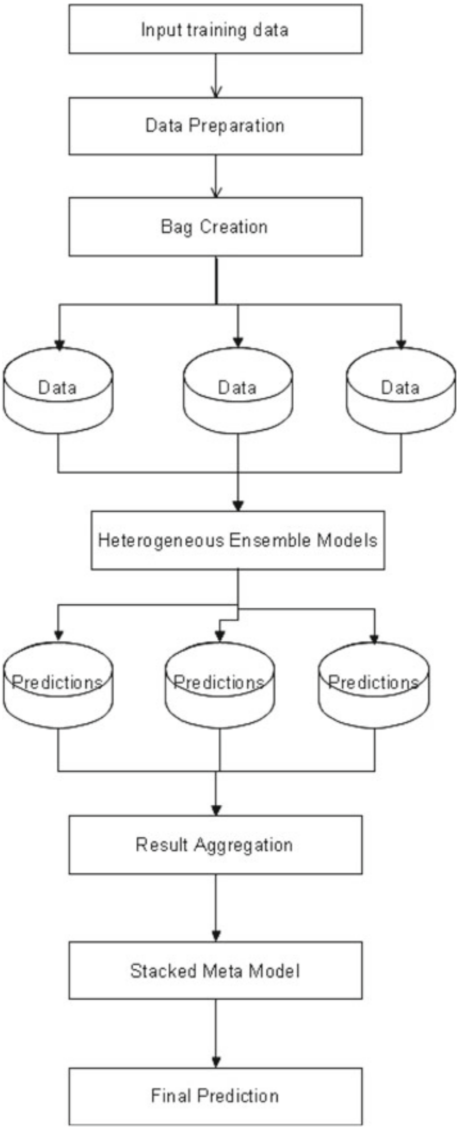
1. *Input training data*
2. *Data preprocessing and data cleaning*
3. *Data sampling to create multiple bags*
4. *Pass bags to heterogeneous ensemble models*
5. *For each obtained data bag b*
    a. *Apply training data b to obtain the trained model*
    b. *Apply test data to model*
    c. *Obtain predictions*
6. *Aggregate predictions from ensemble models*
7. *Append actual predictions with the generated predictions to form the input data for meta-model*
8. *Pass the data to meta-model for training*
9. *To perform final prediction pass validation data to ensemble model*
10. *Aggregate predictions and pass it to the meta-model*
11. *Obtain final predictions from the meta-model*

Data Preparation Input data is composed of network packets that pass through the network. The packet data consist of several internal transfer details. Some data sets might contain missing values, while others may contain erroneous values. These data must be imputed or cleared to make the data fit for processing. This is done during the data preparation or preprocessing phase. The input data is analyzed and the instances containing missing values and erroneous values are deleted. Further, machine learning models operate only on equally distributed double values. Hence, data containing integers are normalized using

$$\text{Norm} = \frac{x - x_{\text{min}}}{x_{\text{max}} - x_{\text{min}}}(\max - \min) + \min \qquad (1)$$

where x is the actual value to be normalized, $x_{\max}$ and $x_{\min}$ are the minimum and maximum values in the attribute, max and min are the interval ranges between which the normalization is to be performed. This work uses a value of 0 and 1 for $x_{\min}$ and $x_{\max}$, respectively. The cleaned data is passed to the stacked ensemble model for analysis.

Fig. 2 DBSEM architecture



Bag Creation Phase The input data is composed of several instances, and the training data is usually composed of the entire data. However, the proposed work uses multiple learning models. Passing the entire data for all the models will result in creation of same decision rules. Hence, the input training data is divided into multiple training data bags, where each data bag is composed of 60% of the entire training data. This process of data sampling results in random distribution of data to each of the heterogeneous learners, and at the same time, results in some similarity in the data patterns between the various base learners. This process of data distribution results in highly effective predictions.

Creation of Heterogeneous Base Learners Heterogeneity in base learners is maintained in the base learners, hence enabling varied rules in-order to create a robust classifier model for prediction. This work utilizes Decision Tree and Random Forest as base learners for the process. Both the base learners are intentionally set as tree-based learners. Tree-based learners are effective in creating decision points with maximum information gain. Hence using them during the ensembling process enables discovery of varied rules. The rules with highest information gain can then be retained for the future processes. Another major advantage of using ensemble models is that the overall model can be tuned effectively such that it avoids overfitting.

All the created bags are passed through the base learners. Every bag is passed through both the base learners and the base learner training is performed. Every base learner is trained using different training data, hence their decision rules are also different. The test data, when passed through each of the base learner provides predictions. However, it results in multiple predictions. A single prediction for each base learner. These predictions are not directly combined, instead, it is passed to a second level meta-learner for final predictions.

Stacked Meta-Model for Final Prediction Predictions from the previous level are passed to the stacked meta-model for the final prediction. All the predictions are combined, along with the actual labels to obtain the training data for the meta-model.

This phase is constructed with logistic regression as the prediction model. The major advantage of using logistic regression as the preferred model is that it utilizes a linear model for fitting the objective function. As the required predictions are to be performed from the previous predictions, utilizing a simple linear model is observed to exhibit effective predictions. Further, Logistic Regression is the de facto model that is usually utilized in stacking models.

The predictions, along with the actual labels are passed to the Logistic Regression model. Logistic Regression is used as the meta prediction model. The main functionality of this model is that it learns the issues of the previous model to provide the final predictions. Results from this model is used as the final prediction.

3.3 Prediction Analysis

Intrusion detection in network transmission data is usually modeled as a binary classification problem. The predictions are usually provided to mark transactions as normal or anomalous. Prediction analysis is performed by initially filtering the anomalous predictions and the transactions that correspond to these predictions. Anomalous transactions exhibit higher significance compared to normal transactions. Hence prediction of such transactions gains considerable significance over the prediction of the normal classes.

The major reason for performing this process is that it is mandatory for the models to reduce False Positive predictions. Hence re-analyzing the anomalous transactions becomes a necessary component of the domain.

3.4 Secondary Prediction of Anomaly Data

The prediction process explained in the previous sections is performed in each node of the network. The anomalous data that has been filtered in the previous phase is passed to all the other nodes in the network. This transmission has been done for two purposes; first, every node must have updated anomalous signatures. This maintains that all the nodes are up-to-date with the anomalous signatures. Further, the anomalous signatures should be confirmed to make sure that they are actually anomalous.

The anomalous signatures identified from each node is passed to all the other nodes. Predictions are obtained from these nodes and these predictions are transferred back to the origin node. The origin node performs voting to identify the final prediction. The final prediction is transferred to all the available nodes to be saved as an anomalous signature.

4 Result Analysis

The proposed DBSEM model has been implemented using Python. NSL-KDD dataset is used to measure the significance of the proposed model. The NSL-KDD data is composed of 14 attributes. Details about the attributes are shown in Table 1. Experiments were performed using 10-fold cross-validation, and the results were obtained. Results have been analyzed in terms of standard classifier performance metrics.

The Receiver Operating Characteristics (ROC) curve for the proposed model is shown in Fig. 3. The graph is created by plotting FPR in the *x*-axis and TPR in the *y*-axis. The area of the obtained curve provides the prediction efficiency of the model. Higher area represents better performance. It could be observed that the below curve exhibits the highest area, exhibiting the efficiency of the proposed model.

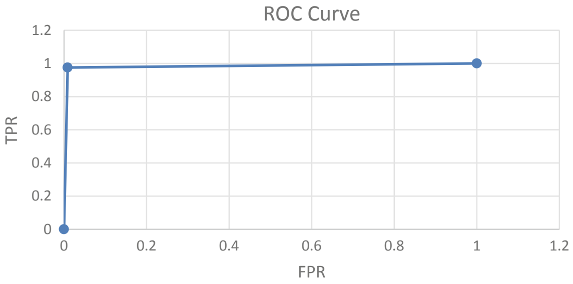
The Precision Recall (PR) curve presents the prediction efficiency of the proposed models. High precision and high recall are the requirements of the classifier model. It could be observed in Fig. 4 that the proposed model exhibits very high precision and recall values that are close to 1, exhibiting the effectiveness of the proposed DBSEM architecture.

The table depicting the performance of the proposed DBSEM model is shown in Table 2. It could be observed that FPR and FNR, shows values closer to 0, while all the other metrics shows values closer to 1. This elucidates the significance of the prediction mechanism.

Table 1 NSL-KDD attributes

No.	Attribute
1	src_bytes
2	service
3	dst_bytes
4	flag
5	diff_srv_rate
6	same_srv_rate
7	dst_host_srv_count
8	dst_host_same_srv_rate
9	dst_host_serror_rate
10	dst_host_srv_serror_rate
11	dst_host_diff_srv_rate
12	serror_rate
13	logged_in
14	Attack

Fig. 3 ROC curve



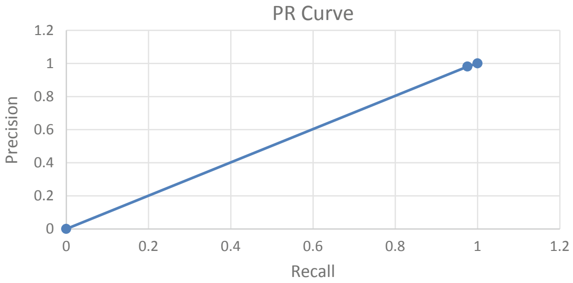


Fig. 4 PR curve

Table 2 Performance metrics of the proposed model

	Proposed model (DBSEM)
TPR	0.98
FPR	0.01
TNR	0.99
FNR	0.02
Accuracy	0.99
Precision	0.98
Recall	0.98
F1 Score	0.98

A comparison of the proposed DBSEM model with the RampLoss model [25] and the previous work of the authors (Reinforcement based Heterogeneous Ensemble Model-RHEM) is shown in Fig. 5 and Table 3. It could be observed that all the models exhibit almost similar predictions. However, it should be observed that the proposed model is decentralized and operates with just a part of the data, while RampLoss model and RHEM are centralized approach utilizing the entire spectrum of available information. Further, the time requirements of the proposed model is much less compared to the RampLoss model and RHEM due to the decentralized nature of the proposed DBSEM architecture.

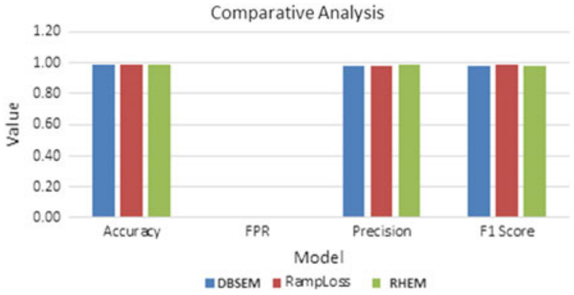


Fig. 5 Comparative analysis

Table 3 Comparison of metrics

	Proposed model—DBSEM	RampLoss (Centralized) Bamakan et al.	RHEM—reinforcement-based model (Centralized) Sanjith et al.
Accuracy	0.99	0.99	0.99
FPR	0.01	0.01	0.00
Precision	0.98	0.98	0.99
F1 score	0.98	0.99	0.98

5 Conclusion

Intrusion detection has been one of the significant areas of research in the current decade, due to the increasing necessity for security in network transmissions. This work proposes an effective intrusion detection model that has been developed in a decentralized fashion to enable faster and more effective detection of anomalies. The Decentralized Bagged Stacking Ensemble Model (DBSEM) architecture has been designed to provide faster and more accurate predictions in a decentralized manner. Input data is converted into data bags and are passed to the base learners. The base learners train on the input data and generates predictions. These predictions are collected and passed to the secondary algorithm for meta-learning. This stacking structure enables improved predictions. Experiments were performed using NSL-KDD data and the results were compared with state-of-the-art models. The results indicate the effectiveness and the high performing nature of the proposed DBSEM architecture. The proposed architecture has been found to be highly scalable and tends well to parallelization. Future enhancements will be towards implementing the model on streaming architectures like SPARK.

References

1. Pontarelli S, Bianchi G, Teofili S (2013) Traffic-aware design of a high-speed fpga network intrusion detection system. IEEE Trans Comput 62(11):2322–2334. https://doi.org/10.1109/TC.2012.105
2. Garcia-Teodoro P, Diaz-Verdejo J, Maciá-Fernández G, Vázquez E (2009) Anomaly-based network intrusion detection: techniques, systems and challenges. Comput Secur 28(1–2):18–28
3. Tang Y, Chen S (2007) An automated signature-based approach against polymorphic internet worms. IEEE Trans Parallel Distrib Syst 18(7):879–892
4. Tan Z, Jamdagni A, He X, Nanda P, Liu RP (2014) A system for denial-of-service attack detection based on multivariate correlation analysis. IEEE Trans Parallel Distrib Syst 25(2):447–456
5. Bhuyan MH, Bhattacharyya DK, Kalita JK (2014) Network anomaly detection: methods, systems and tools. IEEE Commun Surv Tutorials 16(1):303–336
6. Akila S, Srinivasulu Reddy U (2016) Data imbalance: effects and solutions for classification of large and highly imbalanced data. Proc ICRECT 16:28–34
7. Akila S, Srinivasulu Reddy U (2017) Modelling a stable classifier for handling large scale data with noise and imbalance. In: IEEE international conference on computational intelligence in data science
8. Chellam A, Ramanathan L, Ramani S (2018) Intrusion detection in computer networks using lazy learning algorithm. Procedia Comput Sci 132:928–936
9. Cieslak DA, Chawla NV, Striegel A (2006) Combating imbalance in network intrusion datasets. In: GrC, pp 732–737
10. Wang W, Battiti R (2006) Identifying intrusions in computer networks with principal component analysis. In: Proceedings of the first international conference on availability, reliability and security, pp 270–279
11. Shahbaz MB, Wang X, Behnad A, Samarabandu J (2016) On efficiency enhancement of the correlation-based feature selection for intrusion detection systems. In: 2016 IEEE 7th annual information technology, electronics and mobile communication conference (IEMCON), pp 1–7

12. Rathore MM, Paul A, Ahmad A, Rho S, Imran M, Guizani M (2016) Hadoop based real-time intrusion detection for high-speed networks. In: 2016 IEEE global communications conference (GLOBECOM), pp 1–6
13. Dahiya P, Srivastava DK (2018) Network intrusion detection in big dataset using spark. Procedia Comput Sci 132:253–262
14. Wu Y, Zhu Y, Huang T (2015) Distributed discord discovery: spark based anomaly detection in time series. IEEE
15. Dromard J, Roudière G, Owezarski P (2015) Unsupervised network anomaly detection in real-time on big data. Springer, Berlin
16. Hayes MA, Capretz MAM (2015) Contextual anomaly detection framework for big sensor data. Springer, Berlin
17. Bamakan SMH, Wang H, Shi Y (2017) Ramp loss K-support vector classification-regression; a robust and sparse multi-class approach to the intrusion detection problem. Knowl-Based Syst 126:113–126
18. Ghanem TF, Elkilani WS, Abdul-kader HM (2014) A hybrid approach for efficient anomaly detection using metaheuristic methods. J Adv Res
19. Selvakumar B, Muneeswaran K (2019) Firefly algorithm based feature selection for network intrusion detection. Comput Secur 81:148–155
20. Salo F, Nassif AB, Essex A (2019) Dimensionality reduction with IG-PCA and ensemble classifier for network intrusion detection. Comput Netw 148:164–175
21. Shenfield A, Day D, Ayesh A (2018) Intelligent intrusion detection systems using artificial neural networks. ICT Express 4(2):95–99
22. Wang CR, Xu RF, Lee SJ, Lee CH (2018) Network intrusion detection using equality constrained-optimization-based extreme learning machines. Knowl-Based Syst 147:68–80
23. Huang G-B, Chen L, Siew C-K (2006) Universal approximation using incremental constructive feedforward networks with random hidden nodes. IEEE Trans Neural Netw 17(4):879–892
24. Huang G-B, Chen L (2008) Enhanced random search based incremental extreme learning machine. Neurocomputing 71(16):3460–3468
25. Feng G, Huang G-B, Lin Q, Gay R (2009) Error minimized extreme learning machine with growth of hidden nodes and incremental learning. IEEE Trans Neural Netw 20(8):1352–1357

The Process and Application of Dual Extruder Three-Dimension Printer

Kunal Sekhar Pati and A. Karthikeyan

Abstract The three-dimension printer means the three-dimensional printing which is also known as additive manufacturing and it is the advanced manufacturing tool used for producing the most complex shape geometries. We can produce complex geometry shapes without using any kind of computer tools. The three-dimensioned printer is used in many fields in the industries because of its most creating and functioning prototype with minimum human resources and time. 3D printer is used in automobile, architecture, engineering, education, medical industries, and civil engineering. It is most reliable, cost-effective and real-time application. The three-dimension printer is widely used and it is a very interesting technology to look out for.

Keywords Three-dimension printing · Additive manufacturing · Printing layer

1 Introduction

3D printing or additive manufacturing is a process of making a three-dimensional object of any shape from digital model with different shapes. Traditional machining techniques based on cutting the materials layer by layers. Layering technique is used when the material is cutting each layer until the complete object is manufactured. In this way, three-dimension D printer moves away from large amount of human resources and we can modified our product according to user or anyone. We can make and customize any product from home or any other place.

First time three-dimension printer is introduced on 1980s where a pattern is submerged in liquid polymer and that would be traced by computer. The traced pattern

K. S. Pati (✉)
Department of Embedded Technology, School of Electronics Engineering, VIT University, Vellore, India
e-mail: Kunalpati4@gmail.com

A. Karthikeyan
Department of Embedded System Technologies, VIT, Vellore, India
e-mail: karthikeyan.anbu@vit.ac.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_72

is hardened into layer. This is the way built an object out of plastic. After tremendous process additive manufacturing methods is introduced. In additive manufacturing process three-dimension objects are adding layer upon layer of materials. Materials vary from technology to technology. The basic concept of additive manufacturing is using of computer for three-dimension modeling software. First thing we have to create is a three-dimension sketch then AM device reads the CAD file from computer and build a structure layer by layer. The material may be plastic, liquid, powder filament.

Now the cost of acquiring three-dimension printing has been decreasing with advancement of technology. Nowadays the usage of three-dimension printer has been raised with average cost ranging on market. For commercial usage three-dimension printers have been increased in every sector on market, for example, aerospace, spare parts manufacturing, automobile, etc. In fact it is required skilled and expertise person to do both software and final printing work. In production industries three-dimension printers are most emerging product on market.

2 How It Works?

There are different types of three-dimension printers' technology in additive manufacturing. We are using fused deposition modeling (FDM).

Fused Deposition Modeling

Fused Deposition Modeling (FDM) technology was developed by Scott Crump in 1980s. In this method, we can print not only prototype but also know the concepts of modeling and user product. FDM three-dimension printing technology based on the thermoplastics materials so the product is very excellent with mechanical, chemical and thermal.

On FDM technology the three-dimension printing machine build the objects layer by layer from bottom to top heating and extruding the thermoplastics filaments. First design a three-dimension CAD layer by layer model on software and printer extruder calculate it layer by layer. Thermoplastic material is supported by printer extruder. Then the printer heats the thermoplastic material at 220 °C on it melting point and extrude it through nozzle on base. A computer of three-dimension printer translates the dimension of *X*, *Y,* and *Z* coordinate and control the nozzle. The base also moves according to the nozzle it means that it coordinate the nozzle. When one layer completed its printing then the base or bed goes down and start printing the next layers. This process is keep on going until the complete object is not printed. Printing time depends on size and complexity of the object. Small object print fast as compare to large object. After complete printing of an object it is take time harden the thermoplastic materials (Fig. 1).

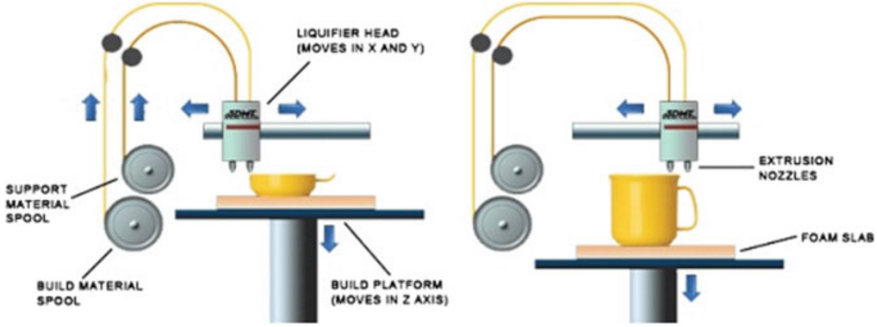
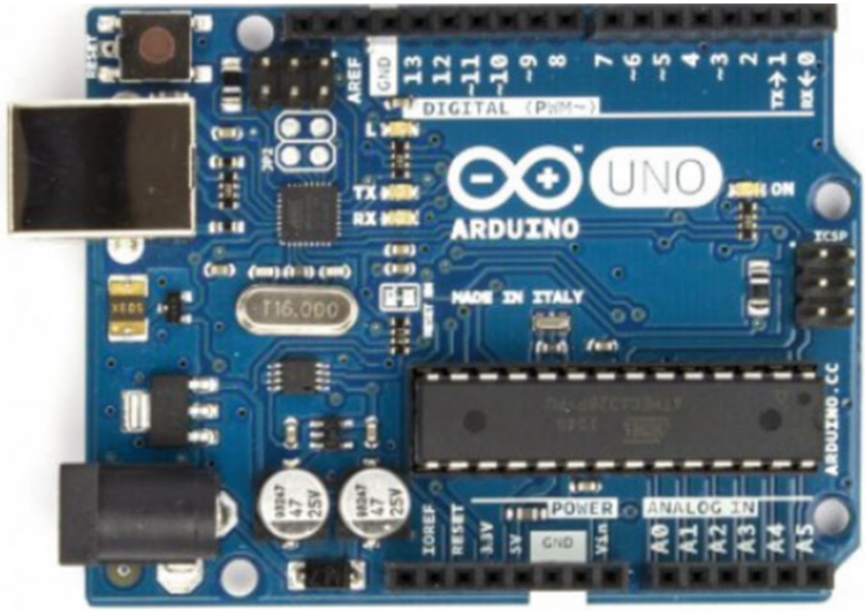


Fig. 1 Fuse deposition modeling process

3 Components

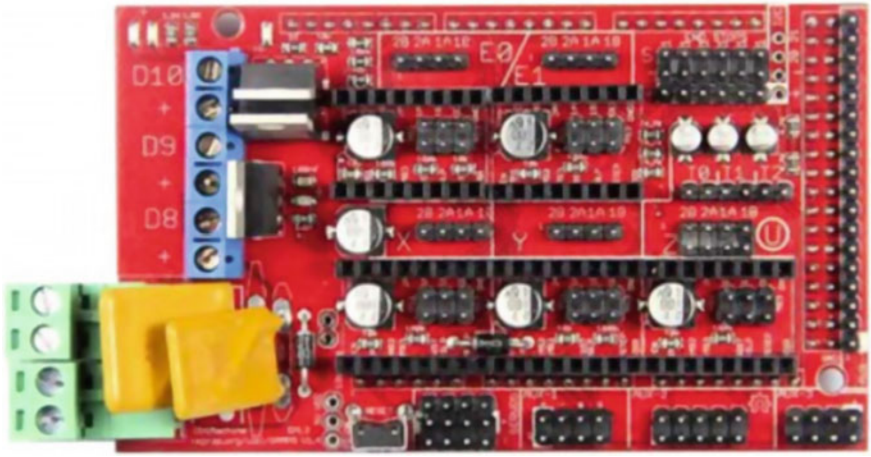
ATmega328 Arduino UNO

- High performance, low power AVR 8-bit microcontroller
- 32 × 8 general-purpose working registers
- 1 kB EEPROM
- 2 kB internal SRAM
- 23 programmable I/O lines
- 2.7–5.5 operating voltage.



Ramp 1.4 3D Printed Control Board

- Expandable to control other component
- 3 MOSFETs for heater and fan
- All MOSFETs are hooked in to PWM
- Option to connect 2 motors on Z
- I2C and SPI pins are also available.



Limit Switch

It is a mechanical block is detected when it is activated. Its help for the alignment between bed and extruder.

Proximity Sensor

It is used for auto leveling and going to need a probe, which can accurate measure the distance of bed at various point.

Servo Motor

Limit switch is used for bed, which is not contact with bottom of the extruder. So servomotor is used for movement of the limit switch, which is fixed besides of the nozzles.

4 Application of Three-Dimension Printers

Product Development

If we need small product then do it as soon as possible. A three-dimension printer is fast, cost effecting, and modified the product as soon as possible at no additional cost with minimum amount of time. It is the best machine to design early-stage design product.

Construction Field

On civil sector, if we construct a huge bridge, building or any other plan so at that time we need first prototype of that structure. Three-dimension printer means early stage of evaluation of the complex and rough design of any construction or architecture.

Medical Field

Hearing aid has been made using three-dimension printing technology. Those brave soldiers who lost his legs or hands-on war field for them three-dimension printer can able to manufacture artificial legs or hands for them. Nowadays doctors are using artificial heart for pharmaceutical testing.

End-Use Parts

Three-dimension printer can produce low volume, customized end-use product. This gives more flexibility to small industries as compare to large batch industries. The cost effecting to this end-use products are low.

5 Advantages

- Three-dimension printer product cost is low as compare to other technology product.
- Three-dimension printer technology saves more time for both human and product those can produce from other technology.
- Three-dimension printers are more efficient, faster and easier.
- Quality of the product more strong and durable.

6 Conclusion

Now the world is changing with the help of three-dimension printer. The use of three-dimension printer in medical sector is going to beyond the level and nobody knows what is in future. The additive manufacturing process helps people in solving many problems. Three-dimension printer is limitless and till now it solves only the scratched, there is still more to be uncovered. Now three-dimension printer is still new technology and continuously improving. It already enhances the life of many patients around the world.

References

1. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6061505/
2. http://www.3dprintingfromscratch.com/common/types-of-3d-printers-or-3d-printing-technologies-overview/
3. https://ultimaker.com/en/blog/52652-the-five-key-3d-printing-applications
4. https://www.medicaldevice-network.com/features/3d-printing-in-the-medical-field-applications/
5. https://www2.deloitte.com/insights/us/en/focus/3d-opportunity/additive-manufacturing-3d-printed-electronics.html
6. https://www.aerospacemanufacturinganddesign.com/article/3d-printings-impact-on-aerospace/
7. https://www.3dnatives.com/en/food-3d-printing220520184/
8. https://www.makersempire.com/7-benefits-of-using-3d-printing-technology-in-education/
9. https://www.teachthought.com/technology/10-ways-3d-printing-can-be-used-in-education/
10. http://www.divbyz.com/industries/education
11. https://www.dovepress.com/3d-printed-patient-specific-applications-in-orthopedics-peer-reviewed-article-ORR
12. https://www.hindawi.com/journals/bmri/2018/4520636/

Face Detection and Natural Language Processing System Using Artificial Intelligence

H. S. Avani, Ayushi Turkar and C. D. Divya

Abstract The objective of this paper is to look at a system based on artificial intelligence that recognizes the faces and the system that processes the natural language. The process of face recognition has three phases: face representation, removal of features, and classification. But the most important phase-out of every phase is extraction. At this stage, the image is extracted from the unique features of the face image. However, variation in appearance remains one of the main factors affecting the accuracy of face recognition systems.

Keywords Natural processing system · Face · Artificial intelligence

1 Introduction

Face recognition technology can verify or identify an individual from a digital image or video source (video frames). Face recognition system works using various methods. Generally, the system compares the selected facial features in the given face image database. Face recognition systems are used to enforce the law, entertainment, monitoring, access to security systems, banking, personal identification, etc. Multiplier reception (MLP), face localization, neural network, Natural Language Processing (NLP), principal component analysis (PCA), hierarchical-PEP, LDA, principle component analysis with RBF, Graphics processing unit, etc. are the most popular face recognition techniques. The face recognition process has three phases, one is faced representation, feature extraction, and classification. Face representation is nothing but a face model and determines the successive algorithm that detects and identifies the face image. The face recognition at the entrance level determines that the given image represents the face. In the next phase, which is the extraction of the function phase, the most unique and useful features (properties) are extracted

H. S. Avani (✉) · A. Turkar · C. D. Divya
Department of Computer Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India
e-mail: avanirao0811@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_73

from the face images. The face image is compared to the images in the database for all the features obtained. This is done in the classification phase. The output from the classification phase gives the identity of the given face image from the database together with the highest matching score (i.e. the smallest differences from the input face image).

2 Literature Review

Face detection and expression recognition using the neural network approach, where the author uses the artificial neural network, the basic propagation algorithm, the multiplier reception (MLP), the principle component analysis, and the RBF and graphics processing unit for the face image process. The basic unit of communication such as body movement facial expressions and physiological reactions are the parameters and the final system should be able to detect facial expression in the same way as the human brain [1].

A face recognition system approach uses artificial neural networks propagation using a face localization or a localized face method. They used biometric, pixel, segmentation, and neuron image processing. First, they check the matching of iso-density lines of subject faces, which means comparisons of sizes or relative distance of facial characteristics such as nose and mouth position of the eyes. The system should recognize the human face at a very high precision density [2].

Using image processing and neural networks, a face recognition system approach based on MATLAB uses methodologies such as discrete cosine transformation, self-recognition map, and neural network. The face image is given as a parameter and has an 81.36% recognition rate for 10 trials [3].

Recognition of the human emotional state by the detection of facial expression is an approach that takes different types of images as the parameter and methodology used is the principle of image pre-processing. And the system is tested with a database of 30 different people with different expressions, the proposed PCM method is more consistently accurate [4].

The processing of natural languages using artificial intelligence uses the NLP approach. Speech, printed text or handwriting are passed to the system as parameters. With this system, we can direct the robot that talks to the computer and nobody need to work as a translator [5].

The artificial intelligence scope and challenges in India and the artificial intelligence revolution. As an artificial intelligence, the computer machine that makes it so intelligent to solve the computer problem that can only be solved by people. Artificial intelligence is generally classified as a large AI and a narrow AI. AI-based games are popular in recent days. The use of artificial intelligence helped to make better use of time and resources. But India lags behind in the area of AI development compared to other countries such as China and the USA. In order to benefit from AI, the government must take the current advances in AI [6].

A face recognition approach using the main component analysis in MATLAB follows the main component analysis methodology. Parameters are the removal of some basic parts of the face, such as eyes, nose, mouth, and chin, with the database. Increasing the number of face images in the database increases the system recognition rate. The recognition rate, however, begins to saturate following a definite increase in own value [7].

An effective face recognition approach using a modified center-symmetric local binary pattern (MCS-LBP). This approach follows the methodology of the Local Binary Modified Center-Symmetric Pattern (MCS-LBP). The face representation, extraction of features, and classification are the three main parts of the process. They have results with an accuracy of 88.7% for LBP and 92.8% for CS-LBP and 96.3% for MCS-LBP [8].

The hierarchical-PEP model for real-world face recognition takes the structure of the face parts as a parameter and the hierarchical PEP model method is adapted and 91.10% accuracy with SIFT [9] is achieved.

Face recognition based on a deep neural network is an approach that uses traditional neural network methodology. It takes face images to extract the feature vector as a parameter. The resulting system will have a mean recognition accuracy of more than 97.5% in LFW marches steadily towards human performance [10].

A classification approach using the radial base function uses the Fusion, LDA, neural networks, and PCA method. The system sets video frames or photo frames as parameters. The system accounts for 98.5% of the recognition rate [11].

3 Proposed Methodology

Artificial neural networks, also known as connection systems, are computer systems that are similar to the animals' biological neural network. The idea of AI neural networks is inspired by the neural biological network. The neural network is a framework for other algorithms such as the algorithm for machine learning. It helps algorithms cooperate and process complex data entries. These systems "learn" to perform tasks by looking at examples, generally without any task-specific rules being programmed.

The methodology of the Principal component analysis also referred to as PCA. It is a statistical approach that uses an orthogonal transformation to change a set of possible related variables (different numerical values are taken by each entity) into a set of values of linearly unrelated parameters known as the principal components as shown in Figs. 1 and 2.

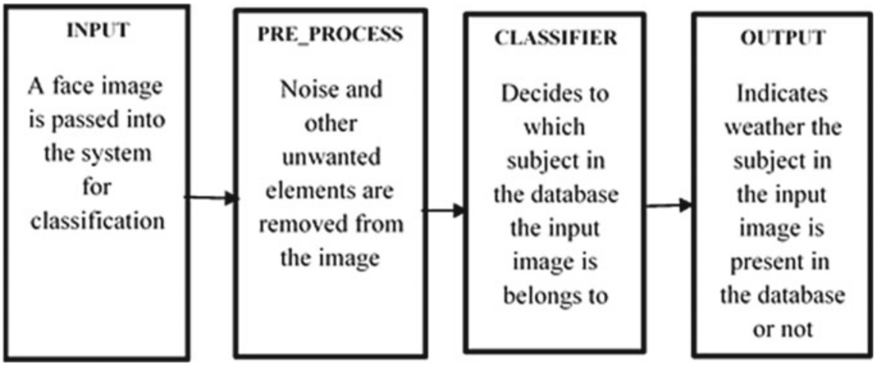

INPUT
A face image is passed into the system for classification
PRE_PROCESS
Noise and other unwanted elements are removed from the image
CLASSIFIER
Decides to which subject in the database the input image is belongs to
OUTPUT
Indicates weather the subject in the input image is present in the database or not

Fig. 1 Generic representation of a face recognition system

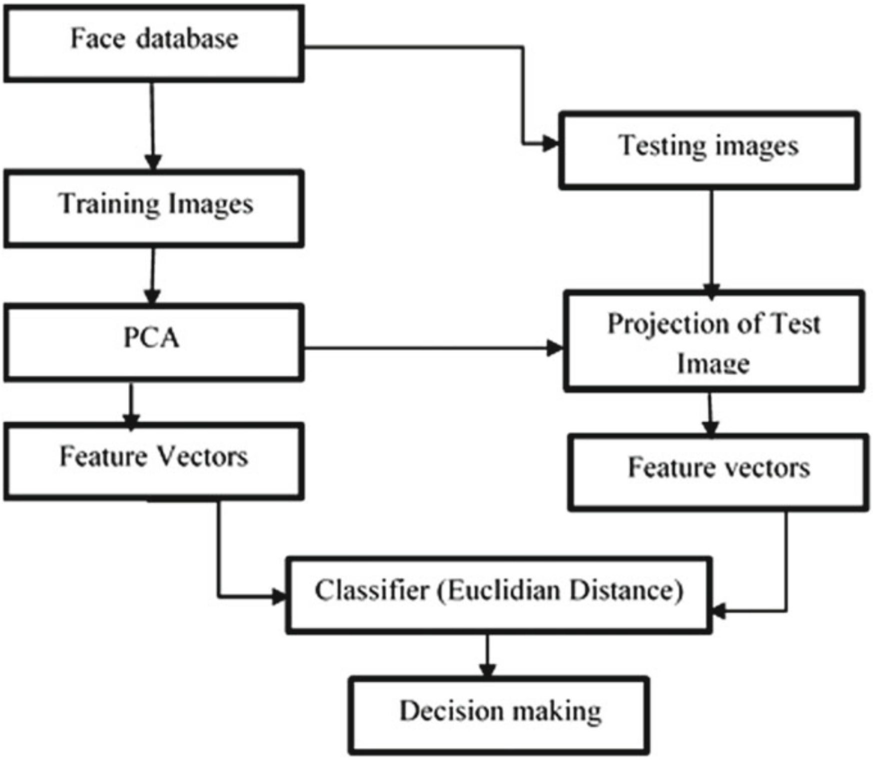


Fig. 2 Overview of proposed system

4 Result Analysis

Ref No.	Approach	Methods	Parameters	Result
1	Face detection and expression recognition using neural network approaches	Artificial neural network, basic propagation algorithm, multiplier reception (MLP), principle component analysis, RBF, graphics processing unit, etc.	The basic unit of communication (Body movement, facial expression, physiological reactions)	Take a decision like the human brain to detect facial expression
2	Face recognition system using backpropagation artificial neural networks	Face localization or localized face, they used image processing, biometric, pixel, segmentation, neuron	Matching of iso-density lines of subject faces which means comparisons of sizes or relative distance of facial features like the position of eyes, nose, and mouth	Performs human face recognition at a very high density of accuracy
3	A MATLAB based face recognition system using image processing and neural networks	Discrete cosine transform, self-recognizing map, neural network	Face image	Recognition rate 81.36% for 10 trials
4	Human emotional state recognition using facial expression detection	The principle of image pre-processing is used [Pre-processing component analysis (PCA)]	Different types of images	The system is tested on a database which consists of 30 different persons with different expressions, the proposed system PCM method have greater accuracy and consistency

(continued)

(continued)

Ref No.	Approach	Methods	Parameters	Result
5	Natural language processing using artificial intelligence	Natural Language Processing (NLP)	Speech, printed text or handwriting	Robot get a direction which helps to do conversation with a computer without the interference of a person who works as a translator
6	Artificial Intelligence revolution and India's artificial intelligence development challenges and scope	Null	Null	The government must adopt the current advancements of artificial intelligence to make use of its benefits
7	Face recognition using principal component analysis in MATLAB	Principal component analysis	Extraction of some basic parts of a face such as eyes, nose, mouth, and chin, with the one stored in the database	We can increase the recognition rate of our system by increasing the number of images of faces in the given database. But the recognition rate will start saturating when a definite sum of the increase in eigenvalue
8	An efficient approach to face recognition using a Modified Centre-Symmetric Local Binary Pattern (MCS-LBP)	Modified Centre-Symmetric Local Binary Pattern (MCS-LBP)	Face representation, feature extraction, and classification	With method LBP we get 88.7% With method CS-LBP we get 92.8% With method MCS-LBP we get 96.3%
9	Hierarchical-PEP model for real-world face recognition	Hierarchical-PEP model	Face part as structures	System achieved 91.10% accuracy with a feature of SIFT

(continued)

(continued)

Ref No.	Approach	Methods	Parameters	Result
10	Face recognition based on deep neural network	Conventional neural network	Feature extraction from face images to get the feature vector	Mean recognition accuracy on LFW marches steadily towards the human performance of over 97.5%
11	Face recognition by classification using radial basis function	Fusion, LDA, neural networks, and PCA	Video frames or photo frames	Gives 98.5% of the recognition rate

5 Conclusion

When looking at previous research papers, artificial neural networks, and pre-processing component analysis (PCA) are the most commonly used methodology. The maximum accuracy for the combination of Fusion, LDA, Neural Networks, and PCA methodologies is 98.5%. And we also observed that the methodology of the neural network always works well. In the future, we will build a face recognition and NLP system that detects or does not lie to a person.

Acknowledgements The authors express gratitude towards the assistance provided by Accendere Knowledge Management Services Pvt. Ltd. In preparing the manuscripts. We also thank our mentors and faculty members who guided us throughout the research and helped us in achieving desired results.

References

1. Nisha SD (2015) Face detection and expression recognition using neural network approaches. Glob J Comput Sci Technol F Graph Vis 15(3)
2. Revathy N, Guhan T (2012) Face recognition system using back propagation artificial neural networks. Int J Adv Eng Technol 3:321–324
3. Nagi J, Ahmed SK, Nagi F (2008) A MATLAB based face recognition system using image processing and neural networks. In: 4th international colloquium on signal process and its applications, pp 83–88
4. Vasani GB, Senjaliya RS, Kathiriya PV, Thesiya AJ, Joshi HH (2013) Human emotional state recognition using facial expression detection. Int J Eng Sci 2:42–44
5. Dhavare U, Kulkarni U (2015) Natural language processing using artificial intelligence. Int J Emerg Trends Technol Comput Sci 4:203–205
6. Singh H (2017) Artificial intelligence revolution and India's AI development: challenges and scope. Int J Sci Res Sci Eng Tech 3(3):417–421

7. Singh P, Sharma A (2015) Face recognition using principal component analysis in MATLAB. Int J Sci Res Comput Sci Eng 3:1–5
8. Alapati A, Kang D (2015) An efficient approach to face recognition using a Modified Center-Symmetric Local Binary Pattern (MCS-LBP). Int J Multimed Ubiquit Eng 10:13–22
9. Haoxiang L, Gang H (2015) Hierarchical-PEP model for real-world face recognition. In: Proceedings of the IEEE conference on computer vision and pattern recognition, 07–12 June, pp 4055–4064
10. Xinhua L, Qian Y (2015) Face recognition based on deep neural network. Int J Signal Process Image Process Pattern Recogn 8:594–598
11. Mandhala VN, Bhattacharyya D, Kim TH (2015) Face recognition by classification using radial basis function. Int J Multimed Ubiquit Eng 10:33–40

A Review on Detection of Online Abusive Text

Bhumika Jain, Chaithra Bekal and S. P. PavanKumar

Abstract Presently, online networking have become a part and parcel of almost everybody's life. Also, it has become major medium of personal and commercial communication. The current popularity of web technologies and social networking has made mandatory for a person to be active on these sites. Therefore, people became closely attached and find a medium to express their feeling, opinions, and emotions through these sites and often share information without bothering what they are sharing and with whom. Such context has become an avenue for cyberbullying. Thus, Internet is a platform for using abusive text or image, which may lead to many problems. Hence, it is important to place an effective system in order to put an end to such activities, through text mining techniques, machine learning, and natural language processing. In this paper, we compare different method of prototype implemented in the detection of abusive content.

Keywords Abusive · Detection · Social networking · Text

1 Introduction

There are a lot of areas to express one's opinion about any social aspects. One can put out their opinion about something through social media. Social media like Facebook, Twitter, etc. provide us the platform to put in our views about an issue through comment boxes, through posting things to reach out people. Some posts or comments might lead to bullying, harassment or even assassinating somebody's personality or character. This can be called as cyberbullying and is done to annoy or hurt somebody intentionally. The comments or messages which are rude and said to irritate somebody also come under this and are of major concern. And, it is a prime important aspect these days that these kinds of abusive texts have to be detected

B. Jain (✉) · C. Bekal · S. P. PavanKumar
Department of Computer Science and Engineering, Vidyavardhaka College of Engineering,
Mysuru, Karnataka, India
e-mail: bhumikajain94@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_74

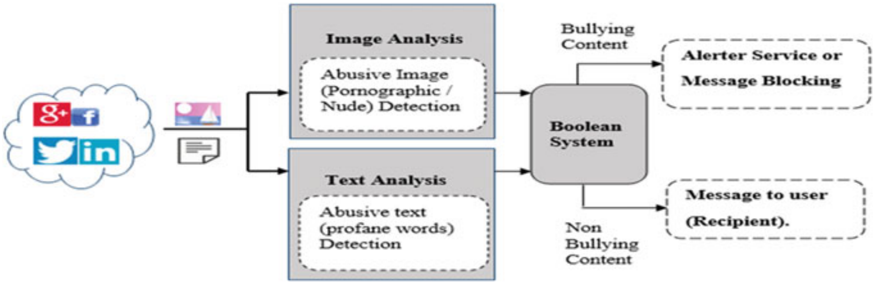


Image Analysis
Abusive Image (Pornographic / Nude) Detection
Text Analysis
Abusive text (profane words) Detection
Boolean System
Bullying Content
Alerter Service or Message Blocking
Non Bullying Content
Message to user (Recipient).

Fig. 1 Framework for the detection of abusive text [2]

automatically and reported. There can be hateful comments on women or religions which are violating their constitutional rights.

A 2007 Pew Research study found 32% of teens have been victims of some type of cyberbullying. And, it is still the same as per 2016 research study. Many children were said to be attempting suicide due to this problem between 2008 and 2016 [1]. In abusive text detection, the framework processes as shown in Fig. 1 [2]. Like these, many research studies have revealed that cyberbullying has been of major concern these days and this problem has to be solved. There are many research studies on this problem. There are many artificial intelligence techniques like text mining, natural language processing, etc. used to solve the problems which have been discussed below.

2 Literature Review

Many researchers have come up with different prototype and systems for detecting offensive material. A lot of people including A. Mahmud, K. Z. Ahmed, and M. Khan [3], Vandersmissen, F.D.T, Baptist., Wauters, T [4] and many more have come up with their methods to detect abusive text, images, etc. In Kansara and Shekokar [2] proposed a framework for detecting negative online interactions in terms of abusive content carried out through text messages as well as images. In abusive image detection, Local Binary Point (LBP) is used to identify interest points and these points or features are then mapped to the existing visual word in vocabulary. Further, support vector machine (SVM) helps in classifying whether image is abusive or not, based on decision planes that define decision boundaries.

Chen et al. [5] have used the concepts of text mining and classifier techniques to detect the abusive texts in any social media. They have taken 8 data sets from social media sources that have already been reported as cyberbullying. Bag of words and N-grams are used for text representation in text mining, whereas in the case of classifiers, they have used two types namely Naïve Bayes (NB) classifier and support vector machines (SVMs). The graphs being plotted according to performance obtained from the above-stated classifiers and text mining algorithms the results were obtained. The results show the comparisons in different data sets by observing chi-square values.

In Nobata et al. [6] from Yahoo labs, NLP can be used as a method to analyze the abusive texts in user comments. They have the Vowpal Wabbit's regression model. They have basically decided to divide into four classes, namely N-grams, Linguistic, Syntactic, and Distributional Semantics. In the first-three processes, they have done few mild preprocessing to remove disturbances and in the fourth process, comments are represented as low-dimensional vectors and are jointly learned with distributed vector representations of tokens using a distributed memory model. The experiments conducted for various data sets using the four processes will produce results.

Yenala et al. [7] have conducted experiments and worked on the same aspect of abusive texts detection but through different methodologies. Deep learning method plays a major role in their work. In this paper, they have taken query completion suggestions in web search and user conversations in messengers. Taking the data sets from these two areas, they have used the method of convolutional neural networks (CNN) and bi-directional LSTMs (BLSTM) to get results for various models and derive conclusions on how it works for solving the problem, i.e., detection of abusive texts.

Spertus [8] put forward a prototype system to automatically recognize flames, called Smokey. It combines natural language processing and sociolinguistic observation to identify messages that not only contain insulting words but use them in an insulting manner [5]. In this prototype, the text is passed through a parser in some common format and then the output is converted to Lisp s-expression by sed and awk scripts. A feature vector is produced for each message as these s-expressions are processed through rules. Further, a decision tree generator C4.5 is used to generator simple rules to evaluate the feature vector [8].

Another automatic flame detection method was given by Razavi et al. [9]. This method extracts features at different conceptual levels and applies multilevel classification for flame detection. They have used machine learning algorithm, i.e., they ran a three-level classification, using the Insulting and Abusing Language Dictionary (IALD). The Complement Naïve Bayes classifier, the Multinomial Updatable Naïve Bayes classifier, and Decision Table/Naïve Bayes hybrid classifier (DTNB) are used, respectively, in the first, second, and third levels. Finally, the decision of whether the text is okay or flame is based on the current instance.

3 Comparison of Different Detection Method for Abusive Text

Table 1 gives us the picturesque idea of the detection techniques used by various authors in the field of anomaly detection techniques using data warehouse. It also gives the list of recommendations which we thought could have been implemented in the system in future.

Table 1 Comparison of different detection methods for abusive text

Reference No.	Approach	Method	Parameter	Advantage	Disadvantage	Result
[2]	A frame for cyberbullying detection in social network	Bag of visual words (BoVW) concept with SVM classifier k-means algorithm	Abusive image or Abusive text	Both image and text are considered; it blocks the abusive contents before broadcasting	Concentrates on only image and text and not on videos and audios	Detects bullying content and either alerts or message blocking
[5]	Deep learning for detecting inappropriate content in text	Convolutional bi-directional LSTM (C-BiLSTM) technique which combines the strengths of convolution neural networks (CNN) and bi-directional LSTMs (BLSTM)	8 data sets from various social medias	Most of the conversations from the datasets give correct output	Errors are encountered such as misspellings, lack of semantic understanding, inadequate training data, borderline cases, and noise	BLSTM significantly outperforms both pattern-based and other hand-crafted feature-based baselines. C-BiLSTM also proved to be better than other individual deep learning-based architectures CNN, LSTM, and BLSTM
[6]	Abusive language detection in online user content	NLP features are used which measure different aspects of the user comment, Vowpal Wabbit’s regression model 5 in its standard setting with a bit rate of 28	Primary data sets and temporal data sets	This model outperforms deep learning- based model	Only character N-grams fare well in noisy data sets	Character N-grams alone fare very well in these noisy data sets
[7]	Harnessing the power of text mining for the detection of abusive content in social media	In supervised machine learning, they have compared alternative text representations and dimension reduction approaches, including features election and feature enhancement	Input text data sets from social media message boards	Large variety of datasets are considered	Concentrates more abusive text only but cyberbullying can be through audio or videos as well	Studied impacts on content detection accuracy

(continued)

Table 1 (continued)

Reference No.	Approach	Method	Parameter	Advantage	Disadvantage	Result
[8]	Smokey: automatic recognition of hostile messages	Smokey: a prototype system message classification	Abusive texts, flames	Checks for syntactic constructs, avoid misclassifying	Fails to detect sarcasm, grammar, mistakes, innuendo, etc.,	Automatic flame detection
[9]	Offensive language detection using multilevel classification	Three-level classification with machine learning algorithm as a software	Flames	16% better accuracy than baseline, uses IALD, software is not very sensitive to punctuation and grammatical mistakes	Focus mainly on abusive text	Efficient flame detection software

4 Fututre Work

In the future work, we could develop a tool that checks for abusive content on social media. This tool should be able to check the text semantically as well for any obnoxious content. We can implement this tool using deep learning, language processing techniques.

5 Conclusion

Social networking is an integral part of most people. And, cyberbullying is a major concern, as the number of online users is increasing. Many techniques and frameworks have been proposed in order to detect offensive content. All these proposed systems consider different variety of data sets and a very few have attempted to compare these; in this paper, we have done it through a review table. Few methodologies use NLP, classifier, bag of words while some use machine learning techniques. All the different methodologies have their own advantages and disadvantages.

Acknowledgements The authors express gratitude toward the assistance provided by Accendere Knowledge Management Services Pvt. Ltd. in preparing the manuscripts. We also thank our mentors and faculty members who guided us throughout the research and helped us in achieving the desired results.

References

1. Cook S. Cyberbullying facts and statistics for 2016–2018. https://www.comparitech.com/internet-providers/cyberbullying-statistics/
2. Kansara KB, Shekokar NM (2015) A framework for cyberbullying detection in social network, vol 5, pp 494–498
3. Mahmud A, Ahmed KZ, Khan M (2008) Detecting flames and insults in text. In: Proceedings of the Sixth International Conference on Natural Language Processing
4. Vandersmissen B, Baptist FDT, Wauters T (2012) Automated detection of offensive language behavior on social networking sites, pp. xiv, 81 p.: ill
5. Chen H, Mckeever S, Delany SJ, Chen H, Mckeever S, Delany SJ (2016) Harnessing the power of text mining for the detection of abusive content in social media. In: 16th UKCI, pp 1–19
6. Nobata C, Tetreault J, Thomas A, Mehdad Y, Chang Y (2016) Abusive language detection in online user content. In: Proceeding of 25th international conference World Wide Web—WWW '16, pp 145–153
7. Yenala H, Jhanwar A, Chinnakotla MK, Goyal J (2017) Deep learning for detecting inappropriate content in text. Int J Data Sci Anal
8. Spertus E (1997) Smokey: automatic recognition of hostile messages. In: AAAI'97/IAAI'97 proceedings of the fourteenth national conference on artificial intelligence and ninth conference on innovative applications of artificial intelligence, pp 1058–1065

9. Razavi AH, Inkpen D, Uritsky S, Matwin S (2010) Offensive language detection using Multilevel classification. In: Farzindar A, Kešelj V (eds) Advances in artificial intelligence. AI 2010. Lecture notes in computer science, vol 6085. Springer, Berlin, Heidelberg
10. Xiang G, Fan B, Wang L, Hong J, Rose C (2012) Detecting offensive tweets via topical feature discovery over a large scale twitter corpus, pp 1980–1984. https://doi.org/10.1145/2396761.2398556

Security of an IoT Network: A VLSI Point of View

Sreeja Rajendran, Azhar Syed and R. Mary Lourde

Abstract Third-party IP cores, outsourcing of IC fabrication to untrusted foundries, have increased the vulnerabilities in IC's and reduced the trust factor of a designer on the manufactured chips. These vulnerabilities are a consequence of malicious modifications of the original design, which have the potential to cause catastrophic damage to the system which uses these IC's. IoT networks require the least vulnerable and highly trustworthy IC's. We present a detailed study of such malicious insertions. Next, we discuss the methods for their identification and we also propose some countermeasures from a VLSI aspect.

Keywords IoT · Hardware Trojans · Security · Processor

1 Introduction

Internet of Things (IoT) is a paradigm which links various realms of technology for applications ranging from smart homes to smart healthcare and even smart agriculture. The Internet of Things (IoT) has a lot to offer and presents us with countless opportunities. Imagine systems that can be controlled and monitored over the Internet, self-driven cars, factories that communicate with warehouses, smart homes with digitized infrastructure. With the impact of Internet in our lives, the applications of IoT are countless. However, with the advancement of such an impactful technology, there is a downside to it. The widespread success of IoT depends on the data and information it collects. The more information shared and stored, greater will be the chances of security breaches, which will increase the risk of theft and manipulation.

S. Rajendran · A. Syed · R. M. Lourde (✉)
Department of EEE, BITS Pilani Dubai Campus, Dubai, UAE
e-mail: marylr@dubai.bits-pilani.ac.in

S. Rajendran
e-mail: sreejamanojnair@gmail.com

A. Syed
e-mail: azharsyed18@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_75

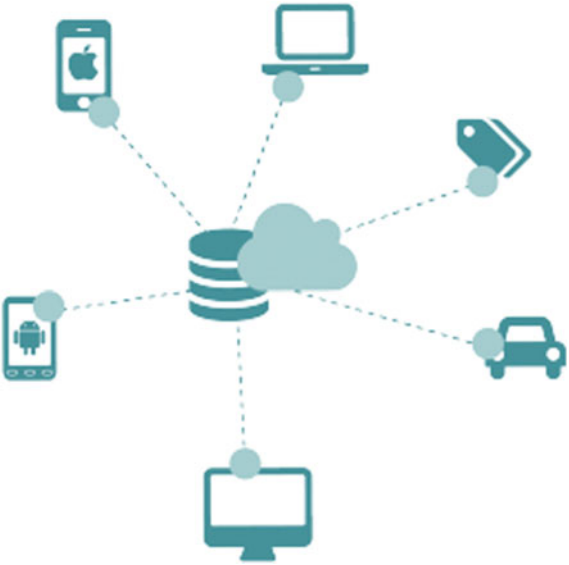


Fig. 1 Diagrammatic representation of a centralized IoT network

The more we increase the applications of the Internet of Things, more will be the requirement for stringent security measures.

The traditional network layout for an application of the IoT is as shown in Fig. 1. It represents a simple centralized structure. However, in recent times, the IoT has moved from a simple structure to a complex network of decentralized devices. The IoT network is highly dependent on different semiconductor technologies which include microprocessors, sensors, and low power devices. IoT helps to provide network connectivity to embedded systems, sensors, and actuators.

2 Security Threats

It is extremely important that security is taken into consideration from the very beginning of the design process. There is a need to focus on security aspects of all devices connected on the network. The security threat classification in the Internet of Things network is shown in Fig. 2.

Physical attacks include reverse engineering and microprobing. Due to the expense involved, it is believed that these attacks are seldom resorted to by adversaries. Timing analysis, power analysis, electromagnetic radiation analysis, etc. fall under the category of side-channel attacks. Cryptanalysis threats include ciphertext attack, plaintext attacks, etc. which attempt to break the encryption in order to obtain the encryption key. Virus attacks, logic bombs, and denial of service fall under the category of software attacks. Due to the broadcast nature of the transmission medium,

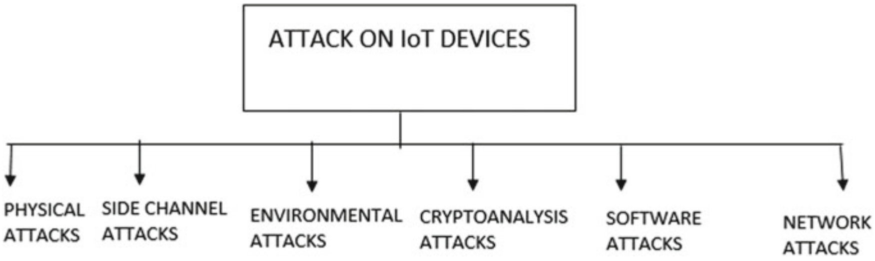


Fig. 2 Attack on IoT systems

wireless systems become vulnerable to network attacks. Denial of service, node capture, routing attacks, monitoring, and eavesdropping can be grouped under network attacks category [1, 2].

3 Hardware Security Threats

Hardware security attacks are extremely difficult to identify but possess the capability to impair a system resulting in devastating effects [1, 3–5]. Attacks carried out on the hardware are generally in the form of Trojans which are specifically called Hardware Trojans. It is defined as an unwanted but intentional alteration of a logic circuit or design resulting in undesired circuit behavior. A clear understanding of Hardware Trojans is quintessential for developing ICs used in highly secure applications.

3.1 Hardware Trojan Taxonomy

The Hardware Trojans (HT) can be inserted either in the design phase or during fabrication. These inserted HT remain dormant during the normal course operation of the IC for a long time, until they are triggered. Once HT is triggered, it will perform the malicious action they are designed for. The classification of Trojans based on their trigger mechanisms and their payloads is shown in Fig. 3 [3, 4, 6].

The Hardware Trojans as classified by Rajendran et al. in Fig. 4 provide us with a good understanding of the effects of Trojans, the different stages of IC manufacturing process, and the different locations of the IC which can be infected by Trojans [6]. The HT can be activated through internal or external mechanisms. Combinational and sequential triggers belong to the class of internal triggers. The occurrence of a certain set of values at internal nodes in the circuit simultaneously activates a combinational trigger. A particular state of a set of internal registers or a specific word on the address bus can be also used as a trigger. Sequential triggers are activated by a series of events. The simplest trigger for sequential circuits is a counter. The HT is triggered when the

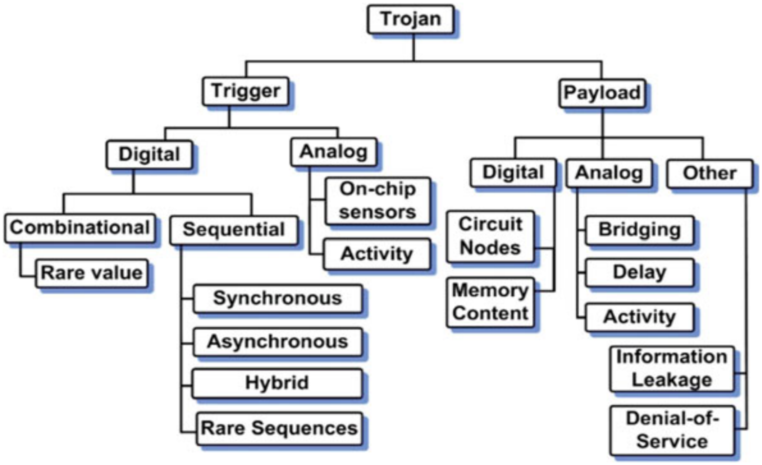


Fig. 3 Trojan taxonomy based on trigger and payload mechanisms

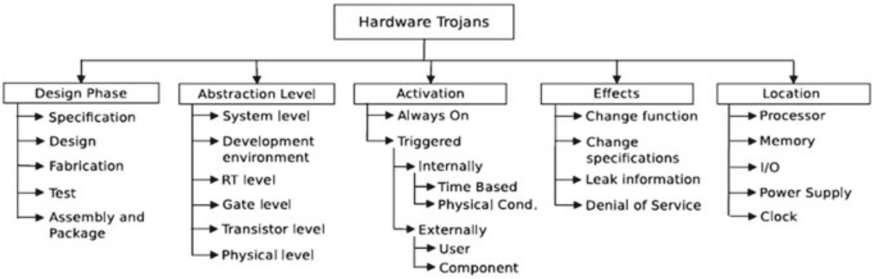


Fig. 4 Hardware Trojan taxonomy

counter reaches its highest count. The external trigger mechanisms are applied from outside the system. Activation of external triggers depends on user inputs like a reset button or a power switch. An externally connected memory device can also act as an external trigger. There is yet another set of Trojans which do not require any trigger mechanism for activation. They are also known as ‘always on’ Trojans. Always on Trojans function by making elusive changes to system specification, timing, etc.

4 Identification of Trojans

The insertion of a Trojan cannot be completely prevented. However, it can be limited to a certain extent. The Hardware Trojan Detection techniques are classified as shown in Fig. 5 [3]. It is very difficult to achieve a high degree of assurance that the probability of a Hardware Trojan being present is zero. Generally, reverse engineering is the

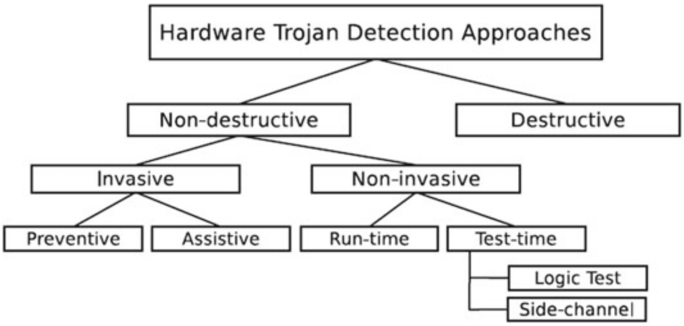


Fig. 5 Trojan detection techniques

most preferred method to identify the Trojan; however, reverse engineering becomes extremely difficult and time-consuming when we use it on complex modern IC. The most common method used for identification of the Hardware Trojan is to compare it with a golden reference. Though this method will not be of any significant help if the Trojan is added prior to IC fabrication, in certain scenarios when the Hardware Trojan is inserted in just a few IC's, reverse engineering can be used. As a part of the fingerprinting method, the reverse engineering process is used to identify a good IC and using the details such as power consumption, temperature and electromagnetic profiles, a reference is generated which is called a fingerprint. This fingerprint is then used against all the IC of the batch as a comparison parameter to find Trojan. This method sounds a feasible option to an extent to identify Trojans in some instances [3, 5].

In order to avoid damaging the IC, techniques which leave the design unaltered are preferred. These methods have better accuracy in Trojan detection. One of these methods involves the insertion of dummy flip flops into the design to increase the Hardware Trojan activity and therefore making it easier to detect the activity of the Hardware Trojan. Adding extra gatekeeper logic along with some modified software, which can monitor all writes to memory will help to identify the illegal writes on which some action can be taken.

There are some suggested and used techniques which do not change the design of the IC while detecting the Hardware Trojan. Adding reconfigurable logic (DEFENSE) to the functional design is a real-time security monitor [7]. Once the IC's are fabricated, this logic is programmed with details regarding how the device should behave. Any deviations can then be easily detected. Side-channel analysis is another method which is used for Trojan detection. In this method, it is assumed that the Trojan triggers itself and alter some important features of the IC like the power consumed, the heat produced in different parts of the IC, the delay time (path delay). Side-channel analysis is said to have the best rate of Hardware Trojan Detection as it does not require the Trojan to be activated [3].

Another modification of the side-channel analysis is the current integration method to identify the Trojans. This technique depends on the amount of current drawn in by the different part of the circuits. Some currents drawn can be so small that they are assumed as an envelope of noise and therefore not detected during measurement. However, this can be avoided by measuring the current locally and at multiple ports in the IC design. These measurements are then compared to a golden chip which is used as a reference and any deviations are used in the detection of Hardware Trojans [5].

5 Basic Architecture of a Secure Processor

The traditional method used to improve security was accomplished with the help of two processors. An embedded security processor is used in conjunction with main processor to provide security as shown in Fig. 6. The embedded security processor is controlled by the main processor. The work of the embedded security processor is to evaluate the data it receives from the network interface before allowing external network to access main processor [8].

The Internet of Things (IoT) network requires processors of small dimension with low power consumption. In order to achieve this requirement, only one processor is preferred instead of the traditional method of using two processors. The most commonly used processors are ARM processors. The major reason for selecting ARM processors is its performance and low power consumption [9].

These processors also face the risk of been affected by Hardware Trojans. The ARM Cortex M4 processor architecture is shown in Fig. 7. The researches show

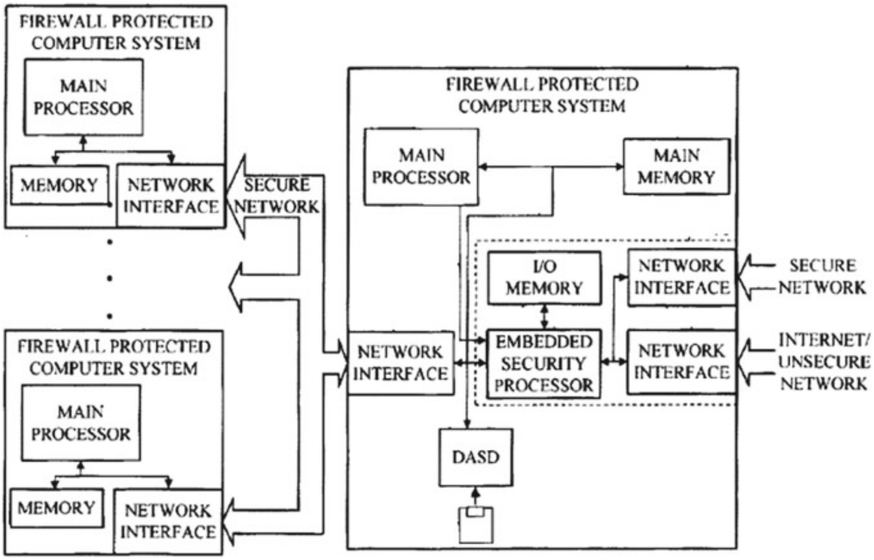


Fig. 6 Basic architecture of a secure processor

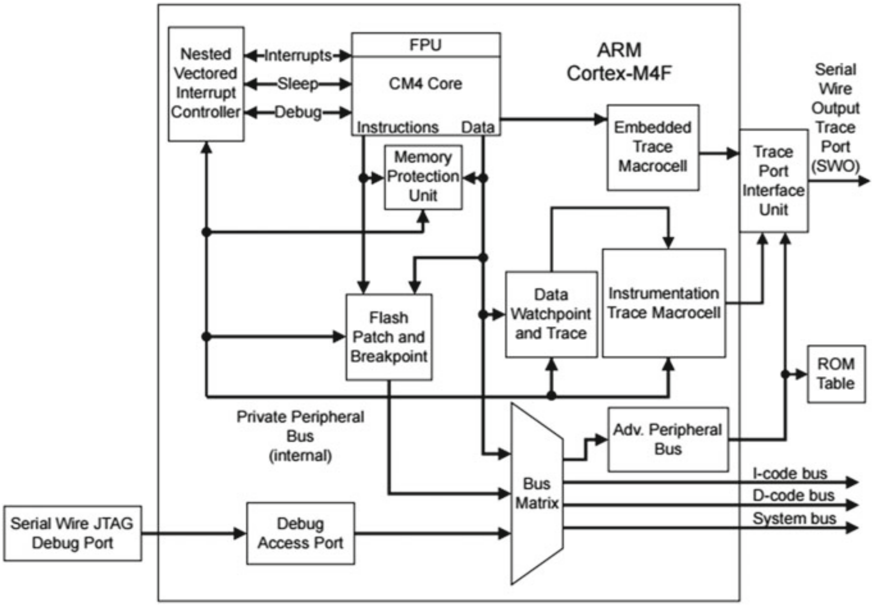


Fig. 7 ARM M4 cortex architecture [10]

that information in such processors can be leaked through radio frequency, optical, power, and timing side channels and by interfaces such as JTAG and RS232. The most prominent locations for detecting Hardware Trojans are memory units and clocking units. As illustrated in Fig. 4, the processor is vulnerable to Hardware Trojans which can be inserted at the design phase and abstraction level. Attack resistant features like advanced memory management unit (MMU), redundant circuitry to thwart power attack analysis and circuitry for fault detection need to be incorporated into the design.

6 Implementation Issues

Basic implementation of hardware security is achieved through cryptographic algorithms. Since key generation involves a great deal of computation, use of a low power embedded device could be challenging. Battery capacity and storage limitations are also issues that need to be tackled in order to develop a complete security solution. Resource sharing which greatly helps to cut the hardware cost is yet another reason which prevents physical separation between modules or partitions. Most of the existing solutions are application-specific, and hence, there is no one golden solution applicable to all systems.

7 Counter Measures

Security solutions are always a trade-off between security, cost, performance, flexibility, and power consumption. Solutions generally look into the optimization of basic security functions like confidentiality, integrity, authentication, etc. and also countermeasures against the security attacks [2]. The semiconductor manufacturing requires a large investment; the importance of foundries has grown drastically, thus increasing the exposure to thefts of masks, insertion of Hardware Trojans, and unauthorized excess fabrication. In order to avoid Trojan insertion at the fabrication level, the authors in [11] propose a system in which the IP consumer needs to provide both hardware specifications and a list of security-related properties. This has to be agreed upon by the IP Consumer and the IP Producer. This idea is similar to the software process proof-carrying code [12].

The designer also plays a vital role in avoiding insertion of Hardware Trojans by making necessary architectural changes. A method developed by Hicks et al [13] uses a Trojan countermeasure called BlueChip. It is a hybrid combination of hardware and software. It includes an Untrusted Circuit Identification Algorithm along with a tool set which identifies Trojan circuits during the verification or testing of the design. Using a hybrid approach helps maximize processing efficiency while meeting the design constraints. Deng et al. [14] proposed a method of using a hardware checksum that is based on checking the authenticity of trusted hardware. As per the concept, the hardware needs to send back a checksum within a stipulated time frame. If it does not receive the expected checksum, it assumes the presence of a Hardware Trojan. This method ensures the absence of Trojan post-fabrication process. However, this process does not guarantee that no Trojans have been inserted during the specification, design, verification, or manufacturing stages. Reconfigurable Architectures are of great help in countering the Hardware Trojans. The best example of reconfigurable architectures is FPGA. Implementation of secure processor is a novel method of reduction of Hardware Trojans. As seen, the Trojans are inserted at various stages such as design and fabrication of the IC. In FPGA, the hardware implementation and design implementation are completely different. In FPGA systems, the design is implemented at a later stage using a configuration bitstream. This process assures us that the design can be implemented independently and it provides a high degree of security from Hardware Trojans.

With the existing methods of Hardware Trojan identification, we still do not get a completely secure IC. Another method which can be implemented to increase the identification efficiency is by using combinations of identification techniques. The basic concept of combinational identification technique is to use two or more identification techniques together [15].

8 Conclusion

Internet of Things (IoT) with a strong network of hardware devices can be of utmost importance for new economic business models. A perfectly secure solution is an ideal requirement. However, such security systems are not easy to develop. Each and every aspect of the network should be totally secure in order to achieve total security. The algorithms available are very much secure from the cryptography point of view. More emphasis is required on other elements of the network. In the IC level, more attention needs to be given to the design, fabrication, and verification stages of the IC. If these things are well addressed, then an ideally secure Internet of Things (IoT) network can be achieved.

References

1. Syed A, Mary Lourde R (2016) Hardware security threats to DSP applications in an IoT network. In: 2016 IEEE international symposium on nanoelectronic and information systems (iNIS). IEEE, pp 62–66
2. Babar S, Stango A, Prasad N, Sen J, Prasad R (2011) Proposed embedded security framework for internet of things (IoT). In: IEEE international conference on wireless communication, vehicular technology, information theory and aerospace & electronic systems technology (Wireless VITAE), pp 1–5
3. Chakraborty RS, Narasimhan S, Bhunia S (2010) Hardware Trojan: threats and emerging solutions. http://www.trust-hub.org/resources/113
4. Chakraborty RS, Bhunia S (2009) Security against hardware Trojan through a novel application of design obfuscation. In: Proceedings of the 2009 international conference on computer-aided design, pp 113–116
5. Wang X, Salmani H, Tehranipoor M, Plusquellic J (2008) Hardware Trojan detection and isolation using current integration and localized current analysis
6. Rajendran J, Gavas E, Jimenez J, Padman V, Karri R (2010) Towards a comprehensive and systematic classification of hardware Trojans. In: Proceedings of 2010 IEEE international symposium on circuits and systems (ISCAS), pp 1871–1874
7. Abramovici M, Bradley P (2009) Integrated circuit security: new threats and solutions. In: Proceedings of the 5th annual workshop on cyber security and information intelligence research: cyber security and information intelligence challenges and strategies, CSIIRW '09, ACM, New York, NY, USA, pp 55:1–55:3
8. McKelvey MA (1999) Embedded security processor. International Business Machines Corporation. Patent Number: 5,896,499 20, Apr 1999
9. Suh G, O'Donnell CW, Devadas S (2005) AEGIS: a single-chip secure processor. Inf Secur Tech Rep 10(2):63–73
10. ARM Processors. www.ti.com/lit/er/spmz637/spmz637.pdf
11. Love E, Jin Y, Makris Y (2011) Enhancing security via provably trustworthy hardware intellectual property. In: IEEE international symposium on hardware-oriented security and trust
12. Necula GC (1997) Proof-carrying code. In: Proceedings of the 24th ACM SIGPLAN-SIGACT symposium on principles of programming languages, pp 106–119
13. Hicks M, Finnicum M, King ST, Martin MMK, Smith JM (2010) Overcoming an untrusted computing base: detecting and removing malicious hardware automatically. In: IEEE symposium on security and privacy, pp 159–172

14. Deng DY, Chan AH, Suh GE (2009) Hardware authentication leveraging performance limits in detailed simulations and emulations. In: Proceedings of the 46th annual design automation conference, DAC '09, ACM, New York, NY, USA, pp 682–687
15. Beaumont M, Hopkins B, Newby T (2011) Hardware Trojans-prevention, detection, counter measures (a literature review) (No. DSTO-TN-1012). Defence Science and Technology Organisation Edinburgh (Australia) Command Control Communications and Intelligence Div

Sreeja Rajendran is currently doing her Ph.D. at BITS Pilani Dubai Campus (BPDC), UAE. She has a Masters degree in Microelectronics from BPDC (2015) and B.Tech in Electronics and Instrumentation from Cochin University of Science and Technology, India. Her research interests include microelectronic circuits, low power circuit design and FinFET analysis and testing.

Azhar Syed has B.Tech in Electronics and Telecommunications from Mumbai University (2013) and Master of Engineering from BITS Pilani, Dubai Campus in Microelectronics in 2017. His current research interests include VLSI Design, Security of processors and Internet of Things.

Dr. Mary Lourde, R did B.Tech in Electrical Engineering from Kerela University, India in 1983 and M. Tech in Electronics from Cochin University of Science & Technology, India in 1987. She is awarded the Ph.D. Degree in Electrical Engineering from Indian Institute of Science, Bangalore, India for the thesis "Design and Analysis of Digital Controllers for high performance Sensorless PMSM Servo drives" in 1998. She was a faculty at Department of Electronics, CUSAT, India since 1990. Presently with Birla Institute of Technology & Science Dubai Campus (BPDC), working as Associate Professor in EEE. Her current area of research includes VLSI Desgin, Signal Processing and its applications and Power Electronics & Drives. She is an MIEEE, LMIETE, LMISTE.

Anomaly Detection Techniques in Data Mining—A Review

K. N. Lakshmi, N. Neema, N. Mohammed Muddasir and M. V. Prashanth

Abstract Detection is one of the biggest threats to the organization. The detection of abnormal behaviors is one of the most difficult tasks for administrators of information systems (IS). Anomaly behavior is defined as any behavior that deviates from normal within or outside the organization IS, including insider attacks and any behavior that threatens the confidentiality, integrity, and availability of information systems for organizations. The detection of anomalies is extremely important to prevent and reduce illegal activities and to provide an effective emergency response.

Keywords Anomaly · Detection · Data mining · Intrusion detection

1 Introduction

The amount of data being generated and stored in growing exponentially, due in huge part to the continued advances in technology. Data mining is often accustomed to extracting helpful information from the data that surround us. Data mining is the method of analyzing data from totally different views. Data warehouse could be a relative database that is designed for question and analysis instead of dealings process. In further to the current, it additionally includes extraction, transportation, transformation, and loading (ETL) solution. Online analytical processing (OLAP) engines consumer analysis tools and different applications that manage the method of gathering knowledge and delivering it to users. It additionally involves subject orienting, integrated, nonvolatilizable, and time variant characteristics. Forms of data processing techniques or strategies are helpful to search out information that is simply understood in large data sets [1].

K. N. Lakshmi (✉) · N. Neema · N. Mohammed Muddasir · M. V. Prashanth
Department of Information Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India
e-mail: lakshmikn63@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_76

Intrusion detection using data mining (IDDM) techniques aims to see the feasibility and effectiveness of knowledge data mining techniques in real-time intrusion detection and produces solutions for this anomalies behavior, so as to develop defense computing networks. To safeguard networks, intrusion detection systems aim to acknowledge attacks with two primary needs high detection and low warning rate. As attacks manifest themselves in two classes, those who are noted and people that are seen antecedently. Data warehousing is recognized as a great tool for extracting regularities in knowledge and so been the target of some investigations for its use in intrusion detection [2].

The IDDM focuses on the utilization of data mining within the context, by manufacturing descriptions of network data using this information for derivation analysis. Variety of existing technologies is offered for this purpose a number of that are evaluated as a part of the project. This method is performed by meta-mining techniques that characterize amendment between network data descriptions; the system will manufacture applicable notices. The end result of the IDDM project is the talents to characterize network knowledge and to sight variations in these characteristics over time. Combining this capability with tools that either acknowledge existing attack patterns or operate equally to IDDM, it strengthens the power to intrusion detection professionals to acknowledge and probably react to unwanted violations to network operations [2]. Developing the anomaly detection system needs various knowledge for training and testing functions.

2 Literature Review

In [2], Abraham has proposed intrusion detection using data mining techniques. Combining data mining algorithms with technologies earned close to real-time operation is the basic result. Increase in a number of alarms generated due to changes in rules to set overtime has adversely affected rules set stability is the application.

Dasgupta et al. [3] suggested multidimensional data anomaly detection using a negative selection algorithm. The result is that PCA reduces a set of five-dimensional data to two-dimensional and one-dimensional. The main advantage is the PCA's data reduction. It usually destroys some information within the method, which is why the system has not detected all the anomalous data records.

Catterson et al. [4] proposed anomaly detection for transformer monitoring in multi-variable data. A type of collective anomaly detection has been applied to a single parameter that could improve the data on engineering anomalies. The main advantage is that the CAD technique was used for online transformer monitoring to detect common behaviors.

Patch and Park [5] proposed a summary of the techniques of detection. The result is anomaly detection systems, a set of intrusion detection systems, which model the network behavior which enables them to find both known and unknowns very efficiently. It is often the main advantage that anomaly detection systems and hybrid intrusion detection systems are widely used.

Ye et al. [6] proposed that probabilistic intrusion detection techniques have been proposed and supported by computer audit data. As a result, a series of studies on the probabilistic properties of activity data are presented in an information system to detect intrusions into the information system. It demonstrates the advantage of the frequency properties of multiple events.

Anna and Krzysztof [7] proposed the detection of anomalies in data storage: the petrol station simulator. This paper introduces the simulator's foundations with the result. This discussion presents future work in the field of data collection and materialization in the warehouse data stream.

Radon et al. [8] proposed that alarm reduction has been proposed in maritime detection of anomalies. AIS technology offers an enormous amount of ship movement information center for maritime research and experimentation (CMRE) technology used in close to real time. It also encourages misalarms to be reduced.

Siraj et al. [9] proposed that a smart intrusion detection system architecture has been proposed in the data fusion intrusion sensor. The decision engine effectively fused information in the detection database and the results of the decision-making were also correctly reported in the alert database.

Siaterlis and Maglaris [10] proposed multi-sensor data fusion for detection of DOS. The main advantage is that the data fusion rate increases, and the false alarm rate decreases.

Balakrishna and Rama Ganesh [11] proposed the detection of anomalies, and SQL prepares data sets for analysis of data mining. The data manipulation pivot of the operator is easy to work out for a wide set of values.

Rameshkumar et al. [12] proposed that intrusion detection has been proposed as a text-based approach to mining. This makes the computation even in binary form accurate. The similarity values vary from 0 to 1.

In [13], Bebel et al. have proposed a formal approach to modeling a multi-version data warehouse. Development of prototype MVDW system is the result. The application involves a multi-version data warehouse that is composed of set of its versions.

3 Comparison of Different Anomaly Detection Techniques

Table 1 gives us the picturesque idea of the detection techniques used by various authors in the field of anomaly detection techniques using data warehouse. It also gives the list of recommendations which we thought could have been implemented in the system in the future.

Table 1 Comparison of different anomaly detection techniques

Reference No.	Approach	Method	Parameter	Result	Advantage
[2]	Intrusion detection technique	Data mining technique	Data mining parameters	Usage of data mining algorithms	Increase in no. of alarms generation
[3]	Immunity-based approach	Negative selection algorithm	Multidimensional data	A result set obtained from five-dimensional data reduce by PCA to two dimension	The data reduction by PCA
[4]	CAD approach	Conditional anomaly detection	Partial discharged data	Enhance the information about anomalies.	CAD technique applied to online monitoring
[5]	Survey of the anomaly detection system.	Network-based on anomaly detection	Intrusion detection system	Model the network behavior which enables the effective detection	Hybrid intrusion systems are widely adopted
[6]	Pattern detection approach	Occurrence, frequency	Anomaly detecting parameters	Presents a series of studies on probabilistic properties	It shows the frequency property of multiple events
[7]	Detection approach	Data extraction technique	Data warehousing parameters	Simulator produces data sets with specified anomalies	Sensor miscalibration, detection of anomalies
[8]	Center for maritime research and experimentation approach	Automatic identification system technique	Kinematic data	Verification for false alarm reduction	Reduces the false alarms and motivates in false alarm detection
[9]	Intelligent intrusion detection approach	Computer research security technique	Fuzzy cognitive maps, fuzzy rule base parameters	Intrusion detection	Effective database detection
[10]	DoS approach	Methods of data fusion	Quantitative measurement	To detect flooding attacks and to use data fusion in a detection technique	Increases the DoS detection rate and decreases the false alarm rate
[11]	SQL code generation approach	PCA technique	SQL parameters	Anomaly detection for data mining analysis	To compute wide sets of values for data manipulating operator

(continued)

Table 1 (continued)

Reference No.	Approach	Method	Parameter	Result	Advantage
[12]	Mining-based approach	Intrusion detection technique	IDS parameters	Results in reducing training testes	Makes the computation accurate even in the binary form
[13]	Schema data versioning approach	Online analytical processing methods	Schema evaluation	Developed a prototype MVDW system	Multi-version data warehouse composed of set of its versions

4 Conclusion

Data fusion can improve the performance and reliability of systems in the art and science of data storage. In addition, the fusion process and data mining operations are discussed. To protect the availability, confidentiality, security, and integrity of critical information infrastructures, IDS is designed. The current state of the art of ID systems is relatively primitive in relation to the recent explosion in computer communications, cyberspace, and electronic equipment. Organizations are fully aware that technology detection can be very important information that flows with optional and inhibitory technical factors. The approach to anomaly detection requires the combination of different disciplines, such as artificial intelligence and statistics. It is applied directly to detections of intrusion and attack.

It also discusses the research problems to be addressed in the detection of intrusions in different processing techniques. It also tells us about the sequence of steps to be taken to improve the efficiency and performance of the mechanism for intrusion detection. Anomaly detection systems are now widely used in all fields due to their efficient performance.

Acknowledgements The authors express gratitude toward the assistance provided by Accendere Knowledge Management Services Pvt. Ltd. in preparing the manuscripts. We also thank our mentors and faculty members who guided us throughout the research and helped us in achieving the desired results.

References

1. Mahi S (2017) Introduction to data mining and data warehouse. Int J Adv Res Comput Sci 8(4):398–400
2. Abraham T (2001) IDDM: intrusion detection using data mining techniques 35

3. Dasgupta D, Sumi Majumdar N, Majumdar NS (2002) Anomaly detection in multidimensional data using negative selection algorithm. In: Proceedings of the 2002 congress on evolutionary computation. CEC'02, pp 1039–1044
4. Catterson VM, McArthur SDJ, Moss G (2010) Online conditional anomaly detection in multivariate data for transformer monitoring. IEEE Trans Power Deliv 25(4):2556–2564
5. Patcha A, Park JM (2007) An overview of anomaly detection techniques: existing solutions and latest technological trends. Comput Netw 51(12):3448–3470
6. Ye N, Li X, Chen Q, Emran SM, Xu M (2001) Probabilistic techniques for intrusion detection based on computer audit data. IEEE Trans Syst Man, Cybern Part A Syst Humans. 31(4):266–274
7. Anna G, Krzysztof P (2015) Anomaly detection in data streams: the petrol station simulator. In: International conference: beyond databases, architectures and structures, pp 727–736
8. Radon AN, Wang K, Glasser U, Wehn H, Westwell-Roper A (2015) Contextual verification for false alarm reduction in maritime anomaly detection. In: 2015 IEEE International Conference on big data. IEEE Big Data 2015, pp 1123–1133
9. Siraj A, Vaughn RB, Bridges SM (2004) Intrusion sensor data fusion in an intelligent intrusion detection system architecture. In: Proceedings of the 37th annual Hawaii international conference on system sciences, 2004, pp 1–10
10. Siaterlis C, Maglaris B (2004) Towards multisensor data fusion for DoS detection. In: Proceedings of the 2004 ACM symposium on applied computing—SAC'04, p 439
11. Balakrishna PV, Rame Ganesh B (2014) Anomaly detection and SQL prepare data sets for data mining analysis. Int J Comput Sci Inf Technol 5:6551–6555
12. RajeshKumar G, Mangathayaru N, Narsimha G (2016) Intrusion detection—a text mining based approach. Special issue on Computing Applications and Data Mining. Int J Comput Sci Inf Secur 14:76–88
13. Bębel B, Królikowski Z, Wrembel R (2006) Formal approach to modelling a multiversion data warehouse. Bull Polish Acad Sci Tech Sci 54(1):51–62

MAIC: A Proficient Agricultural Monitoring and Alerting System Using IoT in Cloud Platform

A. Srilakshmi, K. Geetha and D. Harini

Abstract The Internet of things plays a crucial role in all the fields such as agriculture, health care, wearable's, industrial IoT (IIoT), retail, smart city and smart home. In every field, sensors are used to monitor the device values and provided to alert to the decision-making process. In the proposed Monitoring and Alerting using IoT in Cloud platform (MAIC) work, we predict whether the sensor is sending values based on the predefined time schedule. Changes in the agriculture environment have to be captured by these sensors and should be updated in a regular phase. If not, something would have happened to sensors, and such anomaly can be detected easily with the help of ThingSpeak open-source IoT cloud and its apps. In addition, sensor values (like temperature, moisture, humidity, etc.) need to be validated to reflect the correct measures as per the environmental circumstances. If one of these anomalies is detected, smart alerts could be sent to mobile or Twitter or an e-mail account possessed by the individual involved in agriculture activities. The sensor values captured in cloud are processed, and if any drastic change is detected, instant alert is sent to the individuals. These alert messages are authenticated by performing appropriate tweet analysis using R. The MAIC perms an intelligent monitoring of sensor values, and it gives entire belief to the experts who are involved in the system.

Keywords Internet of things · MAIC · Sensors · Thingspeak · Twitter

1 Introduction

The Internet of things is supported by many cloud platforms such as Amazon cloud, IBM bluemix, Microsoft Azure, ThingSpeak, Thingsworx, dream grove Google cloud, Firebase, Salesforce and many different clouds. All the cloud platforms are used for performing data analytics, monitoring, performance analysis and Bot service, etc. For experimental purpose, here, ThingSpeak is chosen. The sensors used here are supported by dexter industries. The grove shield support is given for Arduino

A. Srilakshmi (✉) · K. Geetha · D. Harini
SASTRA Deemed to be University, Thanjavur, India
e-mail: srilakshmi@cse.sastra.edu

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_77

as well as Raspberry Pi, and this GrovePi can be connected with multiple sensors without breadboard and many external wires. If there is a cloud intervention, first step is to connect any device such as Arduino and Raspberry Pi to the cloud and analyze and act accordingly. The streaming data can be captured on the cloud, and smart alerts are sent. The cloud has capability to store tera and petabytes of data streaming every day. The output of the streaming data can be further exported either on hourly basis or by day basis. With the data set, further analytics can be done where the user need not sit in front of the device until hardware-related anomaly is detected.

Nowadays, this technique is used in almost all the fileds such as automobile, smart cities, health care, bio-informatics, sensing system in educational fields and retail. The sensors are used because more accurate and efficient results could be taken based on the threshold limit. The sensor's communication can be made more efficient with the help of Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocols (COAP). Even the IoT data which is called smart data can be secured with the help of cloud security, where each cloud offers good security authentication, authorization, encryption, reduces cyber risk, etc. So, the users can trust the data which will be secured on the cloud by supporting trust ability. Timely data can be visualized and no need to retain separate record as every sensed smart data can be exported in the form of either JSON or CSV format. This format can be used for further analytics and visualization purpose.

2 Related Work

The study has been made before implementing MAIC with the following list of papers. Corbellinib et al. [1] implemented a cloud-based sensor monitoring for environment. The environmental factors are monitored, and sensed data is stored in mobile app through Cloudino and Azure cloud [2]. The wearable sensors are used to monitor patients health, and data are simply stored in cloud. The sensor is embedded in human's shirt; the values are collected and stored to own cloud through WiFi. Kim et al. [3] shows the application of IoT in smart city how IoT plays a major role with traffic light monitoring, minimizing the pollution smart route finder applications etc., and it shows the basic applications in smart city as a survey report [4]. A detailed survey of all the cloud platforms is done and its domains related to application, device system management, data management and analytics feasibilities are detailed [5]. The smart data in a huge volume is collected, and that streaming data is sent to cloud database, and fuzzy rules are used for performing analysis [6]. A decision-based system has been designed to detect light blight disease on potato crop. The complete weather information is monitored. It uses Xively cloud to display the sensor values. It uses Ubidots to display and monitor the sensor values [7]. The IoT detects the machine status, and it is monitored for the unused resources which can be used later. It uses IoT technologies and cloud to display sensor data. It also used RFID tag for communication [8]. The status of chronic skin wound is automated, and it is monitored in a wireless manner. The sensed values are displayed in a monitor as an output without any cloud intervention. Udawant et al. [9] discusses the implementation of heart rate sensor and blood pressure. ECG sensors are used to monitor patient health and to send SMS to hospital database through cloud. This is done to avoid traffic jams caused during peak time to save patient's life. The messages are sent through GPRS to the cloud [10]. The water level is monitored for overflow, and immediate alerts are sent to the cloud. No specific cloud is mentioned [11]. Agriculture plays a vital role in all farmers field, and it is important for Indian economy. Irrigation is a major problem in agriculture. Because farmers waste lot of time and do not know how much water to irrigate and at what time, this issue has been fixed using sensors. The sensors sense the weather condition very precisely so that the irrigation is done at right time [12]. The Iot-based forest monitoring system has been done to remotely monitor the cutting of high-value trees in forest using WSN technique. Finally, it is equipped with GPRS, and data is collected and sent to the mobile app [13]. An Iot-based decision is made to automate irrigation using machine learning techniques.

3 Proposed Architecture

The MAIC architecture well suits for any applications. This is done for agricultural purpose. It uses three different clouds supported for IoT. Each cloud has different types of services to support the user.

The proposed architecture shows the MAIC implementation that has been done in this paper. The incoming sensor values are collected by the cloud, and alerts are sent using IFTTT maker service. It enables the device to communicate with each other through a maker service usually webhooks are used for if condition.

4 Intelligent Monitoring

4.1 Connecting Sensors

In this implementation, few sensors are connected to grove shield which is placed at the top of the Raspberry Pi board

Connecting sensor to grove shield is too easy and simple. Connecting any sensor to grove shield and simply specifying the port number in the code will make the code to run. In Fig. 1, the topmost part is the grove shield which is connected to Raspberry Pi. Once the connection has been made, sensor starts reading the value. Sensors should be fixed to correct port according to the code that has been written. Once sensor starts displaying the values, monitoring process could be started. Any type and number of sensors can be connected to either Arduino or Raspberry Pi with grove. The temperature sensor for, for example, will be operating at the range of −40 to 125 °C. The accuracy range of the sensor at its operating level is 1.5 °C. Similarly,

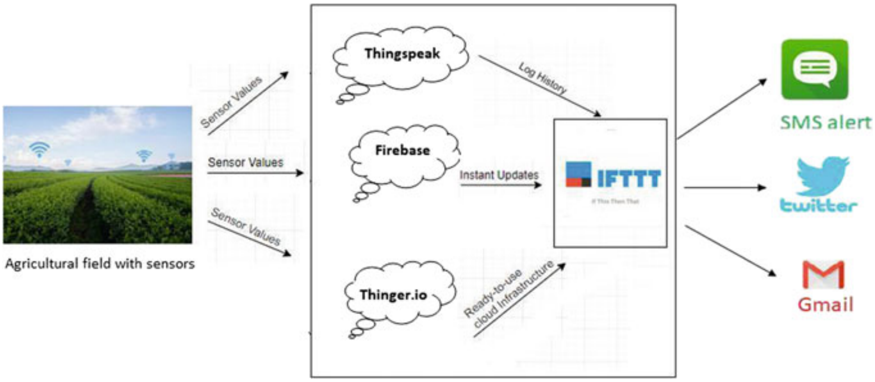


Fig. 1 MAIC architecture

Table 1 Sensor values of moisture

Sensor_Value	Condition
0	Open air
50–250	Dry soil
250–600	Humid soil
600 and above	Floating in water

moisture sensor is connected to another port of grove kit. Then, the minimum, typical and maximum moisture levels are displayed according to the soil condition. The below function senses and displays the sensor values (Table 1).

```
Sensor_value = 0
analogRead(Sensor_value);
```

The sensor values may not be constant for all the time; it will be changing based on the environmental conditions.

The sensors have to be covered with waterproofs to sense precisely.

By monitoring the sensor values, any type of anomaly can be detected such as false alerts or if something happened to sensor. Anamoly here means, whether the sensor has no update for long time, sensor may also be disconnected from the port. Even if it is disconnected, it sends the value as 0. This 0 is different from moisture sensor's (Sensor_value's 0).

4.2 *ThingSpeak Monitoring Service*

The sensor values are monitored via ThingSpeak which directly supports MATLAB for performing analysis. It is an open-source application used for tracking any devices, and smart alerts are sent. First an account has to be created in ThingSpeak and login using MATLAB account. The first step is the channel creation with relevant fields. Based upon the number of sensors, same number of fields has to be created. Figures 2 and 3 show the values of temperature and soil moisture sensor. After creating a channel, the API keys can be used to read and write data into the channel. Both Figs. 2 and 3 show the private view chart of the channel. Here, the channel is not updated frequently. For every twenty minutes, the channel is updated.

The below figure shows the specifications of temperature and moisture sensors (Figs. 4 and 5).

The temperature level which is displayed in Fig. 1 is normal, whereas the moisture level is high. If the moist is between 0 and 300, then the soil is dry. Specifically, if the moist level is 0, 1, 2, 3, etc., then the sensor is in free space. For the range between 300 (min) and 700 (max), the soil is humid and enough for irrigating plants.

As shown in Fig. 2, if the range exceeds 700, then the sensor is floating in water. In this case, it is 761. Once the chart has been displayed, MATLAB visualization can be made to analyze the temperature and moisture variation.

Now based on the temperature, analysis can be done on one of the following.

Case (i): Sending smart alerts from ThingSpeak to Twitter, or by short messaging service or to e-mail account.
Case (ii): If there is no update from the sensor for some time period.

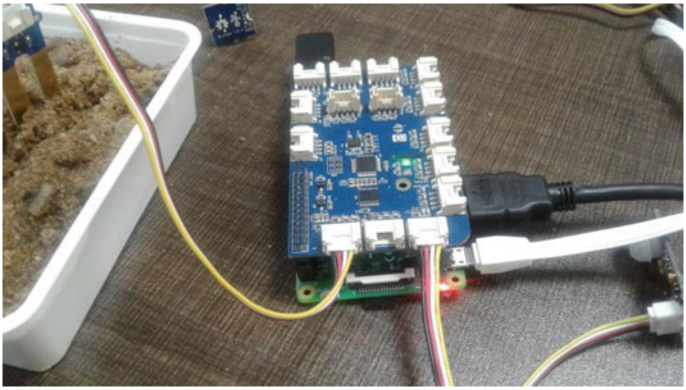
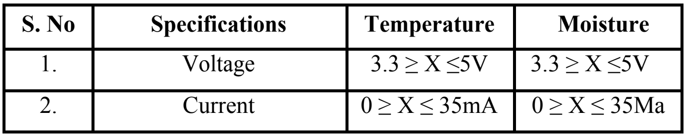


Fig. 2 Raspberry Pi GrovePi



S. No	Specifications	Temperature	Moisture
1.	Voltage	3.3 ≥ X ≤5V	3.3 ≥ X ≤5V
2.	Current	0 ≥ X ≤ 35mA	0 ≥ X ≤ 35Ma

Fig. 3 MAIC specifications

Fig. 4 Temperature values

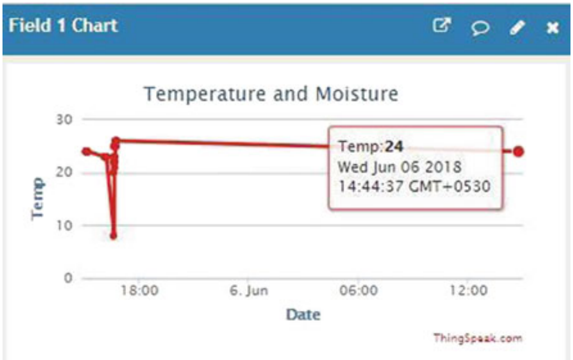
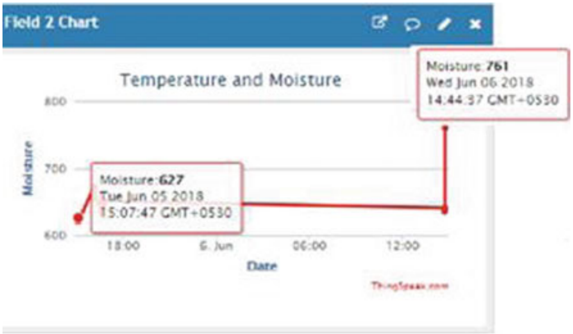


Fig. 5 Moisture values



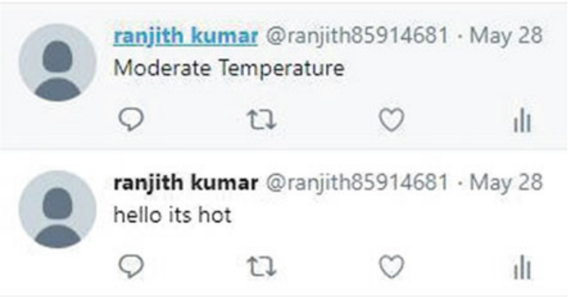
Case I

A ThingTweet app is created from ThingSpeak, refer Fig. A, and it is linked to Twitter account. By authorizing the app, an API key is generated which is later used for any other purposes. Next React app is created, and it is set to react on particular condition, i.e., if temperature is above 35 °C then the phrase too hot is tweeted. The React app is linked to ThingTweet by adding the twit account into it. The condition type of React app is set to numeric, and test frequency is set to data insertion because if the condition is once met the alert can be sent immediately. Based upon the sensor, the condition type is chosen as either numeric or string or status, etc. Figure 2.1 shows the alert message of Twitter. Once, it is greater than 35 °C and moderate in the evening which is 28 °C (Fig. 6).

Case II

In the second case, if there are no updates from the sensor, it is identified and notification is sent to the user. If the channel or channel ID has no update for last 15 min it tweets that there is no update. Note that the same user ID is used for performing future Twitter analysis.

Fig. 6 MAIC alert system 1

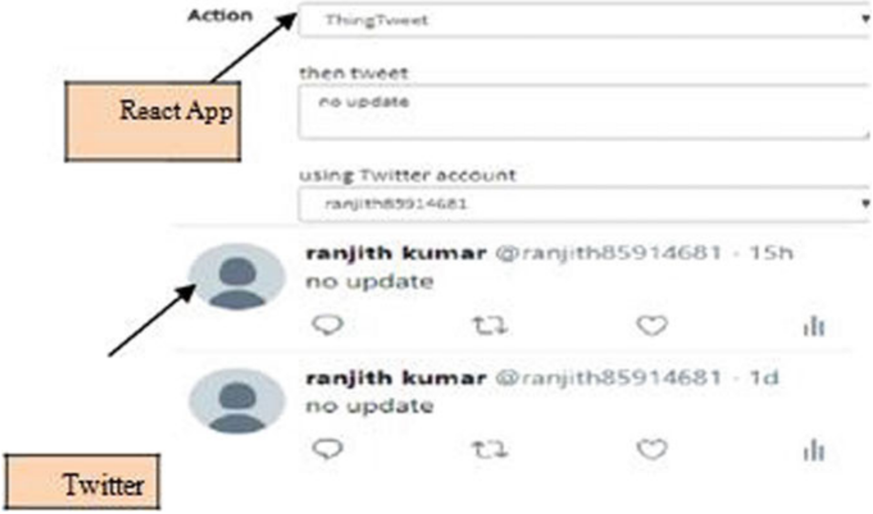


ranjith kumar @ranjith85914681 · May 28
Moderate Temperature

ranjith kumar @ranjith85914681 · May 28
hello its hot

Figure 7 shows the Twitter message when there is no update from the sensor for ling time. The React app is made to run to take action for ThingTweet.

```
ThingHTTP_APIKEYS =
struct('To_Trigger_TalkBack','LOO6RKV2VZWPH5
7Z','To_Trigger_ThingTweet','K2BDUJ30Y7AI37J L');% Your ThingHTTP app API keys
url =
'https://api.thingspeak.com/apps/thinghttp/s
end_request?api_key=HBVE4CS981Z9XR5O';
Trigger_TalkBack =
webread(url,'LOO6RKV2VZWPH57Z',ThingHTTP_API
KEYS.To_Trigger_TalkBack) %Trigger TalkBack
via ThingHTTP
Trigger_ThingTweet =
webread(url,'K2BDUJ30Y7AI37JL',ThingHTTP_API KEYS.To_Trigger_ThingTweet)
%Trigger ThingTweet via ThingHTTP.
```



Action: ThingTweet

then tweet: no update

using Twitter account: ranjith85914681

ranjith kumar @ranjith85914681 · 15h
no update

ranjith kumar @ranjith85914681 · 1d
no update

Fig. 7 MAIC alert system 2

4.3 Sending Alerts Using IFTTT Maker Service

Similar alerts could be sent using the If This Then That (IFTTT) platform. An applet service is created for if condition by choosing a Web hooks app and getting the event name. For the else condition, the alert app can be chosen from the one listed in the applet page.

```
E:g A if{Web hook
      {event = the Temperature is too cool}  → 1
      }
      then
      alert using either
      {
      Messages (sms) or twitter or face book  → 2
      }
```

Once a maker service has been created, it generates a unique URL for every request that has been created. For example, below is the URL for this maker service. This is saved for further use in ThingSpeak.

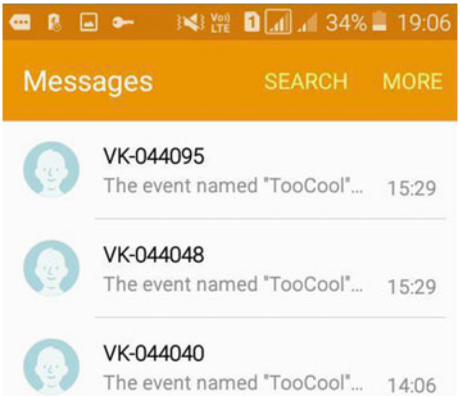
https://maker.ifttt.com/trigger/{event}/with/key/g9nIpq6zJ396aRex-qzeocpEXGgkVixGLlvgtxtnpoM.

To make the above code to work, the URL is configured in ThingSpeak ThingHttp.

The HTTP method used here is GET method which accesses the specified URL. Now, when the React app is configured with ThingHTTP, it starts sending message. The below Fig. 8 shows the messages which are received by the maker service, and the event named TooCool is executed.

Similar alert could be sent to Facebook and e-mail simply by editing the example A which is named number 2.

Fig. 8 MAIC alert system 2



VK-044095
The event named "TooCool"... 15:29

VK-044048
The event named "TooCool"... 15:29

VK-044040
The event named "TooCool"... 14:06

5 Monitoring Using Firebase Cloud

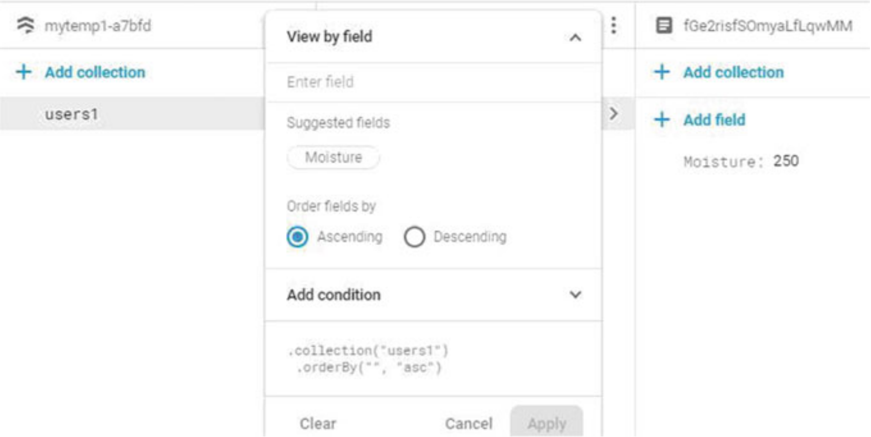
Firebase is a mobile and Web application platform which is supported by Google. It performs many cloud activities and API functions. It also plays a role in Internet of things for displaying the sensor values as real-time database. The real-time streaming database values are displayed in the database, and it is stored separately.

The configuration between Firebase and Raspberry Pi goes like this:

```
 {
 config=’apikey’,’authDomain’,’databaseURL’, ’storageBucket’
 config = {
"apiKey":
"AIzaSyD2bULaxHyZA0RSxksWkz0FJTmShM5eQdM",
"authDomain": "mytemp2-c54cb.firebaseapp.com",
"databaseURL":"https://mytemp2c54cb.firebaseio.com/",
storageBucket": "mytemp2-c54cb.appspot.com"
 }
```

Once the configuration information is verified, the Python code will be successfully connected to Firebase. The pyrebase. initialize_app(config) will be initialized to a variable, and this variable is required to update the data bucket (Fig. 9).

The difference between ThingSpeak monitored values and Firebase values is shown in Fig. 10, i.e., the ThingSpeak displays the sensor values at every second as you can see in Fig. 4, the sensor values starting at the time of 10.07 and continuously printing the values. But in Firebase, the streaming values are updated only if there is change in sensor value as you can see in Fig. 4 that none of the moisture or temperature value is constant either one is changing and hence the data is uploaded

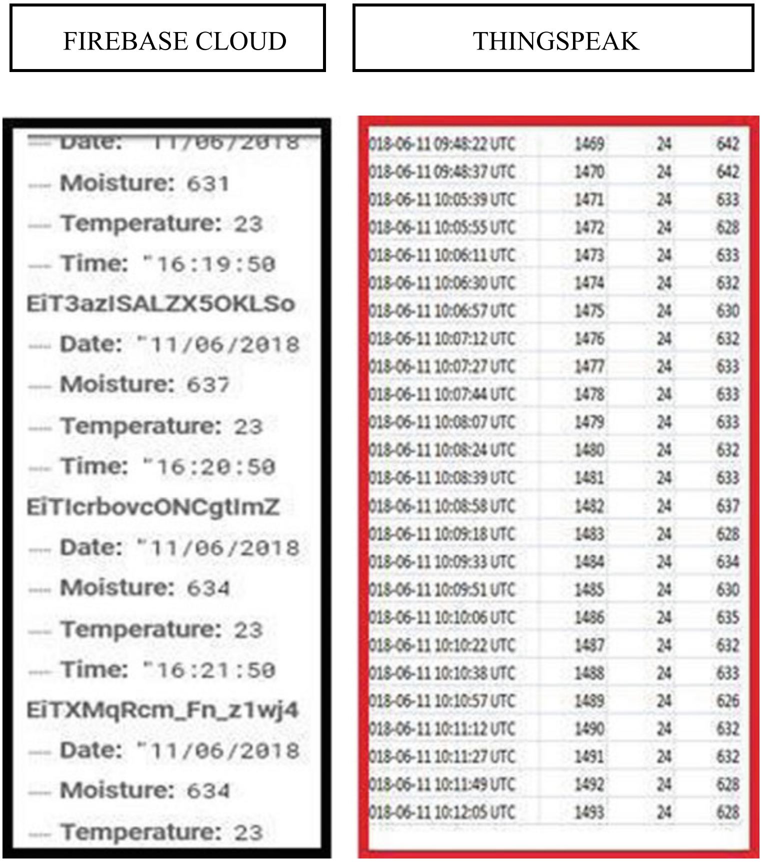


Order fields by: ● Ascending ○ Descending

```
.collection("users1")
 .orderBy("", "asc")
```

Moisture: 250

Fig. 9 Querying MAIC



FIREBASE CLOUD

```
— Date: "11/06/2018
— Moisture: 631
— Temperature: 23
— Time: "16:19:50
EiT3azISALZX5OKLSo
— Date: "11/06/2018
— Moisture: 637
— Temperature: 23
— Time: "16:20:50
EiTIcrbovcONCgtImZ
— Date: "11/06/2018
— Moisture: 634
— Temperature: 23
— Time: "16:21:50
EiTXMqRcm_Fn_z1wj4
— Date: "11/06/2018
— Moisture: 634
— Temperature: 23
```

THINGSPEAK

018-06-11 09:48:22 UTC	1469	24	642
018-06-11 09:48:37 UTC	1470	24	642
018-06-11 10:05:39 UTC	1471	24	633
018-06-11 10:05:55 UTC	1472	24	628
018-06-11 10:06:11 UTC	1473	24	633
018-06-11 10:06:30 UTC	1474	24	632
018-06-11 10:06:57 UTC	1475	24	630
018-06-11 10:07:12 UTC	1476	24	632
018-06-11 10:07:27 UTC	1477	24	633
018-06-11 10:07:44 UTC	1478	24	633
018-06-11 10:08:07 UTC	1479	24	633
018-06-11 10:08:24 UTC	1480	24	632
018-06-11 10:08:39 UTC	1481	24	633
018-06-11 10:08:58 UTC	1482	24	637
018-06-11 10:09:18 UTC	1483	24	628
018-06-11 10:09:33 UTC	1484	24	634
018-06-11 10:09:51 UTC	1485	24	630
018-06-11 10:10:06 UTC	1486	24	635
018-06-11 10:10:22 UTC	1487	24	632
018-06-11 10:10:38 UTC	1488	24	633
018-06-11 10:10:57 UTC	1489	24	626
018-06-11 10:11:12 UTC	1490	24	632
018-06-11 10:11:27 UTC	1491	24	632
018-06-11 10:11:49 UTC	1492	24	628
018-06-11 10:12:05 UTC	1493	24	628

Fig. 10 Comparison between firebase and ThingSpeak

to the cloud. It is is a real-time database; it takes just a fraction of second to update the streaming data to cloud whereas ThingSpeak takes 10–11 s to upload the data in the graph after running the code. The sensor data can be exported in the form of JSON data in Firebase and CSV/JSON/XML in ThingSpeak. The Firebase cloud can display the streaming view of values using stream view. In the future, it is easy to retrieve the moisture data with database options, i.e., to print in either ascending or descending sensor values. It is also easy to retrieve by field using view by field. The below diagram shows the sensor value in the collection field.

The value 250 represents that the soil is humid. Based on the value and the type of plantation, the expert decides when and how much amount of water has to be irrigated. Irrigation is the main source for any agricultural fields

The below table shows the comparison between two cloud techniques. The Firebase shows the streaming data, whereas the ThingSpeak detects the value only after 20 s from connection. Firebase has no inbuilt support to MATLAB analysis and visualization as ThingSpeak does. But it has good machine learning kit, and it can be easily connected to android app. For every activity, an Android app is created so that user can easily monitor from the app itself. IoS is also supported for IoS users. The cloud-based code for Raspberry Pi should be connected and kept running, hence to see the values in cloud. If the Pi device is disconnected, the user or expert may have difficulty in interpreting. Even if the disconnection of sensor happens, such alert can also be sent to the user, so there is no chance to get any incorrect value or missing sensor values. The smart sensor data is always evolving from the device.

In Firebase, it is possible to add and remove fields at run time. The Firebase does not support MATLAB, and it helps in performing the machine learning algorithms and statistical analysis can be done. The Firebase shows the updates only if there is a change in the sensing value of at least one sensor connected to cloud.

6 The Thinger.io Cloud

The thinger.io cloud also displays the streaming data similar to Firebase.

```
#define USERNAME “ggg@gmail.com”
#define DEVICE_ID “temp1”
#define DEVICE_CREDENTIAL “12345678”
#define SSID “Agri”
#define SSID_PASSWORD “12345678” ThingerWifi thing(USERNAME,
DEVICE_ID,
DEVICE_CREDENTIAL);
```

The above one connects to the thinger.io cloud. Similar tweets can also be sent to thinger.io cloud. The thinger.io is a public and open-source cloud platform for IoT and free of cost. It enables the user to connect the IoT devices and monitor the sensor values. The cloud also sends alert to Twitter based on the condition. It also displays the number of devices connected to its dashboards and data buckets. It gives a complete statistics of the implementation and works efficiently with Arduino and Sigfox.

7 Twitter Analysis

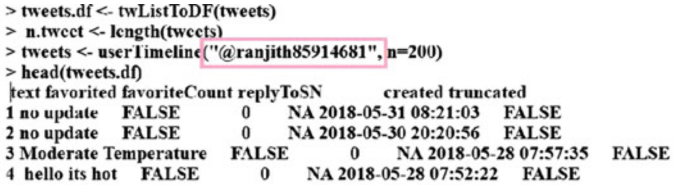
The sensor device is intended to send the sensor data if there is no update from the device for past x minutes or n hour. This itself detects the anomaly from the device, and if there is throughout same values for more than x minutes, the next anomaly is cached and the response is sent either in the form of tweets or mobile SMS.

To ensure that the anomaly is exactly from ThingSpeak or Firebase, the tweet analysis has been made. The security parameters are accessed from the Twitter account such as consumer key, Consumer secret, Access token and Access secret.

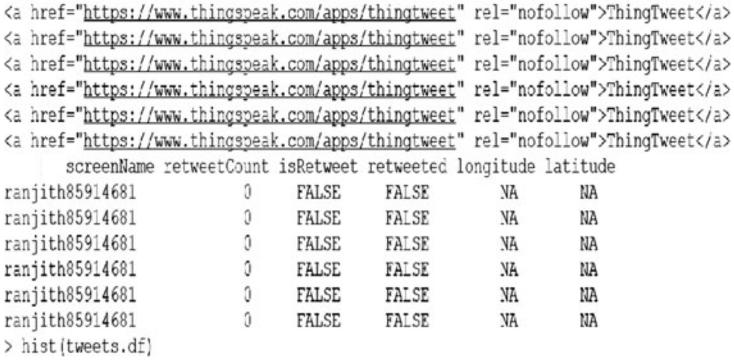
The OAuth information is sent to setup_twitter_oauth() function as arguments. Then, it is possible to access the Twitter account regarding the number of tweets and its origination from the Web page. The R tool is used for performing the analysis, and the tweets are for a particular user. The user account which is created for ThingSpeak uses tweet account of any person to whom the alert has to be sent. As shown in the example code, the user account ranjith85914681 is also there in ThingSpeak Twitter. The user Id is displayed in R code to ensure the identity of the user.

```
consumer_key <- '53Udm77XRtcVgDkWGay7UQT'
> consumer_secret <-'X2FydARqOxxxxxxxybjuWg1qQ0nFtrH4RHkI3vMddKIF h'
> access_token <- '99675463453567557-271k2HFLaeZBOClF3wNVcvblCeoHKbf'
> access_secret 'CqoZNPQMs8o6CZSDXGDFXFGDFWMkicr1bAFU5yR eOYOLlf4LBJC'
> setup_twitter_oauth(consumer_key, consumer_secret, access_token, access_secret)
```

Once the information are authentical, the tweets can be collected. The head(tweets.df) gives the top tweets of the user. It requires packages like Twitter, ROAuth and the same libraries.



```
> tweets.df <- twListToDF(tweets)
>  n.tweet <- length(tweets)
> tweets <- userTimeline("@ranjith85914681", n=200)
> head(tweets.df)
 text favorited favoriteCount replyToSN          created truncated
1 no update    FALSE          0      NA 2018-05-31 08:21:03    FALSE
2 no update    FALSE          0      NA 2018-05-30 20:20:56    FALSE
3 Moderate Temperature    FALSE          0      NA 2018-05-28 07:57:35    FALSE
4  hello its hot    FALSE          0      NA 2018-05-28 07:52:22    FALSE
```



```
<a href="https://www.thingspeak.com/apps/thingtweet" rel="nofollow">ThingTweet</a>
<a href="https://www.thingspeak.com/apps/thingtweet" rel="nofollow">ThingTweet</a>
<a href="https://www.thingspeak.com/apps/thingtweet" rel="nofollow">ThingTweet</a>
<a href="https://www.thingspeak.com/apps/thingtweet" rel="nofollow">ThingTweet</a>
<a href="https://www.thingspeak.com/apps/thingtweet" rel="nofollow">ThingTweet</a>
<a href="https://www.thingspeak.com/apps/thingtweet" rel="nofollow">ThingTweet</a>
       screenName retweetCount isRetweet retweeted longitude latitude
ranjith85914681            0     FALSE     FALSE        NA       NA
ranjith85914681            0     FALSE     FALSE        NA       NA
ranjith85914681            0     FALSE     FALSE        NA       NA
ranjith85914681            0     FALSE     FALSE        NA       NA
ranjith85914681            0     FALSE     FALSE        NA       NA
ranjith85914681            0     FALSE     FALSE        NA       NA
> hist(tweets.df)
```

Thus, the sample tweets are shown, and this is needed only to ensure that the tweet alerts are only from the device connected with cloud-like ThingSpeak or thinger.io or Firebase. Even a normal person may also end a casual message saying that it is too hot or cold in my place and to differentiate from that tweet analysis is done.

8 Conclusion and Future Work

The MAIC implementation helps in effectively monitoring the sensor device remotely. Sometimes, the sensor may be disconnected then also it is able to send alerts to the system with zero values. The expert might not have any knowledge about this. If the temperature of the agriculture field or moisture of the field is zero, then such contiguous zero is detected and written to ThingSpeak and IFTTT saying that if the temperature is zero throughout or same for long time or no update for long time or too cool or too hot or too moist alerts could to send to either mail or SMS or tweets based on the expertise's source usability. The MAIC can be implemented with any other cloud technologies. Similarly, MQTT message queuing could be used to manage communication between IoT devices. It is lightweight protocol which is able to publish and subscribe data between IoT devices where two devices do not know the identity of each other.

In the future, the same alert could be sent via other standard clouds like Microsoft Azure, IBM, Amazon Google Cloud and Salesforce to find different monitoring techniques and perform various machine learning techniques and analytics and finally combining everything and making as an Android app for farmers.

Acknowledgements The work projected in this paper was implemented and tested using Raspberry Pi with grove kit provided at Technology Business Incubator (TBI), Sastra Deemed to be University. We would like to acknowledge the facility extended by TBI for IoT.

References

1. Corbellinib S, Di Franciaa E, Grassinia S, Iannuccib L, Lombardob L, Parvisb M (2018) Cloud based sensor network for environmental monitoring. Measurement 118:354–361
2. Leu F–Y, Ko C–Y, You I, Raymond Choo K–K, Ho C–L (2018) A smartphone-based wearable sensors for monitoring real-time physiological data. Comput Electr Eng
3. Kim T, Ramos C, Mohammed S (2017) Smart city and IoT. Future Gener Comput Syst 76:159–162
4. Ray PP (2016) A survey of IoT cloud platforms 1(1–2):35–46
5. Kumar PM, Lokesh S, Varatharajan S, Babu GC, Parthasarathy P (2018) Cloud and IoT based disease prediction and diagnosis system for healthcare using Fuzzy neural classifier. Future Gener Comput Syst 86:527–534
6. Foughali K, Fathallah K, Frihida A (2018) Using cloud IOT for disease prevention in precision agriculture Procedia Comput Sci 130:575–582
7. Zhong RY, Wang L, Xu X (2017) An IoT-enabled real-time machine status monitoring approach for cloud manufacturing. Procedia CIRP 63:709–714
8. Pal A, Goswami D, Cuellar HE, Castro B Kuang S, Martinez RV (2018) Early detection and monitoring of chronic wounds using low-cost, omniphobic paper-based smart bandages. Biosens Bioelectron 117:696–705
9. Udawant O, Thombare N, Chauhan D, Hadke A, Waghole D (2017) Smart ambulance system using IoT. In: International Conference on Big Data, IoT and Data Science (BID), pp 171–176
10. Perumal T, Sulaiman MN, Leong CY (2015) Internet of Things (IoT) enabled water monitoring system. In: IEEE 4th global conference on consumer electronics (GCCE), pp 86–87

11. Nageswara Rao R, Sridhar B (2018) IoT based smart crop-field monitoring and automation irrigation system. In: 2nd international conference on inventive systems and control (ICISC), pp 478–483
12. Sharma Ak, Ansari MFR, Siddiqui MF, Baig MA (2017) IoT enabled forest fire detection and online monitoring system. Int J Curr Trends Eng Res (IJCTER), 3(5):50–54
13. Navarro Hellin H, Martínez-del-Rincon J, Domingo Miguel R, Soto Valles F, Torres Sanchez R (2016) A decision support system for managing irrigation in agriculture. Comput Electron Agric 121–131

Open Set Domain Adaptation for Hyperspectral Image Classification Using Generative Adversarial Network

S. Nirmal, V. Sowmya and K. P. Soman

Abstract Hyperspectral image (HSI) classification attracted lots of attention due to its complexity in dealing with large dimensions. In recent years, the techniques for dealing with the HSI have been evolved, ensuring the increase in efficiency to some extent in classification and other perspectives. Domain adaptation is a well-established technique for using any trained classification model, when the feature space from target domain is a subset of feature space from source domain. The objective of this paper is to create an efficient and effective model for HSI classification by implementing open set (OS) domain adaptation and generative adversarial network (GAN). This has advantages in quite few ways, such as creating a single training model that deals with various HSI data set with common classes, classifying the features in any data to specific trained classes and unknown (to be labelled) making it easy to annotate. The proposed open set domain adaptation for HSI classification is evaluated using Salinas and Pavia. The proposed method resulted in the classification accuracy for unknown classes as 99.07% for Salinas and 81.65% for Pavia.

1 Introduction

In recent years, machine learning and deep learning techniques depict a remarkable performance in different fields like speech processing, forecasting, computer vision, machine translation, prediction and health care [1, 2]. Hyperspectral remote sensing is one of the areas, where deep learning is applied due to its inexplicable efficacy [3–6]. Hyperspectral remote sensing uses the electromagnetic spectrum to identify

S. Nirmal · V. Sowmya · K. P. Soman (✉)
Center for Computational Engineering and Networking (CEN), Amrita School
of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India
e-mail: kp_soman@amrita.edu

S. Nirmal
e-mail: nirmalsenthilnathan@gmail.com

V. Sowmya
e-mail: v_sowmya@cb.amrita.edu

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_78

and classify the objects, based on spectral response. Hyperspectral images (HSI) consist of spatial and spectral information. Spectral information is given in the form of bands and number of bands varies depending on the sensor.

Generative adversarial network (GAN) [7–9] is a classification technique, which comprises of two portions as follows: a generator and a classifier. Generator in the network considers random data and continuously tries to imitate the input data. the classifier in the network is trained to classify the original data from the generated data. Because of this continuous training between the generator and classifier in GAN network, high accuracy rates can be obtained with less data samples.

Now, there is a high chance that various data sets may or may not contain common classes. In such case, a model trained for one data set can be used in other data set with necessary modifications. This technique is represented as transfer learning (TL) [10–12]. Domain adaptation is a part of TL, where a features of a target data set are a subset of features of source data set [13, 14]. There are two types of domain adaptation namely: closed set (CS) and open set (OS) domain adaptation. CS domain adaptation is used when the number of classes in both source and target domain are exactly the same. Whereas, OS domain adaptation is used when target domain contains unknown classes that are not presented in source domain [15, 16].

In the proposed work, we present a novel approach for dealing with HSI classification using OS domain adaptation and GAN [17]. In practical, the unknown class is unlimited, which makes it difficult to address with high precision, when training source domain. To overcome this issue, we make use of OS domain adaptation by backpropogation [17, 18], for training unknown class samples, as well as increasing the individual class accuracy. Each pixel in the HSI represents the spectral signature of the specific class. This also means that the class labelling has to be done for every pixel, which is very difficult in real-life scenario. Also, pre-processing is done to extract 1D pixel data with class information from 3D HSI image, to train the model.

The methodology is described in detail in Sect. 2. The experiment is carried out on two sets of HSI data after pre-processing, as mentioned in Sect. 3. Experimental results and conclusion are discussed in Sects. 4 and 5.

2 Methodology

In this paper, we have considered the architecture used in [17] to implement OS domain adaptation for HSI. The data x_s and label y_s from source (X_s, Y_s) and data x_t for target (X_t) are considered. The general architecture used in the work is described in Fig. 1.

The class dimension for source data is K (known class) and for target data is K+1 (known + unknown class). Generally, the number of input and output classes in a model must be same. Unlike other open set domain adaptation models [16], we do not provide any data to separately train for unknown classes. To make up for the missing class data, the generated data from generator, which fails to pass through the

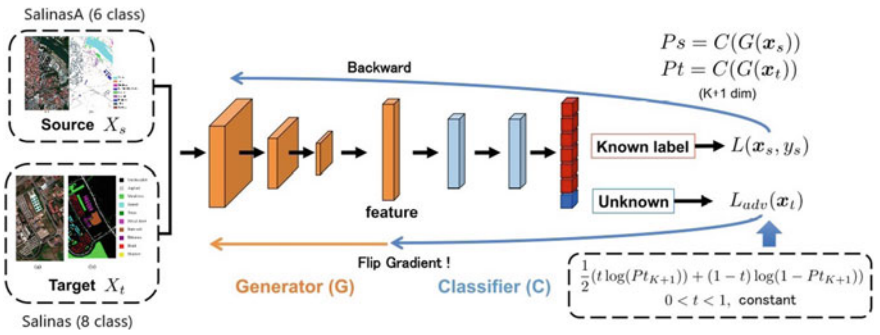

SalinasA (6 class)
Source X_s
Target X_t
Salinas (8 class)
Backward
$Ps = C(G(\boldsymbol{x}_s))$
$Pt = C(G(\boldsymbol{x}_t))$
(K+1 dim)
feature
Known label
$L(\boldsymbol{x}_s, y_s)$
Unknown
$L_{adv}(\boldsymbol{x}_t)$
Flip Gradient !
Generator (G)
Classifier (C)
$\frac{1}{2}(t\log(Pt_{K+1})) + (1-t)\log(1-Pt_{K+1}))$
$0 < t < 1$, constant

Fig. 1 Open set model architecture [17] mapped for hyperspectral image classification

classifier, will be used to train the unknown class in source domain. Hence, there is no need to provide data separately for unknown class during training.

When input data (x) are passed into the network, the generator will try to increase the error rate by generating images. These generated images G(x) are then passed as input to the classifier. The classifier will try to get a boundary between known and unknown target classes. There the common class data (x_s, y_s) present in the target will be classified as known and remaining data as unknown class.

The output of classifier C(G(x)) will have K+1 logits. The softmax function is used to convert the logits into probabilities [17]. Thus, we get K+1 dimensional output for K-dimensional input. The classifier is trained to give output of p($y = K + 1|x_t$) = t, where $0 < t < 1$. In our experiment, the value of t = 0.5 is set as a boundary between known and unknown class [3].

3 Data Set and Model Description

This section provides the intuitive understanding of HSI data set and convolution neural network model used in the experiment.

Salinas is HSI data set collected over Salinas Valley, California, using AVIRIS sensor [19]. The spatial resolution for this data set is 3.7-metre pixels. The dimension of the data is 512 × 217 × 224 with a total of 16 classes.

Salinas-A is one of the extracted subscene of Salinas image, which comprises 86 × 83 × 224 pixels with 6 classes [19]. For one of our experiment, we consider, Salinas-A data set with 6 classes (source) and Salinas data set with 8 classes (target) is used. The class and sample for each class is mentioned in Table 1.

PaviaU is one of the two data sets obtained from Pavia, Northern Italy, using ROSIS sensor [19]. Pavia University is comprised of 610 × 610 × 102 pixels representing nine classes, after discarding few samples with no information.

For next part of the experiment, 5 classes were selected from PaviaU data set with 1000 samples in each class, which is used for source training. Then, the complete

Table 1 Data set description for Salinas-A(source) and Salinas(target)

Class	Features	Source data set (Salinas-A)	Target data set (Salinas)
0	Brocoli_green_weeds_1	391	2008
1	Corn_senesced_green_weeds	1343	3278
2	Lettuce_romaine_4wk	616	1068
3	Lettuce_romaine_5wk	1524	1927
4	Lettuce_romaine_6wk	675	916
5	Lettuce_romaine_7wk	799	1070
6	Unknown (Brocoli_green_weeds_2 and Fallows)	0	5702
Total samples		5348	15969

Table 2 Data set description for PaviaU with 5 classes (source) and PaviaU with 9 classes(target)

Class	Features	PaviaU (source domain—5 classes)	PaviaU (target domain—9 classes)
0	Asphalt	1000	6631
1	Bare Soil	1000	5029
2	Gravel	1000	2099
3	Trees	1000	3064
4	Painted metal sheets	1000	1345
5	Unknown (Meadows, Self-Blocking Bricks and Shadows)	0	24607
Total samples		5000	42775

PaviaU data set with around 42,775 samples with 9 classes is used as target. The data set details are mentioned in Table 2.

The convolutional neural network (CNN) is used for training the model in the architecture. The details regarding layers of CNN used in the experiment is shown in Fig. 2. 1D-batch normalization is used with convolution and fully connected layer.

4 Experimental Results

The parameters which gives the best results for our model during the experiment are mentioned below. In the proposed work, the network is trained for 2000 epochs and batch size of 128. Adam optimization method with learning rate of (0.001) and cosine ramp-down is used for training the network [17].

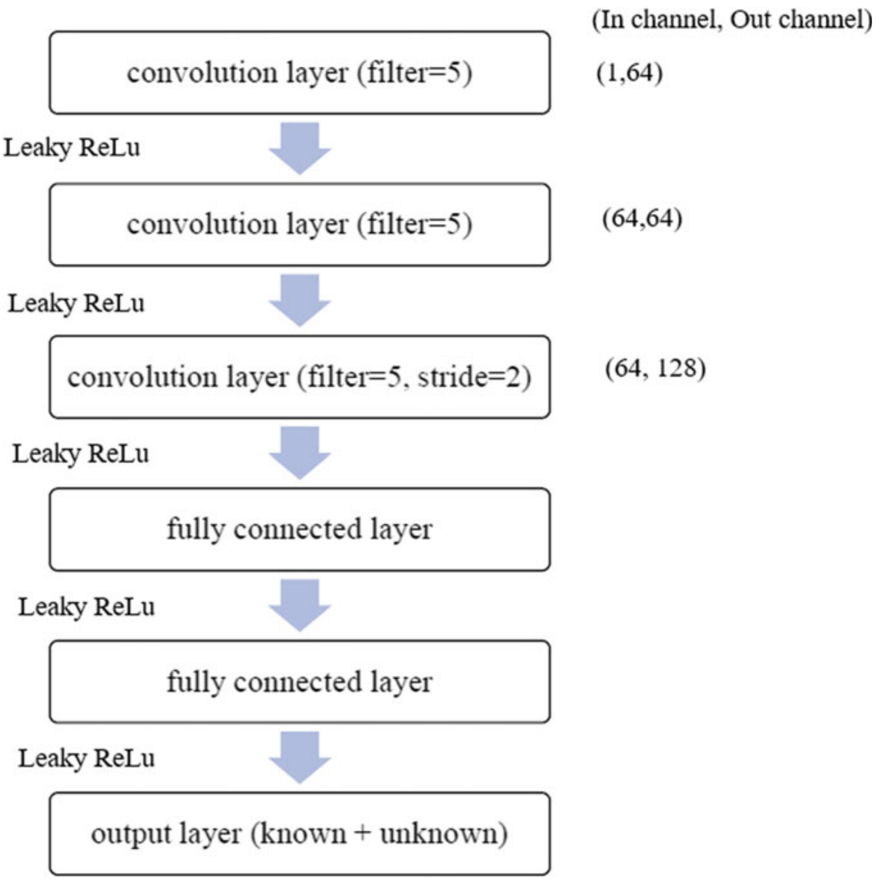

(In channel, Out channel)
convolution layer (filter=5)
(1,64)
Leaky ReLu
convolution layer (filter=5)
(64,64)
Leaky ReLu
convolution layer (filter=5, stride=2)
(64, 128)
Leaky ReLu
fully connected layer
Leaky ReLu
fully connected layer
Leaky ReLu
output layer (known + unknown)

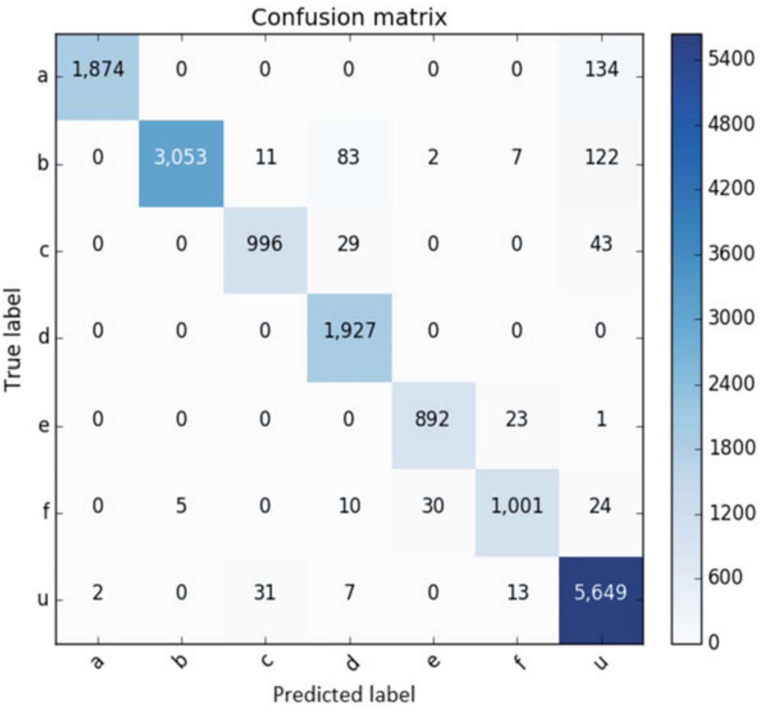
Fig. 2 Convolution neural network used in the proposed open set domain adaptation for hyperspectral image classification

4.1 Salinas Data Set

The main purpose of the work is to identify the model effectiveness in classifying the unknown class. So, precision, recall (classwise accuracy) and f1-score are calculated with contingency values obtained using confusion matrix (CM) and are used to evaluate the model. Table 3 shows the results for first experimental set-up using Salinas-A (source—6 classes) and Salinas (target—8 classes). The receiver operating characteristics (ROC) curve is a plot between true positive rate and false positive rate, in which the area under the curve (AUC) represents the accuracy of various classifier. The average accuracy of the known class is 95.10% and AUC is 98%. By using confusion matrix (CM) in Fig. 3, we can interpret that from unknown class with 5702 samples collected from multiple classes, 53 samples are misclassified into

Table 3 Classwise accuracy for Salinas-A (source) and Salinas (target) obtained using the proposed method

Class	Features	Precision	Recall	F1-Score
0	Brocoli_green_weeds_1	1.00	0.93	0.96
1	Corn_senesced_green_weeds	1.00	0.93	0.96
2	Lettuce_romaine_4wk	0.96	0.93	0.95
3	Lettuce_romaine_5wk	0.94	1.00	0.97
4	Lettuce_romaine_6wk	0.97	0.97	0.97
5	Lettuce_romaine_7wk	0.96	0.94	0.95
6	Unknown (Brocoli_green_weeds_2 and Fallows)	0.95	0.99	0.97
Average		0.97	0.96	0.96



	a	b	c	d	e	f	u
a	1,874	0	0	0	0	0	134
b	0	3,053	11	83	2	7	122
c	0	0	996	29	0	0	43
d	0	0	0	1,927	0	0	0
e	0	0	0	0	892	23	1
f	0	5	0	10	30	1,001	24
u	2	0	31	7	0	13	5,649

Fig. 3 Confusion matrix obtained for the proposed method for Salinas-A (source) and Salinas (target) data set

other classes and classification accuracy of 99.07% and AUC of 0.98%is obtained. We can interpret from above results that our classifier model works well in both known and unknown classes.

Table 4 Classwise accuracy for PaviaU with 5 classes (source) and PaviaU with 9 classes (target) obtained using the proposed method

Class	Features	Precision	Recall	F1-Score
0	Asphalt	0.78	0.98	0.93
1	Gravel	0.91	0.59	0.72
2	Trees	0.61	0.87	0.72
3	Self-Blocking Bricks	0.69	0.87	0.71
4	Bare Soil	1.00	0.99	0.99
5	Unknown (Meadows, Painted metal sheets and Shadows)	0.88	0.83	0.85
Average		0.81	0.86	0.83

4.2 PaviaU Data set

For the second experiment, PavaiU data set is considered to check the authenticity of OS domain adaptation for HSI in classifying unknown class data. Table 4 shows the precision, recall and f1-score results for PaviaU (source— class—5000 samples) and PaviaU (target—9 class—42,775 samples). The average accuracy rate of known class is 85.97%. On further study using CM in Fig. 4, around 4400 samples out of 24,607 unknown samples are misclassified into other classes and the classification accuracy rate of 81.65% is obtained unknown class. when the proportion between known and unknown class sample is taken into consideration, this further proves that the model works well in classifying unknown class samples. We got an average rate of above 80% in both precision and recall (sensitivity) and overall average AUC of 84%, which further proves that open set domain adaptation can implemented in HSI classification.

Table 5 gives the overall accuracy rates for the experiments discussed above. We evaluated the performance of the model using classification accuracy for known and unknown classes. we also calculated precision, recall and f1-score for further studies. It is observed from the results that the model could accurately distinguish the unknown class from known classes in hyperspectral data set. Since the number of training samples chosen in both cases is low, it can be said that GAN plays an important role in obtaining the desired results.

5 Conclusion

In this work, we applied open set domain adaptation to hyperspectral data set using GAN. The obtained results shows that, open set domain adaptation works well with HSI and it will increase the efficiency of HSI classification models. It is clear from the experimental analysis that, various HSI data set can share a common training model

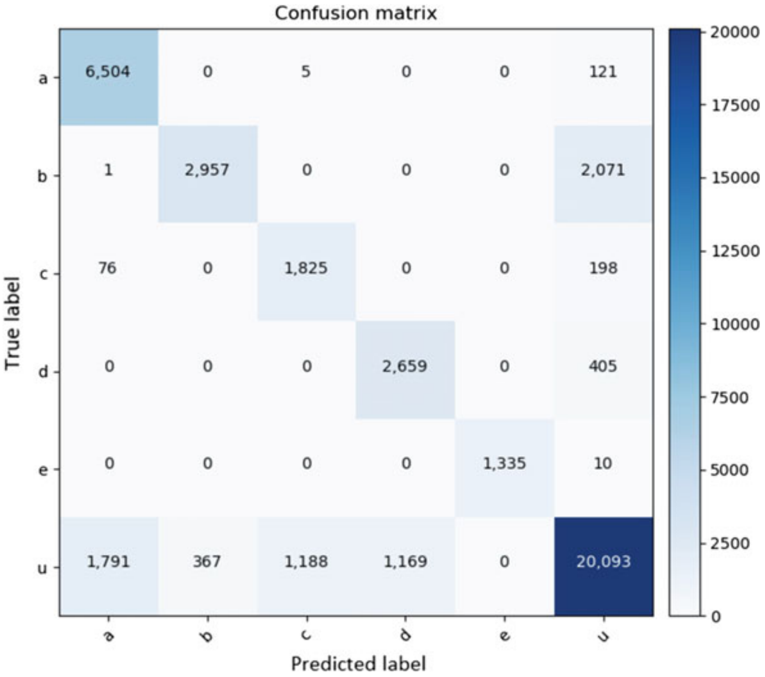


Fig. 4 Confusion matrix obtained for the proposed method for PaviaU data set with 5 classes (source with 1000 samples in each class) and 8 classes (target)

Table 5 Performance of the proposed open set domain adaptation method for hyperspectral image data sets

Data set	Known class accuracy (%)	Unknown class accuracy (%)	Overall accuracy (%)
Salinas-A and Salinas	95.10	99.07	96.38
PaviaU with 5 and 9 classes	85.97	81.65	82.69

irrespective of the number of classes (excluding common classes) and samples with the use of GAN network.

As the future scope of the present work, the hyperparameter tuning can be performed to increase the efficiency of the proposed model and also it can be extended to other HSI data set with different spectral ranges.

References

1. Pathinarupothi RK, Rangan ES, Gopalakrishnan EA, Vinaykumar R, Soman KP (2017) Single sensor techniques for sleep Apnea diagnosis using deep learning. In: IEEE International Conference on Healthcare Informatics (ICHI), pp 524–529
2. Charmisha S, Sowmya V, Soman KP (2018) Dimensionally reduced features for hyperspectral image classification using deep learning. In: Proceedings of the international conference on communications and cyber physical engineering, vol 500, pp 171–179
3. Srivatsa S, Sowmya V, Soman KP (2016) Empirical wavelet transform for improved hyperspectral image classification, intelligent systems technologies and applications, pp 393–401
4. Reshma R, Sowmya V, Soman KP (2018) Effect of Legendre-Fenchel denoising and SVD-based dimensionality reduction algorithm on hyperspectral image classification. Neural Comput Appl 29(8):301–310
5. Lee H, Kwon H (2017) Going deeper with contextual CNN for hyperspectral image classification. IEEE Trans Image Process 26(10)
6. Srivatsa S, Sowmya V, Soman KP (2018) Least square based fast denoising approach to hyperspectral imagery. AISC, vol 518
7. Bousmalis K, Silberman N, Dohan D, Erhan D, Krishnan D (2017) Unsupervised pixel-level domain adaptation with generative adversarial networks. CVPR
8. Tzeng E, Hoffman J, Saenko K, Darrell T (2017) Adversarial discriminative domain adaptation. CVPR
9. Salimans T, Goodfellow I, Zaremba W, Cheung V, Radford A, Chen X (2016) Improved techniques for training gans. NIPS
10. Raina R, Battle A, Lee H, Packer B, Ng AY (2007) Self-taught learning: transfer learning from unlabeled data. In: Conference on machine learning
11. Long M, Wang J, Jordan MI (2017) Deep transfer learning with joint adaptation networks. ICML
12. Pan SJ, Tsang IW, Kwok JT, Yang Q (2011) Domain adaptation via transfer component analysis. IEEE Trans Neural Netw 22(2)
13. Damodaran BB, Kellenberger B, Flamary R, Tuia D, Courty N (2018) DeepJDOT: Deep Joint distribution optimal transport for unsupervised domain adaptation. http://arxiv.org/abs/1803.10081v1 arXiv:1803.10081v1
14. Yan H, Ding Y, Li P, Wang Q, Xu Y, Zuo W (2017) Mind the class weight bias: weighted maximum mean discrepancy for unsupervised domain adaptation. CVPR
15. Panareda Busto P, Gall J (2017) Open set domain adptation. In: IEEE international conference on computer vision. ArXiv1804.10427
16. Bendale A, Boult TE (2016) Towards open set deep networks, CVPR
17. Saito K, Yamamoto S, Ushiku Y, Harada T (2018) Open set domain adaptation by backpropogation, ArXiv :1804.10427v2[cs.CV]
18. Ganin Y, Lempitsky V (2015) Unsupervised domain adaptation by backpropagation, ICML
19. Hyperspectral image dataset available at http://www.ehu.eus/ccwintco/index.php/Hyperspectral_Remote_Sensing_Scenes

AHP-FVIKOR Based Access Network Selection in Vehicular Communications

C. Suganthi Evangeline and Vinoth Babu Kumaravelu

Abstract Providing seamless connectivity is the major challenge in vehicular communication. The vehicles need to perform vertical handover in order to select the best target network. To identify the target network which satisfy the quality of service (QoS) demands is the need of the hour. To provide solution for this issue, a two stage fuzzy logic based target network selection is proposed where factor for handover estimation is carried out in first stage and fuzzy VIKOR based target network selection is developed. Through simulations, the ranking method is compared with other schemes.

Keywords Seamless connectivity · Fuzzy-VIKOR (FVIKOR) · Target network selection (TNS) · Quality of service (QoS) · Vehicular network (VANET) · Handover estimation

1 Introduction

Vehicular Adhoc Networks provide the feature of communicating with other vehicles and also with the infrastructure [1]. The process of communication includes the exchange of messages, toll services, emergency messages, and also infotainment services. To provide better quality of service the vehicle should be Always Best Connected (ABC) with the network [2]. The network providing the services need not be homogeneous but also heterogeneous involving Universal Mobile Telecommunications System (UMTS), Worldwide Interoperability for Microwave Access (WiMAX), Wireless Fidelity (Wi-Fi). Several network selection approaches are available to select the appropriate network during handover process. Quality of service (QoS) always accompanied with the network selection process, which follows three phases like (i) Handoff Initiation, (ii) Network Selection and (iii) Handoff Execution

C. S. Evangeline
Karunya Institute of Technology and Sciences, Coimbatore, India

C. S. Evangeline (✉) · V. B. Kumaravelu
Vellore Institute of Technology, Vellore, India
e-mail: evangelineme4@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_79

phase. As mentioned above, if the handover happens within the same network it is referred as horizontal handover and when it happens between two different networks it is referred as vertical handover.

To have seamless connectivity the heterogeneous network should include the features of third-generation (3G) and fourth-generation (4G). 3G networks such as UMTS and Code Division Multiple Access (CDMA) 2000 have wide coverage but lack in terms of monetary costs and bandwidth meanwhile IEEE 802.16 WiMAX has the feature of providing real-time data in Wireless Metropolitan Area Network (WMAN). The main aim of this paper is to find the exact moment to initiate handover and carry out the network selection process using fuzzy-VIKOR (FVIKOR), which enables the user to select for better QoS in the heterogeneous environment.

2 Related Works

In [3], network selection algorithm based on Simple Additive Weighting (SAW) method is presented in which normalized weight values for all networks and criteria are simply added to produce the best utility factor. The paper [4] analyzed the impacts of user velocity and traffic load on the node (mobile, vehicle) switching from one network to another in heterogeneous wireless network. In [5] Fuzzy-Techniques for Order Preference by Similarity to Ideal Solution (Fuzzy-TOPSIS) provide a QoS aware vertical handover decision by considering bandwidth, jitter, delay, and bit error rate. QoS enabled vertical handover decision is presented in [6], where weights are assigned using Analytical Hierarchical Process (AHP). The comparative analysis of various MADM approaches such as SAW, Grey Relational Analysis (GRA), Multiplicative Exponent Weighting (MEW), VIseKriterijumska Optimizacija I Kompromisno Resenje (VIKOR), and TOPSIS has been presented in [7]. Fuzzy VIKOR (FVIKOR) was presented in [6] which aims to use parallel fuzzy logic controllers (FLC) with minimum number of rules to estimate necessity of handover and select the target network.

Data is disseminated using clustering method [8] efficiently which improves the QoS in VANET applications. The decision process for vertical handover in vehicular adhoc network was proposed in [9], which gives insight about the probability of unnecessary handover and handover failure probability rate with respect to vehicle speed.

3 Proposed Method

The vehicular communication considered is of heterogeneous type as shown in Fig. 1, and handover happening in such scenario is called as vertical handover. For the proposed work, the network considered are UMTS, WiMAX, and Wi-Fi. The proposed algorithm represented in Fig. 2, works in two stages. The stage 1, deals with the

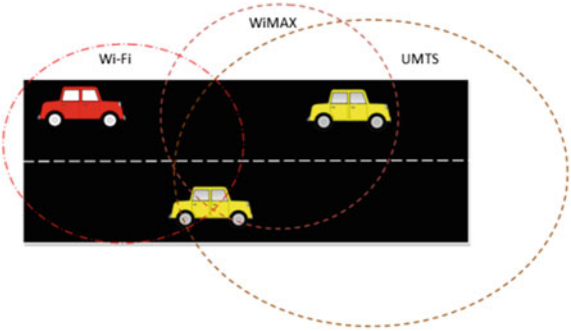
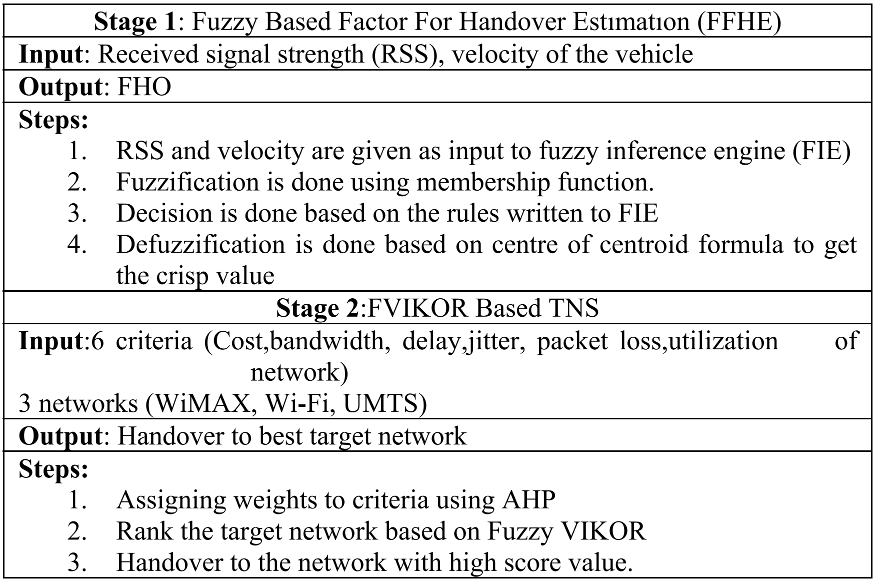


Fig. 1 Heterogeneous vehicular environment



Stage 1: Fuzzy Based Factor For Handover Estımatıon (FFHE)

Input: Received signal strength (RSS), velocity of the vehicle

Output: FHO

Steps:

1. RSS and velocity are given as input to fuzzy inference engine (FIE)
2. Fuzzification is done using membership function.
3. Decision is done based on the rules written to FIE
4. Defuzzification is done based on centre of centroid formula to get the crisp value

Stage 2:FVIKOR Based TNS

Input:6 criteria (Cost,bandwidth, delay,jitter, packet loss,utilization of network)
3 networks (WiMAX, Wi-Fi, UMTS)

Output: Handover to best target network

Steps:

1. Assigning weights to criteria using AHP
2. Rank the target network based on Fuzzy VIKOR
3. Handover to the network with high score value.

Fig. 2 Algorithm for the proposed work

factor for handover (FHO) which initiates the need for performing handover. The vehicle with high FHO is allowed to execute next stage. In stage 2, it deals with the target network selection (TNS) based on Fuzzy VIKOR ranking.

3.1 FFHE

Many handover initiation algorithm deals only with RSS [10]. The values are sampled in each time instant to trigger the handover in heterogeneous environment. For

Fig. 3 FIE for proposed work

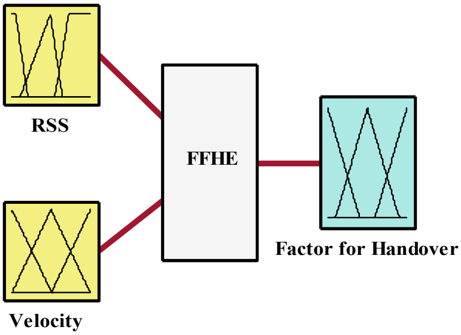
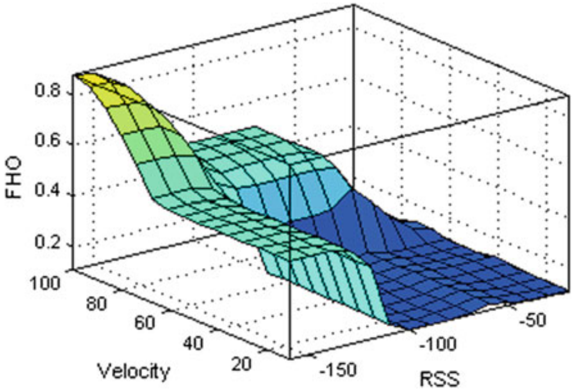


Fig. 4 Surface plot RSS versus velocity against FHO



vehicular communications, in addition to RSS the other main factor which influences mobility is the speed of the vehicle, i.e., Velocity of the vehicle. FIE for proposed work is represented in Fig. 3, surface plot RSS versus velocity against FHO is depicted in Fig. 4 and the rules defined for FIE is mentioned in Fig. 5.

3.2 Weight Assignment Using AHP

AHP stands for Analytic Hierarchy Process. It is a method to support multi-criteria decision-making and was originally developed by Saaty [11]. AHP derives ratio scales from paired comparisons of criteria and allows for some small inconsistencies in judgments. The steps involved in weight assignment in AHP are discussed below:

Step 1. Develop the weights for the criteria by

- developing a single pair-wise comparison matrix for the criteria;
- multiplying the values in each row together and calculating the root of said product;
- normalizing the aforementioned nth root of products to get the appropriate weights;
- calculating and checking the Consistency Ratio (CR).

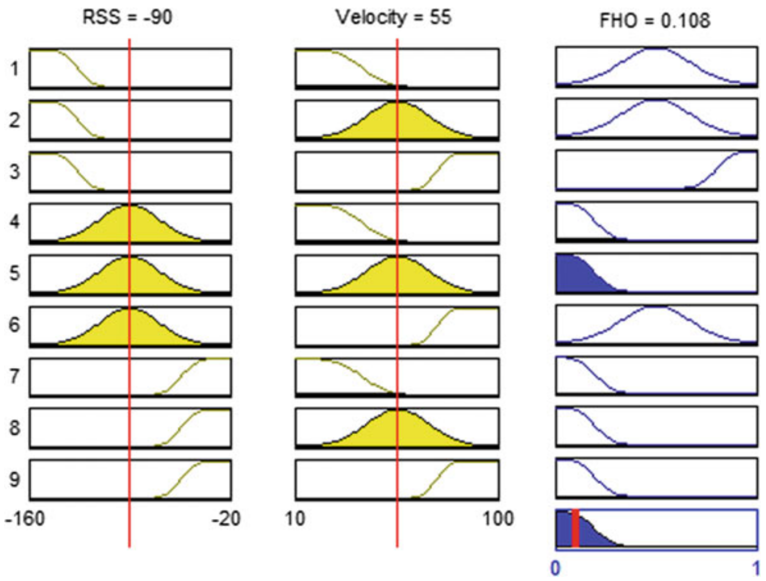


Fig. 5 Rules defined for FIE

Step 2. Develop the ratings for each decision alternative for each criterion by

- developing a pair-wise comparison matrix for each criterion, with each matrix containing the pair-wise comparisons of the performance of decision alternatives on each criterion;
- multiplying the values in each row together and calculating the nth root of said product;
- normalizing the aforementioned nth root of product values to get the corresponding ratings;
- calculating and checking the Consistency Ratio (CR).

Step 3. Calculate the weighted average rating for each decision alternative. Choose the one with the highest score.

3.3 FVIKOR-Based Target Network Selection

Assume there exists m alternative such as $A_1, A_2, A_3 \ldots A_m$ and n criteria. The rating of jth aspect is denoted by $f_{ij,}$ i.e., f_{ij} is the value of jth criterion function for the alternative A_i.

Step 1: Evaluation Matrix formation

$$D = \begin{bmatrix} \tilde{x}_{11} & \cdots & \tilde{x}_{1n} \\ \vdots & \ddots & \vdots \\ \tilde{x}_{m1} & \cdots & \tilde{x}_{mn} \end{bmatrix} \tag{1}$$

where $\widetilde{x_{ij}}$ is the performance alternative j; $j = 1, 2, 3\ldots n$ in terms of criteria i; $i = 1, 2, 3\ldots m$.

Step 2: Normalized fuzzy performance decision matrix construction

$$F = \begin{bmatrix} \tilde{f}_{11} & \cdots & f_{1n} \\ \vdots & \ddots & \vdots \\ \tilde{f}_{m1} & \cdots & \tilde{f}_{mn} \end{bmatrix} \tag{2}$$

where $\widetilde{f_{ij}} = \frac{\widetilde{x_{ij}}}{\sum_{j=1}^{m} \widetilde{x_{ij}}}$

Step 3: Determination of fuzzy best value and fuzzy worst value

$$\widetilde{f_j^*} = \max\widetilde{x_{ij}}\forall i \tag{3}$$

$$\widetilde{f_J^*} = \min\widetilde{x_{ij}}\forall i \tag{4}$$

Step 4: Computation of $\widetilde{S_i}$, $\widetilde{R_i}$

$$\widetilde{S_i} = \sum_{j=1}^{n} \frac{\widetilde{w_j}\left(\widetilde{f_j^*} - \widetilde{x_{ij}}\right)}{\widetilde{f_j^*} - \widetilde{f_j^-}} \tag{5}$$

$$\widetilde{R_i} = \max \frac{\widetilde{w_j}\left(\widetilde{f_j^*} - \widetilde{x_{ij}}\right)}{\widetilde{f_j^*} - \widetilde{f_j^-}} \forall j = 1, 2, \ldots n \tag{6}$$

Step 5: Calculation of $\widetilde{Q_i}$ value

$$\widetilde{Q_i} = v\left(\frac{\widetilde{S_i} - \widetilde{S^-}}{\widetilde{S^+} - \widetilde{S^-}}\right) + (1 - v)\left(\frac{\widetilde{R_i} - \widetilde{R^-}}{\widetilde{R^+} - \widetilde{R^-}}\right) \tag{7}$$

where

$$\widetilde{S^+} = \max_i \widetilde{S_\iota}, \widetilde{R^+} = \max_i \widetilde{R_\iota}$$

$$\widetilde{S^-} = \min_i \widetilde{S_\iota}, \widetilde{R^-} = \min_i \widetilde{R_\iota^i}$$

from [12], v is the weight of VIKOR index value = 0.5

Step 6: Sorting

The values of $\widetilde{S}_i$, $\widetilde{R}_i$,$\widetilde{Q}_i$ are sorting according to descending order. The maximum value of $\widetilde{Q}_i$ is based on merit points and it is denoted by $A^{(1)}$. The second alternative is denoted by $A^{(2)}$.

Step 7: Ranking

The alternative of maximum value of $\widetilde{Q}_i$ is said to be the best alternative.

4 Results and Discussions

In order to validate the proposed method, the numerical calculations are done. The weights for all criteria is assigned using AHP and followed by the ranking process using FIKOR. By adopting the steps given in Sect. 3.2, Table 1 is constructed. Table 2 shows normalized fuzzy decision matrix.

Table 3 is constructed by performing calculations as per the Sect. 3.3 and the ranking order in Table 4 is calculated by FVIKOR with maximum Q value. As per the assumption the network A_3-UMTS is considered to the best alternative.

The aim to find appropriate target network with less number of handovers and decision delay. By comparing FVIKOR, VIKOR, SAW, TOPSIS, and FSAW in terms of executable handovers and decision delay, the proposed method with FVIKOR

Table 1 Calculated weights for criteria

	$C1$	$C2$	$C3$	$C4$	$C5$	$C6$
weights	0.05	0.365	0.154	0.221	0.082	0.128

Table 2 Normalised fuzzy decision matrix

Criteria	A_1	A_2	A_3
$C1$	(0.33,1.33,3)	0.33,1.33,3)	(7.66,9.33,10)
$C2$	(1,2.33,4.33)	(0.33,1.33,3)	(6.33,8,9.66)
$C3$	(8.33,9.66,10)	(4.33,6.33,9.33)	0.33,1.33,3)
$C4$	(5.66,7.66,9.66)	(0.33,1.66,3.66)	(0.33,1.33,3)
$C5$	(6.33,8,9.66)	(6.33,8,9.66)	(4.33,6.33,8.66)
$C6$	(7,8.66,9.66)	(0.33,1.33,3)	(4.33,6.33,8)

Table 3 Computation of S, R and Q value

	A_1	A_2	A_3
Si	[0.7827 1.2562 1.8293]	[0.7284 0.9703 1.1869]	[0.7554 1.0931 1.4733]
Ri	[0.5904 0.7338 0.8181]	[0.7000 0.8700 0.9700]	[0.7000 0.8700 0.9700]
Qi	[0.1969 0.4702 0.5000]	[0.5000 0.5000 0.5000]	[0.5978 0.7021 0.7229]

Table 4 Ranking of the network

	A_1	A_2	A_3
Si	1.2894	0.961	1.107
Ri	0.714	0.846	0.846
Qi	0.389	0.5	0.6742
Rank	3	2	1

performs well in handover reduction as shown in Fig. 6 and gives less decision delay when compared to TOPSIS as shown in Fig. 7.

The ranking methods combined with fuzzy adapts with the changing environment and performs well when compared to the classical approach. The overhead in calculation provides slight higher delay when compared to SAW. But on considered the criteria involved for deciding the target network, FVIKOR is the optimal solution among various MADM schemes.

Fig. 6 Number of handover

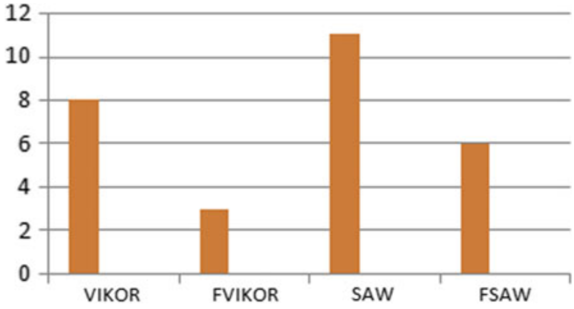
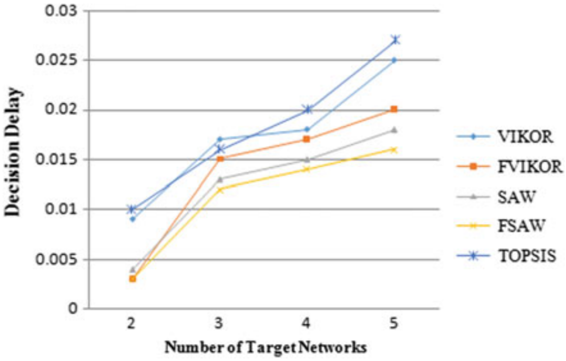


Fig. 7 Decision delay for different target networks



References

1. Miller J (2008) Vehicle-to-vehicle-to-infrastructure (V2V2I) intelligent transportation system architecture. In: IEEE intelligent vehicles symposium, IEEE, pp 715–720
2. Fodor G, Furuskar A, Lundsjo J (2004) On access selection techniques in always best connected networks. In: ITC specialist seminar on performance evaluation of wireless and mobile systems, pp 89–100
3. Afshari A, Mojahed M, Yusuff RM (2010) Simple additive weighting approach to personnel selection problem. Int J Innov, Manag Technol 1(5):511
4. Hasswa A, Nasser N, Hassanein H (2005) Generic vertical handoff decision function for heterogeneous wireless. In: Second IFIP international conference on wireless and optical communications networks, IEEE, pp 239–243
5. Vasu K, Maheshwari S, Mahapatra S, Kumar CS (2011) QoS aware fuzzy rule based vertical handoff decision algorithm for wireless heterogeneous networks. In: National conference on communications, IEEE, pp 1–5
6. Zineb AB, Ayadi M, Tabbane S (2017) An enhanced vertical handover based on fuzzy inference MADM approach for heterogeneous networks. Arabian J Sci Eng 42(8):3263–3274
7. Stevens-Navarro E, Martinez-Morales JD, Pineda-Rico U (2012) Evaluation of vertical handoff decision algorithms based on madm methods for heterogeneous wireless networks. J Appl Res Technol 10(4):534–548
8. Evangeline CS, Appu S (2017) An efficient data transmission in VANET using clustering method. Int J Electron Telecommun 63(3):309–313
9. Evangeline CS, Kumaravelu VB(2017) Decision process for vertical handover in vehicular adhoc networks. In: International conference on microelectronic devices, circuits and systems (ICMDCS), IEEE, pp 1–5
10. Mohanty S, Akyildiz IF (2006) A cross-layer (layer 2 + 3) handoff management protocol for next-generation wireless systems. IEEE Trans Mob Comput 5(10):1347–1360
11. Saaty TL (2005) Analytic hierarchy process. Encyclopedia of Biostatistics 1
12. Musani S, Jemain AA (2015) Ranking schools' academic performance using a fuzzy VIKOR. J Phys: Conf Ser 622(1):012036). IOP Publishing

Measuring Web Content Credibility Using Predictive Models

R. Manjula and M. S. Vijaya

Abstract Web content credibility is a measure of believable and trustworthy of the web content that is perceived. Content can turn out to be unreliable if it is not up-to-date and it is not measured for quality or accuracy and therefore, web content credibility is important for the individuals to access the content or information. The analysis of content credibility is an important and challenging task as the content credibility is expressed on essential factors. This paper focus on building predictive models to discover and evaluate credibility of a web page content through machine learning technique. A corpus of 300 web page contents have been developed and the factors like Readability, Freshness, Duplicate Content are defined and captured to model the credibility of web content. Two different labeling such as binary labeling and numeric labeling are used for defining credibility. In case of binary labeling, the high and low credibility of web content are represented by 1 and 0, respectively, whereas in case of numeric labeling five-point scale rating is used to mark the content credibility. Accordingly, two independent datasets have been developed. Different regression algorithms such as Linear Regression, Logistic Regression, Support Vector Regression (SVR) are employed for building the predictive models. Various experiments have been carried out using two different datasets and the performance analysis shows that the Logistic Regression model outperforms well when compared to other prediction algorithms.

Keywords Web content credibility evaluation · Machine learning · Prediction · Regression

R. Manjula (✉) · M. S. Vijaya
PSGR Krishnammal College for Women, Coimbatore, India
e-mail: manjulacbe.r@gmail.com

M. S. Vijaya
e-mail: msvijaya@psgrkcw.ac.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_80

1 Introduction

Web content credibility is expressed as the believability of web content. Web content credibility is created with two dimensions: trustworthiness and expertise. When a web page conveys both these qualities, people will find, it is a credible content. When it lacks one of these qualities, due to misrepresentation, inaccuracy, credibility will suffer [1]. Content credibility is being utilized in different domain like economy, healthy life-style, politics, personal finance, and entertainment. A credible website can gather huge benefits on to the website and the corporate. People frequently choose to respond to a significant message based on their perception of the communicator [2].

Having a stylish, specialized looking webpage, offer credibility to the contents. The single more crucial attribute of efficient content is credibility. There are four types of web credibility such as Presumed credibility, Reputed credibility, Surface credibility, and Earned Credibility. Presumed credibility describes the general assumptions about the product brand. Reputed credibility refers to the believed third party reference about the brand. Surface credibility expresses how much a perceiver believes something based on simple inspection. Earned credibility states that the personal experience of typographical text. Well-written web content keeps the customers involved, and inspires them to explore their web content [3].

Web content credibility involves the abilities and competencies needed for reading, writing and participating content on the web. Credibility is the single most eminent attribute of great marketing content. Effective content must also be applicable and precious. It’s also clear that lack of trust is weakening the impact of content. In a modern survey of technology buyers by TrustRadius, survey participants are asked to rate the helpfulness and trustworthiness of source of data used in buying decisions. Credible content is authoritative [4].

To solve the problem of predicting web content credibility numerous computational techniques are accepted in the existing research. Machine learning utilizes statistical techniques to realize and improve the performance of the predictive models. Hence, it is proposed in this work to develop an accurate predictive model by learning various influencing parameters through supervised learning.

2 Literature Survey

Various research work had examined and explored on understanding the factors that had an impact on credibility evaluations. In 2017, Michal Kakol et al., proposed “understanding and predicting web content credibility using content credibility corpus”. The factors were based on empirical data. The content credibility corpus (C3) dataset was used from a massive crowdsourced web credibility assessment. The factors such as web media type, advertising, news source, official page, etc., were used to attain a high level of quality. Random forest approach was used to indicate a comprehensive set of credibility evaluation criteria [2].

In 2001, Fogg et al. concentrated on understanding the factors that had an impact on credibility evaluations and spent two approaches for regulating credibility evaluation factors. The first was a declarative approach, where respondents were requested to evaluate credibility and precisely suggest which factor from a list was influencing their decision. In 2003, Fogg et al. produced the second approach, the manual coding of comments left by defendants evaluated credibility by two coders. Unsupervised machine learning and NLP techniques was used from the content credibility corpus (C3) dataset [5].

In 2013, Olteanu et al. proposed "web credibility: feature exploration and credibility prediction". The research work automatically assesses web credibility investigated through various characteristic of webpages. The features were detected from textual content, link structure, webpages design, as well as their social popularity learned from popular social media sites. The random baseline approach for regression was concerned for the real dataset-based experiment under 75% accuracy for classification and 53% of mean absolute error for regression [6].

In 2010, Joo Chung et al., proposed "An anatomy of the credibility of online newspapers". The research work exposed the primary components of credibility of three types of online newspaper and the variance of credibility of news by that type. The credibility scales were determined using seven-point likert-type scales and mean was computed and the scale was explored for the similarities. The factors such as expertise, trustworthiness, and attractiveness were used to show the significant difference between online newspapers [7].

In 2014, Wawer et al. utilized natural language processing methods together with machine learning to look for specific content terms that are predictive of credibility. By this method, they found expected terms, such as energy, research, safety, security, department, fed and gov. linguistic and social features was used based on machine learning methods by the recognized trust level. Content-specific language features were applied that greatly had enhanced the accuracy of credibility predictions. The content organization factor was approximated by the analyzed CSS of the webpage. The factor language quality was approximated using NLP techniques [8].

The factors defining the web content credibility are highly imperative in building accurate prediction model through machine learning [9]. The existing research work focused on prediction of credibility using factors like web media type, advertising, news source, sales offer and objectivity of web page content. But these factors will not contribute in controlling the content credibility [10]. It was detected that the factors like readability, authority, understandability, accessibility, popularity, broken links, freshness, page rank and duplicate content are also needed for evaluating the web content credibility [11]. These factors can be taken and used as evaluation criteria for web content credibility evaluation appropriate to ordinary web content for fine-tuned credibility assessments [12]. Similarly, the quantitative predictive model was built based on content credibility corpus dataset and it has the lower correlation coefficient [13]. Hence, it is proposed in this work to build accurate web content credibility prediction model by capturing the above efficient factors using regression [14]. Several regression methods like linear regression, logistic regression have been applied to boost up the correlation coefficient between the factors [15, 16].

3 Methodology

The main focus of this work is to build an efficient predictive model to evaluate the web content credibility based on leading factors. The bare bones of the proposed methodology involve different phases such as data collection, feature extraction, and building models using regression algorithms such as linear regression, logistic regression, and support vector regression. Various components of proposed methodology are depicted in Fig. 1 and explained in the following section.

3.1 Data Collection

The corpus of 300 web pages have been selected from websites related to different domain such as economy, healthy life-style, politics, personal finance, and entertainment. The contents taken from Economy domain comprised of information about the production and consumption of goods and services. Web page contents related to short- and long-term health benefits, balanced diet is collected from Healthy Life-Style domain. From webpages of politics domain, the contents are gathered based on the activities related with the growth of a country or area. Web page contents based on management of financial decisions are collected from personal finance

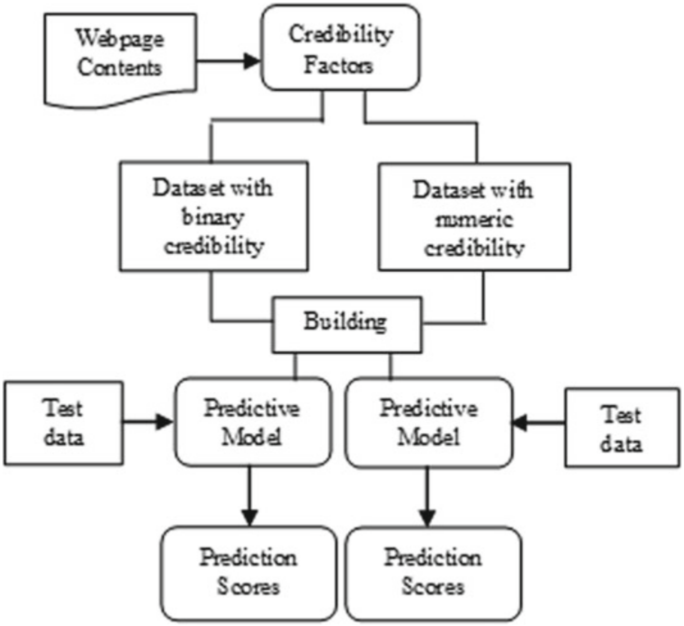


Fig. 1 Methodology for predicting and evaluating web content

domain. From entertainment domain, contents are collected based on information about games, movie, etc., Likewise, details of author, publisher of webpages, webpage updates, particulars of domain are collected from the particular pages. From each of these five domains, 60 instances have been collected and stored in the form of text files. Finally, a corpus with 300 instances have been developed.

3.2 Feature Extraction and Training Data

Feature extraction plays a prominent role for improving the performance of web content credibility. In this work, readability, authority, accessibility, understandability, popularity, freshness, broken links, page rank, and duplicate content are considered as vital factors for evaluating web content credibility. A set of nine factors is derived from each content and are described below and the dataset has been developed.

Readability. The Readability depends on the contents and presentation of the webpage. Readability is determined by the content visibility, reading speed and legibility. Higher readability improves reading effort and speed for any reader. The Flesch–Kincaid readability is used to compute the readability of contents. The value for this readability factor is computed using *R* code.

Authority. Authority of a web page controls the publisher and organization of the webpage and inspect whether it splits from the webmaster. Domain authority helps to measure the authority of a website by comparing it with other websites and it will predict the ranking of a website. A Domain Authority score ranges from one to 100, with higher scores corresponding to a greater ability to rank. The value of this authority factor is derived from nibbler tool.

Accessibility. The accessibility of the web page helps to remove barriers that prevent interaction with or access to websites. Web accessibility depends on various components working together, including web technologies, web browsers, authoring tools, and other user agents, and websites. Accessibility value is obtained from the nibbler tool.

Understandability. Content must be easy to follow and recognize for many users. For most content, understandability simply avoiding overly complex sentences, terminology and providing clear layout and design. The values from 0 to 100 provides the range of content understandability. The understandability value is estimated using *R* code.

Popularity. A webpage popularity is a tremendous way not only to build a website but also to show others how the website is good. If the website or web page is information-rich and attractive, the particular webpage will have high link popularity. The more ratings a post gets, the more reliably the ratings tell the value. The value of this factor is derived from nibbler tool.

Freshness. The freshness factor is an element of search algorithms that provides greater weight to latest content over older content for some search queries. Search engines presented the freshness factor for searches related to trending topics, recurring events (awards, sports scores, and so on) and breaking news. It provides the updates of each web page. Updates of the web page are resulting from nibbler tool.

Broken links. A broken link is a hyperlink of a website which is related to an empty or non-existent external webpage. A broken link or dead link is a link on a web page that no longer works because the website is encountering an improper URL, does not allow outside access. Broken links value is fetched from nibbler tool.

Page rank. PageRank refers to the system and the algorithmic method that Google uses to rank pages as well as the numerical value is assigned to pages as a score. PageRank is often considered to be a number between 0 and 10 (with 0 being the lowest and 10 being the highest). The value of this factor is computed using R code.

Duplicate content. Duplicate content is content that seems on the web page in more than one place. That one place is termed as a location with a unique website address (URL)—so, if the same content appears at more than one web page, duplicate content can be found. The value of this duplicate content factor is derived using *R* code.

The above nine factors are used as values of predictor variables (Xi) of regression algorithms. In this work, the credibility of web content is considered as the response variable (Y) for which the modeling is being done. In order to create the training dataset enabling supervised learning, the value of credibility of web content is also computed as below for each record and it is associated with the corresponding tuple.

Credibility. Credibility is said to be the quality or power of inspiring belief. The credibility value is derived using crowdsourced environment like web of trust (WOT). The binary labeling 0 is assigned to credibility if the content is not believable and 1 is assigned if the content is realistic. In case of numeric labeling 5-point scale rating is used to spot the content credibility, where the rating from 1 to 3 specifies the low credibility of content and the rating 4 and 5 represents high credibility.

Datasets. The factors derived from web page contents are used to train the prediction models using supervised learning. In this work, two separate datasets have been created, one with binary credibility labeling and another with numeric credibility labeling. Both datasets consist of 300 instances with nine dimensions. Each instance of independent variables is associated with binary credibility values and a dataset Binary Credibility Dataset (BCD) is created. Similarly, second dataset named Numeric Credibility Dataset (NCD) is developed by adding numeric credibility values to all the 300 tuples.

4 Experiments and Results

The predictive models for web content credibility have been generated by implementing the regression algorithms using python library in scikit-learn environment. Scikit-learn perhaps the most appropriate library for machine learning in Python. The real-time data has been collected, the content credibility factors are identified and derived. Two separate datasets namely BCD and NCD have been created to show the variations of binary and numeric credibility values of web page content. These two datasets are employed for implementing the models.

In these experiments, prediction algorithms like Linear Regression, Logistic Regression, Support Vector Regression have been employed to build the predictive models. The performance of these models is evaluated using 10-fold cross-validation based on correlation coefficient, mean squared error, root mean squared error and mean absolute error. Correlation coefficient is utilized as a primary performance measure for predicting content credibility values range from −1 to +1. A correlation coefficient of 0 means that there is no relationship and +1 indicates a perfect positive correlation. Mean squared error is said to be the average of the squared error and is used as the loss function for least square regression. RMSE is an absolute measure of fit. Mean absolute error is a measure of difference between continuous variables. MAE is the model evaluation metric and is the mean of the absolute values of each prediction error on all instance of the test dataset. The goodness of fit is evaluated using these measures.

The web content credibility model based on NCD dataset is built using Linear Regression and Support Vector Regression as the value of response variable is a continuous-valued function in these models. The Logistic Regression algorithm is implemented to create predictive model using BCD dataset since response variable is binary in logistic regression. The performance of these regression-based credibility prediction models is measured using metrics such as correlation coefficient, mean squared error, root mean squared error and mean absolute error and are tabulated (Tables 1, 2 and 3).

Comparative analysis. The performance results of the above three predictive models are compared to their metrics. From the comparative analysis, it is detected that the Logistic Regression attains highest result for content credibility prediction model than Linear Regression and Support Vector Regression in the minimal learning time. The Logistic Regression reaches the correlation coefficient of 0.896 and Linear Regression accomplishes the correlation 0.875 and the correlation of 0.816 is gained

Table 1 Predictive performance of linear regression using NCD dataset

Measures	Values
Correlation coefficient	0.875
Mean squared error (MSE)	0.285
Root mean squared error (RMSE)	0.533
Mean absolute error (MAE)	0.314

Table 2 Predictive performance of support vector regression using NCD dataset

Measures	Values
Correlation coefficient	0.816
Mean squared error (MSE)	0.275
Root mean squared error (RMSE)	0.524
Mean absolute error (MAE)	0.307

Table 3 Predictive performance of logistic regression using BCD dataset

Measures	Values
Correlation coefficient	0.896
Mean squared error (MSE)	0.270
Root mean squared error (RMSE)	0.519
Mean absolute error (MAE)	0.301

by Support Vector Regression. The error rate is minimized in Logistic Regression when compared to other two algorithms so the reliability of the system is improved. Hence, it is concluded that Logistic Regression is appropriate than other algorithms for evaluating the web content credibility and the comparative results are presented in Table 4 and illustrated in Fig. 2.

Table 4 Comparative analysis of regression algorithms

Algorithms	Correlation coefficient	Mean squared error	Root mean squared error	Mean absolute error
Logistic regression	0.896	0.270	0.519	0.301
Linear regression	0.875	0.285	0.533	0.314
Support vector regression	0.816	0.275	0.524	0.307

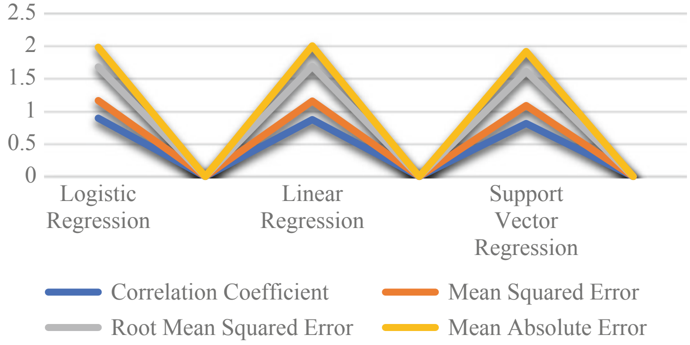


Fig. 2 Comparison of prediction algorithms

5 Conclusion

This paper demonstrates the modeling of web content credibility using machine learning techniques. The content credibility factors are recognized and derived by collecting the real-time data. Two distinct datasets have been created for the variations of binary and numeric credibility values of web page content. A predictive model is designed and built for web content credibility evaluation based on a web content dataset using supervised learning algorithms such as Linear Regression, Logistic Regression, and Support Vector Regression. The performance of credibility prediction model is measured using different metrics such as correlation coefficient, mean squared error, root mean squared error, and mean absolute error. Through the experiment, it is observed that the Logistic Regression model is best fitted for predicting the web content credibility. This work can be further extended by adding more web content instances and dimensions and repeating the experiment with other advanced technique.

References

1. Wierzbicki A, Adamska P, Abramczuk K, Papaioannou T, Aberer K, Rejmund E (2014) Studying web content credibility by social simulation, June 2014
2. Kakol M, Nielek R, Wierzbicki A (2017) Understanding and predicting web content credibility using the content credibility corpus. Elsevier
3. Abdulla RA, Garrison B, Salwen M, Driscoll P, Casey D (2014) The credibility of newspapers, television news, and online news
4. https://mozilla.github.io/content/web-lit-whitepaper/
5. Fogg BJ, Marshall J, Laraki O, Osipovich A, Varma C, Fang N, Paul J, Rangnekar A, Shon J, Swani P, Treinen M (2001) What makes web sites credible? A report on a large quantitative study. In: Proceedings of the SIGCHI conference on human factors in computing systems. ACM
6. Olteanu A, Peshterliev S, Liu X, Aberer K (2013) Web credibility: features exploration and credibility prediction. In: European conference on information retrieval. Springer, pp 557–568
7. Joo Chung C, Kim H, Hyun Kim J (2010) An anatomy of the credibility of online newspapers
8. Wawer A, Nielek R, Wierzbicki A (2014) Predicting webpage credibility using linguistic features
9. Aladhadh S, Zhang X, Sanderson M (2014) Tweet author location impacts on tweet credibility Nov 2014
10. Tumasjan A, Sprenger TO, Sandner PG, Welpe IM (2010) Predicting elections with Twitter: what 140 characters reveal about political sentiment
11. Carlos C, Marcelo M, Barbara P (2013) Predicting information credibility in time-sensitive social media 23(5):560–588
12. Korfiatis NT, Poulos M, Bokos G (2006) Evaluating authoritative sources using social networks: an insight from Wikipedia. Online Inf Rev 30(3):252–262
13. Liviu L Predicting product performance with social media. Inf Educ 15(2):46–56
14. Sundar SS (2008) The main model: a heuristic approach to understanding technology effects on credibility, pp 73–100
15. Sikdar S, Kang B, ODonovan J, Höllerer T, Adah S (2013) Understanding information credibility on twitter. IEEE
16. Kak S (1999) Faster web search and prediction using instantaneously trained neural networks. IEEE Intell Syst 14:79–82

Survey on Privacy-Preserving and Other Security Issues in Data Mining

K. Karthika, R. Devi Priya and S. Sathishkumar

Abstract In present day, an ever-increasing number of researches in information mining increases the seriousness about security issue. The security issues in information mining can't just be tended by limiting data integration or by reducing the utilization of information technology. So as to keep up the security of the customer in the process of data mining, different types of strategies have been proposed that are dependent on the probabilistic perturbation of information records. Information mining service requires precise information for their outcomes to be significant; however, protection concern may impact clients to give fake data. Here, we present a detailed survey on privacy and security issues on data mining by analyzing different techniques from standard publishers of the year from 2010 to 2017. Based on the techniques utilized and types of issues are analyzed and classified. Moreover, to indicate the improvement and accuracy of all the research articles is also discussed. Furthermore, the analysis is carried to find the importance of their approaches so that we can develop a new technique to solve the security threats.

Keywords Data mining · Privacy and security issues · Security threats

1 Introduction

The present-day society achieved a lot of advancements from the advanced science and its applications. It provides effective platform to convert the entire burdensome task into easy tasks. Therefore, many industries and enterprises are focusing on their service to be adopted based on advanced technologies [1]. The development of Internet of Things (IoT) had paved the way to analyze the participatory sensing (PS) where various individuals can gather and outline their information to an outsider information mining cloud administration [2]. The IoT based gadgets directs an

K. Karthika (✉) · S. Sathishkumar
Department of Information Technology, Adhiyamaan College of Engineering, Hosur, India
e-mail: karthikainfoscience@gmail.com

R. Devi Priya
Department of Information Technology, Kongu Engineering College, Erode, India

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_81

outstanding measure of information in streams from different sensors by means of everlasting communication [3]. IoT has reformed numerous fields including health services, prosperity applications, public activity, environment observing, transportation, energy, and so on. The accessibility of minimal effort unavoidable detecting gadgets has empowered IoT to develop in a regularly expanding way, thus IoT sensors had turned into an indispensable source of big information. IoT incorporates the application territories of WSN and RFID with extensional availability along the web.

IoT has numerous applications related to intelligent healthcare services that are controlled by the technical union of Wireless Body Area Network (WBAN), WSN, and mobile crowdsensing (MCS) along with distributed computers [4].

The registered and specialized devices utilized by the cyber-physical IoT empowered system create huge amounts of information. This information gives new accesses yet, in addition, various difficulties arise particularly through their social ramifications [5]. Nowadays, Cloud storage is also very popular due to its service to preserve the user data in the third-party platform. It has extraordinarily changed the manner in which individuals store their information. Not at all like conventional storing, the cloud gives gigantic capacity of storage which gives more benefits to the clients [6]. The outsourcing of users' data into the cloud doesn't concern about the storing of information and maintenance [7]. Associations and people are slanted to utilize the cloud service and takes advantages of the productive and practical nature of the cloud. Cloud services, for example, Google Safe Browsing, PhishTank, and Malwr offers blacklist of known vindictive URLs, domain, emails and so on [8]. The ceaselessly expanding measures of information make their security a challenging and essential task especially when the information are exceptionally dimensional. Numerous information holders need to distribute their miniaturized scale of information for different purposes so that does not uncover the identity of individual [9].

In addition, some protection-sensitive system, for example, money-related and medicinal services does not share their information freely because of the diverse security strategies, yet joint information handling was unavoidable. Uncovering the patients' records is not just untrustworthy yet in addition unlawful as per the Health Insurance Portability and Accountability Act [10]. The profound learning by clinical and bio-medical analysts on their neighborhood data set overfit the learning model and brings about wrong outcomes amid the deduction stage. For this situation, secrecy and security confinements fundamentally lessen utility [11]. Besides, various new methodologies have been advanced so as to control quickly developing spam, malware, and DDoS assaults in the Internet to keep client's information and to accomplish full reliability from the customers [12, 13]. In this manner, these distinctive kinds of trust and notoriety instrument were proposed to control various undesirable traffic delays, for example, email spam. All in all, security protection concerns are identified with verification, information getting to, information encryption and information distributing [14, 15].

2 Literature Survey

2.1 Survey of Security Issues in Data Mining

Data mining is characterized as the way toward digging for certain unidentified and conceivably fundamental data from dreadfully tremendous databases by effective information disclosure systems. The huge open strategy tensions are the protection and security of client data and there are getting increased enthusiasm by the government official and controller, protection advocates, and the media. In this article we consider key online protection, security problems, and concern the job of self-direction and client in protection and security assurances, information insurance laws, administrative patterns and the perspective for security and secure enactment. Normally such a procedure creates new suspicion measurements, identify new attack designs and lift information security issues. Most latest advancements in data innovations has empowered collection and preparing immense measure of user data such as criminals database, web-based shopping, online managing of account, credit and therapeutic history, driving records, and the legislature concerned information [16].

Information mining is depicted as a procedure of find or removing intriguing learning from immense measures of information put away in a few information sources, for example, record frameworks, databases, information stockrooms, and so on. There are a few information mining instruments used to anticipate and bring up patterns and practices and enables companies to make proactive, learning-driven choices. At most and mid-run organizations utilizes incredible frameworks for gathering information and overseeing it in substantial databases. Anyway the bottleneck of transforming this information into your triumph is the hardest assignment of removing learning about the framework that you think about from the gathered information. Information mining and its procedures can be very valuable in numerous regions, for example, industry, business, government, instruction, and agribusiness, medicinal services, etc. To break down huge databases utilizing information-digging apparatuses for conveying answers to questions, for example, Which customers destined to react to my next limited-time mailing, and why? Information mining has numerous favorable circumstances yet at the same time it has disadvantages, for example, part of security issues and hazards. The reason for this paper is to talk about Role of information mining, its application and different difficulties and issues identified with it [17].

For each economy, industry, association, business work and individual, data has turned into an essential part. Big Data is needed to distinguish the datasets and estimate the capacity of database programming devices to store, overview and examine. Thus, Big Data incorporates versatility, stockpiling bottleneck, commotion collection, fake connection, and estimation mistakes and furthermore presents remarkable computational and factual difficulties. These issues are identified and new computational and measurable methods are adopted. This paper shows the survey about the big data and mining with the issues and challenges. It also discuss about few techniques to manage huge data [18].

Late development, fame, and improvement of data mining share the perilous risk on the security of person's data. Privacy protection and data mining (PPDM) is a developing exploration theme in information mining and has been widely examined in late years. PPDM manage the information to perform data mining estimation properly without degrading the privacy of delicate information presented in the data. Ongoing research in PPDM principally center around how to decrease the protection issue caused by data mining, while maintaining the nature of undesirable exposure of data may occur during the time utilized on data gathering, distributing and conveying. In this article we chiefly center the security problem recognized during data mining from a wide point of view and explore diverse methods that can avoid delicate data. We recognize four kinds of users associated with the application of data mining. They are data supplier, data gatherer, data excavator, and leader. For each client the system examines the protection issue and strategies that are received to avert delicate information. The rudiments of related research points are discussed to present best survey and presented some fundamental abstraction on future research bearings. We additionally proposed some survey based on diversion in hypothetical methodologies for investigating the connections among different users in data mining which has their own valuation on the touchy information. By classifying the duties of different users concerning the security of sensitive data we need to give some valuable bits of information in the investigation of PPDM [19].

2.2 Survey on K-Anonymization Techniques

PPDM techniques have been classified into various types such as Anonymization based PPDM, perturbation based PPDM, and Cryptography based PPDM.

Exchange information record distinctive data about people, including their analysis and buys, and are progressively distributed to help substantial scale and minimal effort thinks about in different spaces, for example, drug and showcasing. Be that as it may, the dispersal of exchange information may prompt security ruptures, as it enables an assailant to connect a person's record to their personality. As of late, there are a few methodologies have been suggested that anonymous information by killing certain qualities in a person's record or by supplanting them with regular qualities, yet they frequently produce information of restricted value due to embrace esteem change procedures that don't ensure information utility in planned applications and target estimates that may prompt over the top information mutilation. In this review, we propose a novel methodology for anonymizing information to fulfill information distributors' utility prerequisites and causes uninformed misfortune. To accomplish this, we present a definite data misfortune measure and a successful anonymization calculation that investigates a huge piece of the issue space. A broad exploratory examination, utilizing clickstream, and restorative information, exhibits that our methodology permits commonly more exact question replying than the best in class techniques, while it is practically identical to them as far as proficiency [13].

Prior to the production of delicate information, the anonymization of inquiry logs is a vital procedure that should be performed earlier. This guarantees the namelessness of the clients in the record, an issue that has been as of now found in discharged logs from surely understood organizations. This study utilizes small scale conglomeration to presents the anonymization of question record. Our proposition guarantees the *k*-namelessness of the clients in the question log while saving its utility. We demonstrate the security and utility accomplished, and furthermore provide the analysis of our proposition in real inquiry record, just as giving assessment to the utilization of data in data mining forms based on grouping [20].

Anonymization of static information has been incredible research as of late. There are two normal innovations for semi-identifier's anonymizations are speculation and concealment. Anonymization of information contrast from the anonymization of static information dependent on the characteristics of information streams, for example, potential interminability and high dynamicity. For anonymizing information streams, static information anonymization strategies can't be straightforwardly connected. In this review, grouping based novel *k*-anonymization approach is proposed. The new methodology examines a stream in one swing to perceive and reuse the groups, so as to accelerate the anonymization procedure and decrease the data misfortune and fulfills the *k*-obscurity guideline. It considers the time limitations on tuple distribution and bunch reuse, which are explicit to information streams. Besides, the methodology is improved to adjust the—decent variety standard. The analyses led on the genuine datasets demonstrate that the proposed techniques are both productive and powerful [21].

Information mining assumes an imperative job in examining the substantial measure of information gathered in this day and age. Protection Preserving Data Mining (PPDM) systems have turned out to be fundamental because of the open's rising consciousness of security and absence of trust in association. A PPDM system guarantees singular security while permitting helpful information mining. In this study, we present two novel information quality assessment procedures called EDUDS and EDUSC, novel clamor expansion method called Forest Framework and a security assessment system called SERS. Novel noise addition technique assembles a forest from dataset and preserves every one of the examples (rationale rules) of the backwoods while adding commotion to the dataset. The two frameworks, Forest Framework to its Predecessor Framework have been thought about, and another setup strategy, GADP then the correlation is finished utilizing our three assessment criteria, just as Prediction Accuracy. The proposed work demonstrates the test results and show the accomplishment of expansions to Framework and furthermore the support of our assessment criteria [22].

2.3 Data Sanitization Issue

Moreover, Fosca Giannotti et al. [11] have developed affiliation rule mining assignment inside a corporate security safeguarding structure. Here an assault display dependent on foundation information and devise a plan for protection saving redistributed mining. This plan guarantees that each changed thing is unclear as for the assailant's experience information, from in any event $k - 1$ other changed things. The extensive test is gone up against a substantial and genuine exchange database exhibit that this method is viable, versatile and ensures protection. Moreover, Jaya krushna Sahoo et al.

Sahoo et al. [23] have built up a compacted portrayal for affiliation rules having insignificant predecessor and maximal subsequent. This portrayal is produced with the assistance of high utility shut thing sets (HUCI) and their generators. Here calculations are created to produce the utility-based non-repetitive affiliation standards and strategies for reproducing all affiliation rules. Moreover, they depicted the calculations which create high utility thing sets (HUI) and high utility shut thing sets with their generators. These proposed calculations are executed utilizing both manufactured and genuine datasets. What's more, the test results show better quality in the packed portrayal of the whole standard set under the thought about system.

Li et al. [24] have built up a cloud-helped regular thing set mining arrangement, which is utilized to assemble an affiliation rule mining arrangement. These arrangements are intended for re-appropriated databases that enable numerous information proprietors to effectively share their information safely without settling on information security. This arrangements release less data about the crude information than most existing arrangements. In view of these analysis discoveries utilizing distinctive parameters and datasets, they exhibit that the run time in every one of these arrangements is just a single request higher than that in the best non-protection saving information mining calculations. The asset utilization at the information proprietor end is exceptionally low since the two information and processing work are re-appropriated to the cloud servers. Moreover, Jordi Castro and Jose A. Gonzalez [25] have introduced a substantially less expensive variation of Controlled forbidden modification (CTA) that defines a multi-objective straight improvement (LO) issue, where paired factors are pre-fixed, and the subsequent consistent issue is comprehended by lexicographic streamlining. Broad computational outcomes are accounted for utilizing both business (CPLEX and XPRESS) and open source (Clp) solvers, with either simplex or inside point techniques, on a lot of genuine examples. Most cases were effectively tackled with the LO-CTA variation in under 60 min, while a considerable lot of them are computationally pricey with the MILO-CTA detailing. The inside point technique beat simplex in this specific application.

2.4 Other Issues Based on Cryptography

Database security is imperative as it contains sharpened data. Information digging gives components to middle person portrayal of information. Protection conservation is essential because of the security viewpoints. Protection demonstrates components for enabling the information to be gotten to in verified way. Security is to shield the delicate information from information excavators with the end goal that it isn't doable to get to the touchy information from database. The significant plans to change the dataset from the first informational index are affiliation rule. An affiliation rule with cryptographic procedures has been utilized. This calculation applies on genuine informational collections to exhibit the materialness. An efficient protection conservation information mining plan with information mining irritation blended methodology and the affiliation rules with cryptography procedures, proposed in this examination work. This paper exhibits how a neural system is being connected for foreseeing the medicinal dataset and furthermore gives scope on how profound convolution neural system can be connected for therapeutic investigation [5].

Dispersed information mining has assumed a critical job in different application areas. In any case, in information mining, it is seen that there are number of protection risk in person's delicate data. We propose two conventions to address protection issue in circulate affiliation rule mining, which are safely creating worldwide affiliation administers in evenly appropriated databases. Elliptic-bend based Paillier cryptosystem is the primary convention, which helps in accomplishing the trustworthiness and validness of the messages traded among including destinations over the uncertain correspondence channel. It gives protection of individual site's data against the including destinations and an outside foe and an assailant. Notwithstanding, it influence the security of people because of the intrigue of two destinations. We incorporate Shamir's mystery sharing plan in the second convention to address the issue. It gives security by averting conniving locales and outside enemy assault. We investigate the two conventions to satisfy the protection safeguarding circulated affiliation rule mining necessities [26].

Present-day mechanical advances have started the prominence and accomplishment of cloud. This as of late created procedure is picking up a growing enthusiasm, since it gives cost-productive designs that help the transmission, stockpiling, and serious figuring of information. Be that as it may, these promising stockpiling administrations bring a few testing structure issues, for the most part because of both loss of information control and theoretical nature of mists. The principle objective of this review is to give a steady view about the two information security concerns and protection issues that are looked by customers in distributed storage situations. In this review, it investigates inquire about bearings and innovation patterns to address the assurance of redistributed information in cloud framework and furthermore brings a basic near examination of different cryptographic guard component [6].

In present-day protection saving information, mining has been a noteworthy research. The fundamental objective of this field is to secure individual data and anticipate revelation of this data amid the information mining process. There are diverse methods proposed in the field of security safeguarding information mining. Affiliation rules mining is one systems and the primary motivation behind affiliation rules mining is to conceal delicate affiliation rules. Up until now, unique calculations have been exhibited to this field so as to achieve the reason for delicate affiliation rules stowing away. Every single calculation has its very own particular capacities and techniques. This paper exhibits an electromagnetic field enhancement calculation (EFO4ARH) to conceal delicate affiliation rules. This calculation is utilized

Table 1 Overall analysis of survey

Security issues	2005–09	2010–14	2015–18
Privacy issues		[7, 16, 17, 19]	
K-anonymization		[13, 20, 21]	[22]
Data sanitization		[11]	[23–25]
Other security issues	[27]		[5, 6, 26]

to conceal the delicate affiliation administers by uses the information bending system. Two wellness capacities are utilized to achieve the arrangement with the least symptoms in this calculation and furthermore, the run time has been decreased. This calculation comprises of a strategy for leaving from neighborhood optima point and advancing toward worldwide ideal focuses. To assess the execution of the proposed calculation by doing probes both genuine world and manufactured data set. As we contrasted with the four reference calculations, the proposed calculation demonstrates a decrease in the symptoms and better protection of information quality. The execution of EFO4ARH is tried by standard deviation and means Friedman positions of blunder for standard capacities (CEC benchmarks). Likewise, concealing analyses demonstrate that our proposed calculation beats existing concealing algorithm [27].

3 Analysis and Discussion

In this section, we categorize the existing research work accordance with techniques. This analyzes, very much helpful for which algorithm was mainly utilized in the olden days and how to improve the algorithm further for our research. Here, each research works are developed different years.

Here the Table 1 and Fig. 1 represents the issues of data mining process under various years. Most of the researchers in 2015–18 concentrate on data sanitization issue to protect highly sensitive data.

4 Conclusion and Future Work

Therefore, analyzing those diagnosis techniques can lead to new development in this area. In the interim, straightforward information sharing constrained diverse phishing assaults and malware helped security dangers. There are some protection touchy applications like wellbeing administrations on cloud that are worked with different financial and operational advantages require upgraded security. Therefore, precise the internet security and alleviation against phishing rush ended up required to avoid by and large information protection. In this paper, we have dissected different issued of information mining procedure, for example, privacy saving, information

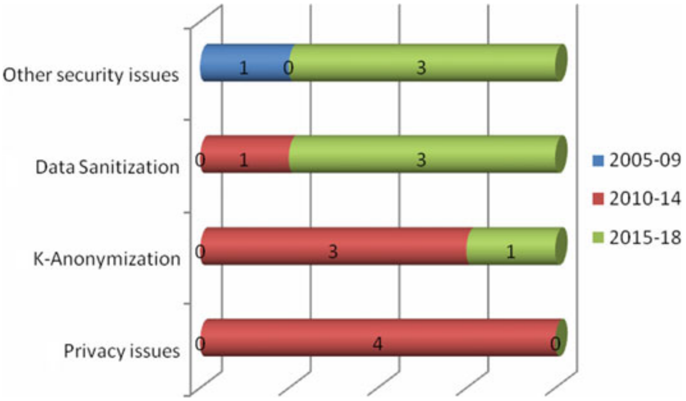


Fig. 1 Categorization based on techniques

cleansing, *K*-anonymization, data security on touchy information and so on. The investigation portrays, to secure the protection data of information proprietor from information clients and specialist organization, cleansing methodology is utilized in this setup. The sterilized data can't be recovered until the cleansing key is gotten. Our proposition gives a productive answer for securing information proprietor's data in database.

So as to beat these security issues, we have built up an ideal method for verifying touchy information.

References

1. Blanco-Justicia A, Domingo-Ferrer J (2018) Efficient privacy-preserving implicit authentication. Comput Commun 125:13–23
2. Lyu L, Bezdek JC, Law YW, He X, Palaniswami M (2018) Privacy-preserving collaborative fuzzy clustering. Data Knowl Eng, corrected proof, Available online 12 May 2018 (in press)
3. Nakamura Y, Harada K, Nishi H (2018) A privacy-preserving sharing method of electricity usage using self-organizing map. ICT Express 4(1):24–29
4. Ali I, Khan E, Sabir S (2018) Privacy-preserving data aggregation in resource-constrained sensor nodes in Internet of Things: a review. Future Comput Inf J 3(1):41–50
5. Rajesh N, Arul Lawrence Selvakumar A (2018) Association rules and deep learning for cryptographic algorithm in privacy preserving data mining. Clust Comput 1–13
6. Kaaniche N, Laurent M (2017) Data security and privacy preservation in cloud storage environments based on cryptographic mechanism. Comput Commun 111:120–141
7. Jaseena KU, David JM (2014) Issues, challenges, and solutions: big data mining. Comput Sci Inf Technol (CS & IT) 131–140
8. Dara S, Zargar ST, Muralidhara VN (2018) Towards privacy preserving threat intelligence. J Inf Secur Appl 38(February):28–39
9. Abdelhameed SA, Moussa SM, Khalifa ME (2018) Privacy-preserving tabular data publishing: a comprehensive evaluation from web to cloud. Comput Secur 72:74–95
10. Ma X, Zhang F, Chen X, Shen J (2018) Privacy preserving multi-party computation delegation for deep learning in cloud computing. Inf Sci 459:103–116

11. Giannotti F, Lakshmanan LVS, Monreale A, Pedreschi D, Wang H (2013) Privacy-preserving mining of association rules from outsourced transaction databases. IEEE Syst J 7(3):385–395
12. Zhang L, Yan Z, Kantola R (2017) Privacy-preserving trust management for unwanted traffic control. Fut Gener Comput Syst 72:305–318
13. Loukides G, Gkoulalas-Divanis A (2012) Utility-preserving transaction data anonymization with low information loss. Expert Syst Appl 39(10):9764–9777
14. Tudor V, Almgren M, Papatriantafilou M (2018) The influence of dataset characteristics on privacy preserving methods in the advanced metering infrastructure. Comput Secur 76:178–196
15. Wang Y, Cai Z, Tong X, Gao Y, Yin G (2018) Truthful incentive mechanism with location privacy- preserving for mobile crowdsourcing systems. Comput Netw 135:32–43, 22 April 2018
16. Singh DK, Swaroop V (2013) Data security and privacy in data mining: research issues & preparation. Int J Comput Trends Technol 4(2):194–200
17. Sharma, BR, Kaur D, Manju A (2013) A review on data mining: its challenges issues and applications. Int J Curr Eng Technol. ISSN 2277-4106
18. Ni L, Yuan Y, Wang X, Zhang M, Zhang J (2017) A location privacy preserving scheme based on repartitioning anonymous region in mobile social. In: The proceedings of the 2017 international conference on identification, information and knowledge in the internet of things Procedia computer science, vol 129, 2018, pp 368–371
19. Xu L, Jiang C, Wang J, Yuan J, Ren Y (2014) Information security in big data: privacy and data mining. IEEE Access 2:1149–1176
20. Navarro-Arribas G, Torra V, Erola A, Castellà-Roca J (2012) User *k*-anonymity for privacy preserving data mining of query logs. Inf Process Manage 48(3):476–487
21. Guo K, Zhang Q (2013) Fast clustering-based anonymization approaches with time constraints for data streams. Knowl-Based Syst 46:95–108
22. Fletcher S, Zahidul Islam Md (2015) An anonymization technique using intersected decision trees. J King Saud Univ-Comput Inf Sci 27(3):297–304
23. Sahoo J, Das AK, Goswami A (2015) An efficient approach for mining association rules from high utility itemsets. Expert Syst Appl 42(13): 5754–5778
24. Li L, Lu R, Choo K-KR, Datta A, Shao J (2016) Privacy-preserving-outsourced association rule mining on vertically partitioned databases. IEEE Trans Inf Forensics Secur 11(8):1847–1861
25. Castro, J, González JA (2017) A linear optimization-based method for data privacy in statistical tabular data. Opt Methods Softw 1–25
26. Chahar H, Keshavamurthy BN, Modi C (2017) Privacy-preserving distributed mining of association rules using Elliptic-curve cryptosystem and Shamir's secret sharing scheme. Sadhana 42(12):1997–2007
27. Teng Z, Du W (2009) A hybrid multi-group approach for privacy-preserving data mining. Knowl Inf Syst 19(2):133–157
28. Upadhyay S, Sharma C, Sharma P, Bharadwaj P, Seeja KR (2016) Privacy preserving data mining with 3-D rotation transformation. J King Saud Univ—Comput Inf Sci, corrected proof, Available online 28 November 2016 (in press)
29. Jia J, Yu J, Hanumesh RS, Xia S, Jiang X (2018) Intelligent and privacy-preserving medication adherence system. Smart Health, accepted manuscript, Available online 5 July 2018 (in press)
30. Demir S, Tugrul B (2018) Privacy-preserving trend surface analysis on partitioned data. Knowl-Based Syst 144:16–20, 15 March 2018

A Study on Different Types of Robotics Applications

B. U. Meghana and M. V. Prashanth

Abstract This paper's main objective is to investigate the different types of robots, their operation, and application. Different types of robots follow different methods such as mobility, weight balance, distributed control system, biopsy, current 3G technology, skid steering, robotic weeding, calculation of Godspeed, suction cups, and network communication protocol. Here we discuss various types of robots, the following methods, the parameters used and their use in different fields. Finally, we can conclude that this paper briefly introduces robotic applicability in various areas.

Keywords Snake robot · Heavy duty robot · Medical robot · Car robot

1 Introduction

Robotics is an interdisciplinary branch of science and engineering. Robotics covers the structure, development, activity, and use of robots and computer frameworks for tracking, sensory feedback, and processing records. These advances are used to build machines to update and imitate human activities. Robots can be used in many situations and for many features, but in recent times many are used in risky situations (bomb identification and deactivation), production techniques or wherein humans cannot tolerate them (e.g., Space). Robots can also take any form, but some appear to be human beings [1]. This is said to help and accept a robotic behavior that people generally perform in certain replicative behavior. Such robots try to reflect walking, lifting, speaking, cognizing and, in essence, something that can be done by people. Many of the robots today are of course inspired and contribute to the bio-inspired robotics enterprise.

B. U. Meghana (✉) · M. V. Prashanth
Department of Information Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India
e-mail: meghana1998megha@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_82

1.1 Robotics and Artificial Intelligence

A robotic is a machine consisting of sensors, manipulators, power components and software, all of which work together to meet a challenge. Motivation is the intrinsic enthusiasm of an employee and the drive to carry out work-related activities. Artificial Intelligence (AI) Artificial robots are artificial dealers in the real world. AI Robot aims to manipulate objects through the perception, selection, movement, and destruction of objects. Robotics is an AI department composed of different branches and robot alertness. Power supply, actuators, electric motors (AC/DC), pneumatic air muscles, muscle wires, piezo motors and ultrasonic motors, sensors are components of AI Robots [2].

1.2 Aspects of Robotics and AI

AI robot has a mechanical design and shape to carry out a specific project. They have electric components that make the machinery strong and manage it. They include a few phases of a computer program that determines what a robotic does, when, and how. AI Robot Locomotion: Locomotion is the mechanism that enables the AI robot to move around it. Various types of locomotives are available: legged, wheeled, a combination of the legged and wheeled locomotive, tracked slip/skid. There are five most important components in the maximum fundamental stage [2].

A frame structure, a muscle gadget to move the frame structure, a sensory device that gets facts approximately the frame and the encompassing environment, a power supply to activate the muscle mass and sensors, a mind machine that strategies sensory records and tells the muscles what to do. Applications of Artificial Intelligence Robotics are Industrial, Medical Applications, Exploration, and Entertainment [2].

There are so many information about Robotics to be acknowledged. The Robots are used in many fields like agriculture, industry, hotel, household works, hospital, school, college, etc. Understanding their working is greater vital, in order that if any problem is given, we can discover the answers by means of creating new varieties of robots.

2 Literature Review

Chaudhry and Sharma [3] talked about snake robots mobility. In the future, snake robots hold a lot and have a great scope in India. In future applications such as agriculture, sanitation, and firefighting, serpent robots are used. The advanced technology helped us to achieve “Beyond Human Capabilities”.

Chung et al. [4], introduced the heavy-duty industrial robot design process particularly for analytical technology to build the native model of KIMM. This model has a payload of 600 kg. For heavy-duty robot in static and dynamic payload more than 300 kg is essential for analysis to manipulate the design to select the basic components. Already much-commercialized software is available in the market. Here the author developed innovative software for inverse dynamic analysis called “Rodan”. By using this software and its application the weight balancing component selection is easily made for manipulation.

Wyeth et al. [5], designed an autonomous humanoid robot for playing soccer with the help of image processing, artificial intelligence, and decision-making. He controlled the Metal Fighter 2 humanoid robot with the communication system and process the image with the Kalman filtering algorithm and proposed the 4 step model based on 6 step reasoning model. Evaluated with the proposed system and got good stability and competition ability towards humanoid robot soccer system. This paper will help us to understand the mentality of human and how these robots behave like human and communicate with a human is described. It works based on Mechanical CAD model, Bipedal Walking Robots, Motor Choice, Electronics. It will illustrate the design of a practical, affordable, autonomous, humanoid robot.

Azar and Samy [6] discussed the working of Medical Robots. These robots are used to assist doctors and nurse. These robots help in telesurgery, brain biopsy, telemedicine, surgical training, remote surgery, telemedicine, teleconsultation, rehabilitation therapy, prosthetics.

Kaur and Kumar [7] worked on the wireless multifunctional robot to help the defense and military applications with the help of 3G technology to monitor the remote and border areas. This multifunctional robotic vehicle helps to examine the border areas and it has to be communicated and controlled by an autonomous and manual system. This robotic has a multifunctional feature like to detect human, bombs, harmful gases and fire at the remote and border areas. For power consumption, the robot uses renewable resources with the help of a solar panel. The limitation behind the system is the frequency of the range. He also assessed the results of the selection of the tilt angle of the solar panel and the energy consumption for the autonomous and manual system. Users can control the movement of robots from any part of the world by receiving live video feedback from the environment. It is used as a security surveillance camera robot and as a rescue operation.

Shekhawat et al. [8], detailed study on Automatic car robot follows the method of a wireless controller with the help of Bluetooth. It is used in our real-life like AGV, used for dropping the parcels. It has the ability to sense the environment and decide the navigation path without any human input.

Pedersen et al. [9], worked on Agricultural Robots, and developed autonomous tractors and automatic steered systems for agricultural purpose. It uses robotic weeding, micro-spraying, crop establishment, crop scouting, selective harvesting, economic scenarios, field scouting, weed detection methods. It reduces labor costs and restrictions on the number of daily working hours.

Hotel Service Robots were evaluated by Tussyadiah and Park [10]. Artificial intelligence and robotics for tourism and hospitality, hotel service robots evaluation, automatic emotional responses to hotel robots. Confirmatory factor analysis was performed using Smart PLS 3.0, a multi-group analysis that compares path coefficients between respondents exposed to two different NAO robots, Relay. It is used in the front desk and delivers items to the room.

Jagtap [11] discussed the use of robots for wall climbing. The study presents an application of a rising glass and wall cleaning automaton. Automated operation during movement, large remote control range. Cleaning robots structure, components used in robots cleaning, robot mechanism, basic design calculations are explained. It is used in a wide range of maintenance, building, inspection and process, and construction safety applications.

The applications of ARP were explained by Clotet et al. [12]. The mobile teleoperated robot is designed as a live robot. Mechanical design, electronic components, implementation of software, the architecture of video conferences, network communication protocol methods. Explains video communication, audio communication, external network server, preliminary usability test, prevention of collisions. This paper presents the design and application of a mobile teleoperated robot as a living tool. It is used as a mobile video conference service, mobile telepresence service, walking tool, scheduling tool, fall detection tool, mobile monitoring platform for the environment.

3 Comparison of Different Kinds of Robotics with Parameters

Table 1 shows the comparison of different kinds of robotics with parameters like mobility, cost, performance, and flexibility. This comparison will help us to know little more to achieve the better result in future.

Table 1 Comparison of different kinds of robotics with parameters

Robotics	Mobility	Cost	Performance	Flexibility
Snake robots	Yes	High	High	Yes
Heavy-duty handling robots	Yes	Low	High	Yes
Humanoid robots	Yes	High	High	Yes
Medical robots	Yes	High	High	Yes
Military robots	Yes	Low	High	Yes
Car robots	Yes	High	High	Yes
Agriculture robots	Yes	Low	High	Yes
Hotel service robots	Yes	Low	High	Yes
Wall climbing and glass cleaning robots	Yes	Low	High	Yes
Assisted personal robots	Yes	High	High	Yes

4 Discussion

This paper presents the uses of different types of robots, such as snake robot that helps in the field of agriculture, heavy-duty handling robots used for industrial purposes, autonomous humanoid robot that helps people interact with machines, medical robots that help in the field of medicine, military robot that is used as a security camera robot and emergency rescue. Car robot that helps to drop parcels, an agricultural robot that reduces labor costs and the number of working hours per day, hotel service robot that helps to deliver items to the room, Wall Climbing which helps in construction, Tele-Operated Assisted Living Robot which is used as mobile videoconference service.

5 Conclusion

Robotics is one of the emerging techniques and used across the world to help people. It will help to a human being and make the work easier to achieve. In this paper, we discussed the different applications of robotics, components, methods, parameters, and their uses to create an innovative robot.

Acknowledgements The authors express gratitude towards the assistance provided by Accendere Knowledge Management Services Pvt. Ltd. in preparing the manuscripts. We also thank our mentors and faculty members who guided us throughout the research and helped us in achieving the desired results.

References

1. Wikipedia—Robotics. https://en.wikipedia.org/wiki/Robotics. Accessed 15 Sept 2018
2. Shailna Patidar.: AI Robot—Robotics and artificial intelligence. https://dzone.com/articles/ai-robot-robotics-and-artificial-intelligence. Accessed 20 Sept 2018
3. Chaudhry N, Sharma S (2015) A review study on future applicability of snake robots in India. IOSR J Comput Eng 17:2278–2661
4. Chung GJ, Kim DH, Park CH (2008) Analysis and design of heavy duty handling robot. 2008 IEEE Int Conf Robot Autom Mechatron RAM 2008. 00, 774–778
5. Wyeth G, Kee D, Wagstaff M, Brewer N, Stirzaker J, Cartwright T, Bebel B (2001) Design of an autonomous humanoid robot. In: Proceedings of the Australian conference on robotics and automation, pp 14–15
6. Azar AT, Samy E (2012) Medical robotics. In: Prototyping of robotic systems: applications of design and implementation, p 35
7. Kaur T, Kumar D (2015) Wireless multifunctional robot for military applications. In: 2015 2nd international conference on recent advances in engineering and computational sciences, RAECS 2015
8. Shekhawat RS, Sain A, Bhardwaj G (2016) Automatic intelligence car robot. Int J Sci Technol Eng 2:504–508
9. Pedersen SM, Fountas S, Blackmore S (2008) Agricultural robots—applications and economic perspectives. Service Robot Appl 369–382

10. Tussyadiah I, Park S (2018) Consumer evaluation of hotel service robots. In: Information and communication technologies in tourism, pp 308–320
11. Jagtap A (2013) Skyscraper’s glass cleaning automated robot. Int J Sci Eng Res 4:806–810
12. Clotet E, Martínez D, Moreno J, Tresanchez M, Palacín J (2016) Assistant personal robot (APR): conception and application of a tele-operated assisted living robot. Sens (Switzerland) 16:1–23

UVRento—Online Product Rental Application Using Cross-Platform Service

Rahul Patil, Siddaram Sonnagi, Ashwini Dhummal, Subhas Kadam and V. Sanju

Abstract According to the current situation of high demand for mobile applications, combined with the mainstream and the enterprise activities (Yang and Zhang in Computing technology, industrial information integration, [1]), the emergence of E-commerce has been playing a vital role in each and every sector of our daily lives. The number of new and different product developments increasing each year, triggers probability of previous technology users, especially in electronic gadgets. There are at least 40% of people who change their smartphones, laptops or any other electronic devices in a minimum of 2–3 years (by social interactions). Hence the cost of living is increasing steadily. For instance, cost of living in Bangalore in the year 2015 was around 5000Rs–6000Rs, and now it has been increased around to 7000–10,000 per month ((B)Grady Booch Rational Santa Clara, California in object-oriented analysis and design, [2]). Hence, Rental applications may reduce cost of living without affecting the mandatory life choices and their preferring lifestyle. This paper gives a detailed hands-on experience with the Rental Platform, UVRento, and how it can be implemented using E-commerce model application services. UVRento is an application developed using Ionic Framework with Firebase as its backend. Ionic being a cross-platform framework, it makes easier to develop powerful and efficient applications for every major platform running out there (iOS, Android, Windows Phone, etc.). While Firebase along with Google's security provides the

R. Patil · S. Sonnagi (✉) · A. Dhummal · S. Kadam · V. Sanju
Department of Computer Science and Engineering, NMAMIT, Nitte, Karnataka, India
e-mail: siddaram.sonnagi@gmail.com

R. Patil
e-mail: rahultpatil007@gmail.com

A. Dhummal
e-mail: ashwinidhummal08@gmail.com

S. Kadam
e-mail: subhaskadam840@gmail.com

V. Sanju
e-mail: sanjuv21@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_83

database facility which is more robust, more reliable and easy to integrate with Ionic Framework (Ionic framework document, [3]; Learn firebase—tutorials, [4]).

Keywords UVRento · Mobile application · Hybrid · Cross platform · Rental application service · Ionic · Firebase · Cost of living · Local marketing

1 Introduction

Most people want to rent out items to save their money. Hence they use the Online Rental website system where they can get their items in lower prices and for a short period of time. But in these systems, there is a communication gap between the real vendors who give the items and the customers who actually use the items because, in these systems, the Rental website organization buys the item from the vendor and give it to the customers. Hence in the present market, there is a need of bridging the gap between Customers and the Vendors for the benefit of the both.

- Our system UVRento aims to bridge the gap between the Customers and Vendors [5, 6].
- Online platform where users can rent or buy items like electronic gadgets, books, cycles, etc. based on their locality [7].
- This leads to efficient local marketing [8].

2 Proposed Business and Implementation Module

A new online rental service business model and Implementation modules in e-commerce industry—UVRento application—is presented in this section.

2.1 Modules in UVRento Application

1. **Admin**:
   - Register
   - Login
   - Verify the vendor details
   - Verify the customer details
   - Approve/Reject products
2. **Vendor**:
   - Register
   - Login

- Upload/Remove products
- Modify details
- Logout

3. **Customer**:

- Register
- Login
- Search product
- Place my order
- View my order
- Logout

2.2 Use Case Diagrams

Use Case Diagram (Fig. 1):

Use Case Diagram (Fig. 2):

2.3 Business Model with Use Case Diagrams

Vendor Side: Once vendor register their ID then about the product description their product is not uploaded! But our admin verifies the product quality, quantity and

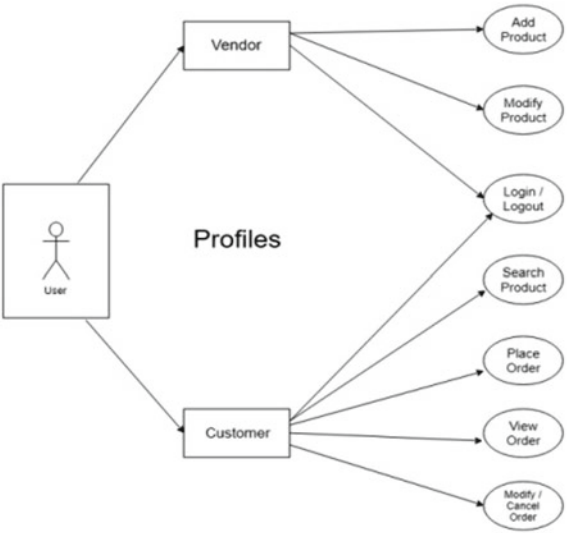


Fig. 1 Use case diagram for profiles [2]

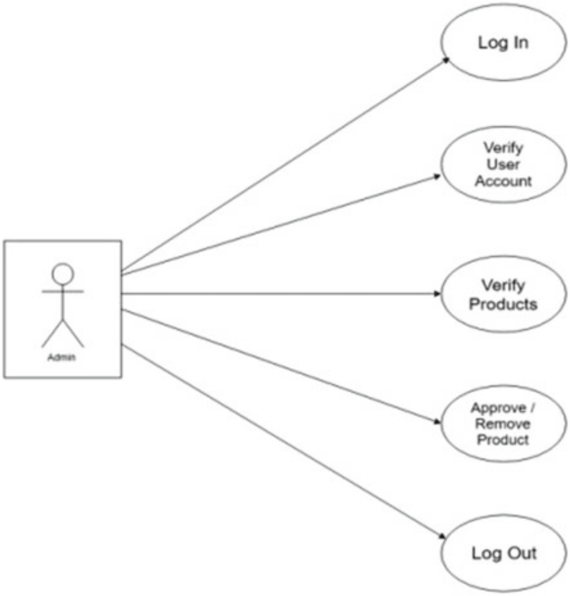


Fig. 2 Use case diagram for admin module [2]

the cost of the product. If our admin is satisfied and pass all the product check then the product is given green signal and it's uploaded to the UVRento platform! This is done because to stop the fake product description uploaded on web by the direct vendor…! And it this we don't support the fake items.

Customer Side: Any customer who wants to take for Rent/Buy the products will create an account and puts the selected products on cart, thus he places an order. The payments of these products are always depends on customer and vendor communication (Fig. 3).

2.4 Implementation Module

User Registration: User may be either Vendor or Customer, he need to register by submitting required details such as mainly Name, Address, Aadhaar card, UID number, PAN card, etc. Aadhaar card must be scanned using UVRento Scanner which provided in application while user registration setup. Thus UVRento achieve security over users.

Profile:

- Basically, UVRento has two profiles Vendor and Customer. Any user is allowed to change his profile and he can act in both the profiles simultaneously as per his requirement.
- Being vendor he can only perform sell/Put for Rent operations, being Customer he can only perform buy/Take for Rent operations.

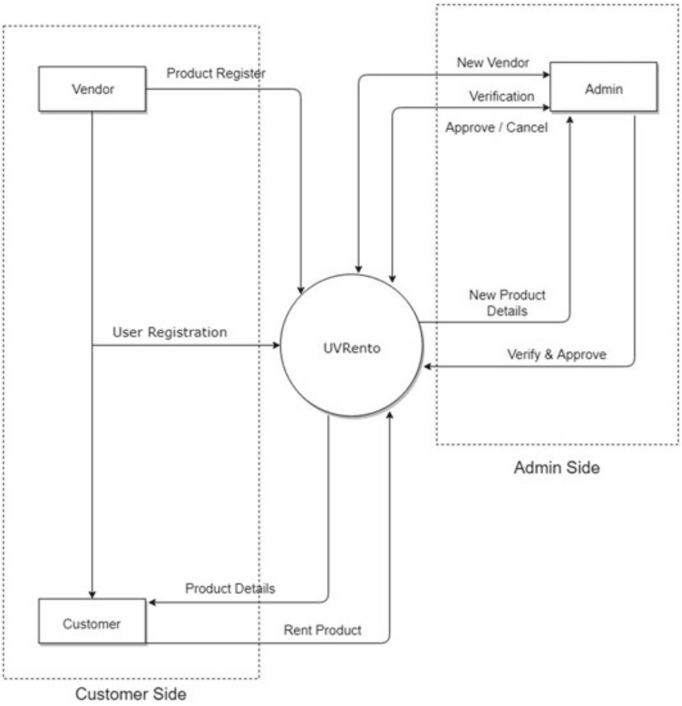


Fig. 3 Data flow diagram of business model

- By activating both the profiles he can perform Buy/Sell/Put for rent/Take for Rent operations.

Vendor Side: Registered vendor is allowed to put any products for Rent by paying the specified charges. Charges are different for each product; it depends on product factors such as original cost, usage, damages, etc.

Admin (Specifically: Verification Team):

- Admin who is in the verification department will verify the product that vendor has requested to put product on online UVRento platform for marketing.
- Admin can approve the product if it meets all the terms and conditions or Reject the Vendor Product if it did not meet terms and conditions after verification.

UVRento Platform: After admin verification and approve procedures, vendor product will be displayed on the marketing platform (UVRento) with all the required details and specifications provided by the vendor.

Customer Side:

- Registered customer can search and browse the details of available products such as specifications, rate, date, ratings, etc.
- If he is interested in any product he can click Request item to notice vendor that he is ready to take it for rent.
- If he gets positive action from vendor then UVRento displays vendor location, phone number, and some other required details.
- By the provided details he can call/message and arrange a meet or courier the item whatever, it's completely depends on both of them.
- Thus, UVRento helps customer to get connected with vendor and to order required product for rent.

2.5 Payments and Delivery

Payment and delivery method completely depends on Customer and vendor interactions. They may go through doorstep delivery or courier process in delivery process or online payment/cash on delivery in payment process.

2.6 Literature Survey

People nowadays don't want to spend on products like Mobiles, Cameras and all such electronic devices that lose up to 50% of its value the moment they purchase it (Depreciation). They just want to use and experience the feel of such products at lower prices. Hence Item Renting Websites such as RentoMojo.com, Furlenco, GrabOnRent, Rentickle, etc. have seen a rise in their usage. But all these item renting websites systems have one thing in common; they all buy the items directly from the vendors. This system doesn't build up communication between the vendors and the customers who actually use the products. And in some cases, the vendor may occur losses due to selling of the items which may have potentiality of returns more than its cost price. This benefit is taken by these existing systems.

3 Screenshots of User Interface (UI) Design

See Figs. 4, 5 and 6.

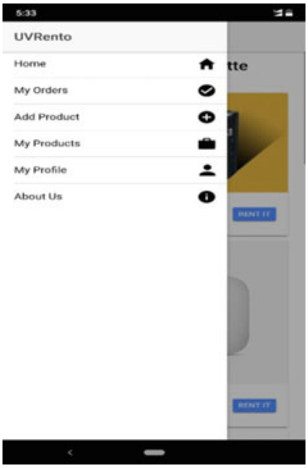
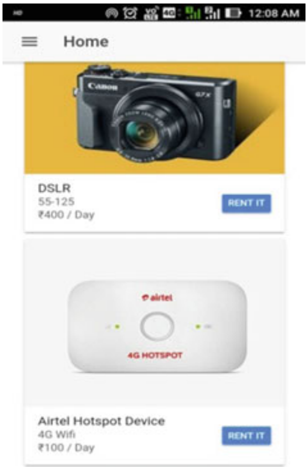


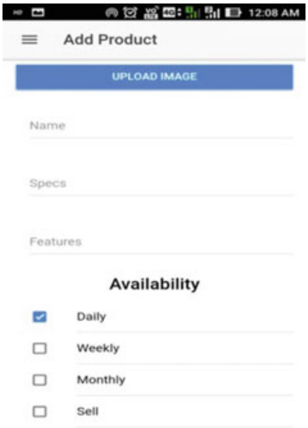
Fig. 4 Menu bar—menu bar is the button used to operate all the pages and activities of UVRento app (References—UVRento application) [3, 4]



DSLR
55-125
₹400 / Day

Airtel Hotspot Device
4G Wifi
₹100 / Day

Fig. 5 Home—after user login home page acts as master node where user can get the nearby available products for rent in UVRento application (References—UVRento application) [3, 4]



☑ Daily
☐ Weekly
☐ Monthly
☐ Sell

Fig. 6 Add product—is a menu node where user can add his products for rent on daily, weekly, monthly and for sale basis (References—UVRento application) [3, 4]

4 Results and Discussion

- Users can get items without actually having to buy it, thus saving money.
- More Usage—Less Cost for Users.
- Vendors can collect their revenue easily with Renting system.
- Users can get items based on their requirements, for a specific period of time.
- UVRento can improve local marketing of Vendors.
- Rental Marketing is a Solid way and Scalable Marketplace.
- With the help of this project, people need not waste money for short term materials. Helps to improve Local marketing. 24*7 Product showcase. Enables more usage less cost for users, it may lead to customer-friendly platform.

References

1. Yang Y, Zhang Y (2017) Computing technology, industrial information integration. In: IEEE conference 2017—mobile terminal development plan of cross-platform mobile application service platform based on Ionic and Cordova
2. (B)Grady Booch Rational Santa Clara, California—Object oriented analysis and design. ISBN 0-8053-5340-2 15 1617181920 DOC 0 1 00 99 98 l5th Printing, Dec 1998
3. https://ionicframework.com/docs—Ionic framework document
4. https://hakr.io/tutorials/learn-firebase.com to learn firebase—tutorials
5. Mutiawani V, Rahmany S, Abidin TF (2018) Informatics department. In: IEEE conference, 2018 international conference on electrical engineering and informatics (ICELTICs), Sept 19–20, 2018
6. Bosnic S, Papp I, Novak S. The development of hybrid mobile applications with Apache Cordova. Research and Development Institute RT-RK, Novi Sad, Serbia
7. Ravulavaru A. Learning ionic. Packt Publishing, Birmingham. ISBN:9781783552603
8. https://www.nestaway.com/info/cost-of-living-in-india-bangalore/—cost of living records

Autonomous Unmanned Ground Vehicle for Enhancement of Defence Strategies

M. Someshwaran, Deepa Jose and P. Paul Jefferson

Abstract This paper explains about the Autonomous Unmanned Ground Vehicle named Lakshman, which has the following features—carry payload (food and medicines), follow the soldier like a companion, autonomous return to the base and it can also locate an enemy, etc. The vehicle can be remotely controlled if required. The technology been targeted are limited cross-county mobility, autonomous following techniques, localization, perception and path planning. It can carry stores and ammunition for three days. The implementation setup is been divided into four sections. They are mechanical, power management, core control, and autonomous section. Lakshman can work continuously for three days. The frame structure is made using mild steel to carry a payload around 200 kg. Power management unit makes the device to sustain more working hours, making it reliable and flexible to the requirement. The core control section controls the entire process and collects data from various sensors. Autonomous section controlled by ARM cortex A53 to process high data speeds. The most important future plan is to provide steganography method of communication, which is a highly secured communication, so the vehicle cannot be easily tracked by other people with enhanced technology. By implementing a dedicated FPGA for encrypted steganography communication will provide greater assist to the A-UGV. Thus Lakshman can be a very effective tool to enhance Indian Defence Strategies.

Keywords SLAM—Simultaneous localization and mapping · ROS—Robot operating system · AUGV—Autonomous unmanned ground vehicle

M. Someshwaran · D. Jose (✉) · P. Paul Jefferson
Electronics and Communication, KCG College of Technology,
Karapakkam, Chennai 600097, India
e-mail: deepa.ece@kcgcollege.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_84

1 Introduction

The growth of technology in the area of Unmanned Ground Vehicles has become vast. The research in autonomous vehicles and artificial intelligence has infinite applications. Using artificial intelligence in the field of autonomous vehicle would be a great revolution, and dynamic in the field of defence. According to India's defence vehicles, this method of implementation of A-UGV provides robust and powerful strategies in defence. This paper explains about the Autonomous Unmanned Ground Vehicle which can do the following features: follow a solider, autonomously return to the base station, transmit live video footage to the receivers end, and also able to control the vehicle in a semi-autonomous way. The vehicle has four sections in it mechanical, power management, core control and the autonomous sections, respectively.

2 Implementation Setup

A. **Mechanical Section**:

For any vehicle, the frame of the vehicle is very crucial for it to withstand weights [1]. Lakshman is carefully designed to carry varying and flexible payloads up to 200 kg. The frame structure is built using mild steel whose density is about 7.85 g/cm^3. Mild steel is cheap and it is available in a large amount. Lakshman is strongly supported by Caterpillar Tracks which provides high stability to vehicle and have better mobility over rough terrains [1]. Track section consists of two sprockets on each end which is permanently connected to High torque driving motor which finds better friction during mobility [1]. The tension on the wheels is equally distributed through the effective shock absorbers with hydraulic. This structure strongly supports the frame from all sides. The basic version of Lakshman is concentrated to carry food and medical supplies to soldiers. The way in which the vehicle has to be used can be changed according to our need and purpose for various platforms like easy transportable module, Articulated platform, Medevac, Supply transport, Reconnaissance, UAV platform and mainly as Remote weapon station [2, 3].

B. **Power Management Unit**:

Power is the basic requirement for any vehicle. To make the system more efficient UGV is been provided with both diesel as well as electrical power sources [1]. Lakshman consists of 1400 VA Diesel/petrol generator which acts as primary source for the UGV. By using diesel generator instead of standalone Battery source enhances the system efficiency higher. The reason for avoiding batteries as the main source for the power consumption is that batteries require double the amount of time to recharge again to be used. Whereas in the case of generators one can fill the diesel and use it efficiently. Lakshman produces an AC output of 220 V @50 Hz and a DC output of 12 V. The AC output is efficiently stepped down to 24 V to drive the

250 W high torque motors which is connected to the sprockets using a shaft. The power management unit in the UGV is designed in such a way that it meets all the constraint and it can work for longer hours more efficiently. Simultaneously two 12 V, 100 A which acts as secondary source. Batteries are charged and used to avoid stall time. Water cooling system makes the vehicle to withstand from overheating.

C. **Core Control and Communication Unit**:

The key feature of this section is that it collects data from various sensors and controls entire A-UGV. Lakshman is controlled by a 16 MHz microcontroller Arduino and 1.2 GHz microprocessor Raspberry pi v3. It comprises of different programmed functions which makes it to work autonomously. The power consumption of this section is very low compared to other sections. The system is made to work autonomous with the help of the Kinect sensor which uses the LIDAR technology. It analyses the depth of every object surrounding it and makes the vehicle to avoid disturbance. Lakshman is controlled through multiple frequency bands 433 MHz and 5.8 GHz [2, 3]. As 433 MHz frequency band has a high penetration through trees it is used for the data control and 5.8 GHZ is used for video transmission and also to get a clear quality of the data been transmitted. 5.8 GHZ is used for dedicated video transmission approximately less than 5 km. The 433 MHz data transceiver unit is used to wirelessly guide Lakshman from a long-distance [3]. Dedicated CMOS camera is been provided to monitor the vehicle as a live feed and it is boosted by 5.8 GHz video transmission unit.

D. **Autonomous Unit**:

Autonomous part of A-UGV has two features, following the group and return to base. Lakshman is operated to a distance of 20 km from the controller side. The vehicle can be controlled by the person at the control section if required. Autonomous functionality is the most crucial system in this UGV where it processes numerous data sets instantly by using 1 GB of flash that located within the Raspberry Pi. Autonomous 3d mapping technology is done through LIDAR system where it collects data through Kinect sensor system and it provides visual data in a 3d architecture which makes the UGV more precise in identifying the objects and location [4]. Green ant algorithm is used to provide an optimal route planning which provides the shortest route to the destination. It uses simultaneous localization and mapping technology. The G-mapping package provides laser-based SLAM as a ROS node called slam G-mapping [5, 6].

By using GPS positioning system that gets saved by the user will provide an additional information to the UGV to return to base. By saving the initial base location it can easily return to base with an optimal and shortest route possible [4].

3 Calculation of Remote Access

See Table 1 and Fig. 1.

Table 1 The calculation of remote access for 433 MHz and 5.8 GHz

Required parameter	433 MHz transmission unit	5.8 GHz transmission unit
Transmit antenna gain	2 dB	2 dB
Transmitting power	17 dB	23 dB
Operating frequency (Hz)	433 * 106	5:8 * 109
Receiver sensitivity	−70 dB	−90 dB
Free space loss	107 dB	−90 dB
Total estimated range (meters)	1554.65	2315.75

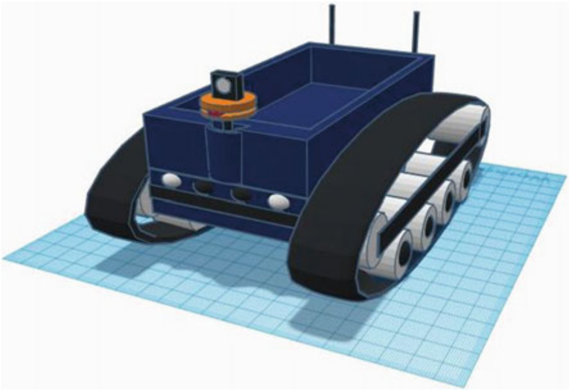


Fig. 1 Sample image of the UGV

4 Discussion of Results

A. Prototype

A small prototype of entire model is been made using thermocol material (Fig. 2).

B. Raspberry Pi Testing

Raspberry Pi is been interfaced with the libraries such as the Open NI and Open CV. Programs which are required to make the motors run are been tested and their results are successful. Motor runs with high amount of torque but at a slight slower speed.

C. Stability and Stress Analysis

A stabilized and more rigid UGV which can hold up to 500 kg has been tested. It is found that the frame structure can withstand 500 kg without causing any degradation in the performance of the vehicle. Below shown image is the frame structure of the UGV (Fig. 3).

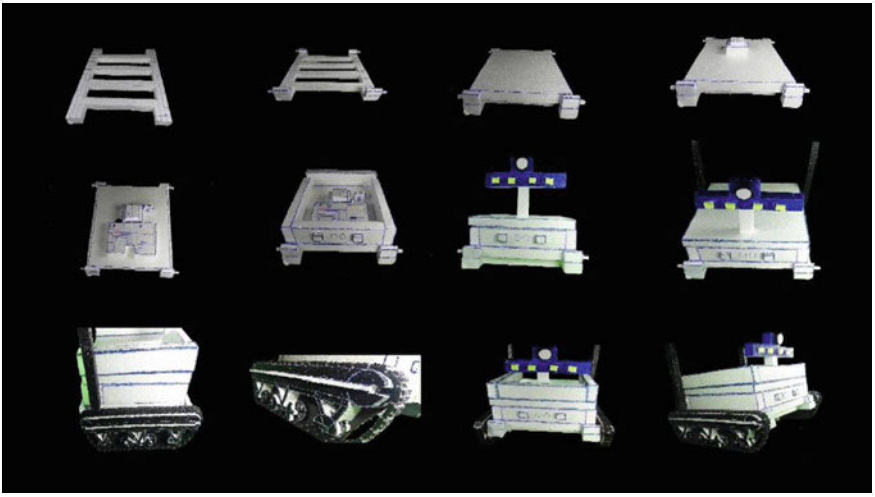
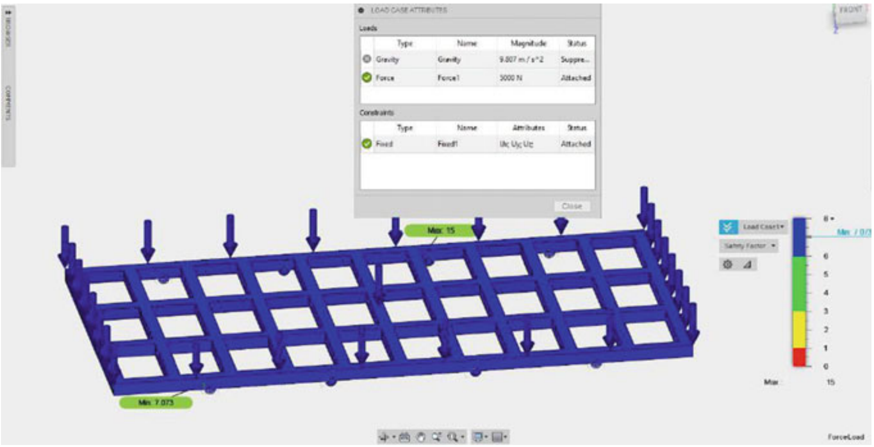


Fig. 2 Prototype model



LOAD CASE ATTRIBUTES

Loads

	Type	Name	Magnitude	Status
○	Gravity	Gravity	9.807 m / s^2	Suppre...
✓	Force	Force1	3000 N	Attached

Constraints

	Type	Name	Attributes	Status
✓	Fixed	Fixed1	Ux; Uy; Uz	Attached

Fig. 3 Analysis of frame structure

D. **Object Detection**

To make the vehicle detect a particular thing and to follow it is been tested. For this purpose, a red-coloured object is been made to detect by the vehicle using the MAT LAB. Results obtained are: the vehicle follows the red-coloured object (Fig. 4).

E. **Outlined View of the UGV**

The below-shown image displays an outlook of how the finished product of the UGV will appear.

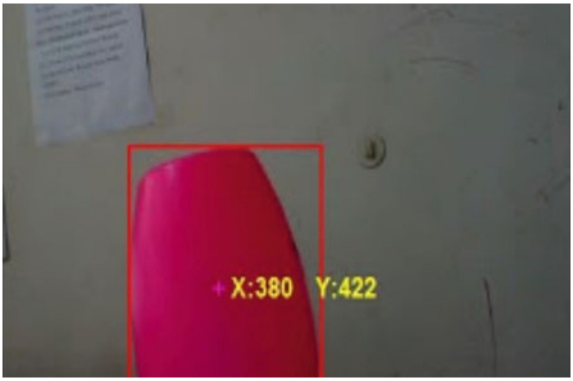


Fig. 4 Red colour object detection using MAT LAB

F. **Suspension and Wheel Assembly**

Types of suspension and the placement of the wheel assembly at the appropriate places are been tested and their results are been obtained (Figs. 5, 6 and 7).

G. **Dimensions**

The below-shown image gives a complete view on how the dimensions of the caterpillar track structures are been designed. The measurements given are been given in millimetres.

H. **Skeletal Tracking**

Human following is important function where UGV takes control of skeletal tracking which is more precise and accurate. ROS system track each joints and follows back (Figs. 8 and 9).

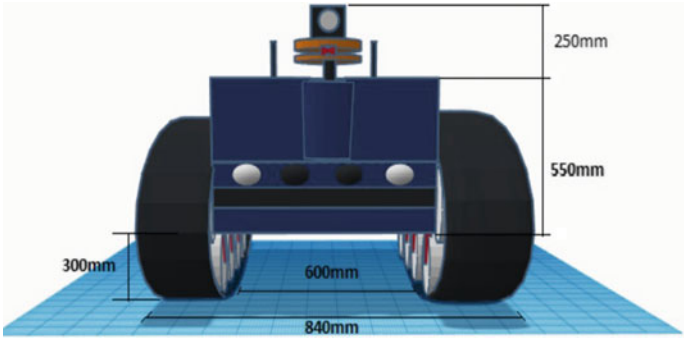


Fig. 5 The final outlined view of the UGV

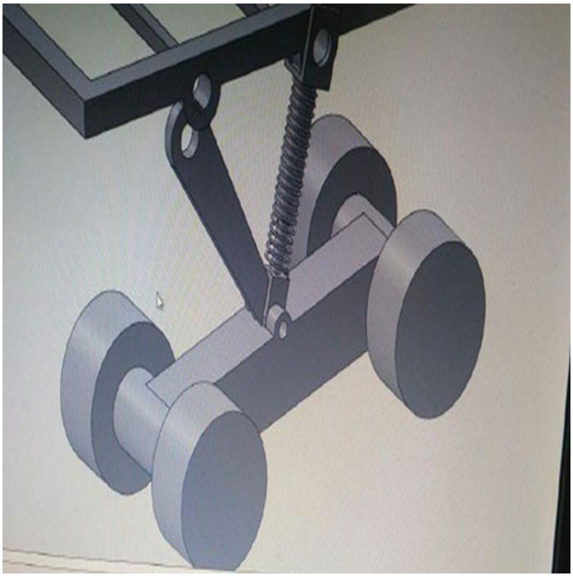


Fig. 6 Image of the suspensions been designed and the placement of the wheel assembly

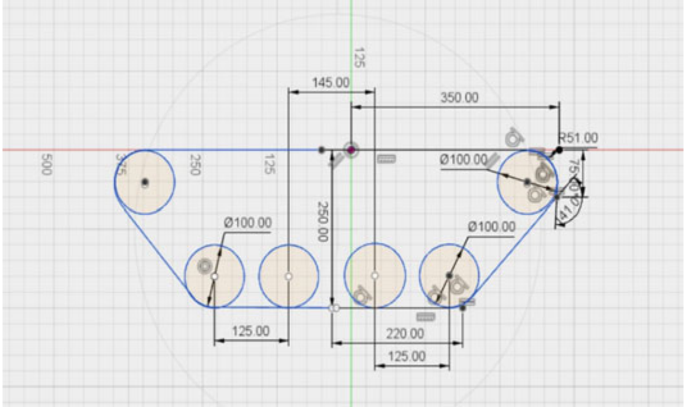


Fig. 7 Dimensions of the caterpillar tracks

I. **Collision Avoidance**

3D mapping is built using ROS system which is effectively used for collision avoidance, path planning, and optimization, autonomous return to base. skeletal tracking is very important for instructing the vehicle to follow the right solider who is been assigned previously for this purpose of making the vehicle to follow him, respectively.

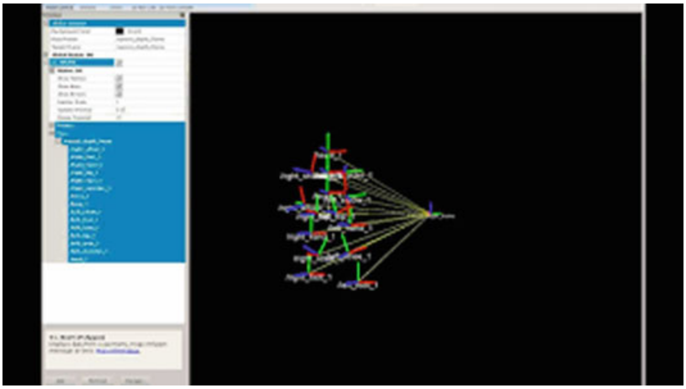


Fig. 8 Skeletal tracking for human following

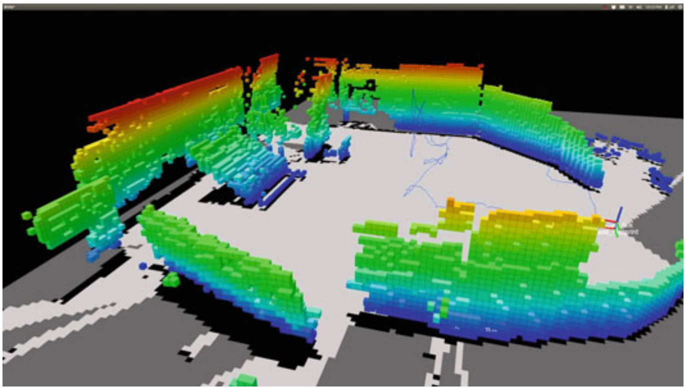


Fig. 9 3D mapping for collision avoidance and path planning

References

1. Carlson J, Murphy RR (2005) How UGVs physically fail in the field. IEEE Trans Robot 21(3)
2. Noor MZH (2013) Design and development of remote-operated multi directional unmanned ground vehicle (UGV). In: IEEE 3rd international conference on system engineering and technology, 19–20 Aug 2013, Shah Alam, Malaysia
3. Murtaza Z (2014) Design and implementation of low cost remote-operated unmanned ground vehicle (UGV). In: 2014 international conference on robotics and emerging allied technologies in engineering (iCREATE), Islamabad, Pakistan, Apr 22–24, 2014
4. Seo DJ, Kim J (2013) Development of autonomous navigation system for an indoor service robot application. In: 2013 13th international conference on control, automation and systems (ICCAS 2013), Oct 20–23, 2013, Kimdaejung Convention Center, Gwangju, Korea
5. Jabbarpour MR, Jung JJ, Kim P (2017) A green ant-based method for path planning of unmanned ground vehicles. Received Dec 30, 2016, accepted Jan 20, 2017, date of publication Jan 25, 2017, date of current version Mar 13, 2017. https://doi.org/10.1109/access.2017.2656999
6. Ullah I, Ullah F, Ullah Q (2015) Real-time object following fuzzy controller for a mobile robot. IEEE

A Parametric Study of Load Balancing Techniques in Cloud Environment

Insha Naz, Sameena Naaz and Ranjit Biswas

Abstract Cloud Computing is one of the rapidly growing areas in the field of computer science. A modern paradigm provides services through the Internet. An Internet-based technology employs pay-as-you-go model (PAYG). Load balancing is one of the important and vital issues in cloud computing. It (load balancing) is a technique which improves the distribution of workloads across various nodes. Load balancing distributes dynamic workload among various nodes so that no specific node breaks down by heavy load. It is crucial to utilize the full resources of a parallel and distributed system. Resource consumption and energy consumption both can be limited by distributing the load evenly and properly using different load balancing techniques. Lowering the use of resources increases the overall working performance of the system thus cutting down the carbon emission rate and providing the greener and safer environment. Different algorithms and techniques are employed to balance the load on nodes. These techniques can be examined on different parameters such as resource utilization, reliability of the system, system performance, related overhead of the system, power saving feature, scalability and many more. This paper presents the insight into the existing load balancing algorithms and their comparison on basis of different parameters.

Keywords Load balancing · Cloud computing · Energy consumption · Green computing

I. Naz (✉) · S. Naaz · R. Biswas
Department of Computer Science and Engineering, Jamia Hamdard, New Delhi 110062, India
e-mail: inshanaz_sch@jamiahamdard.ac.in

S. Naaz
e-mail: snaaz@jamiahamdard.ac.in

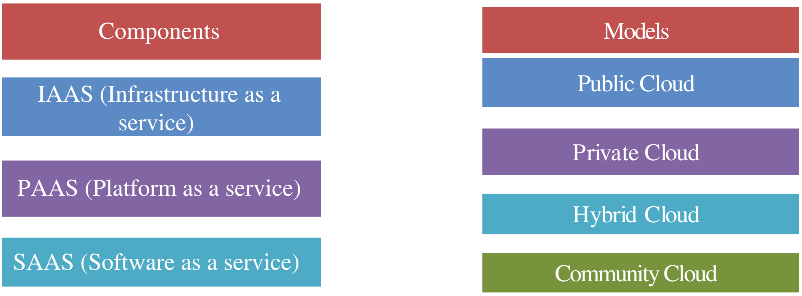
R. Biswas
e-mail: rbiswas@jamiahamdard.ac.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_85

1 Introduction

Cloud computing as a service was first made known by McCarthy in 1961 and later it was analysed by Licklider in 1963 [1]. Nowadays, cloud computing is the most popular term used in the field of computer science and IT. The frame 'Cloud Computing' refers to a kind of Internet-based technology which comprises of applications, storage, on demand services, etc. These cloud computing services are available through various organizations, like Google Cloud, Amazon Web Services and Microsoft Azure, etc. and require a nominal amount of money and time for consumers to access and process their data. There are three major components that describe the cloud computing network and four cloud deployment models.

These components can be described as follows:


Components
IAAS (Infrastructure as a service)
PAAS (Platform as a service)
SAAS (Software as a service)
Models
Public Cloud
Private Cloud
Hybrid Cloud
Community Cloud

1.1 *Software as a Service (SaaS)*

This provides a complete or we can say a whole application as a service to the cloud consumers in virtualized form typically on demand [2]. SaaS is very cost-effective because of the use of the utility-based payment model as no infrastructure investment is involved [3]. Common examples are Google apps like Google Mail and Salesforce, spreadsheets, Zoho, etc.

1.2 *Platform as a Service (PaaS)*

For application development, PaaS platform provides a very convenient and suitable environment. It provides the services to its consumers over the Internet on pay-per-use basis. The user may be able to control the applications and configurations but does not manage the infrastructure [4]. Examples are Microsoft Azure and Force.com.

1.3 Infrastructure as a Service (IaaS)

It uses the virtualization technique. Iaas component provides the services like processing, storage, data centre space, network equipments, etc. to its consumers on demand [3]. In this environment, the consumer gets high degree of responsibility and control. API is used for interaction. Amazon Web Services, GoGrid, 3 Tera are some of the examples.

2 Cloud Deployment Models

2.1 Public Cloud

The public cloud user can easily access the systems and services that are provided by the cloud service provider. In public cloud environment, there is a security risk since applications from different users are mixed together on cloud servers but is cost-effective [5]. Examples are Amazon Web Services (AWS), Microsoft and Goggle.

2.2 Private Cloud

A private cloud set-up is owned and managed by an organization singly. Resources are managed by organization itself somewhat like Intranet [4]. This set-up is more secure than public cloud set-up because the security is handled by the service providers themselves. Eucalyptus system is one of the examples.

2.3 Hybrid Cloud

Hybrid cloud is the mixture of two or more clouds that remain unique entities, or in other words, it can be stated as combination of private and public cloud [1]. Hybrid cloud services are mostly used in healthcare and law.

3 Load Balancing

For the efficient use of resources and faster processing of tasks, we need to balance the load and that is attained through load balancing [6]. Load balancing keeps a check on the work/load on different nodes and makes sure that no particular node or a server is heavily loaded thus preventing the breakdown of the system due to overloading. Domain Name Server (DNS) or a multilayer switch [7] is commonly used for load balancing.

Key Features

1. The performance of the system is considerably improved.
2. To maintain the system stability.
3. To safeguard the machine consistency.
4. Deviations to the system are controlled.
5. Builds fault-tolerant systems by forming backups.

3.1 Load Balancing Algorithms

Load balancer allocates the tasks dynamically to servers/nodes to match up to the increasing demand [8]. For smooth distribution of tasks/workload on different servers, efficient load balancing algorithms and techniques are necessary to be implemented. Depending on how the cloud is configured, load balancing can be dynamic or static.

Static Approach
Non-pre-emptive technique. In the case of static load balancing, previous knowledge of the system is required to balance the load and current state is not considered. It is easily implemented and behaviour prediction is easy also [9].

Dynamic Approach
In case of dynamic approach, the work distribution takes place in runtime environment, and so the present status of the system is not needed to make any decision. This approach is more efficient than static approach [10]. Usually, this algorithm is composed of three strategies, namely the transfer strategy, the location strategy and the information strategy [9].

4 Load Balancing in Cloud

Balancing the load in cloud environment is burning technologies in the current time. As discussed earlier in this paper, load balancing improves the working performance of the system by distributing the tasks among different processors in an efficient manner so that the resources are utilized fully [11]. Due to the increasing number of cloud users, balancing the load in cloud has become a critical issue. In the context of cloud computing, the core intention of load balancing is to increase accessibility of

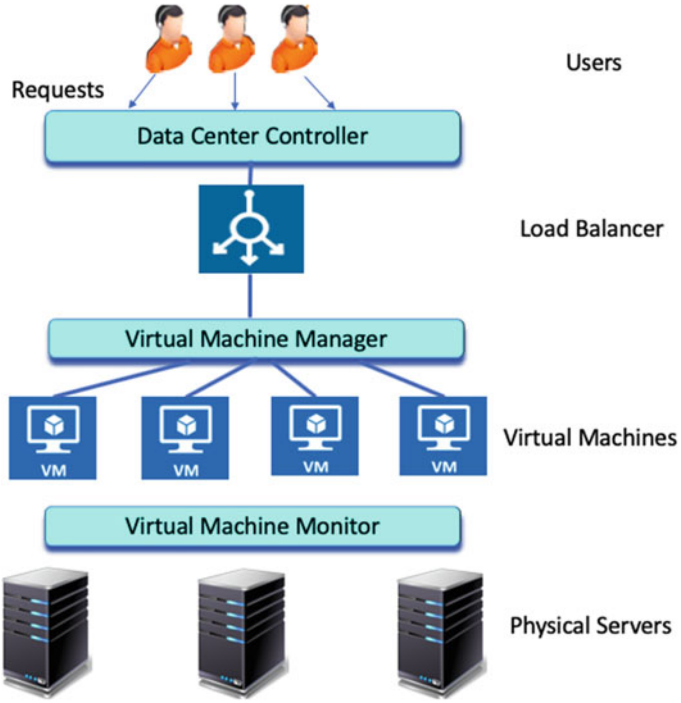


Fig. 1 Load balancing in cloud computing

resources and computing execution, present a backup plan, decrease response time, scalability and reduce overall expenses (Fig. 1).

Some of the existing load balancing algorithms in cloud environment is discussed below.

4.1 Ant Colony Optimization Technique

The ant colony optimization technique or simply ACO provides the finest resource utilization; thus, the performance of the system is enhanced which in turn increases the throughput of the system [12]. ACO is based on ant colony foraging behaviour, the ants jointly hunt for food source then combatively make use of the offered food sources to shift the food return to the shell. A pathway is made by these ants for transferring from one node to another; using the following pathways, ants subsequently go back to the food. These techniques attain efficient resource consumption, guarantee availability, a number of requests taken care by cloud are increased and response time of requests decreased [13].

4.2 Honeybee Foraging Behaviour

HFB is a technique of load balancing which is a direct implementation of natural anomaly. It is a distributed load balancing technique [14]. A nature-inspired algorithm is based on honeybee to gain private organization. It balances the load by means of neighbouring server actions. Because of the increased infrastructure range, the competence of the system is improved but throughput does not increase. This approach is suitable in an environment where distinct sorts of service are needed.

4.3 HBB-LB

A load balancing technique which besides balancing the load also keeps the track of preference of the jobs that were eliminated because of the overloaded VM's [15]. The jobs that were eliminated are considered same as honey bees. The increase in overall throughput reduces the response time of tasks. It is best suited for varied cloud computing systems. Priority is the main key factor in this technique.

4.4 INS

In this approach, IP info and active stage index parameter are used to overcome the network jamming [16]. In this algorithm, information replication and also repetition are eliminated in cloud framework. The INS algorithm has following attributes to compute the perfect fit: hash code of piece of info that is needed to formed, progress state, victimized servers location and best net pace. This algorithm omits scanning procedure of traditional backup thus decreasing the backup cost.

4.5 A2LB

The main contribution of this dynamic technique is proactive load calculations of virtual machines. In this technique, whenever the load of the virtual machine arrives at edge, load manager begins to search for the candidate vm's using other DCs. Anytime a virtual machine is burdened, the load is distributed in such a way that the accessible resources get utilized proper manner such that no virtual machine is overloaded and works properly [17].

4.6 Join-Idle-Queue

For the distribution of load in huge systems, JIQ approach is used. It can be dynamically scaled since this algorithm is extendible in nature from both directions which includes both varied processes and general arrivals. Job arrivals have no communication overheads in between the sender processes [18]. This approach has lower response timings thus manages the load very efficiently.

4.7 PLBS

A centralized procedure-based strategy. The load disproportion on the nodes is removed by boosting the response timings. Computational grid tactic is presented in this approach so that the load unevenness is reduced and resource consumption is increased. This approach works in this way, firstly it goes on hunting for best node for computation purpose for those modules concerning the execution time and then the next step is allotting the modules on specific node but keeping in view the capacity index, and hence in this way, the finest job allocation is achieved [19].

4.8 Response Time-Based LB

Response time-based load balancing approach besides being dynamic in nature and dropping the communication overhead also reduces the additional computation on every server. This approach does not need to know the existing resource of the system thus removing the requirement of unnecessary communication between the load balancer and the virtual machine [20].

4.9 SBLB for Internet Distributed Services

For lessening the response time, this approach redirects the incoming requests to the nearest server keeping in mind the server does not get congested. The time taken by tasks to go from one node to another is quite less and also the time between sending the requests and receiving their responses is smaller thus enhancing the overall efficiency of the system [21]. It is a Unuique server-based load balancing technique.

Table 1 Summary

Approach	Observation
Ant colony optimization	Gives optimal resource utilization, resulting in increase in throughput and performance
Honey bee foraging behaviour	A distributed load balancing technique that achieves load balancing using local server actions
HBB-LB	Works well with heterogeneous cloud computing systems. The increase in overall throughput reduces the response time of tasks in this technique
INS	Information replication and repetition is eliminated
A2LB	Proactive load calculations of virtual machines
Join-idle-queue	A distributed load balancing technique in large systems. This technique efficiently reduces the load without increasing the reaction time
SBLB for Internet distributed services	A technique that redirects requests to nearest server thus limiting service reply time
PLBS	A centralized practice for load balancing multiple tasks where each application is symbolized using direct acyclic graph which has communication requirements
Response time-based LB	Dynamic and also cuts down the communication and extra computation on all servers
Cloud server optimization	A threshold-based contrast and balance approach

4.10 Cloud Server Optimization

This approach is basically a dynamic contrast and balance technique. It lays emphasis on various host machines that need to be switched on so that the cost of cloud services is reduced thus serving the purpose effective utilization of resources. A superior cloud framework is used by this technique at host system level [22] (Tables 1 and 2).

5 Conclusion

After reviewing the existing load balancing techniques above, we came up with several research concerns and breaches which can be treated for further contribution in load balancing. Most of the techniques discussed above focuses on different parameters like scalability, throughput, overhead, etc. but very few techniques focused on power saving and energy consumption issues. Thus, we need to present a load balancing approach that targets these two parameters and thus helps us to tackle high energy consumption and carbon emission rates.

Table 2 Comparison table

Approach	Performance	Throughput	Overhead	Scalability	Resource utilization	Fault tolerance
Ant colony optimization	Low	Low	✓	×	Low	×
Honey bee foraging behaviour	Low	Low	×	×	High	×
HBB-LB	Low	High	×	×	Low	×
INS	High	Low	×	×	Low	✓
A2LB	High	Low	×	✓	High	×
Join-idle-queue	High	Low	✓	×	Low	×
SBLB for Internet distributed services	High	Low	×	✓	Low	×
PLBS	High	Low	×	✓	High	×
Cloud server optimization	Low	Low	×	×	High	×

References

1. Alali FA, Yeh CL (2012) Cloud computing: overview and risk analysis. J Inf Syst 26(2):13–33
2. Harris T (2010) Cloud computing—an overview, Whitepaper, vol 462. Torry Harris Business Solutions, pp 1–5
3. Shyam P, Dheeraj R, Jain P (2012) A survey paper on cloud computing. In: 2012 second international conference on advanced computing and communication technologies. IEEE
4. Nazir Mohsin (2012) Cloud computing: overview and current research challenges. IOSR J Comput Eng 8(1):14–22
5. Prasad MR, Naik RL, Bapuji V (2013) Cloud computing: research issues and implications. Inter J Cloud Comput Serv Sci 2(2):134
6. Deepa T, Cheelu D (2017) A comparative study of static and dynamic load balancing algorithms in cloud computing. In: 2017 international conference on energy, communication, data analytics and soft computing (ICECDS). IEEE
7. Godha R, Prateek S (2014) Load balancing in a network. Inter J Sci Res Publ 4(10)
8. Katyal M, Mishra A (2014). A comparative study of load balancing algorithms in cloud computing environment. arXiv preprint. arXiv:1403.6918
9. Hamadah S (2017) A survey: a comprehensive study of static, dynamic and hybrid load balancing algorithms. IRACST-Inter J Comput Sci Inform Technol Secur (IJCSITS) 7(2):2249–9555
10. Begum S, Prashanth CSR (2013) Investigational study of 7 effective schemes of load balancing in cloud computing. Inter J Comput Sci Issues (IJCSI) 10(6):276
11. Kherani FF, Vania J (2014) Load balancing in cloud computing. Inter J Eng Dev Res 2(1)
12. Gupta E, Deshpande V (2014) A technique based on ant colony optimization for load balancing in cloud data center. In: 2014 international conference on information technology. IEEE
13. Ahmad MO, Khan RZ (2018) Load balancing tools and techniques in cloud computing: a systematic review. Advances in computer and computational sciences. Springer, Singapore, pp 181–195
14. Randles M, Lamb D, Taleb-Bendiab A (2010) A comparative study into distributed load balancing algorithms for cloud computing. In: 2010 IEEE 24th international conference on advanced information networking and applications workshops. IEEE

15. Krishna PV (2013) Honey bee behavior inspired load balancing of tasks in cloud computing environments. Appl Soft Comput 13(5):2292–2303
16. Wu TY et al (2012) Dynamic load balancing mechanism based on cloud storage. In: 2012 computing, communications and applications conference. IEEE
17. Singh A, Juneja D, Malhotra M (2015) Autonomous agent based load balancing algorithm in cloud computing. Procedia Comput Sci 45:832–841
18. Lu Y et al (2011) Join-Idle-Queue: a novel load balancing algorithm for dynamically scalable web services. Perform Eval 68(11):1056–1071
19. Shahid M, Raza Z (2014) A precedence based load balancing strategy for batch of DAGs for computational grid. In: 2014 international conference on contemporary computing and informatics (IC3I). IEEE
20. Sharma A, Peddoju SK (2014) Response time based load balancing in cloud computing. In: 2014 international conference on control, instrumentation, communication and computational technologies (ICCICCT). IEEE
21. Nakai AM, Madeira E, Buzato LE (2011) Load balancing for internet distributed services using limited redirection rates. In: 2011 5th Latin-American symposium on dependable computing. IEEE
22. Sahu Y, Pateriya RK, Gupta RK (2013) Cloud server optimization with load balancing and green computing techniques using dynamic compare and balance algorithm. In: 2013 5th international conference and computational intelligence and communication networks. IEEE

Logical Clustering of Similar Vertices in Complex Real-World Networks

Md A. Rahman and Natarajan Meghanathan

Abstract We show that vertices part of a physical cluster (determined per the edges that connect the vertices) in a complex real-world network need not be similar on the basis of the values incurred for node-level metrics (say, centrality metrics). We adapt a recently proposed approach (based on unit-disk graphs) to determine logical clusters comprising of vertices of similar values for node-level metrics, but need not be physically connected to each other. We use the Louvain algorithm to determine both the physical and logical clusters on the respective graphs. We employ the Silhouette Index measure to evaluate the similarity of the vertices in the physical and logical clusters. When tested on a suite of 50 social and biological network graphs on the basis of neighborhood and/or shortest path-driven centrality metrics, we observe the Silhouette Index of the logical clusters to be significantly larger than that of the physical clusters.

Keywords Logical clusters · Physical clusters · Centrality metrics · Silhouette index · Complex network analysis

1 Introduction

Clustering (also referred to as community detection) is a critical component of complex network analysis. In the traditional sense, a cluster (community) in a network comprises a group of vertices that are more connected to each other than to vertices outside the cluster [1]. We refer to such clusters as physical clusters. Several clustering algorithms (like Girvan–Newman algorithm [2], Louvain algorithm [3], and neighborhood-overlap-based greedy algorithm [4]) are available in the literature to determine physical clusters of vertices of larger modularity. A physical cluster

M. A. Rahman · N. Meghanathan (✉)
Computer Science, Jackson State University, Jackson, MS 39217, USA
e-mail: natarajan.meghanathan@jsums.edu; nmeghanathan@jsums.edu

M. A. Rahman
e-mail: md.a.rahman@students.jsums.edu

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_86

is considered to be more modular [1] if it has high intra-cluster density and low inter-cluster density.

With the objective of maximizing edge-based intra-cluster density, it is difficult to expect a clustering algorithm to group vertices that are similar to each other. Similarity of vertices is typically assessed on the basis of node-level metrics that could be topology or domain-driven. Centrality metrics are classical examples for topology-based metrics that quantify the extent to which a node is important on the basis of its location in the network [1]. The centrality metrics are used as the node-level metrics for our analysis in this paper. We consider the following centrality metrics: neighborhood-driven degree (DEG) [1] and eigenvector (EVC) [5] centrality metrics and the shortest path-driven betweenness (BWC) [6, 7] and closeness (CLC) centrality metrics [8, 9]. For more details on the centrality metrics, the interested reader is referred to [10]. The analysis presented in this paper could be seamlessly extended to any combination of domain-driven or topology-driven metrics as well.

In Fig. 1, we show a motivating example graph wherein the tuple next to a vertex represents the degree (DEG) and eigenvector centralities (EVC) of the vertex. Any well-known clustering algorithm in the literature would determine the two physical clusters in sub Fig. 1a that have high modularity (larger intra-cluster density and lower inter-cluster density). However, a closer look at the tuples for the vertices within a physical cluster would indicate less similarity among the vertices on the basis of their DEG and EVC values. On the other hand, in sub Fig. 1b, we show two clusters each of which comprises vertices that are exactly similar on the basis of their DEG and EVC values. The two clusters in sub Fig. 1b are not very modular (the inter-cluster density is even larger than the intra-cluster density), but each of these clusters would be more cohesive (i.e., comprised of vertices that are similar) on the basis of their DEG and EVC values.

We propose the following approach (more details are in Sect. 2) to determine such cohesive clusters of similar vertices in real-world network graphs. We distribute the vertices in a coordinate system whose coordinates are the normalized values of the node-level (centrality) metrics of the vertices. For such a logical topology,

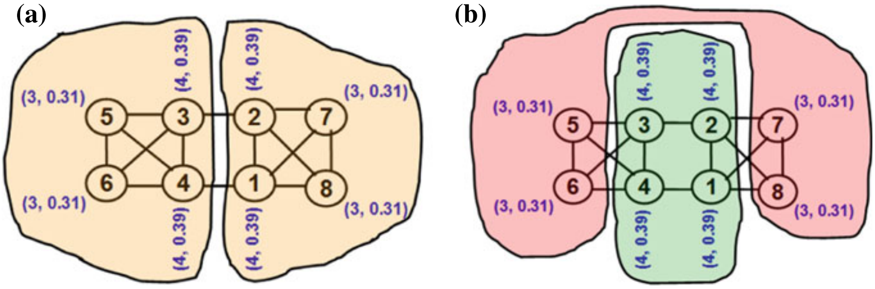


Fig. 1 Example graph: physical modular clusters versus logical clusters of similar vertices. **a** Physical clusters (larger intra-cluster density, but lower vertex similarity). **b** Logical clusters (lower intra-cluster density, but larger vertex similarity)

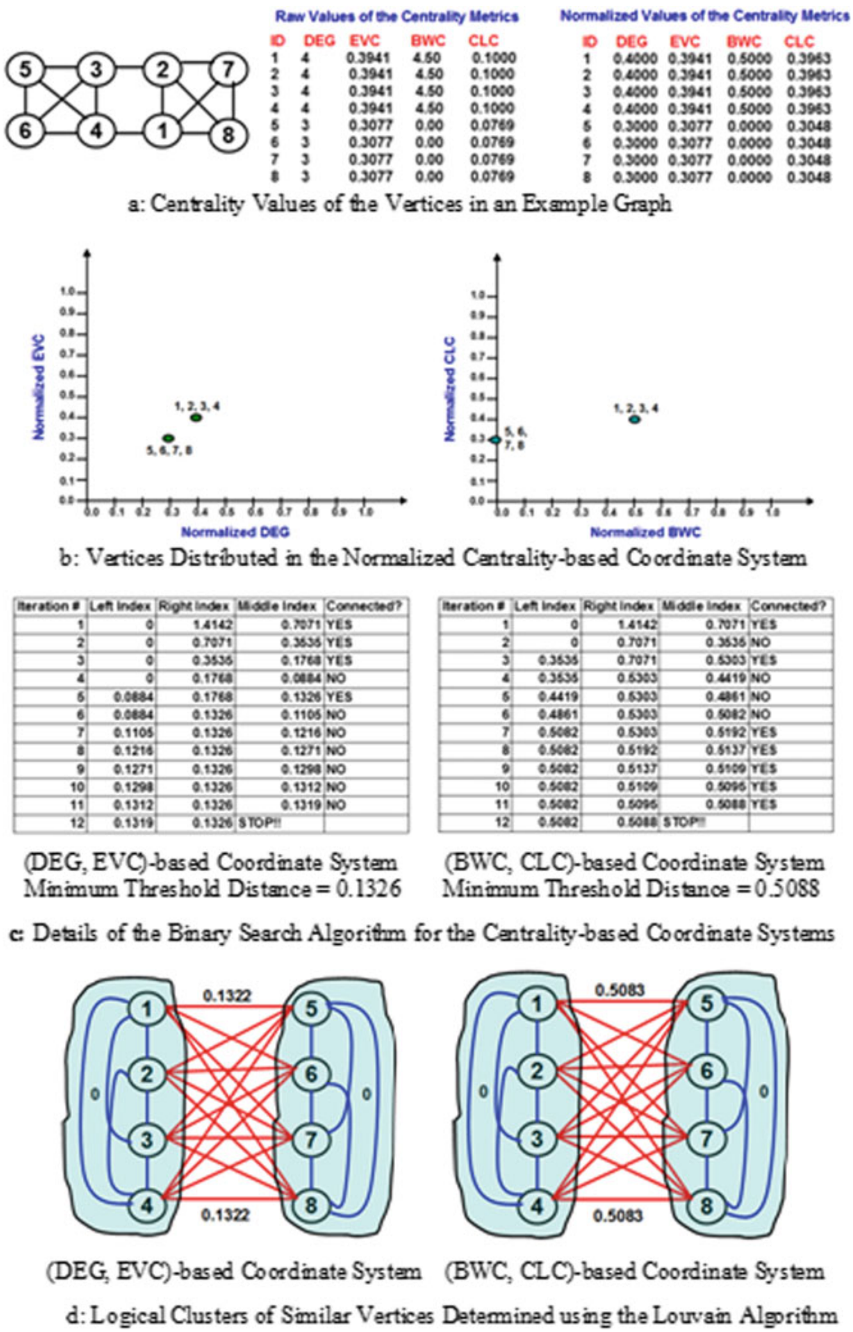
we iteratively attempt to connect the vertices together (an edge exists between two vertices if the Euclidean distance between their normalized coordinate values is within a threshold) in the form of a unit-disk graph. We use a binary search approach to identify the minimum value for the threshold distance that would connect together the vertices in the unit-disk graph. We run the Louvain clustering algorithm [3] on the connected unit-disk graph to determine one or more (logical) clusters whose member vertices are more similar compared to the vertices in the physical clusters obtained by running the Louvain algorithm on the corresponding real-world network graph. We use the Silhouette Index [11] measure to assess the similarity of the vertices in the logical clusters vis-a-vis the physical clusters with respect to the centrality metrics considered. In a recent work [12], we have successfully used the unit-disk graph and binary search-based approach to quantify the similarity between any two vertices in a network (in the form of a metric called the *node similarity index*). Our hypothesis in this research is that for a set of centrality metrics, the Silhouette Index of the logical clusters would be larger than the Silhouette Index of the physical clusters.

The rest of the paper is organized as follows: In Sect. 2, we explain the approach to determine logical clusters of similar vertices on the basis of node-level (centrality) metrics. In Sect. 3, we explain the formulation for the Silhouette Index measure. In Sect. 4, we test our hypothesis on a suite of 25 biological networks and 25 social networks on the basis of three sets of centrality metrics: (DEG, EVC); (BWC, CLC), and (DEG, EVC, BWC, CLC). We present and analyze the Silhouette Index results for the physical clusters and logical clusters obtained for the different combinations of centrality metrics. Section 5 presents our conclusions and outline plans for future work.

2 Logical Clusters of Similar Vertices

We describe the sequence of steps (see Fig. 2) involved in determining logical clusters of similar vertices (for k centrality metrics) in a real-world network graph.

Step (i): Construction of a Logical Topology: Let the number of centrality metrics considered for logical clustering of a real-world network graph be k. To get started, for each of the k metrics, we determine their raw centrality values (see Fig. 2a) and then independently normalize them (using the square root of the sum of the squares of the raw values). Following this, we build a logical topology (k-dimensional coordinate system) of the vertices wherein the coordinates of a vertex are its normalized centrality values (ranging from 0 to 1). See Fig. 2b.
Step (ii): Binary Search Algorithm to Deduce a Connected Unit-Disk Graph: We attempt to deduce (through a sequence of iterations) a unit-disk graph that would connect all the vertices in the logical topology at a minimum threshold distance for an edge to exist. For a set of k centrality metrics, the threshold could range from (0,…, $\sqrt{k}$); if the threshold distance is $\sqrt{k}$, we will have a unit-disk graph that is sure to be connected (completely connected indeed!), but not connected at a threshold



Raw Values of the Centrality Metrics

ID	DEG	EVC	BWC	CLC
1	4	0.3941	4.50	0.1000
2	4	0.3941	4.50	0.1000
3	4	0.3941	4.50	0.1000
4	4	0.3941	4.50	0.1000
5	3	0.3077	0.00	0.0769
6	3	0.3077	0.00	0.0769
7	3	0.3077	0.00	0.0769
8	3	0.3077	0.00	0.0769

Normalized Values of the Centrality Metrics

ID	DEG	EVC	BWC	CLC
1	0.4000	0.3941	0.5000	0.3963
2	0.4000	0.3941	0.5000	0.3963
3	0.4000	0.3941	0.5000	0.3963
4	0.4000	0.3941	0.5000	0.3963
5	0.3000	0.3077	0.0000	0.3048
6	0.3000	0.3077	0.0000	0.3048
7	0.3000	0.3077	0.0000	0.3048
8	0.3000	0.3077	0.0000	0.3048

a: Centrality Values of the Vertices in an Example Graph

b: Vertices Distributed in the Normalized Centrality-based Coordinate System

Iteration #	Left Index	Right Index	Middle Index	Connected?
1	0	1.4142	0.7071	YES
2	0	0.7071	0.3535	YES
3	0	0.3535	0.1768	YES
4	0	0.1768	0.0884	NO
5	0.0884	0.1768	0.1326	YES
6	0.0884	0.1326	0.1105	NO
7	0.1105	0.1326	0.1216	NO
8	0.1216	0.1326	0.1271	NO
9	0.1271	0.1326	0.1298	NO
10	0.1298	0.1326	0.1312	NO
11	0.1312	0.1326	0.1319	NO
12	0.1319	0.1326	STOP!!	

(DEG, EVC)-based Coordinate System
Minimum Threshold Distance = 0.1326

Iteration #	Left Index	Right Index	Middle Index	Connected?
1	0	1.4142	0.7071	YES
2	0	0.7071	0.3535	NO
3	0.3535	0.7071	0.5303	YES
4	0.3535	0.5303	0.4419	NO
5	0.4419	0.5303	0.4861	NO
6	0.4861	0.5303	0.5082	NO
7	0.5082	0.5303	0.5192	YES
8	0.5082	0.5192	0.5137	YES
9	0.5082	0.5137	0.5109	YES
10	0.5082	0.5109	0.5095	YES
11	0.5082	0.5095	0.5088	YES
12	0.5082	0.5088	STOP!!	

(BWC, CLC)-based Coordinate System
Minimum Threshold Distance = 0.5088

c: Details of the Binary Search Algorithm for the Centrality-based Coordinate Systems

(DEG, EVC)-based Coordinate System (BWC, CLC)-based Coordinate System

d: Logical Clusters of Similar Vertices Determined using the Louvain Algorithm

Fig. 2 Example to illustrate the computation of the logical clusters and their evaluation

distance of 0 (unless all the vertices are co-located). We use this observation as the basis to run a binary search algorithm to determine the minimum possible value for the threshold distance to obtain a connected unit-disk graph [12]. We start the binary search algorithm with the left index set to 0 and the right index set to $\sqrt{k}$ and go through a sequence of iterations (see Fig. 2c).

Across all the iterations, the following invariant is maintained: If the threshold distance value corresponds to the left index, the unit-disk graph is not connected; if the threshold distance value corresponds to the right index, the unit-disk graph is connected. In each iteration, we first determine the middle index as the average of the left index and right index, and seek to construct a unit-disk graph with the threshold distance value corresponding to the middle index. If such a unit-disk graph is connected, we set the right index to the value of the middle index; otherwise, we set the left index to the value of the middle index. We continue the iterations until the right index and left index differ not more than a cutoff parameter ($\in$). We use $\in = 0.001$ for all the analysis conducted in this paper. We set the minimum threshold distance to correspond to the value of the right index in the last iteration of the algorithm.

Step (iii): Logical Clustering of the Connected Unit-Disk Graph: On the connected unit-disk graph obtained for a minimum threshold distance, we run the Louvain community detection algorithm [3] to determine (logical) clusters of vertices that have a larger intra-cluster density (and a lower inter-cluster density) in the unit-disk graph. The vertices within a logical cluster are expected to be more similar to each other. The Louvain algorithm (a hierarchical community detection algorithm) is designed to identify highly modular communities. To determine the logical clusters using the Louvain algorithm, the weight of an edge in the connected unit-disk graph is the Euclidean distance between their corresponding normalized coordinate values. Note that the edge weights for the real-world network graphs are "1" when we run the Louvain algorithm to determine the physical clusters.

3 Silhouette Index

We use the Silhouette Index [11] measure (ranges from -1 to 1) to evaluate the extent of similarity among the vertices of the physical clusters and logical clusters with respect to the normalized centrality values of the vertices. The larger the values for the Silhouette Index for a cluster, the more similar are the vertices within the cluster with respect to the centrality metrics in consideration. The Silhouette Index for a cluster is the average of the Silhouette Index values of its member vertices. The Silhouette Index for a network is the weighted average of the Silhouette Index values of its clusters. The Silhouette Index for a vertex i in a cluster C_k is calculated as per formulation (1). Here, $\overline{d_{i,\min}}$ is the minimum of the average of the Euclidean distances for vertex i to vertices in the other clusters; $\overline{d_{i,Ck}}$ represents the average of the Euclidean distances for vertex i to vertices in its own cluster. A negative Silhouette Index for a vertex is an indication that the vertex is not in the appropriate cluster.

A negative Silhouette Index for a cluster is an indication that its member vertices should have been in other cluster(s) for better cohesiveness.

$$\text{Silhouette Index}(i) = \frac{\overline{d_{i,\min}} - \overline{d_{i,Ck}}}{\max\{\overline{d_{i,\min}}, \overline{d_{i,Ck}}\}} \quad (1)$$

4 Evaluation on Real-World Networks

In this section, we test our hypothesis on a suite of 25 biological network graphs and 25 social network graphs of diverse degree distributions and present the results of the Silhouette Index measure evaluated for the physical clusters and logical clusters obtained by running the Louvain algorithm (per the approaches described in the earlier sections). The biological networks analyzed are either gene–gene interaction networks, protein–protein interaction networks, interactions between different animal species in a particular area, etc. The social networks analyzed comprise acquaintance networks that capture the association between two users in a social network over a certain time period and friendship networks for which no such time period is used to capture association between two users.

In Fig. 3, we visually present some of the fundamental statistical information for the biological networks and social networks (for more details, see [12]). The number of nodes in the biological networks ranges from 62 to 2,640 with a median of 813. The number of nodes in the social networks ranges from 22 to 1,882 with a median of 75. The spectral radius ratio for node degree ($\lambda_{\mathrm{sp}} \geq 1$) [13] for a network graph is the ratio of the principal eigenvalue [5] of the adjacency matrix for the graph and the average node degree; the larger the λ_{sp} value, the larger the variation in node degree. The edge density ($0 \leq \rho_{\mathrm{edge}} \leq 1$) is calculated as the ratio of the actual number of edges in the network and the maximum possible number of edges in the network (which is $N(N-1)/2$ for a network of N nodes). The biological networks are characteristic of having larger λ_{sp} values and lower ρ_{edge} values; on the other hand, social networks are characteristic of having smaller λ_{sp} values and larger ρ_{edge} values. For more details on the individual real-world networks analyzed in each of these domains, the interested reader is referred to [12].

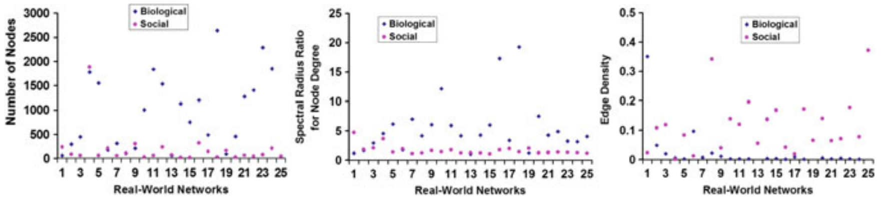
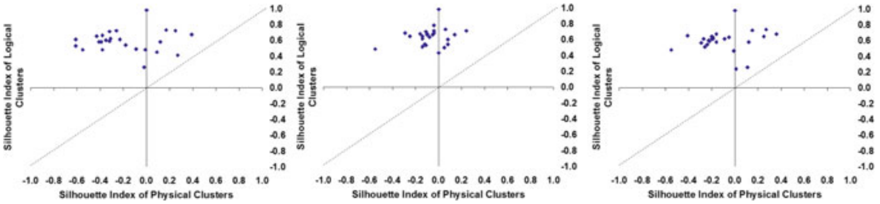


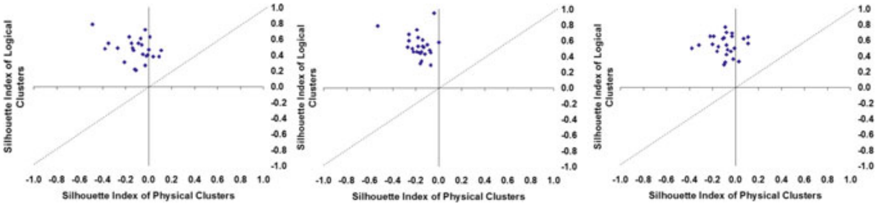
Fig. 3 Statistics for the biological and social networks

In Figs. 4 and 5, we present and visually compare the Silhouette Index values for the physical vs. logical clusters on the basis of the neighborhood-based (DEG, EVC); the shortest path-based (BWC, CLC), and all the four centrality metrics together (DEG, EVC, BWC, CLC). We observe all the data points to be above the dotted diagonal line, indicating that the Silhouette Index values for the logical clusters for all the real-world networks are appreciably larger than the Silhouette Index values for the physical clusters. For each coordinate system and for each network category, we measure (see Fig. 6a for a comparative bar chart) the average of the difference in the Silhouette Index values for the logical clusters versus physical clusters. We observe the biological networks to incur larger average difference in the Silhouette Index values for all the three coordinate systems. The (DEG, EVC) coordinate system incurs, respectively, the lowest (for social networks) and largest (for biological networks) values for the average difference in the Silhouette Indexes for the logical versus physical clusters. We also measure the median (see Fig. 6b for a comparative bar chart) of the Silhouette Index values for the physical clusters versus logical clusters. Through Figs. 4,5, and 6, we observe the Silhouette Index values for the physical (logical) clusters in the biological networks to be relatively lower (larger) than those in the social networks.



(DEG, EVC) (BWC, CLC) (DEG, EVC, BWC, CLC)

Fig. 4 Biological networks: Silhouette Index values for the physical versus logical clusters



(DEG, EVC) (BWC, CLC) (DEG, EVC, BWC, CLC)

Fig. 5 Social networks: Silhouette Index values for the physical versus logical clusters

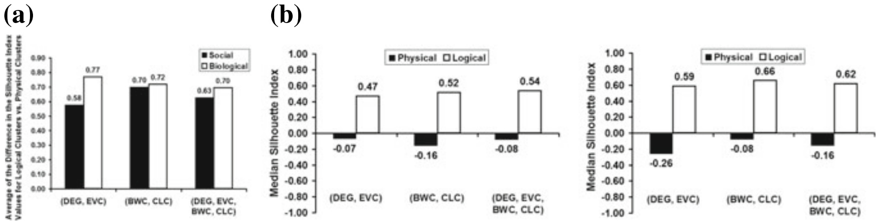


Fig. 6 Statistical comparison of the Silhouette Index values. **a** Avg. difference in the social networks biological networks Silhouette Index values. **b** Median of the Silhouette Index values

5 Conclusions

We show that logical clusters of vertices could be more cohesive with respect to node-level centrality metrics compared to physical clusters of vertices in complex real-world network graphs. In this pursuit, we adapt a recently proposed unit-disk graph approach (for node similarity assessment) [12] to determine such logical clusters of similar vertices. We applied the approach on a suite of 25 biological networks and 25 social networks and evaluated the extent of similarity of the vertices in the logical clusters versus physical clusters using the Silhouette Index measure with respect to three combinations of centrality metrics (DEG, EVC), (BWC, CLC), and (DEG, EVC, BWC, CLC). For each combination, we observe all the 50 real-world network graphs to incur significantly larger Silhouette Index values for the logical clusters compared to the physical clusters. We observe the biological networks to show a relatively larger difference in the Silhouette Index values between the logical clusters and physical clusters. Likewise, the (BWC, CLC) coordinate system has been observed to incur relatively larger Silhouette Index values for several real-world networks. In future, we plan to extend the unit-disk graph approach for outlier detection in complex networks and large datasets.

References

1. Newman MEJ (2010) Networks: an introduction, 1st edn. Oxford University Press, Oxford, UK
2. Girvan M, Newman MEJ (2002) Community structure in social and biological networks. Proc Natl Acad Sci USA 99(12):7821–7826
3. Blondel VD, Guillaume JL, Lambiotte R, Lefebvre E (2008) Fast unfolding of communities in large networks. J Stat Mech Theor Exp P10008:1–11
4. Meghanathan N (2016) A greedy algorithm for neighborhood overlap-based community detection. Algorithms 9(1, 8):1–26
5. Bonacich P (1987) Power and centrality: a Family of measures. Am J Sociol 92(5):1170–1182
6. Freeman L (1977) A set of measures of centrality based on betweenness. Sociometry 40(1):35–41
7. Brandes U (2001) A faster algorithm for betweenness centrality. J Math Sociol 25(2):163–177

8. Freeman L (1979) Centrality in social networks: conceptual clarification. Soc Netw 1(3):215–239
9. Cormen TH, Leiserson CE, Rivest RL, Stein C (2009) Introduction to algorithms. MIT Press, Cambridge
10. Meghanathan N (2016) Assortativity analysis of real-world network graphs based on centrality metrics. Comput Inform Sci 9(3):7–25
11. Rousseeuw PJ (1987) Silhouettes: a graphical aid to the interpretation and validation of cluster analysis. Comput Appl Math 20:53–65
12. Meghanathan N (2019) Unit disk graph-based node similarity index for complex network analysis. Complexity. Article ID 6871874, p 22
13. Meghanathan N (2014) Spectral radius as a measure of variation in node degree for complex network graphs. In: The 3rd international conference on digital contents and applications, Hainan, pp 30–33

Capacity Enhancement Using Delay-Sensitive Protocol in MANETs

V. Sivakumar, J. Kanimozhi, B. Keerthana and R. Muthulakshmi

Abstract In wireless modulation technologies, it has advanced frequency modulation. It is capable of performing in Quality of Service (Qos) for utilizing the scope of mobile ad hoc. It is measured only for calculating the ratio between two nodes. It will form an implementation of single-hop delay. After that, to construct the multicast tree for real-time in delay-sensitive tree, proposed model has been established in MANET. While increasing a network in capacity, this proposed multicast protocol can be minimized in the host and in a particular time the transmission node can block the entire neighboring node so that there is no interrupt and wastage of data that can be occurred in the data for properly adjusting data rates. Simulating results provides lot of accuracy. It induces the expected result at the end of this paper.

Keywords Multicast protocol · Delay-sensitive · Qos · Multi-rate · Capacity enhancement · One-hop delay

1 Introduction

In wireless network, the node moves randomly, and it can be able to communicate with each other by multi-hop transmission. These transmissions would not have a fixed infrastructure. And they do not have utilized centralized administration. Direct transmission of packet is occurred in the initial node to its destination [1]. Multicast

V. Sivakumar · J. Kanimozhi (✉) · B. Keerthana · R. Muthulakshmi
Department of IT, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India
e-mail: kanijoh25@gmail.com

V. Sivakumar
e-mail: sivcse45@gmail.com

B. Keerthana
e-mail: bkeerthan1998@gmail.com

R. Muthulakshmi
e-mail: muthukrishna9816@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_87

forms the cluster in communication; it transmits data packet in sharing the information from source to destination. Multicast tree is efficient for sending same packets. For a specified condition, multicast tree should request for delay requirements, where multicast protocol is in delay-sensitive state. When compared to the predefine value, these end-to-end delays are smaller [2]. For building a tree to find out the shortest path in the given range, they form a large amount of transmission from one part to another part, and delay is nothing but it transmits node from source to destination, it means to its neighboring node.

A maximum cost can be transmitted by transmitter to send successful packets, and it is dependent on the SINR and it is received. It is always directly proportional to the transmission range. If a transmitter transmits, then the receiver has to perceive high in SINR [3]. Most probably, the delay can be found out by the process of hopping data from one node to another node. In order to have a complete transmission of packet, it also requires short range in transmitter. Often in multi-rate MANETs, host may vary in the neighborhood; later it is more difficult for the estimate of delay in MANET. If a transmission occurs, then the neighborhood is blocked in MANETs. They share channels' ratio with their neighbors. If we design Quality of Service (QoS) for a MANET, its neighboring data will be maintained for the estimation of resource, and it is consumed by constructed QoS route to avoid violation in resource from other neighbors. This Quality of Service is able to utilize only the limited wireless resources efficiently.

Previously, multicasting protocols have been designed only for single-rate MANETs or multi-rate. CEDAR and some other algorithm are neither guaranteed by bandwidth, and if it begins to send its packet to nearest node, then the carrier senses to block the neighbor [4]. HRP or HMRP is pointed, for the failing transmitters while they admit the flow. It indicates that it is saturated in network traffic. They can be avoided by two routing algorithms, namely hidden route problem (HRP) or from the hidden multicast route problem (HMRP); it fails to collect information from the neighboring resource [5]. L. Chen and W. Heinzelman have founded how to be provided.

Bandwidth guarantee in QoS. C. C. Hu has been proposed about the delay-sensitive multi-rate protocol. From IEEE system journals, we have read about the single or multi-rate MANETs, when a host starts its transmission from its neighbor to another if the former is within the transmission range of latter.

If the traffic occurs in network, then the bandwidth or requirements in delay performance cannot be satisfied. Unlike other specifics, we use the neighboring transmission to denote the neighbor [6]. Therefore, on-demand routing is resulted in delay estimation method.

To calculate the shortest path and find out the implementation of multicast tree, we have already studied about the existing system how to calculate the delay-sensitive routing protocol in C. C. Hu. This proposed project is used to establish a lot of hopping nodes in the Quality of Service. They would eliminate the hidden problem and similarly they will eliminate the multicast neighbors [7]. There is no reply in late simulation of packet. In existing system, it can be used to exit the unwanted data and calculate multiple packets. It is greater and has large amount of valued data for transmitting the packets. In packet forwarding, it senses and forwards more packets, when it forwards neighbors should be blocked. If the forwarders increases, network performance will go worse.

These systems will tend to minimizing the total transaction of information from the particular node to its destinated node [8]. When choosing the neighboring data packets in multicasting route, it uses single hopping system. Due to this process, the capacity has been increased.

2 Related Work

The Quality of service (QoS) is mainly used in multicasting protocol in single-rate MANETs. The transmission delay can be trying to reduce the protocol. In delay-sensitive multicast tree, they are not delay sensitive, for failing the estimate from the final late coming nodes [9]. If they do not eliminate the hidden multicast, it will suffer from some missing protocol from HMRP. It cannot construct the simultaneous routes.

The range of node can be varied due to its shortest path in algorithm [10]. From this protocol, from given source which has been detected within a range, the capacity in wireless network has been increased. According to delay in neighboring node, a distributed routing protocol can be avoided in hidden problems, and it accepts the requests from neighbor to process the delay control [11].

The simulation of packet can flow the request from every bandwidth in the literature. Markov-modulated Poisson process will be used in the estimation of average delays. While analyzing the channel, most of the conditions were not assigned as parameters in the traffic flows [11]. Estimates of one hop delay can be calculated by using approximate model.

In one ratio analysis, the delay can be used to find out the shortest path within a given range, and they can be able to modify the statement of data with or without the permission of the author. But the irrelevant and incomplete data can be strictly eliminated to make the transaction faster and easier for sender to receiver process [12].

Most probably, all the nodes are sensitive toward the host, and there would not be several attempts or increase in channel that will happen. Due to this existing system, our proposed system gives lot of changes with good accuracy report which has been shown in X-graph.

3 Protocol

The protocol plays a major role in this multi-rate MANET. This system is distributed in the origin data. DSM has multiple attempts that can be used as algorithm to find out the hidden problem with the definitions in MAC. For packet transmission, single physical channel should be available, and every host perceived can be able to monitor

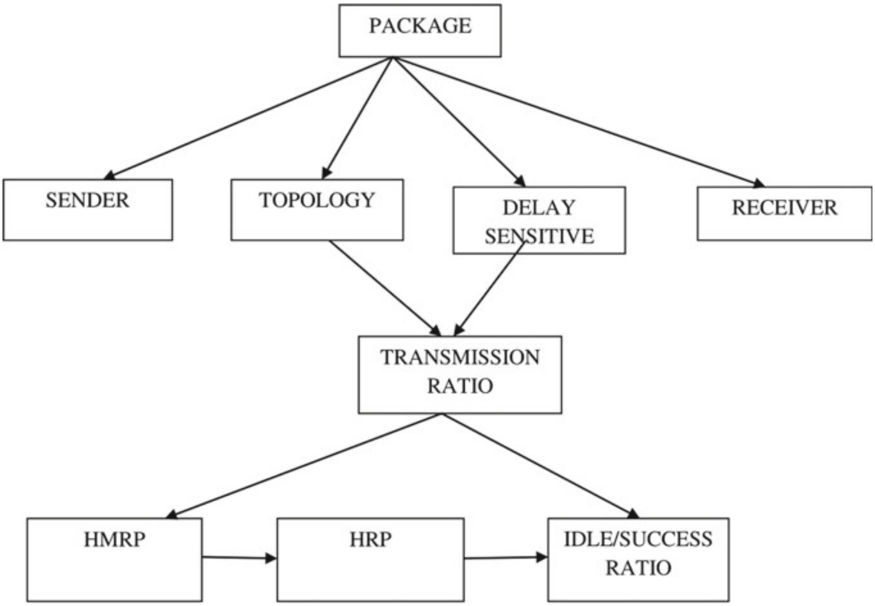


Fig. 1 Architecture diagram

the channel whether it is idle or busy. To sense the message from host with the base rate, here we use MANET. For example, 1 Mb/s is the base rate. In the estimation of delay, it senses the algorithm which uses default method in multicasting the data for deriving all the busy ratio in threshold.

Figure 1 explains about the flow of packet and transmission of data from the source to destination. When they started to share the data, host gets blocked by the route.

3.1 Neighbor Host

In multi-rate MANETs has to identify in order to its r_p—neighbors and from multi-rate MANETs, every neighbors require to have a construction of two tables, named with one-hop neighbors and the two-hop neighboring. $p_{i,j}$ gets transmitted from source host of H_j to H_i. It allows several request flow and eliminates using HMRP [13]. Later, it gets changed by the wireless network of signal has been indicated. An auto-rate algorithm is used in receiver side, and rollback algorithm is used in transmitter side. In Fig. 2, this proposed system explains about the generation of node with the transmission, and HMRP and HRP have been blocked.

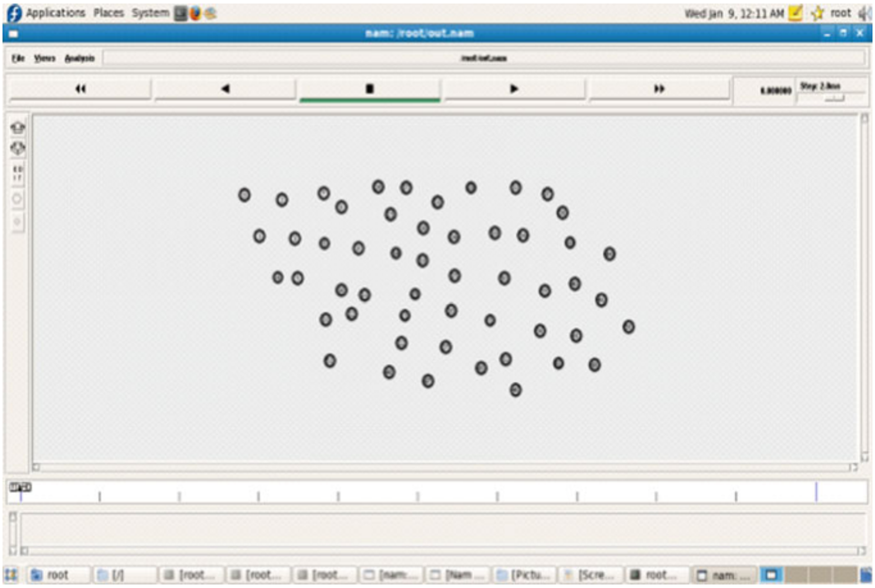


Fig. 2 Creation of nodes

3.2 Construction of Multicast Tree

In this existing system, delay can be reduced for low request when implementing the single node. In order to take the proposed system, weight can be assigned with its transmission of packets and its sum when blocking its overall transmission that can be hosted. If the resources can be hosted in consumed multicast, they have more flows in requesting the capacity of network enhancement.

3.3 Methodology of Implementing Trees

To construct trees, we use heuristic algorithm from proposed multi-rate MANETs. Trade-off range has been used in data rate transmission range. To participate in forwarding trees, higher data rates have been selected in packets. When carrier starts to transmit the packet, the entire neighbor has been blocked. Due to this process, the network degrades with its performance if it has large forwarders in number. In this algorithm, their data rate can be changed.

In delay-sensitive multicast tree, the neighbors are used to sense the forwarders into account. This proposed algorithm has been explained in the above section. A multicast tree is used to invoke iteratively. To construct multicast tree, the basic procedure is used. For specifying the destination of delay-sensitive to construction. In order to consume the resource in reduced construction tree, the main feature is to reduce the total transmission time and minimize the forwarders, and then it blocks the host using blocking time.

In the above section, we explained in-depth and its illustrative example as provided below. Implementation issues can be addressed. Implementation of tree construction in variables can be used. In tree multicast current collect to the current multicast tree, the destination was not connected in tree of multicast [14]. Here, F is used to collect the forwarders. F is represented in forwarders, and R is used in F. D is set as transmission.

There are four topologies, namely

1. Known Topology (singlecast)
2. Unknown Topology (singlecast)
3. Known Topology (multicast)
4. Unknown Topology (multicast)

It minimizes the weight route, in Dijkstras algorithm to find out the nearest path (shortest). It is graphed from the weight graph. Dijkstras algorithm is used for constructing the shortest path which is equal to its weight from source vertex to its other vertices. Multi-rate representation of directed graph in MANET is conveniently used in vertex graph.

Is used as vertex and arch is used as unique element.

Delay-sensitive multicast is temporarily used in maintaining the multicast tree, point to point is used from source to destination which transmits packets from point to point without loss in data. It does not request the flow and delay have been violated. Multicast tree is finally used to avoid the HMRP and HRP.

Especially, *Delay_Sensitive_Route* is being iteratively hosted in appending delay-sensitive routes. If a host is violated in appending route, then it can be temporarily violated delay in multicast for all the ongoing flows.

It may exceed the route delay requirement from one end to another end. In following description, the above mentioned delay requirement can be hosted.

Implementation Issues: *When* recall the neighbors and carrier sense, it is mentioned with some denotations like r_p—neighbors and r_p—carrier sense neighbors. h_i can be estimated. When r_p is used for the nd, later it is stored in neighbors in h data rate. To identify the channel of busy/idle ratio, it is necessary to implement the hop delay of one to one node. First three nodes are stored in hop delays, and the residual delay happens due to the ongoing flow passes.

4 Performance Evaluation

Implementation can be done or perfomed by the ns2 tool. Every evaluation has been required to transmit the channel in performance. The two-ray ground model is adopted for predicting the signaling receiving power from the ground has been considered as a reflection. Hence, in receiving the signal power and transmitting, it in a distance of attenuated as $1/d^2$, where d is represented as the gap in center transmitter and receiver. From CBR traffic, its flows can be injected from the sources to its destination in the network, and every host is provided for a MAC FIFO queue which is arranged in the 50th node [15].

In this existing system, we derived in delay sensitive. Choose delay in particular node to simulation which can be conducted for preference operation using multiple rates. Several operations cannot able to perform at a single delay-sensitive data rate: In the existing system, we use the estimation that may vary in all trees. In evaluation of packet, the data can be explained as follows.

Avoidance of HMRP

When avoiding this, point-to point information will be received in delay manner so it delay and success ratio has been achieved by this two indicators can provide for the effectiveness that can avoid HMRP. The success ratio may vary the flow of an uncast flow, and it has been maintained the information with its successful.

Admission Ratio

To find out the admission ratio in this paper, we are going to implement the complete graph. Therefore, all the node gets request message about the following information which is going to transmit the data. This paper construction is based on few topologies to different methods. These methods contain single and multicast format.

Maximum node can be avoided to get accurate result in the X-graph. At the initial phase, these nodes can move from the start point to end point. Later, the flow would not be affected (Fig. 3).

In Fig. 4, this paper demonstrates the transceiver nodes from source to destination in the nam.nam folder. Finally, the simulation is used to show the shortest path and throughput for the following graph which can be represented in the form of graph.

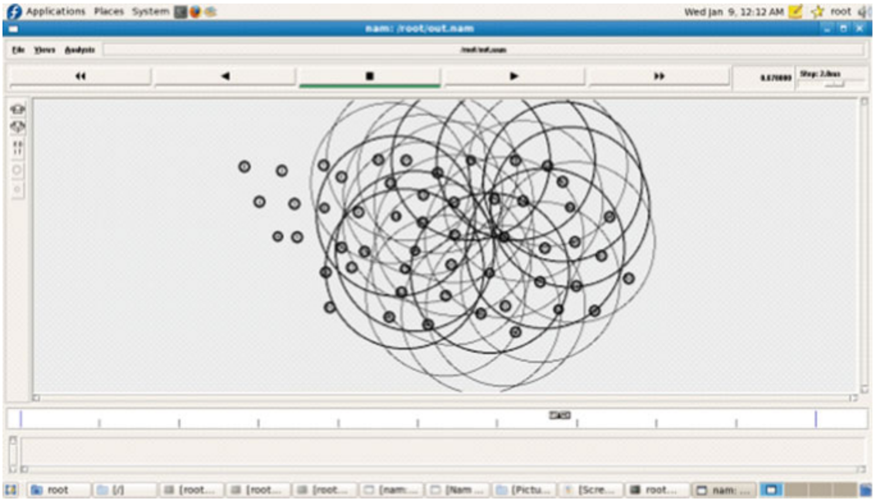
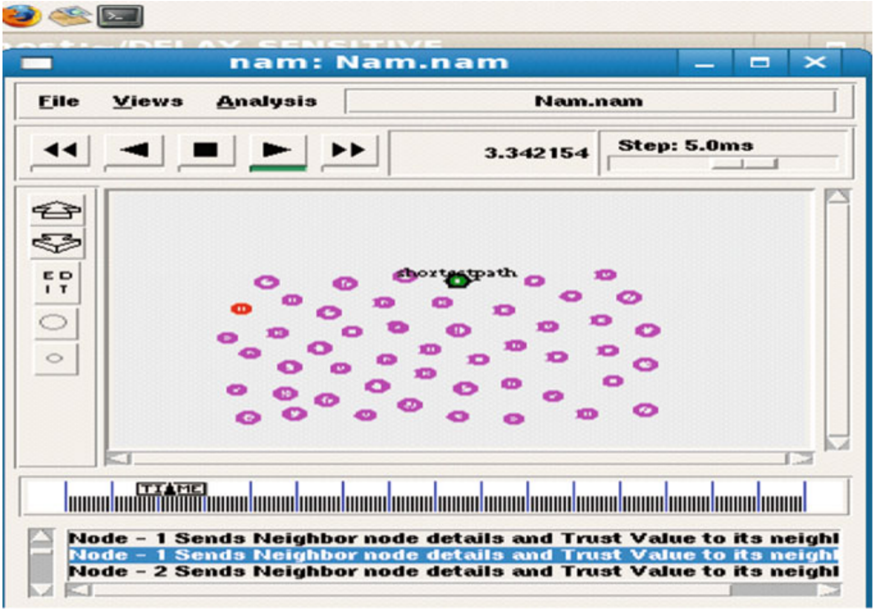


Fig. 3 Simulation of packet



Node - 1 Sends Neighbor node details and Trust Value to its neighl
Node - 1 Sends Neighbor node details and Trust Value to its neighl
Node - 2 Sends Neighbor node details and Trust Value to its neighl

Fig. 4 Delay-sensitive protocol

In Fig. 3 simulation of packet, all the data gets broadcasted with its neighboring node, and they can transmit packet without requesting the host in route. The proposed multicast protocol is constructed by the trees which are shown in result of simulation.

If it was avoided HRP/HMRP, there are no interrupts. If it provided are multiple data rates, same amount of data rates. So, the wireless resources in delay-sensitive protocol can be utilized by its efficiently in crucial.

Figure 5 uses the representation for point to point delay in both existing system. We have developed the proposed system and its rate in MANET for wireless resources in this paper. For shared channel in ratio, our MANETs are an ongoing flow [1]. Mainly, it is used for advanced technologies, and they may tend to satisfaction. The purpose is used for requesting the flows. HRP and HMRP are avoided due to its failure in estimation.

5 Discussion and Conclusion

By constructing and implementing the graph to find out the shortest path in multi-rate. They can be minimized with the total sum of transmission time, and it can be blocked by hosts, since the transmitting ranges are in host.

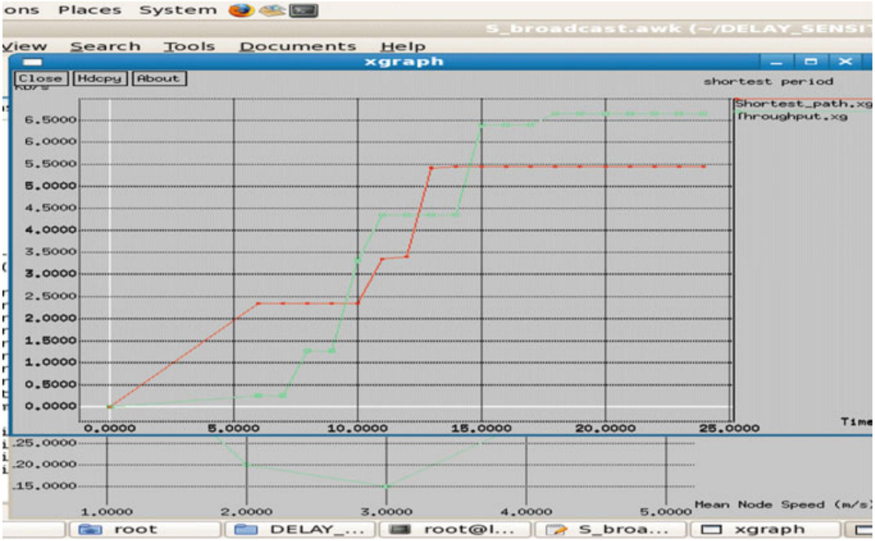


Fig. 5 X-graph

References

1. Sivakumar R, Sinha P, Bharghavan V (1999) CEDAR: a core-extraction distributed ad hoc routing algorithm. IEEE J Sel Areas Commun 17(8):1454–1465
2. Xue Q, Ganz A (2003) Ad hoc quos on-demand routing (AQOR) in mobile ad hoc networks. J Parallel Distrib Comput 63:154–165
3. Chen L, Heinzelman W (2005) Qos-aware routing based on bandwidth estimation for mobile ad hoc networks. IEEE J Sel Areas Commun 23(3):561–572
4. Sinha P, Sivakumar R, Bhanghavan V (1999) MCEDAR: multicast core-extraction distributed ad hoc routing. In: Proceedings of the IEEE wireless communications and networking conference, pp 1313–1317
5. Pagani E, Rossi G (2001) A framework for the admission control of Quos multicast traffic in mobile ad hoc networks. In: Proceedings of the 4th ACM international workshop on wireless mobile multimedia, pp 61–68
6. Darehshoorzadeh A, Dehghan M, Motlagh G (2007) Quality of service support for ODMRP multicast routing in ad hoc networks. Lecture notes in computer science, vol 4686. Springer, New York, pp 237–247
7. Hu CC, Wu EK, Chen GH (2008) Bandwidth-satisfied multicast trees in MANETs. IEEE Trans Mobile Comput 7(6):712–723
8. Zhang B, Mouftah H (2005) Quos routing for wireless ad hoc networks: problems, algorithms, and protocols. IEEE Commun Mag 43(10):110–117
9. Zhang B, Mouftah H (2004) Qos routing through alternate paths in wireless ad hoc networks. Int J Commun Syst 17:233–252
10. Hsu JL, Rubin I (2007) Cross-layer multi-rate routing strategies in wireless multi-hop random access networks. In: Proceedings of the IEEE global telecommunications conference, pp 609–613
11. Venu S, Rahman AMJMZ (2018) FAODV, DSR, DSDV performance analysis for broadcasting in MANET. TAGA J Graph Technol 14:1179–1187

12. Venu S, Rahman MdZ, Rahman AMJ (2014) Efficient routing for broadcasting in mobile ad hoc networks. Inter J Appl Eng Res 9(27):9546–9552
13. Nafaa A, Ksentini A (2008) On sustained Qos guarantees in operated IEEE 802.11 wireless LANs. IEEE Trans Parallel Distrib Syst 19(8):1020–1033
14. Zhai H, Fang Y (2006) Physical carrier sensing and spatial reuse in multi-rate and multihop wireless ad hoc networks. In: Proceedings of the IEEE international conference on computer communications, pp 1–12
15. Ma H, Vijayakumar R, Roy S, Zhu J (2009) Optimizing 802.11 wireless mesh networks based on physical carrier sensing. IEEE/ACM Trans Netw 17(5):1550–1563

SCO-RNN: A Behavioral-Based Intrusion Detection Approach for Cyber Physical Attacks in SCADA Systems

N. Neha, S. Priyanga, Suresh Seshan, R. Senthilnathan and V. S. Shankar Sriram

Abstract Supervisory control and data acquisition (SCADA) systems monitor and control the critical infrastructures (CI) such as power generation, smart grids, oil–gas pipelines, wastewater management, and nuclear power plant. Due to the drastic increase in cyber attacks, maintaining SCADA systems has become a complex task. Difficulty in securing the SCADA has gained the attention of researchers in designing a robust intrusion detection system (IDS). However, existing machine-learning and statistical approaches fail to detect the cyber physical attacks with high detection rate. This paper presents a sine-cosine optimization based recurrent neural network (SCO-RNN) to detect the cyber physical attacks against SCADA systems and the performance of the proposed SCO-RNN was validated using the Secure Water Treatment (SWaT) dataset in terms of accuracy and detection rate.

Keywords Intrusion detection system · Cyber physical system · Supervisory control and data acquisition system (SCADA) · Recurrent neural network · Sine cosine optimization

1 Introduction

Cyber-physical systems (CPS) are embedded systems which incorporate the networking components, physical components, and computational algorithms that play a key role in maintaining the CI [1, 2]. This paper focuses on one such CPS, SCADA. SCADA systems monitor and control a wide range of Industrial Control Systems

N. Neha · S. Priyanga · S. Seshan · R. Senthilnathan · V. S. Shankar Sriram (✉)
School of Computing, Centre for Information Super Highway (CISH), SASTRA Deemed to be University, Thanjavur, Tamil Nadu 613401, India
e-mail: sriram@it.sastra.edu

N. Neha
e-mail: nehanageswaran@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_88

(ICS) linked to networks, causing downtime of the system which in turn can cause disastrous effects for national security [3]. Traditional SCADA systems were isolated that they were not connected with the Internet thus shielded from all the remote attacks [4]. Over the past decades, the SCADA systems were more susceptible to cyber attacks which happened not only on the physical infrastructures but also on the communication network.

There has been a significant increase in the number of attacks which have caused catastrophic effects to the nation. According to the IBM X-Force Report, recent security incidents like Qak-Bot (2017), Botnet-based CMDi LFI attacks (2017/18) in which the attacker attempted to upload malicious files to servers and also attempted to mine CryptoNote-based currencies such as Monero (XMR), IcedID emerges in the USA and UK (2017), etc, accentuate the need to protect the digital ecosystem from the security threats and intrusions [5].

The traditional security measures like firewall, authentication, etc., proved to be less secure and made us understand the necessity for developing an efficient intrusion detection system (IDS) [6]. The main aim of IDS is to detect the anomalies with less false-alarm rate. Based on the detection methodology, IDS can be categorized into two—Signature-based IDS and Anomaly-based IDS [7]. Both approaches have their own advantages and disadvantages which led the researchers to apply several techniques such as statistical analysis, data mining, artificial intelligence, and machine-learning approaches like k-nearest neighbor (KNN), support vector machine (SVM), artificial neural network (ANN), and logistic regression, etc., are used in the anomaly detection [8].

Artificial neural networks play an important role in intrusion detection. Recurrent neural network (RNN) is one among ANN which overcomes the drawback of storage space unlike other neural networks, [3, 9]. RNN plays an important role in speech recognition, human action recognition, computer vision, etc. However, maintaining high detection rate and low false-alarm rate helps in the design of potential IDS, which significantly out-compete other models [10].

In order to achieve better performance, sine–cosine optimization—recurrent neural network (SCO-RNN)-based IDS is proposed in this paper which optimizes the hidden layers [11]. This experiment was carried out using the standard Secure Water Treatment dataset (SWaT) [12], and the performance of SCO-RNN is validated in terms of classification accuracy and detection rate (Table 1).

Table 1 Related works

Authors	Proposed method	Objective	Applications	Advantages	Performance metric
Turabieh et al. [13]	Dynamic L-RNN	Recovery of missing data	IoMT application	Recovery of missing data	• Accuracy
Cinar et al. [14]	Period-aware content attention RNN	Missing value imputation	Time series forecasting	Can be performed on univariate and multivariate time series	• Attention weights
Liu et al. [15]	Modeling asynchronous event sequences	Classification	Medical application	Improved performance	• Macro-F1 • Precision • Recall
Shitharth and Prince Winston [16]	Intrusion-weighted particle-based cuckoo search optimization (IWP-CSP) and hierarchical neuron architecture-based neural network (HNA-NN)	Classification	Attack detection	Increased performance	• Dice • Jaccard • precision • Recall • Accuracy • Sensitivity • Detection rate • Specificity
Zhao et al. [8]	CNN-RNN based multi-label classification	Classification	Weather prediction	Practical implementation is effective	• Precision • Recall • F-score
Maglaras et al. [2]	One class support vector machine	Detection	Information security	Increased accuracy	• Accuracy • System performance
Maglaras and Jiang [6]	IT-one class support vector machine	Detection	Information security	Increased performance	• False-alarm rate
Adepu et al. [17]	State condition graphs (SCGs)	Analysis	Water treatment	Easier and quicker	• Steady-state response
Goh et al. [3]	Recurrent neural network	Detection	Time series prediction	Identifies attacked sensors	• System state

2 SCO-RNN Proposed Methodology

This section discusses the working of proposed improved RNN based on sine–cosine optimization. The workflow of the SCO-RNN as follows.

Pseudo Code—RNN-SCO

1. 51 Attributes of the SWaT dataset are fed as the input to the RNN
2. Now, 80% data of the SWaT data set are trained and 20% are tested
3. Now, set the upper bound and lower bound, the total number of iteration, and initialize a constant ‘a’ as 2
4. Now, build an RNN model
5. While building RNN,

(a) Initialize the number of units in the input layer to 51, which is the total number of attributes in the SWaT dataset.

(b) Now, set the number of hidden units to 20 and grant it to the SCO optimization algorithm as follows:

1. Initialize the set of search agents, upper bound, lower bound, and constant ‘a’ = 2
2. Evaluate each search agents by the fitness function
3. Update the best solution obtained so far
4. Update the value of x_1, x_2, x_3 and x_4 as follows:

$$\text{a.}x_1 = \text{const-curr}_{\text{iter}} * \left(\frac{\text{const}}{\text{tot\_iter}}\right) \tag{1}$$

where, const = 2 is a constant, curr_iter is the current iteration, tot_iter is total number of iterations

$$\text{b.}x_2 = 2\pi * \text{random\_number} \tag{2}$$

$$\text{c.}x_3 = 2 * \text{random\_number} \tag{3}$$

$$\text{d.}x_4 = \text{random\_number} \tag{4}$$

Here, x_1 indicates the region between the destination and solution or outside it, x_2 indicates the distance from destination position, x_3 indicates a random weight for the destination, and finally, x_4 here changes depending on the Eqs. (5) and (6).

5. Now, update the position of each search agent as follows:
   If $x_4 < 0.5$ then,

$$X(i, j) = X(i, j) + (x_4 * \sin(x_2) * |(x_3 * \text{Destination\_position}\ (j) - X(i, j))| \tag{5}$$

else

$$\text{X}(i, i) = X(i, i) + \big(x_4 * \cos(x_2)^{*}|(x_3 * \text{Destination\_position}\ (j) - X(i, j))| \tag{6}$$

6. Repeat till it reaches the maximum number of iterations.
7. Obtain the best solution as the global optimum.

(c) Finally, set the number of units in the output layer as 10, which is a constant, given for better performance.

6. Calculate the fitness value as given in Eq. (7)
7. Now, repeat the steps step 5.b.2 to step 5.b.7 and return the best solution as global optimum
8. Print the accuracy, detection rate, and the fitness value.

2.1 Generation of Initial Population

The working of SCO-RNN starts with the initialization of parameters like search agents, a number of iterations, and computation of parameters like x_1, x_2, x_3, x_4. x_1 depends on the current iteration, total number of iterations and a constant a. x_1 parameter is initialized as given in the Eq. (2). x_2 and x_3 purely depend on random numbers which is calculated as in Eqs. (3) and (4). The fitness function is chosen such that it should give an optimized result compared to the existing technique as in Eq. (7).

2.2 Training and Testing the RNN

The entire SWaT dataset considered for the experiment is divided into training and testing samples. At first, training is done and then the trained samples and parameters obtained from each population is used for training the RNN where its performance is evaluated using fitness function along with the other testing samples.

2.3 Definition of the Fitness Function

The performance of SCO-RNN is assessed using the fitness function as in Eq. (7) in order to bring out a better and optimized result. The performance of SSO-RNN is evaluated in the following equation:

$$f_{\text{Fit}} = W_1(\text{DR}) + W_2 * \text{Acc} + W_3(1 - \text{FAR}) \tag{7}$$

where ‘W’ for weights.

2.4 Termination Condition

The termination condition is satisfied when a maximum number of iteration or optimal number of hidden layers has been reached. If the condition is true, then the optimal number of hidden units is returned. Then, the population will be updated with the best fitness value and with its position, using the Eqs. (5) and (6) accordingly (Fig. 1).

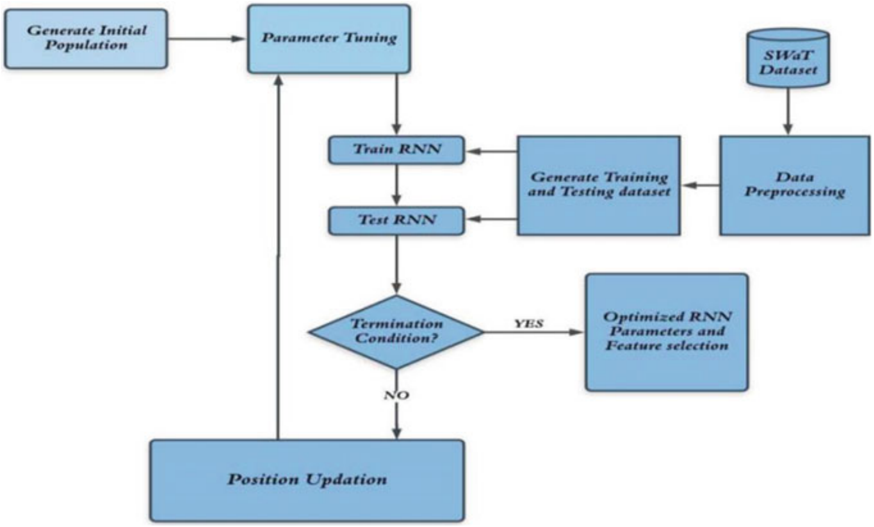

Generate Initial Population
Parameter Tuning
SWaT Dataset
Train RNN
Generate Training and Testing dataset
Data Preprocessing
Test RNN
Termination Condition?
YES
Optimized RNN Parameters and Feature selection
NO
Position Updation

Fig. 1 Proposed flow diagram

3 Results and Discussion

3.1 Experimental Setup

SCO-based RNN was implemented on Python 3.6 with INTEL® Core™ i5-7200U CPU processor @ 2.50 GHz architecture, 8.00 GB RAM and 64-bit OS in x64-based processor running Windows 10, and WEKA tool is used for the validation process.

3.2 Dataset Description

Secure Water Treatment testbed (SWaT) dataset is a six-stage secure water treatment which is a scaled-down version of the real-world industrial water treatment plant. This dataset is collected from Singapore University of Technology and Design (SUTD) [12]. SWaT is the most complex open-source dataset so far with a total of 51 properties and 946,722 samples including six dual programmable logic control (PLCs) each for one stage, along with a backup, 25 sensors, and 26 actuators altogether (Table 2).

Attacks are represented using a six-tuplet as follows: (M, G, D, P, S_0 and, S_e) where

M: Infinite set of procedures to launch the attack
G: Subset of a finite set of attacker events
D: Domain model for the attacks derived from CPS

Table 2 Attack types in SWaT

Attack category	Number of attacks
Single stage single point	26
Single stage multi point	4
Multi stage single point	2
Multi stage multi point	4

P: Finite set of attack points
S_0, S_e: Infinite set of attack points.

3.3 Data Pre-processing

Data pre-processing plays a key role in the simplification of obtained real-world data, which are either incomplete or inconsistent. Here, data normalization is used to improve the efficiency and accuracy of the proposed technique (SCO-RNN). Data normalization generally modifies the data from the existing range to a particular range. Here, normalization is performed for the values on which numerical encoding is performed, which result in each value ranging between 0 and 1. There are many methods in normalization out of which the method performed here is as follows:

$$X_{\text{Norm}} = \frac{x - x\text{min}}{x\text{max} - x\text{min}} \tag{8}$$

where x: Data point, $x\text{min}$: Minimal among the data points, $x\text{max}$: Maximal among the data points, and X_{Norm}: Data point normalized between 0 and 1.

3.4 Results and Discussions

Figure 2 shows a comparison of the accuracy of proposed SCO-RNN with other existing techniques. From this, we can infer the accuracy of SCO-RNN is 98.05% is higher than the existing approaches. The accuracy has been calculated using Eq. (9).

$$\text{Acc} = \frac{\text{True Positive} + \text{True Negative}}{\text{True Positive} + \text{True Negative} + \text{False Positive} + \text{False Negative}} \tag{9}$$

Table 3 shows comparison for the detection rate of the SCO-RNN technique with other existing techniques. The proposed SCO-RNN has a higher detection rate than the other existing approaches. As the proposed algorithm converges at a global optimal solution, it achieves higher accuracy and detection rate in minimal time. The detection rate has been calculated using Eq. (10).

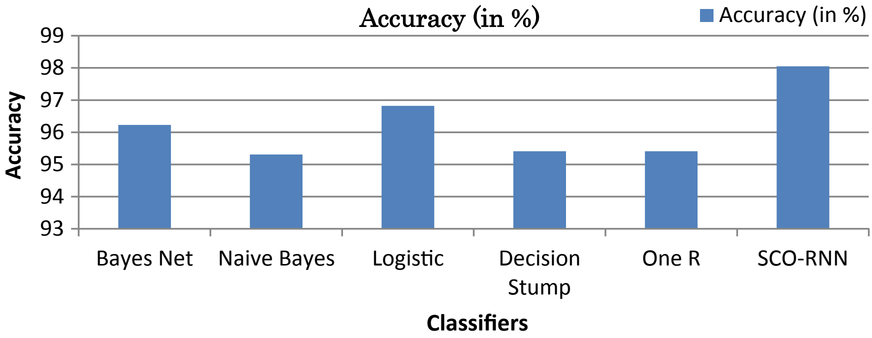


Fig. 2 Accuracy

Table 3 Detection rate

S. No.	Classifiers	Detection rate (%)
1	Bayes net	95.98
2	Naive Bayes	95.1
3	Logistic	96.7
4	Decision stump	95
5	One R	92.1
6	SCO-RNN	97

$$\mathrm{DR} = \frac{\text{True Positive}}{\text{True Positive} + \text{False Negative}} \tag{10}$$

4 Conclusions

In this paper, we have proposed an efficient intrusion detection technique that incorporates the sine–cosine optimization algorithm for optimizing the recurrent neural network parameters. The SWaT, a benchmark intrusion dataset has been used for validating the proposed SCO-RNN. Here, the hyperparameters of the RNN have been optimized, and the outcome of the system shows a better result than other machine-learning approaches in terms of accuracy and detection rate.

Acknowledgements This work was supported by Department of Science and Technology, India through Fund for Improvement of S&T Infrastructure (FIST) programme (SR/FST/ETI-349/2013) and Tata Consultancy Services. The authors would like to thank the DST-ICPS (T-615) for their financial support, Department of Science and Technology, India and “iTrust, Centre for Research in Cyber Security, Singapore University of Technology and Design” for providing the dataset.

References

1. Mahmoud MS, Hamdan MM, Baroudi UA (2019) Modeling and control of cyber-physical systems subject to cyber attacks: a survey of recent advances and challenges. Neurocomputing:1–15
2. Maglaras LA, Jiang J, Cruz TJ (2016) Combining ensemble methods and social network metrics for improving accuracy of OCSVM on intrusion detection in SCADA systems. J Inf Secur Appl 30:15–26
3. Goh J, Adepu S, Tan M, Lee ZS (2017) Anomaly detection in cyber physical systems using recurrent neural networks. In: Proceedings IEEE international symposium on high assurance systems engineering, pp 140–145
4. Senthivel S, Ahmed I, Roussev V (2017) SCADA network forensics of the PCCC protocol. Digital Invest 22:S57–S65
5. IBM (2018) IBM X-Force threat intelligence index 2018 notable security events of 2017, and a look ahead. IBM Secur 43
6. Maglaras LA, Jiang J (2014) Intrusion detection in SCADA systems using machine learning techniques. In: Proceedings of 2014 science and information conference (SAI), pp 626–631
7. Gauthama Raman MR, Somu N, Kirthivasan K, Liscano R, Shankar Sriram VS (2017) An efficient intrusion detection system based on hypergraph—genetic algorithm for parameter optimization and feature selection in support vector machine. Knowl Syst 134:1–12
8. Zhao B, Li X, Lu X, Wang Z (2018) A CNN–RNN architecture for multi-label weather recognition. Neurocomputing 322:47–57
9. Liu H, Lang B, Liu M, Yan H (2019) CNN and RNN based payload classification methods for attack detection. Knowl Syst 163:332–341
10. Kabir E, Hu J, Wang H, Zhuo G (2018) A novel statistical technique for intrusion detection systems. Future Gener Comput Syst 79:303–318
11. Mirjalili S (2016) SCA: a sine cosine algorithm for solving optimization problems. Knowl Syst 96:120–133
12. Goh J, Adepu S, Junejo KN, Mathur A (2016) A dataset to support research in the design of secure water treatment systems
13. Turabieh H, Abu Salem A, Abu-El-Rub N (2018) Dynamic L-RNN recovery of missing data in IoMT applications. Future Gener Comput Syst 89:575–583
14. Cinar YG, Mirisaee H, Goswami P, Gaussier E, Aït-Bachir A (2018) Period-aware content attention RNNs for time series forecasting with missing values. Neurocomputing 312:177–186
15. Liu S et al (2018) Modeling asynchronous event sequences with RNNs. J Biomed Inform 83(May):167–177
16. Shitharth S, Prince Winston D (2017) An enhanced optimization based algorithm for intrusion detection in SCADA network. Comput Secur 70:16–26
17. Adepu S, Mathur A, Gunda J, Djokic S (2007) Algorithms and architectures for parallel processing. Alg Archit Parallel Process 1:785–798

SSO-IF: An Outlier Detection Approach for Intrusion Detection in SCADA Systems

P. S. Chaithanya, S. Priyanga, S. Pravinraj and V. S. Shankar Sriram

Abstract Supervisory Control and Data Acquisition (SCADA) systems play a prominent role in monitoring and controlling the Critical Infrastructures (CIs) such as water distribution, nuclear plants, and chemical industries. On the other hand, SCADA systems are highly exposed to new vulnerabilities as it highly relies on the internet. Machine learning approaches have been employed to detect the cyberattacks injected by the attackers in CIs. However, those approaches failed to protect the CIs against the ever-advancing nature of cyberattacks. This work presents Salp Swarm Optimization-based Isolation Forest (SSO-IF) to build an efficient SCADA intrusion detection system, and the experiments were carried out using power system dataset from Mississippi State University. The performance of SSO-IF was validated over the state-of-the-art intrusion detection techniques in terms of classification accuracy and detection rate.

Keywords SCADA · Intrusion detection system · Isolation forest · Salp swarm optimization

1 Introduction

The Critical Infrastructure (CI) modernizes by the evolution of Cyber-Physical Systems (CPS) [1]. CPS integrates the physical system with computing and networking technologies. SCADA systems are an essential part among the CPS that helps to monitor and control the systems more efficiently and to communicate system issues to mitigate downtime in CIs such as power plants, gas and oil distribution, electrical power, water distribution, and chemical processing plants [2]. Primarily, the SCADA systems are isolated devices, and then these are streamlined by interconnecting all the

P. S. Chaithanya · S. Priyanga · S. Pravinraj · V. S. Shankar Sriram (✉)
School of Computing, Centre for Information Super Highway (CISH), SASTRA Deemed to be University, Thanjavur, Tamil Nadu 613401, India
e-mail: sriram@it.sastra.edu

S. Priyanga
e-mail: priyangas54@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_89

embedded devices with the internet, which produces high reliability in the automation of the system. These sophisticated SCADA systems rely on cyberspace, which makes the system vulnerable to cyberattacks. The cyber attackers focus to create vulnerability on technical parts of the system in CIf.

Recently, the attacks in SCADA systems have increased tremendously which results in compromising of basic security measures such as Confidentiality, Integrity, and Authenticity of the system. This is conspicuous from the "Waterfall" report in 2017, Sophisticated Ukraine Attack causes physical damage to electric substations and rotating equipment, Compromised Remote Site—A physical breach of remote substation, ICS Insider which is a disgruntled insider, and it has the ability to partially shut down the ICS-equipped plant by steal passcode of the equipment's [3]. Therefore, the awareness about reducing these vulnerabilities leads to the evolution of Intrusion Detection System (IDS).

IDS can be categorized into two, based on the detection techniques namely Signature-based and Anomaly-based IDS [4]. The major focus of IDS is to achieve high Detection Rate and reduce False Alarm Rate. Recent research works reveal the importance of machine learning techniques (Decision Trees, KNN, Support Vector Machines (SVM), Neural Networks, etc.) in the design of an efficient and adaptive IDS [5].

This paper proposes the Isolation Forest (IF) technique which directly identifies anomalies instead of identifying normal data points and constructed an ensemble of isolation trees [6]. This technique segregates the records by selecting the features randomly and sets a split value between the supreme and subordinate value. The anomalies are identified by path length or anomaly score. It performs well for the high-dimensional dataset, and the parameter used is the number of isolation trees and sub-sampling size. Parameters are tuned to either increase the predictive power of the model or to make it easier to train the model. Various optimization techniques like a genetic algorithm, fruit-fly optimization, whale optimization, moth-flame optimization, etc., have been used in the literature for tuning the parameters. Among these, Salp Swarm Optimization technique [6] with Isolation Forest (SSO-IF) achieves high detection rate, and it was validated with Mississippi's power system dataset in terms of accuracy and detection rate (Table 1).

Table 1 Related works

Authors	Proposed method	Dataset	Advantages	Performance metric
Puggini and McLoone [7]	Isolation forest	OES data	Better performance	• EV • ENMSE • EMRE • AUC score
Sun et al. [8]	Banzhaf random forest	UCI machine learning repository—12 datasets	Better performance	• Banzhaf power index • Information gain ratio
Maglaras et al. [9]	IT-one class support vector machine	SCADA traffic dataset	Increased performance	• Accuracy • System performance
Alves and Morris [10]	Random forest	Six real-world datasets	Best performance	• Gain metric
Abellán et al. [11]	Credal random forest	50 datasets from the UCI repository of machine learning	Good accuracy, robust under noise data	• Accuracy
Shirazi et al. [12]	Random forest regression	201 experimental data points	High accuracy	• Erosion ratio
Nader et al. [13]	One-class classification	Mississippi State University SCADA laboratory	High error detection, low FAR	• lp NORMS
Trombetta et al. [14]	Critical state analysis and state proximity	Private SCADA traffic data	More feasible	• State-state distance • State-critical states distance • Distance evaluation accuracy
Shitharth et al. [15]	Intrusion weighted particle-based cuckoo search optimization (IWP-CSO) and hierarchical neuron architecture-based NN	Single-hop indoor real data (SIRD), single-hop outdoor real data (SORD), multi-hop indoor real data (MIRD), multi-hop outdoor real data (MORD)	Increase in performance	• Detection rate • False positive rate • Precision • Sensitivity • Specificity • Accuracy

2 SSO-IF Proposed Methodology

This section briefly discusses the working of enhanced Isolation Forest technique based on Salp Swarm Optimization algorithm (SSO-IF) [16]. The following are workflow of SSO-IF.

Pseudocode-SSO-IF:

```
1. Each among 15 datasets is fed as the input to the IF
2. Set the training and the testing ratio of the dataset
3. Now perform the IF with estimators being optimized by SSO technique
    a. Initialize the lower and upper bound and total number of iterations
    b. Calculate the swarm position and then
    c. Update the leader and follower salp position using the parameter $\mathrm{rnd}_1$, $\mathrm{rnd}_2$, and $\mathrm{rnd}_3$
    d. The leader salp is updated by the following equation
       $x_j^1 \leftarrow \begin{cases} \mathrm{BF}_j + \mathrm{rnd}_1\left(\left(\mathrm{ub}_j - \mathrm{lb}_j\right)\mathrm{rnd}_2 + \mathrm{lb}_j\right) & \mathrm{rnd}_3 \geq 0 \\ \mathrm{BF}_j - \mathrm{rnd}_1\left(\left(\mathrm{ub}_j - \mathrm{lb}_j\right)\mathrm{rnd}_2 + \mathrm{lb}_j\right) & \mathrm{rnd}_3 < 0 \end{cases}$   (1)
    e. Here, the parameter $\mathrm{rnd}_1$ is calculated using the Eq. (3), and the $\mathrm{rnd}_2$ and $\mathrm{rnd}_3$ are randomly generated
    f. The follower salp positions are updated by
       $x_j^i \leftarrow \frac{1}{2}\left(x_j^i + x_j^{i-1}\right)$   (2)
    g. Find the best optimum solution for the above
4. Set the best optimum solution as number of estimators
5. Predict the outlier present in the dataset
6. Build the confusion matrix
7. Compute the accuracy and detection rate using the Eqs. (6) and (7).
```

2.1 *Generation of Initial Population*

The working of SSO-IF begins with the parameters initialization such as the number of populations, number of iterations, and computation of parameters like rnd_1, rnd_2, and rnd_3. The parameter rnd_1, rnd_2, and rnd_3 are random numbers. Based on the current and total number of iterations, rnd_2 and rnd_3 are defined and are evenly generated in the interval of [0, 1] [16]. In order to achieve better optimization result, the better fitness function is chosen. The parameter number of trees in IF was generated randomly in a specific range.

$$\mathrm{rnd}_1 = 2\mathrm{e}^{-\left(\frac{4i}{I}\right)^2} \tag{3}$$

2.2 Training and Testing the Isolation Forest

The experiment splits the complete SCADA IDS dataset into training and testing samples by random sampling. Here, the training and testing data ratio is chosen randomly by the system in an appropriate ratio.

2.3 Definition of the Fitness Function

In order to compute the performance of SSO-IF, the weighted fitness function is used and is defined with weights of the DR and FAR as follows:

$$\mathrm{Fitness\_value} = 0.8 * \mathrm{DR} + 0.1 * (1.0 - \mathrm{FAR}) + 0.1 * (1 - (N/Nf)) \tag{4}$$

where N is the no. of selected features, Nf is the total number of features.

2.4 Termination Condition

Here, the termination condition verifies whether it reaches the maximum number of iteration. If so, it returns the optimal parameter or else it would perform position updation (Fig. 1).

3 Results and Discussions

3.1 Experimental Setup

SSO-based IF was implemented on Python 3.5 with INTEL® Core™ i3-5005U CPU processor @ 2.00 GHz architecture running in Windows 10, and validation process was carried out using Weka tool.

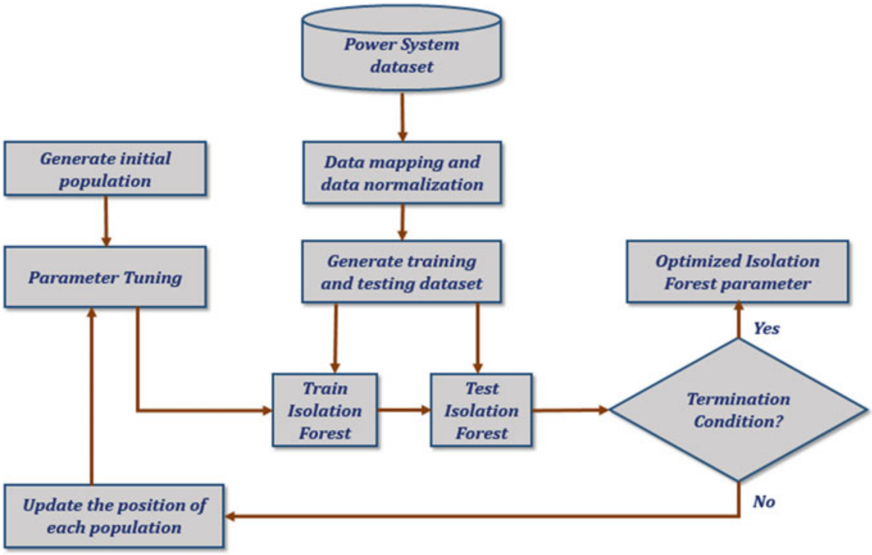

Power System dataset
Data mapping and data normalization
Generate training and testing dataset
Generate initial population
Parameter Tuning
Train Isolation Forest
Test Isolation Forest
Termination Condition?
Yes
No
Optimized Isolation Forest parameter
Update the position of each population

Fig. 1 Workflow of SSO-IF

3.2 Dataset Description

Power system attack dataset from Mississippi State University has been used for this model. This dataset totally contains 128 features and is developed based on 37 event scenarios which include eight Natural Events, one No Events, and 28 Attack Events [17]. It is divided into three datasets binary dataset (CSV format), class dataset (CSV format), and multiclass dataset (ARFF format), in which binary dataset consisting of 15 sets has been used in this work.

3.3 Data Preprocessing

The preprocessing stage generally reduces the dataset size by resampling it or by eliminating redundant records. It contains two main stages, in which initially, the integers are bought between the range of 0–1 after the nominal features are mapped with integer values. Further, to reduce the value range, logarithmic scaling (base 10) is enforced with the integer value ranges. Normalization is one of a kind in preprocessing. The proposed technique SSO-IF uses min-max normalization which finds the maximal and minimal feature value and then transforms them into linearly scaled values ranging from 0 to 1. The formula for min-max normalization is as follows:

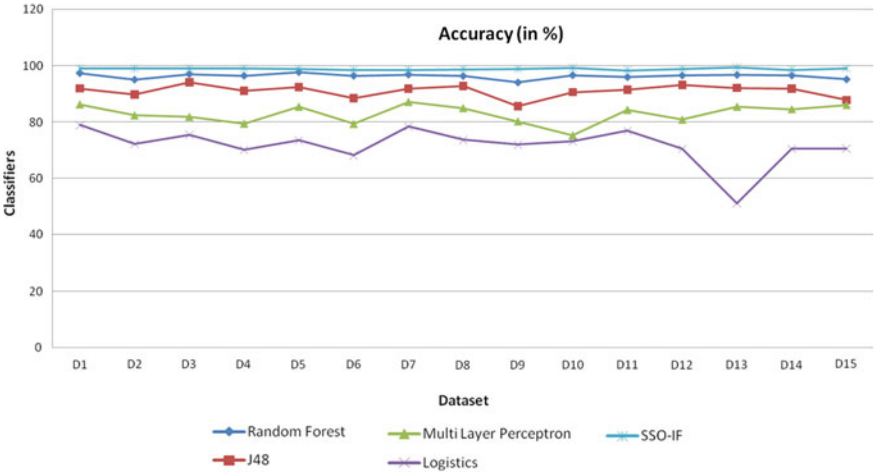


Fig. 2 Accuracy

$$X_{\text{Norm}} = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \tag{5}$$

where x: Data point, $x_{\min}$: Minimal among the data points, $x_{\max}$: Maximal among the data points, and X_{Norm}: Data point normalized between 0 and 1.

3.4 Results and Discussions

Figure 2 shows the accuracy results for SSO-IF compared with other classifiers. From this, it can be deduced that the accuracy of SSO-IF is higher than the other techniques. The accuracy is calculated as in Eq. (6).

$$\text{Acc} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{6}$$

Table 2 shows the detection rate of SSO-IF compared with other classifiers in which the proposed technique got higher DR when compared with other techniques. DR is calculated as in Eq. (7)

$$\text{DR} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{7}$$

Table 2 Detection rate

Dataset	Random forest	J48	Multi layer perceptron	Logistic regression	SSO-IF
D1	95.4	81.4	76.1	55.5	98.9
D2	94.5	83.8	73.1	58	98.9
D3	96	88.3	65	59.1	98.9
D4	96.8	91.1	79.4	70.1	99
D5	97.7	92.4	85.4	73.5	98.8
D6	96.4	78.9	67.7	38.9	98.4
D7	98.4	85	77.1	62.9	98.5
D8	98.8	87.2	82.5	82.6	98.7
D9	93.7	78.7	75.2	64.7	98.8
D10	97.5	88.9	59.1	60.6	99.1
D11	98.6	82.6	67.9	51.7	98.3
D12	96	89.8	81.8	59.2	98.8
D13	98.6	85.8	70.8	53.4	99.3
D14	98.2	86.5	80.6	54.2	98.5
D15	96.2	84.9	82.4	62.4	99

4 Conclusions

In this work, we have proposed SSO-IF approach in which the parameters of isolation forest have been optimized using Salp Swarm Optimization Algorithm to obtain optimal number of trees. The proposed SSO-IF technique has been experimented and validated using the benchmark power system dataset from Mississippi State University. The performance of SSO-IF was evaluated using the metrics such as accuracy and detection rate.

Acknowledgements This work was supported by Department of Science and Technology, India through Fund for Improvement of S&T Infrastructure (FIST) programme (SR/FST/ETI-349/2013) and Tata Consultancy Services. The authors would like to thank the MeitY (AAA-22/7/2018-CSRD-MeitY) for their financial support.

References

1. Goh J, Adepu S, Tan M, Lee ZS (2017) Anomaly detection in cyber physical systems using recurrent neural networks. In: Proceedings of IEEE international symposium high assurance systems engineering, pp 140–145
2. Zhang J, Gan S, Liu X, Zhu P (2016) Intrusion detection in SCADA systems by traffic periodicity and telemetry analysis. In: Proceedings—IEEE symposium on computers communications, pp 318–325

3. Ginter A (2017) The top 20 cyber attacks against industrial control systems, pp 2–4
4. Almalawi A, Yu X, Tari Z, Fahad A, Khalil I (2014) An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems. Comput Secur 46:94–110
5. Maglaras LA, Jiang J (2014) Intrusion detection in SCADA systems using machine learning techniques. In: Proceedings of 2014 science and information conference, SAI 2014, pp 626–631
6. Liu FT, Ting KM (2018) Isolation forest. In: Eighth IEE international conference data mining, 2009
7. Puggini L, McLoone S (2018) An enhanced variable selection and isolation forest based methodology for anomaly detection with OES data. Eng Appl Artif Intell 2017 67:126–135
8. Sun J, Zhong G, Huang K, Dong J (2018) Banzhaf random forests: cooperative game theory based random forests with consistency. Neural Netw 106:20–29
9. Maglaras LA, Jiang J, Cruz TJ (2016) Combining ensemble methods and social network metrics for improving accuracy of OCSVM on intrusion detection in SCADA systems. J Inf Secur Appl 30:15–26
10. Alves T, Morris T (2018) OpenPLC: an IEC 61,131–3 compliant open source industrial controller for cyber security research. Comput Secur 78:364–379
11. Abellán J, Mantas CJ, Castellano JG (2017) A random forest approach using imprecise probabilities. Knowl Syst 134:72–84
12. Shirazi SA, Parvandeh S, McKinney BA, Asgharpour A, McLaury BS, Zahedi P (2018) Random forest regression prediction of solid particle erosion in elbows. Powder Technol 338:983–992
13. Nader P, Honeine P, Beauseroy P (2014) Lp-norms in one-class classification for intrusion detection in SCADA systems. IEEE Trans Ind Inform 10(4):2308–2317
14. Trombetta A, Masera M, Nai Fovino I, Carcano A, Guglielmi M, Coletta A (2011) A multidimensional critical state analysis for detecting intrusions in SCADA systems. IEEE Trans Ind Inform 7(2):179–186
15. Shitharth S, Prince Winston D (2017) An enhanced optimization based algorithm for intrusion detection in SCADA network. Comput Secur 70:16–26
16. Mirjalili S, Gandomi AH, Mirjalili SZ, Saremi S, Faris H, Mirjalili SM (2017) Salp swarm algorithm: a bio-inspired optimizer for engineering design problems. Adv Eng Softw 114:163–191
17. Borges Hink RC, Beaver JM, Buckner MA, Morris T, Adhikari U, Pan S (2014) Machine learning for power system disturbance and cyber-attack discrimination. In: 7th international symposium on resilient control systems, ISRCS

EDF-VD Scheduling-Based Mixed Criticality Cyber-Physical Systems in Smart City Paradigm

G. Naveen Balaji, M. Sethupathi, N. Sivaramakrishnan and S. Theeijitha

Abstract Dynamic data-driven simulation is introduced to improve the scheduling performance. The customer will need a just in delivery of service scheduling. Mathematical model of the scheduling problem is constructed, and a scheduling method is proposed to improve the performance of scheduling. Four different optimizations for the dynamic cloud manufacturing scheduling problems are presented in this paper, namely average service utilization rate, average task delay time, weighted average task delay time, proportion of delay tasks and constraints. The scheduling strategies are constructed and simulated in the SIMSO software.

Keywords Embedded system · Worst-case execution time · Earliest deadline first · Earliest deadline first virtual deadline · Preemptive

1 Introduction

System is a manner of operating, organizing or doing one or greater duties in keeping with the fixed plan, application or set of rules. A system is also an association in which all its units gather and work collectively in step with the plan or software. An embedded system is mixed operation of hardware and software or additional mechanical or technical component to carry out desired characteristic. Any sort of tool which incorporates programmable pc but itself is not always meant to be fashionable motive laptop is said to be embedded system [1]. The lower layer of an embedded system is printed circuit board that consists of busses and semiconductor devices. The top layer is special application layer, and in between those two layers, there are another vital layers referred to as device drivers and verbal exchange protocols. They need electrical powered and digital interference. Embedded structures, all the time, are limited assets to be had in phrases of memory, CPU, show display screen period, key inputs, diskless, and those parameters play a important thing in the route of the format, improvement and trying out of such structures.

G. Naveen Balaji (✉) · M. Sethupathi · N. Sivaramakrishnan · S. Theeijitha
Department of ECE, SNS College of Technology, Coimbatore, India
e-mail: yoursgnb@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_90

1.1 Characteristics of Embedded Systems

In popular, embedded systems are designed to carry out any unique predefined project that ought to meet any real-time constraint. The primary distinction among a laptop and an embedded device is a computer is used to carry out a particular project, and this is predefined by way of manner of the manufacturers.

Assembling all the actual-time tool constraints is a very vital feature of an embedded machine. An actual-time constraint is split into two features. That is hard real-time system and the upcoming one is soft real-time system [2]. Zero degree of flexibility is for hard real-time system, and a determined amount of flexibility is for soft real-time systems. The miss which happens while execution will collapse the whole output of the system. The small amount of miss is accepted in the soft real-time system which does not collapse the whole system. Devices which include MP3s, cameras and TV remotes are the examples of standalone embedded system.

1.2 Architecture of Embedded System

An embedded system is constructed round a processor. The principal processing unit does the important computation based on the enter it receives from diverse external devices [3]. The functionality of the CPU is an embedded device is equal because the capability of the CPU in a desktop, except that the CPU in an embedded system is much less powerful.

The processor has restricted internal reminiscence, and if this internal reminiscence is not always enough for a given application, outside reminiscence gadgets are used [4]. The hardware additionally includes any additives that allow the person-application interaction, including display units, keypads, etc.

A wide variety of 16 and 32-bit microprocessors are to be had from ARM, Atmel, Intel, Motorola, National Semiconductors and so on. In order to increase an embedded system with these processors, you first rate deal of peripheral circuitry. However, microprocessors have better clock speeds and phrase-period, so they are able to address higher reminiscence [5]. These type of processors are used for high-end applications inclusive of hand-held computers, Internet get right of entry to devices and so forth.

The reminiscence utilized in embedded system can be both internal and outside [6]. The internal memory of a processor is very restricted. For small applications, if this memory is enough, there is want to used outside reminiscence [7]. Figure 1 shows the system concept of embedded system.

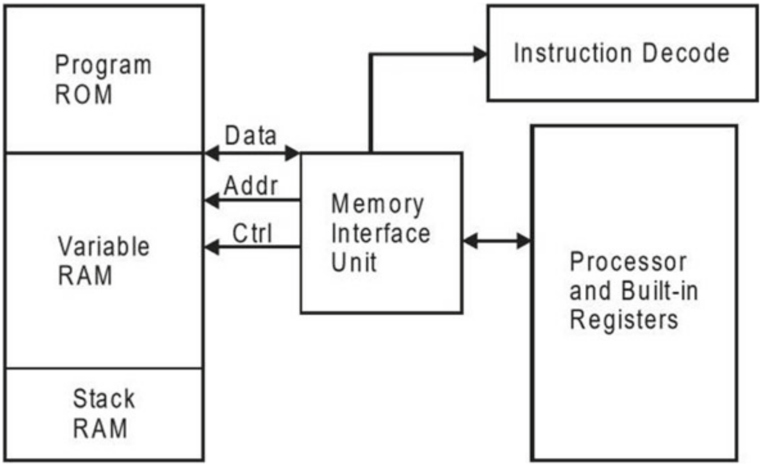


Fig. 1 System concept of embedded architecture

2 Background

2.1 *Cyber-Physical System*

A cyber-physical system is the method wherein the computer primarily based set of regulations is controlled and monitored and tightly included with the internet and its patron [8]. In CPS, the bodily and software program application additives are deeply intertwined, every taking walks on special spatial and temporal scales, displaying more than one and excellent behavioral modalities and interacting with every exceptional in quite some techniques [9]. Examples of CPS encompass clever grid, impartial vehicle structures, scientific tracking, method manipulate functions, robotics and automated pilot avionics.

CPS involves processes, merging concept of cybernetics, mechatronics, design and manner technological know-how [10]. The system manage is known as embedded devices. CPS is likewise similar to the (IoT), sharing the same primary structure, despite the truth that CPS offers a higher mixture and coordination between bodily and computational elements [9]. Figure 2 shows the architecture of Cyber-physical system.

2.2 *Real-Time Operating System*

A real-time operating system (RTOS) imagined to serve real-time applications that manner facts due to the fact it is far available in, normally without buffer delays. RT systems require specific help from OS [11]. Tenths of seconds or the shorter

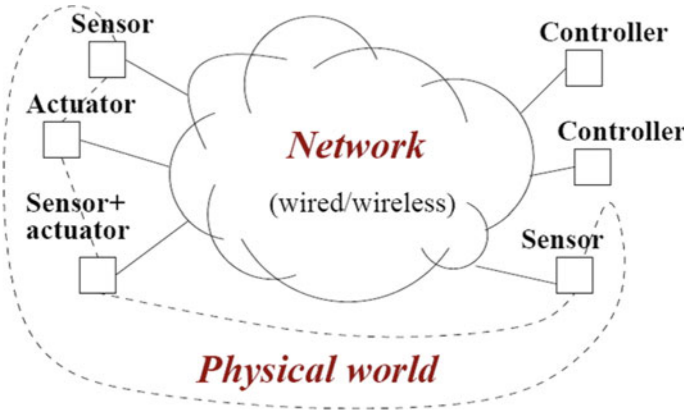


Fig. 2 Architecture of cyber-physical systems

increments of time are for measuring the working system processing time. RTOS is a time positive device which has nicely described steady time constraints. Processing should be carried out inside the described constraints or the failed devices [12]. They both are event driven or time sharing. Event-pushed structures switch among responsibilities primarily based on their priorities, while time-sharing structures switch the challenge primarily based on interrupts. Most RTOS uses a preemptive scheduling a set of rules.

2.3 Kernel

A kernel is the critical part of the working system that manages the operation of the pc and the hardware most appreciably reminiscence and CPU unit. There are two types of kernels. A microkernel, which only incorporates fundamental functionality. A monolithic kernel, which contains many device drivers. It is capable of doing at a simple level, speaking with hardware and handling assets, consisting of RAM and the CPU. The kernel plays a machine check and acknowledges additives, which include the processor, GPU and memory. It also tests for any related peripherals [7]. Kernel is the software program chargeable for running packages and offering comfortable access to the machine's hardware. Since there are many packages, and resources are constrained, the kernel also decides whilst and the way lengthy a software ought to run [5]. Figure 3 shows the architecture of Kernel.

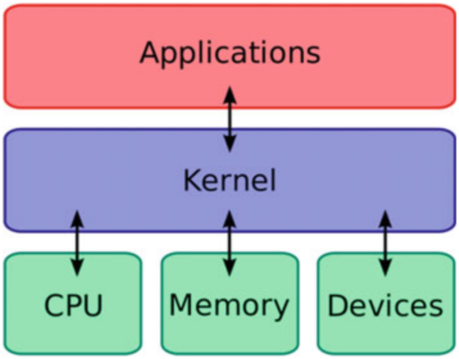


Fig. 3 Architecture of kernel

2.4 RTOS Scheduling Models

- Cooperative multitasking
- Preemptive multitasking
- Rate-monotonic scheduling
- Round robin scheduling.

2.4.1 Cooperative Multitasking

Non-preemptive multitasking is also known as cooperative multitasking is a style of pc multitasking in which the strolling device in no manner initiates a context switch from a system to each other technique. Strategies voluntarily yield and manage periodically in order to permit multiple programs to be run concurrently [13, 14]. This sort of multitasking is referred to as "cooperative" due to the fact all packages must cooperate for the entire scheduling scheme to paintings. The technique scheduler of an operating tool is known as a cooperative scheduler, having its function decreased right down to beginning the approaches and permitting them to move lower back control again to it voluntarily.

In comparison, preemptive multitasking interrupts programs and offers control to other methods out of doors the applications manipulate [15]. Cooperative multitasking is used with look ahead to in languages with a single-threaded event.

2.4.2 Preemptive Multitasking

The time period preemptive multitasking is used to differentiate a multitasking operating tool, which allows preemption of obligations, from a cooperative multitasking system wherein strategies or responsibilities should be explicitly programmed to yield once they do no longer need gadget resources [16]. In easy terms: Preemptive multitasking includes using an interrupt mechanism which suspends the presently executing way and invokes a scheduler to determine which way needs to execute next. Therefore, all techniques get a few amount of CPU time at any given time. In preemptive multitasking, the working device kernel can also initiate a context transfer to fulfill the scheduling insurance's precedence constraint, therefore preempting the lively undertaking. In general, preemption technique "earlier seizure of" is used when the excessive priority assignment at that stage seizes the present undertaking tasks, then it is referred to as preemptive scheduling.

Although multitasking strategies were in the beginning developed to allow multiple users to proportion a single system, it quickly has become apparent that multitasking becomes beneficial no matter the number of users [17]. Many working structures, from mainframes down to unmarried-person non-public computer systems and no-user manage structures (like those in robot spacecraft), have diagnosed the usefulness of multitasking assist for a variety of reasons. Multitasking makes it viable for a undetermined consumer to run multiple applications at the equal time, or to run "historical past" procedures even as keeping manage of the laptop.

2.4.3 Rate-Monotonic Scheduling

In pc technological knowledge, rate-monotonic scheduling (RMS) is a set of rules with priority utilized in real-time operating systems (RTOS) with a static-precedence scheduling elegance [18]. The static-level priorities are assigned in line with the cycle period of the pastime, so a shorter cycle length results in a higher venture precedence. Rate-monotonic system is used alongside the ones systems to provide scheduling ensures for a selected application.

2.4.4 Round Robin Scheduling

Round robin scheduling (RR) is one of the algorithms through device and community schedulers [19]. As the time period is generally used, time slices (additionally called time quanta) are assigned to system of every tasks in identical quantities and in round order, handling the determined processes without precedence (additionally referred to as cyclic government). Round robin scheduling is straightforward, smooth to position into impact, and hunger-loose [9]. Round robin scheduling also can be completed to different scheduling troubles, together with records packet scheduling in laptop networks.

3 Existing System

3.1 Estimation of WCET

The worst-case execution time of *ti* is same to the smallest of *t* gratifying the subsequent equality [20].

$$t = C_{it} + \sum_{j<i} \left[\frac{t}{T_j} \right] C_j. \tag{1}$$

C_{it} Worst-case execution time
D_i Relative deadline parameter
T_i Inter arrival separation time.

The worst-case workload of *i* with maximum precedence tasks over a determined interval of period *t*,

$$\sum_{i} \left[\frac{t}{T_j} \right] C_i \tag{2}$$

The worst-case workload of *i* with maximum precedence tasks over a determined interval of period *t*,

$$H_i(t) = t - W(t) \tag{3}$$

The pseudo-inverse function $X_i(c)$ of $H_i(t)$ is the smallest,

$$X_i(c) = \min_{t}\{: H_i(t) \geq c\} \tag{4}$$

The worst-case response time R_i of task is given by

$$R_{it} = \max_{k=1,2,\ldots} \{X_i - 1(kC_i) - (k-1)T_i\} \ldots \tag{5}$$

3.2 Task Response Time

The task response time has been estimated for the processor,
*K*th job in task T_i

$$R_{it} = \max_{k=1,\ldots k} \{X_i - 1(kC_i) - (k-1)T_i\} \tag{6}$$

$K^* < +\infty$

$$R_{ik} = X_i - 1(kC_i + I) - (k-1)T_i \geq X_i - 1(kC_i) - (k-1)T_i \tag{7}$$

It is non-decreasing function, [21]

$$R_{it} \geq \max_{k>k*}\{R_{ik}\} \geq \max_{k>K*}\{X_i - 1(kC_i) - (k-1)T_i\} \tag{8}$$

We assume that

$$\forall x :: f\mathrm{lb}(x) \leq f(x) \leq f\mathrm{ub}(x) \tag{9}$$

Worst-case response time R_{it},

$$W_i^{\mathrm{ub}}(t) \geq W_i(t) \tag{10}$$

Relationship for idle time,

$$H_i^{\mathrm{lb}}(t) = t - W_i^{\mathrm{ub}}(t) \leq t - W_i(t) = H_i(t) \tag{11}$$

The relationship between pseudo-inverse function,

$$X_i^{\mathrm{ub}}(c) = \min_t\left\{t{:}H_i^{\mathrm{lb}}(t) \geq c\right\} \geq \min_t\{t{:}H_i(t) \geq c\} = X_i(c) \tag{12}$$

$$R_i^{\mathrm{ub}} = \max_{k=1,2,\ldots}\left\{X_{i-1}^{\mathrm{ub}}(kC_i) - (k-1)T_i\right\} \geq R_i \tag{13}$$

The maximum amount of time that the processor executes,

$$W_i(t) = \sum_{j=1}^{t} w_j(t) \tag{14}$$

$W_j^0(t)$ is the maximum amount of time that the processor executes the task at any time interval,

$$\forall_j \forall t \quad w_j^0(t) \geq w_j(t) \tag{15}$$

The equation of linear bound is given by

$$w_j^0(t) \leq U_j t + C_j\left(1 - U_j\right) \tag{16}$$

The linear upper bound function,

$$W_i(t) = \sum_{j=1}^{i} w_j(t) \le \sum_{j=1}^{i} w_j^0(t)$$
$$\le \sum_{j=1}^{i}\left(U_j t + C_j\left(1 - U_j\right)\right) = W_i^{\mathrm{ub}}(t) \tag{18}$$

The worst-case response time for upper bound,

$$R_i \le \frac{C_{i+\sum_{j<i} C_j (1-U_j)}}{1 - \sum_{j<i} U_j} = R_i^{\mathrm{ub}} \tag{19}$$

$$W_i^{\mathrm{ub}}(t) = \sum_{j=1}^{i}\left(U_j t + C_j\left(1 - U_j\right)\right) \tag{20}$$

$$H_i^{\mathrm{lb}}(t) = t\left(1 - \sum_{j=1}^{t} U_{ij}\right) - \sum_{j=1}^{t}\left(C_j\left(1 - U_{ij}\right)\right) \tag{21}$$

It is invertible,

$$X_i^{\mathrm{ub}}(h) = \frac{h + \sum_{j=1}^{i} C_j\left(1 - U_{ij}\right)}{1 - \sum_{j=1}^{i} U_{ij}} \tag{22}$$

4 Proposed System

4.1 The Dynamic Cloud Manufacturing Scheduling

4.1.1 The Average Service Utilization Rate

$$U_r(t_1, t_2) = \left(\sum_{i=1}^{N}\sum_{j=1}^{ni} u_{i,j}(t_1, t_2)\right) \Big/ \left(\sum_{i=1}^{N} n_{ir}\right) \tag{23}$$

The average carrier utilization price U is calculated via price $u_{i,j}$ within the cloud manufacturing platform.

4.1.2 Average Task Delay Time

Reducing the common task put off time of all duties

$$D_r(t_1, t_2) = \left(\sum_{i=1}^{M(t_1,t_2)} d_i \right) \Bigg/ (M_r(t_1, t_2)) \tag{24}$$

$D_r(t_1, t_2)$ is for average task delay time of the cloud manufacturing platform. The delay time d_i of task can be calculated

$$d_{ir} = F_{ir} - a_{ir} \tag{25}$$

The completion time F_i of T_i is equal to the last subtask of T_i

$$F_{ir} = f_{ir,mir} \tag{26}$$

4.1.3 Weighted Average Task Delay Time

In cloud manufacturing environment, the different tasks will have different priority, and the weighted average delay time $W_r(t_1, t_2)$ of all tasks should be considered and can be calculated

$$W_r(t_1, t_2) = \left(\sum_{i=1}^{M_{ir}(t_1,t_2)} p_{ir} d_{ir} \right) \Bigg/ \left(\sum_{i=1}^{M_r(t_1,t_2)} p_{ir} \right) \tag{27}$$

4.1.4 Proportion of Delayed Task

The proportion of delayed task during time span $[t_1, t_2]$

$$R_r(t_1, t_2) = \frac{|B|}{M_r(t_1, t_2)} \tag{28}$$

$$B = \{T_i / C_i < F_i, t_1 \le a_i, F_i \le t_2\} \tag{29}$$

4.1.5 Constraints

There are varieties of constrains for the scheduling solutions for the dynamic cloud production scheduling problems

- Constrains of service selection
- Constrains of subtask start time

Constrains of Service Selection

For the constrains of service selection, the subtask can handiest pick provider which can be able to execute the subtasks

$$v_{h,g} = 1 \tag{30}$$

where

$$h_r = h_{x,y} \tag{31}$$

$$g_r = g_{i,j} \tag{32}$$

Constrains of Subtask Start Time

Here, there are two tasks which are executing in a platform. The begin time of an intermediate mission cannot be earlier than the completion time of the front subtask

$$a_{ir} \leq z_{i,1} \tag{33}$$

$$f_{i,j-1} \leq z_{i,j} \tag{34}$$

where $1 \leq i \leq M_r(t_1, t_2)$ and $2 \leq j \leq m_i$.

5 Results and Discussion

Figures 4, 5, 6, 7, 8, 9 and 10.

6 Conclusion

The challenge contributions may be summarized as follows: the test for a WCET estimation with EDF scheduling algorithm that adopts a worldwide method to task allocation upon uniprocessors. That is, the behavior of algorithm EDF—one such formerly described [10, 12] static-precedence global scheduling set of rules upon uniprocessor systems. The simple sufficient conditions for determining whether any given periodic undertaking system will be successfully scheduled by way of algorithm EDF-VD upon a given uniprocessor platform. The situation of the reaction time was calculated for further scheduling of obligations under EDF-VD algorithm.

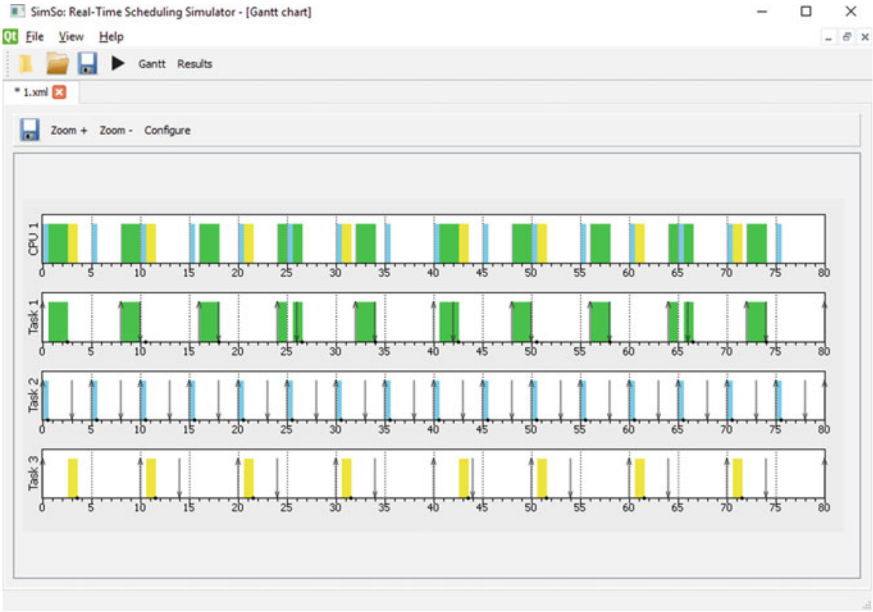
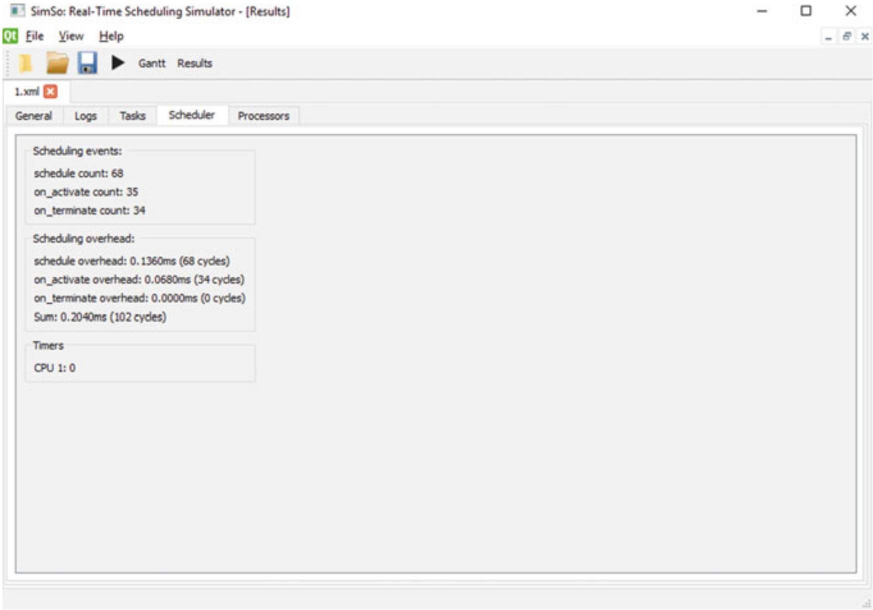


Fig. 4 Gantt chart for uniprocessor scheduler under earliest deadline first


SimSo: Real-Time Scheduling Simulator - [Results]
File View Help
Gantt Results
1.xml
General Logs Tasks Scheduler Processors

Scheduling events:

schedule count: 68

on_activate count: 35

on_terminate count: 34

Scheduling overhead:

schedule overhead: 0.1360ms (68 cycles)

on_activate overhead: 0.0680ms (34 cycles)

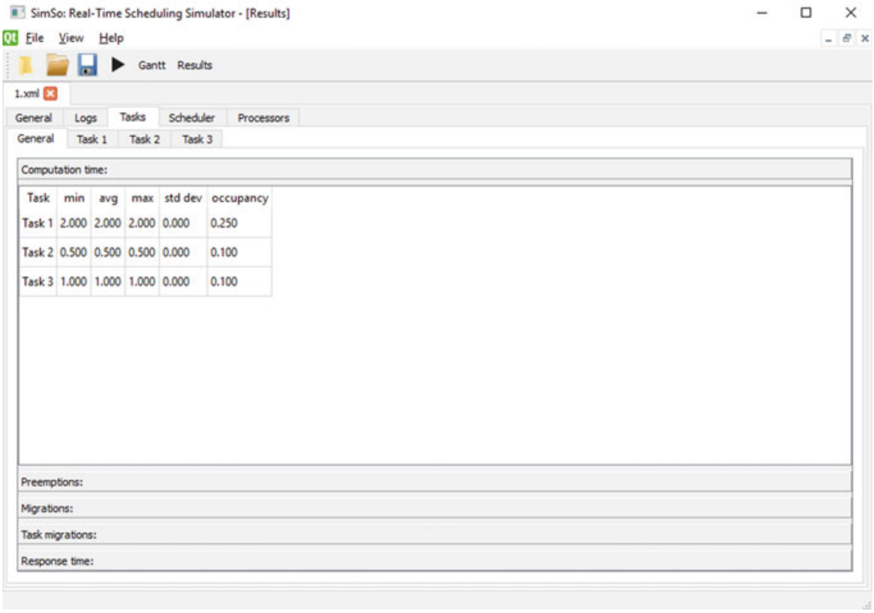
on_terminate overhead: 0.0000ms (0 cycles)

Sum: 0.2040ms (102 cycles)

Timers

CPU 1: 0

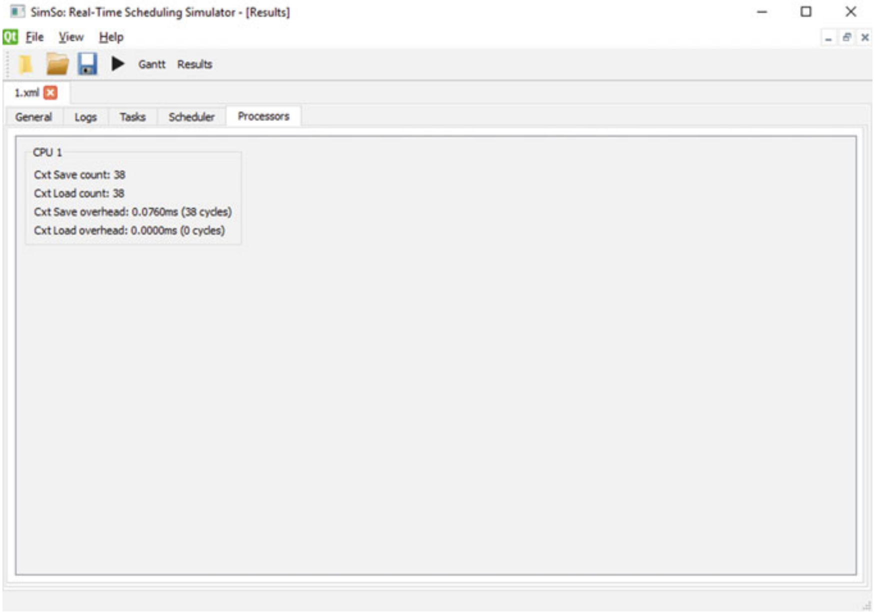
Fig. 5 Timing overhead for uniprocessor scheduling under earliest deadline first


SimSo: Real-Time Scheduling Simulator - [Results]
File View Help
Gantt Results
1.xml
General Logs Tasks Scheduler Processors
General Task 1 Task 2 Task 3
Preemptions:
Migrations:
Task migrations:
Response time:

Computation time:

Task	min	avg	max	std dev	occupancy
Task 1	2.000	2.000	2.000	0.000	0.250
Task 2	0.500	0.500	0.500	0.000	0.100
Task 3	1.000	1.000	1.000	0.000	0.100

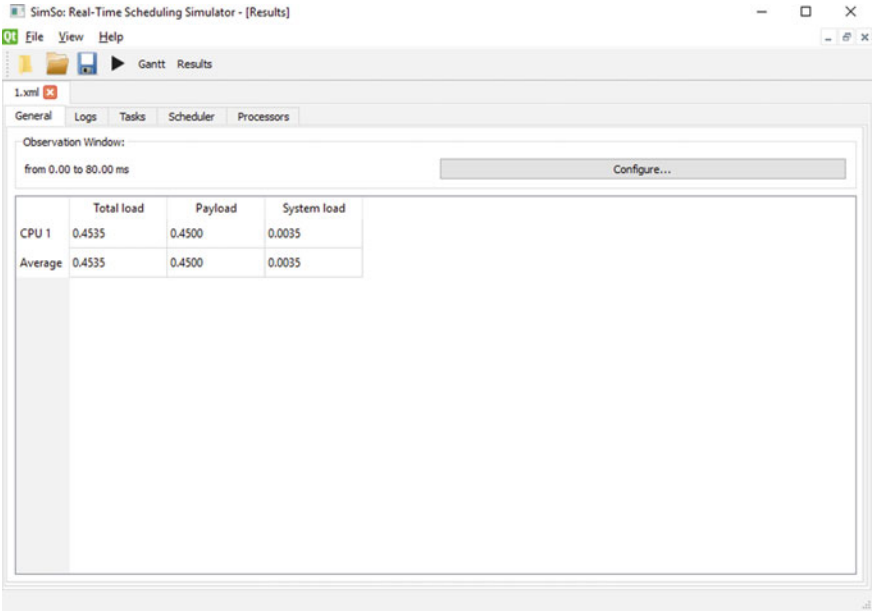
Fig. 6 Task distribution under earliest deadline first scheduler


SimSo: Real-Time Scheduling Simulator - [Results]
File View Help
Gantt Results
1.xml
General Logs Tasks Scheduler Processors

CPU 1

Cxt Save count: 38
Cxt Load count: 38
Cxt Save overhead: 0.0760ms (38 cycles)
Cxt Load overhead: 0.0000ms (0 cycles)

Fig. 7 CPU cycles (save and load count)

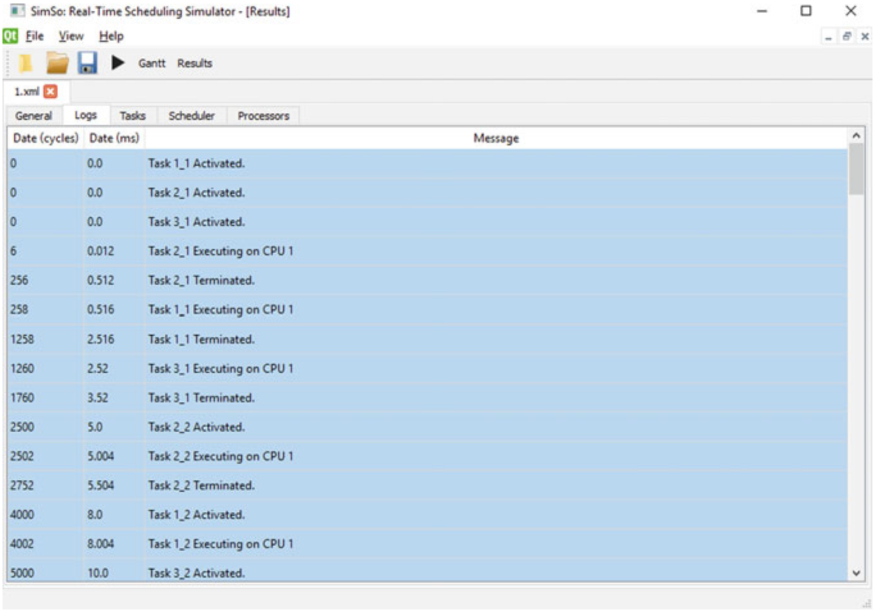

SimSo: Real-Time Scheduling Simulator - [Results]
File View Help
Gantt Results
1.xml
General Logs Tasks Scheduler Processors
Configure...

Observation Window:

from 0.00 to 80.00 ms

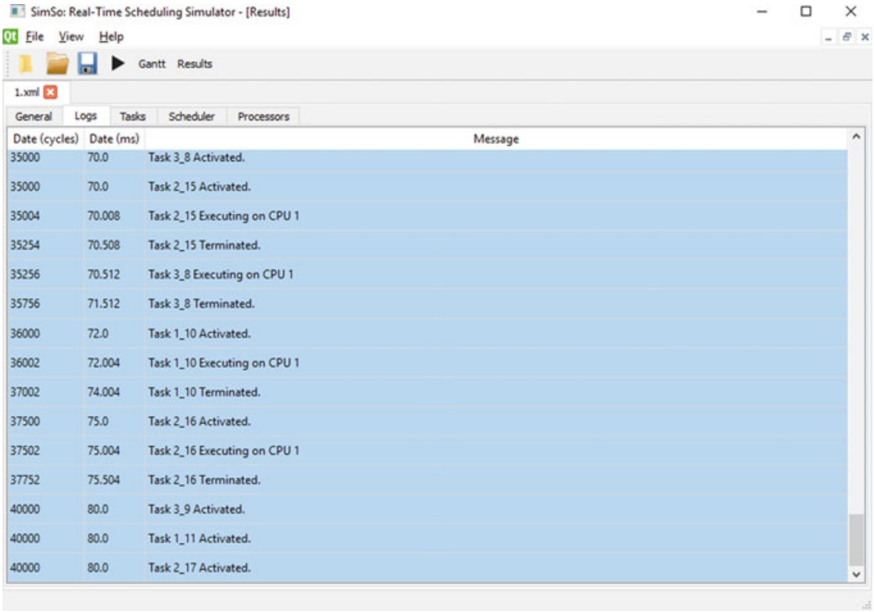
	Total load	Payload	System load
CPU 1	0.4535	0.4500	0.0035
Average	0.4535	0.4500	0.0035

Fig. 8 Load by CPU under simulation


SimSo: Real-Time Scheduling Simulator - [Results]
File View Help
Gantt Results
1.xml
General Logs Tasks Scheduler Processors

Date (cycles)	Date (ms)	Message
0	0.0	Task 1_1 Activated.
0	0.0	Task 2_1 Activated.
0	0.0	Task 3_1 Activated.
6	0.012	Task 2_1 Executing on CPU 1
256	0.512	Task 2_1 Terminated.
258	0.516	Task 1_1 Executing on CPU 1
1258	2.516	Task 1_1 Terminated.
1260	2.52	Task 3_1 Executing on CPU 1
1760	3.52	Task 3_1 Terminated.
2500	5.0	Task 2_2 Activated.
2502	5.004	Task 2_2 Executing on CPU 1
2752	5.504	Task 2_2 Terminated.
4000	8.0	Task 1_2 Activated.
4002	8.004	Task 1_2 Executing on CPU 1
5000	10.0	Task 3_2 Activated.

Fig. 9 Log file of the scheduler under earliest deadline first algorithm



```
Date (cycles)  Date (ms)  Message
35000          70.0       Task 3_8 Activated.
35000          70.0       Task 2_15 Activated.
35004          70.008     Task 2_15 Executing on CPU 1
35254          70.508     Task 2_15 Terminated.
35256          70.512     Task 3_8 Executing on CPU 1
35756          71.512     Task 3_8 Terminated.
36000          72.0       Task 1_10 Activated.
36002          72.004     Task 1_10 Executing on CPU 1
37002          74.004     Task 1_10 Terminated.
37500          75.0       Task 2_16 Activated.
37502          75.004     Task 2_16 Executing on CPU 1
37752          75.504     Task 2_16 Terminated.
40000          80.0       Task 3_9 Activated.
40000          80.0       Task 1_11 Activated.
40000          80.0       Task 2_17 Activated.
```

Fig. 10 Log file of the scheduler under earliest deadline first algorithm

The outputs were visualized the use of the Gantt charts. The deadlines and miss had been honestly seen within the output.

The circumstance of earliest deadline first together with virtual deadline by estimating the shortest last time set of rules, the system model can be designed, and outputs might also explicit sufficient schedulable project over uniprocessor platforms. The uniprocessor set of rules can be better in addition to create a platform on multiprocessor environments.

References

1. Nelissen EG, Nélis V, Tovar E (2015) How realistic is the mixed-criticality real-time system model? In: Proceedings of the 23rd international conference on real time and networks systems (RTNS ’15). New York, pp 139–148
2. Liu C, Layland J (1973) Scheduling algorithms for multiprogramming in a hard real-time environment. J ACM 20(1):46–61
3. Davari S, Dhall SK (1986) An on-line algorithm for real-time tasks allocation. In: Proceedings of real-time systems symposium, pp 194–200
4. Funk S, Goossens J, Baruah S (2001) On-line scheduling on uniform multiprocessors. In: Proceedings of real-time systems symposium, pp 183–192
5. Burns, Davis R (2016) Mixed-criticality systems: a review, 7th edn. http://www-users.cs.york.ac.uk/~burns/review.pdf. Accessed 37 Mar/Apr 2018
6. Oh DI, Baker TP (1998) Utilization bounds for N-processor rate monotone scheduling with static processor assignment. Real-Time Syst Int J Time-Crit Comput 15:183–192

7. Buxton JN, Randell B (eds) (1970) Software engineering techniques: report of a conference sponsored by the NATO science committee, 27–31 October 1969. Scientific Affairs Division, NATO, Rome, Brussels
8. Dertouzos M (1974) Control robotics: the procedural control of physical processors. In: Proceedings of IFIP congress, pp 807–813
9. Vestal S (2007) Preemptive scheduling of multi-criticality systems with varying degrees of execution time assurance. In: Proceedings in real-time systems symposium. Tucson, AZ, pp 239–243
10. Dhall SK, Liu CL (1978) On a real-time scheduling problem. Oper Res 26:127–140
11. Leung J, Whitehead J (1982) On the complexity of fixed-priority scheduling of periodic, real-time tasks. Perform Eval 2:237–250
12. Burns, Davis R (2013) Mixed criticality on controller area network. In: Proceedings of 2013 25th Euromicro international conference on real-time systems (ECRTS '13). Paris, pp 125–134
13. Baruah S, Burns A (2011) Implementing mixed criticality systems in Ada. In: Romanovsky A, Vardanega T (eds) Reliable software technology—Ada Europe. Springer, Edinburgh, pp 174–188
14. Baruah S (2016) Schedulability analysis for a general model of mixed criticality recurrent real-time tasks. In: Proceedings of 2016 IEEE real-time systems symposium
15. Fenn J, Raskino M (2008) Mastering the hype cycle: how to choose the right innovation at the right time, Harvard Business School Press
16. Sha L, Rajkumar R, Lehoczky J, Ramamritham K (1988) Mode change protocols for priority-driven preemptive scheduling. J Real-Time Syst 1(3):243–264
17. Sharma RK et al (2005) Balance of power: dynamic thermal management of internet data centers
18. Ernst R, Di Natale M (2016) Mixed criticality systems—a history of misconceptions? IEEE Des Test 33(5):65–74
19. Davari S, Dhall SK (1985) On a real-time task allocation problem. In: Proceedings 19th Hawaii international conference on system science
20. Baruah S (2016) Schedulability analysis of mixed-criticality systems with multiple frequency specifications. In: Proceedings of the 16th international conference on embedded software (EMSOFT). Pittsburgh
21. Baruah S, Chattopadhyay B (2013) Response-time analysis of mixed criticality systems with pessimistic frequency specification. In: Proceedings of IEEE international conference on embedded real-time computing systems application (RTCSA). Taipei, Taiwan

Automatic Solid Waste Dumping Alert System

K. Bhuvana, S. Deeksha, M. Deepthi and A. D. Radhika

Abstract One of the fundamental problems the world facing today is waste management. The main problem with waste management is that the dustbins placed by the municipal company are filled earlier and overflow before the next cleaning process (Mirchandani in 2017 International conference on big data, IoT and data science (BID), pp 73–76, 2017 [1]). This poses environmental threats and causes health problems. This dangerous scenario can be avoided by installing an alarm system for the dumping of solid waste. The main objective of this paper is to alert the municipal web server to clearance of overloaded dustbins when solid waste flows over the public dustbin. Here, we can build the dustbins using the MCU, RFID, GPS, ultrasonic sensor and Wi-Fi module to prevent the overflow of the dustbins.

Keywords Node MCU · GPS · RFID · Ultrasonic sensor · Wi-Fi

1 Introduction

India's main problem is waste management, which faces rapid population growth, disorganization of the municipal government, lack of public awareness and public involvement. Because of this, the overflow of waste in dustbins leads to an unhygienic environment, which poses health problems, and there is also no clearance of the waste on time. People should be responsible enough to use the dustbins properly and not throw the waste out of the overloaded dustbins [2]. To prevent this, the dustbins can be properly placed. Currently, we do not find advanced systems that use the method of alerting municipal web servers to overfilled dustbins when the amount of garbage

K. Bhuvana · S. Deeksha · M. Deepthi · A. D. Radhika (✉)
Department of Computer Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India
e-mail: radhika.ad@vvce.ac.in

K. Bhuvana
e-mail: bhuvanak703@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_91

exceeds the capacity of the dumpster. This system is mainly focused on this. In order to overcome these problems, we use dumpsters that include alert systems to alert the municipal web server so that they can identify the locations of the dumpsters using the GPS, and RFID is used for the unique ID verification process and helps to provide an alert system for the overloaded dumpsters. When the dustbin is overloaded, the Wi-Fi module sends the notice to the individual concerned. By using this technology, we can achieve the cleanest and efficient use of intelligent dumpsters at a lower cost [3].

2 Existing Methodology

The existing solid waste management system includes the conventional dumping method in a dustbin, and then, the cleaning process performed by the municipality concerned. Although this method is concerned with the management of solid waste, it can lead to unhygienic environments, air pollution and some health problems if there is no proper clearance of waste on time [4]. And there is also no proper way to automatically alert the municipality concerned about clearing the filled dustbins. The waste management system in different countries can be different, and it will also be different in urban and rural areas [5]. It is, therefore, necessary to have an automatic system that senses the waste level in dustbins and alerts the people concerned about the cleaning process so that we can avoid overloading the dustbins. This paper is about giving an alert message about the fully filled dustbins to the municipal web server. Here, we use the efficient and cost-effective node MCU instead of Arduino, using sensors, we feel the level of waste, and RFID tags and GPS are used to locate the fully filled dustbin areas in an amortized manner. This paper, therefore, proposes an automatic solid waste management system that is cost-effective and efficient.

3 System Architecture

We use components such as GPS, MCU node, wireless module, RFID and ultrasonic sensors in system architecture. If the dustbins contain an MCU node, an ultrasonic sensor is connected to the MCU node. This is essentially used to detect the level of dumpsters, whether or not they are fully filled. Then, if the sensor senses the dump level as fully filled, it uses the Wi-Fi module and sends a message to the person or web server of the municipal corporation that the dumpsters are cleaned as they are fully filled. The related people of the municipality will then know that the dustbin is fully filled with the alert system provided. In this case, the GPS is used to locate the location of the dustbins by sending the current position of the dustbin or the actual tracking position of the dustbin, and the RFID is used to provide each dustbin with a unique identification number to ensure which of the dustbin in a located area is to be cleaned. This can be done using the RFID tag and the RFID reader where the

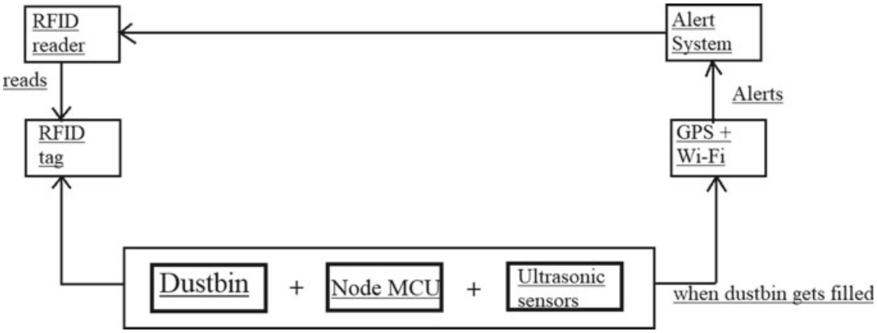


Fig. 1 Architecture of components used in dustbin

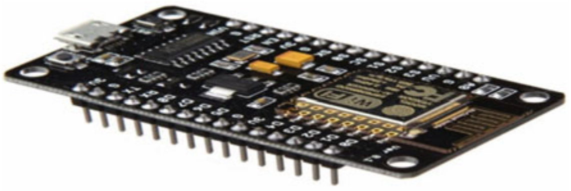
RFID reader is used to obtain information from an RFID tag that is also used for tracking objects. Radio waves are used here to transfer the data to a reader from the tag. Therefore, we can locate the dustbin using the GPS and RFID tags, and the cleaning process is performed by the individual concerned [6] as shown in Fig. 1.

4 Proposed Methodology

4.1 Node MCU

Node MCU is an open-source IoT platform, and it uses a Lua scripting language, a lightweight multi-paradigm programming language designed primarily for embedded systems and customers. MCU node is a development board with a popular Wi-Fi chip ESP8266. Like a microcontroller, ESP8266 can be programmed. It can, therefore, be of great benefit to Arduino, who can connect to the Internet via Wi-Fi. The breakout board ESP8266 has limited pins in the chip itself with many output ports [7] as shown in Fig. 2.

Fig. 2 Node MCU



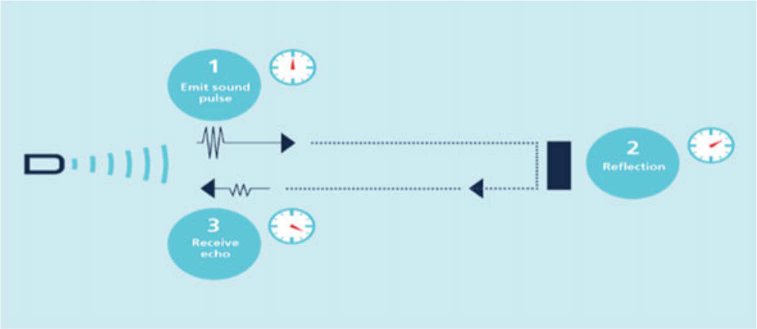


Fig. 3 Ultrasonic sensor

4.2 Ultrasonic Sensors

The HC-SR04 ultrasonic sensors are made of piezoelectric crystals, which use high-frequency sounds to resonate the desired frequency and convert acoustic energy into electric energy and vice versa. The exact distance between the object and the sensor is measured, and the time intervals between transmission and reflection are measured as shown in Fig. 3. The distance change is calculated repeatedly and produced using the formal [8]

$$\text{Test distance} = \text{high level time} * \text{velcity of sound}(340\,\text{M/S})/2.$$

This multiplies the value by 1/2 or 0.5 because 't' is the time for the distance to go and return. Initially, a pulse is generated at the base of the distance in the ultrasonic sensor to send the data to the MCU node. The starting pulse is approximately 10 µs, and the PWM signal at the base of the distance is 150–25 µs. If there is no obstacle, the 38 µs pulse is generated for the MCU node, which determines that no objects are present.

4.3 GPS

GPS is a device that interacts with the GPS satellites to receive the information required from the satellites required to calculate the geographical position of the device. In this article, we will interface the GPS module with the MCU node. A simple server of the local web, i.e. using node MCU, the municipal server is created, and the location details are updated on that server website. The GPS is used here to send tracking position data in real time.

4.4 Wi-Fi Module

Stations (STA) are those devices connected to the wireless network. An access point (AP) provides a Wi-Fi connection. The other access point end is connected to the cable network. Wi-Fi network accesses point to the Internet. SSID recognizes every access point where SSID means identifier service set. This is the network name you choose when you connect a station to the Wi-Fi (or call it a device). Each ESP8266 module can be connected to the Wi-Fi network as a station. It is thus able to connect stations to these modules. The third ESP8266 can operate both in the station and soft point mode at the same time as shown in Figs. 4, 5 and 6.

4.5 Radio-Frequency Identification

Radio-frequency identification (RFID) is essentially used for the purpose of verification. Radio waves are used here for reading and capturing information stored on a tag attached to an object. The main advantage over bar code is that, unlike a bar code, it can be used to read the tag from a distance of up to several feet and does not

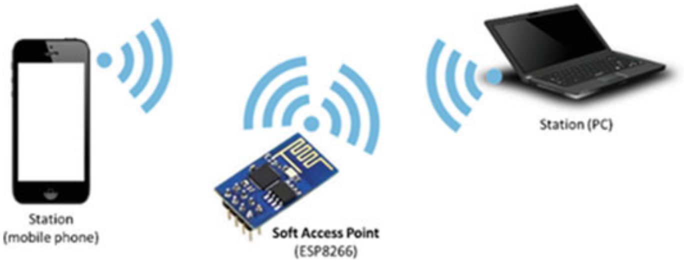


Fig. 4 ESP8266 operating in the soft access point mode

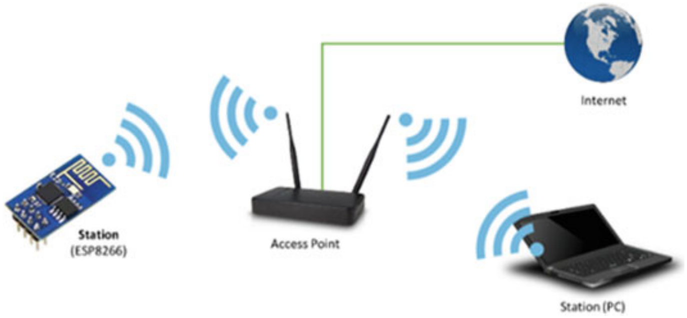


Fig. 5 ESP8266 operating in the station mode

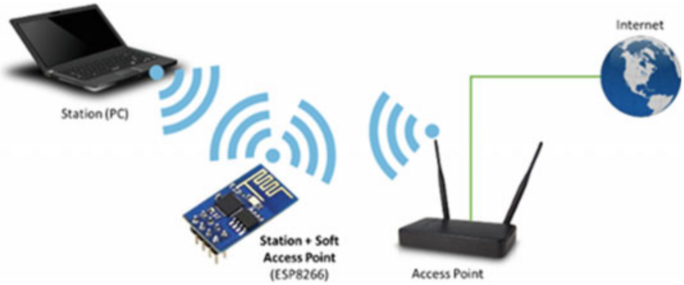


Fig. 6 ESP8266 operating in the station + soft access point mode

need to be in the reader's direct line-of-sight. RFID can, therefore, be used instead of the bar code. An RFID reader is used here to read the information from the tag and therefore to carry out the identification process. It has mainly two types of active and passive RFID. Because the tags do not require batteries or maintenance in passive RFID, we can use them here. The tags are also small enough to fit a label. And it has three parts, an antenna, a semiconductor chip and a kind of encapsulation attached to it. These are used to perform the actual identification operations in which the antenna captures energy and transfers to the ID of the tag, and the chip coordinates this process, whereas the encapsulation maintains the integrity of the tag and protects it against external conditions [9, 10].

5 Conclusion

The aim of the solid waste dumping alert system is to promote a decent quality of life, a clean and sustainable environment. The system proposed is an approach for the planning and management of solid waste. This system prevents the irregular cleaning of public bins by sending an alert to the person concerned at a regular time. The technologies used here give visibility to the management of solid waste and help to clear it regularly in public dustbins. The clearance here depends on whether the dumpster is full, half or empty. It also proposes reducing costs and the efficient use of intelligent dumpers. In general, it is intended to create a clean and green environment.

Acknowledgements The authors express gratitude towards the assistance provided by Accendere Knowledge Management Services Pvt. Ltd. in preparing the manuscripts. We also thank our mentors and faculty members who guided us throughout the research and helped us in achieving desired results.

References

1. Mirchandani S, Wadhwa S, Wadhwa P, Joseph R (2017) IoT enabled dustbins. In: 2017 International conference on big data, IoT and data science (BID), pp. 73–76
2. Vasagade TS, Tamboli SS, Shinde AD (2017) Dynamic solid waste collection and management system based on sensors, elevator and GSM. In: 2017 International conference on inventive communication and computational technologies (ICICCT), pp. 263–267
3. Shrivastava P, Mishra S and Katiyar SK (2015) A review of solid waste management techniques using GIS and other technologies. In: 2015 International conference on computational intelligence and communication networks (CICN), pp. 1456–1459
4. Riya AK, Yuvraj KK (2018) A review paper on IoT based smart garbage alert system. Int J Sci Res 7(5):1810–1813
5. Pardini K, Rodrigues JJPC, Kozlov SA, Kumar N, Furtado V (2019) IoT-based solid waste management solutions: a survey. J Sens Actuator Netw 8(5):1–25
6. Draz U, Ali T, Khan JA, Majid M, Yasin S (2017) A real-time smart dumpsters monitoring and garbage collection system. In: 2017 Fifth international conference on aerospace science and engineering (ICASE)
7. Mamatha D, Priyanka KE, Nidhi R, Pooja K (2017) Smart garbage monitoring system using node MCU. In: international conference on signal, image processing communication and automation, pp. 238–245
8. Kumar NS, Vuayalakshmi B, Prarthana RJ, Shankar A (2016) In: 2016 IEEE region 10 conference (TENCON) IOT based smart garbage alert system using Arduino UNO, pp. 1028–1034
9. Manisha J, Sanket H, Lakshmi HR (2018) SmartBin-automatic waste segregation and collection. In: 2018 Second international conference on advances in electronics, computers and communications (ICAECC)
10. Muthukumaran P, Sarkar SB (2013) Solid waste disposal and water distribution system using the mobile adhoc network. In: 2013 international conference on emerging trends in communication, control, signal processing and computing applications (C2SPCA)

User Authentication for Mobile Phones by Pseudo Signature Using CNN

Christy James Jose and M. S. Rajasree

Abstract Today, majority of the world population has one companion with them always. This companion has all the private information of the person. That companion is the smart phone. Considering the private data its holding, the unauthorized usage by friends, family members and strangers are to be avoided. The traditional way of preventing the unauthorized usage is to lock the device with PIN numbers, graphical patterns, fingerprint sensors and face unlock mechanisms [1]. The last two are available with high-end phones only. Even these mechanisms rely on the first-mentioned methods in case of a sensor failure. Primary authentication mechanisms could be easily breached. In this paper, we are investigating the usage of handwritten signatures as an authentication method. We are suggesting a Pseudo signature, a signature drawn on the touch screen of the phone using the finger tip. We have used convolutional neural network classifiers to classify the genuine user and intruder. Experimental results show our suggestion is promising and it could be used as an easy-to-use user-friendly primary authentication for smart phones.

Keywords Authentication · Classification · Smart phones · Convolutional neural networks

1 Introduction

Primary authentication on smart phones are based on PIN, GUI passwords, fingerprint sensors and face unlock mechanisms. Most of the users are either satisfied with these mechanisms or does not use it at all [2]. Protection of private data and prevention of unauthorized usage of the device are the need of the hour. Problems with these

C. J. Jose (✉)
Government Engineering College, Barton Hill, Thiruvananthapuram, Kerala, India
e-mail: jjchristy@gmail.com

M. S. Rajasree
APJ Abdul Kalam Technological University, Thiruvananthapuram, Kerala, India
e-mail: rajasree40@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_92

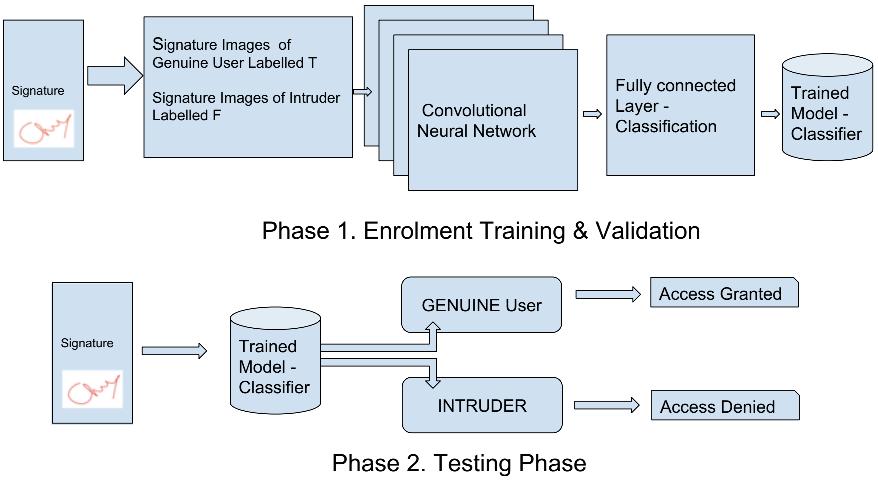
methods lies in the fact that all these methods can be breached and ownership of the device can be taken over by an intruder [3]. Our proposal suggests handwritten signature, more precisely, pseudo signature drawn on the touchscreen of the mobile phones for authentication. The motivation behind the suggestion is the fact that graphical passwords or PIN numbers can be stolen by intruders by the methods like shoulder surfing and smudge attack. Moreover, there is a chance of forgetting the pattern or PIN number by the genuine user himself. Signatures have been used by everyone for the purpose of identification and banking purposes. The advantage of using signature is that usually nobody forgets his signature and we assume that nobody can imitate others signature hundred percentage perfect. So, any person imitating a genuine users signature to unlock a mobile device will be blocked instantly and we expect this method will have highest rate of user acceptance since there is no need to remember anything other than his own signature which is a very personal bio metric. Here, what we suggest is that every user has to draw his signature with his fingertip on the touch screen of his mobile phone. The device will verify the signature with an already trained model and grants access based on the classifier result.

2 Related Work

Khuwaja and Laghari [4] proposed an offline signature recognition system to identify the handwritten signatures using a neural network which is trained with the low-resolution scanned images of the handwritten signatures. Eventhough they could achieve an accuracy of 98%, there was no mention about the capability to reject a forged signature. We could see so many works on signature verification, but the difference with our work is that we are analyzing a signature drawn on the touch screen using the finger, whereas most of the works have studied signature drawn on paper using a pen or signature drawn using a stylus on touch screen. Chen et al. [5] suggested pseudo signature as a bio metric, but the data they have created was of shapes like circle, triangle, etc., drawn by different subjects. They could achieve an FAR of 20%. Nowadays, the number of phones came bundled with a stylus are few. Some of the works had used the well-known algorithms. Fischer et al. [6] used dynamic time warping (DTW). In Wijesoma et al. [7] had used the root-mean-square (RMS). Hidden Markov Model (HMM) was used by Fierrez et al. [12]. These algorithms were used match the time-series data of the signature. The works by Feng and Wah [9] were utilizing a statistical similarity evaluation by making use of the descriptive features of the signature. Fierrez Aguilar et al. [8] has projected unique features like the total duration taken to draw the signature, pen pressure and number of times the pen lost its contact. Our work proposes deep learning as a solution to our problem of classification. We had came through the work by Iranmanesh et al. [10] that has analyzed the possibility of employing machine learning for the classification. According to them, they have used it to improve the accuracy. Their work has shown an accuracy of 82.42 but failed in recognizing an imitated signature. Auto encoder was used in the work by Nam et al. [11] and they could achieve an accuracy of 92% and were successful in recognizing the imitated signatures.

3 Proposed Method

The block diagram of the work is illustrated in Fig. 1. We would capture the signature as an image using a suitable application. Then, use this image to recognize the user. Since its been drawn casually on the screen, it may not be exactly matching a persons signature drawn on a paper. So matching a pseudo signature with a signature drawn on paper is out of scope. But we can be sure that the movement of your finger to draw the signature on the screen would be showing away the same direction and almost same speed in both cases.In Phase 1, Enrollment, Training and Validation, the signatures of both genuine user and intruder are collected and labeled to form the training and testing data. As we can see, the collected number of samples would be low in numbers. In a real-time situation, this would be true. No user would be interested in drawing a lot of his signature for enrollment. Keeping in mind this situation, we are suggesting data augmentation so that the number of samples required for training the CNN would be sufficient. Operations performed were rotation up to 10°, zoom, shear and skew. Our assumption was that the pseudo signatures are time variant and it has all the above-said deformations over time. For our test, we have used 260 samples for training and 32 for validation. Finally, individual signature samples were tested using the trained model. Finally, individual signature samples were tested using the trained model. We can set threshold levels for the confidence levels of the classifier.


Signature
Signature Images of Genuine User Labelled T
Signature Images of Intruder Labelled F
Convolutional Neural Network
Fully connected Layer - Classification
Trained Model - Classifier
Signature
Trained Model - Classifier
GENUINE User
INTRUDER
Access Granted
Access Denied

Phase 1. Enrolment Training & Validation

Phase 2. Testing Phase

Fig. 1 Block diagram

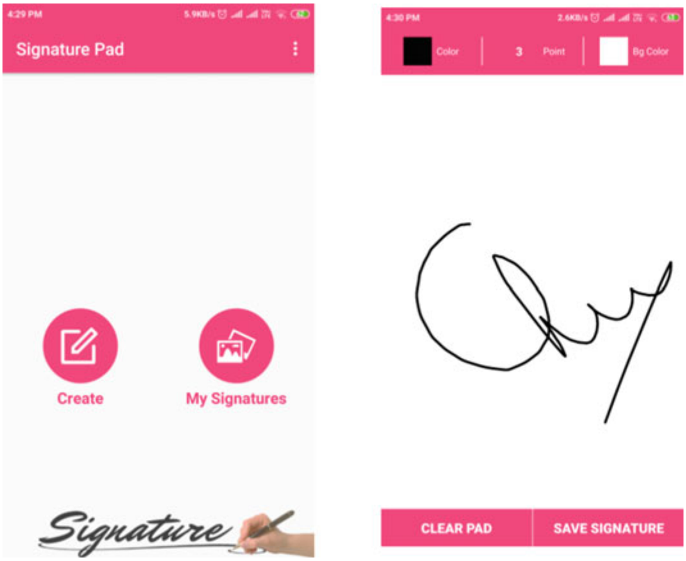


Fig. 2 Signature pad android app

We may grant access to non-critical applications if it is greater than 60% similarity and for critical applications, it may be greater than 90%.

3.1 Data Set Creation

We have created our own data set for the experiment. We have chosen three subjects for this experiment. All male candidates from our department in the age group 24–43 years. Out of this three subjects, 1 is designated as genuine one and other two as intruders. All data has been generated in a single session. Prior to data collection, the designated genuine user was asked to display on the board how he is drawing his signature. The details include the staring point, the direction followed and the normal speed. This was repeated more than once. Genuine user was also directed to sign on the touch screen in the presence of other subjects so that they can see the signature details. For the data collection, we have used an App “Signature Pad” from the Google Play Store. Screen shot of the app is given in Fig. 2. It essentially stores whatever a user draws in the given window on the touch screen of the phone as an image in the phone memory in JPEG format. The Signature Pad application has a fixed size window. On this window, all subjects are supposed to draw the pseudo signature using their finger tip. We have generated the data set in a single session. All the signature images are stored in the internal memory of the phone. We have copied these images and labeled them. Label T is given to the genuine user signature and

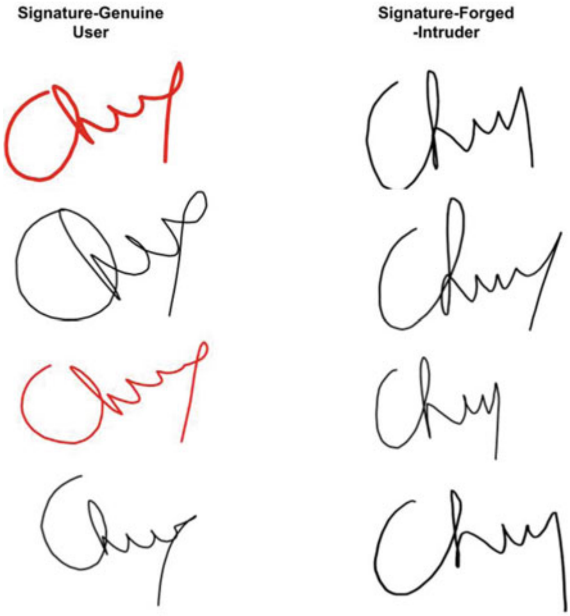


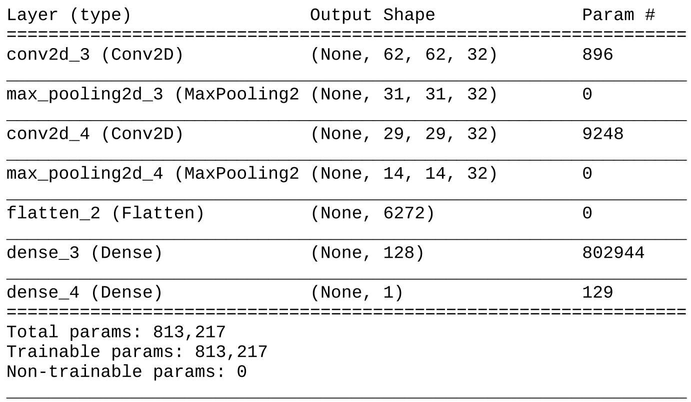
Fig. 3 Signature samples

label F to all other image. So we have taken more than 20 numbers of samples from the genuine user and others are asked to imitate the signature (Fig. 3). Help from the genuine user was there as to show how he signs. This is to ensure that whoever tries to imitate the signature will have a close resemblance to the original one and we would study performance of the classifier in a perfectly mimicked signature. Data augmentation was performed on both training and test data, so as to increase the number of samples. Then, these images were used for training and testing our convolution neural network. We have used the Python 3.6 along with Keras deep-learning library for all the coding and simulations.

In CNN-based classifier, convolution is performed on the image data set and it extracts features in that image. Ultimately, it helps the machine to learn the image characteristics. Pooling is the technique used to reduce the image size without losing features. Flattening is used to transfer two-dimensional matrix of features into vector features, so that it can be given as input to a neural network classifier (Fig. 4).

4 Results and Discussion

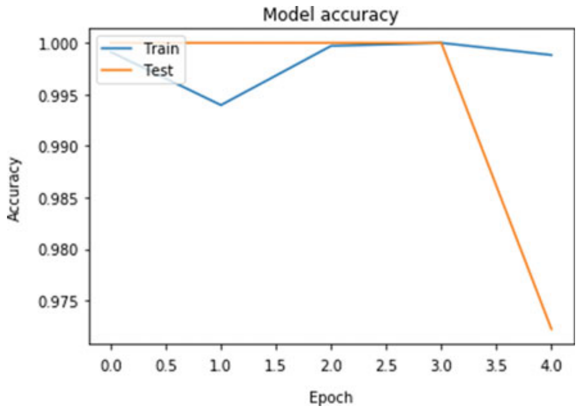
In this study we have used CNN for feature extraction and a fully connected layer for classification of genuine user vs an intruder. The training and validation setup are described as follows, Th epoch set to 5 after some trial and error, each epoch has taken approximate 1–1 min and twenty seconds to complete. Both training loss and



```
Layer (type)                 Output Shape              Param #
=================================================================
conv2d_3 (Conv2D)            (None, 62, 62, 32)        896
_________________________________________________________________
max_pooling2d_3 (MaxPooling2 (None, 31, 31, 32)        0
_________________________________________________________________
conv2d_4 (Conv2D)            (None, 29, 29, 32)        9248
_________________________________________________________________
max_pooling2d_4 (MaxPooling2 (None, 14, 14, 32)        0
_________________________________________________________________
flatten_2 (Flatten)          (None, 6272)              0
_________________________________________________________________
dense_3 (Dense)              (None, 128)               802944
_________________________________________________________________
dense_4 (Dense)              (None, 1)                 129
=================================================================
Total params: 813,217
Trainable params: 813,217
Non-trainable params: 0
_________________________________________________________________
```

Fig. 4 Model summary

Fig. 5 Training graph

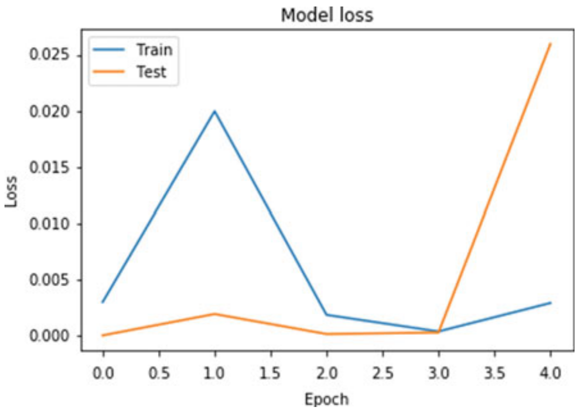


validation loss were decreasing. We have got training accuracy of 99% (Fig. 5) and validation accuracy of 97% (Fig. 6). This shows our proposal is good alternative to traditional primary authentication methods.

Normally, the signature drawing on the touch screen will generate sensor data especially from the accelerometer and the sensors associated with the touch screen, like the coordinates the pressure finger size etc. These features can also be used for recognizing the user, but in this work that is not taken into consideration.

The signature bio metric is known to vary with respect to time, moreover we are drawing our signature using finger which is more likely to have deformations every time. Another factor is the way an user holds the phone during his signing process. Our data set was collected in a controlled environment. Every subject was sitting and holding phone in their hands. In reality they may be lying, walking or the phone may be on a desk. Situations mentioned above were not taken into consideration. It has been observed that during our data collection, frequent errors are happening in

Fig. 6 Validation



signature drawing and if such data is there in the training set, it will affect the overall accuracy.

5 Conclusion

Our study proposed pseudo signature, signature drawn using the finger on touch screen as an authentication method in place of PIN and Graphical Pattern. Simulation results shows that suggestion has a potential to replace the existing entry point mechanism. From the users point of view, the signature bio metric is easy to remember and its resistant to forgery and stealing. Our study has achieved a remarkable accuracy. The shortcomings of the study are as follows. The entire work carried out on a limited data set. The time variance are not taken into consideration. As a future work, we would consider the signature variance of the genuine user over time and the model has to adapt the changes so as to make necessary modifications to the learned model. Further, if we can add the accelerometer readings generated during the signature drawing to the data set accuracy can be further increased.

Compliance with Ethical Standards All studies were conducted in accordance with principles as defined in the Declaration of Helsinki Conference and approved by the relevant departmental review board. Informed consent was obtained from all participants included in the study.

References

1. Bhagavatula R, Ur B, Iacovino K, Kywe SM, Cranor LF, Savvides M (2015) Biometric authentication on iPhone and android: usability, perceptions, and influences on adoption. USEC '15: Workshop on Usable Security, 8 Feb 2015, San Diego, CA. Proceedings. 1–10. Research Collection School of Information Systems. Available at: https://ink.library.smu.edu.sg/sis_research/3967. https://doi.org/10.14722/usec.2015.23003
2. Bonneau J (2012) The science of guessing: analyzing an anonymized corpus of 70 million passwords. In: 2012 IEEE symposium on security and privacy. San Francisco, CA, pp 538–552
3. Harbach M, Von Zezschwitz E, Fichtner A, De Luca A, Smith M (2014) It's a hard lock life: a field study of smartphone (un) locking behavior and risk perception. In: 10th symposium on usable privacy and security (SOUPS 2014), pp 213–230
4. Khuwaja G , Laghari M (2011) Offline handwritten signature recognition. World academy of science, engineering and technology, open science index 59. Int J Comput Inf Eng 5(11):1304–1307. https://doi.org/10.5281zenodo.1085962
5. Chen J, Lopresti D, Ballard L, Monrose F (2013) Pseudo-signatures as a biometric. Int J IT Eng Appl Sci Res (IJIEASR) 2(1), Jan 2013
6. Fischer A, Diaz M, Plamondon R, Ferrer MA (2015) Robust score normalization for DTW-based on-line signature verification. In: Proceedings of the international conference on document analysis and recognition (ICDAR). Nancy, France, 23–26 Aug 2015, pp 241–245
7. Wijesoma WS, Mingming M, Yue KW (2001) On-line signature verification using a computational intelligence approach. In: Proceedings of the fuzzy days. Dortmund, Germany, Oct 2001, pp 699–711
8. Fierrez Aguilar J, Nanni L, Lopez-Pealba J, Ortega Garcia J, Maltoni D (2005) An on-line signature verification system based on fusion of local and global information. In: Proceedings of audio- and video-based biometric person authentication (AVBPA). Rye Brook, NY, USA, 20–22 July 2005, pp 523–532
9. Feng H, Wah CC (2003) Online signature verification using a new extreme points warping technique. Pattern Recognit Lett 24:2943–2951
10. Iranmanesh V, Ahmad SMS, Adnan WAW, Malallah FL, Yussof S (2014) Online signature verification using neural network and Pearson correlation features. In: Proceedings of the IEEE conference on open systems (ICOS). Subang, Selangor, Malaysia, 26–28 Oct 2014, pp 18–21
11. Nam S, Park H, Seo C, Choi D (2018) Forged signature distinction using convolutional neural network for feature extraction. Appl Sci 8:153. https://doi.org/10.3390/app8020153
12. Fierrez J, Ortega Garcia J, Ramos D, Gonzalez-Rodriguez J (2007) HMM-based on-line signature verification: feature extraction and signature modeling. Pattern Recognit Lett 28:2325–2334

Autonomous Mobile Robot Using RGB-D SLAM and Robot Operating System

Jash Mota, Prutha Edwankar, Yash Shetye, Manisha Sampat and Dattatray Sawant

Abstract Generally, the real-world environment is dynamic in nature. The transitory and individuals items seem stationary for some time; however, they are later moved, for example, chairs. A robot must somehow manoeuvre through the moving objects for which it uses the SLAM algorithm. This paper explores Gmapping and HectorSLAM on autonomous mobile robots for indoor applications using Microsoft Kinect Robot Operating System (ROS).

Keywords Autonomous mobile robot · SLAM · RGB-D · Kinect · ROS · Navigation · Differential drive

1 Introduction

This paper explores autonomous navigation—one of the most challenging tasks in robotics. Autonomous mobile robots are a category of robots capable of navigating in a dynamic environment to the goal without any information from the user other than the goal point. The autonomous navigation comprises of knowing where we are in the dynamic environment, what does the environment look like at a particular instant, and what is the transformation between the sensor and the wheelbase. A two-wheeled differential drive with circular base has been chosen for the purpose of this paper. Stepper motors provide the odometry data, while Kinect provides a laser scan of the environment. All computation and communication happen through ROS.

J. Mota · P. Edwankar · Y. Shetye · M. Sampat · D. Sawant (✉)
Department of Mechatronics Engineering, MPSTME, NMIMS University, Mumbai, India
e-mail: dattatray.sawant@nmims.edu

J. Mota
e-mail: jashmota720@live.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_93

2 Slam

Simultaneous Localisation and Mapping is a problem to build an unknown environment's map and to determine its location in that environment after the mobile robot is kept at an initially unknown position and orientation in the environment [1]. The SLAM problem was first posed in 1986 at IEEE Robotics and Automation Conference [2]. Eventually, it was realised that when the problem of mapping and localisation is combined as a single estimation problem, the solution is more accurate. SLAM estimates the location of the robot and the landmarks and plans a path online, without any previous knowledge or a prebuilt map. There are many different solutions to the problem of SLAM, with probabilistic SLAM, Extended Kalman Filter SLAM (EKF SLAM), GraphSLAM and FastSLAM being the most prominent ones [3]. The computation required to solve the problem increases quadratically with an increase in the number of landmarks.

3 Localisation

The pose of the robot is necessary to plan a path to reach the navigation goal. Localisation can be achieved either through an inertial measurement unit (IMU) or by getting feedback of the velocity of each motor [4]. An inertial measurement unit generally comprises of an accelerometer, gyroscope and a magnetometer to calculate linear and angular accelerations in three-dimensional space, which can be integrated to give the value for orientation and position of the robot in space. Meanwhile, the rotation of the wheels can also be measured using sensors like wheel encoders and can be used to calculate linear velocities of each wheel [5]. Depending on the drive mechanism of the robot, proper inverse kinematics can be computed to give the positional and orientation values. For this paper, the robot has a differential drive with two wheels. Also, stepper motors are used for driving the wheels. The advantage of using stepper motors is the accurate open-loop control of the rotation of the motor. This allows to precisely measure the rotation of the wheels, which will yield the angular velocity over time, which would yield linear velocity for that particular wheel. Instantaneous centre of curvature can be applied to find out the new pose of the robot relative to previous pose (Fig. 1).

Mathematical model:

$$\omega = \theta \times \delta t$$

$$v_r = \omega \times \left(R - \frac{L}{2}\right)$$

$$v_l = \omega \times \left(R + \frac{L}{2}\right)$$

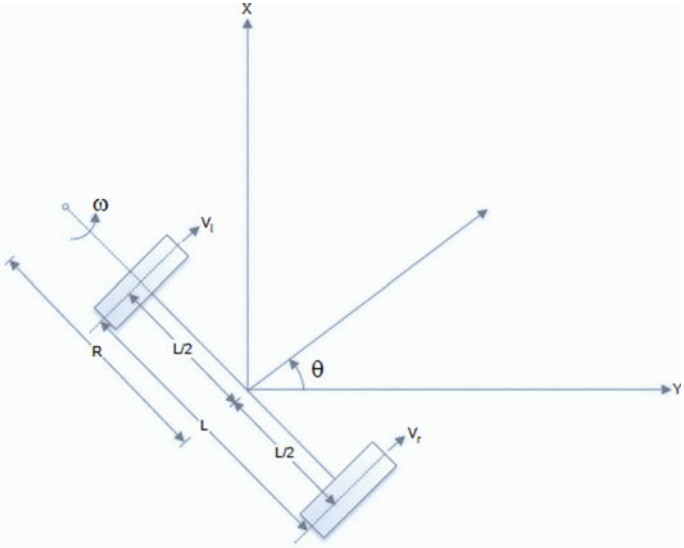


Fig. 1 Computing pose for a differential drive

Which yields

$$R = \frac{L}{2} \times \frac{v_l + v_r}{v_r - v_l}$$

And,

$$\omega = \frac{v_r - v_l}{L}$$

Therefore,

$$\text{ICC} = [x - R\sin\theta,\, y + R\cos\theta]$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} \cos\,\omega\delta t & -\sin\,\omega\delta t \\ \sin\,\omega\delta t & \cos\,\omega\delta t \end{bmatrix} \times \begin{bmatrix} x - \text{ICC}_x \\ y - \text{ICC}_y \end{bmatrix} + \begin{bmatrix} \text{ICC}_x \\ \text{ICC}_y \end{bmatrix}$$

$$\theta' = \omega\delta t + \theta$$

Robot's position and orientation (pose) can be calculated using the above equations.

4 Mapping

In order to manoeuvre, the robot must know the map of its environment. In a dynamic environment case, the map is constantly being updated and fed to the robot. There are numerous ways to map any room. While LIDAR is a very accurate laser scanning method, the sensors are usually expensive. Instead, for the purpose of this paper, a Microsoft Kinect was used to get the landmark estimates. It incorporates several advanced sensing hardware. Kinect contains a depth sensor, an RGB camera, microphone array and an IR emitter. The IR emitter emits infrared light, the intensity of which at different points is captured through an IR camera. The pattern captured is correlated against a reference pattern. This image is matched with the image obtained from the RGB camera image to obtain the distance of each point. The Kinect captures 307,200 depth points at a rate of 30 fps [6]. The data is stored as a point cloud, which is a set of data points in a given coordinate system. Binding these point clouds from various frames gives a 3D map of the environment.

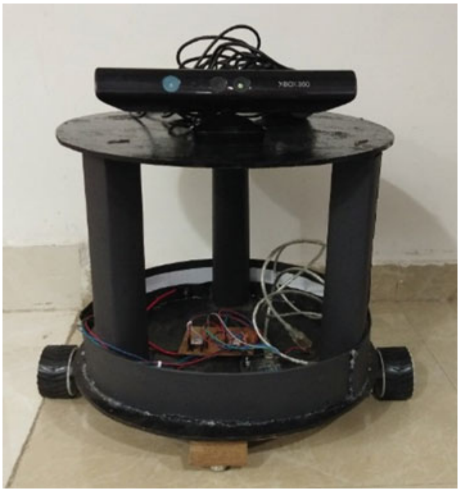
5 System Setup

For our experiments, we built upon the TurtleBot 2 hardware, a set of sensors, equipped with a computing system, microcontroller to communicate between the wheel motors and the computer running Robot Operating System (ROS). ROS is used for modelling, simulation and visualisation of output from laser scan topics, along with providing support for distributed computing and providing packages for navigation [7]. The computational platform is based on Intel Core i5, Radeon graphics, which supports CUDA. Table 1 provides all the system specifications ROS philosophy has the goal of being a peer to peer, tools based, multilingual, lightweight, free and open-source middleware to provide a structured communication layer above the host OS, Ubuntu 16.04 in this case, or a network of computers. Communication happens between different nodes through topics where the data is published and subscribed as messages. A node can publish a message on a topic to several other nodes and subscribe to several other nodes too. This way, the whole procedure can be broken down into modular nodes (Fig. 2).

Table 1 Robot's system configuration

Parameters	Configurations
Processor	Intel Core i5
GPU	Radeon
RAM	12 GB
RGB-D	Microsoft Kinect
OS	Ubuntu 16.04 LTS
ROS	Kinetic Kame

Fig. 2 System setup



A differential drive was used with stepper motors to provide the odometry data. A circular base was chosen to allow the robot to pass through a given cross section in any dimension in extreme cases, which is not possible in square bases.

6 Experimental Environment

The robot was initialised in a completely unknown environment with no prior knowledge. Data from Kinect was published on laser scan topic on ROS. Value from IMU or the wheel revolutions is published in the topic odom [8, 9]. Along with the information about odometry and laser scan, a transforming message is necessary to transform the point cloud value from the Kinect to the frame, in this case, the mobile base frame.

Gmapping [10] is a laser-based SLAM algorithm [11–13] and a widely used SLAM package in the ROS community. Alternative to Gmapping is HectorSLAM, which combines a 2D SLAM system [14] and 3D navigation [15], using an inertial measurement system. Gmapping is recommended by Santos et al.

Gmapping takes input from /laserscan, /odom and /tf and localises the robot and plans a path to reach the goal. Gmapping creates a local occupancy grid which is a grid of estimates of the position of the robot. The estimate improves with more landmarks and with an increase in runtime.

7 Conclusion

This paper demonstrates how a robot can be built or configured to navigate autonomously with the help of a laser scanner and an IMU. The paper also discusses two prominent SLAM algorithms and how ROS helps incorporate communication between various nodes, enforce distributed computing and working with navigation stack of ROS. Further, visual tools like Gazebo and MoveIt! can also be explored for simulation of the project. The experimental prototype setup demonstrated in this paper can be used in homes to carry out routine tasks like cleaning homes or delivering items from one room to another.

Acknowledgements The authors thankful to the NMIMS Deemed to be University's Mukesh Patel School of Technology Management and Engineering, Mumbai, India for providing the necessary facilities for carrying out this work.

References

1. Santos JM, Portugal D, Rocha RP (2013) An evaluation of 2D SLAM techniques available in robot operating system. In: IEEE international symposium on safety, security and rescue robotics (SSRR), pp 1–6
2. Durrant-Whyte H, Bailey T (2006) Part I Simultaneous localization and mapping. IEEE Robot Autom Mag 13(2):99–110
3. Bailey T, Durrant-Whyte H (2006) Part II Simultaneous localization and mapping (SLAM). IEEE Robot Autom Mag 13(3):108–117
4. Quigley M, Conley K, Gerkey B, Faust J, Foote T, Leibs J, Wheeler R, Ng AY (2009) ROS: an open-source robot operating system. In: ICRA workshop on open source software, vol 3, no 3, p 5
5. Ibragimov IZ, Afanasyev IM (2017) Comparison of ROS-based visual SLAM methods in homogeneous indoor environment. In: 14th IEEE workshop on positioning, navigation and communications (WPNC), pp 1–6
6. Thrun S, Montemerlo M (2006) The graph SLAM algorithm with applications to large-scale mapping of urban structures. Int J Robot Res 403–429
7. Sturm J, Engelhard N, Endres F, Burgard W, Cremers D (2012) A benchmark for the evaluation of RGB-D SLAM systems. In: IEEE international conference on intelligent robots and systems, pp 573–580
8. Kerl C, Sturm J, Cremers D (2013) Robust odometry estimation for RGB-D cameras. In: IEEE international conference on robotics and automation, pp 3748–3754
9. Dissanayake MG, Newman P, Clark S, Durrant-Whyte HF, Csorba M (2001) A solution to the simultaneous localization and map building (SLAM) problem. IEEE Trans Robot Autom 17(3):229–241
10. http://wiki.ros.org/gmapping
11. Endres F, Hess J, Engelhard N Sturm J, Cremers, D, Burgard W (2012) An evaluation of the RGB-D SLAM system. In: ICRA, pp 1691–1696
12. Bailey T, Nieto J, Guivant J Stevens M, Nebot E (2006) Consistency of the EKF-SLAM algorithm. In: IEEE international conference on intelligent robots and systems, pp 3562–3568

13. Leonard JJ, Durrant-Whyte HF, Cox IJ (1992) Dynamic map building for an autonomous mobile robot. Int J Robot Res 11(4):286–298
14. http://wiki.ros.org/hector_slam
15. http://wiki.ros.org/navigation

Survey on Data Mining and Predictive Analytics Techniques

S. Sathishkumar, R. Devi Priya and K. Karthika

Abstract Nowadays, predictive analytics is one of the most important big data trends. Predictive analytics is the accumulation of extensive, mostly unstructured data from various sources. The mixture of various information sources, for example, online networking information, climate and traffic are improved by internal information is especially basic. But both predictive analysis and data mining attempt to make divination about possible events in the future with the help of data models. Predictive analytics processes utilize various statistical strategies such as machine learning or neural networks, regression and extrapolation to perceive in the information patterns and infer algorithm. These algorithmic procedures are assessed depending on test data and optimized data. It is to be noted that as data availability increases, the accuracy of the algorithm also improved. By chance if the improvement procedure is finished, the algorithm and the model can be connected to information whose classification is obscure. Predictive analytics model captures connection between various factors to assess chance with a specific set of conditions to distribute a score or weightage. Successfully, on applying predictive examination, the organizations can adequately explain huge information for their benefit. We present a detailed survey on data mining and predictive analytics here, by analyzing 15 techniques from standard publishers (IEEE, Elsevier, Springer, etc.) of the year from 2008 to 2018. Based on the algorithms and methods utilized which are inconvenient, the problems are analyzed and classified. Moreover, to indicate the improvement and accuracy of all the research articles is also discussed. Furthermore, the analysis is carried to find

S. Sathishkumar (✉) · K. Karthika
Department of Information Technology, Adhiyamaan College of Engineering, Hosur, India
e-mail: ssathishkumaraeri@gmail.com

R. Devi Priya
Department of Information Technology, Kongu Engineering College, Erode, India

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_94

the essential for their approaches so that we can develop a new technique to previse the future data. Eventually, some of the research issues are also inscribed to precede further research on the similar direction.

Keywords Data mining · Predictive analytics · Model modules · Parameter estimation

1 Introduction

In present days, data managing becomes an essential task of many fields because of the evolution of information technology leads to enormous amount of data. The information technology provides a lot of information, but extracting only the essential information becomes a difficult task; therefore, many techniques have been proposed to deal with this issue. Among them data mining, data prediction, predictive analytics, etc. become an effective technique in current days. Information is expected to expand as technology enhances the organization units inside the operations and it gets connected in stable. Firms that recover and treat information as a vital resource can make an incentive through predictive analysis [1]. This present work is focused on predictive analytics which the brief introduction about the predictive analytics. Analytics is an essential process of every field because it is utilized for discovering, analyzing and understanding meaningful patterns from widespread data. The significance of predictive analytics is inevitable in many fields because this technique helps to predict the future about the particular field information [2]. With the help of predictive analytics, the information about the future business performance can be elucidated; therefore, the organizations utilized predictive analytics technique to understand the complete growth, to improve the current scenario, to learn about the development possibilities, etc. [3]. Besides, it is utilized for identifying trends, relationships and patterns within data that can be used to monitor the future event and behavior [4, 5]. The general predictive methods often utilized by researchers are: regression modeling, decision tree, Bayesian statistics, neural network, support vector machine and nearest neighbor algorithm [6]. In order to prove, we have studied more about predictive analytics here, and the survey work is conducted based on various papers. In addition, this work is categorized by three parts such as technique, application and parameters measures.

2 Survey on Data Mining and Predictive Analytics Techniques

The survey is done by means of learning information from different research papers from 2010 to 2018 in the standard journals such as IEEE, Elsevier, Springer and miscellaneous international journals. Here, the survey is done by means of different techniques and its categorizations.

2.1 KNN-Based Data Mining and Predictive Analytics

Bendre and Manthalkar [7] have proposed a novel technique for prediction of future conditions on climatic station from big data by addressing the predictive approach on the basis of time series and neural network utilized by MapReduce programming model. They have included predictive analysis approach with a broad spectrum using the models, such as examination and decay, arrangement and forecast. The time arrangement-based decay approach was proposed to disintegrate and discover the pattern, normal and modern components. The direct components were dealt with time arrangement MapReduce-based autoregressive integrated moving average (M-ARIMA) model and nonlinear segments were taken care of by MK-nearest neighbors (M-KNN) display.

Additionally the MapReduce-based hybrid model (M-HM) is suggested to utilize the benefits of time arrangement and neural network to enhance precision of divination. This analytics confirm the viability of developed model over the standard and irregularity part of the information. The performance estimation and measurements are performed to affirm the consistency of checked information. In addition, brilliant accelerate, scale up and scrutinize are tried by varying the measure of information collection. But when the information measure was expanded, the normal execution time was decreased by utilizing the MapReduce-based methodology over the numerous node specialists.

2.2 Random Forest-Based Predictive Analytics

Wang et al. [8] have proposed a novel and effective predictive analytics. Business Intelligence & Analytics (BI&A) had turned into an essential region for the specialists and experts. The ordinary business knowledge featured unmistakable and symptomatic investigation to accomplish execution of estimation and the executives. Besides, business analytics delayed for incorporating predictive and prescriptive analysis to produce responsive activity plan. In the zone of BI&A, the accompanying problems are basic yet hard to handle, particularly to legitimize the reliability of the proposed work, three sorts of personal computer firms included which are business PC, modern PC and creation PC and were correspondingly utilized to describe different plans of action in PC enterprises: Original Brand Manufacturing (OBM), Original Design Manufacturing (ODM) and Electronic Manufacturing Services (EMS).

Appel et al. [9] have demonstrated the feasibility of utilizing methods from machine learning and information mining to decide the upcoming opportunity and dangers of individual properties and for neighborhoods utilizing an assortment of basic, statistic, financial and city movement highlights with high accuracy. A larger system of frameworks has been proposed which allows a city to move from decision-making based on 'educated anecdotes'. It also provided a systems solution that allows the City of Syracuse to begin transforming to a proactive and preventative model using analytics based on mathematical models and available data in the housing ecosystem.

2.3 ANN-Based Data Mining and Predictive Analytics

Lorenzo et al. [10] have suggested a novel technique based on ANN to investigate the benefit of using a commercially accessible cloud-based machine learning stage for examination of careful intercession in babies with pre-birth hydronephrosis (HN). Probabilistic key component examination was utilized for information attribution. Different clinical factors were incorporated into two-class choice wilderness and neural system for model preparing, utilizing careful mediation as the essential result. The predictive models were set out as a web administration in 35 s creating an extraordinary API key for application and web page advancement. Individual prediction dependent on the factors was conveyed as web based and batch execution record in 1 min. This cloud-based ML innovation permits simple construction, arrangement and sharing of predictive investigation solution. Utilizing pre-birth HN, for instance we propose a chance to address contemporary difficulties with information investigation, detailing an inventive arrangement that moves beyond the cutting edge standard.

Talaei-Khoei and Wilson [11] have proposed a novel technique to distinguish the patients in danger of type 2 diabetes (T2D). There was a collection of writing that utilized machine learning characterization calculations to anticipate advancement of T2D among patients. The present investigation corresponds to the execution of the characterization calculations to distinguish patients who were in danger of creating T2D to put it plainly, medium and long terms. To create a balanced dataset syntactic minority oversampling and random under sampling were used. The performance of neural networks, support vector machine to identify the patients developing type 2 diabetes (T2D) in short, medium and long terms are compared. Through significant investigation and data combination methods, the indicators of creating T2D were recognized for short, medium and long haul hazard examination. The discoveries showed that the execution of examination procedures relies on period and nature of expectation whether the prediction is to recognize individuals who will not advance T2D or to decide in danger patients.

Lokhandwala and Nateghi [12] have proposed a new methodology where they have given importance to the statistical and machine learning calculations to recognize the key indicators of cooling request power, utilizing the EIA CBECS information. They compared the utilization levels over the two years to seize how cooling burden had developed. They saw that while the mean and middle estimations of interest force have expanded sensibly since the mid-2000s, there had been a very sharp expansion in greatest use power over that period. At an expansive scale level, their information-driven investigation recognized atmosphere and building type as the most essential indicators of interest in the years. Nourishment administrations and in-persistent medicinal services units were famous as the most vitality serious building types, with higher power.

2.4 Decision Tree-Based Predictive Analytics

Geological uncertainty indicates a natural risk for all mining ventures. Mining tasks used asset square models as a noteworthy wellspring of information in arranging and in basic leadership. Be that as it may, such operational choices were not free from hazard and vulnerability. The idea moves on how vulnerability was dealt with and an ability to enable in zones that make operational adaptability could direct potential misfortunes. Information investigation was promoted as one of the significant intrusions in the twenty-first century and tasks that legitimately used information that could make constant open doors in the time of a dubious future. Since associations had bounty measures of unmistakable land information, a mix of information mining and genuine alternatives could give an upper hand.

Ajak et al. [1] have suggested a new tool in this present work where predictive data mining methods were connected to a real-time mining task to examine the likelihood of experiencing dangerous metal in a mining program. The information mining models yield is utilized to make conceivable genuine choices that the activities could meet to manage dirt vulnerability. The most widely recognized information-digging calculation picked for this errand was the characterization tree, which anticipated the likelihood of dirt with 78.6% precision. Poisson dissemination and Monte Carlo reproductions were connected to inspect different genuine alternatives. The ebb and flow look into uncovered that activities could limit unprogrammed misfortunes in the handling plant and could yield an upgraded esteem, if the prescient information mining calculation was connected to make genuine alternatives.

2.5 Naïve Bayesian Classifier-Based Predictive Analytics

Bellazzi and Zupan [13] have suggested a novel concept. The outstanding accessibility of new calculation strategies and tools for analyzing data and predictive models requires restorative data scientists and professionals to methodically chosen the most appropriate methodology to deal with clinical expectation issues. Especially, Pool of methods are known as 'Data Mining' provides various solutions to deal with the analysis of medical data and construction of various prediction models. A substantial assortment of those strategies needs broad and basic rules that may help experts in the reasonable determination of information mining apparatuses, creation and approval of prescient models, alongside the engendering of prescient models inside clinical situations. The objective of this friend audit was to talk about the degree and job of the exploration region of prescient information mining and to develop a structure to make do with the issues of making, evaluating and using information mining model in clinical drug. It includes the analysis of clinical data warehouses for clinical medicine, epidemiological studies and emerging studies in genomics and proteomics.

Siryani et al. [14] have presented a framework for a decision-support system (DSS) that operated within the IoT ecosystem. An 'Internet of Things' (IoT) that creates a bridge between the society and frameworks speaks to an enormous idea move. The DSS influence the advanced analytics of electric smart meter (ESM) network communication in order to improve predictions of cost for smart meter field operations and also provide recommendations regarding whether to send a expert to a client location to deal with an ESM issue. Based on observation the model was evaluated using data set from a profitable network. The framework of decision support system is express with Bayesian Network prediction model and also it is compared with three machine learning classifiers: Naïve Bayes, Random Forest and Decision Tree. Results demonstrated that their methodology produced factually amazing estimations and that the DSS would improve the cost-effectiveness of ESM arrange tasks and support.

2.6 K-*Means-Based Predictive Analytics*

Ge et al. [15] have found a new technique where they discussed about data mining. Data mining and analytics have assumed an essential job in learning revelation and decision-making/bolstered in the process industry over the previous hundreds of years. As a computational engine to data mining and investigation, machine learning gave us essential instruments to data extraction, information design acknowledgment and forecasts. From the information of machine learning, this exploration work gave a survey on existing information mining and examination applications in the process business over the previous hundreds of years. The best in class of information mining and investigation was reassessed through eight unsupervised learning and ten administered learning calculations, just as the application status of semi-regulated learning algorithms.

2.7 Summary of Survey

In this section, the data about the predictive analytics is grouped based on various peer-reviewed papers from eminent journals includes IEEE, Elsevier Springer, etc. In these papers, the efficiency of various techniques can be understood. In accordance with that, the research has been conducted by different techniques that are utilized. In the forthcoming section, the survey work based on different categorizations will be discussed.

3 Categorization and Its Discussion

All the articles taken for the survey are categorized based on three criteria: technique-, application- and parameter-based measures.

3.1 Categorization Based on the Novel Techniques

In this arena, we categorize the existing research work in accordance with the novel techniques. This analysis meant for usage of algorithm in the olden days and realizes how to improve the algorithm further for current research work. Each research work is developed for different years. So we split the research work into four categories such as 2008–2011, 2012–2013, 2014–2015 and 2016–2018. The number of research work utilized in each year is explained in Table 1 for this survey, which relies totally on 16 papers. The different algorithms used in various paper has been shown in Fig. 1.

Table 1 Overall analysis of survey 2008–2018

Technique	2008–2011	2012–2013	2014–2015	2016–2018
ANN	–	–	–	[7, 10, 11, 12]
KNN	–	–	–	[7]
SVM	–	–	–	[11]
K means	–	–	–	[15, 16]
Random forest	–	[9]	–	[8, 12]
Decision tree	–	–	–	[8]
Naïve Bayesian	[13]	–	–	[10]
PCA	–	–	–	[13, 15]
Nearest neighbor	–	–	[14]	–
Other techniques	[15]	–	[14]	–

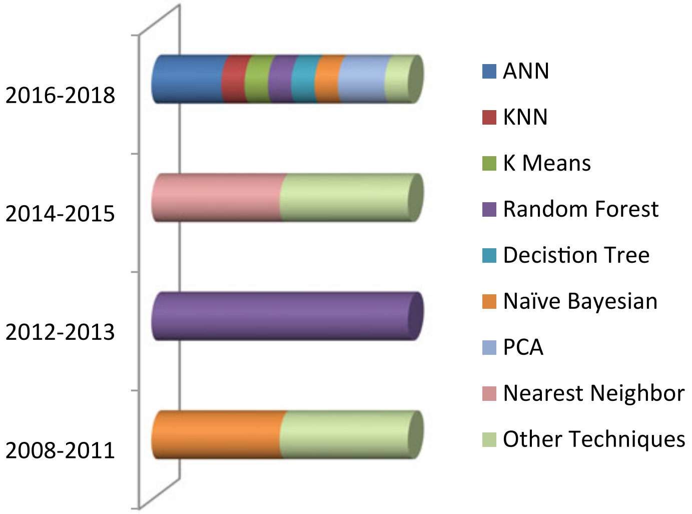


Fig. 1 Summary of the survey

3.2 Categorization Based on Application

In this section, we tabulate the applications based on different papers such as EMS, parallel and distributed processing, medical, etc. (Table 2).

3.3 Categorization Based on Parameters Measures

This section explains about the parameters measures utilized based on various papers from 2008 to 2018 such as *t*-value, profit, *R*-square, etc. Table 3 shows the various parameter measures applied in the literature survey.

This survey is executed for proposing an effective technique in future work with advanced features. This work has shown about the techniques which have been utilized in existing technique and gives us an idea about existing problems in it. With the help of this survey, we can provide an effective predictive analytic technique in our future work.

Table 2 Categorization based on application from 2008 to 2015

Article from 2008 to 2011								
References	EMS	Parallel and distributed processing	Medical	Energy information administration (EIA)	Data classification	Property vacancy policies for cities	Automated library information exchanging network	Computer graphics
[7]		✓						
[8]	✓							
[9]						✓		
[16]							✓	
[10]		✓	✓					
[11]		✓	✓					
[12]				✓				
[13]		✓	✓					
[15]					✓			

Table 3 Categorization based on parameter measure

Measures	2008–2011	2012–2013	2014–2015	2016–2018
t-value	–	–	–	[7]
Profit	–	–	–	[8]
R-square	–	[9]	–	–
Average run time	–	–	–	[10]
Mean	–	–	–	[12]
Other	[13]			[1, 15]

4 Conclusion

Predictive analytics models help to create the connections among numerous components to evaluate chance with a specific arrangement of conditions to allot a score or weightage. By successfully applying predictive analytics, the businesses can effectively interpret big data for their benefits. In this research work, we present a detailed survey on data mining and predictive analytics by analyzing various techniques from standard publishers (IEEE, Elsevier, Springer, etc.) during the year from 2010 to 2018. This survey work gives good vision about current techniques utilized for predictive analytics. This analysis helps to nurture future work in terms of overcoming the current issues. Therefore, the effective predictive analytics can be proposed significantly with effective features in future work.

Future Work
From the above survey work, we came to know the existing predictive analytic techniques have some limitations such as big data handling, distributed computing, predictive analytics in cloud, etc. and therefore, the efficiency of the proposed technique needs to be improved for future work. In addition, the effective advanced algorithm should be utilized for improving the performance by proposing-effective-technique.

References

1. Ajak AD, Lilford E, Topal E (2018) Application of predictive data mining to create mine plan flexibility in the face of geological uncertainty. Resours Policy 55:62–79
2. Alharthi H (2018) Healthcare predictive analytics: an overview with a focus on Saudi Arabia. J Infect Public Health (in press, corrected proof). Available online 8 Mar 2018
3. Rajni J, Malaya DB (2015) Predictive analytics in a higher education context. IT Prof 17(4):24–33
4. Bekiroglu K, Duru O, Gulay E, Su R, Lagoa C (2018) Predictive analytics of crude oil prices by utilizing the intelligent model search engine. Appl Energy 228:2387–2397
5. Rousseaux F (2017) BIG DATA and data-driven intelligent predictive algorithms to support creativity. Ind Eng Comput Ind Eng 112:459–465

6. Dubey R, Gunasekaran A, Childe SJ, Papadopoulos T, Roubaud D (2017) Can big data and predictive analytics improve social and environmental sustainability? Technol Forecast Soc Change (in press, corrected proof). Available online 15 July 2017
7. Bendre M, Manthalkar R (2018) Time series decomposition and predictive analytics using MapReduce framework. Expert Syst Appl (in press, accepted manuscript). Available online 8 Sept 2018
8. Wang C-H, Cheng H-Y, Deng Y-T (2018) Using Bayesian belief network and time-series model to conduct prescriptive and predictive analytics for computer industries. Comput Ind Eng 115:486–494
9. Appel SU, Botti D, Jamison J, Plant L, Varshney LR (2014) Predictive analytics can facilitate proactive property vacancy policies for cities. Technol Forecast Soc Chang 89:161–173
10. Lorenzo AJ, Rickard M, Braga LH, Guo Y, Oliveria J-P (2018) Predictive analytics and modeling employing machine learning technology: the next step in data sharing, analysis and individualized counseling explored with a large, prospective prenatal hydronephrosis database. Urology (in press, accepted manuscript). Available online 30 June 2018
11. Talaei-Khoei A, Wilson JM (2018) Identifying people at risk of developing type 2 diabetes: a comparison of predictive analytics techniques and predictor variables. Int J Med Inf 119:22–38
12. Lokhandwala M, Nateghi R (2018) Leveraging advanced predictive analytics to assess commercial cooling load in the U.S. Sustain Prod Consum 14:66–81
13. Bellazzi R, Zupan B (2008) Predictive data mining in clinical medicine: current issues and guidelines. Int J Med Inf 77(2):81–97
14. Siryani J, Tanju B, Eveleigh TJ (2017) A machine learning decision-support system improves the internet of things' smart meter operations 4(4):1056–1066
15. Ge Z, Song Z, Ding SX, Huang B (2017) Data mining and analytics in the process industry: the role of machine learning
16. Litsey R, Mauldin W (2018) Knowing what the patron wants: using predictive analytics to transform library decision making. J Acad Librarianship 44(1):140–144

Implementation of In-flight Entertainment System Using Light Fidelity Technology

Viraj Savaliya, Kalp Shah, Dharmil Shah, Henish Shah and Poonam Kadam

Abstract We are often directed to switch off our mobile phones and other electronic devices while traveling in a plane due to the interference caused by the radio transmitters installed in these devices. As a result, most customers do not enjoy the benefit of data on-board except for some airlines who provide the paid data services. Also, due to the recent outburst in the demand for data, there is soon going to be a congestion of the radio frequency bands. Thus, developing a technology which can entirely replace the current system of radio frequency-based data transmission is beneficiary [1]. Light fidelity (Li-Fi) is a next-generation technology which uses visible light as a medium for transmitting data [2]. Thus, it serves this increasing demand for data due to its vast bandwidth and does not interfere with airplanes as well. This paper aims on demonstrating the application of light fidelity (Li-Fi) in the entertainment services provided inside the airplanes. All the fundamental principle of visible light communication (VLC), the modulation techniques involved as well as how a circuit can be realized for transmitting data in an airplane using those principles have been discussed in this paper. Light fidelity (Li-Fi) when used to its full potential can certainly prove that everyone can count on it when RF fails to serve the purpose.

Keywords Light fidelity · Visible light communication · Wireless fidelity · Pulse width modulation

V. Savaliya (✉) · K. Shah · D. Shah · H. Shah · P. Kadam
Department of Electronics and Telecommunication, Dwarkadas J. Sanghvi College of Engineering, Mumbai, India
e-mail: virajlee58@gmail.com

K. Shah
e-mail: kshah.shah951@gmail.com

D. Shah
e-mail: dharmil1997@gmail.com

H. Shah
e-mail: henishshah18@gmail.com

P. Kadam
e-mail: poonam.kadam@djsce.ac.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_95

1 Introduction

The current in-flight entertainment system consists of an electronic tablet which is fixed to backside of the seat and offers multiple sources of entertainment like movies, TV series, music, etc. This tablet might be connected to a Wi-Fi or it may have data stored inside it. Wi-Fi systems on-board are very expensive and the users often have to pay an extra amount of money to avail such services. Also, installation and maintenance cost of such electronic equipment on each seat leads to expensive flight tickets. As the screen is attached on the backside of a seat, the user has to adjust the viewing angle each and every time the person on the front seat lies down. Most of the airplane companies use Wi-Fi services, and thus it further leads to the problem of congestion of radio frequency bands [3]. To avoid such drawbacks and difficulties, we can use an alternative wireless technology called Li-Fi.

Li-Fi technology has been proposed to overcome the limitations of finite bandwidth of radio frequency. Li-Fi stands for 'light fidelity' which uses visible light for data transmission. Visible light has a wider spectrum range of 375–775 nm [4]. Visible light communication (VLC) uses ordinary lamps or LEDs to transfer data from one place to another. Light from these sources does not harm the human eye vision and is immune to radio frequency interference [5]. In places, where Wi-Fi is not allowed due to security purpose, Li-Fi makes it possible to have a wireless Internet in specific environments. Also, as Li-Fi does not include the use of routers or optical fiber cables, it is a cheaper alternative to Wi-Fi. The idea behind this project is to use the ON–OFF activity of LEDs to transfer data [6]. LEDs have energy-efficient illumination and high-modulation bandwidth. The devices flicker at a very high rate which makes it possible to send a stream of bits at a very high speed. The transmission is not visible to the naked eye because of the high-switching speeds. Binary bits are used for communication, i.e., when the LED is on, a Binary 1 is transmitted and when the LED is off, a binary 0 is transmitted [7]. This concept of Li-Fi was introduced in a TED talk by Dr. Harald Haas who is a professor at University of Edinburgh [8]. The data transfer between the transmitter and receiver is always done in a line of sight manner. With the help of Li-Fi, it is possible to achieve speed higher than 10 Gbps [9].

Since there is a light source above every seat on an airplane, we make use of that to transmit data to the users (Fig. 1). Thus, we can save a huge amount of money on the installation part of the system. The users can avail the services directly on their mobile phones via a receptor module and there would be no need of any other electronic equipment. With the help of Li-Fi modules, entertainment services can be availed at a much cheaper rate and will not lead to expensive flight tickets. In this paper, we present a methodology that makes use of light bulb to transmit data to the airplane travelers (Fig. 2).

Fig. 1 Li-Fi technology in aircraft using led bulbs

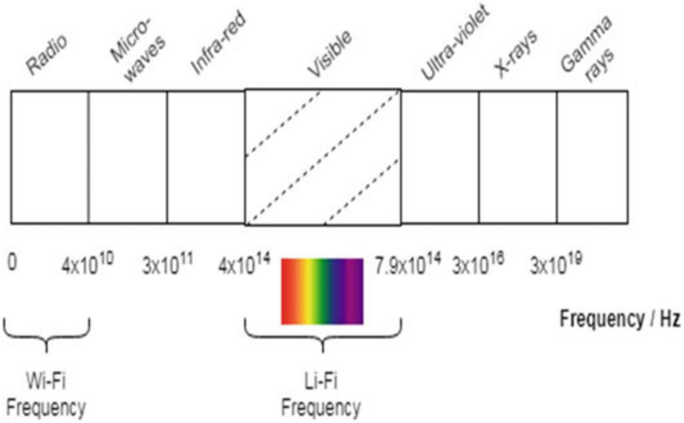


Fig. 2 Light spectrum for different frequencies [10]

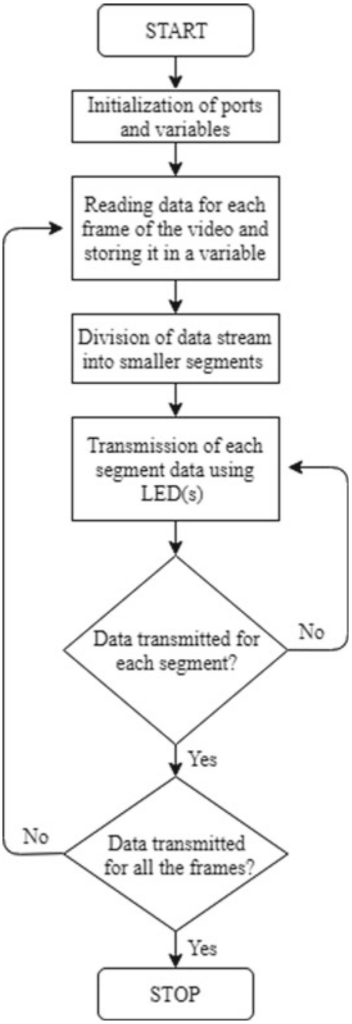
2 Methodology

In the proposed Li-Fi data transmission system, we transmit data stream with the help of Arduino board and LED(s), and receive the binary bits using a sensor (solar panel) and an Arduino board which is at the receiver.

At the transmitter side, the Arduino's code converts the desired data stream to be transmitted into its corresponding binary values. This conversion to binary is done by an in-built function in the Arduino's library, and the binary data stream is modulated using PWM and then sent to the transmitting device [11]. The bits are transmitted using an LED or array of LEDs (LED bulb), and Logical 1 is transmitted as LED 'ON', whereas logical 0 is transmitted as LED 'OFF'. Line of sight (LOS) is essential for correct reception of bits at the receiver site [12].

At the receiver side, initially a trigger detection procedure is established for further bit synchronization during communication. The bit synchronization happens when the receiver detects a constant stream of light for 20 ms (a predetermined threshold is used for this). After bit synchronization, the sensor will detect the binary bits transmitted by the transmitter and the Arduino board reads the sensor's output value. The output values of the sensor are then compared with a predefined threshold for finding the corresponding binary values for each sensor reading. An additional noise removal procedure is done, wherein the first bit which is received is discarded and the array is updated to account for the noise in the first bit. Post noise removal data represents binary for each frame of the video. These updated arrays of binary values are then de-converted to form each frame of the video. Each frame is then displayed with desired frame rate to avoid the flicker effect (Figs. 3 and 4).

Fig. 3 Trasmitter flowchart


START
Initialization of ports and variables
Reading data for each frame of the video and storing it in a variable
Division of data stream into smaller segments
Transmission of each segment data using LED(s)
Data transmitted for each segment?
No
Yes
Data transmitted for all the frames?
No
Yes
STOP

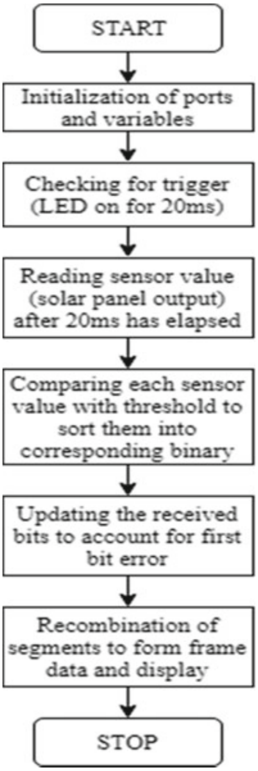

START
Initialization of ports and variables
Checking for trigger (LED on for 20ms)
Reading sensor value (solar panel output) after 20ms has elapsed
Comparing each sensor value with threshold to sort them into corresponding binary
Updating the received bits to account for first bit error
Recombination of segments to form frame data and display
STOP

Fig. 4 Receiver flowchart

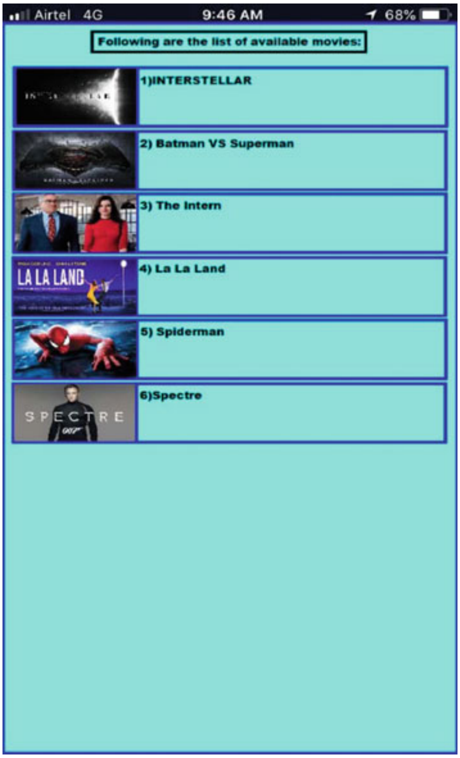
3 Implementation

The entire system consists of a remote, a transmitter circuit, a receiver circuit, array of LED's, a database, and a mobile-based application. The remote is installed on each passenger seats in the aircraft. The transmitter circuit will be installed with the LED lights above each passenger seat. Below the passenger seat, there will be a small device consisting of receiver circuitry and pin provided for connection with a mobile. The application is supposed to be downloaded on passenger's mobile in order to run the received data. The database acts as a central node for each aircraft privately and provides the storage for available entertainment options and gives access to all the passengers seating inside the airplane.

The application developed allows the user to choose from the available movies on the in-flight entertainment system. Once the user selects the movie to be streamed using the on-seat remote, the data transmission process using Li-Fi system begins. An Arduino UNO board is used at both-transmitter and receiver side for doing the desired processing. For transmission of data bits, the array of LED's is connected to the Arduino-based transmitter circuit. The data to be transmitted is initially converted to its binary form using a function called bitRead(). Each frame of the video is initially converted to a set of segments. These segments are less than 64kB in size so as to prevent clogging of Arduino’s serial buffer. This array of binary data is then transmitted using the LED. Bit ‘1’ is transmitted with the output as high, whereas bit ‘0’ is transmitted with the output as low; this will result in corresponding flickering of LED for each bit. At the transmitter side, it is essential to ensure that the array of bits to be transmitted do not clog the buffer of the Arduino board. To avoid buffer overload, a function called flush() is used repetitively after a fixed duration of time to clear the buffer. After transmission of all the segment data for current frame, the segment data for next frame is then transmitted. This process continues till data for all the frames has been transmitted, i.e., till the complete video data is transmitted (Fig. 5).

For data reception, a solar panel is used, which is interfaced with the Arduino - based receiver circuit. To ensure proper bit detection, a bit synchronization procedure is done. In this process, the LED at transmitter side is kept ‘ON’ for 20 ms. This is detected by the receiver, which then proceeds to read the output value of the solar panel. The output is read using a function called as analogRead(). After reading all the data, the output of the sensor is in the form of voltage, hence, to convert the data into binary it is compared with a predetermined threshold. The threshold has to be updated every time the environment around the Li-Fi system changes. The binary data array then undergoes a noise removal procedure to account for the

Fig. 5 Application interface



Following are the list of available movies:

1)INTERSTELLAR

2) Batman VS Superman

3) The Intern

4) La La Land

5) Spiderman

6)Spectre

noisy first bit of the received array. This updated array of bits then undergoes a de-conversion/recombination procedure to make up each segment of each frame of the video. After frame recombination, each frame is then displayed on the application's interface at the receiver site, which generally is a mobile phone or a tablet (Fig. 6).

The central database or the central node is accessed each time the passenger presses the button on the remote to select a movie. The central node is basically connected with all the nodes or passenger seats. The button pressed from a particular remote sends a command to access that particular numbered movie to the central database via a wired connection. Then that particular data is activated to be sent on the node present from where the command was received. The node circuitry (above passenger seat), on-seat remote, central database, and the receiver device connected with the mobile works all in synchronization. The data on the central storage system can be updated regularly (Figs. 7 and 8).

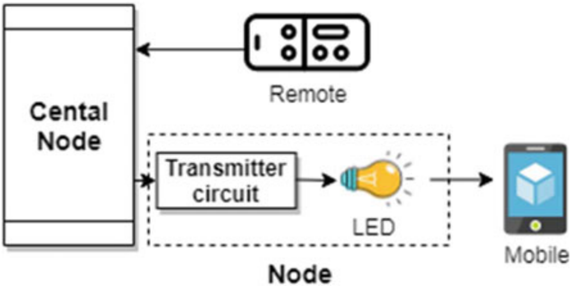


Fig. 6 Flowchart for transfer of data

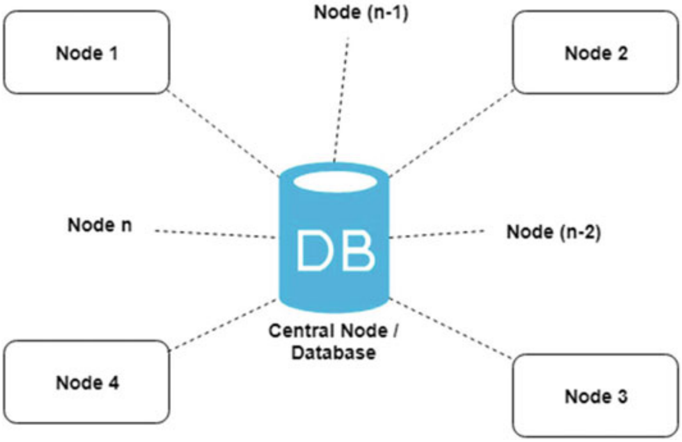


Fig. 7 Central to other nodes connection

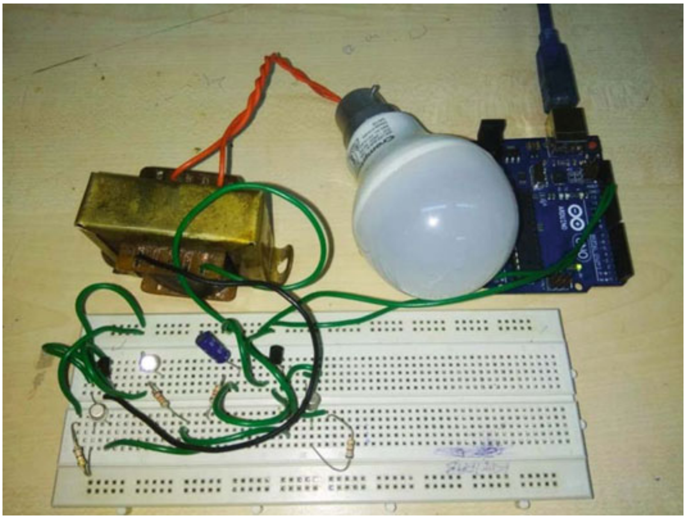


Fig. 8 Transmitter circuit used

4 Results

The proposed system for transfer of data for an entertainment system in airplanes using the visible light frequency spectrum is successfully tested. The system transmits the video data using a transmitter circuit controlled by an Arduino. The transmitter circuit is programmed using a software code via the Arduino. The software code is designed so as to perform the necessary coding and modulations as required by the model. Also the code as well the additional circuitry of the transmitter sections take care of any other modulation or scaling required. The data is then successfully transmitted using an array of LED's and hence using the visible light frequency spectrum. The LED's here blink in a prescribed manner according to the light signal. The receiver solar panel accepts the lights rays falling on it and converts it into electrical signal. Then the software code at the receiver end performs the decoding and carries out demodulation to generate the original signal sent by the user. The transmission of data is successfully done after taking into consideration all the error signal present in the vicinity of the model. Also, the important observations made in functioning of the proposed system are that works to its complete efficiency only for a limited range and also the speed is limited. As the distance between the transmitter and receiver side increases, there starts occurring more errors and false transmission of bits. The bit error rate keeps on increasing with increase in the distance making the system difficult to revive the original signal and hence making the model inefficient. But with better and improved modulations, we can tackle that limitation.

5 Conclusion and Future Scope

The proposed system to transfer video data successfully fulfills its objective and is efficient to work in real-world environment. The system also takes care of the noises present in the vicinity and produces the original signal accordingly. The system has limitations on the range, speed, and capacity of data to be transmitted. All these limitations can be worked upon by performing better modulations and using higher-end processors having more power. But, in comparison with the currently in use entertainment system in flights, the proposed systems outweigh it on many factors. The cost of the systems reduces drastically as it uses the already installed lights for transfer of data and also uses passenger's personal electronic device to run the data. Also, the proposed system is more comfortable for the passengers as they can sit in a position which is relaxing and preferable by them to watch a movie rather than sticking to a fixed installed device. Also, the angle at which the user wants to watch can be adjusted. The maintenance cost of the system also decreases as there is not much circuitry involved and it replaces the currently installed screens in airplanes. Hence, the cost of travel for passengers also reduces along with charges. Also, only those passengers who want to access the entertainment system can access rather than providing it mandatorily to all. The screen size for running the data will also be as preferred by the passenger as they are running it on their personal devices. Hence, passengers will not have to stick to already provided device at their seat. The mobile-based application can also be designed in a way to make it more user-friendly and attractive by the aircraft travel companies which can also give them a chance to enhance their marketing strategies. For extension of the proposed system, more amounts of data can be provided by using a bigger and better database and its management systems. Also, the transmitter and the receiver circuitry can be made more advanced by making necessary modifications for higher speed and data-carrying capacity.

References

1. Sonnad AM (2013) Led recent advancements in Li-Fi technology. Int J Electr Electron Data Commun 1(10). ISSN: 2320-2084
2. Vinnarasi A, Aarthy ST (2017) Transmission of data, audio signal and text using LI-FI. Int J Pure Appl Math 117
3. Proakis JG (2001) Digital communications, 4th edn. McGraw-Hill, New York
4. Abdallah W, Boudriga N (2016) Enabling 5G wireless access using Li-Fi technology: an OFDM based approach. 978-1-5090-1467-5/16/ ©2016 IEEE, pp 1–6
5. Adwani A, Nagtode S (2016) LI-FI: information transferring through LED'S. In: ICEEOT
6. Tanwar K, Gupta S (2014) Smart class using Li-Fi technology. In: IEEE transactions on engineering and science, pp 336–338
7. Mahendran R (2016) Integrated Lifi (light fidelity) for smart communication through illumination. In: International conference on advanced communication control and computing technologies

8. Komine T, Nakagawa M (2003) Integrated system of white LED visible-light communication and power-line communication. IEEE Trans Consum Electron 49:71–79
9. Rani J, Chauhan P, Tripathi R (2012) Li-Fi (light fidelity)-the future technology in wireless communication. ISSN 0973-4562
10. IEEE standard for local and metropolitan area networks—part 15.7: short-range wireless optical communication using visible light, pp 1–309
11. Jovicic A, Li J, Richardson T (2013) Visible light communication: opportunities, challenges and the path to market. IEEE Commun Mag 51:26–32
12. Damodaran S, Shaikh T, Taylor NK (2016) Using mobile phone based camera to read information from a Li-Fi source. 978-1-5090-5527-2/16© 2016 IEEE, pp 165–170

A Survey of Pre-processing Techniques Using Wavelets and Empirical-Mode Decomposition on Biomedical Signals

Prasanth M. Warrier, B. R. Manju and Rajkumar P. Sreedharan

Abstract Recorded biomedical statistics are utilized for predicting various syndromes in humans. Recorded electrical activity of heart can be used for predicting cardiovascular ailment likelihood. Several steps are involved to process biomedical signals, among which the first step related to pre-processing, in which a noisy signal is processed for generating noise-free signal, which can be utilized for further operations. This work gives a detailed understanding of de-noising techniques those have been used for the last decade, for cardiac signals. These techniques utilize the benefits of discrete wavelet transforms (DWT), Bayesian approach, singular value decomposition (SVD), artificial neural networks (ANN), empirical-mode decomposition (EMD), adaptive filtering, and finite impulse response (FIR) filtering. These techniques have been implemented for de-noising of biosignals, individually as well as combining with other techniques, for better results.

Keywords ECG · Empirical-mode decomposition · Filtering · De-noising techniques · DWT

1 Introduction

Biomedical signals can be processed and studied carefully for envisaging anomalies in human body. For example, electroencephalogram (EEG) signals are used for predicting epileptic nature of human brain and electrocardiogram (ECG) can be used for predicting cardiovascular diseases. These biomedical signals are very well applied for applications like biometric identification, emotion recognition, etc.

P. M. Warrier (✉) · R. P. Sreedharan
Department of Electronics and Communication, Amrita Vishwa Vidyapeetham, Amritapuri, India
e-mail: prasanthmw@am.amrita.edu

R. P. Sreedharan
e-mail: rajsreedharan@am.amrita.edu

B. R. Manju
Department of Mathematics, Amrita Vishwa Vidyapeetham, Amritapuri 690525, India
e-mail: manjubr@am.amrita.edu

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_96

Depending on the purpose, the analysis of biomedical signals may contain different phases in which the first phase could be the pre-processing [1]. In this work, several de-noising techniques have been discussed that can eliminate or deteriorate effect of noises embedded in data acquired through electrodes, from subject's body. In the case of ECG, noises can be from different sources like (1) power-line interference (50 or 60 Hz), (2) baseline wander (0.5–0.3 Hz), (3) muscle artifacts (electromyography: EMG), (4) electrode contact noise, (5) electrode motion artifact, (6) electrosurgical noise, and (7) instrumentation noise. To explore, significant studies in this literature, works were taken from IEEEXplore, and ScienceDirect. This paper is prearranged as, Sect. 2 contributes details of pre-processing techniques, developed in the last decade, Sect. 3 gives data base details, Sect. 4 gives details about various parameters for success measures, Sect. 5 discusses inference from the work and finally, the Sect. 6 gives conclusion.

2 Pre-processing Techniques

The eminent techniques implemented in various environments are briefed here.

2.1. **Savitzky–Golay filtering**: This method helps to smooth the noisy ECG signal. Since sequential operations of polynomial fitting and reevaluation are identically same as discrete convolution with finite impulse response, SG filtering can be termed as a simple finite impulse response (FIR) filter [2]. If $x(n)$ represent the data and $h(n)$ is the impulse response, then the convolution result is given by [2],

$$y[n] = \sum_{k=0}^{N-1} h(k) \cdot x(n-k) \tag{1}$$

2.2. **Adaptive filter**: For removing power-line interface (50/60 Hz), an adaptive filter, which is tuned with ECG signal morphology, can also be used. If the width of morphological filter is larger than width of noise, useful signal can be separated from noisy signal. A disadvantage found is, QRS wave, along with pits and peaks of nearby regions will too be removed [3].

2.3. **Wavelets transform**: Different wavelets transform (WT) techniques used for de-noising purpose has been discussed here (Fig. 1).

2.3.1. **Adaptive filter with WT and neural network**: An adaptive filter method, which combines discrete wavelets transform (DWT) and artificial neural network (ANN), can be used for de-noising ECG [4]. Instead of using an inverse DWT, ANN utilized for finding inverse and a nonlinear adaptive filtering to remove noise [4] (Fig. 2).

2.3.2. **DWT with hybridizing β-hill climbing**: Beta-hill climbing algorithm has been utilized for choosing the finest wavelet parameters and

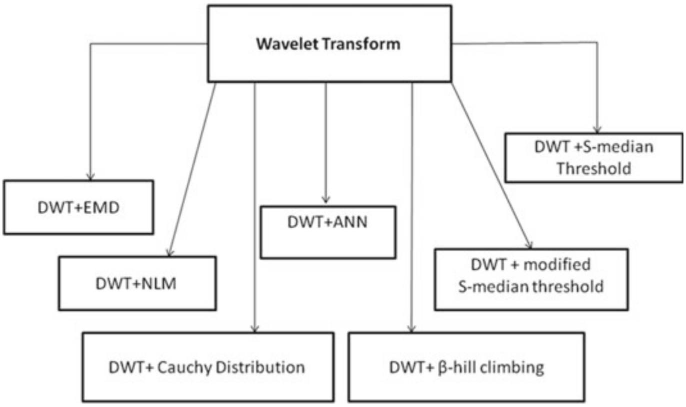


Fig. 1 Combinations of WT and other different techniques

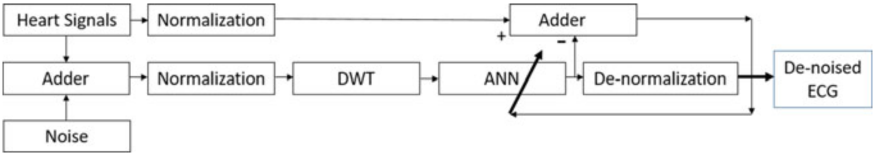


Fig. 2 Combination of adaptive filter, DWT, and ANN

used with DWT techniques, so that mean squared error is minimum [5].

2.3.3. **Discrete wavelet transform (DWT) and cauchy distribution at sub-bands**: A cauchy probability function can be used for modeling wavelet coefficients in each sub-band, where thresholds are being calculated at each level. Individual lead noisy ECG records from cardiovascular Centre of Glasgow University are being used [6].

2.3.4. **To de-noise ECG signal by using non-local estimation with DWT**: Though DWT technique is highly effective with larger decomposition levels, in removing HF noise, it can be also used to eradicate low frequency [7]. A method has been proposed, in which a combination of DWT with non-local means estimation is applied. Denoising using NLM would give a minimized mean error and falsehood improvement but with longer computational time [7].

2.3.5. **Discrete wavelet transform (DWT) and S-median threshold**: ECG signal is converted into wavelets and then the variance of noise signal in each sub-band is estimated using mean absolute deviation (MAD) [8]. Threshold is evaluated using S-median (sub-band level-dependent median threshold) and a soft thresholding is applied with sub-band level-dependent threshold, after which signal reconstruction is implemented using inverse wavelet transform (IWT) [8].

$$t_{l,k} = \left(\sigma_k \cdot \sqrt{2 \cdot \log(n)}\right) / \left(S_{l,k} + b\right) \text{ where, } k = 1, 2, \ldots, l. \quad (2)$$

$$S_{l,k} = 2^{L-\frac{k}{L}} =_{-\text{band}} \text{level dependent parameter.} \quad (3)$$

L deepest level of decomposition,
σ_k variance of noise,
k level at which thresholding is done.

$$\text{variance of noise, } \sigma_k = \frac{\text{median}(|x|)}{0.6745}, \quad k = 1, 2, 3, 4, \ldots, l. \quad (4)$$

S-median DM utilizes mean-value differences of both sets and found that S-median DM is better [8]. In modified S-median thresholding technique, an optimal Symlet function has been used along with a tuning factor [9].

2.4. **Empirical-mode decomposition (EMD)**: Empirical-Mode decomposition characterizes random signal as sum of intrinsic mode functions (IMFs) which are chosen and processed for de-noising [10]. Figure 3 represents various combinations of EMD, for de-noising purpose.

2.4.1. **Adaptive switching mean filter in EMD**: Three types of noises have been considered here namely, EMG, WGN, power-line interference [11] (Fig. 4).

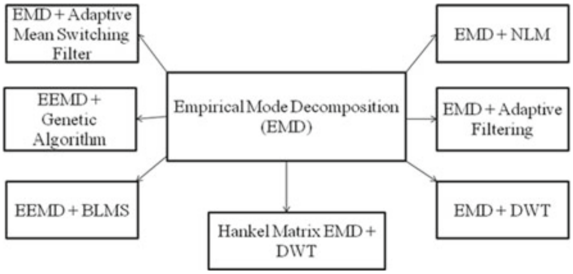


Fig. 3 Combination of EMD with other techniques

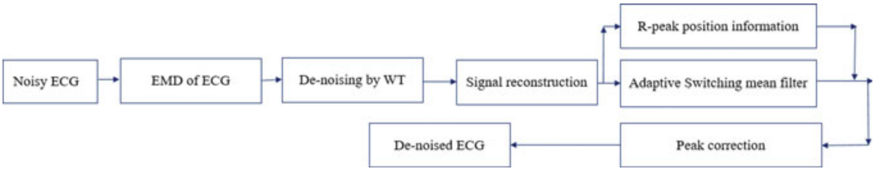


Fig. 4 De-noising method using EMD and adaptive switching mean filter

2.4.2. **Ensemble EMD (EEMD) with genetic algorithm-based thresholding for adaptive de-noising of ECG**: Kullback-Leibler divergence method and a probability density function is used for segregating IMFs into signal dominant group and noise dominant group. Adaptive de-noising is performed with the help of genetic algorithm, and then signal dominant IMFs and de-noised noise dominant IMF are selected for reconstructing pure signal [12].

2.4.3. **Combination of ensemble empirical-mode decomposition (EEMD) and block LMS adaptive algorithms as well as discrete wavelet transform (DWT) and neural network (NN)**: Those combinations have been developed for de-noising and they have been analyzed in [13]. Their performance was later compared with conventional EMD (CEMD), CEEMD, EEMD + LMS and DWT thresholding methods. Among the above mentioned techniques, based on performance, EEMD + LMS stands best.

2.4.4. **Noise exclusion from ECG using Eigenvalue decomposition (using Hankel matrix EMD with DWT)**: Eigenvalue breakdown of Henkel matrix is utilized for de-noising process of ECG [14]. Notch filters can be used for removing PLI, but with ringing issue. For decomposition, basis functions which are Eigen vectors are obtained by decomposition of Hankel matrix and for reconstruction, Eigenvalue pairs are used [14].

2.4.5. **EMD with NLM**: Non-local means (NLM) technique has been combined with empirical-mode decomposition (EMD) to preserve the edges in ECG signal [15] (Fig. 5).

2.4.6. **EMD with adaptive filtering**: Morphological structure of ECG signals can get fluctuated by power-line interference of 50 Hz. That is, a noise cancelation should work within 48–51 Hz [16]. In this proposed method, 50 Hz noise is removed using adaptive filter in first IMF, since only first IMF contain PLI and rest are free from PLI, and those coefficients are regulated according to LMS [16].

2.4.7. **Combination of EMD and wavelet techniques for de-noising ECG**: In this work, a combination of EMD and DWT has been tried, in which no IMFs have been omitted and thresholding for wavelet transform has been done adaptively [17] (Fig. 6).

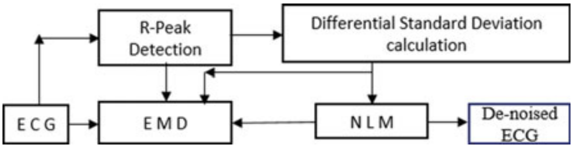


Fig. 5 De-noising process using EMD and NLM

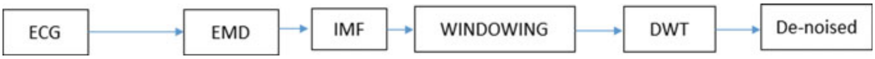


Fig. 6 Noise reduction using EMD and DWT

2.5. **Extended Kalman filter**: 2-d EKF structure has been modified into 17-d EKF structure, for de-noising, compression, and estimation of 15 model parameters, by utilizing benefits of synthetic ECG signal proposed by McSharry and co. An SNR improvement of 1.8 dB has been observed and found it better than multi-adaptive bionic wavelet transform (MABWT) and EKF2 though it suffers from filtering performance [18].

2.6. **Periodicity-based NLM de-noising technique for ECG in small SNR conditions**: De-noising of ECG signals is tried along with NLM, by making use of periodic nature of ECG [19]. Using FIR and IIR filters, it is challenging to remove EMG noises or other noises that overlay, in 20–200 Hz [19].

2.7. **Mean-shift algorithm**: Discrete-time ECG samples are synthesized to continuous signal, keeping signal morphology, using embedded Gaussian smoother and the extreme of continuous-time signal can be located, which corresponds to peak values in original ECG signals [20]. For modeling, mainly Gaussian functions were used, while wavelet synthesis and neural network are poor in adjusting morphology of typical output [20].

2.8. **Adaptive Fourier decomposition**: Signal is represented as sum of monocomponents and standard remainder [21].

$$G(t) = \sum_{k=0}^{\infty} C_k \cdot e^{jkt} \in H^2 \text{ space} = \sum_{n=1}^{N} S_n(t) + R_n(t);$$
$$\text{where } \sum_{k=0}^{\infty} (|C_k|)^2 < \infty. \tag{5}$$

AFD found better than Butterworth LPF, WT, EMD, EEMD, for muscle and motion artifacts. Results obtained were better than EMD/EEMD algorithms, in which, it shows, later algorithms do not hold strong mathematical basis [21].

2.9. **Bayesian approach with phonocardiogram (PCG)**: Phonocardiogram is a graphical representation of acoustic vibrations of heart, which may contain heart sounds and murmurs [22]. Based on PCG morphology, a dynamical model for PCG is constructed for synthetic PCG signals and a Bayesian framework has been opted for de-noising [22].

2.10. **Approximation of EMG in ECG signals**: Translation invariant approximation is done using stationary WT. It is very difficult to identify and remove EMG noise and patient electrode motion artifacts. Karhunen-Loever transform (KLT) is the one, which is used for noise removal in [23].

2.11. **Wearable ECG monitoring devices and ECG de-noising**: Using multi-stage decision tree algorithm, once small and large frequency components are detected, then it classifies, small frequency into BW/ABC using local dynamic amplitude feature range and classifies high frequency into PLI/EMG, using local autocorrelation function extreme peak feature. Parameters like average sensitivity was observed to be 97.88%, positive productivity = 91.18%, and accuracy = 89.06% [24].

2.12. **Compression and noise reduction of biomedical signals by singular value decomposition**: In this method, Bijective mapping of signal vector into matrix is done for de-noising any biomedical signal [25]. This matrix is decomposed to get rank-1 matrices, which are summed up to give singular values. SVD de-noising is accomplished by attenuating all small singular values [25].

3 Data Bases

Research and analysis of arrhythmia and related things have been supported by MIT-BIH. Data base provides data from 47 subjects as given in Table 1 [1, 26, 27].

4 Improvement Measures

4.1. SNR improvement measure

$$\mathrm{SNR}_{\mathrm{improvement}}[\mathrm{dB}] = \mathrm{SNR}_{\mathrm{output}} - \mathrm{SNR}_{\mathrm{input}} = 10 \cdot \log\left[\frac{\sum_i (|x_n(i) - x(i)|)^2}{\sum_i (|x_d(i) - x(i)|)^2}\right], \tag{6}$$

x pure ECG,
x_d de-noised ECG signal, and
x_n noisy ECG.

Table 1 MIT-BIH data base details used often by researchers

Data bases	Records	Subjects	Duration (min)	Sampling frequency	Bits per sample	Channels (leads)
MIT-BIH arrhythmia	48	47	30	360	11	2
MIT-BIH normal sinus rhythm	18	18	24 h	128	–	2

Table 2 Four possibilities of dimension and class

True condition	Positive assessment	Negative assessment
Real-positive	Positive-true	Negative-false
Real-negative	Positive-false	Negative-true

4.2. Error measurements

$$\text{Rootmean Square Error, RMSE} = \frac{1}{N}\sqrt{\sum_{i=1}^{N}[w(i) - z(i)]^2}, \qquad (7)$$

w Original-signal and
z Filtered-signal.

4.3. Success measures

In problem of statistical classification, error matrix or confusion matrix allows performance visualization of an algorithm (Table 2).

While classifying signals, constraints such as average sensitivity, precision or positive predictivity and accuracy have been utilized.

$$\text{Average Sensitivity, } S_e = \left(\frac{\text{TP}}{\text{TP} + \text{FN}}\right) * 100 \qquad (8)$$

$$\text{precision or positive predictivity, } +P = \left(\frac{\text{TP}}{\text{TP} + \text{FP}}\right) * 100 \qquad (9)$$

$$\text{accuracy} = \left(\frac{\text{TP}}{\text{TP} + \text{FN} + \text{FP}}\right) * 100 \qquad (10)$$

5 Discussion

In this work, 22 different algorithms have been discussed, which are used for denoising biomedical signals, especially ECG. From this survey, it became apparent that wavelet transform techniques are more mathematically stable and whose combination along with neural networks can give faster results, thereby saving lot of computation time. On the other hand, de-noising techniques, in real time, still needs lot of improvement.

6 Conclusions

For pre-processing, various techniques are being followed and this work discusses about various de-noising techniques. Methods like discrete wavelet transforms and various thresholding techniques, Bayesian approach, artificial neural networks, empirical-mode decomposition, singular value decomposition, adaptive filtering, and finite impulse response filtering, have been studied. Parameters of interest, for success measures, utilizes error matrix/confusion matrix, for SNR improvement, in most existing works. Above-mentioned methods as well as their combination also being tried to improve overall result. This paper gives an insight about significant de-noising techniques that were developed, in the past one decade.

Acknowledgements We would like to thank our beloved Chancellor Sri (Dr). Mata Amritanandamayi Devi, for giving a superior inspiration to implement this research work.

References

1. Berkaya SK, Uysal AK, Gunal ES, Ergin S, Gunal S, Gulmezoglu MB (2018) A survey on ECG analysis. Biomed Signal Process Control 43:216–235
2. Savitzky A, Golay MJ (1964) Smoothing and differentiation of data by simplified least squares procedures. Anal Chem 36(8):1627–1639
3. An-dong W, Lan L, Qin W (2012) An adaptive morphologic filter applied to ECG de-noising and extraction of R-peak at real time. AASRI Procedia 1:474–479 (Elsevier, ScienceDirect)
4. Poungponsri S, Yu X-H (2013) An adaptive filtering approach for ECG signal noise reduction using neural network. NeuroComputing 117:206–213 (ScienceDirect)
5. Alyasseri ZAA, Khader AT, Al-Betar MA, Awadallah MA (2018) Hybridizing β-hill climbing with wavelet transform for de-noising ECG signals. Inf Sci 429:229–246
6. Manthalkar R, Ardhapurkar S, Gajre S (2010) Wavelet based ECG de-noising by employing Cauchy Distribution at sub bands. In: ICSP2010 proceedings
7. Singh P, Pradhan G, Shahnawazuddin S (2017) De-noising of ECG signal by non-local estimation of approximation coefficient in DWT. Biocybern Biomed Eng 37:599–610
8. Poornachandra S (2008) Wavelet based de-noising using sub-band dependent threshold for ECG signals. Digit Signal Process 18:49–55 (ScienceDirect)
9. Awal MA, Mostafa SS, Ahmad M, Rashid MA (2014) An adaptive level dependent wavelet thresholding for ECG de-noising. Biocybern Biomed Eng 34:238–249
10. Blanco-Belasco M, Wengb B, Barnerc KE (2008) ECG signal de-noising and baseline wander correction based on empirical-mode decomposition. Comput Biol Med 38:1–13
11. Rakshit M, Das S (2018) An efficient ECG de-noising methodology using EMD and adaptive switching mean filter. Biomed Signal Process Control 40:140–148
12. Nguyen P, Kim J-M (2016) Adaptive ECG de-noising using genetic algorithm based thresholding and EEMD. Inf Sci 373:499–511
13. Kærgaard K, Jensen SH, Puthusserypady S (2016) A comprehensive performance analysis of EEMD-BLMS and DWT-NN hybrid algorithms for ECG De-noising. Biomed Signal Process Control 25:178–187
14. Sharma RR, Pachori RB (2018) Baseline wander and power line interference removal from ECG signals using Eigen value decomposition. Biomed Signal Process Control 45:33–49

15. Kumar S, Panigrahy D, Sahu PK (2018) De-noising of electrocardiogram (ECG) by using empirical-mode decomposition (EMD) with non-local mean (NLM) technique. Biocybern Biomed Eng 38:297–312
16. Suchetha M, Kumaravel N, Jagannath M, Jaganathan SK (2017) A comparative analysis of EMD based filtering method for 50 Hz noise cancellation in ECG signal. Inform Med Unlocked 8:54–59
17. Kabir MA, Shahnaz C (2012) De-noising of ECG signals based on noise-reduction algorithms in EMD and Wavelet domains. Biomed Signal Process Control 7:481–489
18. Sayadi O, student member, IEEE, Shamsollahi MB, member, IEEE (2008) ECG de-noising and compression using a modified extended Kalman filter structure. IEEE Trans Biomed Eng 55(9)
19. Lee Y, Hwang D (2018) Periodicity based NLM de-noising method for ECG in low SNR non-white noisy conditions. Biomed Signal Process Control 39:284–293
20. Yan J, Lu Y, Liu J, Wub X, Xu Y (2010) Self-adaptive model based ECG de-noising using features extracted by mean shift algorithm. Bio-med Signal Process Control 5(2):103-113. https://doi.org/10.1016/j.bspc.2010.01.003
21. Wang Z, Wan F, Wong CM, Zhang L (2016) Adaptive Fourier decomposition based ECG de-noising. Comput Biol Med 77:195–205
22. Almasi A, Shamsollahi MB, Senhadji L (2013) Bayesian de-noising framework of phonocardiogram based on a new dynamical model. IRBM 34:214–225 (Elsevier, ScienceDirect)
23. Marouf M, Saranovac L, Vukomanovic G (2017) Algorithm for EMG noise level approximation in ECG signals. Biomed Signal Process Control 34:158–165
24. Satija U, Ramkumar B, Manikandan MS, School of Electrical Sciences, Indian Institute of Technology Bhubaneswar (2015) A simple method for detection and classification of ECG noises for wearable ECG monitoring. In: 2015 2nd international conference on signal processing and integrated networks (SPIN)
25. Schanze T (2018) Compression and noise reduction of biomedical signals by singular value decomposition. IFAC-PapersOnLine 51(2):361–366 (Elsevier)
26. MIT-BIH Arrhythmia database. Available Online https://physionet.org/physiobank/database/mitdb/,accessed on 25-8-2018
27. Goldberger AL, Amaral LAN, Glass L, Hausdorff JM, Ivanov PCh, Mark RG, Mietus JE, Moody GB, Peng C-K, Stanley HE (2000) PhysioBank, PhysioToolkit, and PhysioNet: components of a new research resource for complex physiologic signals. Circulation 101(23):e215–e220. Circulation Electronic Pages; http://circ.ahajournals.org/content/101/23/e215.full. 13 June 2000

Analysis of Process Scheduling Using Neural Network in Operating System

Harshit Agarwal and Gaurav Jariwala

Abstract Process scheduling plays a vital role in multitasking for any operating system. There are many factors involved during process scheduling like priorities, free memory, user demand and processor which if not handled properly can be very complex and time consuming. Neural network has adaptive nature which can be used to handle the complex part easily. The main aim of this paper is to review different types of scheduling algorithms working on the principle of neural network and offer constructive criticism to improve their efficiency.

Keywords Backpropagation · Bayesian system · Decision tree learning · Genetic algorithm · Neural network · Process scheduling · Rule-based system

1 Introduction

Since different users use their computer systems in a different ways, neural network in process scheduling will help to optimize the work. Neural network has the ability to learn and solve complex problems while finding the most optimal solutions.

Efficient process scheduling and context switching is the most important step of multitasking. This could be the stepping stone for the AI-based programs and neural network. Their applications are endless. Knowing what job is to be scheduled by studying the user behavior and doing that in an optimal way is a crucial step. It is necessary for the operating system to understand which processes are important and which are not. Researchers have focused on developing algorithms for learning the user behavior on system by recording the application's use and generating a predictive loop. The drawback of this system is that it requires a lot of time to process and is unpredictable.

H. Agarwal (✉) · G. Jariwala
Sarvajanik College of Engineering and Technology, Surat, India
e-mail: 9arshit@gmail.com

G. Jariwala
e-mail: gjariwala9@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_97

For process scheduling, there are many algorithms used. All techniques have some merits and demerits to them which we will discuss in this paper. Methods that will be discussed are job shop scheduling, preemptive scheduling, multithreading, genetic algorithm, decision tree learning, Bayesian system, rule-based system and neural network.

The remainder of this paper is organized as follows. Section 2 reviews related work. Section 3 describes process scheduling based algorithm in detail. Section 4 describes AI techniques based algorithm in detail and existing research. Section 5 shows comparison table between different algorithms. Finally, Sect. 6 draws conclusions and discusses future work.

2 Related Work

Ajmani and Sethi [1] proposed a fuzzy logic-based CPU scheduling algorithm to overcome drawbacks of conventional algorithms for efficient utilization of CPU. This paper has compared the proposed fuzzy CPU scheduling algorithm (PFCS) with priority algorithm; they found that the priority algorithm has more average waiting time and average turnaround time than PFCS. Rehaiem et al. [2] presented an approach for real-time scheduling of reconfigurable embedded systems using neural networks. Sharma et al. [3] have given a optimize credit based scheduling algorithm based on load balancing to improve the performance in cloud computing.

3 Process Scheduling Algorithms

Process scheduling is a procedure that arranges the order and time period of different processes during which they can use the CPU. If not for processing algorithms, a lot of CPU cycles would have been wasted ideally when the process is waiting for I/O or memory. Algorithms in use make our system efficient and fair.

3.1 Job Shop Scheduling

Job shop scheduling is also called linear workshop process scheduling [4]. It can be considered the simplest form of process scheduling. There are different job shops presently capable of handling the jobs, see [5]. They accept the contract and complete the work. In this case, the processes are jobs that are to be finished. The problem is to schedule these jobs in such a way that the jobs have to wait for minimum amount of time before they are processed, and the entire system works efficiently.

For example, before data analysis process is done, it is necessary to obtain data. Hence, I/O process cannot be scheduled after analysis process. Job shop scheduling requires details for the process, time of completion beforehand. We cannot add a new process at runtime which is unsuited for OS. Hence, this method is too static for process scheduling in OS [4].

3.2 Preemptive Scheduling

A scheduling discipline is categorized as preemptive if once the process has been given the CPU, it can be taken away. In preemptive scheduling, a process is given a quantum time during which it is allowed to run. After the quantum time is expired for a process, the CPU control is returned to kernel. This is done using a clock interrupts. The kernel then saves the state, and then, it decides which process will now be given control of the CPU.

If the process has completed before its quantum time expires, the process can forfeit its ownership of the CPU voluntarily to the kernel. This system is unlike non-preemptive scheduling where only when the process itself gives up the CPU kernel cannot access it. If the process is not completed, it goes back to the ready queue and waits for its turn again. The priority of the process in that queue is then depended on the algorithm the processor is running on.

Algorithm that is based on preemptive scheduling is Round Robin. The shortest job first (SJF) and priority scheduling under specific circumstances can be classified as preemptive scheduling. This kind of algorithm is better suited for background process than user process as shutting down the user process against their need will defeat the purpose of user-friendly OS.

3.3 Multithreading

Threads are called lightweight processes (LWP). Threads within a process share address space and other resources. The term multithreading is used to describe multiple threads in same process. When a multithreaded process is running on single-CPU system, the threads run one at a time just like processes in multiprogramming on single-CPU system. The CPU switches between threads so quickly that it gives an illusion of threads running in parallel. True parallelism of running threads can be achieved using multithreaded processors. The minimum requirement for multithreaded processor is the ability to pursue two or more threads in parallel within the processor pipeline—i.e., it must provide two or more independent program counters—and a mechanism that triggers a thread switch [6].

The best way to understand the usefulness of threads is through example. Word processors use threads to increase productivity and improve interactivity. When a user types a character at the keyboard, one thread is used to read that character. Word processor can execute other threads between keyboard interrupts. Like, storing the document in the disk to prevent data loss and checking for spelling mistakes. Each feature is implemented using different threads so even if a thread is blocked due to an I/O operation (storing the document), the word processor can response to keyboard interrupt.

Researchers have attempted to combine advantages of both user threads and kernel threads called scheduler activation (M:N model) [7]. The goals of the scheduler activation work are to mimic the functionality of kernel threads, but with the better performance and greater flexibility usually associated with threads packages implemented in user space [8]. A neural network scheduler can be designed for threads and process in similar way so in this paper we will concentrate on process scheduling rather than thread scheduling.

4 AI Technique Based Algorithms

Algorithms discussed above may not always work. They might be efficient, but they are too static. In order to create a perfect neural system-based operating system, it is necessary to have components that learn from the user over a period of time. AI techniques can be used for process scheduling. It learns user behavior and reprograms the system to predict user's need.

4.1 Genetic Algorithm

Genetic algorithm was inspired by the Darwin theory of natural evolution. This algorithm reflects the process of natural selection where the fittest individuals are selected for reproduction in order to produce offspring of the next generation [9]. The solutions are selected on the bases of their fitness and then promoted further. They are grouped in pairs and combined using genetic operator like mutation and crossover. The child solution created from the parent using these methods then acts like a parent in further iterations.

Figure 1 shows the flowchart of genetic algorithm where initial set of individual solutions are called population. An individual is characterized by a set of parameters (variables) known as Genes. Genes are joined into a string to form a chromosome (solution) as presented in Fig. 2. This process is repeated and evaluated until there is a solution in the set that exceeds a minimum fitness. Crossover operator is applied to the selected chromosomes during which better string is created, while the information in the parent string is optimally preserved. The crossover is done in hope of creating a better string, but the result obtain may or may not be the desired one depending on the use. After crossover, the strings are subjected to mutation [10]. Mutation causes bit-wise reversal. The bit's position is chosen with probability of Pm. The process of mutation is done to maintain diversity in population since selection process may

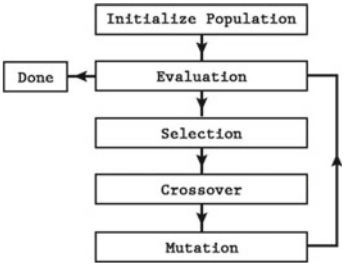


Fig. 1 Flowchart for genetic algorithm. *Source* [9]

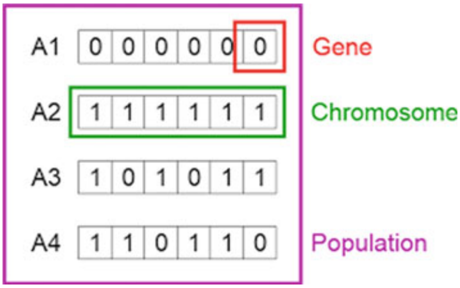


Fig. 2 Elements of genetic algorithm. *Source* [9]

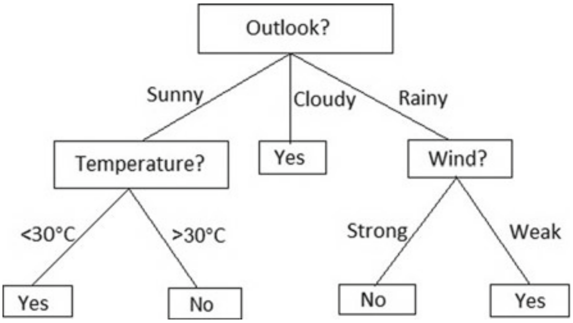
promote same breed of strings which does not optimize search algorithm and helps to retrieve information that may be lost during crossover operator.

Limited research projects have been on implementing genetic algorithm-based schedulers [11, 12]. The process scheduler based on genetic algorithm shows similar results like shortest job first algorithm [13] in certain cases. But shortest job first algorithm cannot be implemented at the level of short-term CPU scheduling. There is no way to know the length of the next CPU burst. Here, performance can be improved by using genetic algorithm. The other studies involved did not use algorithm in the scheduler but rather in the application. The study showed that genetic algorithm had same result as the priority scheduler and the algorithm was time consuming. But the time consumption was mostly due to hardware. With even more simplified algorithm, this problem can be easily solved. The genetic algorithm evolving technique does provide more flexible mechanism than FIFO [8] scheduling and adapts itself to changing environment.

4.2 Decision Tree Learning

As the name says it is a tree-like model of decision. A decision tree contains non-leaf (internal nodes) nodes which represent input features and the leaf nodes are the possible solutions. The splitting at non-leaf nodes is done according to certain discrete function of input attribute values (as in our case) is called classification tree.

Fig. 3 Decision tree to play football



As shown in Fig. 3, an example decides whether to play football or not (in this case Yes or No). At the root node, an instance is classified by testing the attribute specified by this node, and then moving down tree branch according to the value of the attribute. This process is repeated at each node until leaf node is reached.

This algorithm is recursive in nature as same approach is used at each node to split the groups formed. As this algorithm never backtracks to reconsider earlier choices, it is also called greedy algorithm. The algorithm is very simple and easy to implement. The main disadvantage of using this algorithm is its very sensitive to noise meaning small variations in data might result in completely different tree being generated. Furthermore, due to the greedy characteristic of decision tree it cannot guarantee the globally optimal solution. See Doh et al. [14] for decision tree base scheduling for flexible job shops.

4.3 Bayesian System

Bayesian networks also known as belief networks are a graphical model that shows probabilistic relationships among set of variables [15]. It is a graph called a directed acyclic graph (DAG) which contains no directed cycles. Bayesian network requires probability distribution $P(Y|X)$ for each node Y. If node Y has no parents, then it is just $P(Y)$. $P(X|Y)$ is known as conditional probability. For example, to calculate the probability of computer failure, see [16].

Bayesian network can be used, even in the case of missing data, to learn the causal relationships and gain an understanding of the various problem domains and to predict future events [17]. As Bayesian network is a DAG, it cannot be used when the graphical model contains cycle. This approach is computationally expensive. In our case, there is no real structure that can easily be imposed on the data of the system.

4.4 Rule-Based System

Rule-based system uses a set of IF-THEN rules for classification. If the condition mention on the “if” side is satisfied, then the rule is said to be triggered, and the action corresponding in the “then” part executes. This system is the most accurate in comparison with other systems; this is because other system works on probability functions that may not give us always the desired or the most appropriate result. The rule-based system is only as accurate as the rules programmed in the system, but this turn creates problems such as, what if more than one rule is fired or none of them does. This issue can be solved with help of size ordering, rule ordering or class-based ordering [18], the programmer needs to cover the entire basis which makes this impractical for complex systems.

An example of a rule-based system is the domain-specific expert system that uses rules to make deductions or choices. For example, an expert system might help a doctor choose the correct diagnosis based on a cluster of symptoms or select tactical moves to play a game [19].

However, by creating a hybrid system using decision tree and rule-based system can have vast applications with the least amount of drawbacks. We can extract rule from the decision tree system where rules are created from the path of root to leaf node. Using this system helps to convert “IF-THEN” static system to dynamic system which increases its application arena.

4.5 Neural Network

Neural networks or artificial neural networks (ANNs) are analogy from biological neural networks in which neurons are used to transmit signals, while in ANNs nodes are used for the same. These nodes form layers, and each node is connected with every node of next layer with some weights.

There are three types of layers in ANNs, input layer, hidden layers and output layer. Any number of hidden layers can be there in a neural network. The input layer is used to feed the data to the neural network, while the output layer gives the result of the provided input. Each node has its activation upon which the output is decided. The activation of each node is calculated by summing the products of activation of every incoming node with their associated weight and adding it with the bias. Then, the resultant value is passed to a function called sigmoid to get the activation value of the node between 0 and 1.

Backpropagation algorithm is the most commonly used technique in ANNs. In this, each weight is adjusted from the output layer to input layer so that the network error can be reduced. There are other techniques that are used in ANNs which are out of scope for this paper.

Neural network is the most fitting technique to be used in process scheduling as it can adapt to different situations. Since the data of the process are continuous in

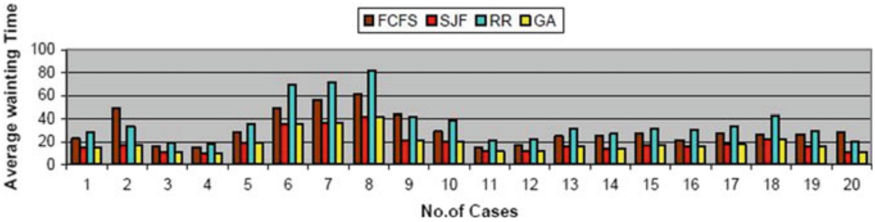


Fig. 4 Comparision of scheduling algorithm. *Source* [20]

nature so are input and output. The demerit of the neural networks is that it is hard to interpret the model as they are trained.

Many studies were done in which stimulations were run for using different algorithms on kernel level. Results obtained from these studies showed that neural network-based algorithms were faster than conventional system used currently.

As shown in Fig. 4, genetic algorithm had the least waiting time among the different algorithm used for job scheduling. Its use also provides more flexibility than other algorithms [20]. Results obtained from different studies [4, 14] were also in favor of neural network-based kernel. During initial phase of the use, system was slow which caused the running applications' performance in percentage of FPS drop and loading speed of the multimedia. But with time, the system was trained and performance showed significant improvement in waiting time for the jobs and percentage of FPS drop. The initial stage problem was reduced with help of pretraining but was not eliminated. Use of decision tree-based approach reduced flow time and increased tardiness. Stable performance was achieved with improvement in the method.

5 Comparison of Algorithms

See Table 1.

Table 1 Comparison between different scheduling algorithms

Name	Method	Merits	Demerits	Improvements
Job shop scheduling	– Queues the job in linear manner	– Simplest form of scheduling – Compatible with all the systems	– Creates a static system – Limits multitasking	– Using multilayer function for scheduling to increase productivity
Preemptive scheduling	– Assigns quantum time to process during which process takes the CPU. After which it is put back into queue	– Single process cannot monopolize the CPU – Priority-based quantum time can be assigned	– It is not suitable for user-based background processes	– User-based processes should have programming to override quantum time
Multithreading	– More than one thread work concurrently within a process	– Improves system's performance – Better use of CPU resources	– Debugging becomes complex – Increase occurrence of deadlock	– Banker's algorithm can be used to avoid deadlock but for using this algorithm maximum numbers of resources needed by each process should be known
Genetic algorithm	– Selection, crossover and mutation functions are used to select the most suitable process	– It overcomes the limitations of shortest job first algorithm	– Crossover may cause unwanted results to reoccur – Results are based on probability function's accuracy	– Creation of simpler program to avoid complexity – Using adaptive crossover function
Decision tree learning	– Non-leaf nodes are split, and the output is generated by the series of decisions	– It is easy to implement – Nonlinear parameters can be handled	– Overfitting is caused due to noise in the dataset – Does not produce globally optimal solution	– Using pruning size of the decision tree can be reduced to tackle overfitting

(continued)

Table 1 (continued)

Name	Method	Merits	Demerits	Improvements
Bayesian system	– It works on the bases of probabilities	– Can be used even in the case of missing data	– It cannot be used when the graph contains cycle – It is computationally expensive	– Its accuracy is very good on small datasets but it may asymptote to a high error rate, making it less useful as a classifier for very large databases [15]
Rule-based system	– Uses set of IF-THEN rules to trigger the rule	– Most accurate system – Can be integrated with any system	– All the rules need to be mentioned manually	– Hybrid system of rule based and decision tree can have more applications
Neural network	– It works on layered structure and output is generated using the activation	– Creates a user-specific system – Adapt to different situations	– Specialized hardware needs to be used to process data – Hard to interpret the structure of neural network	– Creating better compression system for fast computing

6 Conclusion and Future Work

In this paper, process scheduling algorithms and AI-based techniques were analyzed for their implementation in operating system. While in comparison study of some of these algorithms gave similar results, the more advance approach of neural network-based algorithms had the advantage of being more flexible. With recent increase in research in field of artificial intelligence and machine learning, these systems are more likely to use in the future. Job shop scheduling is obsolete and static to handle multitasking used in the current system, while Bayesian system implementation proves to be only theoretical in our case. Though initial uses of neural network systems were slow in comparison with regular process scheduling algorithms, with respect to time the training program and prediction loop provided more efficiency. Until training program reaches to optimal level use of generic algorithms will be more beneficial and then switching of algorithms could take place.

References

1. Ajmani P, Sethi M (2013) Proposed fuzzy CPU scheduling algorithm (PFCS) for real time operating systems. BIJIT - BVICAM's Int J Inf Technol 5(2) (New Delhi, India)
2. Rehaiem G, Gharsellaoui H, Ahmed SB (2016) A neural networks based approach for the real-time scheduling of reconfigurable embedded systems with minimization of power consumption. In: IEEE/ACIS 15th international conference on computer and information science (ICIS), Okayama, 2015, pp 1–6
3. Sharma A, Gupta AK, Goyal D (2018) An optimized task scheduling in cloud computing using priority. In: Proceedings 3rd international conference on internet of things and connected technologies (ICIoTCT), Jaipur, India, 26–27 Mar 2018
4. Bex P (2008) Implementing a process scheduler using neural network technology. Radbound University Nijmegen
5. Yoo BY (1977) Methods and techniques used for job shop scheduling. University of Central Florida
6. Ungerer T, Robic B, Silc J (2002) Multithreaded processors. Comput J 45(3):321–348
7. Anderson TE, Berchad BN, Lazowska ED, Levy HM (1992) Scheduler activations: effective kernel support for the user-level management of parallelism. ACM Trans Comput Syst 10(1):53–79
8. Tanenbuam AS (2009) Modern operating system (3rd edn). Upper Saddle River, NJ, 07458
9. Mallawaarachchi V, Introduction to genetic algorithms. https://towardsdatascience.com
10. Pai GAV, Rajasekaran S (2011) Neural networks, fuzzy logic and genetic algorithms - synthesis and applications, India, July 2011
11. Sharma M, Sindhwani P, Maheswari V (2013) Genetic algorithm optimal approach for scheduling processes in operating system. Int J Eng Res Technol 2. ISSN: 2278-0181
12. Elrad T, Jinlong L, Cork DJ (1998) Evolutionary computation for scheduling controls in concurrent object-oriented systems. Int J Comput Their Appl 5(3):11–20
13. Arpaci-Dusseau RH, Arpaci-Dusseau AC (2014) Operating systems: three easy pieces. Arpaci-Dusseau Books
14. Doh HH, Yu JM, Kwon YJ, Shin JH, Kim HW, Nam SH, Lee DH (2014) Decision tree based scheduling for flexible job shops with multiple process plan. World Acad Sci Eng Technol 8(3):621–627

15. Kohavi R, Becker B, Sommerfield D (2001) Improving Simple Bayes. In: Proceedings of the European conference on machine learning
16. Horný M (2014) Bayesian networks. Technical report no. 5, Department of Health Policy & Management, Boston University School of Public Health, Apr 2014
17. Ben-Gal I (2007) Bayesian networks. In: Ruggeri F, Faltin F, Kenett R (eds) Encyclopedia of statistics in quality & reliability. Wiley, London
18. Jiawei H, Kamber M, Jian P (2012) Data mining concepts and techniques (3rd edn)
19. Gupta A, Newell A, Wedig R, Forgy C (2005) Parallel algorithms and architectures for rule-based systems. IEEE Computer Society Press, Los Alamitos, CA. Tokyo, Japan
20. Dr. Kumar R, Er. Kumar R, Er. Kaushik A, Er. Gill S (2010) Genetic algorithm approach to operating system process scheduling problem. Int J Eng Sci Technol 2:4247–4252

An Enhanced Trust Based Fuzzy Implicit Cross-Layer Protocol for Wireless Sensor Networks

Kompalli Anusha and Ambidi Naveena

Abstract Cross-layer procedure integrates functionalities from first layer of OSI model (physical layer) to transport layer. It enables flexibility, trustworthy and effectiveness in communication process. In this approach, it collects system parameters from multiple layers to enhance the capability of the network. The standard level is decreased by enabling flexibility through inter-layer information exchange. The node selection mechanism is done through fuzzy logic system to provide an efficient communication. Among these benefits, the cross-layering approach faces a problem with security threats in a network. To mitigate these attacks in a network, a trust based cross-layering framework (T-XLM) initiates a trust estimation mechanism using fuzzy logic system to articulate approximate experimental knowledge which is used in reputation building in nodes to avoid defaults in future actions. The TRUFIX is a T-XLM based protocol which is used to permit and hold inter-layer data exchange to accommodate traffic awareness and improve system version. The extension of TRUFIX is E-TRUFIX in which the node if it identifies a malicious node it takes an alternate neighbor route and sends the packet toward the destination. By taking into account with simulation results, E-TRUFIX was compared with FUGEF and TRUFIX which shows an increment in the packet delivery ratio and delay due to the alternate neighbor route.

Keywords Cross-layer approach · Resource bound security solutions · Fuzzy logic system · Wireless sensor networks · Black hole · Sybil · Malicious node

K. Anusha (✉)
Branch of WMC, G. Narayanamma Institute of Technology and Science, JNTUH, Hyderabad, India
e-mail: anusha.kompalli22@gmail.com

A. Naveena
Department of ETM, G. Narayanamma Institute of Technology and Science, JNTUH, Hyderabad, India

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_98

1 Introduction

Wireless sensor network comprises massive amount of nodes that gather and sense physical variables from the sensing limit and transfers the data toward the destination. As sensor node has definite energy resources, less energy must be consumed which in turn improves the effectiveness of the system. The dynamic transport procedures, such as Greedy Perimeter Routing protocol [1], Contention-Based Forwarding [2], Implicit Geographic Forwarding protocol [3] and cross-layer routing protocol [4], are designed using cross-layer method. An improvement in energy and QOS is achieved by cross-layer protocols than traditional layered protocols. In traditional layered protocols, the information is not exchanged between layers compared to cross-layer protocols. In cross-layer approach, most of the approaches failed to consider the concept of entire security phenomenon to contempt its value in the present system and communication methods. In order to provide security in cross-layer protocols, they failed in bringing security at less than three layers which in turn consume resources to implement security mechanisms such as encryption and decryption mechanisms which include keys, respectively, which tend to exert substantially on resources. The memory, bandwidth and energy are tended to be consumed more in key management mechanism which employs cryptography when affirmed to multi-hop network at each sender node required to perform encryption and decryption while preserving original sender cipher. Due to these circumstances in a network, it faces the problem of raised delay, minimum lifetime and null delivery due to drain nodes. To overcome these problems, the trustworthy system is introduced to provide secure data delivery.

Trust is assuredness of honesty between two entities which are involved in communication and it is executed in a field of network security to protect and handle interactions between nodes. This process is accomplished by accommodating generated evidence from previous events and restored to give a report to manage future nodes interactions. This trust theory arises from secured loop feedback rule method joining subjectivity, uncertainty. The superimposed layout of node is not able to create a code which is capable of mitigating all threats in a network. In this paper, our proposed framework has extraordinary adaptable feature which builds on cross-layer module. The framework which is implemented on the basis of XLM is trust based cross-layer module which employs the concept of trust in it to secure a sensor based network. The protocol which is implemented based on these two frameworks is trust based fuzzy implicit cross-layer protocol, and the enhancement of this protocol is E-TRUFIX that holds a modified IEEE 802.11 Distributed Coordination Function Media access Control and uses FLS to design a report mechanism to deliver easy transmission mechanism. Among the simulation observations held, the assured performance of E-TRUFIX and TRUFIX, FUGEF was compared in the presence of malicious node and obtained better performance.

2 Literature Survey

The protocols inspired by this XLM framework include cross-layer routing protocol [4] which drags parameters from the layers of OSI model which involves physical, MAC and transport layer to give a decision which determines that nodes are ready to participate in a communication process. Energy-efficient beaconless geographic routing protocol [5] provides a guaranteed loop-free delivery from source to sink until the network is connected. It utilizes functionalities related to physical, MAC and routing. EBGR is further extended to lossy sensor networks to deal with dynamic topology. It is accessible only to attack free environments and suffers from energy insufficiency problem. MACRO [6] integrates data layer and routing layer operations in order to transfer packet to destination.

SIGF [7], a resource bound security solution, is based on IGF non-deterministic/MAC transmission protocol which has no state and which permits to manage dynamic topologies. It consists of three protocols and implements protection by modifying their routing semantics. It keeps no state and routing information, but it accomplishes an increase in PDR probabilistically. DWSIGF [8] routing protocol enhances performance on selection process in SIGF in order to select malicious nodes by implementing collection window period which increases its window period dynamically to create shift in time in protocol interpretations. This protocol uses data link layer and routing layer functionalities. FUGEF [9] is implemented to select a forwarding candidate node which eliminates substantial packet losses in network and provides better security in network acquisition. It has low packet delivery ratio, and spatio-temporal predictions are not possible. The FUGEF outdoes DWSIGF in terms quality of service performance, energy consumption and overall performance of security provision when subjected to black hole attacks. When subjected to Sybil attacks, no results were shown as with DWSIGF and FUGEF as these are tuned only to black hole attacks. It has low packet delivery ratio.

3 Proposed Method

The proposed protocol trust based fuzzy implicit cross-layer protocol is implemented based on two frameworks:

1. XLM framework.
2. T-XLM framework.

3.1 The XLM Framework

The XLM framework plots its parameters to the sensor protocol store to acquire its combination. It pulls the minimum accessible resources to fend successful communication. The above process was acquired by the combination of the most built in layer capabilities to a single component to fend necessities for efficient communication. In this XLM framework, it gives whole information to a node about when to take part in the transmission mechanism. The communication method starts with a initialization phase which involves a variable initiative denoted as I_d is assigned to 1 if the neighboring node satisfies all the four conditions and 0 if elsewise as shown in Eq. (1). The following conditions are identified by parameters which illustrate the inherent capabilities of the protocol stack and which consists: relay packet level λ_{relay}, left over buffer capacity β, availability and survivability of node E_{rem} and signal-to-noise ratio ξ_{rts}.

$$
\mathrm{I_d} = \begin{cases} 1 \quad \text{if} & \begin{cases} \varepsilon_{RTS} \geq \varepsilon_{RTS}^{Th} \\ \lambda_{relay} \leq \lambda_{Th} \\ \beta \leq \beta^{\max} \\ E_{rem} \geq E_{rem}^{min} \end{cases} \\ 0 & \left[\text{elsewise} \right. \end{cases} \tag{1}
$$

The method of node selection in transmitting data is known as initiative determination. This method is initiated whenever a sender node broadcasts the RTS messages to the neighboring nodes in available broadcast range. On receiving this messages, the nodes are ready to take part in the communication process by sending a CTS messages which include values defining the beginning constants like ε_{RTS} which defines connection reliableness among the neighboring node and sender node, λ_{relay} the control of traffic which avoids congestion, β avoids barrier redundancy due to uncontrollable passage and E_{rem} the remaining energy of a node through span of transmission. The only node which satisfies the above conditions is chosen as forwarding candidate. This framework acquires less energy absorbed using congestion control measures $(\lambda_{\text{relay}}, \beta)$ to avoid packet loss which causes to retransmission. This subject is to have a reliable, disseminative, adjustable communication model.

3.2 Trust Estimation Processes

Trust is defined as a credit which is generated from control theory suggested in the field of E-commerce to choose dependable trade objects. Investigation progressed by applying the notion into various realms using qualified policies to effectively estimate trust through the transacting objects in Fig. 1.

The trust is evaluated from preceding originated proofs combined with reputation transferred from participating objects within a network. The trust estimation process is divided into four classes as shown in Fig. 2.

Probability based approach: This approach was based on two theories which are Dempster–Shafer evidence theory and Bayesian probability theory [10–14]. This process was furthermore divided into:

i. **Objective estimation**: It hangs on information break out of entities over immediate attention.
ii. **Subjective estimation**: It reasonably switches on record of the proof supplied directly or indirectly as gathered from entities.

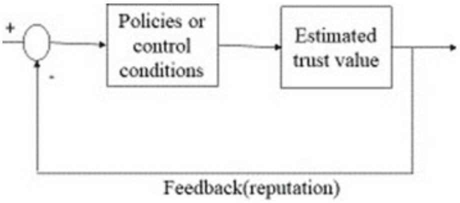


Fig. 1 Typical trust model

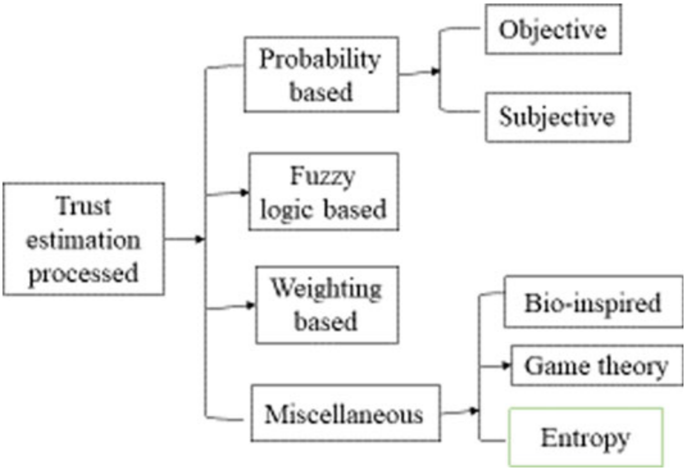


Fig. 2 Trust estimation processes

Outputs acquired after the evaluation stick exactly to a dual outcome.

Fuzzy based estimation approach: Evaluation of trust estimates is pertained through the act of system so that the act can be graded perfect or faulty up to certain extent.

Priority depended evaluation: This method is published by weighting the dealings of sharing nodes through certain duration.

Miscellaneous approach: These are implemented using adopted process or embolden concepts from scientifically and non-scientifically proven thesis.

3.3 The T-XLM Framework

The trust based XLM scheme is a prolonged edition of cross-layer module framework. It exploits trust in choosing a data transferring node to forward packet toward destination. The trust based cross-layer module theory TI is explained in Eq. 2, a connection among the original resolution (I) and report (R).

$$\mathrm{TI} = I \otimes R \tag{2}$$

The modified initiative resolution (I) is shown in Eq. 3

$$\boldsymbol{I} = \begin{cases} \text{positive if} \begin{cases} \boldsymbol{\omega}_{\text{relay}} \leq \boldsymbol{\omega}_{\text{relay}}^{\text{Th}} \\ \boldsymbol{\beta}_{\text{op}} \leq \boldsymbol{\beta}_{\text{op}}^{\text{Th}} \\ \boldsymbol{T} \geq \boldsymbol{T}^{\text{Th}} \\ \boldsymbol{E}_{\text{rem}} \geq \boldsymbol{E}_{\text{rem}}^{\text{Th}} \\ \boldsymbol{\varepsilon}_{\text{rts}} \geq \boldsymbol{\varepsilon}_{\text{rts}}^{\text{Th}} \end{cases} \\ \text{neutral if} \begin{cases} \boldsymbol{\varepsilon}_{\text{rts}}^{\text{min}} \leq \boldsymbol{\varepsilon}_{\text{rts}} < \boldsymbol{\varepsilon}_{\text{rts}}^{\text{Th}} \\ \boldsymbol{\omega}_{\text{relay}}^{\text{min}} \leq \boldsymbol{\omega}_{\text{relay}} < \boldsymbol{\omega}_{\text{relay}}^{\text{Th}} \\ \boldsymbol{\beta}_{\text{op}}^{\text{Th}} < \boldsymbol{\beta}_{\text{op}} \leq \boldsymbol{\beta}_{\text{op}}^{\text{max}} \\ \boldsymbol{T}^{\text{min}} \leq \boldsymbol{T} < \boldsymbol{T}^{\text{Th}} \\ \boldsymbol{E}_{\text{rem}}^{\text{min}} \leq \boldsymbol{E}_{\text{rem}} < \boldsymbol{E}_{\text{rem}}^{\text{max}} \end{cases} \\ \text{Unsuitable if elsewise} \end{cases} \tag{3}$$

I is stated in a congenital language that is easily derived. The parameters are outlined as ε_{RTS} is the derived SNR value of the Request To Send telecast resolved from derived SNR, ω_{relay} is defined as relay packet rate of a node deducted by the holding interval of packets gathering the RTS telecast and β_{op} is the barrier residency interval, E_{rem} is known as remaining energy of node.

$$\boldsymbol{R} = \left\{ \begin{array}{ll} \textbf{Entrusted } (T \geq T^{Th}) \textit{ if} & \left\{ \begin{array}{l} \boldsymbol{sr \geq sr^{Th}} \\ \boldsymbol{fr \leq fr^{Th}} \\ \boldsymbol{\tau \leq \tau^{Th}} \end{array} \right. \\ \textbf{Unclear } \boldsymbol{if} \\ (\boldsymbol{T^{min} \leq T < T^{Th}}) & \left\{ \begin{array}{l} \boldsymbol{sr^{min} sr < sr^{Th}} \\ \boldsymbol{fr^{Th} \leq fr < fr^{max}} \\ \boldsymbol{\tau^{Th} \leq \tau < \tau^{max}} \end{array} \right. \\ \textbf{Mistrusted } \textit{if} & \textit{elsewise} \end{array} \right. \tag{4}$$

R determine value of the node report that is the modernize trust T value. Additionally, sr expresses strike rate to illustrate a nodes capability in transmission of packet, fr is integrity rate to assure way modification and τ amounts the duration of data transmission. The trust value of node n $\left(T_m^n\right)$ by node m inside its transmission domain as detail of the transit stats (∅) and transit capacity (Ω) as shown in Eq. 5:

$$T_m^n = f(\emptyset, \Omega) \tag{5}$$

The traffic statistics and traffic volume are variables observed for a single leap acquaintance, it is defined in Eqs. 6 and 7:

$$\emptyset = g(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6) \tag{6}$$

$$\Omega = h(\partial_1, \partial_2) \tag{7}$$

α_1 packets forwarded through m to n that are dripped by m
α_2 entire no. of packs dripped over m
α_3 packs dripped through m due to obstruction
α_4 packs dripped through m overdue to undetermined details
α_5 n's imposition of m's priority to m's self-packet versus all other nodes Packets
α_6 packets transferring waiting period by m
∂_1 packs diverted through m
∂_2 packs maliciously inserted through m.

3.3.1 Routing Process in T-XLM

The routing process initializes with channel reservation phase in which the forwarding entity sends a request to send packet to the neighboring points to begin the contending process. At this instant, invader resolves coherently to forward such a broadcast message that helps the forwarding entities in packet transmission and also affects the energy consumption among hosts aspiring to compete. Evaluating span of the acquired request to send a telecast beacon and the total count of forwarded packets aids to determine that the signal was reproduced through malignant system or none.

The reception of RTS among nodes initiates to take part by replying off CTS signal by attaching the variables $\varepsilon_{\mathrm{RTS}}$, ω_{relay}, β_{op}, T and E_{rem} as a result of certain span of time. At this instance of time, an invader fight toward election by speeding up in order to make visible a similar response rates like less halting period, connection level and anything as its reply. Suitable election in such times is done once clear to send replies which are resolved utilizing border constraints, such as interval compared to level is lesser than neglected or connection level upon some level is selected. The variables implemented to weight a neighbor node are graded as positive, neutral, unsuitable derived on rated responded through nodes.

A chosen sending host is permitted in order to continue to the subsequent stage, wherein information is forwarded to it. On completion of transmission process, the forwarding entity is dissected down the variables Sr, fr, τ and graded entrusted, unclear and mistrusted. Assaults here involve wherein fewer malignant points determine to grip data drip each and every and few implicit volume of the information afore transmitting to rear system accomplishment. This suggested framework must be able of discovering and mollifying the result of strikes like blocking, black hole, gray hole and Sybil. Due to the new threat involving more kinds of threats to a network, our framework is not vulnerable to all security threats in a network.

3.4 The Proposed TRUFIX Protocol

The TRUFIX protocol excluded persuasions that hold trust and distrust as contradictory offsets of scale. Here nodes congested behavior is marked for malicious behavior and marked distrusted. The TRUFIX protocol that implements routing process in two phases:

1. Channel allotment phase
2. Packet substitution phase

The FLS is used in both phases to route packets toward destination.

3.4.1 The Channel Allotment Phase

In this process, the sender node S sets the NAV timer and on its expiry it perceives a vacant channel for distributed inter-frame space-time duration and transmits an ORTS signal containing the sender position and the destination position to neighboring hosts inside its transmission extent. The transmission orbit contains transmitting contestant nodes and halting contestant nodes. On taking message, the halting nodes abort their replies by fixing their network allocation vector timer. On the other hand, setting their CTS response time, and upon its termination, it reacts back with CTS replies.

The gathered response variables consist of forward range value (d) representing the gap among the transmitting point and the sender node S, clear to send reply interval (ω), that is a behavior of link excellence derived from node allocation interaction to range and added holding interval because of inter-frame spacing and the original trust rate that is fixed to 0.5. Each and every host reply is operated by the first fuzzy logic system to choose the subsequent transmitting contestant node and rated them as positive, neutral or unsuitable.

3.4.2 The Packet Substitution Phase

In this process, information is transmitted out of transmitting node S to the chosen delivering contestant. After the finalization of data substitution, the sending node is analyzed based on three parameters which contains; strike rate Sr that is a measure of trust ability in packet transmission, data transfer period τ that measures the amount of time held out of initiation of data swap interval to its accomplishment corresponding to count of packs transferred inside that time duration and fairness ratio (fr) which raises the dispersal of subsequent stage broadcast options between alike functioning acquaintances and reached to FLS and rated as (trusted, distrusted, unsuited) and returned as feedback to update the trust value by reputation R as shown in Fig. 3.

The mandatory fairness method permits every node to maintain a schedule of the nodes that take part in the pathfinding method. A node selected in order to take part within transferring method, if identified to have performed in the method before is punished by decreasing its fairness ratio and data transfer period rates to guarantee that the node is not chosen in the preceding steps. Identically malignant nodes that

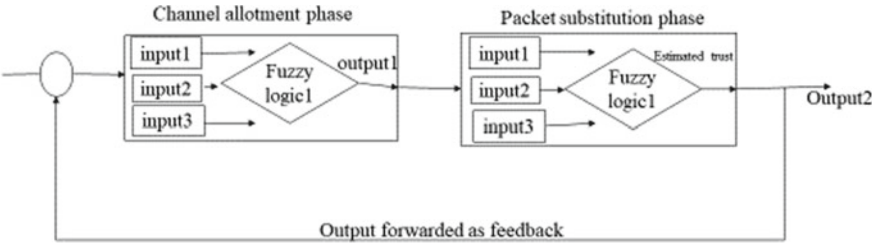


Fig. 3 Proposed fuzzy logic design

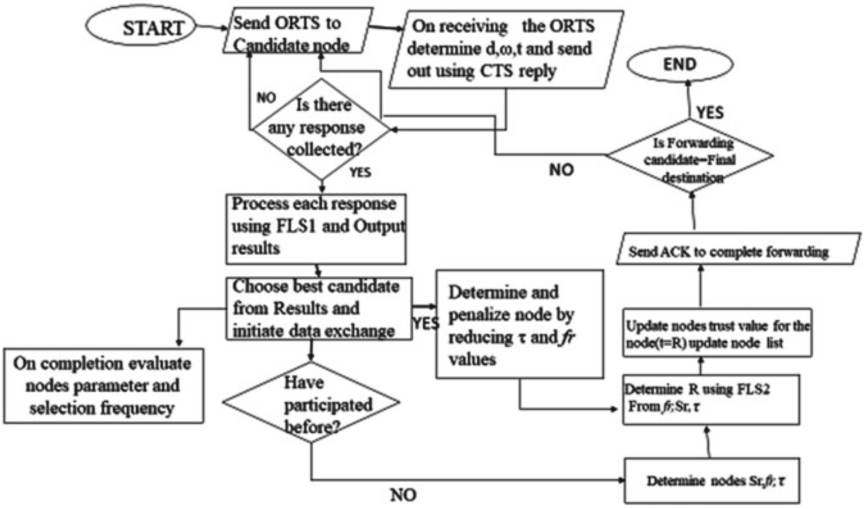

START
Send ORTS to Candidate node
On receiving the ORTS determine d,ω,t and send out using CTS reply
END
NO
Is there any response collected?
YES
YES
Is Forwarding candidate=Final destination
NO
Process each response using FLS1 and Output results
Send ACK to complete forwarding
Choose best candidate from Results and initiate data exchange
YES
Determine and penalize node by reducing τ and fr values
Update nodes trust value for the node(t=R) update node list
On completion evaluate nodes parameter and selection frequency
Have participated before?
Determine R using FLS2 From fr,Sr,τ
Determine nodes Sr,fr,τ
NO

Fig. 4 Flowchart for routing process

have manipulated to work out in performing greater than once are also punished. The whole transmission procedure is outlined in Fig. 4.

The Fuzzy Logic System (FLS)

The FLS is a computationally intelligent system which is used to perform human like decisions that are simple and easy to understand. From Fig. 3, fuzzy logic system manages three variables using 27 rules. In the first fuzzy logic system, the distance calculated between the sender and chosen candidate, reply time and trust to select a forwarding candidate node and rated as (positive, neutral and unsuitable). The FLS2 process the variables sr, fr and τ and graded as entrusted mistrusted and unclear. The result generated is restored back as trust input to the first logic system which is generated from the second fuzzy logic system, thus updating the preceding misprision value 0.5 as original trust value for that detail node. The greatest chance value is selected as the best transmitting candidate and the trusted sender node from Fig. 5.

3.5 *The Extended E-TRUFIX Protocol*

In this protocol, after the processing of the two fuzzy logic systems the packet transmission takes place. In the packet transmission process, if a malicious node occurs in the process, it takes an alternate route and delivers packet toward destination which shows an improvement in the packet transfer rate. The total delay in the transmission process is increased as it takes an alternate route to choose a candidate node in order to forward packet toward destination.

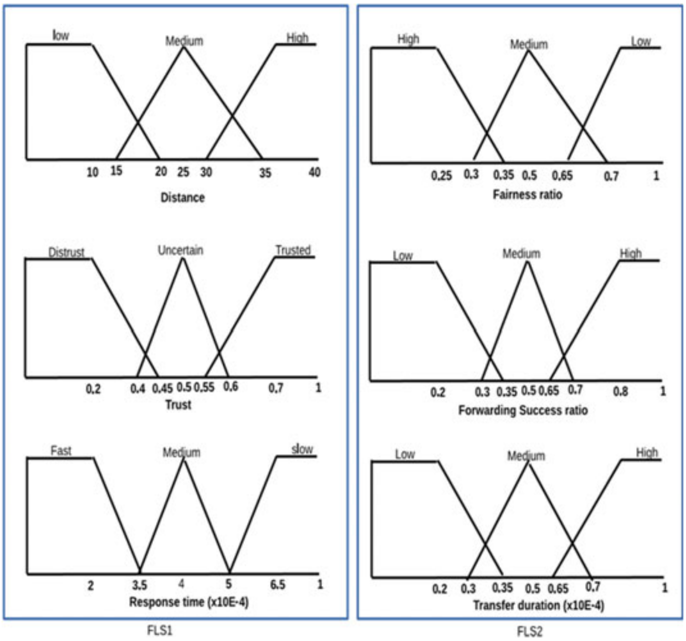


Fig. 5 Input membership functions for TRUFIX

4 Performance Evaluation

The performance of the RBSS based protocols existing protocol (FUGEF), TRUFIX and E-TRUFIX is implemented using NS2 simulation. The variables which are evaluated in these protocols are packet transfer rate (PDR) and end-to-end delay.

From Fig. 6 among existing (FUGEF), TRUFIX and E-TRUFIX, the proposed protocol has achieved high packet delivery ratio and less possibility of attacker selection. Thus, our proposed protocol outperforms all the other three protocols by mitigating the security threats in a network.

From Fig. 6, the enhanced protocol E-TRUFIX achieved high packet delivery ratio due to the node selection criteria by using forced fairness approach and FLS.

From Fig. 7, the E-TRUFIX has high delay due to the processing in fuzzy logic system and to choose an alternate neighbor route which increases delay than other protocols TRUFIX and existing protocol (FUGEF).

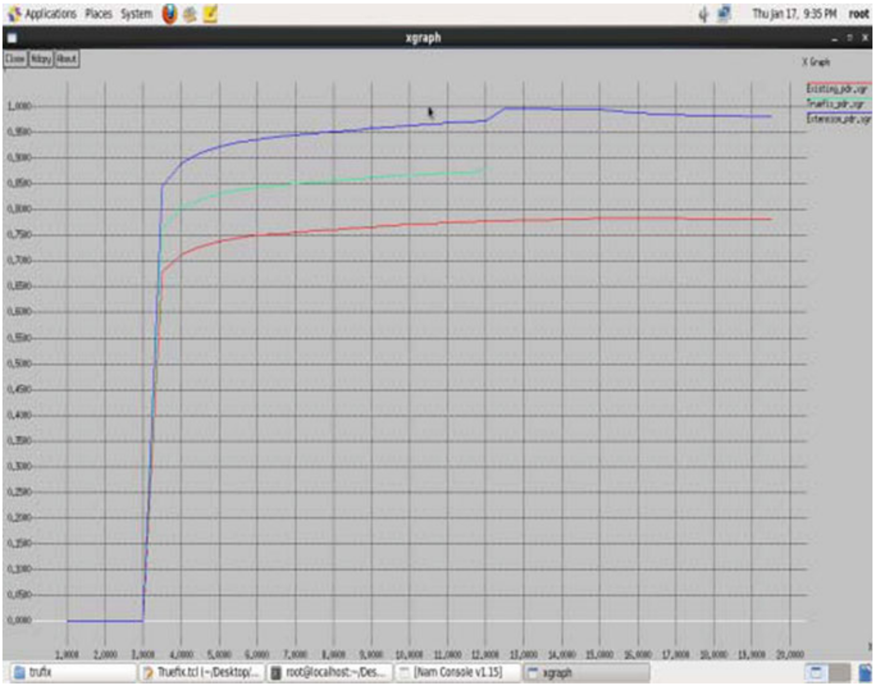


Fig. 6 Packet delivery ratio

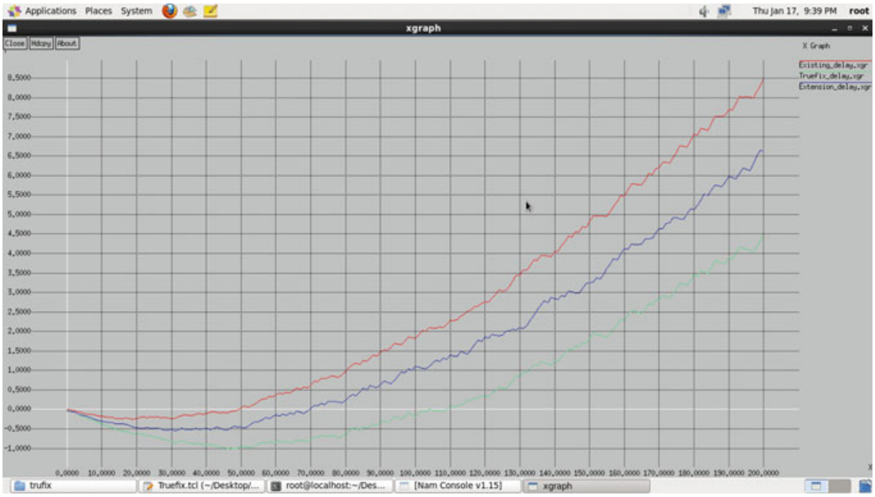


Fig. 7 End-to-end delay

5 Conclusion

The proposed T-XLM based protocol lacks. So, in order to enhance security the proposed protocol TRUFIX is implemented. The FUGEF protocol provides security by changing their routing metrics to nodes by applying fuzzy logic for node election. The proposed TRUFIX involves node election process using fuzzy logic based trust evaluation, and mandatory fairness approach attains optimally suggestive commutation between security and quality. The extension of this proposed protocol is E-TRUFIX has shown an improvement in packet delivery ratio by providing an alternate route and high possibility of attacker selection. In this process, the delay is increased due to alternate route selection.

References

1. Karp B, Kung HT (2000) GPSR: greedy perimeter stateless routing for wireless networks. In: Proceedings of the ACM 6th annual international conference on mobile computing and networking 2000, pp 243–254
2. Füÿler H, Widmer J, Käsemann M, Mauve M, Hartenstein H (2003) Contention-based forwarding for mobile ad hoc networks. Ad Hoc Netw 1(4):351–369
3. Son S, Blum B, He T, Stankovic J (2003) IGF: a state-free robust communication protocol for wireless sensor networks. Tech. Rep., 2003, Department of Computer Science, University of Virginia, Charlottesville, VA, USA
4. Vuran MC, Akyildiz IF (2010) XLP: a cross-layer protocol for efficient communication in wireless sensor networks. IEEE Trans Mobile Comput 9(11):1578–1591
5. Zhang H, Shen H (2010) Energy efficient beaconless geographic routing in wireless sensor networks. IEEE Trans Parallel Distrib Syst 21(6):881–896
6. Galluccio L, Leonardi A, Morabito G, Palazzo S (2007) A MAC/routing cross-layer approach to geographic forwarding in wireless sensor networks. Ad Hoc Netw 5(6):872–884
7. Wood AD, Fang L, Stankovic JA, He T (2006) SIGF: a family of configurable, secure routing protocols for wireless sensor networks. In: Proceedings of the 4th ACM workshop on security of ad hoc sensor networks 2006, pp 35–48
8. Hanapi ZM, Ismail M, Jumari K, Mahdavi M (2009) Dynamic window secured implicit geographic forwarding routing for wireless sensor network. In: Proceedings of the international conference on wireless communication sensor networks. World Academy of Science, Engineering and Technology 2009, pp 173–179
9. Umar IA, Hanapi ZM, Sali A, Zulkarnain ZA (2016) FuGeF: a resource bound secure forwarding protocol for wireless sensor networks. Sensors 16(6):943
10. Quercia D, Hailes S, Capra L (2006) B-trust: Bayesian trust framework for pervasive computing. In: Proceedings of the international conference on trust management 2006, pp 298–312
11. Zouridaki C, Mark BL, Hejmo M, Thomas RK (2009) E-hermes: a robust cooperative trust establishment scheme for mobile ad hoc networks. Ad Hoc Netw 7(6):1156–1168
12. Zouridaki C, Mark BL, Hejmo M, Thomas RK (2005) A quantitative trust establishment framework for reliable data packet delivery in MANETs. In: Proceedings of the 3rd ACM workshop on security ad hoc and sensor networks 2005, pp 1–10
13. Shaikh RA, Jameel H, d'Auriol BH, Lee H, Lee S, Song Y-J (2009) Group-based trust management scheme for clustered wireless sensor networks. IEEE Trans Parallel Distrib Syst 20(11):1698–1712
14. Yao Z, Kim D, Doh Y (2006) Plus: parameterized and localized trust management scheme for sensor networks security. In: Proceedings of the IEEE international conference on mobile adhoc sensor systems (MASS), Oct 2006, pp 437–446

Kompalli Anusha Pursuing M.Tech in the department of WMC, G. Narayanamma Institute of Technology and Sciences, under JNTUH, Hyderabad, Telangana, India.

Ambidi Naveena at present working as Assistant Professor in ETM Department , G. Narayanamma Institute of Technology and Sciences, Hyderabad, She completed B.Tech from G. Narayanamma Institute of Technology and Sciences, Hyderabad. M.E from Osmania University, Hyderabad. At present pursuing Ph.D from JNTUH. She has 12 years of teaching experience.

Implementation of Public-Key Infrastructure for Smart Parking System Using MQTT Protocol

Rajilal Manathala Vijayan, R. Ezhilarasie and A. Umamakeswari

Abstract Applications of IoT are endless, and it has been into many fields like wearable devices, home appliances, etc. This paper investigates the smart parking management application domain, in which the focus is on the users (user requesting for the parking) privacy. Since the number of devices connected to the IoT network grows exponentially, security of the user connected to IoT network is of paramount importance. A scenario like hacking the confidentiality of high-profile users can happen. Thus, this system proposes a solution to protect the identity of the user's by averting the exchange of private information by adapting the zero-knowledge protocol (ZKP) with elliptic curve cryptography (ECC) implementation. ECC, compared with other public-key crypto algorithms, is the best choice for cryptographic implementation on resource-constrained devices. In this framework, the MQTT protocol has been used to establish efficient communication between the user and parking system.

Keywords IoT · MQTT · Security · ZKP · ECC

1 Introduction

IoT applications are spread into many fields like military, medical [1], health monitoring, industrial, intelligent and smart transport system, smart homes, and smart grids [2]. Smart city concept is now becoming possible with the advent of the Internet of Things. One of the critical issues that needed to be taken care in smart cities is car parking facilities [3, 4]. Car parking facility system issues include searching an available parking spot and security issues related to user privacy. Many types of research have been done on developing algorithms for web-based parking management. But, little research has been done on the security issues related to unveiling the identity of users during data transmission between the user and parking system. The hiding of user's location privacy is of much importance as discussed in [5]. Sensitive

R. M. Vijayan (✉) · R. Ezhilarasie · A. Umamakeswari
School of Computing, SASTRA Deemed University, Thanjavur 613401, India
e-mail: rajilalmv@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_99

information like the privacy of high-profile users, for example, where does the person spend the majority of the time, an address of residence, user with disabilities, etc., needs to be secured. The proposed system provides a novel solution that is smart enough to preserve the privacy of the user.

The proposed smart parking application provides security and privacy to the users by averting the interchange of vital information. The user's privacy is protected by adopting ZKP over ECC.

ECC, a public-key cryptography (PKC), provides an adequate level of security compared with other PKC algorithms.

ZKP is a technique where the prover proves the apprehension of a secret, without revealing the confidential information to verifier [6]. Schnorr's interactive protocol, a type of ZKP, is used in the proposed system for implementing zero-knowledge algorithm.

While considering the data transmission between systems, the established communication protocols which are used on the internet cannot be directly used in IoT network. Because certain things like resource-constrained environments of controllers, unreliable networks, security, etc., need to be considered. The proposed smart parking system application used the message queuing telemetry transport (MQTT), an IoT communication protocol, between the user and parking system. MQTT, an IoT application protocol, is a lightweight, open source, simple, and easy to implement publish/subscribe protocol suitable for resource-constrained environments and applicable in the Internet of Things (IoT) context.

The leftover sections in the paper are structured as Sect. 2 talks about the literature survey done on smart parking systems. Section 3 describes preliminaries required for implementation. Section 4 presents the formulated work. Section 5 explains experimentation and validation done on the proposed system.

2 Related Works

While investigating the smart parking management system, the papers listed mainly concentrate on either directing the users to the free or unparked slots or its automation [7, 8]. In [9], a smart parking system is proposed, in which users can view, choose, and reserve an available parking slot before reaching the parking area. But, a little research has been done on the user's privacy. In [10], user security is discussed, in which security research is limited to network security. But, no study has been done on how security protocols can be implemented on resource-constrained devices.

In [11], constrained application protocol (CoAP) protocol is used as a communication protocol for resource-constrained devices. User datagram protocol (UDP)-based CoAP has less overhead than the transmission control protocol (TCP)-based MQTT. However, due to the lack of TCP retransmission mechanisms, the chance of packet loss is more when using CoAP. Hence, MQTT protocol is preferred for communication between systems over CoAP, as CoAP needs to re-transmit the whole message more often than MQTT does, with a high packet loss, which leads to better performance under these conditions for MQTT.

3 Preliminaries of the Work

3.1 ECC

Security is one of the main concerns in the IoT paradigm. Even though MQTT provides the network layer security, the proposed smart parking system application describes the security at application level. The idea behind the smart parking system application is to protect the identity of the users by not revealing any information during the communication between the user and parking system. The advantages and disadvantages of existing internet protocol (IP)-based security, in the context of the IoT paradigm, are examined in [12]. The research portrays that PKC is more appropriate for IoT networks.

ECC replaces RSA on environments, having memory and computation limitations [13]. A 160-bit key in an ECC cryptosystem provides an identical amount of security to that of a 1024-bit key in a conventional cryptosystem as proposed by National Institute of Standards and Technology (NIST). These reasons make ECC suitable for constrained environment implementations as it saves memory space and computational time, and consequently reduces energy requirements.

3.2 ZKP

Implementation of ZKP demonstrates how the privacy of the user can be protected by adapting zero-knowledge proofs based on ECC. ZKP consists of two operators, a prover and a verifier. This proof helps the prover to prove the knowledge of a secret without revealing any vital information [6]. Completeness and soundness are the two properties of zero-knowledge proofs. Complete property describes that a proof is complete if the protocol triumphs with overwhelming probability and if an honest prover and verifier are given. Sound property describes that a proof is sound, if the dishonest prover has negligible probability to complete the proof [14].

4 Proposed System

Little research has been done in the area of maintaining privacy and identity of the users in the smart parking system application. User privacy can be secured either by securing the data that is meant for communication or by maintaining the anonymity of the user itself. The first method of maintaining user privacy is vulnerable to attack from third parties as the data transmission happens between systems. This paper approached the second method, where a novel solution is proposed to maintain the anonymity of the user by totally averting the exchange of private information. The proposed solution uses ZKP over ECC for establishing the protection of user's privacy. MQTT protocol is used for establishing communication between the devices as this protocol is the best application protocol in the IoT paradigm.

4.1 Algorithm

Schnorr's interactive protocol depends upon the elliptic curve discrete logarithm problem (ECDLP), is used to implement the ZKP algorithm.

The following are the Schnorr's protocol steps based on an elliptic curve: Prover and verifier consent on an elliptic curve E, over a prime field F_n, and a generator point $G \in E/F_n$. Prover and verifier know $M \in E/F_n$ and former needs to prove that he/she knows y such that $M = y \cdot G$ to later without revealing y.

4.2 Schnorr's Protocol Steps

1. User calculates the point $N = r \cdot G$, where r is a random value $r \in F_{n.}$
2. Point N is sent to parking system by the user.
3. Parking system computes random $d = HASH\ (G, M, N)$ and sends d to user.
4. User computes $x = r + d \cdot y \pmod{n}$ and sends m to parking system.
5. Parking system checks that $Z = x \cdot G - d \cdot M = (r + d \cdot y) \cdot G - d \cdot M = r \cdot G + d \cdot y \cdot G - d \cdot y \cdot G = r \cdot G = N.$

The implementation of ECC in the work follows the library in [15]. A NIST-approved elliptic curve [16] over prime fields having equation $y^2 = x^3 + a \cdot x + b \pmod{p}$ is used in this work. Order of the curve (r) and the generator point $G(x, y)$ are given in Table 1. Secure hash algorithm-2 (SHA-2) is used [17] for computing the random value "c."

Table 1 Elliptic curve implementation variables

Variable	Value
r	FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141
x	79be667ef9dcbbac55a06295ce870b07029bfcdb2dce28d959f2815b16f81798
y	483ada7726a3c4655da4fbfc0e1108a8fd17b448a68554199c47d08ffb10d4b8

5 Experimentation and Validation

The proposed smart parking management system consists of two systems. The approaching vehicles can be termed as prover, and parking system can be termed as the verifier. The terms prover and verifier are with respect to the ZKP. In this work, only one verifier and one prover are implemented. To validate the work, a system is designed (Fig. 1) using Raspberry Pi 3 model B, along with force sensor (FSR402) and nodeMCU (ESP8266). The force sensor detects the presence of the vehicle and passes the information to the parking system. After this, parking system starts processing the requests from the vehicle. Data flow representation of the system is shown in Fig. 2.

The prover and verifier communication is established using the MQTT protocol. Raspberry Pi controller is used for programming in both sides. The Raspberry Pi at the verifier side serves as the server with MQTT broker. Since the interactive ZKP requires multiple communications between prover and verifier, both prover and verifier serve as both MQTT publisher and MQTT subscriber. After this step, prover subscribes a computed random value from the verifier. And based on the subscribed random value, prover computes a value and published the value to the verifier.

In the experiment, free open-source Mosquito broker and Paho Python MQTT client are used for doing programming in Raspberry Pi.

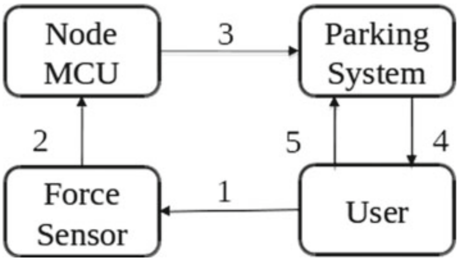
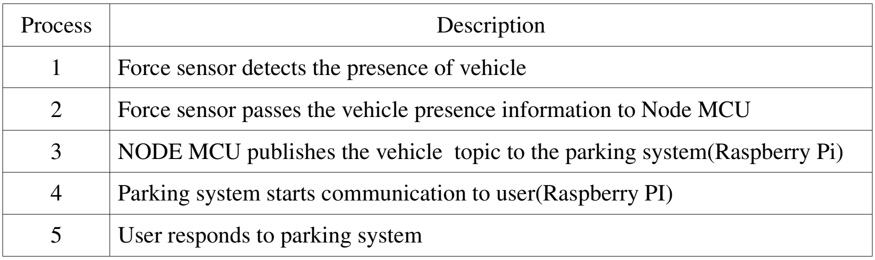


Fig. 1 The system designed using Raspberry Pi along with nodeMCU and force sensor



Process	Description
1	Force sensor detects the presence of vehicle
2	Force sensor passes the vehicle presence information to Node MCU
3	NODE MCU publishes the vehicle topic to the parking system(Raspberry Pi)
4	Parking system starts communication to user(Raspberry PI)
5	User responds to parking system

Fig. 2 Data flow representation of the proposed system

5.1 Prover System

The prover wants to prove that he/she is the authorized user approaching for the parking slot. Prover can be connected to the MQTT server by using *mqtt.Client().connect(mqtt_server_ip, Port_no,keepalive)*. The parameter *keepalive* describes the maximum portion of time in seconds that is allowed between communications with the broker. *publish("Topicname", data)*, can be used to publish data, to which topic name and data are passed. *mqtt.Client().subscribe("Topic_name")* is used to subscribe data from a topic on the broker.

5.2 Verifier System

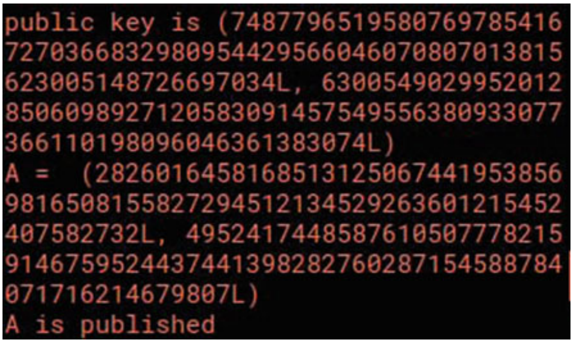
The verifier verifies whether the approaching user is a valid user or not. Verifier is programmed to subscribe data from only one topic. If the verifier is programmed to set separate topics for the receiver, the computation process and code size will be more. So, a single topic is maintained.

5.3 Cheater System

A cheater can cheat or act unfairly toward the system if he/she could find the value of $Z = x \cdot G - d \cdot M$, before the arrival of verifier's hash value, d. Otherwise, the cheater will not be able to act upon the system.

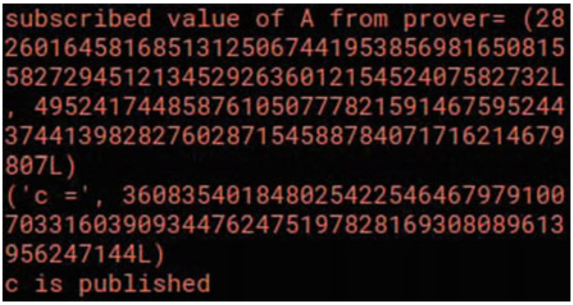
Below are the simulation snippets.

Step 1: Prover (user) sends the computed value to the verifier, as shown in Fig. 3.
Step 2: Verifier (parking system) receives the key from prover and computes the hash value and sends back to prover, as shown in Fig. 4.



```
public key is (7487796519580769785416
7270366832980954429566046070807013815
623005148726697034L, 6300549029952012
8506098927120583091457549556380933077
366110198096046361383074L)
A =  (2826016458168513125067441953856
9816508155827294512134529263601215452
407582732L, 4952417448587610507778215
9146759524437441398282760287154588784
071716214679807L)
A is published
```

Fig. 3 Prover sends the computed value

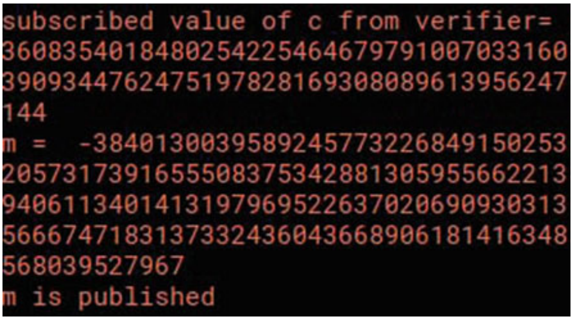


```
subscribed value of A from prover= (28
26016458168513125067441953856981650815
5827294512134529263601215452407582732L
, 495241744858761050777821591467595244
37441398282760287154588784071716214679
807L)
('c =', 360835401848025422546467979100
70331603909344762475197828169308089613
956247144L)
c is published
```

Fig. 4 Verifier sends the computed hash value

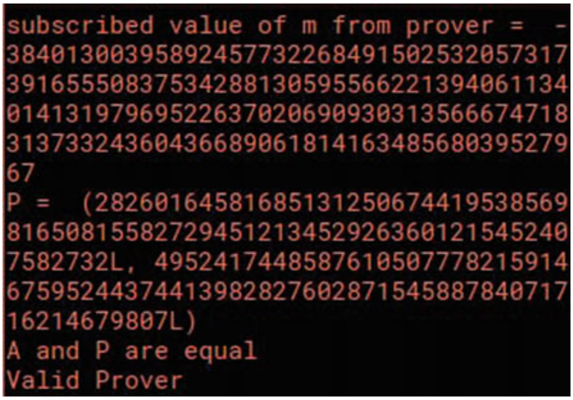
Step 3: Prover receives the hash value and computes the hash value and sends it to the verifier, as shown in Fig. 5.
Step 4: Verifier receives the value and verifies it, as shown in Fig. 6.

Hence, the verifier verifies the proof from the prover and validates the prover.



```
subscribed value of c from verifier=
3608354018480254225464679791007033160
3909344762475197828169308089613956247
144
m =  -3840130039589245773226849150253
2057317391655508375342881305955662213
9406113401413197969522637020690930313
5666747183137332436043668906181416348
568039527967
m is published
```

Fig. 5 Prover sends the computed value



```
subscribed value of m from prover =  -
38401300395892457732268491502532057317
39165550837534288130595566221394061134
01413197969522637020690930313566674718
31373324360436689061814163485680395279
67
P =  (28260164581685131250674419538569
81650815582729451213452926360121545240
7582732L, 4952417448587610507778215914
67595244374413982827602871545887840717
16214679807L)
A and P are equal
Valid Prover
```

Fig. 6 Verifier validated the prover

6 Conclusions and Future Work

Maintaining the privacy of the user in the IoT paradigm is of uppermost importance. Preserving the anonymity of the high-profile users who are approaching the parking system is of high importance. An algorithm, based on ZKP over ECC, is proposed to protect the anonymity of the user identity. ECC has the advantage of providing equivalent security with lesser key size when compared with other public-key cryptographic algorithms (e.g., RSA). The future works include the establishment of an algorithm which offers less proof size than the interactive ZKP used which will be helpful in the resource-constrained environments.

Acknowledgements The authors are grateful to the Department of Science and Technology, New Delhi, India (SR/FST/ETI-371/2014). They also wish to acknowledge SASTRA University, Thanjavur for extending infrastructural support to carry out the work.

References

1. Khan R, Khan SU, Zaheer R, Khan S (2012) Future internet: the internet of things architecture, possible applications and key challenges. In: 10th international conference on frontiers of information technology
2. Bhat SM, Ahmed S, Internet of things: an insight into emerging applications and architectures, national conference on recent advances in computer science and IT (NCRACIT). Int J Sci Res Comput Sci Eng Inf Technol 4(1). ISSN: 2456-3307
3. Zhang Z-K, Cho MCY, Wang C-W, Hsu C-W, Chen C-K, Shieh S (2014) IoT security: ongoing challenges and research opportunities. In: 2014 IEEE 7th international conference on service-oriented computing and applications
4. Zhou F, Li Q, Parking guidance system based on ZigBee and geomagnetic sensor technology. In: 2014 13th international symposium distributed computing and applications to business, engineering and science (DCABES), pp 268–271
5. Krumm J (2009) A survey of computational location privacy. Pers Ubiquitous Comput 13(6):391–399
6. Menezes AJ, Vanstone SA, Oorschot PCV (1996) Handbook of applied cryptography. CRC Press Inc, Boca Raton, FL
7. Wang H, He W (2011) A reservation-based smart parking system. In: 2011 IEEE conference on computer communications workshops (INFOCOM WKSHPS). IEEE, pp 690–695
8. Pala Z, Inanc N (2007) Smart parking applications using RFID technology. In: RFID Eurasia, 2007 1st annual, pp 1–3. https://doi.org/10.1109/rfideurasia.2007.4368108
9. Mutiara GA, Agung AAG, Handayani R (2018) Implementation of smart parking system with real time monitoring. Far East J Electron Commun 8(2):277–290
10. Alqazzaz A, Alrashdi I, Aloufi1 E, Zohdy M, Ming H (2018) SecSPS: a secure and privacy-preserving framework for smart parking systems. J Inf Secur 9:299–314
11. Li W, Jung C, Park J (2018) IoT healthcare communication system for IEEE 11073 PHD and IHE PCD-01 integration using CoAP. KSII Trans Internet Inf Syst 12(4)
12. Nguyen KT, Laurent M, Oualha N (2015) Survey on secure communication protocols for the internet of things. Ad Hoc Netw 32(C):17–31. https://doi.org/10.1016/j.adhoc.2015.01.006
13. Gura N, Patel A, Wander A, Eberle H, Shantz SC (2004) Comparing elliptic curve cryptography and RSA on 8-bit cpus. In: Cryptographic hardware and embedded systems-CHES 2004. Springer, pp 119–132

14. Almuhammadi S, Sui NT, McLeod D (2004) Better privacy and security in e-commerce: using elliptic curve-based zero-knowledge proofs. In: CEC, pp 299–302
15. Malan DJ, Welsh M, Smith MD (2008) Implementing public-key infrastructure for sensor networks. TOSN 4(4)
16. Certicom research (2010) Sec 2—recommended elliptic curve domain parameters. http://www.secg.org/SEC2-Ver-1.0.pdf
17. Eastlake D, Hansen T, US secure hash algorithms (SHA and HMAC-SHA). https://tools.ietf.org/html/rfc4634

Non-bipolar Evaluation and Visualization of Online Text Reviews

Keerthana Chigateri and Rekha Bhandarkar

Abstract Research in the field of Sentiment analysis is blowing day by day exponentially in the recent past and currently it is the much-acknowledged discipline. This is due to the outpouring users of internet and thus generated effusion of data in the form of reviews, comments, blogs, communications, etc. These are treasure trove of information needed to comprehend the fact-based opinions of diverse consumers. Elucidating those contents is propitious to various stakeholders as right sentiments can be gathered through it. But trading with such ginormous unstructured inputs embodies diverse challenges. These challenges trigger the raise in desideratum and thus summon the need to instigate pioneering logics to meet the same and to optimize the existing approaches. Sentiment analysis and opinion mining terms are used equivalently. This existed from ancient days. But the modes employed to perform this were different like in the form of surveys, elections, etc. It was carried out either by individuals or a group or an organization. Individuals used to consult friends or family before changing themselves from strangers to customers of any product or audience of any events. Groups or Organizations used to conduct surveys. But gradually most of the decisions were to be data-driven and thus appropriate decisions were to be made in short-run to bridge the gap between businesses and consumers and to gain the competitive advantage in market. So now this process was to be automated for mutual benefits by exploiting the escalation in technology. Various approaches are emerging every day to strengthen and ease the process. In the same direction, this paper addresses how sentiment analysis of online reviews can serve as suggestions to strangers and help them better in gaining additional insights to make well-judged decisions or choice by visualizing the analysis in the graph form.

Keywords Reviews · Sentiment · Opinion · Suggestive · Non-bipolar

K. Chigateri (✉)
Department of CSE, N.M.A.M.I.T, Nitte, India
e-mail: keerthanabc@nitte.edu.in

R. Bhandarkar
Department of ECE, N.M.A.M.I.T, Nitte, India

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_100

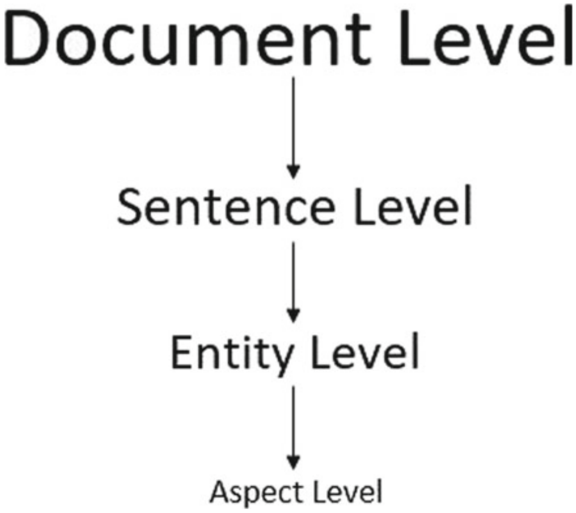
1 Introduction

In ancient times the amount of data available was very less. This was due to various reasons like the absence of smart gadgets, or access to internet by very less people. Initially many people were associated with one basic communicative device with no other option. It was many-to-one association. So the amount, quality and kind of data generated was very less. This data was productive only for telephone industry. Gradually phones with more options other than just communications like camera surfaced the markets. Along with this, association also increased from many-to-one to one-to-one. Thus the data and the kinds of data generated was more than before. Analysis of these data was not very challenging as data was of less variety and infrequently produced compared to present-day environment. Later smartphones slowly flooded the market which supported various features. Along with smartphones, smart devices also floated into the market. So the scenario again advanced from one-to-one association to one-to-many association. Increase in smart devices and their associations with humans not only eased the lifestyle but also led to increase frequency and the kinds of data generated enormously [1]. Now life is almost irrevocable without these smart devices. There is almost no field untouched by this smart technology. Every domain generates its own kind of data different from other domains [2]. So the approach of collecting, processing, extracting, interpretation of data differs to certain degree. These steps need to be carried out regularly, swiftly and meticulously. Thus lot of data is made available on everyday basis which is highly concentrated with valuable information, analysis of which would mitigate the gap between public and service providers effectively by targeting right style of customers at the right time for the right product based on the demographic factors. This yields tangible benefits wholly. To accomplish this, analysis system demands augmentation in techniques continuously. Either the good tool or good data should be available. Having both is almost impossible. So first is recommended solution as latter is less attainable. The analysis needs to get more precise and relevant eliminating the redundancies. More the relevance less is the data entered, collected. Thus processing, storage required also is less and speed increases thereby improving efficiency. The current conventional review system allows the user to review the entire product. This is very abstract as the information provided by most of such reviews is insufficient to make decisions as they do not spot fundamental criteria as of the product. Researchers are focusing and exploring this area to address these limitations. This paper also contributes to the same by analyzing only those reviews targeting the duration of working of hard-disk in non-bipolar way in terms of days, months and year unlike only positive, negative and neutral analysis of the whole reviews.

2 State of the Art

Technology and so our lives are flourishing parallelly. Ergo presently, internet and Smart gadgets are the indispensable part of today's lifestyle of any person through various surveys as they are available within the financial means of people. This has not only led to very effortless communication but also equally in verbalizing of individual's panorama. Research needs to go beyond the current binary (positive and negative) or ternary (positive, negative and neutral) analysis of these panoramas. Reviews along with being positive, negative, neutral or sarcastic, they can also serve as suggestions to others [3]. Such suggestive reviews need to be identified, extracted and analyzed [4]. The largeness of data does not matter but the richness of data matters very much. So analysis of this data is much acknowledged across the globe as it yields many tangible benefits. Initially, this analysis was carried out at the document level usually for blogs to categorize blogs into binary or ternary classes. Gradually this analysis was narrowed down to Sentence level like reviews [5]. Later it was further narrowed down to entity-level like a particular product is positive/negative/neutral. Finally, it's now attenuated to aspect level where a particular feature of a particular entity is positive/negative/neutral [6]. Figure 1 shows this hierarchy of sentiment analysis. Figure 2 represents these five elements of an opinion. Figure 3 shows the block diagram of the approach. The outcomes of the present Bipolar and tri-polar assessment of data is two labels positive or negative and three labels positive, negative or neutral, respectively. But a review can be positive for some aspects, negative for certain features and neutral for few factors [7, 8]. Thus a single review can be positive, negative and neutral at the same time. So concluding it with only one polarity is incorrect. But non-bipolar assessment of data determines multiple labels which connects more to the strangers [9]. It also helps the trade to understand the

Fig. 1 Hierarchy of sentiment analysis



demographics. It is observed through research that changing the colour of the button increases the conversion by 15% [10]. Comprehending the sentiments of consumers to a greater depth and more precisely is very important to ameliorate the customer satisfaction through which business can lead in the competitive market [11]. Such analysis refrains vague services and enables grasping and focusing on the prime preferences of consumers. Thus the resources and time are used effectively and wastage of the same is reduced and productivity is boosted. This paper addresses the analysis of text reviews which is an extension to binary analysis. The emphasis of binary analysis is on only one dimension, i.e., direction-positive/negative. Besides this, there are other four more dimensions of an opinion which needs to be analyzed [12] viz.,

- Intensity: It unfolds the severity or extremity of buyer's viewpoint. It is usually expressed using certain adjectives. For example, worst is more intense or severe form of negativity. Excellent is the extreme form of positivity.
- Stability: based on the context, it conveys various factors like the firmness in services, durability of the product, reliability on a service provider, etc.,
- Informational: it contributes additional details about prime aspect based on which the direction of the opinion can alter.
- Social Support: It enhances the quality of business by giving broader focus on one's particular service/brand/product, etc. It by-product is positive image and well-being in the marketplace.

These other dimensions serve as suggestive to strangers who can choose easily to change into customers or not on viewing this diagrammatic analysis [13].

3 System Design

The main objectives of this research are to design an algorithm to extract only informative data from large repository and to develop optimized techniques for pre-processing the data extracted from the data warehouse. An algorithm to efficiently identify different sentiments if present and to identify and classify the different dimensions of the sentiment needs to be established. This paper works on the dimension, i.e., Stability. Similarly, the other four dimensions viz, Direction, Intensity, Social Support, Information, needs to be worked upon. The meaning of stability differs from context to context. Here, stability means the length of duration or the time period during which its working or functioning is considered to be normal or as expected. Rest of the cases are considered to be abnormal.

4 System Implementation

Here dataset containing 443 reviews on hard disk is considered. In this set, only those reviews are targeted which are expressing about its functioning. It is very laborious and time-consuming to identify only relevant reviews when the number of reviews is very huge. Figures 4 and 5 represents the frequency of working and not working of hard disk, respectively. The *Y*-axis represents duration in terms of days, months and years and the *X*-axis represents the number of people speaking for each case in both figures. This representation is very comprehensive, effortless and less time-consuming in making decision and benefits mutually for both service providers to improve services or to identify loopholes and thus bridge the gap between them, connect effectively and customers to decide quickly. This analysis is beyond binary or ternary analysis. Hence the name non-bipolar. Following is the algorithm for analyzing the reviews speaking about the working and not working of the hard disk in terms of days, months and year. The frequency of reviews about its working is considered as positive and the frequency of reviews about it not working is considered as negative. The keywords found for were 2 days, 2 months, 8 days, 15 days, 10 days, 1 week, 3 years, 1 month, 1 day, 1 year, 20 days, 2 weeks, 8 years, 3 months, 7 months, 5 months, 2 years, 3 days, 3 weeks, 12 days. If the term "working" or any other positive terms (in dictionary) appeared within the window size less than five terms after days/months/years, it was listed under working. Similarly, the term "not working" or any other negative terms (in dictionary) appeared within the window size less than five terms after days/months/years, it was listed under not working. This window size can be varied. For example, in the review "I got these product 8 days before but the hard-disk is unable to detect". Here the stop words like the, but, etc., were remove while pre-processing. The term "unable" appeared within window size <=5 and it is in the dictionary of negative terms. Thus, it is classified under frequency of non-working reviews. The same explanation holds good for positive reviews classification.

Every opinion can contain five main elements:

$$\{E_2, F_{\mathrm{ab}}, O_{\mathrm{abcd}}, H_{\mathrm{c}}, T_{\mathrm{d}}\}$$

where

E_{a} Entity *a*
F_{ab} Feature *b* of Entity *a*
O_{abcd} Opinion of entity *a* for feature *b* by opinion holder *H* at the time *d*.
H_{c} Opinion holder *c*
T_{d} at the Time *d*.

Along with these five elements [5], every opinion should contain a target. An opinion without a target is not substantial for analysis and thus its lifespan is very short. Figure 2 represents these five elements of an opinion.

Step 1: Read the excel file and store it in the form of a DataFrame object

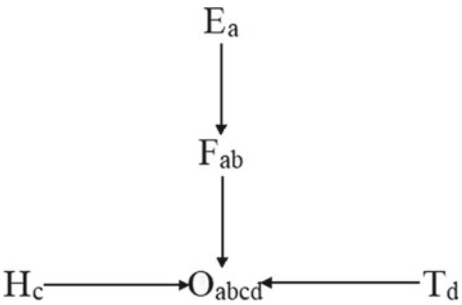


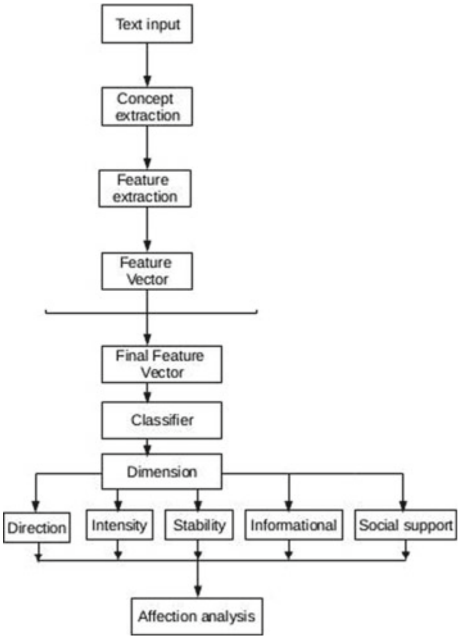
Fig. 2 Five elements of an opinion

Step 2: Calculate the shape of the DataFrame
Step 3: Read the reviews, break it down into individual reviews and store it as an individual element in a list
Step 4: Make lists of factors to review the comments and two lists for all the positive and negative keywords for the keyword search
Step 5: Set the counters for all the review factors as zero
Step 6: Create a dictionary to make a key-value pair of the keywords and its occurrence counters
Step 7: Search for the key in the list and match it with the required reviews and store it in the dictionary along with its count
Step 8: For plotting the graph use the matplotlib library
Step 9: Append all the required labels in one list, calculate the required rows and columns and plot the bar graph
Step 10: Repeat the steps for more sections of the analysis (Figs. 3, 4 and 5).

5 Conclusion and Future Enhancements

In this paper, non-bipolar assessment of opinions of text input processing. The same idea can be made domain-independent in future. It turns out to be the prerequisites for the companies in the current and future scenarios for the business to prosper. By adopting this, they can enjoy the tangible benefits like grasping the issues and acknowledge the trends and competitors influencing the society, embrace fresh customer visions, optimize the strategies, and meet the warnings in the preliminary stages to build an enduring system and services.

Fig. 3 Block diagram of the methodology



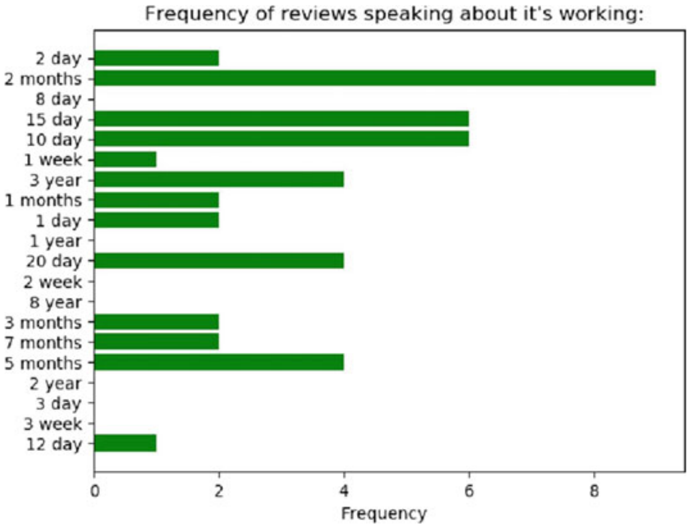


Fig. 4 Graph of reviews on working

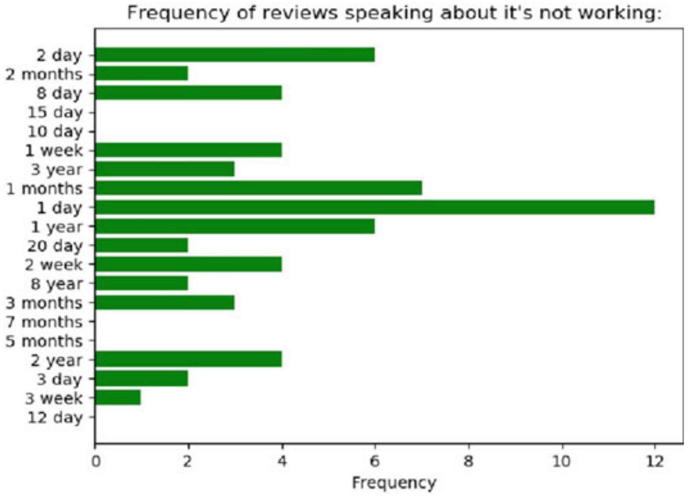


Fig. 5 Graph of reviews on not working

References

1. Shayaa S et al (2018) Sentiment analysis of big data: methods, applications, and open challenges, vol 6. IEEE
2. Mäntylä MV, Graziotin D, Kuutila M (2018) The evolution of sentiment analysis—a review of research topics, venues, and top cited papers. Comput Sci Rev 27:16–32. ISSN 1574-0137
3. Qazi A, Raj RG, Hardaker G, Standing C (2016) A systematic literature review on opinion types and sentiment analysis techniques: tasks and challenges. Internet Res 27(3)
4. Shayaa S, Jaafar NI, Bahri S, Sulaiman A, Wai PS, Chung YW, Piprani AZ, Al-Garadi MA (2018) Sentiment analysis of big data: methods. Appl Open Challenges. IEEE
5. Vo A-D, Nguyen Q-P, Ock C-Y (2018) Opinion–aspect relations in cognizing customer feelings via reviews, vol 6. IEEE Access
6. http://www.e2matrix.com/blog/2017/12/26/sentiment-analysis/
7. Songpan W (2017) The analysis and prediction of customer review rating using opinion mining. IEEE SERA 2017(June):7–9
8. Al-Smadi M, Al-Ayyoub M, Jararweh Y, Qawasmeh O (2019) Enhancing aspect-based sentiment analysis of Arabic Hotels' reviews using morphological, syntactic and semantic features. Inf Process Manag, vol 56(2):308–319
9. Bouazizi M, Ohtsuki T (2017) A pattern-based approach for multi-class sentiment analysis in Twitter, vol 5. IEEE Access
10. https://datafloq.com/read/consumer-behavior-big-data-psychology-evolving/5511
11. Qazi A, Raj RG, Tahir M, Cambria E, Syed KBS, Enhancing business intelligence by means of suggestive reviews. Sci World J 2014
12. https://www.coursehero.com/file/8445224/Comm-303-Five-dimensions-of-Public-Opinion/
13. https://www.experfy.com/blog/suggestion-and-opinion-mining-from-qualitative-surveys, 2015. Available [Accessed 1 Dec 2018]

Status Monitoring System-Based Defense Mechanism (SMS-BDM) for Preventing Co-resident DoS Attacks in Cloud Environment

S. Rethishkumar and R. Vijayakumar

Abstract Co-occupant DoS assaults are discovered as most defenseless dangers in relation to distributed computing which is an asset and generally is obligatory in nature. Co-inhabitant DoS assaults would deplete out the cloud assets which impair the certifiable cloud clients from executing cloud utilization. Consequently, aversion and conclusion of the event related to co-inhabitant assaults result in fundamental assignment of cloud form. In our past research strategy, two-player game approach (TPGA) is acquainted which points that show evasion of co-inhabitant DoS assaults by learning and arranging the virtual machine requested from clients on account of the low, medium, and high hazard demands. Anyway, this strategy decreased in its execution regarding discovery of hazard dimension of client ask for VMs. There is no predefined method for recognizing hazard estimation of VM assets. And furthermore, it would be troublesome to keep up and refresh the hazard status data of the cloud assets. This is settled in the proposed research strategy by presenting the system called status monitoring system-based defense mechanism (SMS-BDM) or state observation-based co-resident DoS attack detection (SO-CRDoS-AD). In the proposed research technique, at first, hazard estimation of each asset dependent on client demands is assessed by utilizing hazard recognition metric. In light of this hazard metric esteem, state estimation of each client asks for as far as VM is refreshed. The states that are considered in this work are security state, vulnerability state, attacked state, positive state, negative state, degenerate state, and failure state. These state estimations of VM assets are refreshed occasionally with the assistance of Markov chain display. This examination technique is actualized in the CloudSim condition from which it is demonstrated that the proposed research strategy can guarantee the exact recognition of assault status of VM asks for; therefore, the security level can be upgraded.

S. Rethishkumar (✉) · R. Vijayakumar
School of Computer Sciences, Mahatma Gandhi University, Kottayam, Kerala, India
e-mail: rethishsnair3@gmail.com

R. Vijayakumar
e-mail: vijayakumar@mgu.ac.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_101

Keywords Cloud security · Defense mechanism · Status monitoring or state observation · Attack state · Risk level of requests

1 Introduction

Virtualization has turned into an appealing study in the present distributed computing condition [1]. The capacity to share the procedure are forms of assets of a solitary physical machine server between a few detached virtual machines (VM) empowering a more streamlined equipment use, and in addition, the less demanding administration and movement of a virtual framework contrasted with its physical partner have offered to ascend to new security policies and VM portion designs [2]. Specifically, virtualization procedures are a key component in distributed computing [3].

In cloud platform, the security issues are related to virtual machine allocation, while distributed computing gives numerous points of interest in availability, versatility, and cost proficiency, and it additionally presents various new security dangers [4]. This paper focuses on the co-resident hit, where malicious users are targeted to genuine VMs through co-locate VM from the same server and then provide side-channel attacks to the targeted VMs and taken private data from genuine VMs [5]. Majority of the previous works are connected with avoiding of the side channels [6]. Be that as it may, sometimes are unrealistic for the current business cloud platform [7].

We approach the issue from an alternate point of view, and concentrate on how to limit the assailant's probability of co-finding their VMs with the objectives, while keeping up a palatable remaining task at hand at par and one with low power utilization for the framework [8]. Our answer does not require any progressions to the fundamental foundation. Subsequently, it tends to be effortlessly actualized in existing distributed computing stages [9].

VM allocation policies against co-resistance attacks in cloud infrastructure are based on the elimination of malignant users from VMs for reducing side-channel attacks and lead to secure the VMs from co-resident attacks [10]. Previous works focused that malignant user targeted a VM called victim VM who is utilizing the side channels [11].

The primary commitment of this exploration work is to present the anchored system for keeping the co-occupant DoS assaults occurring on the cloud assets; subsequently, the ideal asset dealing with can be guaranteed. The principal objective of this examination strategy is to arrange the required asset for the clients ask for according to their necessities and avert pointless use of cloud assets from wastage.

2 Related Works

VM level assurance is pivotal in a virtualized or distributed computing condition. By making a security edge around each VM along these lines, the undertaking can co-find applications with various trust levels on a similar host and can shield VMs in a common, multi-inhabitant condition. In this area, distinctive VM security calculations have been talked about in detail.

Yinqian Zhang et al. depicted about "Home Alone: Co-Residency Detection in the Cloud by means of Side-Channel Analysis" [12]. The abode itself is a framework that gives an occupant a chance to confirm its VMs' select utilization of a current machine.

Adam Bates et al. clarified about "Identifying Co-Residency with Active Traffic Analysis Techniques" [13]. Co-occupant watermarking, a traffic investigation assault that permits a malevolent co-inhabitant VM to infuse a watermark signature into the system stream of an objective example. Thus, our methodology is hard to protect without expensive underutilization of the physical machine.

Yi Han et al. depicted about "Security Games for Virtual Machine Allocation in Cloud Computing" [14]. It focuses on the co-occupant assault, where pernicious clients expect to co-find their virtual machines (VMs) with target VMs on the equivalent physical server, and afterward, abuse side channels to remove private data from the person in question.

Rodrigo N. Calheiros et al. clarified about "CloudSim: a toolbox for displaying and recreation of distributed computing situations and assessment of asset provisioning calculations" [15]. The ongoing endeavors to plan and create cloud advancements center around characterizing novel strategies, arrangements, and instruments for effectively overseeing cloud foundations.

3 Status Monitoring System-Based Defense Mechanism (SMS-BDM) or State Observation-Based Co-resident DoS attack detection Model

The proposed research strategy is presenting the procedure called status monitoring system-based defense mechanism (SMS-BDM) or state observation-based co-resident DoS attack detection (SO-CRDoS-AD). In the proposed research technique, at first, hazard estimation of each asset dependent on client demands is assessed by utilizing hazard discovery metric. In light of this hazard metric esteem, state estimation of each client asks for as far as VM is refreshed. The states that are considered in this work are security state, vulnerability state, attacked state, positive state, negative state, degenerate state, and failure state. These state estimations of VM assets are refreshed intermittently with the assistance of Markov chain demonstrated work.

3.1 Problem Definition

Think about the accompanying situation: in a distributed computing arrangement of:

K servers $S = \{s1, s2, \ldots, sK\}$,
M clients $U = \{u1, u2, \ldots, uM\}$ & begin
N virtual machines $V = \{v1, v2, \ldots, vN\}$.

A mapping X: $U \times V \rightarrow S$, apportions each VM from every client to an explicit server, $XV \times S{\times}U = \{\text{xv}, s, u \mid xv, s, u = 1$ iff VM v of client u is allotted to server $s\}$. An assailant A means to co-find their VMs with the VMs of legitimate client L, i.e., Target (A) = $\sum t$ VM (L, t). Amid, one assault began at time t, A dispatches |VM (A, t)| VMs, and the objective is to expand the proficiency and additionally inclusion rate. Given this assault situation, our new arrangement ought to fulfill the accompanying destinations:

1. Security—Under the new strategy, the aggressor needs to begin countless to accomplish a nonzero productivity or inclusion rate; i.e., VM_{min} is high. Likewise, the inclusion rate does not increment or increments gradually with |VM (A, t)|. So as to accomplish these two, one outstandingly prominent case is that VMs of various clients are never allotted to a similar server. In view of such a thought, we limit the normal number of clients per server, i.e.,
   S: min $\llbracket 1/K \sum\_\ (s \in S)[|u|u \in U, x\_(v, s, u) = 1, \forall v \in V|]\rrbracket$
2. Remaining burden balance—As we referenced in the presentation, the significance of outstanding task at hand balance is twofold. For cloud suppliers, equally disseminating VMs helps decline the likelihood of servers being over-used. For straightforwardness, in our new arrangement, we utilize the quantity of running VMs per server as the rule to spread the outstanding task at hand (equivalent to the least VM strategy). What is more, clients would likewise lean toward if their VMs are not all distributed together on a similar server. As it were, overall, the quantity of servers that have a client's VMs ought to be amplified, i.e.,
   W: max $\llbracket 1/M \sum\_\ (u \in U)[|s|s \in S, x\_(v, s, u) = 1, \forall v \in V|]\rrbracket$
3. Power consumption—How to successfully decrease the power utilization is a significant issue for cloud suppliers. So as to rearrange the issue, here, we just think about the most direct methodology—limiting the quantity of running servers, i.e.,
   P : min$|\{s|s \in S, \exists u \in U, v \in V,\ x_(v, s, u) = 1\}|$

What is more, we make the accompanying presumptions:

1. The limit of a server is not expressly included. Be that as it may, when another VM asks for are being prepared and just the servers with adequate assets left are considered—we allude to these as authentic servers. As it were, we center around structuring a calculation to sort these genuine servers and dispense the new VM to the best-positioned server, with the goal that the over three destinations can be fulfilled.

2. The multi-target improvement is improved the situation each approaching VM ask for when it arrives, with the end goal that just the present framework state and the VM asks for are mulled over; i.e., no look-forward system is utilized;
3. VM live relocation is not mulled over, which implies once a VM is dispensed to a server, it will keep running on that server until the point when it is halted or ended by the client.
4. Cloud suppliers do not have any earlier information of the aggressors or unfortunate casualties, and all VM asks for are dealt similarly.

3.2 *Risk Value Measurement*

The risk value of every user request is calculated by using RISK equation, and the state value of every VM is also updated by using a Markov chain model. Finally, a risk detection metric is used with state transition model so as to optimize the VM allocation in cloud infrastructure. The connection motor uses a tree of consistent conditions, i.e., rules, or AND/OR tree, and it is actualized by OSSIM, an open-source framework. The motor uses Eq. 1 to characterize the hazard an incentive for each gathering of cautions and at whatever point the hazard winds up bigger than or equivalent to one, an alert will be let go:

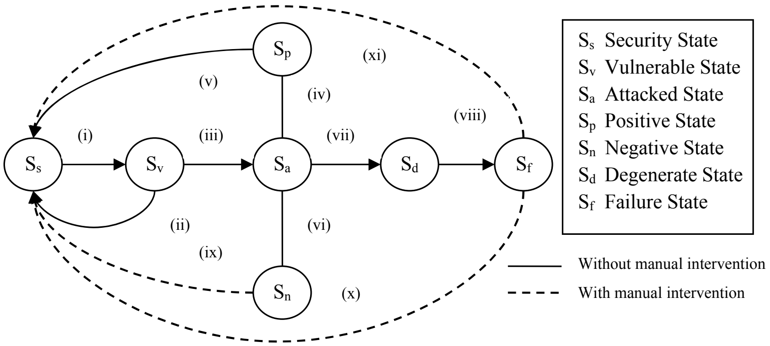
$$\mathrm{RISK} = (\mathrm{AssetValue} * \mathrm{AlertPriority} * \mathrm{DetectionReliability})/\mathrm{NF} \qquad (1)$$

where

AssetValue → value of the attacked resource.
AlertPriority → how dangerous the alert is. This value is set by the firing IDS and is adapted in the normalization step.
DetectionReliability → the probability that the attack defined in a correlation level is real.
NF → fixed normalized factor defined by the administrator in the IDS configuration phase.

3.3 *State Value Observation and Updation Using Markov Chain Model*

The risk factor of every user request is calculated by using risk detection metric, and after that, the state value of every resources is updated by using a Markov chain Model because the security situation of a cloud has been changed in each point of time. The HMM comprises a state change likelihood network P, a perception likelihood framework Q, and an underlying state circulation vector π and is signified by a tuple



(i) accident or pre-attack action
(ii) detect before attack
(iii) begin scanning
(iv) eliminate all negative effect
(v) transparent recovery
(vi) undetected
(vii) graceful degradation
(viii) fail with alarm
(ix) restoration/reconfiguration/evolution
(x) restoration/reconfiguration/evolution
(xi) restoration/reconfiguration/evolution

Fig. 1 State transition model

(P, Q, π). In this work, 7 states are considered. The states that are considered in this work are security state, vulnerability state, attacked state, positive state, negative state, degenerate state, and failure state. The state change model of this exploration technique is shown in the accompanying Fig. 1.

Figure 1 shows the state transition (ST) demonstration where the state set $I = \{S_\mathrm{s}, S_\mathrm{v}, S_\mathrm{a}, S_\mathrm{p}, S_\mathrm{n}, S_\mathrm{d}, S_\mathrm{f}\}$ can be commonly traveled as a system of depicting the dynamic practices of security in cloud. Because of the dynamic use of cloud assets, the security is without a doubt impacted by the accomplished setting. The state change of ST model can be portrayed as pursues.

(i) If the protective techniques, e.g., verification, get to control, encryption, and fix for known vulnerabilities lose adequacy, the framework will enter the helpless state S_v from the security state $S_\mathrm{s}$and effectively experiences being infiltrated and investigated by an aggressor. Be that as it may, if catching the assaults previous interruption, the framework could in any case remain in the state S_s.

(ii) If recognizing the assaults amid being entered and investigated, the framework could come back to the state S_s from the defenseless state S_v. The framework will as often as possible sweep the present state and could quickly dispatch the correct countermeasure after distinguishing assaults.

(iii) If the powerlessness is misused effectively, the framework will be under the assaulted state S_a and the potential harm may happen. In the assaulted state S_a, the framework needs to lead different conceivable ways to deal with recouping from harm and to relieving the misfortune. In spite of the fact that there may be more than one reaction accessible, the framework essentially means to reestablish the security state S_s.

(iv) If the framework dispenses with every single ruinous impact caused by an assault and effectively reestablishes the security state S_s, and afterward, the framework will go into the positive state S_p.

(v) By straightforward recuperation, the framework will recoup from the positive state S_p to the security state S_s.

(vi) If the framework neglects to perceive the dynamic assaults and along these lines takes no reaction, the framework will enter the negative state S_n.

(vii) Having distinguished assaults however unfit to dispense with every one of the impacts, the framework needs to contract the degree of harm while keeping up the basic administration, which is known as the savage state S_d. The fundamental administrations allude to the functionalities that ought to be kept up to fulfill the foundational necessities regardless of whether confronting the unfriendly, disappointments, and mishaps.

(viii) If the above countermeasures do not work by any stretch of the imagination, the framework needs to enter the disappointment state S_f at long last.

(ix), (x), and (xi) By manual mediation, the framework recoups the full administrations after an assault and comes back to the security state S_s from the negative state S_n, the savage state S_d, and the disappointment state S_f, individually.

After calculating the risk value of every user request, then the alert risk of each stage has been verified by using the below-mentioned equation.

$$\mathrm{AR}^s = \left(\mathrm{AC}^s * \mathrm{AP} * \mathrm{DR}^s\right)/\mathrm{NF}^s = \left(\mathrm{AC}^s * \left(C_{\text{severity}} * N_{\text{occurance}}/A_{\text{frequency}}\right) * \mathrm{DR}^s\right)/\mathrm{NF}^s \quad (2)$$

where

AR^s → alert risk at a specific state s.
AC^s → asset cost at a specific state s. AC is computed using the C vector, and it represents the potential consequences of the state s on the asset in question.
AP—<alert priority. It is computed based on C_{severity}, $N_{\text{occurance}}$, and $A_{\text{frequency}}$ as shown in Eq. 2.
C_{severity} → current alert severity defined by the firing IDS.
$N_{\text{occurance}}$ → number of occurrences of current alert in a specified correlation time slot defined in the correlation process.
$A_{\text{frequency}}$ → acceptable frequency of this alert per day based on the training data computed from the attack dataset.
DR^s → detection reliability at a specific state s. It is computed according to the alert position corresponding to s in Matrix Å.
NF^s → A fixed normalization factor that is computed according to the maximum values appeared during training phase for AC^s, AP, DR^s, and maximum alert risk (MR) where AR^s belongs to the range (0–MR^s). All these values are computed for each state independently. Thus, $\mathrm{NF}^s = (\mathrm{Max}(\mathrm{AC}^s) * \mathrm{Max}(\mathrm{AP}) * \mathrm{Max}(\mathrm{DR}^s))/\mathrm{MR}^s$.

3.4 Two-Player Security Game

As expressed [5], when the client accounts are characterized, the diversion approach is utilized for upgrading the barrier system. The assailant's conduct, as found prior, when the aggressor begins their first VM (there is no motivating force for aggressors to begin more than one VM at first, as none of them will co-situate with the objectives), they are marked as medium hazard. So as to be renamed as okay, the assailant needs to keep the first VM running before beginning more VMs. This is known as the underlying expense. Subsequent to being named as generally safe, the aggressor can make the same number of VMs as they need. In any case, they need to deliberately control the pace, with the goal that they won't be renamed as medium or even high hazard. When it turns out to be progressively costly to keep the present record being considered as okay than to make another record (i.e., pay the underlying expense once more), the assailant will dispose of the present record.

4 Results and Discussion

The execution of the proposed status monitoring system-based defense mechanism (SMS-BDM) or state observation-based co-resident DoS attack detection (SO-CRDoS-AD) is assessed in CloudSim. The outcomes are contrasted, and the co-area safe (CLR) calculation proposed in [24], PSSF-based amusement hypothetical methodology (alluded as PSSF in charts) [10], and out past work two-player diversion approach-based protection system (alluded as two-player approach in diagrams) as far as record order exactness, accuracy, review, and assailants by and large expense.

***Accuracy**: Characterization exactness*

Exactness is the rate relating to the effectively done order of client accounts as lawful and vindictive clients.

$$\text{Accuracy} = \frac{(\text{TP} + \text{TN})}{(\text{TP} + \text{FN} + \text{FP} + \text{TN})} * 100$$

Figure 2 shows the comparison of the defense mechanisms in terms of accuracy. From the graph, it can be found that the proposed SO-CRDoS-AD provides highly accurate classification. The proposed research method SO-CRDoS-AD shows 3.2% increased accuracy than the two-player approach, 7.9% increased accuracy than PSSF approach, and 14.4% increased accuracy than the CLR approach.

Precision

Precision is the correctness of the classification of the user accounts.

$$\text{Precision} = \frac{\text{TN}}{(\text{TP} + \text{FP})} * 100$$

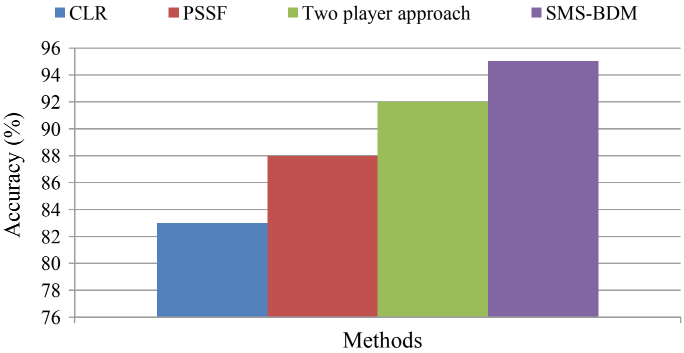


Fig. 2 Accuracy comparison

Figure 3 shows the comparison of the defense mechanisms in terms of precision. From the graph, it can be found that the proposed SO-CRDoS-AD provides précised classification, thanks to the optimal solutions for the large-size data center. It is evident that the proposed defense mechanism can avoid the possibility of attacks with greater probability. The proposed research method SO-CRDoS-AD seems to provide 3.3% increased precision rate than two-player approach, 6.8% improved precision outcome than the PSSF method, and 17.7% improved precision outcome than the CLR method.

Recall

Recall is the completeness of the classification done in the cloud user accounts.

$$\text{Recall} = \frac{\text{TN}}{(\text{TP} + \text{FN})} * 100$$

Fig. 3 Precision comparison

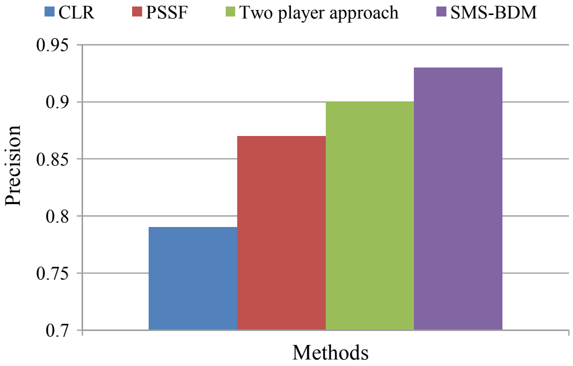


Fig. 4 Recall comparison

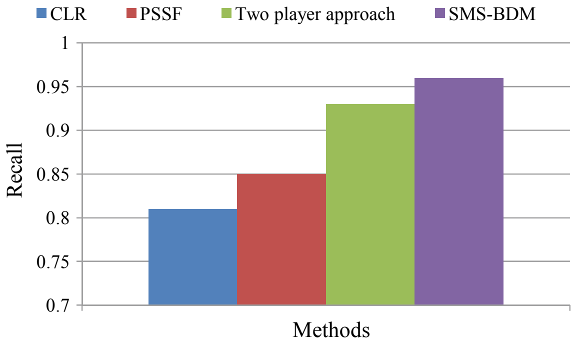


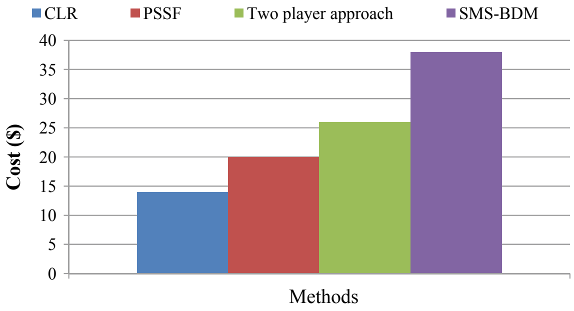
Figure 4 shows the comparison of the defense mechanisms in terms of recall. From the graph, it can be found that the proposed SO-CRDoS-AD provides classification with high recall. The proposed approach increases the defense against co-resident DoS attacks with higher accuracy. Recall of the proposed research method is improved 3.2% better than the two-player approach, 12.9% better than PSSF method, and 18.5% better than the CLR method.

Attacker's Overall Cost

This parameter helps in assessing the expense caused for starting an assault, i.e., making another record for starting another VM. The expense is spoken to in US dollars ($) for normal cost assessment.

Figure 4 shows the comparison of the attacker's overall cost for initiating a new VM for beginning a co-resident DoS attack in the presence of evaluated defense mechanisms. From the graph, the cost incurred by the attacker to initiate a co-resident DoS attack is higher in proposed SO-CRDoS-AD than the other methods. It is evident that the proposed defense mechanism makes it difficult for an attacker by making an attack process highly expensive. Thus, it forces the attacker to reduce risks and behave as a normal user. The proposed research method shows 346% improved performance than two-player approach, 90% improved performance than the PSSF method, and 171% improved performance than the CLR method (Fig. 5).

Fig. 5 Attacker's overall cost comparison



5 Conclusion

In this work, we focus on a specific threat—the co-resident attack that targets the virtualization level and the bottom of the software stack. In this type of attack, the attacker has a clear set of target virtual machines (VMs), and they intend to extract private information from these victims, by co-locating their own attack VMs with the target VMs on the same physical server and then building different kinds of side channels. This is resolved in the proposed research method by introducing the technique called status monitoring system-based defense mechanism (SMS-BDM) or state observation-based co-resident DoS attack detection (SO-CRDoS-AD). In the proposed research method, initially, risk value of every resources based on user requests is evaluated by using risk detection metric. Based on this risk metric value, state value of every user request in terms of VM is updated. This research method is implemented in the CloudSim environment from which it is proved that the proposed research method can ensure the accurate detection of attack status of VM requests; thus, the security level can be optimized.

References

1. Yan Q, Yu FR, Gong Q, Li J (2016) Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: a survey, some research issues, and challenges. IEEE Commun Surv Tutorials 18(1):602–622
2. Cardosa MD, Gopisetty S, Korupolu MR, Singh A (2016) U.S. Patent No. 9424094. U.S. Patent and Trademark Office, Washington, DC
3. Mijumbi R, Serrat J, Gorricho JL, Bouten N, De Turck F, Boutaba R (2016) Network function virtualization: state-of-the-art and research challenges. IEEE Commun Surv Tutorials 18(1):236–262
4. Han Y, Chan J, Alpcan T, Leckie C (2017) Using virtual machine allocation policies to defend against co-resident attacks in cloud computing. IEEE Trans Dependable Secure Comput 14(1):95–108
5. Han Y, Alpcan T, Chan J, Leckie C, Rubinstein BI (2016) A game theoretical approach to defend against co-resident attacks in cloud computing: preventing co-residence using semi-supervised learning. IEEE Trans Inf Forensics Secur 11(3):556–570
6. Zuo P, Hua Y, Wang C, Xia W, Cao S, Zhou Y, Sun Y (2017) Bandwidth-efficient storage services for mitigating side channel attack. arXiv preprint arXiv:1703.05126
7. Beaumont O, Eyraud-Dubois L, Lorenzo-del-Castillo JA (2016) Analyzing real cluster data for formulating allocation algorithms in cloud platforms. Parallel Comput 54:83–96
8. Nalinipriya G, Varalakshmi PJ, Maheswari KG, Anita R (2016) An extensive survey on co-resident attack in dynamic cloud computing environment. Int J Appl Eng Res 11(5):3019–3023
9. Levitin G, Xing L, Dai Y (2017) Co-residence based data vulnerability versus security in cloud computing system with random server assignment. Eur J Oper Res
10. Qiu Y, Shen Q, Luo Y, Li C, Wu Z (2017, August) A secure virtual machine deployment strategy to reduce co-residency in cloud. In: Trustcom/BigDataSE/ICESS, 2017. IEEE, pp 347–354
11. Ezhilchelvan PD, Mitrani I (2017) Evaluating the probability of malicious co-residency in public clouds. IEEE Trans Cloud Comput 5(3):420–427
12. Zhang Y, Juels A, Oprea A (2011) Home alone: co-residency detection in the cloud via side-channel analysis. In: 2011 IEEE symposium on security and privacy

13. Bates A, Mood B, Pletcher J, Pruse H, Valafar M (2010) Detecting co-residency with active traffic analysis techniques
14. Han Y, Alpcan T, Chan J, Leckie C (2011) Security games for virtual machine allocation in cloud computing
15. Calheiros RN, Ranjan R, Beloglazov A, De Rose CAF (2010) CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms

Resource Scheduling Algorithms for Cloud Computing Environment: A Literature Survey

V. Arulkumar and N. Bhalaji

Abstract Nowadays, resource scheduling in cloud environment is a challenging task as the number of customers increases for utilizing the cloud services. In this cloud environment, allocation of suitable resources to the corresponding VM depends on the QoS requirement of the specified applications. Researchers have developed so many resource scheduling algorithms. However, the service providers in cloud environment still find it difficult to choose the appropriate algorithm for their applications. This is due to the heterogeneity of resource types, interdependencies, uncertainty and dispersion of assets in the cloud environment. This paper reviews all the available load balancing algorithms in a nutshell.

Keywords Load balancing · Cloud computing · Resource scheduling

1 Introduction

Cloud computing recently emerged as a promising technology for providing unusual services through Internet to satisfy customer requirements based on their demand with least spending. As a matter of fact, cloud is a broadly shared figuring which is determined by economies of scale, where a pool of preoccupied, virtualized, progressively versatile, oversaw registering power, stockpiling, stages, and any administrations could be conveyed to outer clients given by devoting Internet. The client can profit or anticipate all kind of administrations or assets without building, observing and keeping up their interior resources. It delivers infrastructure, platform and software as a service to the customers. The cloud computing provides added services, which are system infrastructure dependent even if the clients do not have infrastructure. Since customers using the cloud providers' infrastructure on pay as used and on demand basis, all of us can accumulate resources and operational venture.

V. Arulkumar (✉) · N. Bhalaji
Department of Information Technology, SSN College of Engineering, Chennai, India
e-mail: arulkumarv@ssn.edu.in

N. Bhalaji
e-mail: bhalajin@ssn.edu.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_102

Due to this, customers can upload their data on the providers' platform instead of on their own environment. Their task could run on the cloud and share the server's space within the cloud to do dealing out and manipulation of data, etc. A bundle of specialist co-ops are putting forth distributed computing administrations by conveying server farms at different areas around the globe. In flow situation, the specialist co-ops evaluated that server farms expend 0.5% of the world's all out power use. Supplier server farms are requesting more vitality, and it continues multiplying every year. This prompts harm of condition and furthermore builds consumption of the specialist organization. Eventually, situation demands for the researchers to find reasonable scheduling or resource management plan to deploy on the service providers' data centers to ensure their customers to serve speedy manner. Advanced scheduling scheme supports to cloud service providers in effective way of deploying their data centers. Resource scheduling can be achievable through any of the following ways: schedule VMs to conserve data center utilization, effective way of managing the VMs and primary infrastructure, decrease working inefficiencies for non-essential tasks and optimize data center load. Existing work investigates the compelling method for VM executives for the most part fits on any of the followings: watch cloud utilization and machine load in this circumstance when load diminishes: Live relocate VMs to increasingly used hubs and shutdown unused hubs. The potential outcomes of opposite side for example load builds: Use hold up states to fire up holding up hubs and timetable new VMs to new hubs. Burden adjusting is an imperative undertaking in cloud executives to accomplish most extreme use of assets. Large burden adjusting task has been investigating either static or dynamic techniques. Static strategy is easy to reproduce yet does not suit heterogeneous condition. The dynamic technique is hard to recreate; however, it suits for heterogeneous condition. Here, primary center dimension is at which hub the static or dynamic calculation has been actualized. This assumes a noteworthy job in choosing the adequacy of calculation. Successful method for actualizing load adjusting calculations on cloud foundation basically centers around proficient usage of assets and finishes the assignment in least time with least use charges. Figure 1 gives an overview of LB algorithms in cloud computing environment.

In this paper, we present an audit of current LB algorithms in cloud computing situation. Examination of various algorithms is done bringing out notable parts of every one of the categories.

The benefits of various algorithms are viewed as dependent on numerous parts of the execution. Some of the aspects are shown in Table 1.

2 Literature Review

Numerous specialists have worked in the region of LB in cloud computing condition. These are gone for decreasing the overutilization or under usage of VMs in the cloud. There are static and dynamic LB plans. Opportunistic load balance (OLB) is one of the generally utilized LB plans, in which the undertakings are additionally

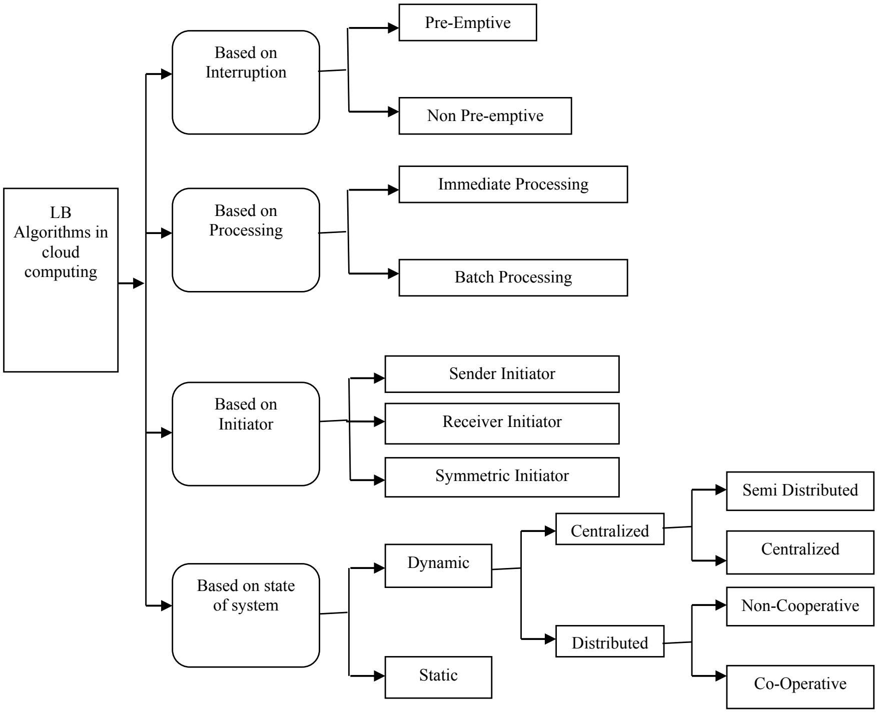


Fig. 1 Load balancing algorithms in cloud computing

Table 1 Performance metrics considered for load balancing

S. No	Parameter	Remarks
1.	Throughput (TP)	In light of the quantity of assignments finished effectively
2	Migration time(MT)	Time elapsed when the resources move between nodes
3	Response time (RT)	Time taken to respond by the resources to respond for a request
4	Fault tolerance (FT)	The ability of a calculation to complete uniform burden adjusting notwithstanding when interface falls flat
5	Resource utilization (RU)	Measured utilization of resources
6	Scalability (Sc)	Capacity of a calculation to execute as arranged when the quantity of hubs increments

partitioned into sub-errands and are doled out for completing the remaining task at hand at all conceivable time. The OLB algorithm offers better efficiency with the hosts being kept busy to the maximum extent. However, makespan suffers in typical cloud environment. Another dynamic algorithm is known as Minimum Execution Time (MET) algorithm. This approach tries for better makespan in the system by appropriate balancing of cloud resources. This methodology offers fluctuated contrasts in the heap over the framework. A Minimum Compilation Time (MCT) is a calculation, in which prepared to-execute time and the normal execution time are viewed as together for adjusting. This methodology can be considered under static and dynamic techniques. The Simulated Annealing calculation looks to abstain from getting kept to neighborhood minima and scans for all inclusive ideal arrangement. The First Come First Served (FCFS) calculation is one of the most straightforward calculations. In this, the primary occupation in the line is dispensed to the main free VM, with no inclinations. This calculation is non preemptive. The turnaround and the reaction time in this calculation are extremely high when contrasted with numerous calculations. min–min scheduling depends on the idea of allocating an undertaking having least fulfillment time first for execution on the asset, which has the base consummation time (quickest asset). In any case, this algorithm is disadvantageous if the quantity of bigger measured errand is more than the quantity of shorter assignments. Max–min scheduling depends on the idea of doling out an assignment having greatest finishing time first for execution on the quickest asset. Be that as it may, this approach is required to expand the all out reaction time of the framework. Specialists have dealt with the above general plans and have displayed better exhibitions in regard to certain aspects. The service provider is relied upon to pick whichever suits the prerequisites close by.

Rajput and kushwah [1] surveyed distinctive static and dynamic LB calculations in-task planning established on load balance, opportunistic load balancing algorithm (OLB), round-robin load balancer, max–min calculation, min–min calculation, randomized, FCFS serve calculation, most brief reaction time first, similarly spread current execution and asset mindfulness scheduling algorithm regarding their relative favorable circumstances and weaknesses.

Aslan and shah [2] reviewed diverse intuitive LB algorithms which are tending to various issues from various perspectives and give distinctive arrangements. The authors classified the focal points and weaknesses of different static calculations like static LB, round-robin, min–min, max–min and dynamic calculations like honey bee, ant province, container and throttled LB calculations. The exhibitions of every one of these calculations are classified for various parameters, for example, fairness, response time, throughput, overhead, adaptation to internal failure, execution, asset use, speed and multifaceted nature.

Nitaka [3] proposed another strategy for appropriating the heap in cloud condition by actualizing round robin, similarly spread current execution calculation and throttled LB algorithm successively so as to improve the general framework reaction time and furthermore to get diminished postponement with the server farm preparing time. The proposed work is executed in three unique dimensions. In level 1, round-robin calculation is executed which disperse the heap on irregular premise, second dimension similarly spreads the outstanding burden and considers less VM as per the circulation procedure and third dimension is executed by throttled calculation.

Samal and Mishra [4] made a near examination of variations of various round-robin calculations, to be specific, round-robin (RR), modified round robin (MRR), time slice priority-based round robin (TSPBRR). The investigation is accomplished for different parameters like setting switch, throughput, CPU usage, turnaround time, holding up time and reaction time. They opined that the TSPBRR calculation gives better throughput least turnaround time, holding up time and reaction time contrast with RR and MRR.

Zhang et al. [5] proposed a double tree-like structure comprising of leaf hubs, child hubs, parent hubs and so forth which partition the simulation region into subdomains. The outstanding task at hand will be isolated into sub-areas dependent on quick adjusting calculation. Outstanding burden is determined dependent on the calculation which gives high productivity, quicker adjusting rate and less correspondence overhead. Be that as it may, the topology is not kept up.

Dhinesh Babu and VenkataKrishna [6] proposed a method dependent on characteristic conduct of honey bee for finding and harvesting sustenance to adjust the remaining task at hand between the virtual machines for amplifying the throughput. It plainly distinguishes the VM with work of lesser need. At the point when high need remaining task at hand comes, it will be coordinated to VMs with lesser need work. It is exceptionally intended to give most extreme throughput, minimum waiting time and with less correspondence overhead. In any case, the principle downside of this calculation is that in the event that more works with higher need come, at that point the lower need work will sit tight in the line for long-lasting.

Chandrakanta and Piyush [7] have likewise proposed a novel honey bee enlivened LB calculation dependent on scavenging conduct of honey bees in a cloud situation. The undertakings are doled out to VMs which are running in parallel to create the yield with less execution time. It utilizes the pare to predominance idea for both choosing ideal VM, and diverse QoS parameters are considered for setting needs to the assignment. It is expected that the assignments are free, and the VMs utilizes preemptive errands scheduling.

Dong et al. [8] proposed a LB concept dependent on a distributed architecture to conquer the issues of dynamic file movement, versatility and accessibility of the parallel record framework. In this method, an appropriated leader will be utilized, in which every I/O server can take their very own choice to allocate remaining tasks at hand to VMs contingent on the present circumstance of the framework to give better adaptability and accessibility.

Deng and Lau [9] proposed two warmth dispersion algorithms global and local dissemination for circulated virtual conditions where the load has gotten to by simultaneous clients may make issues when number of clients increments. In this propose, the virtual condition is part into huge number of square cells and each square cell having a hub. Global diffusion algorithm comprises of two phases (i) global scheduling stage and (ii) local load migration stage. In local diffusion algorithm, local decision making and effective cell choice plans are utilized which basically contrast the neighboring hub loads with the contiguous hub loads. In the event that heap is little, at that point, the exchange of load ends up conceivable. Here, global dissemination works better and give less correspondence overhead, fast and require just less measure of figuring, however, needs in system delay.

Esch and Tobias [10] presented the idea of overlay systems to interconnect each one of the machines that makes the foundation of an online situation. LB algorithm encourages the whole system to be separated into littler cells, and every cell is furnished with different hotspots which are utilized to figure without a doubt the mass of the item. Every single cell is checked and overseen by an open server. Hotspot precision expanded when the system load increases. It gives dependable, versatility, proficient directing and adaptation to internal failure and furthermore gives number of connections doled out to every hub when the system over-burden. In any case, it sets aside some effort to adjust the heap as the open servers are put haphazardly.

Godfrey et al. [11] have presented the idea of virtual server to improve the execution of the system in a dynamic load balancing system. In this, load information of the peer nodes is stored in different directories which are used to schedule the workload to different virtual servers for better balance. It is more qualified for shifting remaining tasks at hand and number of hubs with high hub use and improved versatility. Be that as it may, the reassignment work of virtual server is troublesome.

Kokilavani [12] proposed a min–min method. It is a basic and quick executing approach. In this method, the allotment happens in two stages. In the main stage, every single autonomous undertaking without any information reliance on different assignments is gathered, and their individual least execution time is determined. The second stage comprises of designation of undertaking with least execution time to the reasonable assets. The fulfillment time of the offset assets is refreshed with the expansion of the culmination time of as of now running project. When an undertaking is finished, it will be expelled from pending rundown until all errands are allotted. Despite the fact that this calculation offers better throughput, reaction time and asset use, it creates high correspondence overhead. This calculation cannot adjust the outstanding task at hand legitimately since it focuses on the little undertakings first.

Chen et al. [13] presented another priority-based improved min–min load balancing calculation standard to diminish the fulfillment time of assignments and increment the asset uses. It depends on the standard min–min algorithm. The authors executed standard min–min, improved min–min and priority-awarded load balancing min–min algorithm using MATLAB. The outcomes for makespan, average resource utilization range, average VIP tasks completion time and average ordinary tasks completion time are contrasted by shifting the assets and diverse speed and errand with various size. The outcome demonstrates that this calculation decreases 20% of the normal finish time of VIP errands.

Anandharajan and Bhagyaveni [14] proposed a load balancing algorithm based on random sampling of the system. This method, which is appropriate for extensive framework, works in decentralized manner accomplishing self-association in adjusting the outstanding task at hand. This is conceivable by developing a virtual chart with the availability of every server. The graph is drawn depicting the degree directed to the free resources of the server. But, it is found that the performance is degraded when there is an increase in population diversity.

Chauhan and Joshi [15] have developed max–min algorithm by modifying only in the second phase of min–min algorithm. In this, the task with maximum expected completion time is taken first and assigned to suitable resources. It gives importance to long tasks first and suitable for some environments.

Bhoi and Ramanuj [16] built up an upgraded max–min planning calculation by completing a little change in improved max–min calculation. This calculation depends on expected execution time as a determination premise rather than culmination time. Be that as it may, it allocates assignments with normal execution time to asset that produces least consummation time in improved max–min. On the off chance that biggest undertakings are excessive since quite a while ago contrasted with different errands, it expands the general make-length since it is executed just by slowest asset first. Different errands are executed by quicker assets. This downside is overwhelmed by upgraded max–min calculation. The calculation is simulated by CloudSim for different assets. The outcomes demonstrate that it diminishes by large makespan and can adjust the heap crosswise over assets.

Li et al. [17] proposed an improved max–min task scheduling algorithm. Their algorithm provides elasticity in cloud computing by maintaining a status table for all tasks and calculates the existing workload for each machine along with expected time of completion for each task. This table helps in allocating the remaining workload among VMs. The algorithm is assessed by simulation by using CloudSim. The parameters considered are task pending time, task reaction time, hypothetical simultaneousness and asset use. This Elastic cloud Max–Min (ECMM) calculation gives 21.4–30% improvement in results for normal undertaking pending time as contrasted and max–min and round-robin calculations. Be that as it may, ECMM needs in assignment reaction time proportion contrasted with max–min calculation.

Konjaang et al. [18] introduced a new optimized scheduling algorithm based on max–min algorithm. It identifies the tasks with maximum completion time and minimum completion time. The algorithm assigns anyone of the tasks to the available resource to increase the throughput. This helps to overcome the increased makespan time of standard max–min algorithm. Comparison between the results with standard max–min and round-robin algorithm concludes that the max–min offers better results in terms of makespan time and load balancing.

Elzeki et al. [19] presented an improved max–min calculation making a remarkable change in the standard max–min calculation. It considers the effect of RASA calculation in appointing errands alongside max–min methodology. It allocates the undertaking with greatest execution time to asset with least fruition time. RASA is a hybrid algorithm of max–min and min–min algorithms. The calculation ascertains the normal consummation time for each assignment on the accessible assets. After the computation, max–min and min–min calculations are connected again to exploit the two calculations wiping out their disadvantages. The calculations of max–min, RASA and improved max–min are reproduced utilizing CloudSim to check for makespan. The reproduced outcomes demonstrate that improved max–min dependably offers less makespan contrasted with standard max–min and same or littler makespan as RASA calculation.

Tawfeek et al. [20] proposed another closed task scheduling algorithm dependent on ant colony optimization to minimize the makespan time for the given errand administration. This algorithm takes care of NP-hard problem, for example, voyaging sales rep issue, graph shading issue and vehicle routing algorithm. This calculation is reenacted utilizing CloudSim, and the makespan is evaluated for various errands with round-robin and FCFS calculation. The outcomes are acquired with the presumption that the errands are commonly free and not preemptive. The outcomes demonstrated that the ant colony algorithm works better as far as makespan time as contrasted and round-robin and FCFS.

Gupta and Garg [21] proposed a meta-heuristic methodology of ant colony optimization calculation to take care of the LB issue in distributed computing condition. It is intended to accomplish least makespan or execution time and better LB. The calculation is mimicked in CloudSim for ascertaining makespan time and burden adjusting level by shifting the quantity of undertakings and processors. Results contrast well and most famous calculations, for example, NSGA-II with the presumption that the errands are autonomous. The reproduction results demonstrate that the ACO calculation delivers less makespan time, and LB level contrasted with NSGA-II.

Shah et al. [22] proposed a algorithm that combines the concepts of opportunistic load balancing (OLB) and Load balance Min-Min (LBMM). This load scheduling algorithm achieves the advantages of both algorithms, namely, better executing efficiency, better utilization of resources and load balancing of the system.

Ru and Keung [23] proposed a scheduling calculation which is created with mix of undertaking gathering, prioritization of data transfer capacity mindfulness and shortest job first (SJF) calculation so as to lessen the processing time, waiting time, finish time (makespan) and overhead. In this calculation, the outstanding burdens are made utilizing Gaussian distribution, and resources are generated using random distribution. This work is mimicked in CloudSim condition, and the outcomes demonstrate that the calculation produces 30% improved outcomes for holding up time, preparing time and makespan alongside better use of assets with minimum overhead.

Agarwal and Jain [24] proposed a new generated priority algorithm working based on the priority of tasks. The priority of the tasks is defined based on the cloudlet size, memory, bandwidth scheduling policy, etc. Here, the authors compared time shared, space shared and a generalized priority algorithm. The above work simulated using CloudSim for various data centers, host VMs, scheduling and provisioning policies, and the results are compared with FCFS and round-robin.

Zheng and Zhang [25] proposed a streamlined water wave optimization algorithm dependent on three wave propelled administrators to be specific, propagation, refraction and breaking. The proposed improved WWO calculation disentangles the computation by overlooking the refraction administrator. It acquaints a populace estimate decrease with equalization the load better. They reason that the simplified WWO works better when contrasted with WWO as far as computations; however, they do not know whether simplified WWO can supplant WWO totally.

Ghanbari and Othman [26] proposed a priority-based job scheduling algorithm based on the theory of Analytical Hierarchy Process (AHP). T. Saaty has developed the AHP model based on a mathematical model combining multi-criteria decision making (MCDM) and multi-attribute decision making (MADM). The algorithm considers three levels of priorities such as Scheduling level (Objective level), Resources level (attribute level) and Job Level (alternative level). But this algorithm suffers from complexity, consistency and finish time.

Wang et al. [27] proposed a new job spanning time and load balancing genetic algorithm (JLGA) based on the original adaptive genetic algorithm. It considers the new characteristic of cloud computing to improve the performance. This algorithm initializes the population and describes the load existing among nodes and weight multi-fitness function. The simulation is done for comparing the performance of AGA and JLGA with no priorities among jobs. The results prove that JLGA works better in both total tasks and average task consuming of jobs, and it balances the load among the systems.

Dubey et al. [28] proposed a new modified Heterogeneous Earliest Finish Time (HEFT) algorithm to overcome the drawback of inefficient task distribution by HEFT algorithm. Their algorithm distributes the workload between different resources in an effective way to reduce the makespan. The algorithm works in two different phases. In the first phase, the nodes are assigned with a weight, and communication costs between the nodes are setup. Then rank is calculated for every task in DAG traveling from the last node toward the root node. In second phase, the task will be effectively assigned to available resources based on results obtained from the first phase. The results of the simulations show that the modified HEFT produces less makespan time as compared to HEFT and CPOP algorithm.

3 Conclusion

There are different alternatives accessible for giving resource scheduling in cloud computing condition. The researchers, as talked above, have not executed or mimicked their calculations for comparative situations, in the sense, the quantity of servers and their capacities and furthermore the quantity of clients utilizing the cloud and the assignments that they are performing are not indistinguishable. Each methodology might be reasonable for one circumstance. In this way, there cannot be a straightforward measuring stick to quantify the exhibitions of various mists on various angles. The specialist co-op must think about all angles and introduce a heap adjusting calculations that may best suit the individual prerequisites as far as CPU use, memory utilization and every other parameter, for example, makespan, throughput and so forth.

References

1. Rajput SS, kushwah VS (2016) A review on various load balancing algorithms in cloud computing. Int J Adv Res Comput Sci Soft Eng 6(4). ISSN: 2277 128x
2. Aslam S, Shah MA (2015) Load balancing algorithms in cloud computing: a survey of modern techniques. NSEC, IEEE
3. Nitika M, Shaveta M, Raj MG (2012) Comparative analysis of load balancing algorithms in cloud computing. Int J Eng Sci 1(1)

4. Samal P, Mishra P (2013) Analysis of variants in round robin algorithms for load balancing in cloud computing. Int J Comput Sci Inf Technol 4(3):416–419. ISSN: 0975-9646
5. Zhang D, Jiang C, Li S (2009) A fast adaptive load balancing method for parallel particle-based simulations. Simul Model Pract Theory 17:1032–1042
6. Dhinesh Babu LD, VenkataKrishna P (2013) Honey bee behavior inspired load balancing of tasks in cloud computing environments. Appl Soft Comput 13:2292–2303
7. Chandrakanta K, Piyush G (2015) A novel honey bee inspired algorithm for dynamic load balancing in cloud environment. Int J Adv Res Electr Electron Instrum Eng 4(8)
8. Dong B, Li X, Qimeng W, Xiao L, Ruan L (2012) A dynamic and adaptive load balancing strategy for parallel file system with large-scale I/O servers. J Parallel Distrib Comput 72:1254–1268
9. Deng Y, Lau RWH (2010) Heat diffusion based dynamic load balancing for distributed virtual environments. In: Proceedings of the 17th ACM symposium on virtual reality software and technology, ACM, pp 203–210
10. Esch M, Tobias E (2010) Decentralized scale-free network construction and load balancing in massive multiuser virtual environments. In: Collaborative computing networking, applications and work sharing, collaborate com, 6th international conference on IEEE, pp 1–10
11. Godfrey B, Lakshminarayanan K, Surana S, Karp R, Stoica I (2004) Load balancing in dynamic structured P2P systems. In: INFOCOM 2004, twenty-third annual joint conference of the IEEE computer and communications societies, vol 4. IEEE, pp 2253–2262
12. Kokilavani T (2011) Load balanced min-min algorithm for static meta-task scheduling in grid computing. Int J Comput Appl (0975–8887) 20(2)
13. Chen H, Wang F, Helian N, Akanmu G (2013) User-priority guided min-min scheduling algorithm for load balancing in cloud computing. In: National conference on parallel computing technologies, pp 1–8
14. Anandharajan TRV, Bhagyaveni MA (2011) Co-operative scheduled energy aware load-balancing technique for an efficient computational cloud. Int J Comput Sci Issues (IJCSI) 8(2)
15. Chauhan SS, Joshi RC, A weighted mean time min-min max-min selective scheduling strategy for independent tasks on grid. Electronics and Computer Engineering Department, Indian Institute of Technology Roorkee-247667, India
16. Bhoi U, Ramanuj PN (2013) Enhanced max-min task scheduling algorithm in cloud computing. Int J Appl Innov Eng Manag (IJAIEM) 2(4). ISSN No: 2319-4847
17. Li X, Mao Y, Xiao X, Zhuang Y (2014) An improved max-min task-scheduling algorithm for elastic cloud. In: International symposium on computer, consumer and control
18. Konjaang JK, Ayob FH, Muhammed A (2017) An optimized max-min scheduling algorithm in cloud computing. J Theor Appl Inf Technol 95(9). ISSN: 1992-8645
19. Elzeki OM, Reshad MZ, Elsoud MA (2012) Improved max-min algorithm in cloud computing. Int J Comput Appl (0975–8887) 50(12)
20. Tawfeek MA, El-Sisi A, Keshk AE, Torkey FA (2015) Cloud task scheduling based on ant colony optimization. Int Arab J Inf Technol 12(2)
21. Gupta A, Garg R (2017) Load balancing based task scheduling with ACO in cloud computing. In: International conference on computer and applications IEEE transactions
22. Shah R, Veeravalli B, Misra M (2007) On the design of adaptive and decentralized load-balancing algorithms with load estimation for computational grid environments. IEEE Trans Parallel Distrib Sys 18(12)
23. Ru J, Keung J (2013) An empirical investigation on the simulation of priority and shortest job first scheduling for cloud-based software systems. In: 22nd Australian conference on software engineering
24. Agarwal A, Jain S (2014) Efficient optimal algorithm of task scheduling in cloud computing environment. Int J Comput Trends Technol 9
25. Zheng Y-J, Zhang B (2015) A simplified water wave optimization algorithm. Evolutionary computation (CEC), IEEExplore.ieee.org

26. Ghanbari S, Othman M (2012) A priority based job scheduling algorithm in cloud computing. In: International conference on advances science contemporary engineering, pp 778–785
27. Wang T, Liu Z, Chen Y, Xu Y (2014) Load balancing task scheduling based on genetic algorithm in cloud computing. In: International conference on dependable, autonomic and secure computing 978-1-4799-5079-9/14, IEEE transactions
28. Dubey K, kumar M, Sharma SC (2017) Modified HEFT algorithm for task scheduling in cloud environment. In: 6th international conference on smart computing and communications ICSCC, Elsevier

Cloud-Based Healthcare Portal in Virtual Private Cloud

R. Mahaveerakannan, C. Suresh Gnana Dhas and R. Rama Devi

Abstract Healthcare system providing cloud-based storage makes possible to store the patient's therapeutic records to the remote server than keeping the files and radiological images on a hard drive or local storage device which enables the patient to access their medical records at any place from the Internet through a web-based application. The structure of cloud application guarantees the privacy and security of health-related data to preserve the sensitive health information. The architectural design of cloud computing is to alleviate the privacy concern and to fulfill the confidence and trust of the cloud-based healthcare organization. This work proposes a structure for a cloud-based healthcare system to allow patients get to their medical images and reports from the cloud, ensuring that the data are available when it meets the prerequisite of a particular contract that is authorized. The requirements, architecture design, software components, and validation methods of cloud-based healthcare system are introduced.

Keywords Healthcare system · Public cloud · VPC · VPN · NAT · Client system

1 Introduction

The organization requires different types of software and hardware to run. They need a different expert to maintain the software and hardware [1]. These are the challenging task before cloud computing. After cloud computing, an organization can get rid of those problems. If the organization has not had enough resources

R. Mahaveerakannan (✉)
Information Technology St. Peter's University, Chennai, India
e-mail: mahaveerakannan10@gmail.com

C. Suresh Gnana Dhas
Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai, India
e-mail: sureshc.me@gmail.com

R. Rama Devi
Janson Institute of Technology, Coimbatore, India
e-mail: ramarengaraju@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_103

to invest in infrastructure and platforms to deploy their applications, they can take advantage of the cloud services to suit their specific needs. Since the cloud provides a scalable infrastructure to handle the load effectively, the organization can pay for what they used based on a pay-as-you-go model. Since they can deploy and run the different application in the cloud, they do not have to buy and maintain the infrastructure like hardware, software, networking, security, firewall, etc. The cloud service provider should product their data from the negative impact on business. So, the cloud service provider provides a high level of services as the expectation of the organization. Google and Microsoft provide web-based email service. The emails are stored in a Google server and Microsoft server instead of storing in a client computer. Microsoft also offers a web-based office online app, web-based apps, social networking sites, and media services. Healthcare sensitive data must be treated with high-level security of current legislation [2]. This work encompasses to preserve the privacy and technical requirement of the healthcare data to allow ubiquitous and secure access in the cloud environment and highlight the threats to the health data in the cloud and present the requirements to be fulfilled to mitigate the threats [3]. Public cloud computing provides the virtual private cloud (VPC) which allows the organization to isolate their cloud instance from other organizations in order to meet the security issues and provides great control over the cloud environment, and also, it creates a hardware virtual private network (VPN) to connect the own data centers with public cloud.

2 Requirements

Cloud-based healthcare system should maintain the security and privacy of data within the organization in order to protect the sensitive data.

The cryptographic and non-cryptographic methods are used to preserve the privacy and security concerns [4]. The taxonomy of security and privacy requirements [5] is shown in Fig. 1.

2.1 Confidentiality

The sensitive healthcare data are not only protected from cloud service provider but also protected from unauthorized insiders.

2.2 Integrity

The health care data should not be modified through any illegal action of authorized or unauthorized persons. Identifying attributes such as name, date of birth, and address

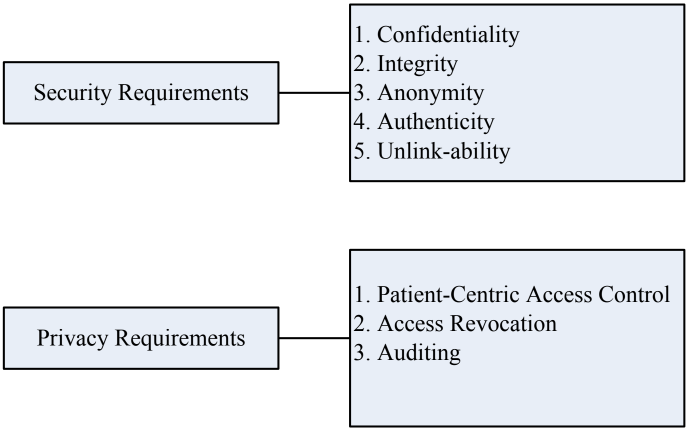


Fig. 1 Security and privacy requirements

are encrypted with cryptographic method and access control mechanism enforced on the attribute of healthcare data file stored in the cloud.

2.3 Collision Resistance

Collision resistance mechanisms provide resistance among unauthorized users or authorized users to prevent the illegitimate actions among authorized or unauthorized users. It ensures the privacy of health data not only from the unauthorized users, but also from the authorized users.

2.4 Anonymity

The methodology of pseudonyms is identifiers that are used to identify the data owner instead of real name. The methodology is used to prevent the revealing of the data owners' identities such as name, security number form CSP, authorized, and unauthorized users.

2.5 Authenticity

Develop the robust public-key infrastructure through message encryption and digital signature and provide the valid authentication code and keys that should only grant the users access their health-related data.

2.6 Unlink-Ability

Maintain the unlink-ability between patient identifiers and their health-related data to protect the patient's privacy. Develop the policy to request query to classify whether the query is malicious or legitimate.

2.7 Patient-Centric Access control

Patients can encrypt their personal health data before storing at the cloud. Users are permitted to access the patient's data based on role, such as doctor, nurse, and insurance broker and based on access control such as read, write, and print.

2.8 Access Revocation

Since the patients can able to revoke the access rights to different entities over the health information, other users should not be able to access the health information.

2.9 Auditing

Auditing of healthcare data ensures that manipulation activities of patients' record are monitored by either themselves or another role nominated by a patient.

2.10 Architecture Design

2.10.1 Healthcare System (HCS) in the Public Cloud Service

The following architecture is proposed in the figure. It comprises the three systems:

1. The health care system (server)
2. Amazon web service (public cloud)
3. Client system (authorized clients).

The public cloud supports sensitive data of different departments in HCS. The client application is running under the HTTP and interacts with HCS. The architecture of HCS in public cloud is shown in Fig. 2.

HCS can create the different application, web services, and database storage in elastic cloud computing (EC2) instance in the public cloud. Moreover, other organization can create the instance in the EC2 server in the public cloud, and the instances

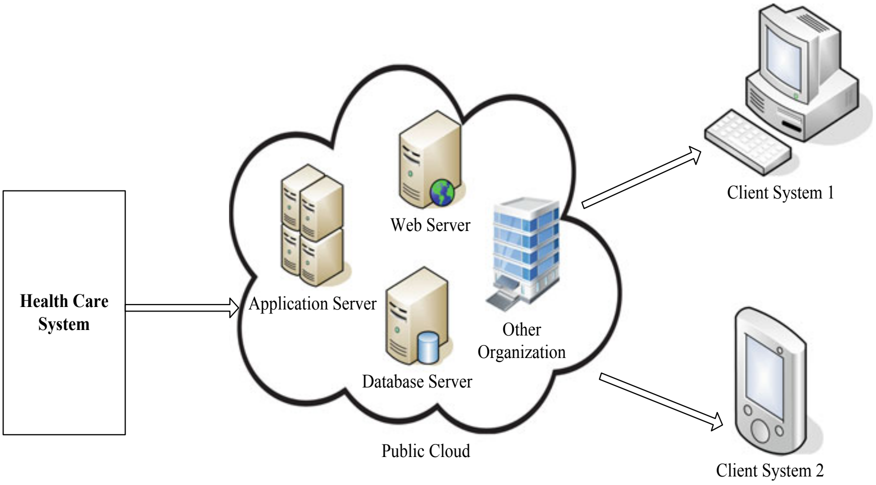


Fig. 2 Healthcare system in flat network

are shared by flat network. Since no organization has own network or own IP address, it is not possible to prevent the others to try to get accessing own instance in the cloud. Anyone can directly launch EC2 anywhere in the cloud. Each instance can be directly accessed by public IP address and based on access control mechanism, so each entity should be individually managed. Since the hackers are easier to intercept data on the flat network, it is creating network security issues on the network [5].

2.11 Proposed Architecture

2.11.1 Healthcare System (HCS) in Virtual Private Cloud (VPC)

The work introduces the virtual private cloud (VPC) in the public cloud to allocate the part in the public cloud. So, the existing network and VPC become as a single network. The own defined virtual network allows the organization to control the network environment. When the existing customer gateway (CG) in HCS is connected to virtual private gateway (VPG) in VPC using VPN or direct connect to establish the VPN connection, it allows internal system (IS) in HCS to connect to the VPC through the private IP address without the Internet or public IP address. It can also allow VPC peering in different region in public cloud that can connect the multiple VPC within public cloud to talk with each other without the Internet or direct connect which is shown in Fig. 3.

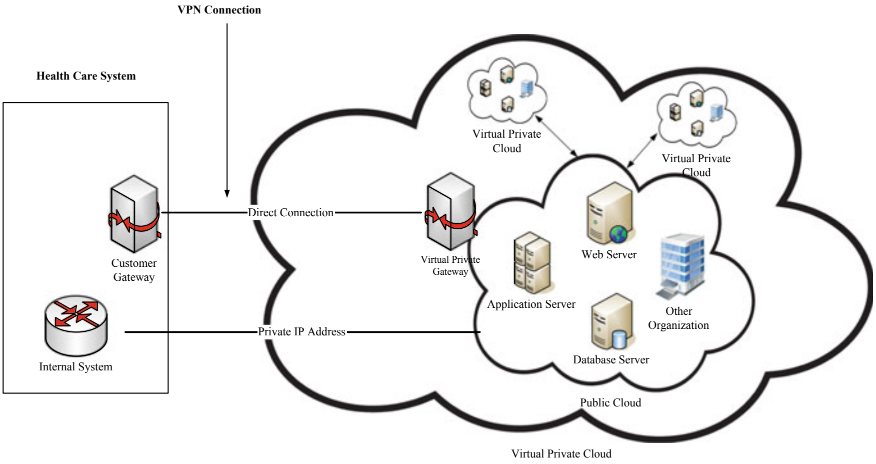


Fig. 3 Virtual private cloud for security

3 Establish Flexibility of Access in VPC

HCS has different server, such as application server, web server, and database server. It can improve the security in the EC2 instance and in public cloud by providing appropriate access control to a different server, and each server can be individually controlled by providing appropriate subnet, for example, connect the Internet gateway (IGW) to the web server to establish the external access to the web server [6]. The database server and application server are protected from external server. The large network is segmented by subnet to provide public and private subnet to increase flexibility of access. Customer gateway in HCS can connect privately with private IP address into the VPC in public cloud through virtual private gateway (VPG) without using the Internet gateway. It can protect the sensitive data by providing private IP address if it properly secures the network, which is shown in Fig. 4.

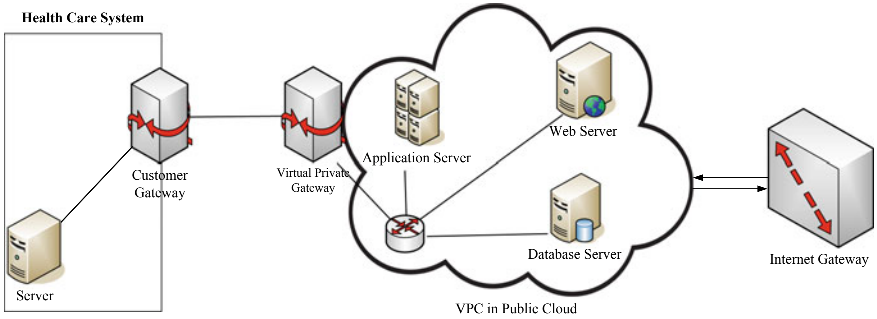


Fig. 4 Create private cloud for healthcare system

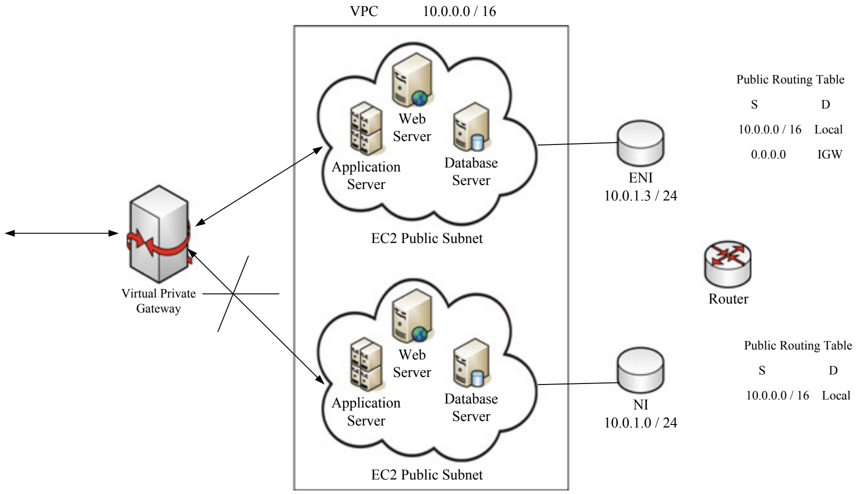


Fig. 5 Public and private subnet for servers

3.1 Create the Public and Private Subnet for VPC IP Address 10.0.0.0/16

RFC 1918 standard of IP Range: 10.0.0.0/16
Availability Zone1
Public subnet1A: 10.0.1.0/24 for web servers
Private subnet1B: 10.0.2.0/24 for database servers.

Access control lists (ACL) act as a firewall for controlling the traffic into and out of the subnet [7]. All web servers are managed in public subnet to allow inbound and outbound access. The public subnet 10.0.1.3/24 wants to communicate to the private subnet 10.0.3.48/24 which sends the request to the router to search for the routing information. It checks the destination IP address is local to the VPC that communicate locally; otherwise, it communicates through the Internet gateway [8]. Since public routing table is associated with the public subnet, it can possibly communicate both locally and outside. All the database servers have managed in the private subnet to prevent the inbound and outbound access [9]. Since private routing table is associated with private subnet, it has the only possibility to communicate local subnet which is shown in Fig. 5.

3.2 Network Address Translation (NAT)

Proposed works introduced network address translation (NAT) gateway which is used instead of developing software to perform IP filtering and intrusion detection

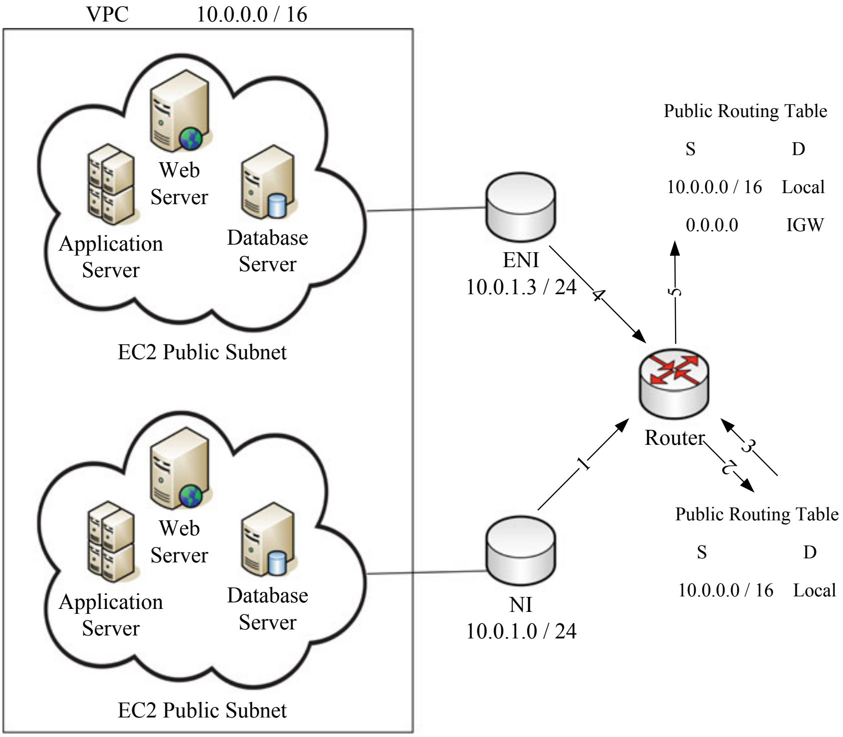


Fig. 6 Secured database server with NAT gateway

and prevention (IDP) to enable connection in the private subnet to the Internet or other services in public cloud and also block the inbound public access through the Internet [10]. For example, private subnet can communicate with the external IP address 52.19.1.4 through a NAT gateway which is shown in Fig. 6.

1. Database server wants to communicate with external IP address 52.19.1.4, and it sends the request to router.
2. Router search in the private routing table.
3. Get the NAT gateway.
4. NAT gateway connects the router.
5. Communicate with external IP address through IGW.

The healthcare system's web server can handle the patients' request and delivers the medical information anywhere through the NAT gateway with the corresponding security policy of authorization and authentication [11]. Then, it is responsible for information is wrapped with their authentication keys for converting the data into an encrypted object under the security and privacy requirements [12].

Table 1 Evaluations parameter

Goal	Metric
Patient can access medical images and reports	Patients name, identification number, and number of tries
Patient's privacy protected	VPC, access control list
Patient's data protected	Private subnet

4 Evaluations Framework

The goal of evaluations parameter of patient's authentication and privacy requirements is given in Table 1.

5 Conclusion and Proposed Work

The healthcare system keeps up and protects the health-related data in VPC architecture. They can keep the advantages of public cloud with respect to flexibility, scalability, elasticity, performance, availability, and the pay-as-you-use pricing model for both small- and large-scale health organizations. The healthcare sensitive data in VPC are intended to meet the prerequisite of security, privacy, and confidentiality. The future work is to extend to the analysis of cryptographic solutions along with a digital signature and build up the robust methodologies of SSH-based layered encryption approach to ensure the integrity for transferring data from one point to another. The cloud-based healthcare system can gain the overall acceptance by providing strong security mechanisms to protect the patients' records.

References

1. Abbas, Khan SU (2014) A review on the state-of-the-art privacy preserving approaches in e-health clouds. IEEE J Biomed Health Inf 18(4):1431–1441
2. Jacob A (2009) Infrastructure in the cloud era. In: Proceedings at international O'Reilly conference velocity
3. Zhang R, Liu L (2010) Security models and requirements for healthcare application clouds. In: 3rd IEEE international conference on cloud computing, Miami, FL, pp 268–275
4. Li J (2013) Electronic personal health records and the question of privacy. Computers. https://doi.org/10.1109/MC.2013.225
5. Leng C, Yu H, Wang J, Huang J (2013) Securing personal health records in the cloud by enforcing sticky policies. TELKOMNIKA Indones J Electr Eng 11(4):2200–2208
6. Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl 34(1):1–11
7. Metri P, Sarote G (2011) Privacy issues and challenges in cloud computing. Int J Adv Eng Sci Technol 5(1):001–006

8. Li ZR, Chang EC, Huang KH, Lai F (2011) A secure electronic medical record sharing mechanism in the cloud computing platform. In: 15th IEEE international symposium on consumer electronics (ISCE 2011), pp 98–103
9. Ramgovind S, Eloff MM, Smith E (2010) The management of security in cloud computing. In: Information security for South Africa (ISSA), IEEE, pp 1–7
10. Fabian B, Ermakova T, Junghanns P (2015) Collaborative and secure sharing of healthcare data in multi-clouds. Inf Sys 48:132–150
11. Google Online Documentation (2009) Google's approach to IT security. Google White Paper. Winkler V (2011) Securing the cloud computer security techniques and tactics. Elsevier. ISBN: 978-1-59749-592-9
12. Balaram A, Pushpa S (2018) Sybil attack resistant location privacy in VANET. Int J Inf Commun Technol 13(4)

A Hybrid Approach for Video Steganography by Stretching the Secret Data

B. Karthikeyan, M. M. Anishin Raj, D. Yuvaraj and K. Joseph Abraham Sundar

Abstract In this Internet era, the digital communication is unavoidable, and its contribution to the development is significant. Due to the enormous data communication, there is always a question about the security of the data. In this paper, a hybrid reversible data hiding method is proposed to transmit the data in secure manner through video files. Secret data like one-time password (OTP) can be embedded into one of the frames in the video. This achieves more security than the regular ways. The proposed method has compared with mean square error (MSE) and peak signal-noise ratio (PSNR).

Keywords Steganography · Video · Stretching · Least significant bit (LSB) · Video frames

1 Introduction

Steganography is a technique used to hide the data, and in this technique, a steganographic model is represented which uses cover video files to obscure the existence of other subtle data without considering their format [1–4]. In this technique, the secret message is divided into blocks before being embedded into the cover image. In this paper [5], the four models of secret data which are quantitatively evaluated are proposed. This scheme can be used in both spatial and frequency domain streams. In this technique, the technique the encoding capacity is high as compared to the

B. Karthikeyan (✉) · K. Joseph Abraham Sundar
Computer Vision & Soft Computing Lab, School of Computing, SASTRA Deemed University, Thanjavur, India
e-mail: mbalakarthi@gmail.com

M. M. A. Raj
Department of CSE, Viswajyothi College of Engineering & Technology, Vazhakulam, Kerala, India

D. Yuvaraj
Department of CSE, Chian University, Cihan University, Duhok, Kurdistan Region, Iraq

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_104

other techniques. The key data, transform domain and the number LSB bits encoded must be known for the hackers to extract a data from the cover file in this proposed scheme.

2 Related Works

Steganography is a process which involves hiding the data inside a cover data in order to protect it from illegal access. The basic discrete cosine transform (DCT) and discrete wavelet transform (DWT) are applied on the multiple object tracking (MOT) algorithm, and error-correcting codes are implemented for a secure and robust method for video steganography. In this proposed system, first the secret message is encrypted and then encoded using Hamming code and BCH codes, and later, it is embedded into the DCT coefficients of the video frames. In this, proposed algorithm is three-fold, specified as the option-based MOT algorithm, data embedding and the data extraction. In this technique, a better way for the visual quality is achieved compared to the other steganographic techniques used for video steganography. This method improves the security in multimedia field and makes it undetectable. The proposed algorithm provides privacy and protects it from various illegal accesses. By applying both MOT and error-correcting codes (ECC), it improves the privacy of the data [6].

This is a paper which presents a method of motion vector-based video steganography. In this improved technique of video steganography, the modification is made on the LSB. The motion estimation method searches the least MV value. Experimental techniques are performed on the illegally accessed videos, and by different steganographic methods, the values are converted into bit rates and video codes [7].

This paper discusses about illegal attacks against the governmental agencies are focused. Video compression on standard H.264/AVC, an algorithm is implemented on secret sharing and the error-correcting codes. Discrete cosine transform (DCT) blocks are chosen by grey relational analysis along with a partition mode in video compression standard H.264/AVC. First and foremost, the secret information is processed by the technique called secret sharing, and later on, ECC technique is used to process the obtained information. We choose the DCT blocks using GRA, and later rules are used to hide the pretreated information to DCT coefficients form of the video frames. This implemented algorithm provides robustness and invisibility as compared to other steganographic techniques. This reduces the attacks and the PSNR ratios. Videos have a very great capacity of hiding information, and in this technique, symmetric blocks have been used which increases the capacity to hide the information secretly and in a large amount [8].

In this paper [9], hiding of data in an efficient method is being discussed. Here, the data is hidden in such a way that the data is hidden in a tricky way. Patch-Wise Code Formation (PCF) is used for secure video transformation. The main purpose of this technique is to transfer the data efficiently and to maintain the secrecy of the data which is to be transmitted. This method reduces the time complexity and increases the security as compared to other methods. In this paper, a technique is proposed to hide the existence of the message so that it becomes hard for the attacker to notice it. In Patch-Wise Code Formation method, the entire video is divided into patches. In this method, the numbers of bits are reduced and increase the security as compared to other methods.

Steganography is the method of hiding secret data. In this, proposed system of video steganography method using spiral LSB and factorization methods is used. Factorization of the cover frames of cover video files is done. Later, the secret file is embedded into the scramble of the cover frames. This is done using spiral LSB techniques. As compared to the other methods, this method is quite efficient and is undetectable to the attackers. By applying prime factorization method on the cover frames, scrambling and descrambling are done, respectively. This method is much more efficient and provides more security and robustness, and PSNR technique is used to measure the quality of steganography [10].

A 2D chaotic map is used for shuffling the pixel positions, and in this technique, it is based on nonlinear feedback shift register and Tinkerbell chaotic maps. Using the technique of chaotic map and NLFSR, a video steganography mechanism is developed in which the data is hidden into segregated frames by embedding them. Unlike other hiding techniques, in this technique, the hiding limit is exponential. In Internet and the mobile system video-based steganography, the files are in video formats. It is hard to get the encoding position if the initial value of the chaotic map is not known. For the security factors of the steganographic data, it is aimed that the improved LSB is good for steganography [11].

In paper [12], the author discusses about how data is hidden in compressed videos. This improves the security of the motion vector-based steganography with the presently available steganographic techniques. A syndrome-trellis code is used to minimize the overall embedding impact. In this proposed scheme, it provides higher security and the smaller level of the impact on coding as compared to the other video steganographic methods. The entire embedding effect is reduced by using the syndrome-trellis code, thereby increasing the security and privacy [12].

3 Design Methodology

Sample video file is converted into number of frames. Randomly, two frames have been chosen out of the n-1 frames, i.e. except the first frame. The first frame is used to store the metadata like frame number and length of the secret data. The metadata can be stored in some other frames also. Figure 1 shows the overall procedure for the entire scheme.

After selection of two frames, the secret data is expanded [13] which introduces more complexity for the intruder. The secret data can be expanded in many ways, but it should be well suited for decoding procedure to get back the secret data. The first character of secret data is taken, and it is divided by 256. The remainder is stored in the first pixel of cover image 1, and the remainder is stored in the first pixel of cover

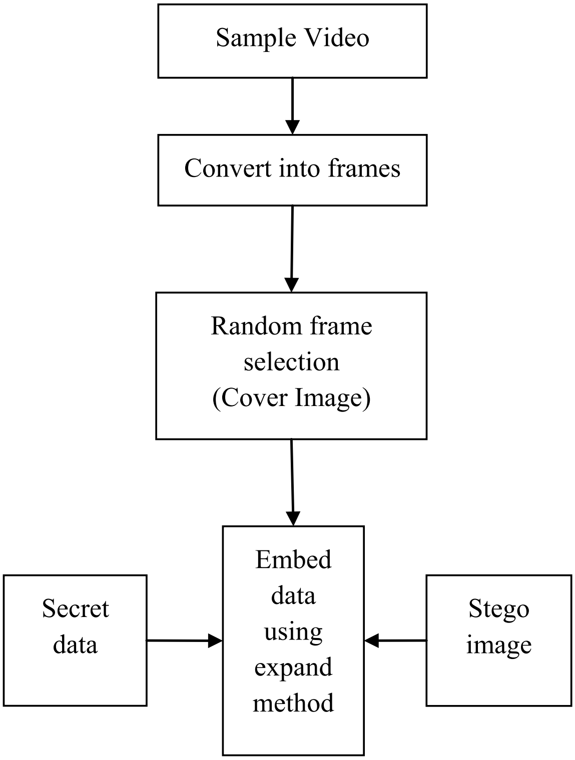

Sample Video
Convert into frames
Random frame selection (Cover Image)
Secret data
Embed data using expand method
Stego image

Fig. 1 Data embedding procedure

image 2. The secret data is embedded in the cover images by using least significant bit (LSB) substitution method. This repeated for all the characters in the secret data. Since all the steps are reversible, the secret data is extracted from the cover images with the help of first frame, i.e. metadata. The decoding procedure is shown in Fig. 2.

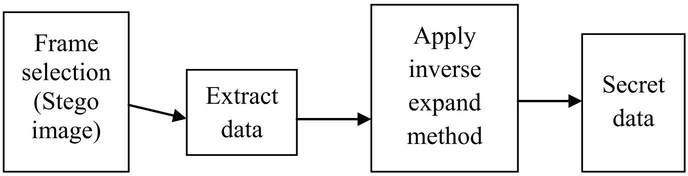


Fig. 2 Decoding procedure

4 Results and Discussion

Proposed method has been tested with number of images with various size of secret text. The sample results are shown in Fig. 3.

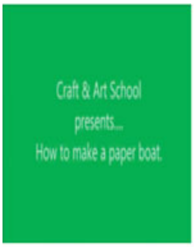
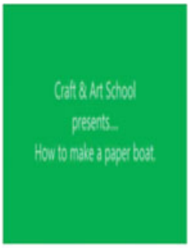
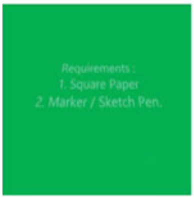
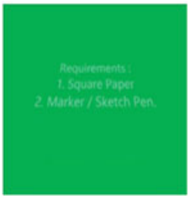
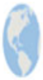
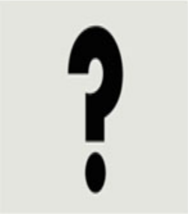
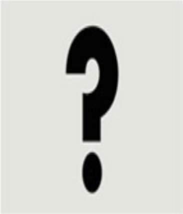
Size of Secret Text	Cover Image	Stego Image
50	 Craft & Art School presents... How to make a paper boat.	 Craft & Art School presents... How to make a paper boat.
50	 Requirements : 1. Square Paper 2. Marker / Sketch Pen.	 Requirements : 1. Square Paper 2. Marker / Sketch Pen.
100		
100		

Fig. 3 Sample cover and stego images taken from video clip

Table 1 Performance comparison for sample images

Size of text	MSE	PSNR
50	0.0018	173.8668
50	0.0008	181.7260
100	0.0083	158.7158
100	0.0013	177.2854

The proposed work achieves not only high-level complexity in embedding the text but also better results in mean square error (MSE) and peak signal- to- noise ratio (PSNR). The results are tabulated in Table 1.

5 Conclusion

The stretching concept proposed in this paper increases the security of the data to be embedded. If the intruder wants to know the secret data which is embedded in the cover image, then they are supposed to know the stretching procedure and the key frames. Because of this, the proposed work on video-based steganography achieves better security than other techniques. Experimental result shows a better accuracy.

References

1. Sriram S, Karthikeyan B, Vaithiyanathan V, Raj MMA (2015) An approach of cryptography and steganography using rotor cipher for secure transmission. In: 2015 IEEE international conference on computational intelligence and computing research, ICCIC 2015, 17 Mar 2016, Article number 7435669
2. Karthikeyan B, Ramakrishnan S, Vaithiyanathan V, Sruti S, Gomathymeenakshi M (2014) An improved steganographic technique using LSB replacement on a scanned path image. Inter J Netw Secur 16(1):14–18
3. Charan GS, Kumar SSVN, Vaithiyanathan V, Lakshmi D, Karthikeyan B (2015) A novel LSB based image steganography with multi-level encryption. In: ICIIECS 2014–2015, IEEE international conference on innovations in information, embedded and communication systems, 12 Aug 2015, Article number 7192867
4. SSVN Kumar, Charan GS, Karthikeyan B, Vaithiyanathan V, Reddy MR (2016) A hybrid approach for data hiding through chaos theory and reversible integer mapping. In: International conference on computational intelligence, cyber security and computational models, ICC3 2015, vol 412. Coimbatore, pp 483–492
5. Hanafy AA, Salama GI, Mohasseb YZ (2008) A secure covert communication model based on video steganography. In: IEEE military communications conference, San Diego
6. Mstafa RJ, Elleithy KM, Abdelfattah E (2017) A robust and secure video steganography method in DWT-DCT domains based on multiple object tracking and ECC. IEEE Access 5:5354–5365
7. Wang K, Zhao H, Wang H (2014) Video steganalysis against motion vector-based steganography by adding or subtracting one motion vector value. IEEE Trans Inf Forensics Secur 9(5):741–751

8. Zhang Y, Zhang M, Yang X, Liu L, Guo D (2017) Novel video steganography algorithm based on secret sharing and error-correcting code for H.264/AVC. Tsinghua Sci Technol 22(2):198–209
9. Rajalakshmi K, Mahesh K (2017) Video steganography based on embedding the video using PCF technique. In: International conference on information, communication and embedded systems
10. Jha VK, Roy S, Mukherjee S, Sanyal G (2017) Video Steganography technique using factorization and spiral LSB methods. In: International conference on computer, communications and electronics
11. Kar N, Aman MAA, Mandal K, Bhattacharya B (2017) Chaos-based video steganography. In: 8th international conference on information technology
12. Cao Y, Zhang H, Zhao X, Haibo Y (2015) Covert communication by compressed videos exploiting the uncertainty of motion estimation. IEEE Commun Lett 19(2):203–206
13. Karthikeyan B, Sameer SZ, Srinath P, Raj MMA, Vaithiyanathan V (2017) A novel stretching approach for multiple image steganography using bit stuffing. In: International conference on communication and Security

An Acknowledgment-Based Approach for Implementing Trusted Routing Protocol in MANET

K. Dhanya, C. Jeyalakshmi and A. Balakumar

Abstract Security and dependable transmission is testing errand in portable ad hoc system along the portability of system gadget bargained with assault and loss of information. For the aversion of assault and dependable transmission, different creators proposed a technique for verified directing convention, for example, SAODV and SBRP (secured backup routing protocol). The procedure of these strategies works alongside route disclosure and route maintenance, inventing, and route prolong kept up required more power utilization for that procedure. For the verification of gathering hub, gathering mark procedure is utilized, and rest mode edge idea is utilized for power minimization. Our proposed strategy is reenacted in ns-2 and contrast with other directing convention gives a superior act in contrast with vitality utilization and throughput of system. There are various approaches to compute trust for a node such as fuzzy trust approach, trust administration approach, and hybrid approach. Adaptive information dissemination (AID) is a mechanism which ensures the packets in a specific transmission, and it analyzes if there are any attacks by hackers. It encompasses of ensuring the packet count and route detection between source and destination with trusted path. Trust calculation based on the particular condition or context of a node, by sharing the context data onto the other nodes in the system would give a better solution to this problem. Here, we present a review on different trust association approaches in MANETs. We bring out immediate response from the methodologies for building up trust of the taking part hubs in a dynamic and unsure MANET atmosphere.

Keywords Internet of things · Mobile ad hoc network · Trust management approach · Adaptive information dissemination · Route discovery · Attacker · Data transmission

K. Dhanya (✉) · C. Jeyalakshmi · A. Balakumar
K. Ramakrishnan College of Engineering, Trichy, India
e-mail: dhanyaeece2506@gmail.com

C. Jeyalakshmi
e-mail: lakshmikrce.2016@gmail.com

A. Balakumar
e-mail: balakumar2712@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_105

1 Introduction

Remote sensor networks (WSNs) and wireless sensor and actuator networks (WSANs) both assume a key job in the work of Internet of things (IoT) frameworks since they portray the association between the present computational frameworks and the physical world. In a WSAN, the two sensors and actuator control the physical area with amounts, for example, temperature, weight, sound dimension, and light force being continuously estimated by gadgets associated with either a WSN or a WSAN. Estimated information are sent by remote transportations to handling gadgets for investigation, and the essential control information are passed on back to WSAN-associated actuators. Both WSNs and WSANs are utilized in a countless of utilization spaces including environmental checking and area/following, basic assembling applications, shrewd networks, and medicinal services. WSN and WSAN transportations for the most part include multi-jump which commands directing usefulness of all related gadgets that are not end framework hubs.

To fabricate, trust association relies upon some factor setting, conduct, and understandings. It is all the more difficult to figure precisely. So, enhancement can be capable by considering those setting mindful measurements which measure MANET execution. Setting mindful measurements could incorporate versatility mindfulness, vitality mindfulness, control mindfulness, accessibility, difference mindfulness, and clog cognizance. Counting such measurements in the created conventions should propel MANET execution.

2 Existing System

So as to exploit the trust in neighbour hubs, keen enemies may profess to be generous hubs by encouraging bundles preceding propelling parcel dropping assaults. Be that as it may, course of action number assaults propelled by parcel lessening foes may create explicit sort of examples in manufacturing some field esteems (e.g., grouping number and jump tally), in the control bundles amid course disclosure process. A trust-based plan (TRS-PD) embraces an example revelation instrument [1] to break down the set down system esteems to caught/got the command bundles. The system principles are set down in two gliding windows: (i) the main gliding window (GL1) set down end hub's character, recent time, jump tally, and finally, goal plan count and (ii) the second gliding window (GL2) set down goal hub's personality and recent time, then alteration among the end arrangement quantities around the got answer parcel and accommodating solicitation bundle.

A calculation tolerating the [2] representation technique of same distinction investigates [3] the set down information and then yields in case the connecting hub pursues the assault design [4–6]. Course revelation procedure can upheld through the instrument insolating the boycotted opponent who can dispatch bundle falling on assaults (Fig. 1).

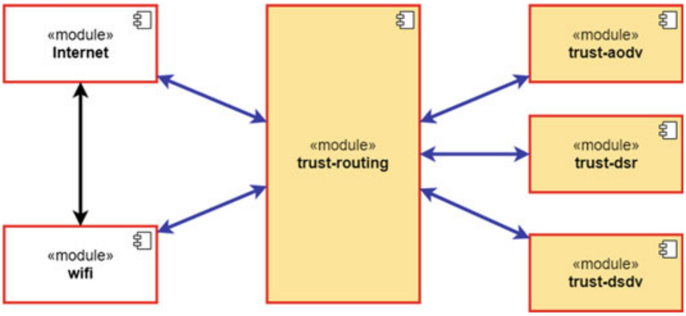


Fig. 1 Block diagram for routing proposal

2.1 Drawbacks

- While enemy's consequent certain assault examples may get saw byte theme disclosure instrument, the other bundle dropping foes (which do not pursue any example) are recognized by the trust display.
- Nonetheless, such hub repossession its trust is expelled from the boycott later on the off chance that it doesn't pursue assault designs and believed neighbors have additionally not recommended it as a questioned hub.

3 Proposed System

A proposal filtering component is used to adequately screen out false honors even in amazingly threatening surroundings in which the larger part recommenders are noxious. It utilizes hub to-undertaking task MANET accommodation with multi-target improvement (MOO) necessities. Versatile information dissemination (AID) is a system which guarantees the compartments in a specific communicate, and it investigates if there are any assaults by programmers. It involves shielding the bundle check and course revelation among source and endpoint with confided in way, with the goal that the parcel plunging proportion is decreased and conveyance rate of bundles is expanded. It likewise gives the safe information communicate through IOT with MANET condition.

3.1 Trust Models

The accompanying tributes for secure IOT steering convention configuration have been proposed in [7]:

- Secure course development [8].
- Self-adjustment [9].
- Effective pernicious hub ID framework.
- Lightweight computations [9].
- Location protection.

4 Proposed Algorithm for Information Routing

On making trust perceptive course assurance plans, we acknowledge the WSN can be an outline with vertices specialist indicator center points along outskirts addressing affirmation interfaces along pinnacle. Charts are sensible portrayal to delineate composite frameworks, for instance, WSN. The hugeness on a vertex implies extra essentialness of that center point, and the weight on an edge exhibits the measure of imperativeness that a center requires to transmit a unit of information along the edge [10]. The lingering vitality in a course is characterized as the most minimal vitality dimension of any hub on the course.

4.1 Distributed Trust Evaluations

Conveyed trust appraisal can be delegated: neighbor detecting (direct trust), proposals-based trust, and half-and-half technique. In appropriated impromptu systems, trust levels are contrived from the examination of gathered information from perceptions for explicit activities. It could log that a particular node forwards some packages as normal and then drops other packets. It could receive this through direct neighbor sensing and calculate trust from direct knowledge.

- The node state is initialized.
- The value is set 0 for initial selection.
- Ascertain the intensity of vitality of chose hub for demand as $P = \sum, + 1$. Here, the gathering of hub is $M-1$, and hub determination is 0 to M. In the event that power of hub is least Pi, at that point, gathering of enactment is chosen.
- The activation phase group should be created.
- $\mathrm{GAi[t]} \leftarrow 0, \mathrm{t} = 0 \ldots\ldots \mathrm{GA} - 1$
- $\mathrm{ti} \leftarrow 0$
- Presently, determination of single hub in gathering hub figure completes intensity of Transceiving power as $= \sum (, + 1 +)$ for choice of dynamic hub and for ascertaining a neighbor edge as
- $\mathrm{Tval} = -$
- In the event that estimation of Tval is not

exactly chosen hub control esteem, at that point, lower control hub is chosen as ace.

(1) Secured course revelation over the hub.
(2) Backup hub setup.
(3) Route upkeep over the hub.

5 Results and Discussion

The proposed work has obtained a healthy network by considering the distinctive features like mobility, security, and excellence of service (Figs. 2, 3, 4, 5).

The above results explained that secure routing path can be established in MANET. Throughput measurement analysis, efficiency analysis, and data bandwidth measurement analysis (Table 1).

5.1 *Performance Parameter*

Throughput. It is the part of the channel limit utilized for helpful transmission (Data bundles accurately conveyed to the goal) and is characterized as the complete number of parcels gotten by the goal. It is actually a proportion of the viability of a directing convention.

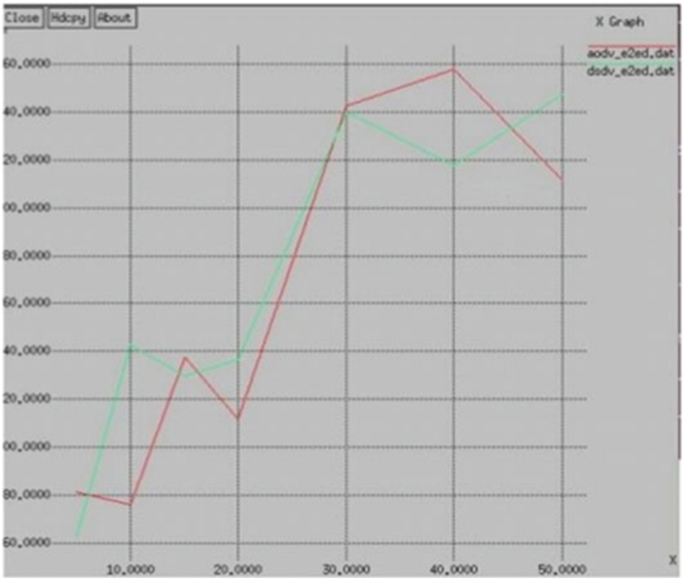


Fig. 2 Result analysis of secure routing in MANET

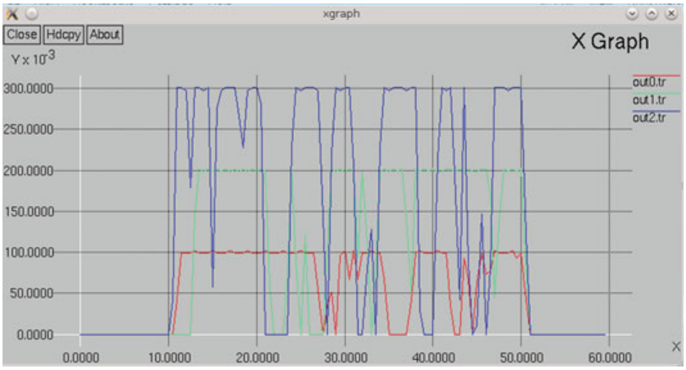


Fig. 3 Result for throughput with routing proposal

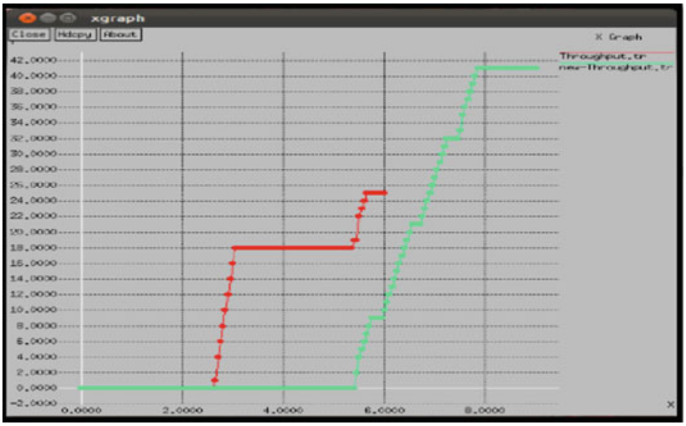


Fig. 4 Comparison result for efficiency

Average delay. This incorporates all conceivable deferrals brought about by buffering amid course disclosure inertness, lining at the interface line, retransmission delays at the MAC, and spread and exchange times.

Packet delivery proportion. The proportion of the information parcels conveyed to the goals to those created by the traffic sources.

6 Conclusion

In this paper, we adjusted the verified stateless convention for verified directing and limited the use of intensity amid way finding and foundation. For the validation of gathering hub, gathering mark method is utilized, and rest mode edge idea is utilized

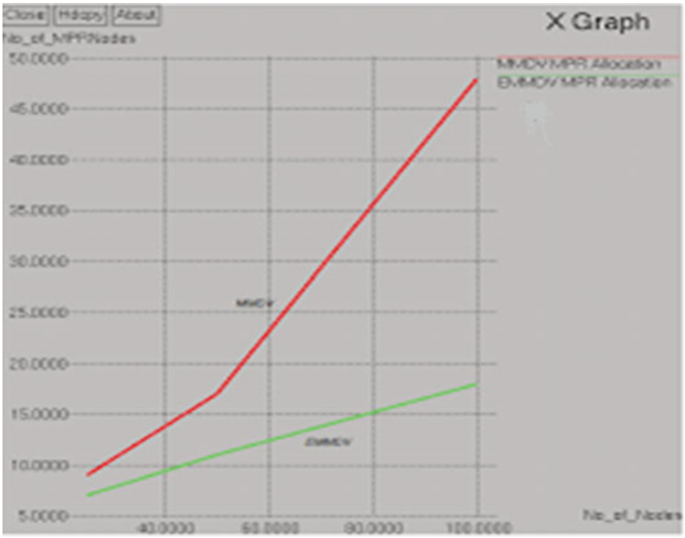


Fig. 5 Result analysis for data bandwidth

Table 1 Parameters simulated in our network

Parameters	Value
Duration	98 s
Area	950*950
Mobile node count	50
Packet rate	4 packet/ s

for power minimization. The proposed calculation partition hub in two states is rests mode and dynamic mode. Transmission from hub rest to to dynamic mode figures need of all rest hub and contrast and number-crunching mean of edge. The estimation of rest mode is more noteworthy, and the equivalent to limit along these lines goes about as ace hub in gathering. In this style, the usage of intensity limited the on time of gathering correspondence. Our trial result indicates most extreme lifetime arrange in contrast with AID steering convention. Trust is a multifaceted, complex, and setting subordinate idea. The trust establishing and the executives in MANET face difficulties from the serious hold requirements, the open idea of the remote medium, the mind boggling reliance between the correspondences framework, the interpersonal organization, and the application arrange, and consequently the perplexing reliance of any trust metric to highlights, parameters, and interchanges inside and among these systems.

References

1. Argyroudis P, Mahoney D (2005) Secure routing for mobile ad hoc networks. In: IEEE communication
2. Zhang Z, Nait-Abdesselam F, Ho PH, Lin X (2008) RADAR a reputation based scheme for detecting anomalous nodes in wireless mesh networks. In: IEEE communications society
3. Djahel S, Nait-Abdesselam F, Khokhar A (2008) An acknowledgment-based scheme to defend against cooperative black hole attacks in optimized link state routing protocol. In: IEEE communications society
4. Nakayama H, Kurosawa S, Jamalipour A, Nemoto Y, Kato N (2009) A dynamic anomaly detection scheme for AODV-based mobile ad hoc networks. In: IEEE transactions on vehicular technology
5. Li Z, Chigan C, Wong D (2008) AWF-NA: a complete solution for tampered packet detection in VANETs. In: IEEE communications society
6. Djahel S, Nait-Abdesselam F, Zhang S (2011) Mitigating packet dropping problem in mobile ad hoc networks: proposals and challenges. In: IEEE communications surveys
7. Chang JM, Tsou PC, Chao HC, Chen JL (2011) CBDS: a cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture. In: IEEE transaction
8. Akyildiz IF, Wang X, Wang W (2004) Wireless mesh networks: a survey in Science Direct
9. Sunderasan K, Papagiannaki K (2008) The need for cross layer information in access point selection algorithms. In: ACM IMC
10. Liu K, Deng J, Varshney PK, Balakrishnan K (2007) An acknowledgment-based approach for the detection of routing misbehavior in MANETs. In: IEEE transaction
11. Cho JH, Swami A, Chen IR (2011) A survey on trust management for mobile ad hoc networks. In: IEEE communications surveys
12. Bali S, Machiraju S, Frost V (2007) On the performance of ad-hoc networks in scheduling techniques. In: WPN

On-line Frequency Reallocation for Call Requests in Linear Wireless Cellular Networks

Narayan Patra

Abstract On-line frequency allocation problem (FAP) for wireless linear cellular networks reusing the frequency of drop calls is studied. In this paper, FAP is investigated on ring networks. The coverage area of highway that surrounds a large mountain is divided into number of regular hexagonal regions called cells. Each of the cells is aligned with exactly two adjacent cells, thus forming a ring topology of the network. Base station (BS) which heads a cell is the transceiver of new or drop call requests from users of same or neighbouring cells. Utilization of spectrum must be properly managed so that no calls generated from same or adjacent cells should be left without getting services from the BSs. In the proposed on-line algorithm for FAP, the drop call releases frequency, and it is reallocated to an ongoing call using greedy strategy. The algorithm is also implemented on 2- or 3-colourable graph model of ring depending on even or odd number of cells that constitute the network, respectively. The performance of the algorithm is analysed on 2-colourable ring network, and it is found that the competitive ratio of the algorithm is $\chi/2$, where the chromatic number of ring network is χ. It has been also shown that there is no on-line algorithm of less than 1 and 3/2-competitive ratios for FAP in 2-colourable and 3-colourable ring networks, respectively.

Keywords Competitive ratio · Frequency reallocation · On-line algorithm · Off-line algorithm · Ring topology

1 Introduction

The problem of frequency interference and its optimal use in wireless cellular networks is highly affected today due to the exponential growth in cell phones. The commonly used frequency division multiplexing (FDM) technology in wireless networks separates the local area into disjoint cells known as regular hexagons. As per

N. Patra (✉)
Department of Computer Science and Engineering, Siksha O Anusandhan Deemed to be University, Bhubaneswar, India
e-mail: narayanpatra@soa.ac.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_106

[1], the centrally located base station (BS) of a cell provides service to the mobile users from inside and outside periphery of the cell. To receive signals from each parts of the coverage area, it divides the local area into small regions (cells). Mobile users send requests to BSs, whenever they require frequency to transmit message to other mobile users. Depending on the way of receipt of requests and get served by base station, the frequency allocation problem is classified as on-line and off-line. In off-line procedure, the entire requests to be responded must be known in advance to the system, whereas in on-line procedure, requests feed to the system partially over time. Therefore, the frequency allocation problem is of two types known as off-line FAP and on-line FAP. Distinguished researchers have been investigated on aforesaid varieties of FAPs for wireless cellular networks over the last decade [1–8]. Due to the recent technological innovations in software as well as in hardware for wide use of digitization with limited availability of spectrum, the researchers are encouraged to adapt on-line version of FAP.

The wireless traffic on a highway that surrounds a large mountain area in the heart of a busy metropolitan city forms a ring topology known as ring highway network. Thus, frequency allocation problem for this type of networks is called FAR. Since ring topology is a model of cycle graph, it is considered as a special case of linear network. From Figs. 1 and 2, it is observed that the small geographical regions known as cells in the network are arranged in such a way that each of the cells has exactly two neighbouring cells. As an illustration, Fig. 1 shows the topology of general ring

Fig. 1 Ring cellular wireless network

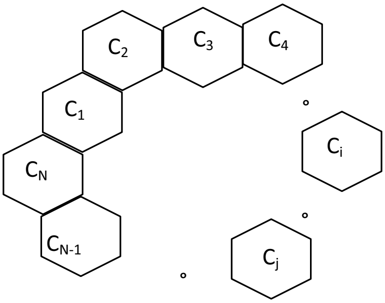
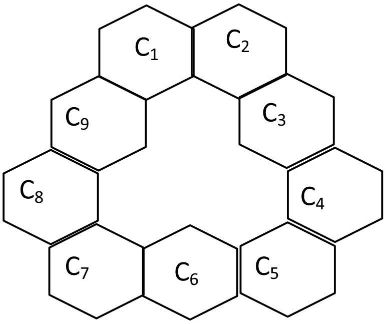


Fig. 2 Ring cellular wireless network $N = 9$



wireless cellular network with N number of cells, and Fig. 2 shows the network with $N = 9$ cells.

Let $S = \{C_1^r, C_2^r, \ldots C_i^r, \ldots C_j^r, \ldots C_n^r\}$ be the sequence of call requests received by the base station of a cell from n-mobile users in a given time period, where $1 \le i \le j \le n$. Each of $C_i^r \in S$ identifies the cell from which ith call initiates. The Boolean values of r in C_i^r classify the call requests either a new call or a drop call depending on $r = 1$ or $r = 0$, respectively. Whenever the base station receives a new call request from its own or from two adjacent cells, it instantly serves the request allocating available frequency if and only if the request is a new call request. On the other hand, if the request is drop call request, it reallocates the frequency of dropped call to an active call in the same cell or free this frequency. Let $Z^+ = \{2, 3, 4, \ldots\}$ be the set of positive integers such that frequency $f_i \in Z^+$ is allocated to the ith—call request in C_i^r for $r = 1$. Then, for some integer $j > i$ and frequency $f_j \in Z^+$, $f_j \neq f_i$ is allocated to C_j^r, where either $C_i^r = C_j^r$ or C_i^r is adjacent to C_j^r. Depending on the duration of calls, FAP can view as finite or infinite scenario. In infinite scenario, call never terminates, and the frequency once allocated remains unaltered until end of call. On the other hand, if a call terminates after a finite time interval, the frequency released from this terminated (dropped) call may be reused for other existing calls. However, the basic objective of FAP for wireless cellular network (WCN) is to serve all the call requests using optimum span of frequency.

The competitive analysis cited in [9] is a metric for measuring the performance of an on-line algorithm over an off-line algorithm. It is defined as follows.

Let cost (*ALGO*) and cost (*OPT*) be the span of frequencies of an on-line algorithm *ALGO* and an optimal span of an off-line algorithm *OPT*, respectively. An on-line algorithm is α-competitive if and only if there is a constant $\alpha \ge 1$ such that $\cos t(ALGO) \le \alpha * \cos t(OPT) + \beta$, for some constant β. The competitive ratio becomes absolute for $\beta = 0$.

1.1 Overview of Graph Colouring

Since last many years, it has been observed that using graph colouring techniques, various kinds of optimization problems have been solved by the researchers. In this paper, the theory of chromatic number of a graph is used in order to increase the efficiency of FAP. Let the graph $G = (V, E)$, where V is non-empty set of vertices called cells, and E is set of edges known as links among the base stations and the mobile phones. Using vertex colouring strategies, the vertices are coloured such that two adjacent vertices should be assigned with distinct colours. So, colouring is a function c: $V(G) \to Z^+$ such that if $(i, j) \in E$, then $c(i) \neq c(j)$, where $c(i)$ and $c(j)$ are colours of vertices i and j, respectively. Graph colouring is an optimization problem in order to minimize the maximum number of colours required to colour all the vertices of G, i.e. $\max_{i \in V}(c(i))$ is minimized. The least number of colours required to colour G is called chromatic number of G denoted by $\chi(G)$.

Since regular hexagonal graph is a suitable model for ring highway network, each of the nodes in this graph is treated as a cell. These cells are topologically regular hexagonal and are aligned in such way that every cell has exactly two neighbouring cells. The number of cells required to form a ring highway network which surrounds a large mountain area depends on the geographical region to be covered by the network. Let N be a positive integer, the number of cells required to design the network whose value depends on the length of the highway to be covered by the traffic. Therefore, the chromatic number of the corresponding graph varies depending on the values of N. Hence, there is a theorem on the chromatic number of ring graph.

Theorem 1 *The chromatic number* (χ) *of a ring graph depends on the number of vertices N of the graph G.*

Proof Assuming $N \geq 3$, we will apply proper colouring to the vertices of the graph G. Since G is a ring, every vertex has exactly two neighbours. Let us suppose each vertex is indexed with $1, 2$ and $3 \ldots N$ in a sequence. Using one colour for even indexed vertex and another colour for odd indexed, it is observed that when N is even minimum number of different colours required to colour the graph is 2. Similarly, when N is odd, it needs minimum number of distinct colours to colour the graph is 3. Thus, $\chi(G) = 2$, when N = even number and $\chi(G) = 3$, when N = odd number.

Finally, the contributions to this paper are listed below.

- The proposed on-line algorithm HYBRID_RING is for solving the frequency allocation problem using the special case of linear network which is known as ring network.
- This algorithm is investigated on two models of WCN with ring topology that are of 2-colourable and 3-colourable ring networks.
- For 2-colourable ring highway, the performance of the proposed on-line algorithm demands a competitive ratio 1 subject to call duration is limited, and the existing calls may be reallocated with the frequency of drop call.
- By similar assumption, in case of 3-colourable ring highway, the proposed algorithm proves a competitive ratio $3/2$.

The rest of this paper is organized as follows. In Sect. 2, related work explores the frequency allocation algorithms using on-line strategies with different constraints for WCN. Section 3 presents the proposed work in which HYBRID_RING, an on-line algorithm for solving FAP for ring network with frequency reallocation (FAR_RE), is discussed. The theoretical results are proved using the bounds for the competitive ratios of the proposed algorithm in Sect. 4. And the paper is concluded with future scopes in Sect. 5.

2 Related Work

The on-line algorithm HYBRID_RE in [10] solves the frequency allocation problem using graph colouring technique. In this case, the networks are modelled as $\chi-$

colourable graphs, where χ is called chromatic number (least number of colours needed to satisfy the property of perfect colouring) of the graph. Fixed assignment (FA) [1] and greedy algorithm [11] are jointly used in HYBRID_RE.

Using FA, each of the cells in a cellular network is treated as independent set depending on frequency distributions among the cells. In general, 3-colourable graph is a suitable model of WCN. Authors [11] claim that the competitive ratio of their on-line algorithm meant for frequency allocation to the network is 3.

On the other hand, greedy strategy allocates frequency to the new call request by selecting lowest available frequency from the frequency spectrum. However, frequency allocated to call requests in this way should not be interfered with the frequency allocated to calls from the same or adjacent cells. The performance of on-line algorithm [11] for FAP in WCN proves competitive ratio is at least $17/7$ and at most 2.5. It finds a tight bond of competitive ratio $17/7$ in [2] using greedy strategy. An on-line version of HYBRID algorithm [12] states that there is a competitive ratio of $(\chi + 1)/2$ for χ-colourable network. In particular, it has been shown by them that the competitive ratio for solving FAP in WCN is 2, which is also optimal. For χ-colourable network, [10] claims HYBRID_RE is $(\chi + 1)/3$-competitive.

The algorithm cited in each of [1, 11–13] deals with infinite call duration. Therefore, as a consequence, frequency allocated initially to a call will be remained unaltered for the entire call duration. In this scenario, it results in a poor usage of frequency spectrum.

In general, the initiation and termination of a call take place after a finite interval of time, and also, the availability of frequency spectrum is limited. It is also observed that the hybrid algorithm in [12] does not consider the drop call for limited time period. To serve all the new and drop call requests, [10] resolves all the pitfalls of FAP in WCN considering the call duration is finite instead of infinite.

3 Proposed Work

The frequency allocation problem for the ring (highway) cellular network (FAR) is investigated in this paper. Since ring graph is a model of aforesaid network, χ-colourable graph is considered for the solution of FAR. A new on-line algorithm for FAR is proposed using χ-colourable network called HYBRID_RING, whose competitive ratio is at most $\chi/2$.

Let us consider a χ-colourable ring network in which $\chi = 2$ or $\chi = 3$. Whenever the base station receives a call request, it instantly allocates the available frequency or reallocates the frequency to existing call in the same cell. In order to avoid frequency interference, the given integer frequency set $Z^+ = \{1, 2, 3, \ldots\}$ is partitioned into two sets using equivalence classes $F_R = [0]_\chi$ and $F_G = [1]_\chi$ when $\chi = 2$.

Thus, for $\chi = 2$,

$$\left.\begin{aligned} F_R &= \{2, 4, 6, 8\ldots\} = \{2\chi, 4\chi, 6\chi, \ldots\} \\ F_G &= \{3, 5, 7, 9\ldots\} = \{\chi + 1, \chi + 3, \chi + 5, \ldots\} \end{aligned}\right\} \tag{1}$$

When $\chi = 3$, the frequency set $Z^+ = \{1, 2, 3, \ldots\}$ is divided into three partitions $F_R = [0]_\chi$, $F_G = [1]_\chi$ and $F_B = [2]_\chi$, where

$$\left.\begin{array}{r} F_R = \{3, 6, 9, 12, \ldots\} = \{\chi, 2\chi, 3\chi, \ldots\} \\ F_G = \{4, 7, 10, 13\ldots\} = \{\chi + 1, \chi + 4, \chi + 7, \ldots\}\text{and} \\ F_B = \{5, 8, 11, 14, \ldots\} = \{\chi + 2, \chi + 5, \chi + 8, \ldots\}. \end{array}\right\} \qquad (2)$$

3.1 HYBRID_RING Algorithm and Its Principles

Depending on types of call request received by a cell, it serves each of the requests allocating available frequency to a new call using greedy approach or reallocating the released frequency of the dropped call to another call with the highest frequency. It follows two schemes for serving the each call request.

Allocation Scheme: Let us suppose a new call request is generated in some node (cell) say v with colour red or green. Then, it allocates frequency either from F_R or from F_G based on the following rules:

I. Let $f_r = \min(F_R)$ such that no call from v or from its adjacent uses frequency f_r.
II. Let $f_g = \min(F_G)$ such that no call from v uses frequency f_g.
III. Let $f_m = \min(f_r, f_g)$. Then, allocate frequency f_m to the new call.

The reallocation of released frequency from drop call is done as per the given scheme.

Reallocation scheme: For each drop call request $C_i^{r=0}$, supposing that it originates from a node v with colour red or green. The highest frequency f_h to a call $C_i^{r=1}$ is reallocated with the frequency f_d of dropped call $C_i^{r=0}$, if $f_d < f_h$ and both requests $C_i^{r=0}$ and $C_i^{r=1}$ belonging to same cell, otherwise free f_d.

Input: Request sequence ($S = \{C_1^r, C_2^r, \ldots C_i^r, \ldots C_j^r, \ldots C_n^r\}$), where r = 0 or 1.

Output: Allocating the optimal span of frequencies.

Let us suppose that node (cell) v with colour red or green received a new call request $C_i^{r=1}$ or a drop call request $C_i^{r=0}$ in time period t.

```
  Let $f_p$ and $f_q$ be the minimum frequencies available in $F_R$ and $F_G$ respectively.
  if (request==$C_i^{r=1}$) // new call request
  {
          Calculate $f_{\min}$ = minimum ($f_p$ , $f_q$)
          if ($f_{\min}$ == $f_q$) then
                          Allocate $f_q$ to call $C_i^{r=1}$

          else
                          Allocate $f_p$ to call $C_i^{r=1}$
  }
  else        // drop call request
  {
  Let $f_d$ be the frequency of dropped call.
  Let highest frequency $f_h \in F_R$ being allocated to a call in $C_i$ and highest frequency $f_{h'} \in F_G$
  being allocated to the call in its adjacent cell $C_{i-1}$ or $C_{i+1}$ .
      if ($f_h < f_{h'}$ )
      {
          then $f_{new} \leftarrow f_{h'}$ // where $f_{new}$ is new highest frequency in the $C_i \cup C_{i-1} \cup C_{i+1}$
      }
      else
      {
          $f_{new} \leftarrow f_h$   // where $f_{new}$ is new highest frequency in the cells $C_i \cup C_{i-1} \cup C_{i+1}$
      }
      if ($f_d < f_{new}$ && ($f_d$ and $f_{new}$ are allocated to the calls in the same cell))
      {
          $f_{new} \leftarrow f_d$
      }
      else
      {
                  free frequency $f_d$.
      }
}
```

4 Result Analysis

The proposed on-line algorithm HYBRID_RING is implemented on $\chi-$ colourable ring network, and it determines the upper and lower bounds for its competitive ratio in theorem 2 and theorem 3, respectively. As 2- or 3-colourable graph is the suitable model for a ring network, it has been shown the counter results in corollary 4.1 and corollary 4.2 with respect to the results that were previously found for FAP.

Theorem 2 The on-line algorithm HYBRID_RING for $\chi-$ colourable networks is $\chi/2$ is competitive.

Proof Suppose C_i cell with colour red or green receives the sequence of call requests S in an instance of time period. If each of the requests is a new call and the frequency once allocated to it survives until call ends, authors in [12] prove that the competitive ratio does not exceed $\chi + 1/2$. Assuming call duration is finite, and possibly, the call may be terminated due to various reasons. In this case, frequency allocated earlier to a call may be altered later. In view of getting better competitive ratio and also to minimize the frequency span, it is wise to reuse the released frequency from drop call allocating to some active calls in the same cell of the same network. Let us suppose that the highest frequency f_h is currently allocated to a call in a particular cell with one of the colours say red or green. If the next request in the same cell is a drop call request, the proposed algorithm HYBRID_RING proves the competitive ratio is at most $\chi/2$.

Case 1. Let $f'_h = \chi l$, for some integer $l \geq 1$ be the highest frequency belonging to the frequency set F_R being allocated to the call originates from the cell C_i with colour red or its two adjacent cells with colour green. So l-calls are being in active through the allocated frequencies in the cell C_i or its adjacent cells C_{i-1} or C_{i+1}.

Suppose $f_d = \chi l'$, be the frequency of dropped call belonging to the frequency set F_R such that $f_d < f_h$ for some integers l and l' with $l' < l$. Then, f_d is allocated to a call holding the highest frequency f_h provided both the calls originate from the same cell say C_i. On the other hand, if the existing call with highest frequency f_h is in C_i and the dropped call with frequency f_d is either in C_{i-1} or in C_{i+1}, then f_h cannot be reallocated with f_d in order to avoid interference of frequencies in the neighbouring cells. Again, similar arguments can also be made for the case when frequency of dropped call is $f_d = \chi l' + 1$,

Case 2. Let $f''_h = \chi m + 1$, for some integer $m \geq 1$ be the highest frequency belonging to the frequency set F_G being allocated to the call originates from the cell C_j with colour red or its two adjacent cells with colour green. So m-calls are being in active through the allocated frequencies in the cell C_j or its adjacent cells C_{j-1} or C_{j+1}.

Suppose $f_d = \chi m' + 1$, be the frequency of dropped call belonging to the frequency set F_G such that $f_d < f_h$ for some integers m and m' with $m' < m$. Then, the call with highest frequency f_h is reallocated with f_d provided both the calls originate from the same cell say C_j. On the other hand, if the existing call with highest frequency f_h is in C_j and the dropped call with frequency f_d is either in C_{j-1} or in C_{j+1}, then f_h cannot be reallocated with f_d in order to avoid interference of frequencies in the neighbouring cells. Now, similar arguments can also be made for the case when frequency of the dropped call is $f_d = \chi m'$,

From case 1 and case 2, it is observed that the total number of calls including the recent most call request is $l + m + 1$, which are allocated with frequencies from set $F_R \cup F_G$.

If $f'_h < f''_h$, this implies $\chi l < \chi m + 1$, for some integers m and $l, m \geq l$.

Therefore, the net highest frequency becomes $f_h = \chi m+1$. By using the proposed algorithm, the new highest frequency is now denoted by $f_h^{ALG} = \chi l$. However, the optimal span of frequencies required for allocation to avoid frequency interference using off-line algorithm is not less than $2l + 1$.

Hence, upper bound of competitive ratio is $f_h^{ALG}/2l + 1 = \chi l/2l + 1 \leq \chi/2$, for $m \geq l$.

If $f_h'' < f_h'$, this implies $\chi m + 1 < \chi l$, for some integers m and l, for $l \geq m + 1$.

Therefore, the highest frequency becomes $f_h = \chi l$. The proposed HYBRID_RING algorithm updates the highest frequency to $f_h^{ALG} = \chi m + 1$. Again, the well-known off-line algorithm uses minimum of $2(l + 1)$ frequencies to avoid interference among frequencies.

Hence, the upper bound of competitive ratio be $f_h^{ALG}/2(l + 1) = \chi m + 1/2(l + 1) \leq \chi/2$ because $l \geq m + 1$.

In both cases, the competitive ratio is at most $\chi/2$.

Thus, theorem 2 proves the upper bound of the competitive ratio using the proposed on-line algorithm is $\chi/2$ which dominates the competitive ratio $\chi + 1/2$ cited in [12] using infinite call duration. Moreover, $\chi/2$-competitive is logically more efficient than $\chi + 1/3$-competitive due to [10].

Since the ring networks in FAR are a special case of linear networks and also a model of ring topology, the number of cells used in these networks is either even or odd. Therefore, the chromatic number of the proposed ring graph is either 2 or 3 depending on the even or odd number of cells, respectively.

Corollary 4.1 *On-line algorithm HYBRID_RING for* 2*-colourable networks reduces the competitive ratio to 1 which exploits the competitive ratio* $5/3$ *for FAL due to* [14].

In [14], authors proposed an algorithm BORROW with competitive ratio is at most $5/3$ in 2-colourable ring networks. Algorithm suggested in [5] with chromatic number 2 proves its competitive ratio 1. Using 2-colourable network and applying theorem 2, HYBRID_RING algorithm finds at most 1-competitive ratio which opposes the less tight upper bound $5/3$ due to the algorithm BORROW. Therefore, corollary 3.2 states the following statement.

Corollary 4.2 *Algorithm HYBRID_RING for 2-colourable networks obtains a tighter upper bound than the upper bound of competitive ratio of BORROW.*

Thus, HYBRID_RING algorithm generalizes the works of [14] *using a special case of linear networks.*

Lower Bound

Theorem 3 *Frequency allocation problem for 2-colourable ring cellular network contributes minimum of 1-competitive ratio.*

Proof Consider a ring cellular network with cells C_1, C_2, C_3, C_4, C_5, C_6, C_7 and C_8 with colour red and green alternatively in Fig. 3.

Suppose there is an on-line algorithm *ALGO* for solving FAR. Let us consider three calls in cell C_1 and two calls in C_2 are in active with frequency sets {2, 3, 4}

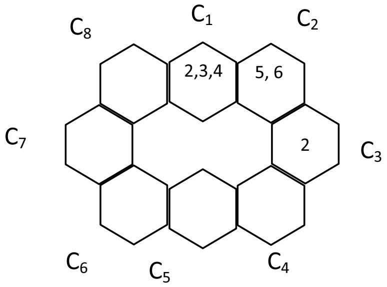


Fig. 3 2-colourable ring cellular network

and {5, 6}, respectively. If the highest frequency among the five calls in both the cells is given by the integer frequency $f_h = 6$ and the current drop call request with frequency f_d, then three situations arise. First, if $f_d = f_h$ and both frequencies are used in same cell, then *ALGO* supports maximum span of frequency is not more than 5, and the adversary makes one call in cell C_2 which needs optimally at least five different frequencies. Thus, at least 1-competitive ratio results due to on-line algorithm ALGO. Secondly, if a new call is made in C_3, then the algorithm allocates integer frequency 3 without conflicting with other frequencies. In this case, it is observed also the maximum span of frequency be 5 which proves the same bound for competitive ratio. Third, if $f_d = 2$ such that $f_d < f_h$ and both being allocated in the same cell either in C_1 or in C_2, where adversary generates a new call in C_3, then the highest integer frequency be 5. These arguments prove that proposed on-line *ALGO* is at least 1-competitive, as there must exists an off-line algorithm which takes an optimal span of frequency 5.

Corollary 4.3 *Frequency allocation problem for* 3*-colourable ring cellular networks contributes minimum of* 3/2*-competitive ratio.*

Proof Let there is odd number of cells that constitutes the proposed ring cellular network. According to theorem 1, this network is 3-colourable, and the chromatic number is 3. Suppose, as an illustration, Fig. 4 is a 3-colourable network which contains cells C_1, C_2, C_3, C_4 and C_5 using colours red, green and blue such that no two adjacent cells have same colour.

From this network, it is concluded that $f_h = 7$ being the highest frequency, and it is allocated to a call in cell C_5. If the call request is a drop and it is also generated in cell C_5, *ALGO* finds new highest frequency $f_h = 6$. Since it requires at least four distinct frequencies optimally using an off-line algorithm, thus the proposed on-line algorithm proves at least 3/2-competitive ratio.

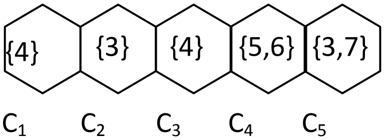


Fig. 4 3-colourable ring cellular network

5 Conclusion

The proposed algorithm divides the frequency set into 2 or 3 partitions depending on whether the ring network is 2-colourable or 3-colourable, respectively. Considering the duration of calls is finite and reusing the frequency free from drop calls for some existing calls, it has been proved that the competitive ratio $(\chi + 1)/3$ is reduced to $\chi/2$ for χ-colourable wireless ring cellular networks. The lower bounds of the algorithm for 2-colourable as well as 3-colourable ring networks have been derived. It is shown that for 2-colourable ring, the lower bound is at least 1, and for 3-colourable ring, it is at least 3/2. The future study will focus on the randomized version of on-line HYBRID_RING algorithm for both linear and nonlinear networks.

References

1. MacDonald VH (1979) Advanced mobile phone service: the cellular concept. Bell Syst Tech J, 15–41
2. Chan JWT, Chin FYL, Zhang D, Ye Y, Zhu H (2007) Greedy on-line frequency assignment in cellular networks. Inf Process Lett 102(2–3):55–61
3. Aardal KI, van Hoesel SPM, Koster AMCA, Mannino C, Sassano A (2007) Models and solution techniques for frequency assignment problems. Ann Oper Res 153(1):79–129
4. Hale W (1980) Frequency assignment: theory and applications. Proc IEEE 68(12):1497–1514
5. Christ MG, Favrholdt LM, Larsen KS (2013) On-line multi-colouring on the path revisited. Acta Informatica 50:343–357
6. Pantziou GE, Pentaris GP, Spirakis PG (2002) Competitive call control in mobile networks. Theory Comput Syst 35(6):625–639
7. Katzela I, Naghshineh M (1996) Channel assignment schemes for cellular mobile telecommunication systems: a comprehensive survey. IEEE Pers Commun 3(3):10–31
8. Chrobak M, Sgall J (2009) Three results on frequency assignment in linear cellular networks. In: 5th international conference on algorithmic aspects in information and management, vol 5564, LNCS, Springer, pp 129–139
9. Borodin A, El-Yaniv R (1998) On-line computation and competitive analysis. Cambridge University Press
10. Patra N, Ray BNB, Mohanty SP (2014) On-line frequency reassignment for new and drop calls in wireless cellular networks. In: 13th international conference on information technology, proceedings, pp 137–141
11. Caragiannis I, Kaklamanis C, Papaioannou E (2002) Efficient on-line frequency assignment and call control in cellular networks. Theory Comput Syst 35(5):521–543
12. Chan JWT, Chin FYL, Ye D, Zhang Y (2007) On-line frequency assignment in cellular networks. In Proceedings of 19th Symposium on Parallel Algorithms and Architectures (SPAA)
13. Chin FYL, Zhang Y, Zhu H (2007) A 1-local 13/9-competitive algorithm for multi-colouring hexagonal graphs. In: Proceedings of the 13th annual international Computing and Combinatory Conference (COCOON)
14. Chan JWT, Chin FYL, Ye D, Zhang Y, Zhu H (2006) Frequency assignment problems for linear cellular networks. In: Proceedings of the 17th annual International Symposium on Algorithms and Computation (ISAAC), pp. 61–70

A Novel Secure IoT Based Optimizing Sensor Network for Automatic Medicine Composition Prescribe System

M. Bowya and V. Karthikeyan

Abstract Growing population and continuous increase in health issues increases the significance on the healthcare centers which are demanding for an efficient healthcare system. 24/7 clinical service is not available to all common people and many life losses occurs due to unavailability of medicine on time and many researches were made to make the medicine globalized. We propose an IoT based module where the health-related parameters of patients are recorded using sensors, symptoms computed are uploaded to the server, by comparing the computed symptoms to the database the problem is detected and the medicine and dosage level for the detected health problem is prescribed automatically. Database must be created by group of authorized specialist doctors and the database management can be done with the help of SQL server.

Keywords IoT (Internet of Things) · Database management · Medicine prescription

1 Introduction

Healthcare monitoring is an essential one to maintain the well being of the people. Due to increased health-related issues, there has been continuous increase in pressure on the hospitals and the clinical services are not available to all rural areas. The existing healthcare methodology is hospital-based which is time-consuming and cost-intensive. This adds to long queues in hospitals and there are several cases that life loses occurred since the timely medical solution is not obtained. This fast-moving world needs technology-based advanced healthcare monitoring especially for elderly people [1]. IoT is creating a great impact on most of the fields today and medical field is not an exception [2]. Remote patient monitoring can be achieved with the help of

M. Bowya (✉) · V. Karthikeyan
Department of ECE, Vivekanandha College of Engineering for Women, Namakkal, India
e-mail: bowya217@gmail.com

V. Karthikeyan
e-mail: karthick77keyan@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_107

biomedical sensors and the parameters recorded can be sent to healthcare providers with the help of IoT, thus the health parameters can be recorded continuously and an alert intimation may be given in case of emergency. In addition it serves the purpose of maintaining the medical history of patients but does not provide any solution to the patients. In this paper, we propose a module where with the combined technology of Embedded Systems and IoT the health parameters of the patients are sensed and the health issue is detected by analyzing the symptoms and an immediate medicinal solution is suggested, i.e., the prescription for the detected problem is generated automatically with the help of database.

2 Existing System

The existing healthcare system is hospital-based which requires presence of doctors manually. It leads to more transportation time, waiting time in queue, pre-appointment, and anytime consulting service. Continuous hospitalization is required for patients with chronic diseases [3] where in such cases the patients may feel isolated from the external world, thus distance monitoring is quite important in this fast-moving world especially for the people with chronic disorders. Remote monitoring of patients can be achieved with the help of IoT technology where patients at home can be monitored continuously using sensors [4]. The at most work done in existing methodology is to send the sensed health parameters of the patients as real-time data to the health care centers [5]. This existing method does not focus on providing solution to the patients, it only focuses on maintaining the perfect medical history of the patients so that the further decision regarding the type of treatment that the patient can be proceeded with is determined effectively. Only in some emergency cases, alert is created that the patient is to be hospitalized immediately. The Architecture of existing system is shown in Fig. 1.

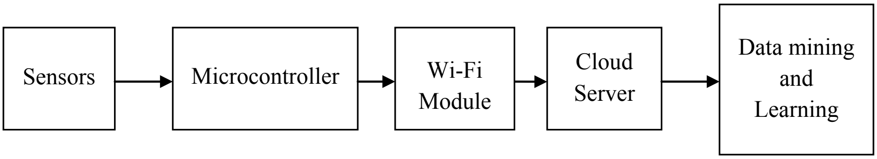


Fig. 1 Architecture of Existing system

2.1 Sensors

The health parameters are collected by sensing using biomedical sensors and various wearable sensing devices [6]. Certain important signs including body temperature, heartbeat rate, respiratory rate and value of blood pressure are monitored and recorded [7]. Other parameters like blood glucose level need to be monitored in case of diabetic patient. Thus the parameters to be sensed depends upon the medical status of the patients, e.g., the factors such as ECG, rate of heartbeat, saturation level of oxygen and weight are sensed for heart failure patients. For people with disabilities and elderly people, continuous activity monitoring is required [8].

2.2 Microcontroller

It is mandatory to process the sensed parameters into transmittable format using smartphones [9], FPGA (Field Programmable Gate Array), hardware platforms, microcontrollers or microprocessors. This combines the data from sensors, transfers the data to server for storing and then finally processes the data. It is the computational block of the architecture and is an essential one for decision making and further analysis in future.

2.3 Wi-Fi Module

The sensed and recorded data are to be sent to the microcontroller. This involves several protocols by which the connection and data transmission can be done. The technologies like Wi-Fi [10], Bluetooth, ZigBee, LTE (Long-Term Evolution) or any other high-level communication protocols can be implemented. Both Bluetooth and Wi-Fi provide wireless communication but the difference resides in their efficiency. Various devices can be connected without the usage of cable by using Bluetooth while the access to internet can be achieved using Wi-Fi.

2.4 Cloud Server

The collected and processed data need to be stored for further analysis. The data is stored without any loss using cloud servers. There are several platforms available for data storage including ThingWorx, Open IoT, Google Cloud, Amazon, GENI [11]. Cloud computing is used to manage the large database thus the efficiency of data storage is improved. Here the data is stored in distributed server so that the data is available on demand without any sort of traffic.

2.5 Data Mining and Learning

This layer focus on converting the collected and stored data into knowledge in decision making. Data mining is an algorithm-based process of generating new information by analyzing and examining huge database. Here the frequency of similar data of patient is registered. Machine Learning provides the system the ability to automatically learn and improve from experience.

3 Proposed Work

The overall architecture of proposed system shown in Fig. 2a consists of several client devices (i.e., the device the patients are provided with) connected to a server via IoT. Patient's health parameters are sensed, processed and finally uploaded to the authorized server using the client device. The server is connected to the database where the symptoms and basic details of patients are analyzed, the health issue of the patient is detected and the standard medicine for the problem and dosage level according to the age factor is suggested to the patient instantly.

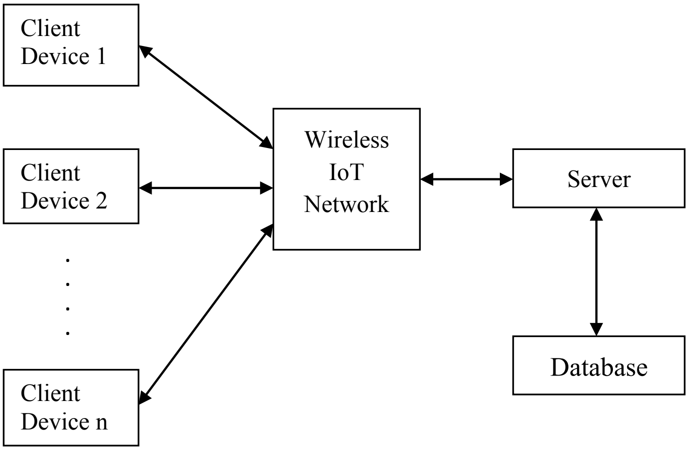


Fig. 2 **a** Overall Proposed Architecture

3.1 Client Device

Each client device consists of n number of biomedical sensors which are used to sense the vital signs of patients [12]. The recorded data are fed as input to the signal conditioning circuit which is used to manipulate the recorded values and covert them from analog to digital signal since the sensed parameters can't be directly given as input to the Digital Signal Controller. Both Digital Signal Controller and signal conditioning unit are provided with the power supply unit [13]. DSCs can be used in variety of applications including power conversion, motor control, and sensor processing applications. Here the Digital Signal Controller uploads the health parameters of patients to the server. And after analyzing the recorded symptoms of patients the detected problem and the medicine along with dosage level is sent to the client device. Client module is shown in the Fig. 3.

3.1.1 Power Supply Unit

Every electronic system is to be provided with DC power supply. Different circuits operate under different power supplies and the rating depends upon the load current and voltage. The load current depends on the load resistance, i.e., the load current is inversely proportional to load resistance. So it is quite mandatory to provide the electronic circuit with matched designation of power supply. In our proposed module we use two power supplies, DC 5v with GND and DC 12v with GND. A LM341 is a three-terminal positive voltage regulator is used to maintain the output voltage constant irrespective of its input voltage.

3.1.2 Sensors

The biomedical sensors are implemented in the client device to sense the health parameters of the patients. In our proposed module Temperature sensor (LM35)

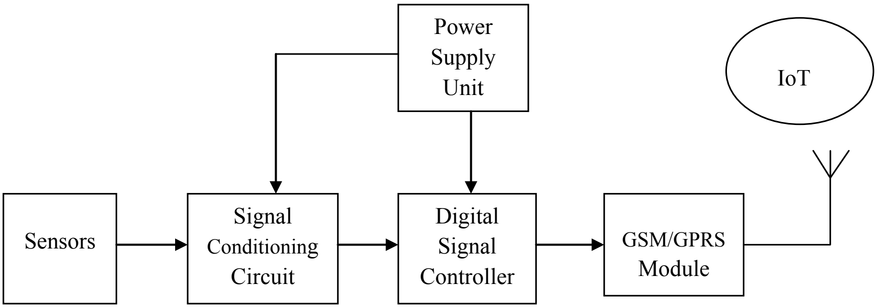


Fig. 3 Client device

and Heartbeat sensor are used to record the body temperature and heartbeat rate. The output of LM35 series shown in Fig. 5 is a voltage which is comparative to temperature in Celsius. The light source (LED) is made to be incident onto any muscular region and the amount of light reflected back is estimated using light detector. The amount of light reflected changes with respect to the change in the volume of blood flow, thus the rate of heartbeat can be estimated. Ultrasonic sensors with low power oscillators [14] can be implemented for better efficiency.

3.1.3 Signal Conditioning Circuit

The sensed analog value cannot be directly given as input to the next stage thus the signal conditioning circuit is implemented so that the measured analog health parameter of the patient is processed into a form such that the input requirements of the next stage is met. The signal conditioning circuit accepts any type of sensor inputs and the outputs can be voltage, current, frequency, timer or counter.

Signal conditioning processes: Signal Conditioning circuit involves two main process including Filtering and Amplifying. The analog parameter sensed by sensors is subjected to filtering so that any high-frequency noise present can be eliminated, then the resultant signal is amplified. Amplified analog signal is converted into digital signal using ADC converter. Thus, its function is to convert the measured analog signal into processed digital signal which is the input to next stage (Digital Signal Controller).

3.1.4 Digital Signal Controller

A Digital Signal Controller (DSC) is considered to have advanced features than Digital Signal Processors (DSPs) and Microcontrollers. The digital output from the Signal-Conditioning circuit need to converted into proper symptoms so that it can be uploaded to server and compared with the database in the authorized server. DSC performs the major role of processing the data and uploading the processed data to the server using GSM/GPRS module and DSC can be generally programmed using the C programming language.

3.1.5 GSM/GPRS Module

GPRS module is used to efficiently transfer the data between client and server by using circuit-switched mechanism. It is the responsibility of the GSM/GPRS module to find the best path with minimal traffic to transfer the processed data from the DSC to the authorized server. Both uploading of parameters to server and receiving the feedback response given by the server, i.e., prescribed medicine and dosage level, at high speed can be achieved using this module.

3.1.6 IoT

The **Internet of Things (IoT)** plays a major role in our work since it allows the communication between the client and server module. It is the network of devices which allows connection, interaction and exchanging of data between various things. IoT is the technology involving extending of internet connection beyond standard devices to the devices that are used in day to day life. With the IoT technology, the devices may be able to communicate among one another and controlling of a device from is remote location can also be achieved.

3.2 Server and Database Management

The collected and processed health parameters of the patients are uploaded to the authorized server which is connected to the database. The database management is done with the help of Microsoft SQL server and the programming is done using php. Php is an easiest web programming language that is used to create a database. The basic details of patients would be registered at the hospital server. Once registered the further login can be done using the provided username and password. The database created consists of the health issues which is selected based on the recorded parameters of patients and the dosage level is selected according to the age factor of the patients.

4 Results and Discussion

Each client device consists of n number of biomedical sensors which are used to sense the vital signs of patients. The recorded data are fed as input to the signal conditioning circuit which is used to manipulate the recorded values and covert them from analog to digital signal since the sensed parameters can’t be directly given as input to the DSC. Both DSC and signal conditioning unit are provided with the power supply unit. Here the DSC uploads the health parameters of patients to the server. And after analyzing the symptoms of patients the detected problem and the medicine with dosage level is sent to the client device (Fig. 4).

Server and Database Management:

The basic details of the patients would be registered to a authorized hospital server and once registered the patients can be provided with the user name and password with which the patient can log in (Figs. 5, 6 and 7).

Once the login is done the patient’s health parameters are uploaded to the server via GPRS module and the symptoms of the patients are compared to the database created and the detected problem, medicine for the problem detected along with the dosage level is displayed to the patients instantly (Fig. 8).

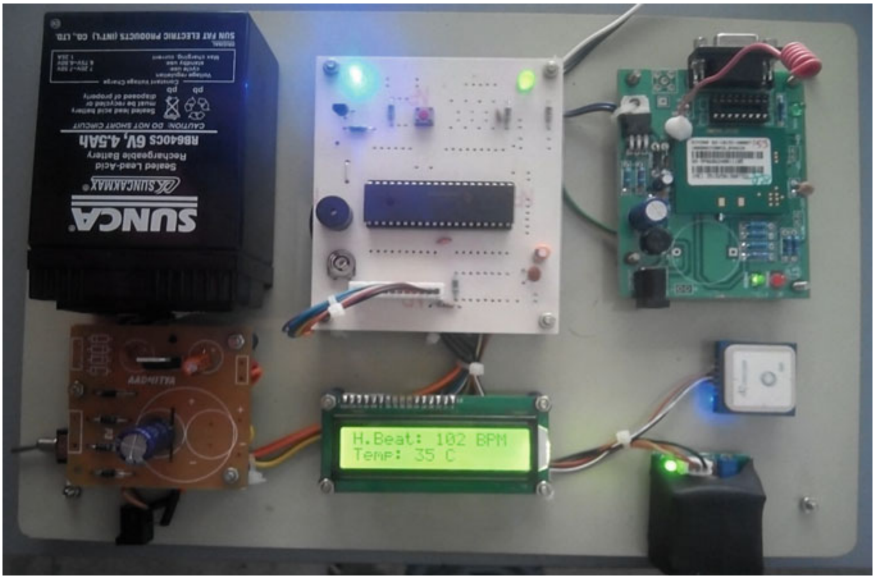
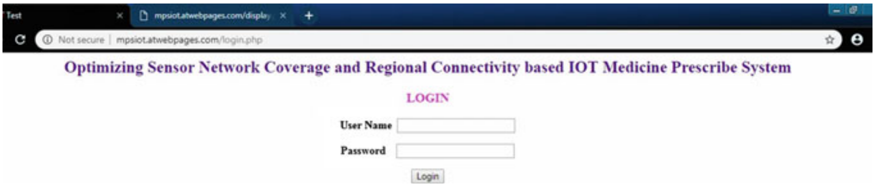


Fig. 4 Client Device


Test
mpsiot.atwebpages.com/display
Not secure | mpsiot.atwebpages.com/login.php

Optimizing Sensor Network Coverage and Regional Connectivity based IOT Medicine Prescribe System

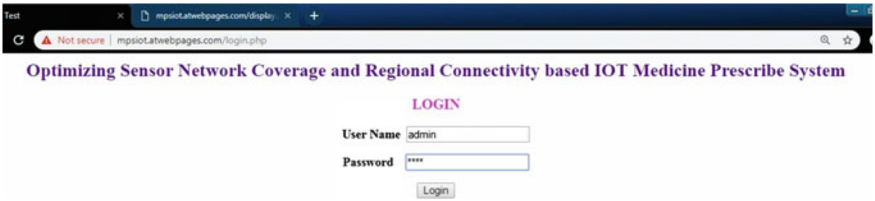
LOGIN

User Name

Password

Login

Fig. 5 Login page of automatic medicine prescribe system


Test
mpsiot.atwebpages.com/display
Not secure | mpsiot.atwebpages.com/login.php

Optimizing Sensor Network Coverage and Regional Connectivity based IOT Medicine Prescribe System

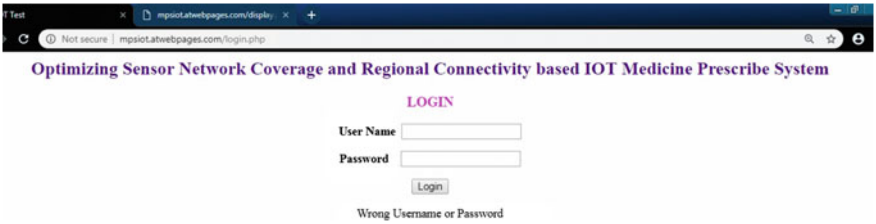
LOGIN

User Name admin

Password ****

Login

Fig. 6 Login can be done using corresponding username and password


T Test
mpsiot.atwebpages.com/display
Not secure | mpsiot.atwebpages.com/login.php

Optimizing Sensor Network Coverage and Regional Connectivity based IOT Medicine Prescribe System

LOGIN

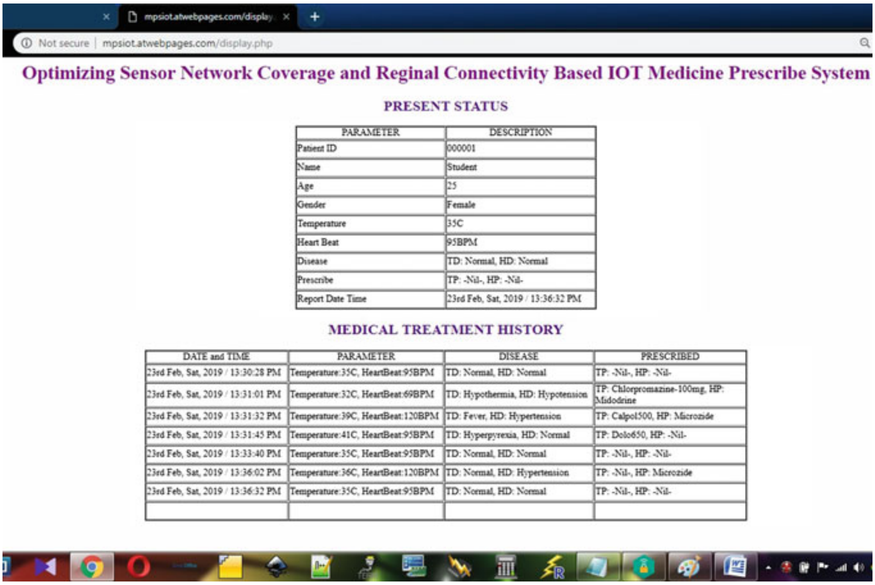
User Name

Password

Login

Wrong Username or Password

Fig. 7 No invalid login can be done


mpsiot.atwebpages.com/display
Not secure | mpsiot.atwebpages.com/display.php

Optimizing Sensor Network Coverage and Reginal Connectivity Based IOT Medicine Prescribe System

PRESENT STATUS

PARAMETER	DESCRIPTION
Patient ID	000001
Name	Student
Age	25
Gender	Female
Temperature	35C
Heart Beat	95BPM
Disease	TD: Normal, HD: Normal
Prescribe	TP: -Nil-, HP: -Nil-
Report Date Time	23rd Feb, Sat, 2019 / 13:36:32 PM

MEDICAL TREATMENT HISTORY

DATE and TIME	PARAMETER	DISEASE	PRESCRIBED
23rd Feb, Sat, 2019 / 13:30:28 PM	Temperature:35C, HeartBeat:95BPM	TD: Normal, HD: Normal	TP: -Nil-, HP: -Nil-
23rd Feb, Sat, 2019 / 13:31:01 PM	Temperature:32C, HeartBeat:69BPM	TD: Hypothermia, HD: Hypotension	TP: Chlorpromazine-100mg, HP: Midodrine
23rd Feb, Sat, 2019 / 13:31:32 PM	Temperature:39C, HeartBeat:120BPM	TD: Fever, HD: Hypertension	TP: Calpol500, HP: Microzide
23rd Feb, Sat, 2019 / 13:31:45 PM	Temperature:41C, HeartBeat:95BPM	TD: Hyperpyrexia, HD: Normal	TP: Dolo650, HP: -Nil-
23rd Feb, Sat, 2019 / 13:33:40 PM	Temperature:35C, HeartBeat:95BPM	TD: Normal, HD: Normal	TP: -Nil-, HP: -Nil-
23rd Feb, Sat, 2019 / 13:36:02 PM	Temperature:36C, HeartBeat:120BPM	TD: Normal, HD: Hypertension	TP: -Nil-, HP: Microzide
23rd Feb, Sat, 2019 / 13:36:32 PM	Temperature:35C, HeartBeat:95BPM	TD: Normal, HD: Normal	TP: -Nil-, HP: -Nil-

Fig. 8 Medicine and dosage level prescription

5 Conclusion and Future Work

In this paper, remote monitoring and diagnosing using sensors and automatic medicine prescription generation using the database is achieved. In our work minimum parameters like body temperature and heartbeat rate are analyzed and different health status along with the corresponding medicine and dosage level to be taken is given as response to the patients. Initial dosage level suggestion would be based on the age factor and further dosage level is based on response of patient's health response to the medicine (with the help of medical history maintained in the server). It decreases pressure on hospitals and reduces healthcare cost. In future furthermore biomedical sensors can be added and by analyzing further more symptoms many health issues can be detected and the prescription for many problems can be generated. The database of medicine can be created by super-specialist doctors, and it can act as an life-saving equipment by providing immediate first aid medicine in emergency situations like heart attack.

References

1. Jimenez F, Torres R (2015) Building an IoT-aware healthcare monitoring system for elderly people. In: 34th international conference of the chilean computer science society (SCCC), pp 1–4
2. Karthikeyan V, Bowya M (2018) A review on IoT based healthcare monitoring. Indo-Iran J Sci Res 2:24–30
3. Dierckx R, Pellicori P, Cleland JGF, Clark AL (2015) Tele monitoring in heart failure: big Brother watching over you. Heart Fail Rev 20:107–116
4. Kelly SDT, Suryadevara NK, Mukhopadhyay SC (2013) Towards the Implementation of IoT for environmental condition monitoring in homes. J IEEE Sens 13:3846–3853
5. Nguyen HH, Mirza F, Naeem MA, Nguyen M (2017) A review on IoT healthcare monitoring applications and a vision for transforming sensor data into real-time clinical feedback. In: International conference on computer supported cooperative work in design, pp 257–62
6. Karthikeyan V (2016) A novel design of low energy oscillator based ultrasonic sensor edge for intravascular applications with CMUT technology. J Middle-East J Sci Res 24:3716–3720
7. Karthikeyan V, Christina J (2016) Review of ultrasonic transducers for medical applications with CMUT implementation. J Int J Adv Eng Glob Tech **7**
8. Bjorkman M, Causevic A, Fotouhi H, Ahmed MU, Linden M (2015) An overview on the Internet of Things for health monitoring systems. In: 2nd EAI international conference on IoT technologies for healthcare healthyIoT 169:429–36
9. Bisio I, Lavagetto F, Marchese M, Sciarrone A (2015) A smartphone centric platform for remote health monitoring of heart failure. Int J Commun Syst 28:1753–1771
10. Narendra Swaroop K, Chandu K, Gorrepotu R, Deb S (2019) A healthcare monitoring system for vital signs using IoT. Internet Things 5:116–129
11. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M (2015) Internet of Things: a survey on enabling technologies, protocols, and applications. IEEE Commun Surv Tutorials 17:2347–2376
12. Fortino G, Parisi D, Pirrone V, Di Fatta G (2014) Body Cloud: a SaaS approach for community body sensor networks. Future Generation Comput Syst 35:62–79
13. Karthikeyan V, Christina Jasmine (2017) A squat energy oscillator based readout edge with CMUT technique for medical applications. J Adv Nat Appl Sci 11:364–641
14. Karthileyen V, Jasmine Christina J (2017) Design of low power oscillator for medical ultrasonic sensors with CMUT implementation. Asian J Appl Sci Technol 1:68–72

High-Speed Polar Decoder Architecture for Next Generation 5G Applications Using Radix-k Processing Engine

R. Kavipriya and M. Maheswari

Abstract Among the various coding techniques, polar codes are very useful, since it achieves the ultimate channel coding characteristics. In this paper, a decoding architecture is proposed which reduces the memory consumption and delay. To overcome the problem of concurrency, a parallel processing is done. The further research is in processing on the polar codes to be applied for next-generation applications. Polar code is preferred since it increases the speed of the operation for large number of bits (i.e.) for large code length. This implementation process is further extended by combining the encoding and decoding process by using radix-k based design.

Keywords Polar decoder · Polar codes · High speed

1 Introduction

The main aim of coding theory is to approach a new code in order to satisfy the Shannon limits as compared with the other codes [1]. Turbo codes and LDPC codes is found to satisfy the Shannon limit. Apart from these codes, Polar codes is found to be an ultimate capacity-achieving code so it is used for next-generation 5G applications. It is also utilized in order to perform reliable data transmission.

Channel coding is employed to mitigate the occurrence of error. Generally encoding is an operation which transforms the original code into another code at the time of transmission. To recover the original information which is transmitted a decoding is required. The channel at which the information is transmitted can be any base station [2]. In polar codes, the information is transmitted at bit positions ‘0’ and ‘1’. If the information is sent at ‘1’ position then it guarantees the transmission of information and it is found to be unreliable if it is sent at ‘0’ position [3].

R. Kavipriya (✉) · M. Maheswari
K. Ramakrishnan College of Engineering, Tiruchirappalli, India
e-mail: kavipriya1096@gmail.com

M. Maheswari
e-mail: kousi.rhithi@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_108

Many efforts are done in order to implement polar code for encoding and decoding operation without increasing its complexity and robustness during transmission [4]. In the next chapter, we outline the survey of the various decoders. In the chapter III, the proposed polar decoding is implemented and its operation is explained in brief. In the last chapter, the simulated results are shown for the above-mentioned code.

2 Literature Survey

To reduce the complexity in the Successive Cancellation decoding algorithm the abandoned frozen bits are used so that it reduces 20% of its complexity without increasing the loss [5]. By reducing the redundancy, the complexity is also reduced. The pipelined architecture method is employed by performing the FFT operation so that the efficiency is high.

In the SC decoder, Merged Processing Element is employed since it reduces many conversions such as magnitude and sign conversions, thereby increasing the throughput [6]. The latency increases as the complexity is increased. In order to avoid that problem, the original decoding graph is diving into many small graphs to overcome various problems [7]. This problem can be further reduced by using multiple decision approach [8, 9].

To balance the latency of the adjacent stages, the processing elements are separated from each other and then combined together in Fast SSC decoding algorithm to optimize its critical path [10]. The frequency and the power consumption is also found to be reduced. To avoid the problem of reordering of the information bit butterfly diagram is preferred [11]. Since the decoder is directly placed at the router it can correct the error after decoding the bits [12].

In Successive cancellation List Decoding, a pruning technique is employed to overcome the time complexities and space complexities by using the Maximum Likelihood method of decoding [13].

3 Proposed System

The output of the encoder is applied as the input to the decoder and the resulting output will be the original information bit which undergoes various steps to avoid the leakage of the information. Figure 1 indicates the basic channel diagram of the polar code. The basic polar code channel is shown in Fig. 2.

The whole operation is subdivided into many small stages. The encoded output x0, x8 is applied as the input to A0 and x1, x9 is applied as the input to A1. Similarly x2 and x10 is applied as input to A2, x3 and x11 is applied as input to A3, x4 and x12 is applied as input to A4, x5 and x13 is applied as input to A5, x6 and x14 is applied as input to A6, x7 and x15 is applied as input to A7. The outputs is obtained by performing XOR operation and the process goes on.

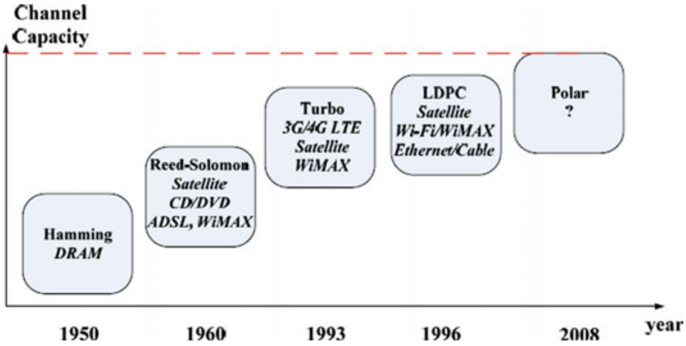
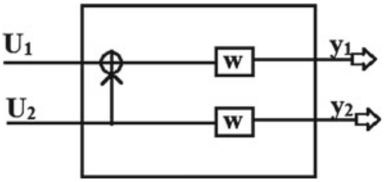


Fig. 1 Various coding techniques

Fig. 2 Basic polar code channel



The output of A0, A1, A2, A3, A4, A5, A6, A7 is applied as the input to stage 1 and it is denoted by w_{ij} where the edge is denoted by '*j*' and the stage is denoted by '*i*'. By performing the addition operation with the inputs A0 and A4, the output B0 is obtained. Similarly, by performing the subtraction operation of the above inputs, the output B4 is obtained. The above operation is repeated with the input values A1 and A5 from the previous value obtained to generate B1 and B5 which is obtained by performing addition operation and subtraction operation. Likewise, with the inputs A2, A3, A6, A7, the corresponding outputs B2, B3, B6, and B7 are obtained. Stage 1 output is applied as the input to stage 2 for processing.

The outputs of stage1 is multiplied with the complex coefficients W_N^K before passing as the input to stage 2. The complex coefficients W_N^K is also known as phase factors or twiddle factors which can be calculated by using the formula as shown below,

$$W_N = \mathrm{e}^{-j2\pi/N} \tag{1}$$

The values of phase factors W_8^0 is found to be 1, W_8^1 is found to be 0.707 + j0.707, W_8^2 is found to be j. Similarly W_8^4 is found to be −0.707 + j0.707. The output A4 is multiplied with W_8^0 and the corresponding value is applied as the input to stage 2. Similarly A5, A6, and A7 is multiplied with W_8^1, W_8^2, W_8^3 to generate the corresponding outputs. Figure 3 represents the data flow graph of polar decoding.

In the second stage, the values which are obtained after performing multiplication operation with the multiplier coefficients is applied as the input, i.e., the output C0

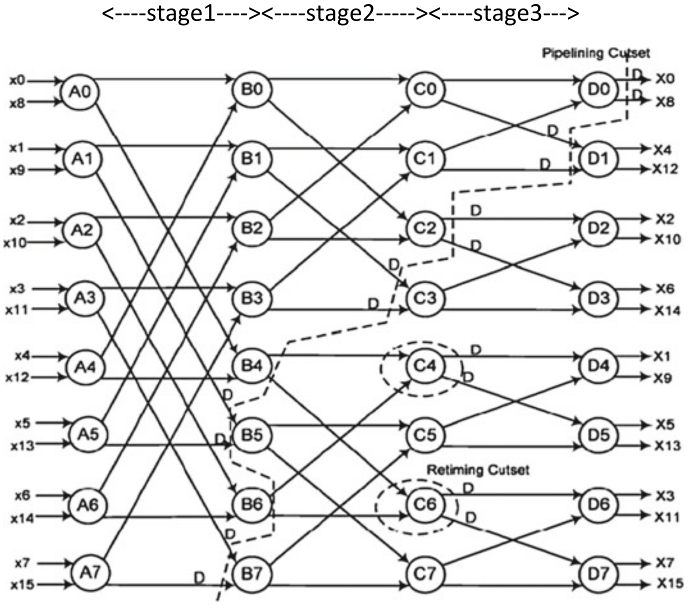


Fig. 3 Data flow graph of polar decoding

is obtained by performing addition operation with the inputs B0 and B2, the output C2 is obtained in a similar manner by performing subtraction operation instead of addition operation. The outputs C1 and C3 is obtained by performing addition and subtraction operation with the inputs B1 and B3. The operation which is performed with the first four information bits are repeated to generate C4, C5, C6, C7 but with the different input values B4, B5, B6, B7.

The outputs obtained in the second stage is then multiplied with the complex coefficients before passing to next stage for processing. The output C2 and C3 is multiplied with the twiddle factors W_8^0 and W_8^1 and then passed to next stage for processing. Similarly, C6 and C7 is multiplied with W_8^0 and W_8^1. The phase factors comprises of complex values and so the output will be the combination of both the real and the imaginary values.

The output of stage 2 is then applied as the input to stage 3. D0 is obtained by performing addition operation with the inputs C0 and C1, D1 is obtained by performing the subtraction operation with the same inputs shown above. The above process is repeated with different inputs such as C2, C3, C4, C5, C6 and C7 to generate the outputs D2, D3, D4, D5, D6, and D7.

The entire process is divided into various stages and the operation of next stage depends upon the previous stage values, therefore a register is needed in order to store the values. The final decoded outputs are generated in the normal order which is then divided by N to generate the decoded values. The above process is said to be decoding process which increases the security during the transmission through the channel.

4 Results and Discussion

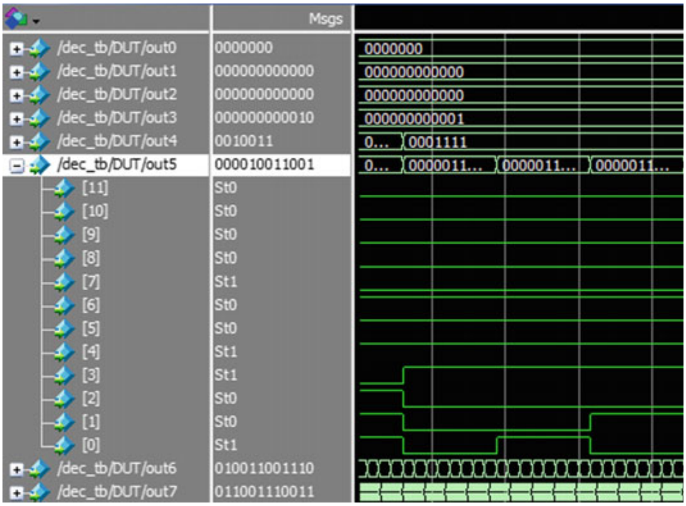
In this chapter, the proposed system simulation results are outlined. The process is simulated with various inputs and the related outputs are obtained. The inputs is of 7 bits for out0 and out4 and 12 bits for out1, out2, out3, out5, out6, out7. The input information bits are shown in the Fig. 4,

The decoder accepts the inputs in the bit reversed order and generates the associated outputs in natural order (i.e.) the order is found to be the same as the input values. The 12-bit information is decoded by using the polar decoding scheme and the corresponding outputs are generated.

The proposed decoding scheme is implemented in Model Sim version 10.4a software. To generate the synthesis report it is also implemented in Xilinx ISE (Integrated Synthesis Environment) Software. It provides various information regarding the utilization of logic gates and the number of slice LUTs and bonded IOBs. The outputs of the proposed system, i.e., decoding operation are shown in Fig. 5.

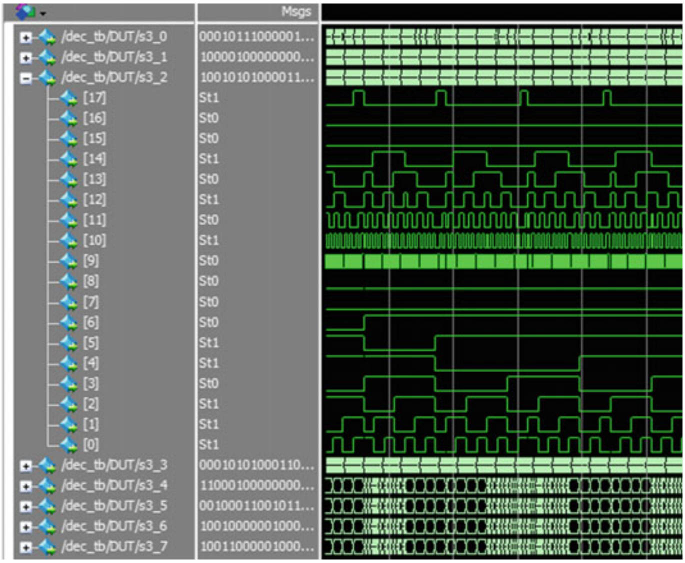
The synthesis report of the proposed system which comprises of the number of slice LUTs and number of bonded IOBs is shown in Table 1.

The Maximum combinational path delay for the proposed decoder system is 48.646 ns. The memory consumption of the proposed decoding process is 265,712 kilobytes.



```
                        Msgs
/dec_tb/DUT/out0        0000000
/dec_tb/DUT/out1        000000000000
/dec_tb/DUT/out2        000000000000
/dec_tb/DUT/out3        000000000010
/dec_tb/DUT/out4        0010011
/dec_tb/DUT/out5        000010011001
    [11]                St0
    [10]                St0
    [9]                 St0
    [8]                 St0
    [7]                 St1
    [6]                 St0
    [5]                 St0
    [4]                 St1
    [3]                 St1
    [2]                 St0
    [1]                 St0
    [0]                 St1
/dec_tb/DUT/out6        010011001110
/dec_tb/DUT/out7        011001110011
```

Fig. 4 Inputs generated before decoding



```
                          Msgs
/dec_tb/DUT/s3_0          00010111000001...
/dec_tb/DUT/s3_1          10000100000000...
/dec_tb/DUT/s3_2          10010101000011...
  [17]                    St1
  [16]                    St0
  [15]                    St0
  [14]                    St1
  [13]                    St0
  [12]                    St1
  [11]                    St0
  [10]                    St1
  [9]                     St0
  [8]                     St0
  [7]                     St0
  [6]                     St0
  [5]                     St1
  [4]                     St1
  [3]                     St0
  [2]                     St1
  [1]                     St1
  [0]                     St1
/dec_tb/DUT/s3_3          00010101000110...
/dec_tb/DUT/s3_4          11000100000000...
/dec_tb/DUT/s3_5          00100011001011...
/dec_tb/DUT/s3_6          10010000001000...
/dec_tb/DUT/s3_7          10011000001000...
```

Fig. 5 Proposed decoder output

Table 1 Synthesis report

Logic utilization	Used	Utilization (%)
Number of slice LUTS	1836	20
Number of bonded IOBs	230	123

5 Conclusion

The decoding complexity should be considered while decoding the information bits since it can change based on various parameters. The complexity varies based on the encoding outputs and the code length. In our proposed system, to overcome these kind of problems the encoded outputs are checked before decoding and if there is no occurrence of imaginary part then there is no need for usage of multiplier coefficients. Therefore, the memory requirement is reduces which in turn speeds up the performance. The proposed system is implemented using Model Sim 10.4a Software and its synthesis is done using Xilinx ISE Suite 14.7.

References

1. Srinath P, Samuel John J (2016) Implementation of parameter based partially parallel encoder architecture for long polar codes. IJARECE 5(10), October
2. Robert G, Maunder CTO (2018) The implementation challenges of polar codes. AccelerComm, February

3. Korada SB, Sasoglu E, Urbanke R (2010) Polar codes: characterization of exponent bounds, constructions. IEEE Trans Inf Theor 56(12):6253–6264
4. Condo C, Land I, Biogloi V (2018) Design of polar codes in 5G new radio. arXiv:1804.04389v2[CS.IT]
5. Liu A, Zhang Q, Yi X, Liang X (2017) A reduced complexity successive cancellation decoder of polar codes. In: 3rd international conference on computer and communications
6. Babu GS, Madala LR, Gopalakrishnan L, Sellathurai M Low complex processing element architecture for successive cancellation decoder. Integr, VLSI J
7. Viterbo E, Vangala H, Hong Y (2014) A new multiple folded successive cancellation for polar codes. In: IEEE information theory workshop (ITW)
8. Yuan B, Parhi KK Low-latency successive-cancellation list decoders for polar codes with multibit decision. IEEE Trans Very Large Scale Integr (VLSI) Syst
9. Gross WJ, Leroux C, Raymond AJ, Sarkis G (2001) A semi-parallel successive- cancellation decoder for polar codes. IEEE Trans Sig Process 61(2):289–299
10. Cui J, Zeng Q, Higgs R, Yan X, Zhang X (2018) High throughput fast SSC polar decoder for wireless communication. Wireless Mobile Computing
11. Duhamel P (1986) Implementation of split-radix FFT algorithms for complex, real and real-symmetric data. IEEE Trans Acoust Speech Sig Process (ASSP) 34(2)
12. Maheswari M, Murugeshwari B (2018) Random and triple burst error correction code with low redundancy for network-on-chip link. In: International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, 4–6 Jan 2018
13. Lin J, Chen K, Niu K (2013) Improved successive cancellation decoding of polar codes. In: IEEE transactions on communications, 61(8)

PAPR Reduction in F-OFDM Modulation Scheme for 5G Cellular Networks Using Precoding Technique

Sasidharan Jiji and M. Ponmani Raja

Abstract The emerging 5G system has promising advances in the near future. The 5G system will be offering many features that are not being possessed in the past generations. To meet the several requirements, orthogonal frequency division multiplexing (OFDM) is a best choice. In the existing OFDM technique, model and framework of 4G LTE, chosen mainly for mobile broadband (MBB) service, are not that sensitive to recession or authenticity. Despite the fact that OFDM provides high spectrum efficiency through orthogonal frequency multiplexing, the OOBE (out-of-band emission) of OFDM is still not very satisfactory, and also, OFDM requires global synchronization which comes at the price of extra signaling. Indeed, when the user is perfectly synchronized both in time and frequency domain with the base station (BS), in terms of bit error rate (BER), the performance offered by OFDM is very good and resistance to the carrier frequency offset (CFO). These circumstances are energy costly as the user needs to exchange messages with the BS to ensure this synchronization. Therefore, if these conditions are not satisfied, the OFDM BER may be high. Nevertheless, the OFDM modulation suffers from high side lobes which decrease the spectral efficiency and create adjacent channel interferences. For these reasons, several MCM schemes have been developed these recent years as candidates for 5G systems such as filtered OFDM (F-OFDM). Filtered OFDM (F-OFDM) is an alternative to the OFDM modulation in 5G system. It offers all the advantages maintained by OFDM such as efficient performance and flexible frequency multiplexing that meets the needs of future generation. It also meets OOBE requirements and thus helps in efficient spectrum utilization.

Keywords Adjacent channel interference (ACI) · Bit error rate (BER) · Complementary cumulative distribution function (CCDF) · Cyclic prefix (CP) · Fast Fourier transform (FFT) · Filtered orthogonal frequency division multiplexing (F-OFDM) · Inter-channel interference (ICI) · Inter-symbol interference (ISI) ·

S. Jiji (✉) · M. Ponmani Raja
Electronics and Communication Engineering, Jyothi Engineering College, Thrissur, India
e-mail: jijisasidharan95@gmail.com

M. Ponmani Raja
e-mail: ponmani@jecc.ac.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_109

Inverse fast Fourier transform (IFFT) · Orthogonal frequency division multiplexing (OFDM) · Out-of-band emission (OOBE) · Peak-to-average power ratio (PAPR) · Power amplifiers (PA) · Power spectral density (PSD)

1 Introduction

Nowadays, the field of multimedia wireless communication is growing rapidly which influences the life of people creating unstoppable demands and needs that increase day by day. People are in search of a technology that is faster than the current generation, which has very high-speed transmission rates, and supports mobility and efficient utilization of the network resources and available spectrum. The current modulation scheme used in 4G system is orthogonal frequency division multiplexing (OFDM), and it is one of the best solutions to achieve these goals. OFDM is having high spectral utilization. The basic method is encoding digital data on multiple carrier frequencies. It improves the bandwidth efficiency and effectively combats the multipath fading channel. At the same time, to provide a reliable transmission, it increases the system capacity. In OFDM, it first splits the high-rate data stream into a number of lower rate data streams which are then transmitted simultaneously over a number of subcarriers. These subcarriers are overlapped with each other and are orthogonal, where each frequency channel is modulated with simpler modulation scheme. However, it introduces inter-symbol interferences (ISI) and inter-channel interferences (ICI). ISI is the effect of adjacent symbols, whereas ICI is the effect exerted by the subcarriers. In order to reduce the effect of ISI and ICI, we introduce a guard interval in between the OFDM symbols.

One of the major drawbacks in OFDM is that a very high peak-to-average power ratio (PAPR) is being exhibited by the composite transmit signal when the input sequences are highly correlated. Corresponding to different phase values, the signal will be having different values with respect to each other. The output symbol will be having peak points in the overall envelope, when all the points achieve the maximum value simultaneously. The uneven peaks in the OFDM system occur due to the signal distortions. The presence of large number of subcarriers makes the peak values very high. Peak-to-average power ratio is defined as the ratio of the peak power to average power value of the system. PAPR and bandwidth efficiency are directly proportional, i.e., when the number of subcarriers increases PAPR, it also increases the bandwidth efficiency. Thus, a reduction of PAPR affects the efficiency of the system being very crucial situation.

We are aiming for a new generation (5G) in mobile communication which will be providing us with the new features that were not employed in 4G generations. The main application will be provided by it are divided into three major categories: enhanced mobile broadband (eMBB), ultra-reliable and low-latency communication (URLLC), massive and machine-type communication (mMTC). [1] Figure 1 depicts the applications of 5G [1].

The properties that an ideal waveform should have are the following [1]:

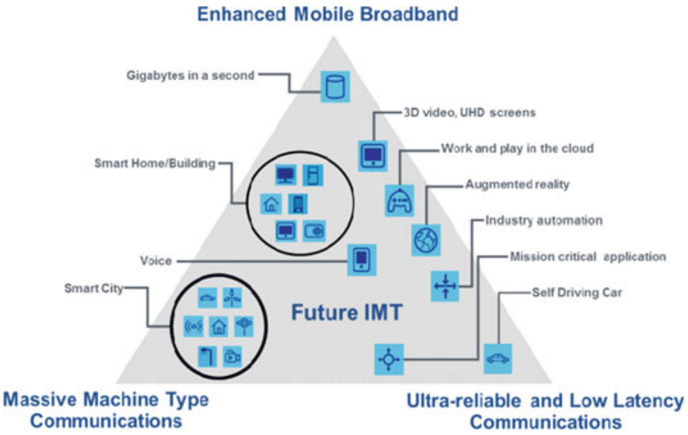

Enhanced Mobile Broadband
Gigabytes in a second
3D video, UHD screens
Work and play in the cloud
Smart Home/Building
Augmented reality
Industry automation
Mission critical application
Voice
Self Driving Car
Smart City
Future IMT
Massive Machine Type Communications
Ultra-reliable and Low Latency Communications

Fig. 1 Future applications of 5G [1]

- **Low complexity**—low-cost transceivers are needed for machine-type communication (MTC); thus, low complexity should be maintained.
- **Good spectral containment**—the use of guard bands in between the OFDM symbols may affect the spectrum utilization; thus, spectrum for each service must be efficiently utilized.
- **Carrier frequency offset (CFO)**—CFO at the receiver can be amplified by the use of poor oscillators; thus, it will be robust against CFO.
- **Support multiple input multiple output (MIMO)**—MIMO is the best technology for the future since spatial multiplexing is a multiple antenna technique; as compared to single antenna techniques, it increases the data rate.
- **Time localization**—a well-localized waveform in time domain is needed for fulfilling the demand of low latency.
- **Flexible numerology**—in order to satisfy different traffic types, a flexible waveform is needed.

From these benefits, it is clear why OFDM can be considered for future generation. Even though there are several benefits of OFDM, there also exist several limitations which enable the generation of a new modulation scheme that can efficiently satisfy the requirements for an efficient future generation (5G). Several limitations of OFDM systems are as follows [1]:

- **Sensitivity to frequency and time offset**: Due to CFO and Doppler effect, several impairments occur. Similarly, if the signals are not synchronized well, then it will result in fading and irregularities of signals; hence, synchronization is an important factor.
- **Cyclic prefix overhead**: The addition of cyclic prefix to reduce the interferences in the symbol results in overhead in the transmission and performance degradation.

- **Large peak-to-average power ratio (PAPR)**: Larger PAPR occurs due to alterations or signal distortions which will result in unwanted peaks in the resulting signal; this will degrade the performance and efficiency of the system.
- **Large out-of-band emissions (OOBE)**: In time domain, each OFDM symbol has a shape of rectangular pulse which seems as a sinc function in the frequency domain. Therefore, it results in a bad spectral behavior as the OOBE falls very slowly and imposes the need for large guard.

From the limitations listed above, we can understand that the OFDM cannot provide an efficient performance in the future 5G systems. However, we can think of making use of the advantages offered by OFDM to produce a new modulation scheme. The main goal of this paper is to provide a new waveform that imposes all the advantages of OFDM and at the same time introduces an efficient technique to reduce the demerit of high PAPR in it. In [2–9], we can see the several techniques used in modulation techniques in several channels. It will provide us with a detailed study of related works in the field of OFDM.

In Section I, we have given a brief introduction of the paper. In Section II, the literature survey related to the topic is being done. Section III mainly focuses on the proposed methodology, and finally, section IV concludes the paper with corresponding results.

2 Related Work

In [10], Vipul D. Sahni, Nitesh Kumar, and Vishal Narain Saxena had discussed about several hybrid techniques for reducing the high PAPR in OFDM. Four main techniques like

(1) *Precodings with repeated clipping and frequency domain filtering (RCF).*
(2) *Companding techniques along with RCF.*
(3) *Repeated frequency domain filtering and clipping (RFC) along with companding.*
(4) *Precodings along with companding.*

are being introduced in their work. From that, they are concluding that precoding has been considered better among all these techniques, because it improves the PAPR without increasing more complexity and without hindering with the orthogonality between subcarriers. It also increases the BER performance in comparison with other stated hybrid methods because of diversity gain.

In [11], Dan Wu, Xi Zhang, Jing Qiu, Liang Gu, Yuya Saito, and Anass Benjebbour discuss that to enable flexible waveform for 5G and improve the spectrum utilization, a new modulation scheme, named filtered OFDM (F-OFDM), is being introduced. In that work, they have mainly discussed about the filter design and its implementation. In this work, they have recommended the use of sinc filter design for F-OFDM. According to their results, they are concluding that the F-OFDM is having more efficiency than OFDM which is currently being used. F-OFDM enhances spectrum efficiency over the conventional OFDM by providing a reduced spectrum leakage.

In [12], Qiwei Zheng, Fanggang Wang, Xia Chen, Yinsheng Liu, Deshan Miao, and Zhuyan Zhao focus on performance evaluation of waveforms in the fifth generation, i.e., universal-filtered multicarrier technique (UFMC), resource block-filtered orthogonal frequency division multiplexing (RB-F-OFDM), filtered OFDM (F-OFDM), and filter bank multicarrier (FBMC) in high-speed scenarios. With respect to signal-to-noise ratio (SNR), terminal speed, and carrier frequency offset (CFO), the block error rates (BLERs) of the channel model of tapped-delay-line-D (TDL-D) defined in 3GPP TR 38.900 are evaluated. Simulation results indicate that RB-F-OFDM is recommended for high-speed scenario due to the robustness in terms of high mobility and CFO. Main disadvantage is the high peak-to-average power ratio. A single-input and single-output (SISO) system is considered; here, the principle of filtering-based waveforms UFMC, RB-F-OFDM, F-OFDM, and FBMC are proposed for future 5G and compared their performance in high-speed scenario, using the TDL-D channel model in 3GPP TR 38.900. Simulation results show that RB-F-OFDM outperforms other waveforms in terms of high mobility and robustness against ISI and CFO.

In [13], Lei Zhang, Ayesha Ijaz, Pei Xiao, Mehdi Molu, and Rahim Tafazolli propose that F-OFDM system is an efficient modulation scheme for 5G system. In their work, they are concentrating on the mathematical model of F-OFDM, and then, they have discussed about how to reduce the interferences in the system, thus leading to equalization. Then, they aimed on reducing the computational complexity of the system. The efficient obtained results reduce the computational complexity of the subcarriers.

From the above discussed works, we can conclude that F-OFDM is an efficient modulation scheme for efficient communication of the future generations. There still persists the demerit of high peak-to-average power ratio. From [10], it is clear that the efficient technique for reducing the high PAPR in OFDM is precoding technique; thus, we can implement the precoding technique for reducing the PAPR in F-OFDM.

3 Proposed Work

In order to fulfill the need for 5G cellular communication, we are hereby implementing a new modulation scheme F-OFDM. Basic difference between the OFDM and F-OFDM is that there is filtering at both the transmitter and the receiver sections. The block diagram of F-OFDM is given in Fig. 2.

In filtered OFDM (F-OFDM), a filtering algorithm is used after the IFFT/cyclic prefix of OFDM system; the entire assigned bandwidth is first divided into several sub-bands. In each sub-bands, the different services are being accommodated as per the requirements. Compared to conventional OFDM technique, the F-OFDM provides throughput gain. Significant reductions on usage of guard band are also being offered in F-OFDM which leads to more efficient spectrum utilization. Even

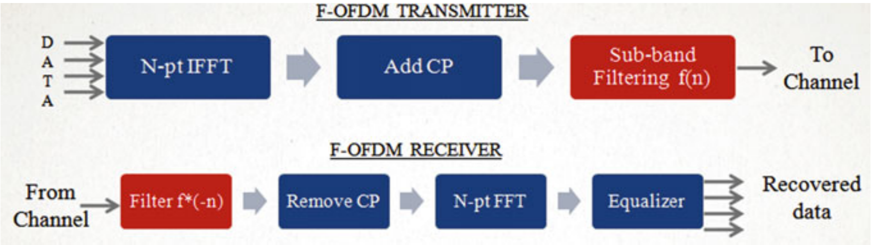


Fig. 2 Block diagram of F-OFDM

though it is having several advantages, still a demerit that is high PAPR which will affect the performance of the system persists. Thus, as per [10], we are proposing a precoding-based technique to reduce the PAPR in F-OFDM modulation scheme.

3.1 Filter Design

F-OFDM should satisfy certain criteria for achieving appropriate filtering. It includes flat passband, sharp transition band, and sufficient stop-band attenuation. Thus, these criteria can be fulfilled by using a filter with a rectangular frequency response, i.e., a sinc impulse response; hence, a soft truncated filter with specific window is recommended to achieve the appropriate filtering in F-OFDM. This in turn will create a trade-off between time and frequency localization (i.e., ISI and ICI). It is an easy implementation for flexible sub-band configuration. From Fig. 2, we can see that in F-OFDM, the input signal is first sent to the N-point IFFT which is a serial-to-parallel converter, and then, it is added with cyclic prefix to reduce the interferences in the symbol. After that, we are applying designed filtering to the system. This is the transmitter section; output from filtering is being sent through the channel to the receiver and a similar filtering is being applied at the receiver part. Then, the reverse operation of transmitter part is being employed at the receiver such as removal of cyclic prefix followed by N-point FFT; then finally, equalization is being employed. The filtering algorithm employed enables the spectrum efficiency, improves latency, and reduces the out-of-band emission. Even though F-OFDM has all the advantages of OFDM, still there persists the high PAPR ratio. Thus, to reduce the PAPR, we can use the precoding technique [10] which is very efficient. From the papers [10, 14–20], we can get a detailed comparison of several techniques for reduction of PAPR in OFDM, and from that, we can understand that a very efficient technique for PAPR reduction is precoding technique.

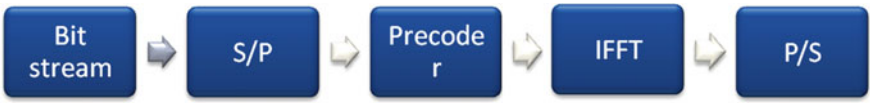


Fig. 3 Basic block diagram of precoding technique

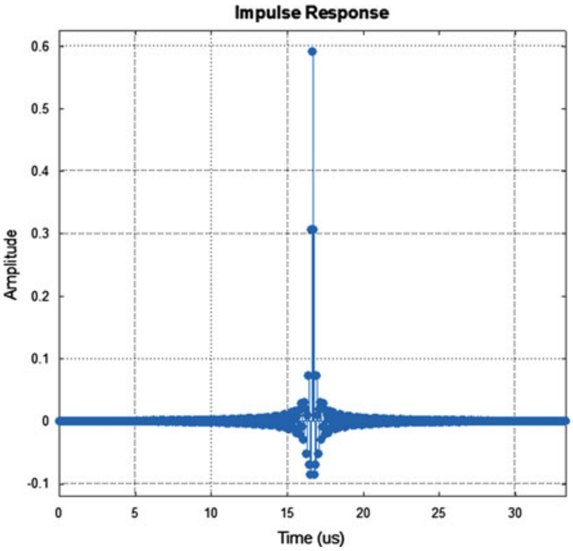
3.2 Precoding Technique

In precoding technique, we will multiply the modulated symbols of OFDM and F-OFDM with the precode matrix before IFFT block, and this precode matrix P is of a dimension of $L \times N$ where $L = N + N_{\text{p}}$, N is the number of baseband modulated signals, and overhead subcarriers as $0 \leq N_p < N$. When an input matrix 'x' is multiplied to a precoding matrix P, then the output Y will be $Y = P \otimes X$. Figure 3 implies the block diagram of precoding technique. It depicts that the precoder is being used after the serial-to-parallel converter and before the IFFT block. The transpose of the precoding matrix is being multiplied to the receiver part in precoding technique. From [20] & [21] we can find the precoding technique beings depicted on ofdm modulation scheme along with companding technique.

4 Result Analysis

In Fig. 4, we can see the impulse response of the rectangular pulse sinc filter used in F-OFDM. Figure 5 depicts the power spectral density of OFDM and F-OFDM. Table 1 depicts the values of parameters being used in this modulation technique. In

Fig. 4 Impulse response of sinc filter



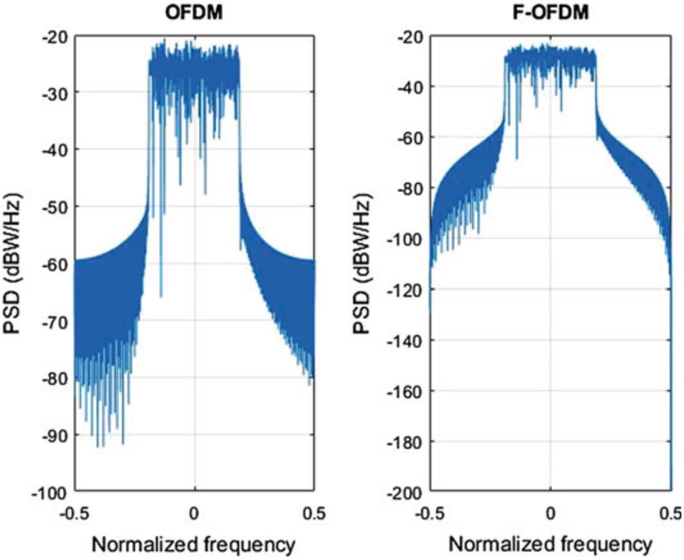


Fig. 5 PSD of OFDM and F-OFDM

Table 1 Parameters required in the modulation schemes

Parameters	Values
Number of FFT points	1024
Number of resource blocks	50
Number of subcarriers per resource block	12
Cyclic prefix length	72
Modulation	64 QAM
Channel model	AWGN
Filter length	513
Tone offset or excess bandwidth (in subcarriers)	2.5

Fig. 6, we can see the CCDF plot of PAPR for F-OFDM and OFDM before applying precoding technique, whereas Fig. 7 depicts the CCDF plot of PAPR for F-OFDM and OFDM after applying precoding technique. Table 2 shows the results of PAPR in both OFDM and F-OFDM before applying precoding technique and after applying precoding technique.

Comparing the plots of the spectral densities for OFDM and F-OFDM schemes, we can see that F-OFDM has lower side lobes that allow a higher utilization of the allocated spectrum, hence leading to increased spectral efficiency. It also depicts that the OOBE is reduced in F-OFDM as compared to the OFDM.

From Table 2, it is very clear that the PAPR for OFDM is very large compared to F-OFDM even after applying precoding technique; thus, F-OFDM is an efficient mechanism for 5G systems.

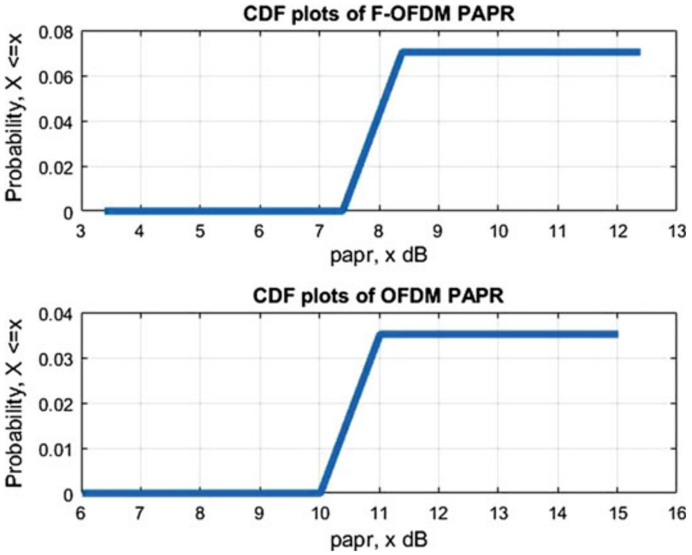


Fig. 6 CCDF plot of PAPR for OFDM and F-OFDM without precoding technique

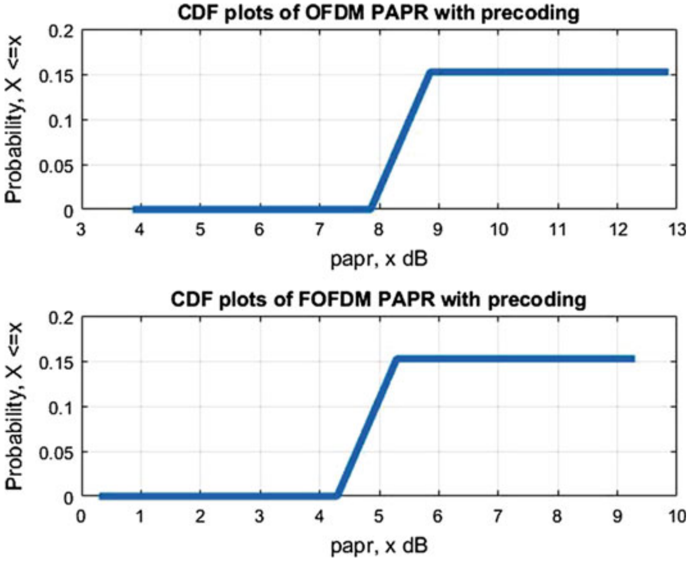


Fig. 7 CCDF plot of PAPR for OFDM and F-OFDM with precoding technique

Table 2 Final values of PAPR in dB

Parameter	Value in dB
PAPR of OFDM without precoding	11.0173
PAPR of F-OFDM without precoding	8.3904
PAPR of OFDM with precoding	8.8571
PAPR of F-OFDM with precoding	5.2942

Figures 8, 9, 10, and 11 depict the BER versus SNR in dB plots. BER values range in between 10^{-2} and 10 which is an optimum value for efficient transmission rates.

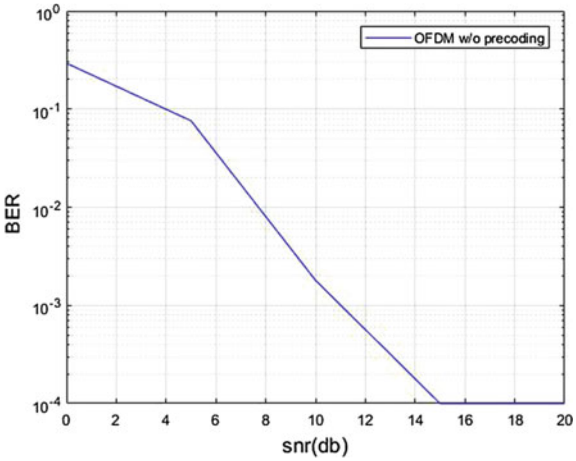


Fig. 8 BER V/S SNR plot of OFDM without precoding technique

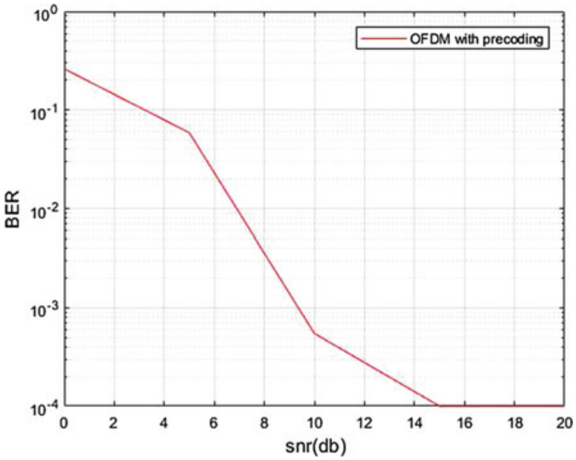


Fig. 9 BER V/S SNR plot of OFDM with precoding technique

Fig. 10 BER V/S SNR plot of F-OFDM without precoding technique

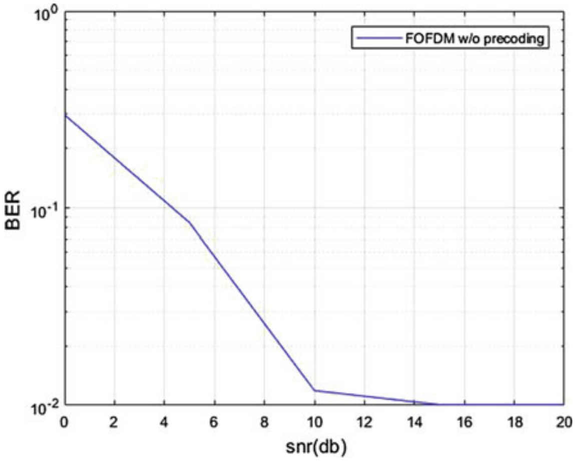
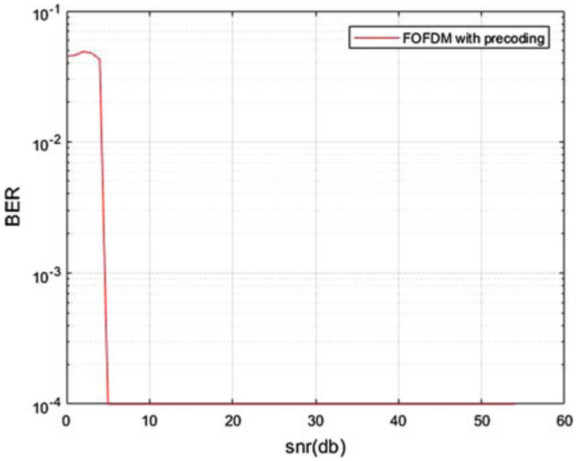


Fig. 11 BER V/S SNR plot of F-OFDM with precoding technique



References

1. Kodheli O OFDM-based schemes for next generation wireless systems. PhD diss.
2. Larsen Y, Leus G, Giannakis GB (2004) Constant modulus and reduced PAPR block differential encoding for frequency-selective channels. IEEE Trans Commun 52(4):622–631
3. Kim Y-J, Kwon U-K, Seol D-Y, Im G-H (2009) An effective PAPR reduction of SFBC-OFDM for multinode cooperative transmission. IEEE Sig Process Lett 16(11):925–928
4. Wang C-L, Ku S-J, Yang C-J (2010) A low-complexity PAPR estimation scheme for OFDM signals and its application to SLM-based PAPR reduction. IEEE J Sel Top Sig Process 4(3):637–645
5. Sohn I (2014) A low complexity PAPR reduction scheme for OFDM systems via neural networks. IEEE Commun Lett 18(2):225–228
6. Lasya PR, Kumar MS (2015) PAPR and out-of-band power reduction in OFDM-based cognitive radios. In: 2015 International conference on Signal Processing and Communication

Engineering Systems (SPACES). IEEE

7. Ogunkoya FB, Popoola WO, Shahrabi A, Sinanovi'c S (2015) Performance evaluation of pilot-assisted PAPR reduction technique in optical OFDM systems. IEEE Photonics Technol Lett 27(10):1088–1091
8. Khan MA, Rao RK (2016) Low-complexity PAPR reduction technique for OFDM systems using biased subcarriers. Can J Electr Comput Eng 39(1):19–25
9. Hossain MS, Shimamura T (2016) Low-complexity null subcarrier-assisted OFDM PAPR reduction with improved BER. IEEE Commun Lett 20(11):2249–2252
10. Sahni VD, Kumar N, Saxena VN (2016) Novel hybrid technique (s) for PAPR reduction in OFDM systems. In: 2016 International Conference on Signal Processing and Communication (ICSC). IEEE
11. Wu D, Zhang X, Qiu J, Gu L, Saito Y, Benjebbour A, Kishiyama Y (2016) A field trial of f-OFDM toward 5G. In: 2016 IEEE Globecom Workshops (GC Wkshps), pp 1–6
12. Zheng Q, Wang F, Chen X, Liu Y, Miao D, Zhao Z (2017) Comparison of 5G waveform candidates in high speed scenario. In: General assembly and scientific symposium of the international Union of Radio Science (URSI GASS), 2017 XXXIInd. IEEE
13. Zhang L, Ijaz A, Xiao P, Molu MM, Tafazolli R (2018) Filtered OFDM systems, algorithms, and performance analysis for 5G and beyond. IEEE Trans Commun 66(3):1205–1218
14. Ermolova N (2002) A comparison of two schemes for peak-to-average power ratio reduction in a multicarrier transmission. In: Proceedings of ICCSC'02. 1st IEEE international conference on circuits and systems for communications, 2002. IEEE
15. Xin Y, Fair IJ (2005) Low complexity PTS approaches for PAPR reduction of OFDM signals. In: 2005 IEEE International Conference on Communications, 2005. ICC 2005, vol 3. IEEE
16. Yang L, Chen RS, Siu YM, Soo KK (2006) PAPR reduction of an OFDM signal by use of PTS with low computational complexity. IEEE Trans Broadcast 52(1):83–86
17. Jiang T, Ni C, Guan L (2013) A novel phase offset SLM scheme for PAPR reduction in Alamouti MIMO-OFDM systems without side information. IEEE Sig Process Lett 20(4):383–386
18. Badran EF, El-Helw AM (2011) A novel semi-blind selected mapping technique for PAPR reduction in OFDM. IEEE Sig Process Lett 18(9):493–496
19. Sohn I, Kim SC (2015) Neural network based simplified clipping and filtering technique for PAPR reduction of OFDM signals. IEEE Commun Lett 19(8):1438–1441
20. Agarwal D, Sharan N, Raja MP, Agarwal A (2015) PAPR reduction using precoding and companding techniques for OFDM systems. In: 2015 International Conference on Advances in Computer Engineering and Applications (ICACEA). IEEE
21. Lakamana AS, Prasad AM (2016) An effective composite PAPR reduction technique of OFDM by using DFT precoding with piecewise linear companding. In: International Conference on Communication and Electronics Systems (ICCES). IEEE

Privacy Preservation Using Top K Multi-Keyword Synonym Fuzzy Search Scheme

Manjubala Sekar and Kamalanathan Kandasamy

Abstract Owing to the numerous advantages arising out of storing data in the cloud such as flexible costs, improved mobility, many users are outsourcing their data to the cloud. However, it poses security challenges and rigidity issues. The cloud is often honest but curious, and hence, the need to encrypt the data arises. However, it renders the basic processes like searching difficult. Hence, there is a need to implement search algorithms on encrypted data. Plaintext fuzzy search and semantic search techniques cannot be implemented on encrypted data. To save its resources, the cloud may return partially correct results, and thus, there is a need for verification of the results returned. Access control mechanisms for multiple users should be implemented ensuring the confidentiality of unauthorized data. This paper deals with the design and analysis of a privacy-preserving top k multi-keyword synonym/similarity fuzzy search.

Keywords Fuzzy search · Cloud computing · Privacy preserving · Synonym · Multi-keyword

1 Introduction

Advancements in cloud computing have made storing data in cloud a popular choice. Numerous benefits include reduced costs in provisioning whenever storage is needed and de-provisioning when it is not needed, reduction in data center footprint, availability of data anytime from anywhere and more. Cloud is of three types: public cloud, private cloud and hybrid cloud. Private cloud stores sensitive information, and hybrid cloud contains both public and private cloud services. Services provided by the cloud are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) and Recovery as a Service. IaaS provides pre-installed

M. Sekar (✉) · K. Kandasamy
Amrita Center for Cyber Security Systems & Networks, Amrita Vishwa Vidyapeetham, Amrita University, Kollam, Kerala, India
e-mail: manjubalasekar@gmail.com

K. Kandasamy
e-mail: kamalanathan@am.amrita.edu

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_110

and configured hardware through a virtualized interface. PaaS provides computing platform and solution stack in addition to IaaS services. SaaS and RaaS provide web-based applications and backup service, respectively.

However, storing data in a remote server is not fully secure. The cloud is honest but curious. Sensitive information must remain integral and confidential. Hence, the need to encrypt the data but processes like searching becomes difficult. The existing solutions are homomorphic encryption of the data, oblivious RAM and search encryption to search through encrypted data. Search encryption is so far the best approach. The traditional and secure method of searching was to extract all the files from the cloud, decrypt the files and conduct plaintext search on the decrypted files. This will be a waste of computation power, decryption of all the encrypted files.

Thus, we must employ techniques to search through encrypted data. There are three techniques, (i) search in the encrypted data (ii) secret sharing and (iii) index-based approach as discussed by Brinkman [1]. In the first approach, all the files and the keywords are encrypted, and the encrypted keyword is searched through every line of the encrypted files. In secret sharing method, the cryptographic secret is split into m secrets such that any n out of m secrets can be used to construct the original secret. In this context, for example, if 7 is the data and it is split among three owners as 32,5,11 and 7 is obtained by adding them and applying modulo 41 over them. In the index-based approach, keywords are extracted from the files before encryption, and secure index is constructed. Both the index and files are encrypted, and when a user sends a query, the keywords are encrypted, and a match is searched for in the index. This reduces search time in searching over the entire file documents.

The basic entities are data owner, data user and the cloud server. The data owner uses the key extraction algorithm to extract the relevant keywords. Then, he/she encrypts the keywords to form the secure index along with the file ids and send it to the cloud server. When the data user sends a search request, the query is encrypted, and if it matches with the keywords in the secure index, then the encrypted files corresponding to the file ids are returned to the user (Fig. 1).

The rest of the paper is organized as follows. Section 2 deals with the related work, Sect. 3 explains the methodology followed in this paper, and Sect. 4 provides the implementation details. The results of our experiments are given in Sect. 5 and followed by conclusion in Sect. 6.

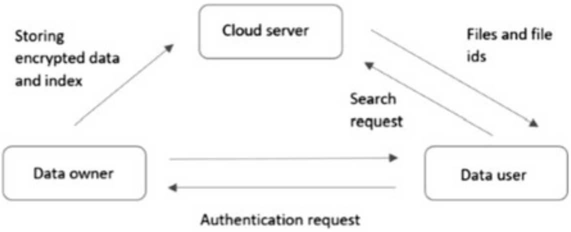


Fig. 1 Index-based approach general procedure

2 Related Work

Fuzzy Search: Since the data is encrypted along with keywords, a spelling mistake in the keyword will be encrypted to a different value and the search fails, i.e., there is no tolerance for typing errors. Words which originate from the same stem are also encrypted to different values, and the search fails unless the exact keyword is specified. In wild card-based approach [2], the possible fuzzy words are formed with a pre-defined edit distance. For example, the wild card fuzzy set of 'cloud' with edit distance 1 will be {*cloud, *loud, c*loud, c*oud, cl*oud, cl*ud, clo*ud, clo*d, clou*d, clou*, cloud*, cloud}. The possible combinations are n *2 +2 where n is the length of the keyword. In the K-gram-based approach [3–5], the keywords are split into k-grams and the encrypted individually in the index. A search query containing the same or almost similar keyword will have more k-grams in common. For example, the bi-gram representation of the word 'secure' is {se, ec, cu, ur, re}. Symbol-based trie-traverse search scheme [6] has trapdoors of the keywords mapped to a pre-defined symbol set, and it is inserted into trie-based tree where the root node is null. The keywords with the common prefixes are grouped together.

Another technique involving bloom filters and LSH is described as follows [5, 7]. This eliminates the need for a dictionary, and the index for each file is a bloom filter. Every keyword is converted into a bi-gram set. There are 26 *26 possible bi-grams, and the bit is set to one if a bi-gram is present. If there is a single spelling mistake, only two bi-grams will vary. The vector is then hashed using LSH from p-stable LSH family. This hashing ensures that two keywords with one letter difference are mapped to a hash value of almost similar value. This similarity is measured by Euclidean distance. The vector is then inserted into the bloom filter. The query is also generated in the same way. When the user sends a query, the inner product of the query and the index will give a high value as the vectors will be set to one in similar positions. This scheme also supports dynamic update, new files can be inserted, and files can be deleted as each file is indexed separately. The disadvantage of this scheme is false positives introduced by bloom filter which can be mitigated by setting a minimum threshold for the inner product and at the same time ensuring that the relevant files are not missed out.

In another fuzzy method, it is assumed that the user may omit, swap, include up to two characters maximum, and hence, the positioning of letters in the keyword can be moved up or down by a maximum of two [8]. The example for positioning in case of one letter addition, omission or swapping is as follows for the word 'secure' {s0, s1, e1, e2, e3, c2, c3, c4, u3, u4, u5, r4, r5, r6, e5, e6, e7}. When the position of 'c' comes in either second, third or fourth position, the letter is mapped like 'seecure.'

Semantic Search: In a query, certain keywords should be given higher importance, certain words are general terms, and some are specific. For example, if the query is 'blue pants,' it means pants are more generic to blue. First, the results containing pants should be found and narrowed down to blue pants. To understand and implement this, semantic relations must be studied, and search made on that basis. Synonym search is essential as users may search for files with different keywords but with the same meaning. For example, university/college both refer to a institution, and hence, both the words should form the keyword set for the files containing any one of the keyword. Improving fuzzy search [9, 10] instead of discarding the remaining elements or the fuzzy set of the keyword when the exact match succeeds, the trapdoors of the fuzzy set of the keyword are also formed to search for similar words.

Porter's stemming algorithm [5] is used to extract the root word from which the derivatives can be constructed, thus enabling more matches. For example, the root word of 'detected' will be 'detect,' and other words derived from the root word are 'detectable,' 'detects,' 'detecting,' 'detective.' The above words are then used to construct the keyword set with the root word as the head node. The assigning of keyword weights [11] will ensure the importance of a keyword in the search query, and thus, a higher score for the document containing keyword will be calculated. Conceptual hierarchy [12] is a tree-like structure where the leaf nodes will have a more specific meaning, and the nodes at the top will have a general meaning. E.g., 'college,' 'institution,' 'university' will occupy the higher level of nodes, and 'Amrita school of engineering' and 'Kollam' will occupy the lower level of nodes. Another method is applying sentence scoring followed by conceptual graphs [13]. First, the most relevant sentence is extracted from the document known as sentence scoring. A conceptual graph consists of objects and relations, and every object is connected to another object by a relation.

Preserving Privacy: Apart from encrypting the data in the files, it is also necessary to protect the privacy of the keywords and other statistical data associated. Else, the cloud will be able to deduce which set of files are accessed more frequently and which files are sensitive. The keyword is split [14, 15] into two and then encrypted such that even when the attacker obtains the trapdoor, he/she will not be able to determine the keyword. Smaller keywords will be subjected to keyword guessing attack, and hence, randomizing [16] and increasing the keyword length will secure it against keyword guessing attacks, and similarly, dummy keywords [17] are also introduced into the secure index. To protect against the cloud from determining the words in the encrypted files, the same keywords in various files are encrypted to different cyphertexts [18].

Verifiable Results: Since the cloud is not a trusted entity, the results returned by the server should be authenticated. Sometimes, to save its resources, the server may not complete its search process and may return partial results. Check mechanisms should be employed to ensure the authenticity of the data. In this challenge-based verification technique [19], the user composes a challenge from the returned results and sends it to the cloud. If the cloud can solve the challenge, thus verifying the authenticity of the ciphertext, the ciphertext is accepted by the user else, it is discarded.

In another random challenge technique [20], similarity scores are asked for any random documents. If the cloud has returned the top k results, the similarity scores of the random documents requested by the user should be less than the similarity scores of the top k documents. In this technique [21], a verifiability code is generated for each file based on the file and the similarity score. The cloud will return the set of files along with the VC code when a request has been made. The data user will reconstruct the VC from the file and the shared secret key and verify if it matches with the returned VC code.

Ranking of Results: When a user sends a query, certain results may be more relevant than some, and hence, the results should be ordered with the most relevant results at the top. Thus, the need for similarity score arises. The scores are usually calculated based on how unique yet frequent the word appears in the document relative to other documents. Some common algorithms are TF-IDF, Cosine similarity [22] and Co-ordinate matching.

Dynamic Update: The search index should facilitate dynamic update [7, 23] as new files might be added, and old files might be replaced and modified. This will lead to a change in keywords and similarity scores. Hence, the secure indices must support dynamic update.

Multi-user Access Control: There are two types KBAC and ABAC. KBAC assigns each file's decryption key directly to authorized users. ABAC attaches a set of attribute values to a user and designs access policy for a file. A file can be accessed if and only if the attribute values satisfy the access policy. Predicate encryption [24] is a very powerful technique for enforcing fine-grained access control where the owner of the ciphertext can provide partial keys to the users for decrypting partial data.

In this paper, LCS algorithm is applied initially followed by calculation of distance between the words returned to obtain the most relevant word (Fig. 2).

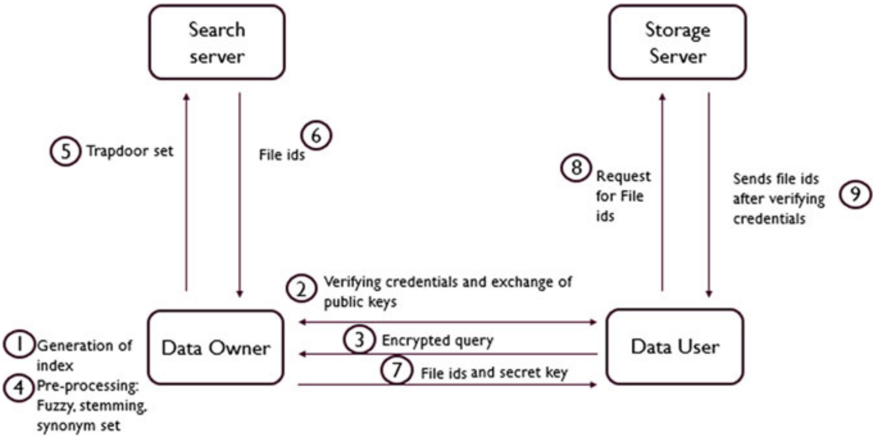

Search server
Storage Server
5 Trapdoor set
File ids 6
8 Request for File ids
Sends file ids after verifying credentials 9
2 Verifying credentials and exchange of public keys
3 Encrypted query
7 File ids and secret key
1 Generation of index
4 Pre-processing: Fuzzy, stemming, synonym set
Data Owner
Data User

Fig. 2 Architecture

3 Methodology

3.1 Model Description

The components are data owner, data user, search server and storage server. The data owner extracts all the keywords from the files and forms synonym/similar keywords. He/She forms a linked list of the keywords with the keyword found in the file at the top of each linked lists (dictionary). It will have m distinct keywords, and n is the highest number of elements in the synonym and fuzzy set of each keyword. The data owner extracts the frequency of the keywords from the data files as well. He/She encrypts the keyword and the frequency to form the secure index (trie-based structure) and sends it to the search server along with file ids. The file ids, encrypted files and the access control of each file are sent to the storage server. The data user encrypts his query using public key of the data owner and sends the query to the data owner. The data owner decrypts the query using his private key and tries to find a match in the dictionary. For fuzzy search, the LCS algorithm is used to find the edit distance between two words. If there is a match with any keywords, i.e., exact match or fuzzy match within the specified edit distance, trapdoors of the keyword, synonyms and similar words are computed and sent to the search server. The search server compares the trapdoors are compared with the index table, and the file ids are returned.

The top k results are obtained by calculating the frequency of the keywords using term frequency * inverted document frequency (TF*IDF). The files which have all the keywords of the query are at the top even if its individual frequencies are comparatively lesser than other files having higher frequency but not all the keywords of the query. The data user receives the file ids and sends the file ids to the storage server to obtain the encrypted files. The storage server sends the encrypted files that match with the file ids to the user after verifying the access controls of the user. The data user will decrypt the received file.

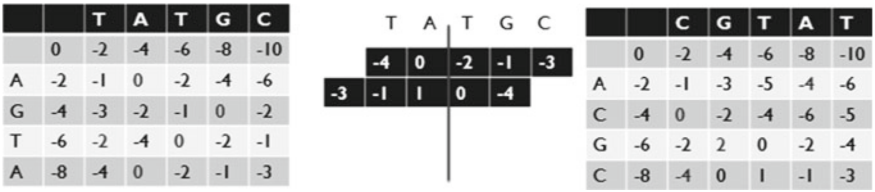
3.2 Assumptions

This model is applicable where there is a single owner like a corporate company where the company-related projects are to be made available to only its employees. Here, the encryption of keywords does not vary, i.e., the same keyword will be encrypted to the same value, and hence, the cloud may reduce the frequency of the encrypted keywords queried. Similarly, the cloud might deduce the files which are accessed frequently and form a relationship between the encrypted keywords and the encrypted files.

3.3 Algorithm Description

Hirschberg's Algorithm: This algorithm finds LCS of two strings in $O(mn)$ time complexity and $O(m + n)$ space by applying divide and conquer method. This follows the divide and conquer method where the strings are split recursively, and string comparison is done. In the above example, the strings are 'TATGC' and 'AGTACGCA' where the second string is split into two, and the following method is done to determine where to split the first string to obtain LCS sequence.

This algorithm saves space as it does not store the entire table but just two rows at any time. LCS algorithm is applied on the first half of the string as it is and applied on the reversed half of the second string as shown in the figure above. Here, it is assumed that if the characters match, a value if 2 is added, and if does not match, -2 is added in case of insertion and deletion and -1 in case of substitution. Whether a character must be inserted, deleted or substituted is done by comparing the diagonal, top and left values, and the minimum is taken for the operation, i.e., -2 is added if the top or left value is minimum, and -1 is added if the diagonal value is minimum. Finally, the last two rows are aligned, and the subsequent columns are added. The column which yields the minimum values is taken as the divider. Therefore, the LCS of the above two strings is TAGC (Figs. 3 and 4).



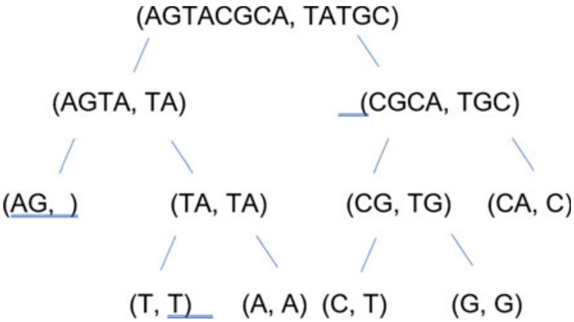
		T	A	T	G	C
	0	-2	-4	-6	-8	-10
A	-2	-1	0	-2	-4	-6
G	-4	-3	-2	-1	0	-2
T	-6	-2	-4	0	-2	-1
A	-8	-4	0	-2	-1	-3

	T	A	T	G	C
	-4	0	-2	-1	-3
-3	-1	1	0	-4	

		C	G	T	A	T
	0	-2	-4	-6	-8	-10
A	-2	-1	-3	-5	-4	-6
C	-4	0	-2	-4	-6	-5
G	-6	-2	2	0	-2	-4
C	-8	-4	0	1	-1	-3

Fig. 3 Hirschberg's algorithm

Fig. 4 Divide and conquer LCS algorithm output



4 Implementation Details

'Reuters-21578, Distribution 1.0' comprising over 20,000 documents (appeared on the Reuters newswire in 1987) was encrypted and used as a dataset and used Python. For the formation of the index, the keywords formed are nouns and noun-phrases. Stemming algorithm is applied to increase the match frequency. The ranking of the results is done based on TF-ID where

$$\mathrm{TF}-\mathrm{IDF}=\mathrm{TF}*\mathrm{IDF};$$

TF = Frequency of words in the text
IDF= 1/log $(1+p)$; $p=$ Total documents/Number of documents containing the keywords.

A split-keyword matrix structure as described in [6] is constructed with keywords, TF-IDF value and, the file ids. When a keyword is encrypted, the attacker can reconstruct the plaintext of the encrypted keyword by brute force. If it is split and encrypted, the attacker may not be able to reconstruct the keyword. For example, unive, 5, (0.2215879871480701, '1_49'), (0.4238681120052753, '1_49'), rsity, 5. The index is then encrypted using AES-CBC ad stored in the search server. The synonym set is formed using WorldNet, and it is the matrix containing the keyword present in the file in the first column followed by the synonyms. For the search process, the query to be sent to the owner is encrypted using the RSA algorithm. The received query is decrypted at the owner side, and pre-processing is done where fuzzy search, construction of synonym sets and stemming process. The trapdoor is formed and sent to the search server. The file ids of the matched trapdoor are returned from the search server, and the corresponding files are obtained from the storage server.

5 Results

The time taken for generating the search index was studied, and it is found to increase linearly as shown in the graph below. Using the TF-IDF algorithm is inefficient when the number of documents increases for every keyword, the whole document set must be checked.

Using an intermediate server to correct spelling mistakes and the formation of synonym set increases the accuracy rate. However, using the LCS algorithm has its disadvantages as explained below.

The algorithm described is inefficient in differentiating two words which are similar but semantically different. In the table below, it is shown that the distance between the actual word and the word that forms after applying LCS is the same. However, it is evident that the user meant to search for 'cloud.' It observed that the edit distance of the first entry is four compared to five in the second entry. Therefore,

Table 1 Disadvantage of LCS algorithm

Actual word	Entered word	Applying LCS
Cloud	Cluod	Clud
Loud	Cluod	lud

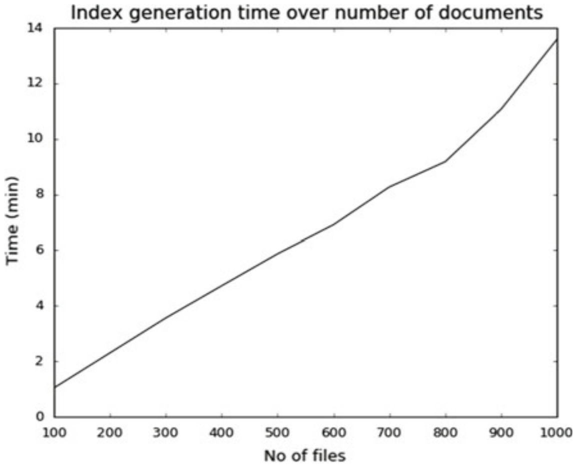


Fig. 5 Index generation time versus number of files

the results should be returned such that results related to 'cloud' to be returned first followed by results related to 'loud' (Table 1).

This can be improved by studying the edit distance between the words formed after applying the LCS algorithm and the entered word. It is observed that the difference is one in the first case and two in the second case. Hence, it can be concluded that the entered word was supposed to be 'cloud' and not 'loud' (Fig. 5).

6 Conclusion and Future Work

This system model improves fuzzy search and preserves privacy by the combination of split-keyword technique, and the query is transmitted after encrypting with RSA. The usage of two separate servers will prevent the cloud from forming a relationship between the search query and the files, and usage of the LCS algorithm followed by calculation of edit distance between the actual word and the returned words will return the most relevant result. The runtime of LCS algorithm can be improved by using Kuo-Cross algorithm whose runtime is $O((r + n) \log(n))$. In the future, this system will be modified to see if the cloud returns the correct results and enables multi-user access.

References

1. Brinkman R (2007) Different search strategies on encrypted data compared. Data-centric systems and applications. Security, privacy, and trust in modern data management, Part 3, pp 183–196
2. Li J, Wang Q, Wang C, Cao N, Ren K, Lou W (2010) Fuzzy keyword search over encrypted data in cloud computing. IEEE INFOCOM. San Diego, CA
3. Zhou W, Liu L, Jing H, Zhang C, Yao S, Wang S (2013) K-gram based fuzzy keyword search over encrypted cloud computing. J Softw Eng Appl 6(1):29–32
4. Wang D, Fu S, Xu M (2013) A privacy-preserving fuzzy keyword search scheme over encrypted cloud data. In: 2013 IEEE 5th international conference on cloud computing technology and science, Bristol, pp 663–670
5. Wang B, Yu S, Lou W, Hou YT (2014) Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud. In: IEEE INFOCOM 2014—IEEE conference on computer communications, Toronto, ON, pp 2112–2120
6. Raghavendra S, Girish S, Geeta CM, Buyya R, Venugopal KR, Iyengar SS, Patnaik LM (2015) IGSK: index generation on split keyword for search over cloud data. In: 2015 International Conference on Computing and Network Communications (CoCoNet), Trivandrum, pp 374–380
7. Fu Z, Wu X, Guan C, Sun X, Ren K (2016) toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement. IEEE Trans Inf Forensics Secur 11:2706–2716
8. Ahsan MAM, Chowdhury FZ, Sabilah M, Wahab AWBA, Idris MYIB (2017) An efficient fuzzy keyword matching technique for searching through encrypted cloud data. 2017 International Conference on Research and Innovation in Information Systems (ICRIIS), Langkawi
9. Wang C, Wang Q, Ren K (2011) Towards secure and effective utilization over encrypted cloud data. In: 31st international conference on distributed computing systems workshops, pp 282–286
10. Wang C, Ren K, Yu S, Urs KMR (2012) Achieving usable and privacy-assured similarity search over outsourced cloud data. IEEE INFOCOM, Orlando, FL, pp 451–459
11. Shen Z, Shu J, Xue W (2018) Preferred search over encrypted data. Front Comput Sci 12(3):593–607
12. Fu Z, Xia L, Sun X, Liu AX, Xie G (2018) Semantic-aware searching over encrypted data for cloud computing. IEEE Trans Inf Forensics Secur 13(9):2359–2371
13. Fu Z, Huang F, Sun X, Vasilakos A, Yang C (2016) Enabling semantic search based on conceptual graphs over encrypted outsourced data. In: IEEE transactions on services computing
14. Raghavendra S, Girish S, Geeta CM, Buyya R (2018) Split keyword fuzzy and synonym search over encrypted cloud data. Multimedia Tools Appl 77:10135
15. Li J, Wang Q, Wang C, Cao N, Ren K, Lou W (2009) Enabling efficient fuzzy keyword search over encrypted data in cloud computing. IACR Cryptology ePrint Arch 593
16. Ahsan MAM, Idna Bin Idris MY, Bin Abdul Wahab AW, Ali I, Khan N, Al-Garwi MA, Rahman AU (2018) Searching on encrypted e-data using Random Searchable Encryption (RanSCrypt) Scheme. Symmetry 10:161
17. Shen Z, Shu J, Xue W (2017) Keyword search with access control over encrypted cloud data. IEEE Sens J 17(3):858–868
18. Khan NS, Krishna CR, Khurana A (2014) Secure ranked fuzzy multi-keyword search over outsourced encrypted cloud data. In: 2014 International Conference on Computer and Communication Technology (ICCCT), Allahabad, pp 241–249
19. Miao Y, Ma J, Wei F, Liu Z, Wang XA, Lu C (2016) VCSE: verifiable conjunctive keywords search over encrypted data without secure-channel. In: Springer Science + Business Media New York
20. Wan Z, Deng RH (2018) VPSearch: achieving verifiability for privacy-preserving multi-keyword search over encrypted cloud data. In: IEEE transactions on dependable and secure computing, vol 15, issue no 6, pp 1083–1095, 1 Nov–Dec 2018

21. Dai H, Zhu X, Yang G, Yi X (2017) A verifiable single keyword top-k search scheme against insider attacks over cloud data. In: 2017 3rd international conference on Big Data Computing and Communications (BIGCOM), Chengdu
22. Fu Z, Sun X, Xia Z, Zhou L, Shu J (2013) Multi-keyword ranked search supporting synonym query over encrypted data in cloud computing. In: 2013 IEEE 32nd International Performance Computing and Communications Conference (IPCCC), San Diego, CA, pp 1–8
23. Xia Z, Wang X, Sun X, Wang Q (2016) A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. IEEE Trans Parallel Distrib Syst 27(2):340–352
24. Katz J, Sahai A, Waters B (2008) Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Smart N (eds) Advances in cryptology—EUROCRYPT 2008, EUROCRYPT

High-Speed Variable-Length Decoder Using Segmented Code book

Sujata Bhavikatti and R. M. Banakar

Abstract Various communication applications from Internet video streaming to video broadcasting require high-speed throughput variable-length code decoder. The fundamental techniques (parallelism and pipelining) used to improve the speed of algorithm cannot be applied to VLC decoder, due to variable length of symbol codes and due to no boundary defined between symbols. Considering the basic algorithm of VLC decoder, the speed of decoder is improved by reducing the processing time while identifying the code word and corresponding code length from lookup table. The rearrangement of code words in code book is proposed in this paper to minimize the time. For variable-length code of 17 bits, the proposed design depicts an improvement of 46% in speed compared to traditional single length code book.

Keywords VLC decoder · Code book · Lookup table

1 Introduction

The video from Internet, personnel devices, television, movies, etc., use compressed form of digital video. Video codec is the basic building blocks of various communication applications including health monitoring systems, defense services, and multimedia services. These applications crave for high resolution, high frame rate which necessitates larger bandwidth. Video compression is essential to reduce the size of video, so that storage requirements are brought down to a manageable level. Even the video data can be brought to channel capacity level. Basically, there exist two types of video compression techniques: (a) Lossy type of compression is used in Internet-connected devices and telecommunication applications. The data that is produced after decompression does not exactly match the original form; instead, data

S. Bhavikatti (✉)
Tontadarya College of Engineering, Gadag, India
e-mail: sujatabhavikatti@yahoo.co.in

R. M. Banakar
BVB College of Engineering & Technology, Hubli, India
e-mail: banakar@bvb.edu

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_111

is reconstructed in a useful form. (b) Lossless compression technique is based on the removal of redundant data so that decompression gives exactly original data.

With an intention of making the compressed video data observable by all devices across the globe, compression techniques are defined as IEEE standards by ISO/IEC and ITU-T, for example, MPEG standards and H.264 standards. MPEG-2 standard was defined in 1993 by ISO. The encoder and decoder architecture requirements are defined in the form of syntax and semantic rules. Codecs contain lossy and lossless compression tools. Variable-length coding is a lossless compression tool.

The appropriate use of source residual redundancy is the key point of decoding technique. VLC decoder is the first tool of MPEG-2 decoder. The VLC generates code word for each symbol with different length. Frequently occurring symbols are represented using less number of bits, whereas less common symbols are represented using long length code word. During the design of MPEG-2 decoder, various optimized algorithms are developed to implement VLC decoder. VLC decoder architecture is a bitwise operator. Hence, VLC decoder contributes major computation time for MPEG-2 decoder. VLC produces code word for each symbol. Each input symbol is mapped to a code word, and code words may have varying length, but contain integral number of bits. Frequently occurring symbols are represented using less number of bits, whereas less common symbols are represented using long VLCs. Over a sufficiently large number of encoded symbols, data is compressed.

Following are the main steps of VLC decoder:

- Identify the code word length and code word: Code words are identified from the series of encoded input bit stream. Using code book in the form of lookup table, the (run, level) values are identified.
- Shift the input bit stream by the length of the previous decoded symbol: After identifying the length of the previous decoded symbol, the bits of input sequence are discarded from input bit stream.
- Arrange the decoded symbol: The decoded symbol from code book is the output of the decoder.

1.1 VLC Code book

The VLC decoder requires knowledge of source symbols, code word, and corresponding code length. These details are stored in the form of lookup table called code book. The size of code book is decided by the number of symbols and the probability of symbols. ISO 13818-2 defines 15 VLC tables for the video data, motion vectors, and syntax elements necessary for decoder. The statistical analysis of 15 tables shows that Tables B-14 and B-15 defined as “VLC for DCT coefficients Table zero” and “VLC for DCT coefficients Table one,” respectively, are larger in size. So VLC decoder design is illustrated by designing a code book for these two tables, which are available in ISO 13818-2 document.

The further arrangement of paper is as follows. Various algorithms of VLD are designed to reduce the complexity, minimize power, and increase the speed and are listed in Sect. 2. Section 3 explains the parallel decoder architecture using table lookup method and partitioning of lookup table to improve index speed. The simulation results are given in Sect. 4. The proposed work focuses on the simulation of VLC decoder design referring to lookup table using the system-level simulation and hardware implementation. Finally, the paper ends with the conclusion.

2 Observations

The VLC encoder and decoders have different implementation requirements. The encoder finds the VLC value from the standard tables and generates bit stream. The bit stream is the sequence of binary data without any field identification of code "begin" or "end." The symbols are encoded using table lookup defined as per the IEEE standard specifications. The run, length combinations, and respective code words are defined in the tables. The run and length combinations are generated during encoding. In encoding process, after DCT and quantization, zigzag scanning generates the array of values. This array is represented in the form of run-length combination. Each of these run-length values is assigned with code word. As each symbol is encoded independently, parallelism technique can be used to speed up the coding process.

The input to decoding algorithm is the bit stream, and decoding procedure uses standard tables. Since bit stream does not contain any information of start or end of the code, the decoder architecture is complex. Basically, VLD is implemented using binary tree approach or parallel decoding approach. The tree-based approach uses the concept of Huffman tree. The direct implementation of VLC decoder is bit-by-bit sequential decoding. Thus, VLD algorithm implementation has a tradeoff between decoding speed and size of memory. For example, a simple and efficient representation of VLCs for a frame is using binary tree. An associated decoding algorithm starts at the root node, extracts a bit from the input, and follows the corresponding branch to the next node. The process repeats until a leaf is reached, which in turn indicates the symbol. The complexity of this algorithm depends on the depth of the tree. Thus, the main constraint of the approach is it decodes one bit at a time.

In [1] the use of concurrent method to improve the throughput is explained. The algorithm is based on pipelined tree-based architecture. The fully pipelined design is implemented using concurrent decoding of independent bit stream. Due to pipelining method, high-level optimization is achieved in terms of speed and bit length. Since algorithm is based on VLSI architecture, the main limitation is reprogramming for change in source statistics, hence less flexible. The PLA-based algorithm is improved by using plane separation. The performance of this architecture is improved by parallel processing in feedback path.

The soft input and soft output VLC decoder algorithm [2] uses the source redundancy appropriately at decoder and improves the error correction capability. This gives better results for concatenated schemes with VLC codes. The algorithm is less complex. There is small loss due to insufficient quality of the soft outputs generated. Since the delay is inserted during code book indexing during decoding process, it counts for overall delay of VLC decoder.

The author in [3] proposes an algorithm to reduce the complexity of VLC decoding by using SOSA algorithm. The reliable information of bits is collected from VLC encoder. This information is used during decoding to minimize the errors. The reliable information is about tree structure, probability of symbols. The iterative decoding algorithm is less complex and also more robust to errors. The advancement in technology introduced many international video codec standards, which contain VLC decoder as one of the tools. Lamy and Perros-Meilhac [4] propose multi-standard VLC decoder. The hardware complexity is reduced by efficient representation of code word table. The reduced hardware complexity gives better results for MPEG-2 and H.264 video decoders. In [5], a high-speed Huffman decoder algorithm is proposed. By using typical nature of Huffman coding which is based on single-side growing, the search time is reduced. The memory efficiency is improved. Simulation results are tabulated for MP3 type video.

In [6], a method to reduce the complexity of VLC decoder is explained. The method is commonly defined for both MPEG-2 standard and H.264 standard. VLD is implemented using sub-tree (ST) methods. Sub-tree refers to the prefix part and tree part of VLCs. Since prefix part is redundant, using ST type of classification, the redundancy appearing between different VLC trees is removed. This minimizes the storage requirements.

In [7], VLCs are compared to fixed-length codes (FLCs). Since number of bits used by VLC is less compared to FLC, VLCs are used in IEEE standards. It is observed that VLCs are more prone to errors. By using trellis-based representation for VLCs and BCJR algorithms, the error effect in VLCs is minimized. The author Jae proposes a plane separation method to improve the speed of VLC decoder. The delay involved in the feedback path of data flow is minimized. Shifting operations and decision process of correct code word identification are carried out simultaneously. Due to parallelism in process, the delay is reduced. Tsai and Chen in [8] propose architecture based on parallel VLD. The architecture consists of code detector and lookup table. The arrangement of code book is done such that VLC itself acts as address. The size of lookup table and code detector implementation is considered to design low-power algorithm. Subtable concept is used in code book arrangement. The code search process is executed sequentially to find match in each subtable. The table partitioning is done to minimize power consumption. The amount of power consumed in code detection is explained with examples.

3 Parallel Decoding Approach

The parallel decoding technique of VLD is a search algorithm for finding match for multiple bits from input bit stream to the code book. The algorithm implementation includes the code book arrangement and comparing unit as the main parts. Code book arrangement is considered to speed up the decoding process. The code book is arranged in an increasing order of its code length. The lowest length code is the most frequently occurring code. During search time, the number of memory references can be minimized by arranging the code book in the increasing order of code length. The code book reference and comparison are sequential processes performed till the bits of input sequence are defined with symbol. Thus, decoding procedure is defined using sequential finite state machine modeling as shown in Fig. 1. The FSM input is VLC-coded bit stream, and outputs are decoded source symbols. The main hurdle for designing of high-speed decoder is recursive dependency.

The decoder is loaded with bit stream indicated by flag "load." Then comparison is done for search with code book contents. During search, load = "0." Search is an iterative process done by comparing input bit stream with every code in code book. Once the match is found, the load is reset. The input bit streams are shifted by length of code word identified. The search process continues till all bits of a block are decoded.

Figure 2 is the architecture of variable-length decoder. Input MPEG-2 bit stream is serial input data to VL decoder. The variable length of the code words makes the decoding to a sequential process. In order to decode a code word, the previous code words must be decoded in sequence in order to determine where in the input buffer the code word starts. This data dependency is limiting the throughput of the VLC decoders. The variable-length decoder consists of a barrel shifter, comparator, and code book. The comparator is designed to match the input bit stream with the code word of code book. The code book is the main functional block, in the form of a table. It contains information about number of code words, code length, and code word. The major drawback here is the relatively large critical timing path in the feedback loop that includes barrel shifter, code word table (ROM), and accumulator. This feedback path cannot be pipelined and will therefore limit the performance of this architecture. During decoding, the input bits are serially read. The length of code word is unknown. It requires serial search in the code book. In order to speed up the decoding process, search algorithm [9] is to be framed. By changing the arrangement of code book [6], the search time can be minimized.

Fig. 1 Conventional FSM of VLC decoder

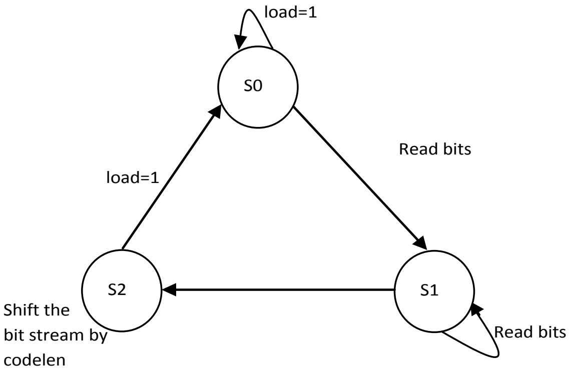
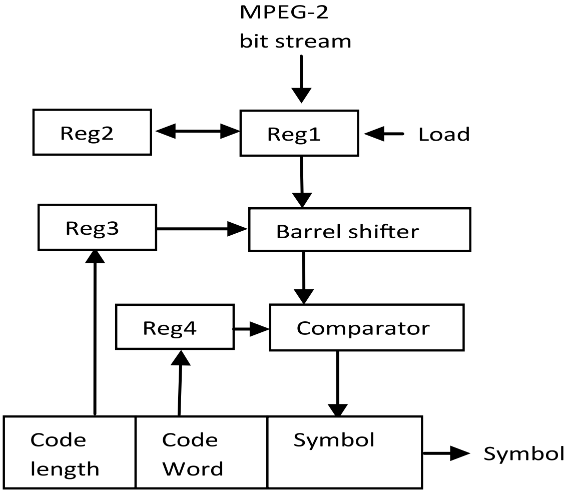


Fig. 2 Parallel VLC decoder architecture



The decoding logic is based on the code book access which in turn depends on code book arrangement and overhead involved in code book access. The partitioning of VLC tables into two parts is considered to minimize the power. This method is considered to partition the code book into segments. These segments are defined based on the code length. The address length required to refer to code book location is reduced by two bits. ISO/IEC defines the total of 15 tables for variable-length code assigned as per the MPEG-2 standard. The tables include the VLC of run-length pair, motion vectors, and DCT coefficients. Among these tables, T14 and T15 are the maximum length tables. The VLC decoder implementation is illustrated with respect to Table T14. The length of Table T14 is 114. Since the arrangement of 114 VLCs into one code book requires 7 bits address length. The address length is reduced due to dividing the code book into segments.

Figure 2 shows the parallel decoding architecture of VLC decoder. The input is MPEG-2 bistream. VLD architecture is composed of code book and decoding logic. Further decoding logic consists of reading the code book, comparing logic to identify the code match and find the symbol. The low-power design approach considers the code book arrangement and decoding logic. Tsai and Chen [8] say that the VLC decoding logic and size of VLC table decide the power and throughput. Thus to minimize the power, the code book arrangement is considered. With the normal code book arrangement, the complete code book is selected for the decoding operation. During decoding, the data of selected row is transferred to register. The code book remains in active state until the code is decoded and symbol is identified. The amount of power consumed to keep the code book as a whole is more compared to memory segment form. Using memory segmentation approach, the memory segment which is referred for code access is activated keeping other memory segments in idle state. Thus, the power consumption is minimized due to activating the part of code book.

Bit stream contains the frame data coded, as per MPEG-2 standard and syntactic and semantic rules, necessary information to decode the bit stream. "maxlen" represents the highest length of code word in code book. In synchronous with clock, number of bits = "maxlen" is read from MPEG-2 bit stream into reg1 and buffered in reg2. The code word from code book and corresponding code length are read into reg3 and reg4. The reg1 content is shifted by the number of bit positions equal to the length of code word read from the code book. The inputs to the comparators are shifted bits of reg1 and code word from code book. If comparator output is one, the corresponding symbol is output. If match is not found, then comparator gives output as zero. The comparator iteration continues for next code word from code book. After finding the symbol, the contents of reg2 are shifted by that code word length and rest of bits in reg2 are concatenated with input MPEG-2 bit stream. The process repeats till all bits of block are decoded.

4 Simulation Results

In this paper, VLC decoder algorithm is verified using FPGA hardware implementation. The algorithm is tested using system-level simulation. For testing of algorithm, bit stream is generated using system-level simulation and text file "data1.txt" is generated. Using data1.txt bit stream is generated. The serial input to VLC decoder is given using buffer. The lookup tables or code book is in the form of ROM memory. Discrete ROM memory separately for code of particular length eliminates the need of length storage in code book. Since 17 is maximum length to read maximum of 17 values, 5 bits address length is assigned. Thus, the total memory length required is 5 * 114 = 570. Total memory length = 570 + 1921 = 2491. Thus, it is concluded that memory segmentation minimizes the memory size. For memory segmentation method, the number of bits is identified by referring to bits values which are referred. It counts to 1879. The amount of memory saving is (1879/2491) * 100 = 75%. The address length is reduced by 2 bits.

Table 1 Search time of single code book and segmented code book

Variable length	Single code book (ns)	Segmented code book (ns)
4	8.3	8.2
6	10	8.3
10	11.8	8.1
14	15.9	8.1
17	18	8.2

The bit stream of a block contains VLC of differential DC and run-length pair. The decoder module is simulated using Spartan-6, XC6SLX45T device. The simulation results are tabulated comparing the search time of VLC for different lengths considering a single code book and segmented code book in Table 1. It is observed that the search time remains almost the same for segmented code book arrangement as compared to the single code book arrangements. The search time increases with increase in length for single code book arrangement, whereas the search time remains almost the same for segmented code book arrangement. The average clock rate is 120 MHz in this design.

5 Conclusion

A new hardware-based VLC decoding algorithm is implemented using code book. VLC decoder is the first block in MPEG video decoders. The modified VLC decoder algorithm is simulated using system-level simulation, and power minimization is shown with hardware implementation. The algorithm uses sequential decoding of symbols. Since we assume that the number of symbols and code length is known, the exact number of symbols can be decoded. The code book arrangement according to the code length improves the memory indexing and reduces the memory access time. The functioning of algorithm is tested on “xylophone.mpg” file. ISO/IEC 13818 data is used to design the VLC decoder.

References

1. ISO/IEC JTC1/SC29 (1994) Generic coding of moving pictures and associated audio, ISO/IEC 13818-2. Draft International Standard
2. Jeon JH, Park YS, Park HW (2000) A fast variable length decoder using plane separation. IEEE Trans Circuits Syst Video Technol 10(5):806–811
3. Aspar Z, Yusof ZM, Suleiman I (2000) Parallel Huffman decoder with an optimized look up table option on FPGA. In: TENCON, Proceedings, vol 1, pp 73–76
4. Lamy C, Perros-Meilhac L (2003) Low complexity iterative decoding of variable length codes. In:THALES communications, pp 1–6
5. Fryza T, Prokopec J (2009) Experimental application of channel coding for wireless transmission of compressed video data. In: Ultra modern telecommunications & workshops, 2009. ICUMT ‘09. International conference, pp 1–4
6. Venugopal N, Ramachandran S (2009) Design and FPGA implementation of fast variable length coder for a video encoder. IJCSNS Int J Comput Sci Netw Secur 9(7):178–184
7. Lo C-C, Hsu CW, Shieh M-D (2013) Low complexity multistandard variable length coding decoder using tree based partition and classification. IET Image Process 7:185–190

8. Tsai T-H, Chen W-C (2003) A low power VLSI implementation for variable length decoder in MPEG-1 layer 3. IEEE Tran
9. Zhu K, Liu WD, Du J (2012) Hardware JPEG decoder and efficient post-processing functions for embedded application. In: Computer and information technology (CIT), 2012 IEEE 12th international conference, pp 814–817

Efficient Cruise Control of Electric Motorcycle Using PID

Rohan Sawant and Andrew Kidd

Abstract The automotive industry is progressing expeditiously. The popularity of electric vehicles (EV) has shot up over the last few years. As a matter of fact, electric drive systems such as DC motor drives, one of the electrical drives, are rapidly gaining prominence because of their high efficiency, better dynamic response and low upkeep. The following work deals with the drivetrain of the pre-existing electric motorcycle comprised of a brushed DC motor. In this work, a system is developed to maintain the speed of the electric motorcycle at a set speed, under various disturbances using PI control. A detailed mathematical model, transfer function and simulation of the same are obtained using the software package MATLAB, SIMULINK. The controlled DC motor is made to track a variable speed set point with zero steady-state error and desirable disturbance rejection capabilities.

Keywords DC motor · PID · Matlab

1 Introduction

DC motor drives play a significant role in mechanical and other applications such as steel moving plants, electric trains and robotics. For the most part, an elite engine drive framework must have great powerful speed order and load controlling reaction to perform undertaking. DC drives, due to their straightforwardness, simplicity of utilization, dependability and favourable cost have for quite some time been a spine of mechanical and robotic applications where speed and position control of motor are required. DC drives are less complex, as when it comes to motorcycles, the power conversion factor from DC to AC is eliminated. Also, the speed-torque attributes of a DC motor are robust [1].

R. Sawant (✉)
Vidyalankar Institute of Technology, Mumbai, India
e-mail: rohansawant96@gmail.com

A. Kidd
Teesside University, Middlesbrough, UK
e-mail: A.Kidd@tees.ac.uk

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_112

Although three-phase induction motors are the most widely recognized sort of motors utilized in industrial applications, DC motors are expanding in prevalence because of their execution points of interest over AC motors for applications ranging from high-speed automation to electric motorbikes. Applications where speed should be varied, or torque should be controlled with high exactness, brushed DC motors are used. Today, locomotives are being offered with powered gadgets, in addition designers are seeking to improve the performance of the equipment they design, which often entails upgrading from AC motor to a DC motor, specifically, places where increasing accelerations are required. DC drives are additionally being fabricated in regularly expanding volumes for much Bijou applications, such as solar-based gadgets, toys and cell phone handsets [2].

In this work, a corresponding DC motor similar to the one used in an electric motorcycle is considered. A transfer function model of the motor is obtained using the reaction curve method and analysed in MATLAB, compared to physical data from the test motor to check for goodness-of-fit. Further using this model and the direct design synthesis (DDS) control design approach, the speed of the motor will be made to track a variable set point and then be maintained under the influence of disturbances, such as a change in the inclination of the surface the bike is travelling on (i.e. up/down a hill) (Fig. 1).

2 Mathematical Modelling

2.1 Transfer Function Derivation of a DC Motor (Bottom-Up Approach)

A separately excited DC motor system is considered. To obtain the mathematical model of the same, consider, supply voltage 'v' applied to the motor circuit (refer Fig. 2), and the motor generates torque (T) that is proportional to the product of the

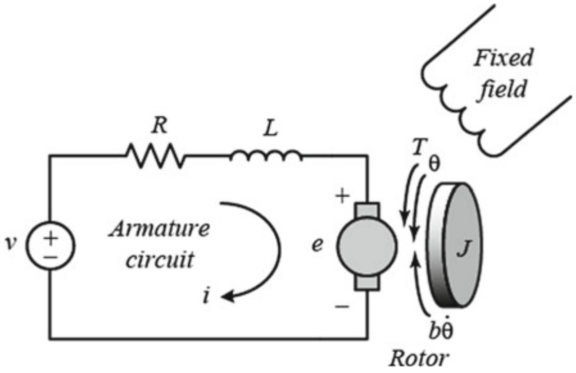


Fig. 1 DC motor equivalent circuit

magnetic field flux 'ϕ' and the rotor armature current 'i',

$$T = K_T\, i\, \phi$$

The Back EMF is a counter voltage that is proportional to the product of magnetic field flux (ϕ) and the rotor angular velocity (ω),

$$e = K_E \phi\, \omega$$

Making use of KVL voltage law in the above motor circuit,

$$v = Ri + L\frac{\mathrm{d}i}{\mathrm{d}t} + e$$

Considering the above fundamental equations into Laplace transform, respectively, and further simplifying it [3, 4], we get the first-order transfer function model of the DC motor as,

$$\frac{\Omega(s)}{v(s)} = \frac{\frac{1}{K_E}}{1 + \tau_m s} \tag{1}$$

where $\tau_m =$ Electromechanical time constant.

2.2 System Identification—Reaction Curve Method

The first-order plus time-delay (FOPTD) model has been widely used to design and implement the process controllers of the system. The terms related to the low-order plus time-delay processes are very useful for describing the dynamic characteristics of given process. The FOPTD process derived for DC motor system is given in Eq. (1).

From Eq. (1), it can be realized that K and τ are called the static gain and the time constant, respectively. The step input applied to the motor is Δu, and the maximum rated voltage under which the motor operates is represented by Δy. Using the formulae, the terms K, τ and d are computed.

$$K = \frac{\Delta y}{\Delta u} \quad \text{(System Gain)}$$

$$\tau = 1.5(t_2 - t_1) \quad \text{(Time Constant)}$$

$$d = 1.5\left(t_1 - \frac{t_2}{3}\right) \quad \text{(Time delay)}$$

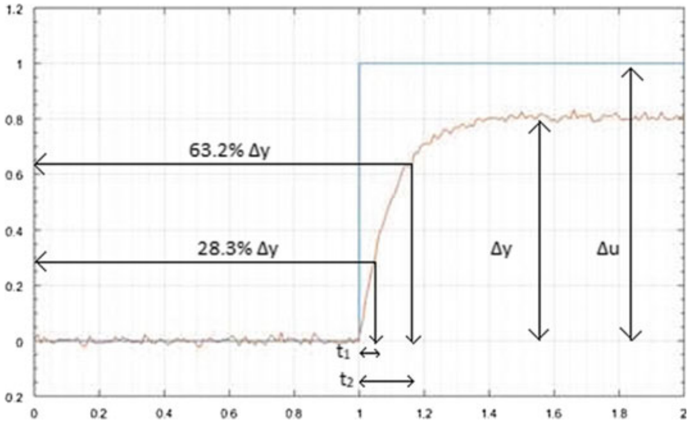


Fig. 2 Sample DC motor behaviour plot

The computed values are fed in the FOPTD model of the motor and from the schematic obtained in the SIMULINK (refer Fig. 3), and a transfer function graph of the DC motor is acquired [5].

In the proposed system, from Eq. (1), the term *d*, i.e. time delay is eliminated since the value derived from the transfer function graph is insignificant (refer Fig. 4). Also, the transfer function acquired from the reaction curve method is in time domain, i.e. continuous transfer function. It is further converted to discrete form so as to get the same sampling time, and the discrete and continuous elements do not mix within the SIMULINK model to be used in the digital circuit. The sampling frequency used is kept same as that in the input.

A comparison between the actual DC motor response and the transfer function model developed using the above-derived terms is plotted. It can be observed that the transfer function model developed is a decent fit.

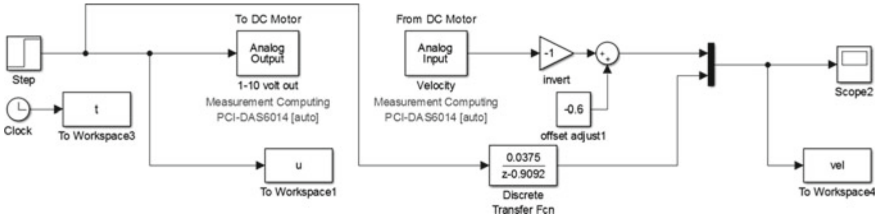


Fig. 3 SIMULINK schematic to acquire TF

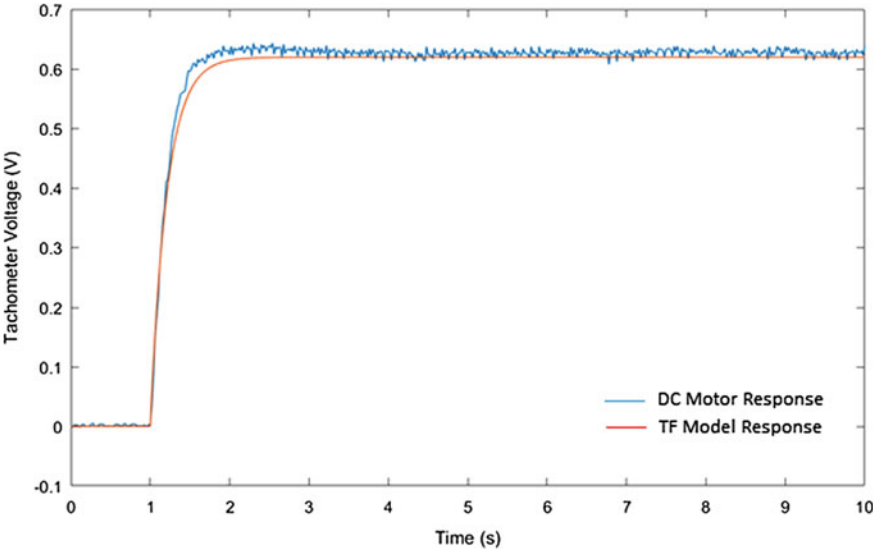


Fig. 4 Transfer function response

3 Control System Design

A proportional controller makes the control signal directly proportional to the magnitude of the error signal. One of the main drawbacks of proportional—only control is its inability to leave zero steady-state error. Increasing the gain reduces the offset but can lead to noise problems and instability. Alternatively, by introducing the Integral action in the controller, which perhaps act as an automatic bias adjuster can eliminate the offset without introducing much of instability. But, the downside is that the integral action can actually introduce oscillatory behaviour, and this is eliminated only if the parameter is set correctly. The introduction of an integrator now exhibits dynamic behaviour of its own. Now, the system will have two adjustable parameters K_P and K_I, the proportional and the integral gain.

Using Pade approximation [6, 7], slight variations in the approach of direct design synthesis (DDS), which has achieved widespread industrial acceptance, are used to compute the proportional and integral parameters of the system.

For a FOPTD model with a PI controller, the parameters are derived as follows,

$$K_P = \frac{2\tau + d}{2K\lambda}$$

$$K_I = \frac{2}{2\tau + d}$$

Derivative control is highly susceptible to noise. The noise sensitivity is due to high rate of change within the signal when there are noise spikes. Also, in the proposed system, the output of the DC motor consists of fair share of noise. Hence, by incorporating derivative control in the system, entire system can turn unstable. As a matter of fact, the given system attains stability by incorporating PI control only.

4 Implementation

4.1 PI Control Observed Under Disturbances

The output (speed) of the DC motor is measured and fed back to the PI controller via a closed-loop system. The feedback signal is first compared with the reference signal. An error signal is generated at the summing point by calculating the difference between the actual output and the reference signal by simple subtraction. This error signal is passed through to the PI controller for the required modification set by specification of controller parameters. The control outputs an appropriate control signal such that the error is then eliminated (Fig. 5).

A mechanical disturbance in the form of brake can be applied to the motor. This is analogous/equivalent to an electric bike travelling on a now steeper gradient (i.e. uphill). Due to the incorporation of PI control, it now maintains the speed of the motor at the certain set speed.

4.2 PI Control Observed Under Varying Pre-defined Speeds

PI control is also observed whilst setting different set point speeds. The proposed system consists of manual/auto switch. If the switch is on manual mode, the driver will have to control the speed of the motorcycle manually using the throttle. If the switch is on auto mode, a set point speed is decided by the driver, and the motorcycle

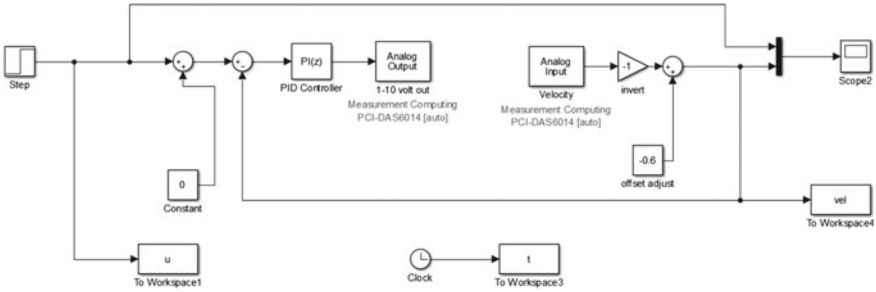


Fig. 5 PI control under disturbances, schematic

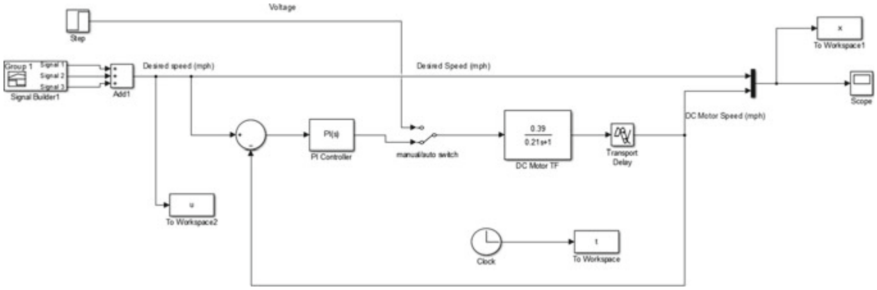


Fig. 6 PI control under varying pre-defined speeds, schematic

will drive at the set speed even under most disturbances. For the purpose of simulation only, the varying set point speed block can be represented by signal builder in the SIMULINK. The varying signals are the step signals of different magnitudes. The PI controller will try to eliminate the error signal as mentioned and match with the new set speeds at earliest (Fig. 6).

5 Results and Discussions

5.1 Disturbance Rejection Capability

Mechanical disturbance is added to the system in the form of braking. It can be seen that the disturbance is added in the system at $t = 5.5$ s, and it takes around 4 s to settle at pre-defined value since $\lambda = 4$. The PI controller recovers from this disturbance and adjusts itself to the pre-defined speed. This is the disturbance rejection capability of the PI controller in the system.

5.2 Set Point Tracking Capability

Set point tracking capability allows the user to set the set point speeds of the motorcycle. In the proposed system, signal builder allows to set varying amplitude for the step input for the motor (Figs. 7 and 8).

This varying step input does act like different set point speeds for the motorcycle, and PI controller tries to adapt to these speeds.

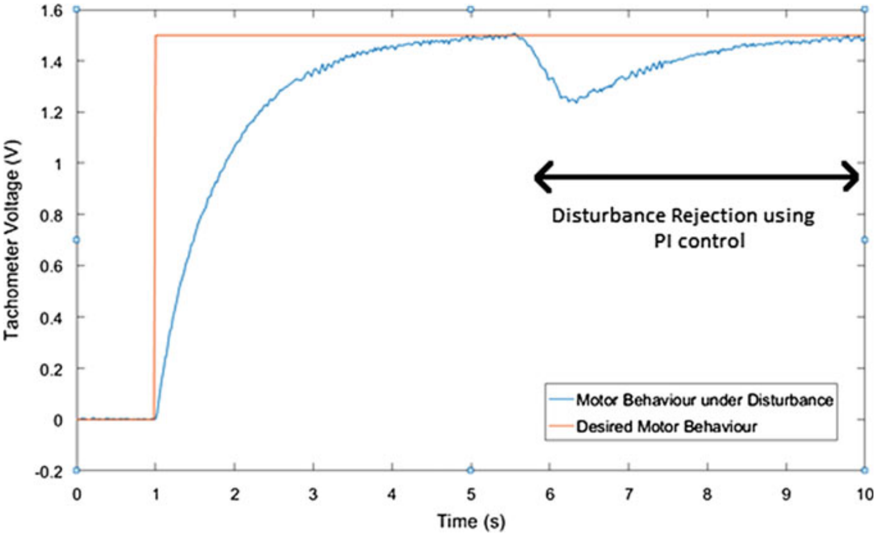


Fig. 7 Disturbance rejection behaviour using PI

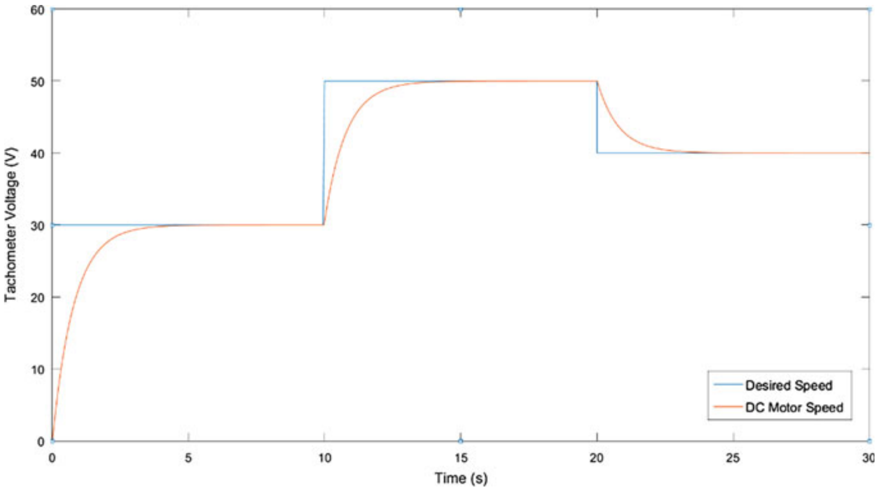


Fig. 8 Set point tracking capability using PI

6 Conclusions and Future Enhancements

The transfer function model derived from the reaction curve method finds a decent fit with the motor output. This transfer function can be used as a basis for tuning. PI control approach is incorporated to trace this transfer function model. The proposed system can efficiently work in maintaining the speed of the motor and perform the function of cruise control in electric motorcycles.

Induction motors are now used widespread. One such notable example would be four-wheel based electric vehicles. An equivalent mathematical model of an induction motor can be computed using the process defined in the proposed system. Further analysis can be resolved, and a similar cruise control system for four-wheeled system based on induction motors can be devised.

References

1. Wang JB (2001) Control of electric machinery. Gau Lih Book co., Ltd, Taipei, Taiwan
2. DC motor drives. https://www.engineerlive.com/content/21329
3. Huang G, Lee S (2008) PC-based PID speed control in DC motor. In: International conference on audio, language and image processing, 2008. ICALIP 2008, pp 400–407. IEEE
4. Hanselman DC (2003) Brushless permanent magnet motor design, The Writers' Collective
5. Sung SW, Lee J, Lee IB (2009). Process identification and PID control. Wiley
6. Rivera DE, Morari M, Skogestad S (1986) Internal model control: PID controller design. Ind Eng Chem Process Des Dev 25(1):252–265
7. Al-Mashakbeh ASO (2009) Proportional integral and derivative control of brushless dc motor. Eur J Sci Res 35(2):198–203

Transmission of Watermarked Image in WSN Using ELSM Algorithm

A. Umapriya and P. Nagarajan

Abstract To improve the copyright protection of the digital image, the watermarking technique is used. By changing the entropy, identify the location where the secret data gets embedded into the original image. It provides less distortion and high robustness. The watermarked image is send to the receiver through the wireless sensor network. In WSN, clustering is the best technique to save the energy. In cluster-based WSN, cluster head requires more energy to receive the data from the sensor nodes and transmitting it to the base station. To maintain the lifetime of WSN, the proper selection of CH is essential. In this paper, we propose the energy-based least squares multiple algorithms. Simulation results show that the ELSM algorithm is more efficient compared to the WLSM algorithm to improve the range of bandwidth, cluster overhead, skew rate, offset rate, carrier signal, reference signal and control output signal.

Keywords Wireless sensor network · Cluster head · Energy-based least squares multiple · Weight-based least squares multiple

1 Introduction

Data security is necessary for every field to transfer the secret data. For this purpose, we use the digital watermarking technique. It provides high robustness to the host images. To improve the quality of image and strength and to remove the noises, many processes are available.

[1] The host image provides self-recovery, tampered localization and ownership verification. Greyscale watermark is proposed to the watermark insertion. The last two LSBs get changed after the insertion of watermarking. While using LSB, it is easy to identify the host image.

A. Umapriya (✉) · P. Nagarajan
Department of ECE, Vivekanandha College of Engineering for Women, Namakkal, India
e-mail: umapriyakaviarun@gmail.com

P. Nagarajan
e-mail: greennagarajan@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_113

[2] The survey of digital watermarking techniques provides discrete cosine transform, discrete Fourier transform, discrete wavelet transform and also the performance analysis metrics. All these techniques are compared.

[3] Clock synchronization using least common multiple algorithm is used to avoid the clock skew and clock offset. Two levels of synchronizing are used. One is nodes within the cluster synchronize and another level is the cluster head synchronize to remove the cluster overhead.

[4] Using particle swarm optimization algorithm in wireless sensor network, the energy-efficient head cluster selection is proposed.

[5] Using this algorithm, it provides a better performance of the total energy consumption, lifespan of the network and also the base station that received many packets.

[6] For the security purpose, we use the watermarking technique to embed the data in the image [7]. The image gets watermarked. In wireless sensor network [8], it contains many sensor nodes that are available to transfer the data from the sender to the receiver through the base station [9]. To save the energy, network gets divided into groups called as cluster using the energy-based least squares multiple algorithms. Each cluster has its own cluster head used to find the path among the sensor nodes [10].

Cluster heads are used to find the shortest path to the bath station. The base station communicates with the public networks [11]. Then the watermarked image received at the receiver end. The secret data can extract from the host image [12]. The ELSM algorithm is used to improve various parameters such as the range of bandwidth, cluster overhead, skew rate, offset rate, carrier signal, reference signal and control output signal [13].

2 Methods and Materials

2.1 *Watermark Insertion*

In any field, we hide some information for security purpose. When we transfer the secret data, it gets stolen by someone. To avoid this problem, we use the watermarking technique. The watermark insertion is the process of embedding the secret data in the original image. After the insertion of secret data in the image, the secret key will generate. The image gets watermarked. Figure 1 shows the watermark insertion.

2.2 *Clock Synchronization in WSN*

Wireless sensor network contains more number of sensor nodes. When we transmit the image from sender to receiver, it consumes huge power because of the presence

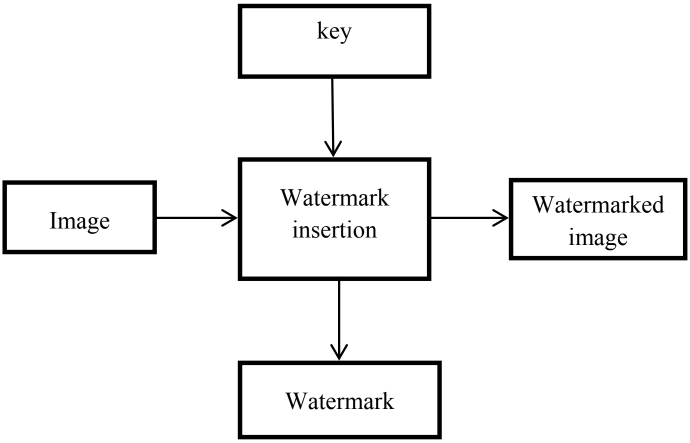
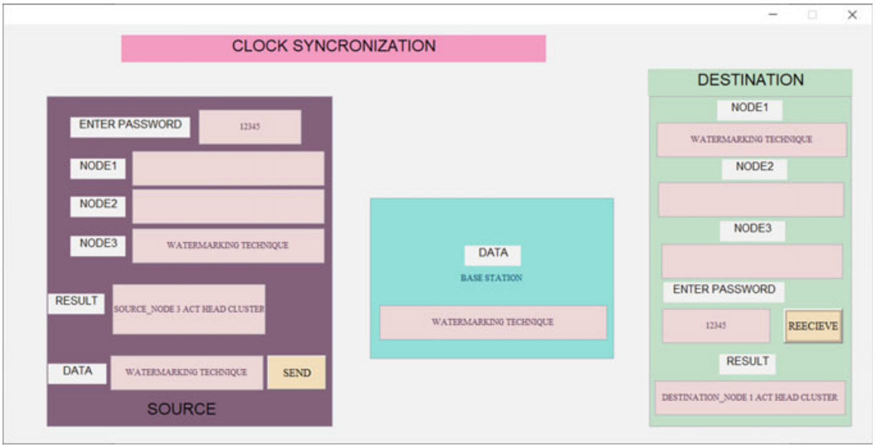


Fig. 1 Watermark insertion

of more sensor nodes. For saving the energy in wireless network, we propose the energy-based least squares multiple algorithms. In this technique, divide the sensor nodes into groups. Each group contains the superior called as cluster head which is used to select the shortest path of the transmitting image.

Figure 2 shows the clock synchronization in WSN using ELSM algorithm. The cluster head is automatically selected in the network using ELSM algorithm. Two levels of synchronizing are used. One is nodes within the cluster synchronize and another level is the cluster head synchronize to remove the cluster overhead. Cluster head transmits the image to the base station. And also the ELSM algorithm is used to improve the range of the bandwidth, cluster overhead, skew rate, offset rate, carrier


CLOCK SYNCRONIZATION

SOURCE
ENTER PASSWORD: 12345
NODE1:
NODE2:
NODE3: WATERMARKING TECHNIQUE
RESULT: SOURCE_NODE 3 ACT HEAD CLUSTER
DATA: WATERMARKING TECHNIQUE

BASE STATION
DATA: WATERMARKING TECHNIQUE

DESTINATION
NODE1: WATERMARKING TECHNIQUE
NODE2:
NODE3:
ENTER PASSWORD: 12345
RESULT: DESTINATION_NODE 1 ACT HEAD CLUSTER

Fig. 2 Clock synchronization using ELSM algorithm

signal, reference signal and control output signal. Then the base station sends the image to the public networks. Finally, the receiver receives the image by giving the correct password.

By saving the energy consumption, the bandwidth gets improved and reducing the overhead. And also provides the long distance to transmit the image.

2.3 Transmitting and Receiving Process of WSN

The transmitting and receiving processes of the wireless sensor network using ELSM algorithm are given below. We need to set the password. If we give the password correct, the secret data can be embedded in the original image by using watermark technique. Then the secret key will generate automatically.

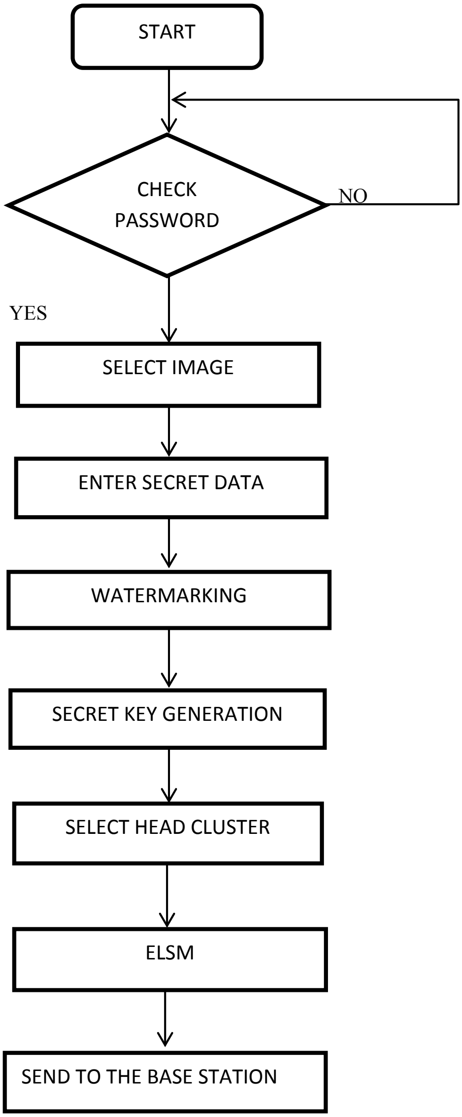
The host image is sent from the source to the destination through the wireless sensor network. In this network, there are more number of sensor nodes which are available. When we transmit the image through this network, the energy loss will occur for more sensor nodes. The sensor nodes are grouped by the cluster. Each cluster has its own cluster head. For choosing the proper cluster head, we use the ELSM algorithm. The cluster head is used to select the shortest path via sensor nodes. The cluster head selects the sensor nodes which have the highest residual energy. When we select the proper cluster head, we can save the energy. By saving the energy, we can transmit the image for long distance. Then the transmitted image reaches the base station (Fig. 3).

The receiving section using ELSM represents Fig. 4. We need to give the password. If the receiver gives the wrong password, the secret data does not generate instead they receive the ordinary image. The same process will continue for selecting the cluster head in transmitter side. Finally, the data can be retrieved by using the watermark extraction. By using this technique, we can save the energy of all sensor nodes. Each iteration will continue by using this algorithm.

2.4 Watermark Extraction

The watermark extraction is used to extract the secret data from the watermarked image. Figure 5 represents the watermark extraction process. When we provide the correct password, we can receive the secret data. Otherwise, we can receive the ordinary image.

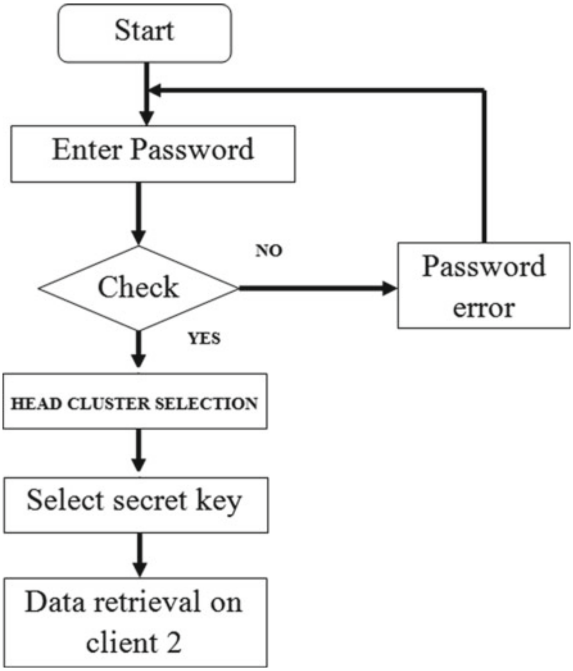
Fig. 3 Transmitting section using ELSM



3 Result and Discussion

The simulation result is taken by MATLAB using C program. For the security purpose, we use the watermarked image. Simulation results show that the ELSM algorithm is more efficient compared to the WLSM algorithm to improve the range of bandwidth, cluster overhead, skew rate, offset rate, carrier signal, reference signal and control output signal.

Fig. 4 Receiving section using ELSM



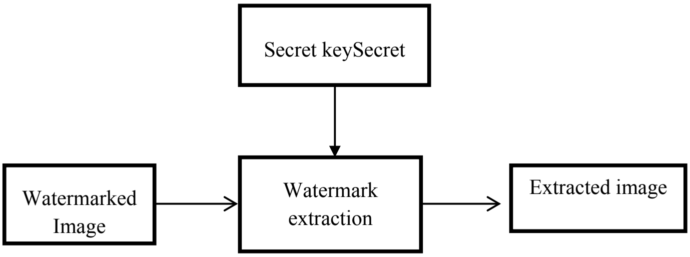


Fig. 5 Watermark extraction

Figure 6 represents the graphical representation of error rate, carrier signal and control signal using ELSM algorithm. Figure 7 represents the graphical representation of skew rate, offset rate and cluster overhead. By saving the energy, we improve the lifespan of the network and also provide the long transmission distance. Finally, we extract the secret data using the watermark extraction.

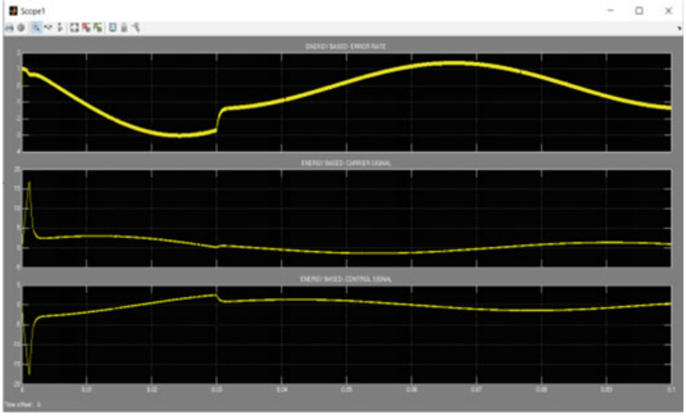


Fig. 6 Error rate, carrier signal, control signal

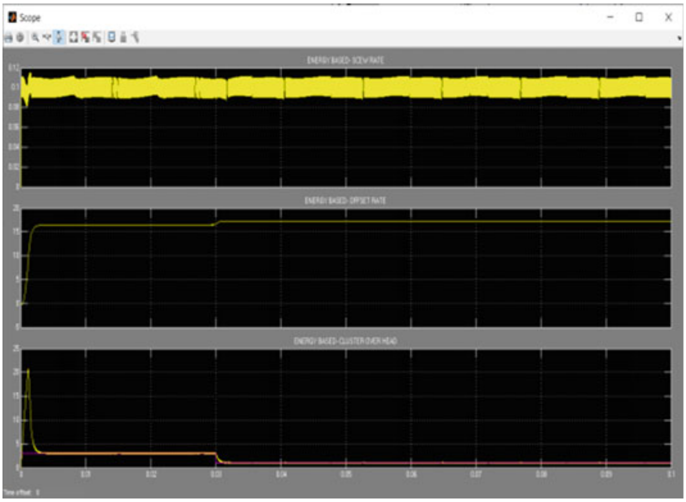


Fig. 7 Skew rate, offset rate, cluster overhead

4 Conclusion

In this research, we proposed the ELSM algorithm for the proper selection of the cluster head to save the energy. This algorithm is to extend the lifespan of the network by saving the energy among the nodes. Two levels of synchronizing are used. One is nodes within the cluster synchronize and another level is the cluster head synchronize to remove the cluster overhead. The watermarked image was received by receiver. By saving the energy, the transmission range is for a large distance. The experimental results of ELSM algorithm performs better than the existing algorithm in terms of bandwidth, cluster overhead, skew rate, offset rate, carrier signal, reference signal and control output signal.

References

1. Ansari IA, Pant M (2017) Multipurpose image watermarking in the domain of DWT based on SVD and ABC. Pattern Recogn Lett
2. Hemani, Singh S (2017) A survey of digital watermarking techniques and performance evaluation metrics. IJETT
3. Tabassum N, Geetha D (2017) Clock synchronization in wireless sensor networks using least common multiple. AEU
4. Srinivasa Rao PC, Jana PK (2016) A particle swarm optimization based energy efficient cluster head selection algorithm for wireless sensor networks, Springer Science Business Media
5. Ernawan F, Kabir MN (2018) A blind watermarking technique using redundant wavelet transform for copyright protection. In: 14th IEEE colloquium on signal processing and its applications
6. Panda J, Mouriya S, Dang R (2016) Analysis of robustness of image watermarking algorithm using the dual tree complex wavelet transform and just noticeable difference. In: International conference on signal processing and communication
7. Tyagi S, Singh HV (2016) Digital watermarking techniques for security applications. In: International conference on emerging trends in electrical, electronics and sustainable energy systems
8. Ernawan F (2016) Robust image watermarking based on psychovisual threshold. J ICT Res Appl
9. Fazli S, Moeini M (2016) A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks. Optik Int J Light Electron Opt
10. Kakkirala KR, Chalamala SR (2014) DWT-SVD based blind audio watermarking scheme for copyright protection. In: IEEE conference
11. Makbol NM, Khoo BE (2013) Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. Int J Electron Commun (AEÜ)
12. Ling H-C, Phan RC-W, Heng S-H (2013) Comment on robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. Int J Electron Commun (AEU)
13. Abu NA, Ernawan F, Suryana N, Sahib S (2013) Image watermarking using psychovisual threshold over the edge. In: Information and communication technology, ICT-EurAsia

International Students' Gender Impact to Use Mobile Learning in Tertiary Education

Sujit Kumar Basak, Marguerite Wotto and Paul Bélanger

Abstract This study aims to design a model on mobile learning used by international students in tertiary education. It has used a survey questionnaire distributed through the LimeSurvey. A total of 12 international students from a tertiary education (6 female students and 6 male students) participated in Canada. The results revealed that male students got higher impact to the performance expectancy (PE), social factors (SF), and facilitating condition (FC) but on the other hand, female students got an impact on PE and FC. Furthermore, female students got a significant impact on PE and SF on behavioral intention (BI). Gender is having an impact on EE and FC. Finally, PE and SF have an impact on the BI to use mobile learning in tertiary education. These findings will help practitioners, educators, policymakers to implement mobile learning in tertiary education for international students in Canada and abroad.

Keywords Mobile learning (ML) · International students · UTAUT · SEM

1 Introduction

In tertiary education, mobile learning (ML) has significantly increased and is playing a crucial role for international students. Therefore, use of mobile learning in tertiary education helps for international students to be connected anywhere and anyplace. Berking et al. [1] stated that m-learning has a significant impact on the teaching and learning environments. In this context, the tertiary education may encourage international students to use m-learning for learning purposes. According to [2], a mobile device is used by many users because it is affordable and easy to carry than

S. K. Basak (🖂) · M. Wotto · P. Bélanger
Université du Québec à Montréal (UQÀM), Montreal, Canada
e-mail: sujitbasakmca@gmail.com

M. Wotto
e-mail: wotto.marguerite@uqam.ca

P. Bélanger
e-mail: belanger.paul@uqam.ca

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_114

personal computers. The development of mobile and technology has opened a new window to learn. Students believe that mobile learning has positive influence on the learning environment, although students are well known with barriers [3]. Levy's study indicated that learners of mobile devices are significantly higher motivated as compared to who did not use mobile device [2]. Using mobile devices, various materials can be downloaded. However, most of the smart mobile devices can easily play video features and also record where learners use their mobile devices to collect scientific data and visual materials [4]. The implementation of mobile learning can add a significant impact on the existing formal learning and assessment [5].

Gender issue in m-learning has been identified in the past decades on the computer and education research [6]. Male or female does not use the technology in a similar way, but as a result, some differences exist [7]. On the other hand, female students got significantly higher attitudes as compared to their male counterparts [8]. Moreover, a study by Muhanna and Abu-Al-Sha'r [9] indicated males got more positive attitudes than females. Similarly, Kwon and Chidambaram [10] argued that there is no significant impact on the gender attitude.

2 Problem Statement

Wang et al. [11] stated that although mobile technology use is increasing, using ML still in the infancy stages. The limitations of ML are categorized into four categories, namely physical attributes, network connection, physical environmental (using mobile devices outdoors), and limitations of the software design (difficult to install and also built in function) [12]. In this context, implementing ML for students could be a challenge because students are already used to what they are using in the past. Several researchers indicated that gender differences exist among college students or adult users about Internet use, attitudes toward the Internet, frequency to use Internet, and to measure self-skills of the Internet [13, 14]. Using a small keyboard and touch screen need more time to search for some information and to read them [15]. Existing research shows that female got anxiety than males on the computers and Internet use [8, 16]. Above, evidences show that the use of mobile learning by international students is increasing day by day. "The comparative analysis of the variables shows that social factors have a significantly higher impact on the behavioral intention to use for the m-learning by the first-year international students followed by performance expectancy, effort expectancy, and facilitating condition" [17]. In addition, evidences also show that students (male and female) are meeting more challenges to use mobile learning. This study is very important because it will help to analyze the international students' gender impact on the mobile learning very broadly in Canada.

3 Literature Review

The existing study shows the impact of gender plays a crucial role in tertiary education. A study with the undergraduate university learners in using a digital library [18] indicated male students got a higher impact on the perceptions than female students. Another study was conducted by Enoch and Soker [19] with students who use the Web-based instruction method. The results found that male students and female students both are continuously increasing the use of the Internet and the difference is still significant. Recent development on the Internet technology, namely online "gender difference, is believed to be less significant" [20]. A study on the differences of male and female students indicated that male students have more positive impacts on a computer use. In addition, male students use more frequently computer as compared to female counterparts [21].

Similarly, Hilao and Wichadee [22] also conducted a study on 122 students (65 females and 57 males) on gender differences to use a mobile phone. Results revealed there is no difference in the usage and attitudes of male and female students in terms of language learning and performance. Most of the research findings show that male students were well experienced and very positive toward m-learning as compared to female students [23, 24]. In Taiwan, conducted a study by Ong and Lai [25] on 156 employees where 67 of them female employees and 89 of them male employees. These employees participated from six multinational companies. Results revealed male's usages decisions are having a significant impact by their perceptions of the usefulness of mobile learning. Morahan-Martin [26] study also argued female students used the Internet very less frequently, and they also spend less time than their male counterparts.

A study was conducted by Li and Kirkup [27] with 465 students where 220 students were Chinese and 245 students were British. Their study indicated that there is a difference with the gender in Chinese and British students. A study conducted by Kay [28] with 659 secondary school students on gender differences, and the results found that there is a positive attitude with the male students than female students. Tsai and Tsai [29] "investigated and compared the gender gaps of college students' Internet use and Internet attitudes between 1995 and 2002 with a conclusion that both gaps were lessoning or disappearing altogether in 2002." A study was conducted by Wang et al. [11] in Taiwan and their respondents were 330. Results from [11] indicated that gender has a positive influence on the social as well as on self-learning.

3.1 Theoretical Framework

This study will use the UTAUT model. The UTAUT model was proposed by Venkatesh et al. [30], and it was developed by merging eight models of technology acceptance to information technology or information system research study. In this research, “performance expectancy” means the belief of use ML by the international students; “effort expectancy” means international students are associated with the ML; “social factors” means international student usages with the ML; “facilitating conditions” means that the technical infrastructure, as well as the organizational infrastructure, are available to use ML; and finally, the “behavioral intention” means performance of international students’ interaction.

4 Aim

This paper’s aim is to design a model for the international students’ gender impact to use mobile learning in tertiary education.

4.1 Research Questions

(a) Analyze the first-year international students’ gender impact on “performance expectancy” to the “behavioral intention” in tertiary education;
(b) Analyze the first-year international students’ gender impact on “effort expectancy” to the “behavioral intention” in tertiary education;
(c) Analyze the first-year international students’ gender impact on “social factors” to “behavioral intention” in tertiary education;
(d) Analyze the first-year international students’ gender impact on “facilitating condition” to “behavioral intention” in tertiary education.

To design a model for the international students’ gender impact to use mobile learning in tertiary education.

4.2 Research Hypotheses

The following research hypotheses were taken into consideration:

$H_0$1 Gender influence positively on “performance expectancy” to “behavioral intention” m-learning by international students in tertiary education;
$H_0$2 Gender influence positively on “effort expectancy” to “behavioral intention” m-learning by international students in tertiary education;
$H_0$3 Gender influence positively on “social factors” to “behavioral intention” m-learning by international students in tertiary education;
$H_0$4 Gender influence positively on “facilitating condition” to “facilitating condition” m-learning by international students in tertiary education.

5 Methodology

This pilot study began by collecting data anonymously from first-year international students, and these students participated voluntarily from a tertiary education in Canada. The questionnaires of this study were distributed between November 27 and December 23, 2017. International students (first year) participated anonymously from various departments. Before distributing questionnaires, a permit was granted from the Comité institutionnel d'éthique de la recherche avec des êtres humains (CIEREH) of the institution where the research took place. In this study, 17 international students participated, but 12 international students were considered for this study due to the equal number of participants were considered (6 female international students and 6 male international students). All the data were captured on Microsoft Excel. Having captured data on the Microsoft Excel, data were analyzed using the WarpPLS 5.0 version. Furthermore, a UTAUT model was used to validate the questionnaire and these variables were "performance expectancy (PE)" (section A), "effort expectancy (EE)" (section B), "social factors (SF)" (section C), and the "facilitating conditions (FC)" (section D) that predict the "behavioral intention (BI)" (section E) [30].

6 Results

6.1 Cronbach's Alpha Values

According to [31], if the value of α is 0.70 or even greater 0.70, then the alpha value (α) is considered acceptable. On the other hand, Cronbach [31] indicated that when variables are less than 10 items, in that case, the alpha value (α) may be 0.5 or less. This study considered five variables and Table 1 shows that alpha (α) coefficients are less than 0.5 only with the facilitating conditions, but with all other variables Cronbach's alpha coefficients are greater than 0.7.

Table 1 Cronbach's alpha (α) values, composite reliability values, and total items used in each variable

Variables	Alpha (α) values for Cronbach	Composite reliability coefficients	Total item used
PE	0.870	0.907	5
EE	0.884	0.916	5
SF	0.876	0.914	5
FC	0.498	0.666	5
BI	0.983	0.986	5

6.2 A Model for Female International Student's to Use M-Learning

Figure 1 shows that female students have a significant impact on the performance expectance (PE) with a value of $\beta = -0.42$ (when $P < 0.01$) and facilitating condition (FC) with a value of $\beta = -0.54$ (when $P < 0.01$) but female students do not have significant impact on the effort expectancy with a value of $\beta = -0.12$ (when $P = 0.13$) and social factors with value of $\beta = -0.14$ (when $P = 0.08$). Figure 1 also shows that female international students having impact on the performance expectancy and social factors to behavioral intention to use the mobile learning in tertiary education when $R^2 = 0.89$. However, female students do not have much impact on the effort expectancy and facilitating condition to behavioral intention using mobile learning by international students in tertiary education.

Figure 2 shows that male students have a significant impact on the performance expectance (PE) with a value of $\beta = -0.51$ when $P < 0.01$, social factors (SF) with a value of $\beta = -0.38$ when $P < 0.01$ 01, and finally, the facilitating condition (FC) with a value of $\beta = -0.27$ when $P < 0.01$. Nevertheless, male student does not influence significantly to effort expectancy ($\beta = -0.15$ when $P = 0.07$). Figure 2 also shows that male students got a significant impact on the PE, EE, to behavioral intention to use mobile learning in tertiary education when $R^2 = 0.98$. Furthermore, male international students do not have much impact on the SF to BI the mobile learning in tertiary institutions.

Having analyzed Fig. 1 as well as Fig. 2 show that male international students got a significant higher impact on the PE, SF, and FC; but on the other hand, female student having an impact on the PE and FC. Female international students got a significant

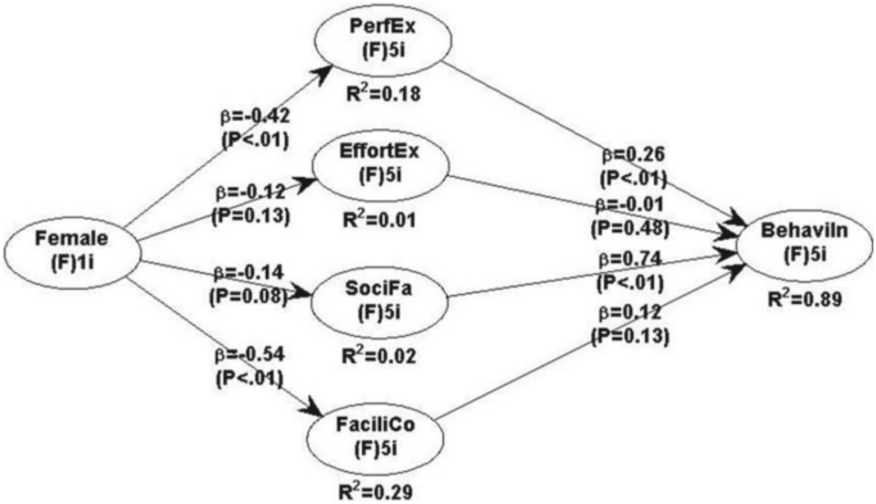


Fig. 1 Female usages of m-learning in tertiary education

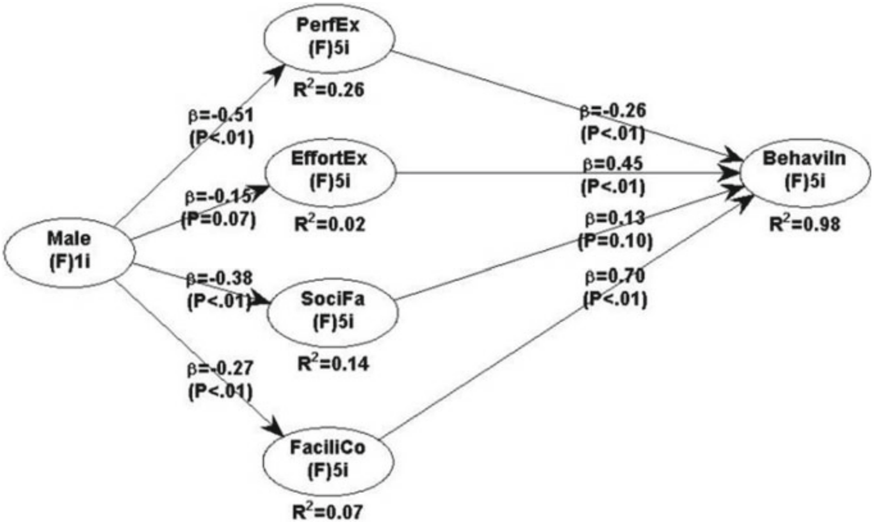


Fig. 2 Male usages of m-learning in tertiary education

impact on the PE and SF to BI to use mobile learning in tertiary education. Finally, PE, EE, and FC also significantly influence to *BI* to use mobile learning in tertiary education by male students.

Figure 3 shows that gender has a significant impact on the effort expectance (PE) with a value of $\beta = -0.51$ when $P < 0.01$, facilitating condition (FC) (when $\beta = -0.46$ and $P < 0.01$). On the other hand, gender does not have a significant impact on the performance expectancy and social factors. Finally, the PE (when $\beta = 0.26$ and $P < 0.01$) and social factors with a value of $\beta = 0.74$ when $P < 0.01$ got a

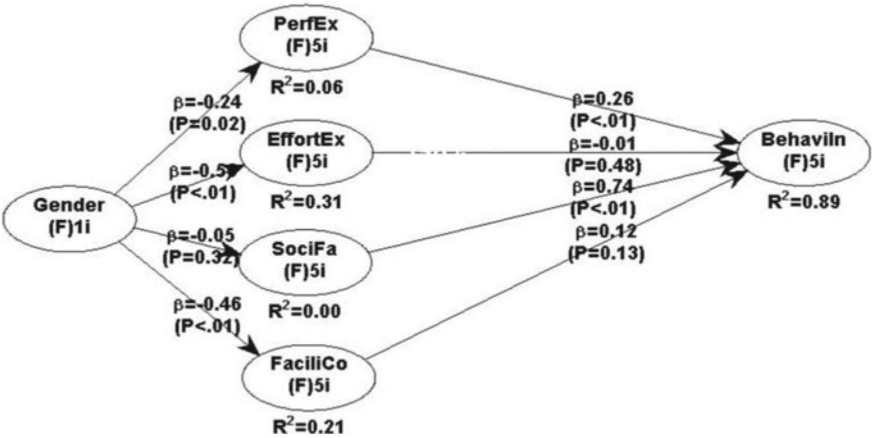


Fig. 3 A model of the gender (male and female) impact to use the m-learning in tertiary education

Table 2 Fit index, model, and recommendation

Fit index	Model	Recommendation
APC	0.303	$P = 0.002$
ARS	0.294	$P = 0.003$
AARS	0.214	$P = 0.012$
AVIF	2.530	Acceptable if ≤5, ideally ≤3.3
AFVIF	6.121	Acceptable if ≤5, ideally ≤3.3
GoF	0.461	Small ≥0.1, medium, ≥0.25, large ≥0.36
SPR	0.875	Acceptable if ≥0.7, ideally = 1
RSCR	0.999	Acceptable if ≥0.9, ideally = 1
SSR	0.875	Acceptable if ≥0.7
NLBCDR	1.000	Acceptable if ≥0.7

APC Average path coefficients, *GoF* Tenenhaus GoF, *ARS* Average R-squared, *SPR* Simpson's paradox ratio, *AARS* Average adjusted R-squared, *RSCR* R-squared contribution ratio, *AVIF* Average block VIF, *SSR* Statistical suppression ratio, *AFVIF* Average full collinearity VIF, *NLBCDR* Nonlinear bivariate causality direction ratio

significantly positive impact to BI to use mobile learning by international students in tertiary education.

6.3 Model Fit and Quality Indices

A model can be measured two ways are namely convergent and the discriminant validity. In the case of convergent, it is analyzed with different categories. These categories are the questions, the reliability, constructions of the reliability, and the variance extracted with the help of constructs. On the other hand, discriminant validity can be measured based on the correlation [32]. Table 2 shows how good the model fit is.

6.4 Mean and Standard Deviation for PE, EE, SF, FC, and BI

Table 3 shows that PE significantly influence on BI to use the mobile learning by international students in tertiary education when the mean of PE is 2.50 and standard deviation of PE is 1.00 for the x-axis. Similarly, in the case of y-axis, the mean of BI is 2.17 and standard deviation of BI is 1.27. EE got a significant influence to *BI* in order to use mobile learning by international students in tertiary education when

Table 3 Mean and standard deviation of x-axis and y-axis for PE, EE, SF, FC, and BI

Variables	Mean	SD	Axis
PE BI	2.50 2.17	1.00 1.27	X Y
EE BI	2.08 2.17	0.51 1.27	X Y
SF BI	2.42 2.17	1.08 1.27	X Y
FC BI	2.42 2.17	1.16 1.27	X Y

SD Standard deviation, *X* x-axis, *Y* y-axis

the mean of EE is 2.08 and the standard deviation is 0.51 for the x-axis. Similarly, in the case of y-axis, the mean of BI is 2.17 and the standard deviation is 1.27. *Social factors* (SF) also influence BI to use the mobile learning by international students in tertiary education when the mean of SF is 2.42 and the standard deviation is 1.08 for the x-axis. Similarly, in the case of y-axis, the mean of BI is 2.17 and the standard deviation is 1.27. FC also influence to BI in order to use the mobile learning by international students in tertiary education when the mean of FC is 2.42 and the standard deviation is 1.16 for the x-axis. Similarly, in the case of the y-axis, the mean of BI is 2.17 and the standard deviation is 1.27.

6.5 Correlation

Table 4 indicates *p*-values correlations when PE is 1.000, EE is 1.000, SF is 1.000, FC is 1.000, BI is 1.000, and finally GN (gender) is 1.000 for the use of mobile learning in tertiary education.

Table 4 Values of correlations for PE, EE, SF, FC, BI, GN

	PE	EE	SF	FC	BI	GN
PE	*1.000*	0.271	0.005	0.455	<0.001	0.457
EE	0.271	*1.000*	0.467	0.445	0.369	0.060
SF	0.005	0.467	*1.000*	0.507	<0.001	0.887
FC	0.455	0.445	0.507	*1.000*	0.948	0.135
BI	<0.001	0.369	<0.001	0.948	*1.000*	0.358
GN	0.457	0.060	0.887	0.135	0.358	*1.000*

7 Discussion and Conclusion

The m-learning aspects are very important in tertiary education in Canada because it is in the early stage. Twelve participants participated in this pilot study, and all the participants were from first-year international students. A questionnaire was distributed through the line survey among first-year international students. This study has used the UTAUT model, and all the variables in the questionnaire were validated by the UTAUT model. Firstly, data were captured in the Microsoft Excel. Secondly, having captured the data, it was analyzed using the WarpPLS 5.0 version. Three structural equation modelings have designed, and these are for the male students, female students, and for the gender (male and female). Model for **male** students' shows that male students having an impact on the PE, SF, and on FC. Furthermore, PE, EE, and FC described 98% of the difference in the BI to use mobile learning. Structural equation model (SEM) for **female** students' shows that female students having an impact on the PE and on the FC. Moreover, PE and SF described 89% of the difference to BI in terms of using mobile learning. Structural equation model (SEM) for **gender** shows that gender has an impact on the EE and on the FC. In addition, PE and SF described 89% of the difference to the BI in order to use mobile learning and these results are in line with the findings [33].

The findings of this research in line with research question and the first research question answer indicated that PE ($\beta = -0.24$ when $P = 0.02$) does not have a significant impact on BI to use the mobile learning in the tertiary education. The *second research question answer indicated* that EE ($\beta = -0.50$ when $P < 0.01$) has a significant impact to BI to use the mobile learning in tertiary education. *Third research question indicated* that SF ($\beta = -0.05$ when $P = 0.32$) does not have a significant impact to *BI* in terms of using the mobile learning in tertiary education. *Fourth, research questions answered* FC ($\beta = -0.46$ when $P \leq 0.01$) got a significant impact to BI in order to use the mobile learning in tertiary education. *Second and fourth hypotheses* got accepted; however, *first and the third hypotheses* got rejected since PE and SF do not significantly get the impact to BI in order to use the mobile learning by international students. Having comparatively analyzed, it shows that male international students got a significantly higher impact on the PE, SF, and FC; nevertheless, female students got a significant impact on the PE and SF to BI in order to use the mobile learning in tertiary education. Finally, PE, EE, and FC have a significant impact on BI to use mobile learning by male students in tertiary education.

Acknowledgements Consent: All the author state that there is no conflict of interest. We take the responsibility involved in the publication of our paper.

References

1. Berking P, Birtwhistle M, Gallagher S, Haag J (2013) Mobile learning survey report. Advanced Distributed Learning Initiative
2. Taleb Z, Sohrabi A (2012) Learning on the move: the use of mobile technology to support learning for university students. In: International conference on education and educational psychology (ICEEPSY 2012). Proc Soc Behav Sci 69:1102–1109
3. Mansouri S, Kaghazi B, Kharmali N (2010) Survey of students attitude about M-learning in Gonbad Payam-noor University. In: The first conference of Iran's mobile value-added. IRIB Conference Center, pp 1–9
4. Kafyulilo A (2012) Access, use and perceptions of teachers and students towards mobile phones as a tool for teaching and learning in Tanzania. Educ Inf Technol 19(1):115–127
5. Ozuorcun NC, Tabak F (2012) Is m-learning versus e-learning or are they supporting each other. Proc Soc Sci Behav 46:294–305
6. Turkle S (1997) Life of the screen: identity in the age of the internet. Touchstone, New York
7. Mitra A, Willyard J, Platt C, Parsons M (2005) Exploring web usage and selection criteria among male and female students. J Comput Mediat Commun 10(3)
8. Zhang YX (2005) Age, gender, and Internet attitudes among employees in the business world. Comput Hum Behav 21:1–10
9. Muhanna W, Abu-Al-Sha'r A (2009) University students' attitudes towards cell phone learning environment. Int J Interact Mob Technol 3(4)
10. Kwon HS, Chidambaram L (2000) A test of the technology acceptance model the case of cellular telephone adoption. In: Proceedings of the 33rd Hawaii international conference on system sciences, 2000. IEEE, Hawaii, pp 1–10
11. Wang Y, Wu M, Wang H (2009) Investigating the determinants and age and gender in the acceptance of mobile learning. Br J Edu Technol 40(1):92–118
12. Kukulska-Hulme A (2009) Will mobile learning change language learning? Recall 21(2):157–165
13. Hargittai E, Shafer S (2006) Differences in actual and perceived online skills: the role of gender. Soc Sci Quart 87(2):432–448
14. Li N, Kirkup G (2007) Gender and cultural differences in Internet use: a study of China and the UK. Comput Educ 48(2):301–317
15. Motiwalla LF (2007) Mobile learning: a framework and evaluation. Comput Educ 49(3):581–596
16. Ong C, Lai J (2006) Gender differences in perceptions and relationships among dominants of e-learning acceptance. Comput Hum Behav 22(5):816–829
17. Basak SK, Wotto M, Bélanger P (2018) University students' m-learning adaption behavioral factors: a pilot study. In: 2018 IEEE 9th annual information technology, electronics and mobile communication conference (IEMCON), pp 68–73
18. Koohang A (2004) Students' perceptions toward the use of the digital library in weekly web-based distance learning assignments portion of a hybrid program. Br J Edu Technol 35(5):617–626
19. Enoch Y, Soker Z (2006) Age, gender, ethnicity and the digital divide: University students' use of web-based instruction. Open Learn 21(2):99–110
20. Pew Internet and American Life Project (2008). http://www.pewinternet.org
21. Kay RH (1992) An analysis of methods used to examine gender differences in computer-related behaviour. J Educ Comput Res 8(3):323–336
22. Hilao MP, Wichadee S (2017) Gender differences in mobile phone usage for language learning, attitude, and performance. Turk Online J Distance Educ TOJDE 18(2):68–79
23. Durndell A, Thomson K (1997) Gender and computing: a decade of change. Comput Educ 28(1):1–9
24. Whitely BE Jr (1997) Gender differences in computer related attitudes and behavior: a meta analysis. Comput Hum Behav 13(1):1–22

25. Ong CS, Lai JY (2006) Gender differences in perceptions and relationships among dominants of e-learning acceptance. Comput Hum Behav 22:816–829
26. Morahan-Martin J (1999) Women and internet: promise and perils. Cyber Psychol Behav 3(5):683–696
27. Li N, Kirkup G (2007) Gender and cultural differences in Internet use: a study of China and the UK. Comput Educ 48:301–317
28. Kay RH (2009) Examining gender differences in attitude toward interactive classroom communications systems (ICCS). Comput Educ 52:730–740
29. Tsai MJ, Tsai CC (2010) Junior high school students' Internet usage and self- efficacy: a re-examination of the gender gap. Comput Educ 54:1182–1192
30. Venkatesh V, Morris M, Davis G, Davis F (2003) User acceptance of information technology: towards a unified view. Manage Inf Syst Quart 27(3):425–478
31. Cronbach LJ (1951) Coefficient alpha and the internal structure of tests. Psychometrika 16(3):297–334
32. Hair JF, Black WC, Babin BJ, Anderson RE (2010) Multivariate data analysis, 7th edn. Prentice Hall, Englewood Vliffs
33. Alharbi S, Drew S (2014) Mobile learning system usage: scale development and empirical tests. Int J Adv Res Artif Intell (IJARAI) 3(11):31–47

Industrial Automation of Process for Transformer Monitoring System Using IoT Analytics

Vaishali Khairnar, Likhesh Kolhe, Sudhanshu Bhagat, Ronak Sahu, Ankit Kumar and Sohail Shaikh

Abstract Multiple devices interconnected with each other via the Internet are the key concept behind IoT. It allows autonomous devices with the possibility to use the Internet for communication and exchange of data. This paper focuses on monitoring the transformer in real-time fault detection and records distinct operating parameters of the transformer like voltage imbalance, load current, transformer oil levels, temperature, vibration. Based on these parameters, the transformers fail state (i.e. a state where transformer malfunctions or completely stops working) and health (i.e. voltage, current, oil levels, temperature and vibration) are predicted by making use of an artificial neural network (ANN) algorithm. Use of this technology can minimize working efforts, thereby improving accuracy, stability, efficiency. Thus, remote monitoring and machine control are achieved, as well as ANNs help to determine the performance and yield appropriate measures accordingly. In this case, sensors are used to sense the important parameters of equipment such as current, voltage oil level in any operating transformer. By analyzing relevant data using ANNs, this system will be beneficial in many industries. Likewise, this system is generalized to be used in a wide array of industrial automated machines.

V. Khairnar · L. Kolhe · S. Bhagat (✉) · R. Sahu · A. Kumar · S. Shaikh
Information Technology, Terna Engineering College, Navi Mumbai, India
e-mail: sudhanshubhagat101@gmail.com

V. Khairnar
e-mail: vaishalikhairnar@ternaengg.ac.in

L. Kolhe
e-mail: likhesh8@gmail.com

R. Sahu
e-mail: ronaksahu0204@gmail.com

A. Kumar
e-mail: akumar.kumar043@gmail.com

S. Shaikh
e-mail: sohailks118@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_115

Keywords Real-time monitoring · Artificial neural networks · Prediction · Communication module

1 Introduction

In our daily life, electricity has become very essential and life without electricity is hard to imagine. Similarly, electricity is also very crucial for different industries, and an industry comprises a variety of different machines and appliances which need a constant supply of electricity for their smooth functioning. These machines are also responsible for effective production and manufacturing services which determine the growth of any industry. Malfunctioning of these machines due to voltage instabilities and currency fluctuations will lead to losses on large scale also due to the heavy current applications of the industry, and the workers working on the field can be subjected to dangerous shocks.

In order to avoid any damage to the machine as well as glitches like voltage and current, distortions can be resolved and fixed with the help of a transformer. A custom current transformer constantly measures the electric current, and even if the current level exceeds due to electric fluctuations, the transformer automatically eliminates excess current flow, thereby reducing the damage to a bare minimum. In other words, transformers are designed to use electromagnetic induction to modify an alternating current voltage that runs from one electric circuit to another. Proper care and maintenance of the transformer are often neglected largely due to its reliability leading to a cutback in the life span of the transformer, which will eventually result in downturn and loss. Keeping this in mind, perception, veracity, and analysis of data are important, which is obtained by monitoring of the transformers. To improve the transformer's functioning and reliability, evaluation of the maintenance data gathered during monitoring is important. Furthermore, by making use of powerful (ANNs) artificial neural networks, relevant information on existing issues can be obtained that may result in predicting the need for the replacement or repair of the transformer.

2 Literature Survey

Transformers are important to power system components whose health condition needs to be ensured for safe and reliable operation of any power system network [1]. The main aim of this system is the distribution transformer monitoring and controlling through IOT. If there are any deviations from the normal or an emergency situation occurs, the system sends SMS messages to the mobile phones containing information about the deviation according to some predefined instructions programmed in the microcontroller [2].

3 Methodology

In this automated transformer monitoring system, we make use of technologies like IoT and analytics which help to increase in the performance and throughput of the system.

In order to perform analytics on any system using neural networks, we require a large amount of dataset. This dataset is collected in real-time using different sensors like temperature sensor (LM35), vibration sensor, humidity sensor (DHT11), and ultrasonic sensor. These sensors are controlled and monitored with the help of Arduino UNO microcontroller which is an open-source microcontroller board based on the Microchip ATmega328p, developed by https://www.arduino.cc.

The data collected by these sensors is then stored in SQL database with regular time intervals. These sensors also notify the real-time state of the transformer. If a condition arises with the transformer where it is overheating or damaged, it will be quickly detected by the sensors attached to it and the microcontroller will inform the server. A web portal is developed to interface this complex system so that the user can have a high benefit of the system. This web portal has admin and user access. The admin will have the privilege to monitor the entire system in real time, whereas the user will focus on the output of the system.

Furthermore, once a large amount of data related to different factors of the transformer that influence its performance are collected by different sensors attached to the transformer, the next step is to feed this data to the neural network algorithm. The end goal of this system is to analyze the different sensor data and to determine the fail state of the transformer. With the help of neural networks algorithm, we can predict the health and the life of a transformer, and we can repair any damage to the transformer prior to the further loss in the system (Fig. 1).

The functional block is divided into four fundamental blocks of the system. The first block is being the power supply module which powers the entire system and provides adequate voltage to the entire sensor network.

The second block includes the sensor section which includes all the different sensors which help to monitor the different influential factors of the transformer. The DHT11 sensor is used to measure the external temperature and humidity level around the transformer. The ultrasonic sensor monitors the oil level in the oil tank of the transformer and helps to calculate the oil consumption of the transformer. Vibration sensors are sensors used for measuring and analyzing linear velocity and displacement. It is used to identify and determine the condition and state of the transformer. The LM35 temperature sensor is used to detect the precise temperature in centigrade. It is used to measure the internal temperature of the transformer.

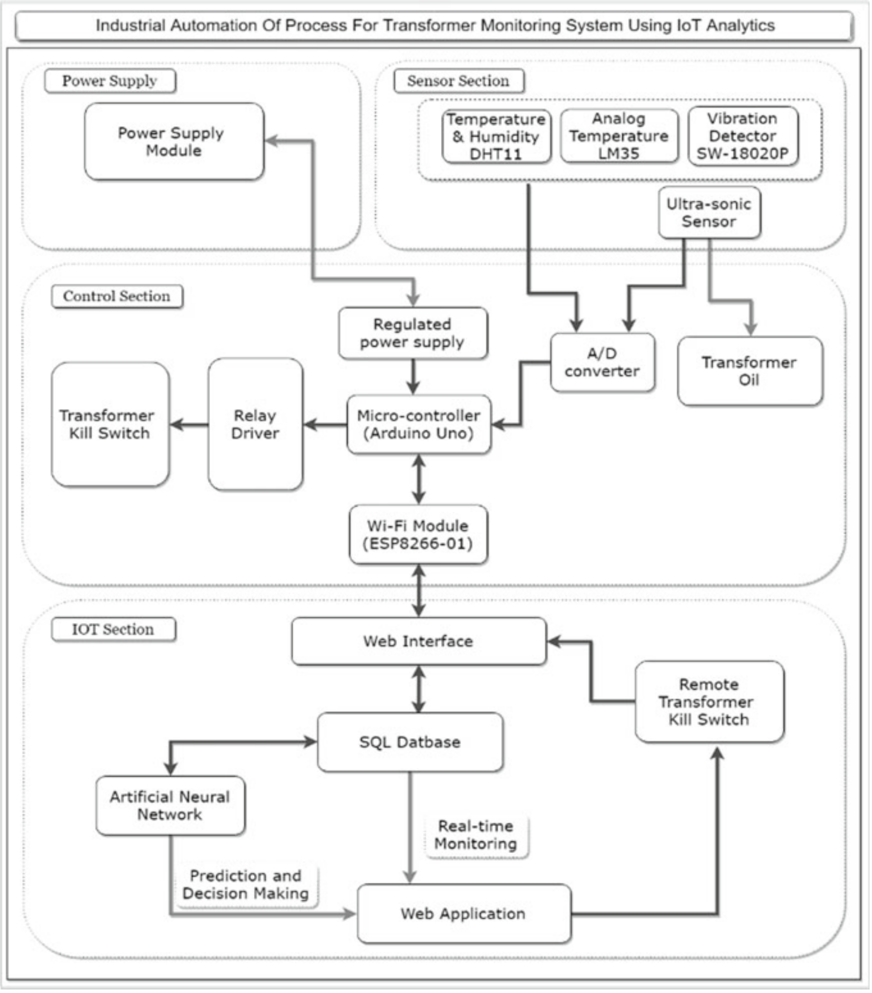

Industrial Automation Of Process For Transformer Monitoring System Using IoT Analytics
Power Supply
Power Supply Module
Sensor Section
Temperature & Humidity DHT11
Analog Temperature LM35
Vibration Detector SW-18020P
Ultra-sonic Sensor
Control Section
Regulated power supply
A/D converter
Transformer Oil
Transformer Kill Switch
Relay Driver
Micro-controller (Arduino Uno)
Wi-Fi Module (ESP8266-01)
IOT Section
Web Interface
Remote Transformer Kill Switch
SQL Datbase
Artificial Neural Network
Real-time Monitoring
Prediction and Decision Making
Web Application

Fig. 1 Functional block

The next and very important block is the microcontroller where the sensors are connected and controlled by the Arduino UNO microcontroller. These sensors are programmed to calculate and measure different parameters of the transformer and record them at regular time intervals on the server. These parameters determine the present state and health of the transformer, and also in any conditions where the sensors parameters indicate an irregular behavior of the transformer leading to malfunction of any kind; in such cases, the microcontroller is programmed to take appropriate measures suitable for the transformer in that present state which includes powering down the transformer, thereby reducing the risk of high damage to the transformer.

The final and most crucial block of this system is the IoT block where the web portal plays a major role in interfacing the entire system to the user, thereby making it simpler to manage the system. Furthermore, the powerful neural network algorithm is used for the prediction of the fail state of the transformer and also to determine the health so that we can take necessary actions before the damage to the machine increases. The ANN algorithm provides better accuracy and more precise results.

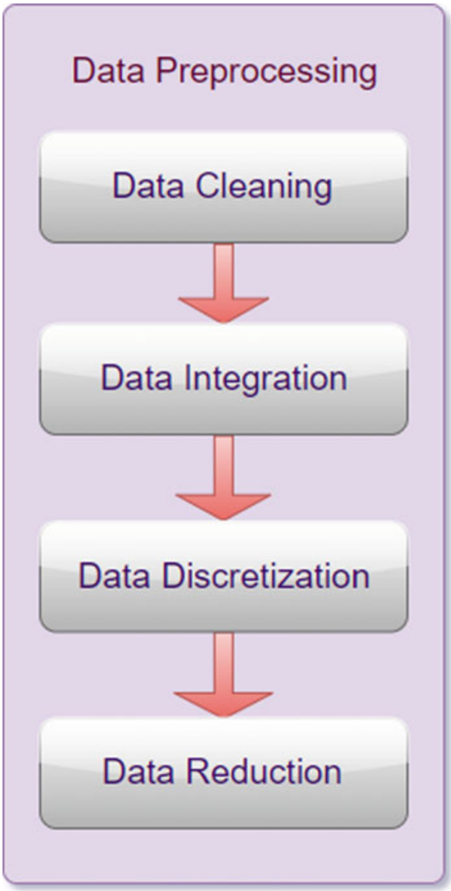
3.1 Artificial Neural Networks (ANNs)

The artificial neural network is the key element of this system, which takes in the sensor values, stores in the database as an input parameter, processes this parameter to produce a predictive analysis of the transformer, and determines its fail state. The ANN algorithm undergoes data preprocessing which prepares the raw values stored in a database for further processing. Relevant data might not get recorded due to misunderstandings like equipment or sensor malfunction, the recorded data history or modifications to the data can be overlooked the missing data, and particularly, some attributes of tuples with missing values may need to be inferred. Data preprocessing is a form of data mining approach where raw data is converted into a logical format. It is a proven method for resolving such issues. The traditional data preprocessing method starts with data which is assumed ready for analysis without any feedback. The main difficulty for data preprocessing is an inconsistency between datasets. The following are the major tasks involved in data preprocessing (Figs. 2 and 3).

- **Data Cleaning**: It is the process of filling the missing values, identifies, removes outliers, smoothes the noisy data, and resolves inconsistencies.
- **Data Integration**: It is the process of integrating multiple files, data cubes, and databases.
- **Data Transformation**: It involves the task of data normalization and data aggregation, e.g., to transform V [min, max] to V′ [0, 1].
- **Data Reduction**: It is the process of reducing representation in terms of volume but producing similar analytical results.
- **Data Discretization**: It is a part of data reduction along with specific importance for numeric data.

We make use of ‘Keras’ library which gives a high level of abstraction and is built on top of TensorFlow library, and we use TensorBoard to analyze our model’s efficiency.

Fig. 2 Steps involved in data preprocessing

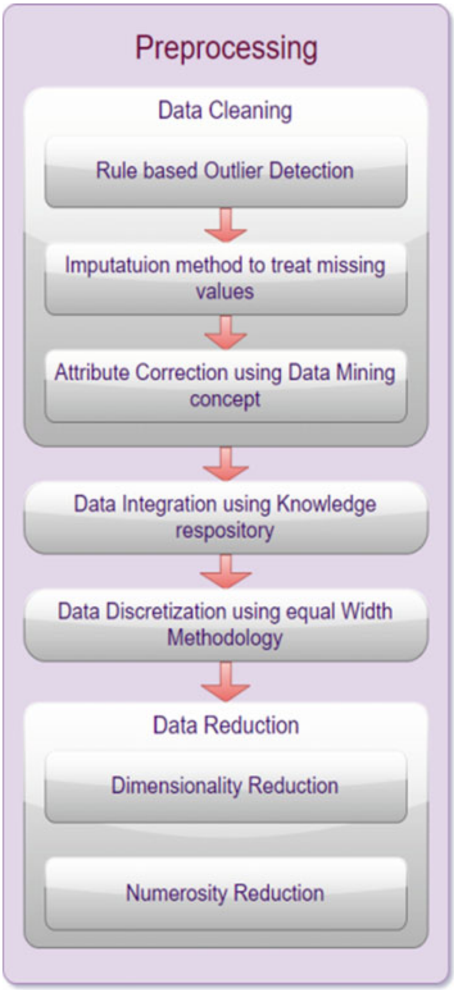


4 Results

Predicting the fail state of a transformer is the most crucial part of this system. The ANN will consider the transformer parameters for prediction and notify the user accordingly. The developed system is designed in such a way that it can activate the emergency alert. Figure 4 shows the confusion matrix of the ANN model.

Figure 5 is the accuracy graph which shows the comparison of accuracy of training set of the data with accuracy of testing set of the data. Figure 6 is the loss graph which compares the losses occurred in the training set of the data with the testing set of the data. Real-time data is collected and processed by ANN, and the result is predicted; taking into consideration, the testing set of the data is displayed on the web application.

Fig. 3 Process of preprocessing


Preprocessing
Data Cleaning
Rule based Outlier Detection
Imputatuion method to treat missing values
Attribute Correction using Data Mining concept
Data Integration using Knowledge respository
Data Discretization using equal Width Methodology
Data Reduction
Dimensionality Reduction
Numerosity Reduction

5 Conclusion

This paper discusses the complete solution for monitoring and controlling the transformer by using sensors, relay module, communication module, and web application. The designed system also can predict the fail state of the transformer and alert the user about it.

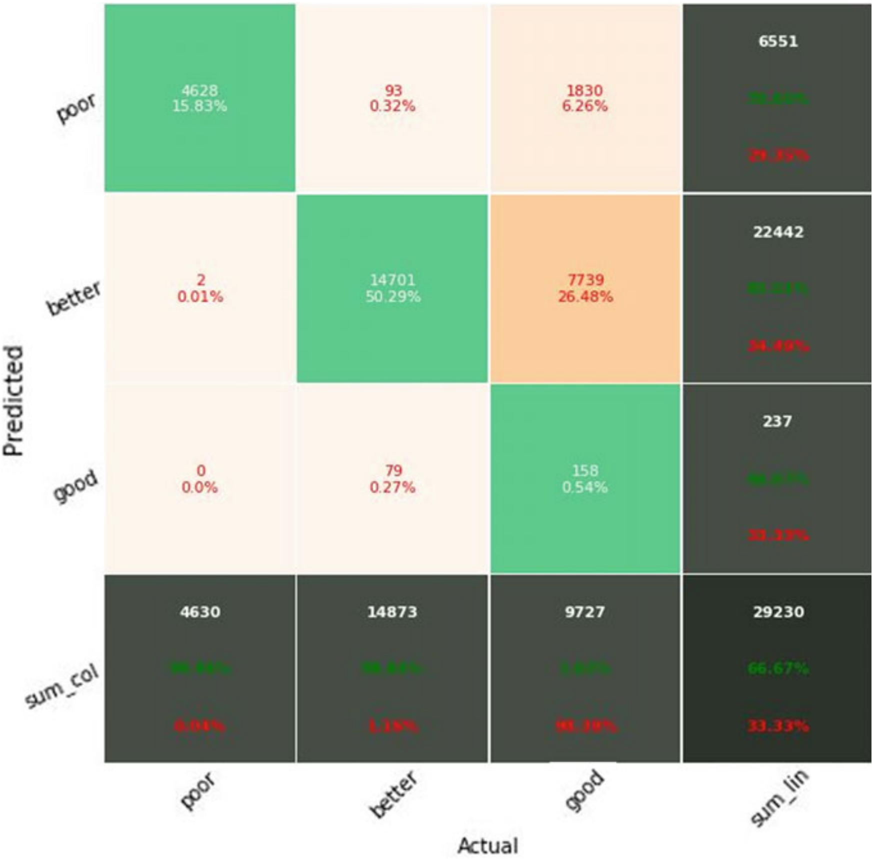


Fig. 4 Confusion matrix

All the transformer sensors are continuously monitored by ANN. The user is notified when the transformer experiences an abnormal condition, appropriate actions can be taken to prevent any disastrous failure of a power transformer.

By using web application, user can view historical data and monitor real-time parameters of the transformer easily.

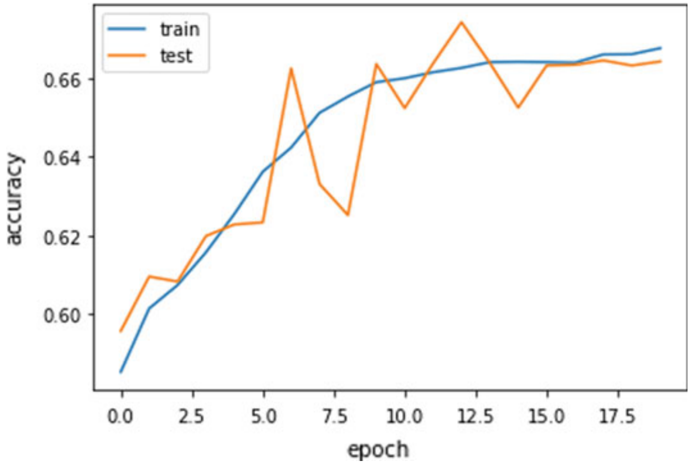


Fig. 5 Accuracy graph

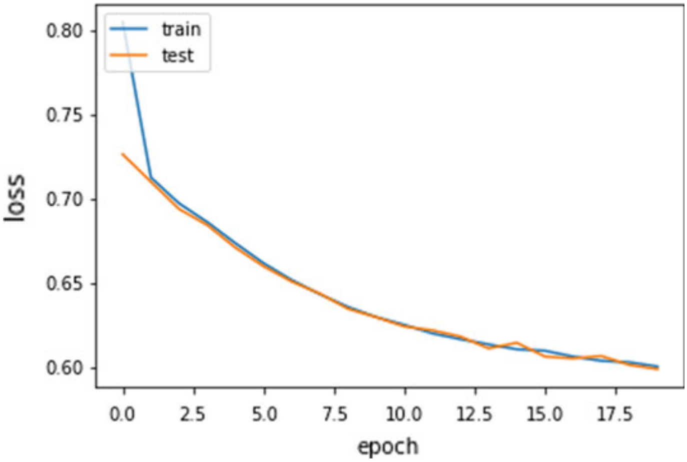


Fig. 6 Loss graph

References

1. Balaji Kamlaesan K, Kumar A, Alex David S Analysis of transformer faults using IOT. In: 2017 IEEE international conference on smart technologies and management for computing, communication, controls, energy and materials. Veltech Dr. RR & Dr. SR University, Chennai
2. Sivaranjani S, Lokesh S, Vignesh M, Vijayaragavan N, Goutham S IOT based distribution transformer monitoring system. Int J Current Trends Eng Res (IJCTER) (Department of Electrical and Electronics Engineering, V.S.B Engineering College, Karur)

A Comparative Study on Various Search Techniques for Gaming Applications

B. Sunil, M. R. Naveen Kumar, B. N. Gowrishankar and N. S. Prema

Abstract The main objective of this research work is to deduce best among the existing search techniques. The various methods or the algorithms that we are going to discuss here are breadth-first search, depth-first search, and A* algorithm. Comparing various search techniques that are used in artificial intelligence problems for gaming applications.

Keywords Search techniques · DFS · BFS · A*

1 Introduction

Searching is a process of determining whether an element is a part of the data set or not. Most of the search belongs to either sequential or binary. A sequential search is conducted on small data sets where the list is unsorted. Binary search is performed on large data sets of the sorted list. The motivation behind the searching technique is to solve artificial intelligence problems; here, we are considering many gaming applications and how the different search algorithms are used to solve the game problems and how the searching algorithms are modified to get accurate results depending on the type of problems. Performance of artificial intelligence problems mainly depends on the complexity of the searching techniques.

2 Review of Literature

In [1], the author has proposed a better algorithm to solve the Japanese puzzle which is a combination of logical rules and DFS where the performance of the algorithm is better than the DFS. The results which they have got are for 5 * 5, 5 * 6 and 10 * 10;

B. Sunil (✉) · M. R. Naveen Kumar · B. N. Gowrishankar · N. S. Prema
Department of Information Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India
e-mail: sunilbayanaboyana12@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_116

the time taken is less than 0.1 s. The author has concluded that the Japanese puzzle problem is solved by two phases; first, with the logical rules to solve cells as many as possible and in the second phase, the unknown cells are solved using DFS with branch and bound scheme based on column information. The method which they have used gives correct answers for black patterns quickly and also fastens the DFS algorithm.

In [2], the author has proposed efficiency, comparison rapidity, and intelligence about seven pathfinding an algorithm for 3D gaming applications and also proposed depth direction A* method which uses linear graph theory to find shortest paths in maps and to avoid barriers in the multilayer environment. The result which they have got for one layer of ground that is outdoor is as follows for different search algorithms considering various maps. The author has concluded that the iterative depth *D* A* algorithm uses the least memory with time complexity $O(b * d)$ and space complexity $O(d)$. The depth direction A* expands more node than A* and has a very smooth pathway.

In [3], the author has proposed an algorithm for Babylon tower game that uses DFS column by column to reach the goal state. The game goal is to sort each ball of the same color on the same column and sort each ball in each column based on the brightness of the color of the ball. The average number of steps taken to reach the goal state is 151 steps for easy, 295 steps for medium difficulty, and 431 steps for hard difficulty. And, the time taken for easy is 9.17680325 ms, for medium difficulty 13.659335 ms, and for hard difficulty 16.8398884.

In a study in [4], the author has proposed the combination of A* algorithm and dynamic pathfinding A* algorithm for a game of racing car which states about the obstacles in the dynamic environment of the game and how dynamic pathfinding A* addresses this problem. In the result, the author has proposed the comparison between the combined algorithm A* and DPA with DPA for different states of car bending at 60°, 90°, spiral trajectory, lane letter S, empty trajectory and trajectory with obstacles based on the results of all the abovementioned states combination of A* and DPA has given the car reaching the final state and in the case of obstacles, the finish line is reached three times out of five experiments, and finally, the author has concluded that by combining A* and dynamic pathfinding algorithm can be implemented in car racing game; the grid representation method used has an effect on the route real obtained by A* algorithm. The DPA has affected by the obstacle position and trajectory shape.

In [5], the author used the concept of artificial intelligence where goat must escape the enemies, so the player playing in goat's place must win the game. A* algorithm is used to find the shortest distance between the goat and the plants in the form of a labyrinth and should be able to mislead the enemy. Pathfinding is the application of the A* algorithm to the game.

A* is an algorithm used to solve many problems. In pathfinding, this algorithm checks the most promising node location it has ever seen. If the node visited is the promising or the target node, then the algorithm will stop the execution. If not, the algorithm will store the node's neighboring data for further nodes. It is the famous algorithm used to find the path in the artificial intelligence field [6].

3 Search Techniques Methodology

3.1 Breadth-First Search

If we consider the BFS searching technique, a guaranteed solution will be given if the searching element is in the list. The complexity in BFS is that it visits each and every node in the list or tree and those nodes will be stored. If memory is not a constraint in your problem, then BFS technique gives a very good result.

BFS is most similar to Dijkstra's Algorithm for the shortest path. Here, the search is exhaustive, entire graph or tree at each level is expanded, and the search operation is performed [7]. The search will go up to the deepest level of the tree and memory to store each and every node is more.

Algorithm: BFS

a. Create a Node_List variable and set it to start.
b. Until there is a goal state or Node_List is empty:

    a. Remove from Node List the first element and call it E. If Node_List has been empty, quit.
    b. For each instance where each rule corresponds to the state described in E do:
        i. Use the rule to create a new state.
        ii. If the goal state is the new state, quit this state and return it.
        iii. If not, add the new state to Node_List's end.

3.2 Depth-First Search

It works on the technique of uniform search by generating the decedents of most recently expanded node until the goal node cutoff reached and then backtracked one of the most recently expanded nodes. In Depth-first search, only the nodes from initial to goal node are stored, so less memory is required [8]. One of the limitations of DFS is that if the goal node is not present in the graph or tree, then the search will be exhaustive and it searches only one side of the tree and reach deadlock situation.

Algorithm: DFS

a. If the starting state is the goal state, quit success and return it.
b. Otherwise, do the following until you find or fail the goal state.

    a. Generate the initial state's successor, E. Signal failure when there are no more successors.
    b. Call DFS as the starting state with E.
    c. Signal success if success is returned. Continue in this loop otherwise.

3.3 A* Algorithm

A* is the most popular algorithm used for finding a path between two locations in the map area [9]. The A* algorithm has two sets one is an open set and another one is the closed set. The open set is used to record the areas adjacent to those already evaluated and the closed set is used to record the areas already evaluated [10]. The heuristics which is used in A* algorithm are

$$F(n) = g(n) + h(n)$$

where $g(n)$ represents the cost of the path and $h(n)$ represents the heuristic value that is estimated cost form vertex n to goal.

a. Two sets are OPEN and CLOSED. The OPEN node contains the candidate nodes for examination. There is only one element in the OPEN list which is the starting position.
b. The CLOSED set contains the nodes that were already examined and will be empty initially closed.
c. There is a loop that repeatedly pulls out and examines the best node n in the OPEN list; if n is the goal node, then we are done. Otherwise, n for the OPEN list will be removed and moved to the CLOSED list.
d. A neighbor who is CLOSED has been seen before, so we do not need to look at it, so if his f value becomes the lowest in OPEN, a neighbor who is in OPEN will be examined. Otherwise, we will add it to OPEN, the parent being set to n. The cost of the path is n', $g(n)$ is $g(n)$ + momentcost (n, n').

4 Comparison of Various Search Techniques

Table 1 gives the idea of how the various search techniques are performing under different parameters for gaming applications.

5 Conclusion

By comparing the different search techniques for gaming applications to identify the shortest path, A* algorithm is better than the DFS and BFS. A* algorithm is well suited for gaming applications in a dynamic environment with obstacles to play. In future planning to propose a new algorithm for the shortest path from the initial state to a final state of gaming applications.

Table 1 Comparison of various search techniques

Parameters	Breadth-first search	Depth-first search	A* algorithm
Memory	High	Low	Low
Structure of constructed tree	Wide and short	Narrow and long	Straight line
Optimality	Optimal, not in cost	Not optimal	Optimal
Data structures to store nodes	Queue	Stack	Graph
Performance	Low	High	High
Space complexity	More critical	Less critical	Less critical
Time complexity	Less	High	Less
Basic	Vertex-based algorithm	Edge-based algorithm	Abstract data type
Traversing fashion	Oldest unvisited vertices are explored at first	Vertices along the edge are explored in the beginning	Predecessor

References

1. Jing MQ, Yu CH, Lee HL, Chen LH (2009) Solving Japanese puzzles with logical rules and depth first search algorithm. Proc Int Conf Mach Learn Cybern 5:2962–2967
2. Khantanapoka K, Chinnasarn K (2009) Pathfinding of 2D & 3D game real-time strategy with depth direction A* algorithm for multi-layer. In: 2009 8th international symposium national language processing SNLP'09, pp 184–188
3. Rahmat RF, Harry Syahputra MF, Sitompul OS, Nababan EB (2018) The depth-first search column by column approach on the game of Babylon Tower. In: Proceedings of the 2nd international conference on informatics and computing, ICIC 2017, pp 1–6
4. Sazaki Y, Satria H, Syahroyni M (2017) Comparison of A∗ and dynamic pathfinding algorithm with dynamic pathfinding algorithm for NPC on car racing game. In: 2017 11th International conference telecommunication systems services and applications, pp 1–6
5. Harsani P, Mulyana I, Zakaria D (2018) Fuzzy logic and A* algorithm implementation on goat foraging games. IORA-ICOR 2017. IOP Conf Ser Mat Sci Eng 332:1–7
6. Xiao C, Hao S (2011) A*-based pathfinding in modern computer games. Int J Comp Sci Netw Secur 11(1):125–130
7. Breadth First Search. https://en.wikipedia.org/wiki/Breadth-first_search
8. Depth First search. https://www.geeksforgeeks.org/depth-first-search-or-dfs-for-a-graph/
9. Introduction to the A* Algorithm. http://mnemstudio.org/path-finding-a-star.htm
10. A* Search Algorithm. https://en.wikipedia.org/wiki/A*_search_algorithm

Crowdsourcing Data Analysis for Crowd Systems

Vignesh Loganathan, Gopinath Subramani and N. Bhaskar

Abstract Crowdsourcing permits huge scale and adaptable summon of human contribution for information social affair and examination, which presents another world view of information mining process. Customary information mining techniques frequently require specialists in investigative areas to comment on the information. In any case, it is costly and ordinarily takes a long time. Crowdsourcing empowers the utilization of heterogeneous foundation information from volunteers and circulates the explanation procedure to little segments of endeavors from various commitments. The data analytics process is done via logistic regression.

Keywords Crowdsourcing · Data analytics

1 Introduction

Crowdsourcing is a type of human calculation, where human calculation is a technique for having individuals do things that we may somehow think about doling out to a processing gadget to compute consequently, e.g., a dialect interpretation errand. A crowdsourcing framework encourages a crowdsourcing procedure to finish an indicated errand. To do an undertaking, a crowdsourcing framework enrolls a "swarm" of human specialists to help take care of a characterized issue. Data analytics is the study of breaking down data to change over data to helpful information. This information could enable us to comprehend our reality better and in numerous settings empower us to settle on better choices. While this is the wide and fabulous

V. Loganathan (✉) · G. Subramani · N. Bhaskar
Department of Information Technology, KCG College of Technology, Chennai, India
e-mail: vigneshloganathan0598@gmail.com

G. Subramani
e-mail: gopinathss.subramani@gmail.com

N. Bhaskar
e-mail: bhaskar@kcgcollege.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_117

target, the most recent 20 years have seen steeply diminishing expenses to accumulate, store, and process data, making a considerably more grounded inspiration for the utilization of experimental ways to deal with critical thinking.

2 Overview

2.1 Automated

With the data analytics necessities and data as the information sources, it can naturally achieve end-to-end data analytics assignments with human exertion. It understands the struggle between the requirement for critical data examination in little and medium assembling undertakings also, existing data investigation stages being time [1].

2.2 Well-Disposed to Non-master Clients

An easy to understand interface is not excessively intricate, however rather is direct, giving brisk access to normal highlights or directions. This approach is highly reliable to non-expert users [1].

2.3 Human Intelligence

A Human Intelligence Task, or HIT, is an inquiry that needs an answer. A HIT speaks to a solitary, independent errand that a worker can chip away at, present an answer, and gather a reward for finishing [2].

2.4 Applications

There are several examples can be given for the process of crowdsourcing and data analytics. Among that, the most important and popular example of crowdsourcing was Amazon Mechanical Turk. Amazon Mechanical Turk (MTurk) is a commercial center for work that requires human insight [2]. The crowdsourcing has been utilized in number of research and business applications. The Wikipedia is a precedent in which set of data is being distributed and later on number of individuals can include and upgraded the data at long last the best of the best-upgraded information is accessible for the client which is impossible by utilizing a solitary PC alone and could be costly to accomplish through expert domain process [3].

3 Related Work

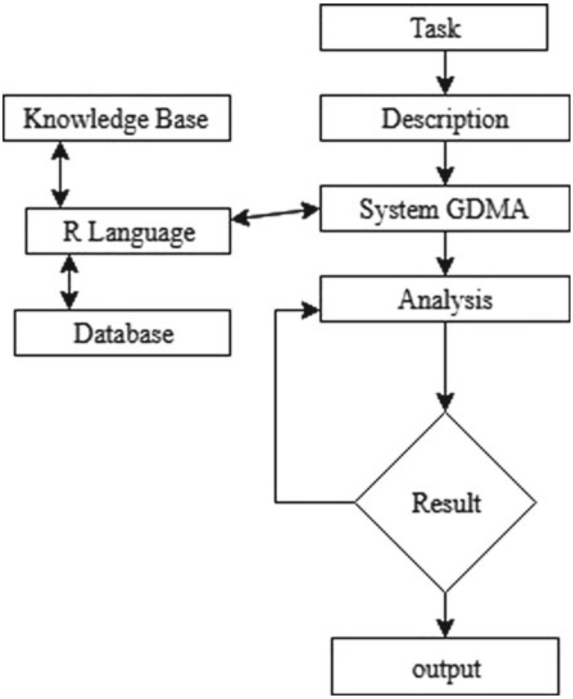
3.1 Data Analysis Framework [1]

Data analysis depends on R language. Every one of the information investigation tasks in Data analysis are converted into R proclamations. Data analysis resembles an interlayer between information investigation prerequisites and information investigation undertakings portrayed by R language [4]. The general system structure of GDMA is appeared in Fig. 1. To be exceptionally mechanized and conventional, GDMA mostly depends on three noteworthy framework parts, an information processor, a calculation selector, and a parameter enhancer.

System workflow

An entire information investigation process starts with a client's order. GDMA gets

Fig. 1 GDMA framework



the errand depiction and information processer naturally chooses the properties type and shows it to the client. The client can modify the traits sort utilizing directions on the off chance that they wish. At that point, calculation selector chooses the most suitable calculation as indicated by the errand type and information attributes point by point. On the off chance that fundamental information processor will process the information to ensure that it is appropriate for the chosen calculation. For instance, multilayer perceptron does not endure missing or discrete qualities and these must be evacuated. Next, if the calculation has parameters to be resolved, parameter streamlining agent will decide the ideal parameter values, as point by point. Following this, GDMA utilizes the chose calculation and decided parameter settings to dissect the handled information and build up an investigation demonstrate. At last, the examination results are acquired and clients can affirm on the off chance that they are happy with it, if not, they can modify the parameters or even change the calculation until the point that they are.

Advantages
In this framework, the major advantage was to analyze the data given for query processing and publish the satisfied result to the user.

Challenges
In this concept, the greatest challenges were to optimize the parameter [5] and selection of algorithm for query processing.

3.2 Data-Less Big Data Analytics [6]

Scalable, efficient, and accurate (SEA) examination is getting to be the holly vessel of information science research in the enormous information time. All research networks associated with enormous information science have perceived and grasped the intrinsic difficulties. Since the turn of the century, new frameworks, encouraging adaptability with enormous capacity, the board and parallel/conveyed preparing have been created. Also, the requirement for additional productivity, notwithstanding adaptability, was getting to be clear and new frameworks for quick investigation developed to fulfill such needs [7, 8].

Imagine an information framework, which can process examination questions without getting to any base information, while giving precise answers! This would be a definitive in versatility (as question preparing times move toward becoming accepted obtuse to information sizes), what is more, a definitive in effectiveness, as tedious, asset hungry co-operations inside appropriated and complex enormous information examination stacks are totally stayed away from. Figure 2 given below will explain the process of data-less big data analysis. The upper half portrays traditional processing, while the base demonstrates the data-less processing worldview. Inquiries are submitted to the framework as previously. Utilizing known and generally acknowledged outstanding burden qualities, (i.e., that questions commonly

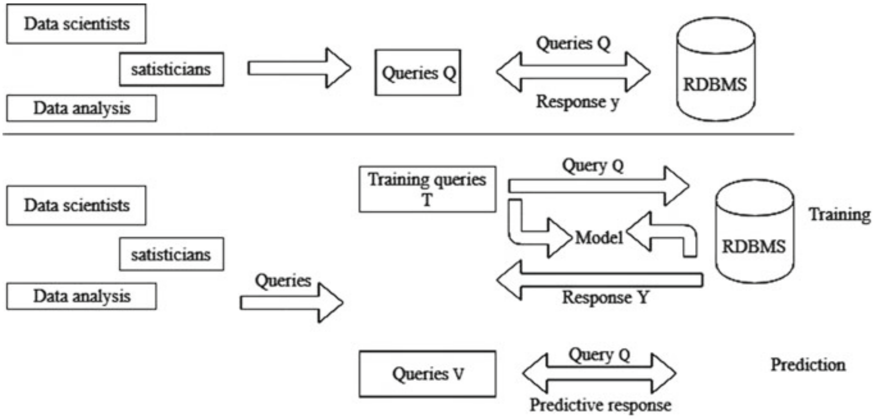


Fig. 2 Data-less analytics processing

characterize overlapping data subspaces), our methodology basically infuses an "intelligence" which screens and gains from the investigator framework collaborations and creates novel ML models which are utilized to precisely foresee answers to future inconspicuous diagnostic questions [6].

The endeavors here spotlight on comprehension and utilizing the conduct of investigators (clients), explicitly, to determine novel calculations, structures, and models, which can gain from what investigators are doing. What are their questions? Which data subspaces would they say they are focusing on? At the point, when do their interests move? Up until now, we have favored a demonstrating of investigative inquiries as vectors in multidimensional vector spaces. Checking what is more, gaining from client conduct at that point adds up to, in pith, inquiry space quantization. This comes connected at the hip with portion works that characterize likeness between said inquiry quanta and new approaching inquiries.

In the meantime, the emphasis is on creating novel models, calculations, and structures that gain from what the framework does in light of explicit examiner questions. What are the appropriate responses to examiner inquiries? How were they registered? Utilizing which data subspaces? The end objective here is to learn and display the attributes of questioned data subspaces. For instance, what are the circulations of measurements on enthusiasm for the data things inside questioned subspaces.

Advantages
Analytical query preparing then continues by utilizing a fitting closeness separate capacity for deciding the nearest query quanta(s) to the query point. [9, 10, 11].

Disadvantages

1. Maintain said models within the sight of query space updates and information space refreshes.
2. Infer the most suitable models for the question and data spaces.

3.3 Crowdsourcing Predictors [2]

The fundamental idea of this framework is to make accessible a spot where farmers can make inquiries and answer the inquiries asked by their friends. Figure 3 demonstrates the stream of the framework. The new client needs to enlist her/him to the framework. After an effective login, the existing client will choose the classification of organic products, blooms, vegetables. As indicated by the class, she/he will post an inquiry and can give a response to an unanswered inquiry. The arrangement of posting the pictures of surrendered and harmed items is given. The job of domain expert is predominant. On the off chance that client is not happy with the appropriate responses given by different clients, at that point, she/he can tap on not fulfilled. After that, the inquiry will send to the domain expert. Domain expert will give the response to that question and that answer will be given back to the clients. A client

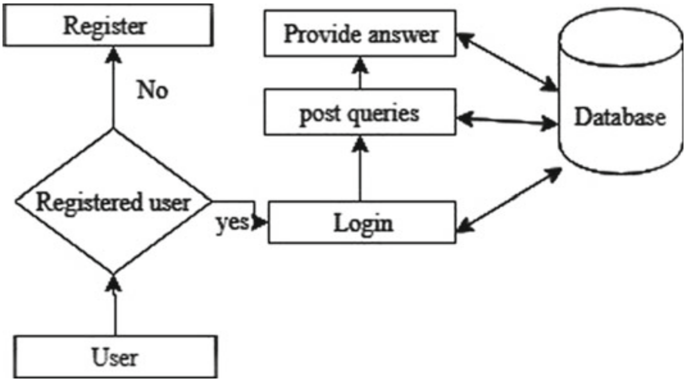


Fig. 3 System flow diagram

can give a rating to the appropriate response of different clients. The beneath Fig. 3, clarifies the stream of the framework and will clarify the working of framework.

Advantages
The facility of giving pictures as opposed to utilizing words to clarify makes the framework not quite the same as others. The framework is totally free of expense and only a piece of administration to serve the country [2].

Disadvantages
System does not show the predicted result since this has no analysis of data and shows all results regarding the queries [2].

4 Proposed System

The proposed system comprises the process of crowdsourcing and data analytics. Our approach overcomes the limitations that are occurred in the previous system. Crowdsourcing system is designed in a way to help the farmers to gather the suggestions in the new/alternate techniques of the agriculture. The system helps to share information between the farmers. The farmer can able to post queries as a requester and farmer can able to share their suggestions as a worker. The suggestions are getting shared throughout the system. This suggestion is getting monitored by the expert in the system. The expert has the authority to remove the unwanted suggestions given by the workers/requestors. The analysis of queries is done using the Logistic regression algorithm for categorical data.

Logistic Regression
The idea of Logistic Regression is to find a relationship between features and probability of particular outcome. E.g.… This type of a problem is referred to as Binomial Logistic Regression, where the response variable has two values 0 and 1 or pass and fail or true and false.

Prediction from categorical data using Logistic Regression Algorithm (sample) (Table 1):

Table 1 Analysis of the process

	GDMA framework	Data-less analytics	Expert system	Proposed system
Data analysis	✓	✓	✘	✓
User friendly	✘	✘	✓	✓
Analysis of data (by Logistic Regression)	✓	✓	✘	✓

```
#Farm dataset and test

> farm < - alldata[!(is.na(Survey))]
> farm [,Survey : = as.factor(Survey)]
> test < - alldata[is.na(Survey)]
> test [,Survey : = NULL]
#Logistic Regression
> model < - glm(Survey ~ ., family = binomial(link = ‘logit’),
data = farm[,-c(“FarmerId”,“Name”,“Location”)])
> summary(model)
```

5 Conclusion

Crowdsourcing approach audits ongoing work on crowdsourcing-based data mining strategies. Crowdsourcing can do data mining and concentrate expansion data from the datasets more effectively and keenly than conventional techniques. It needs to manage bunches of difficulties like the low nature of answers from the groups to apply crowdsourcing to data mining. In our approach, we bring up research process to overcome these challenges and present the general systems of an incorporated data mining undertaking in crowdsourcing.

References

1. Zhang H, Wang H, Li J, Gao H (2018) A generic data analytics system for manufacturing production. Big Data Min Anal 1(2): 160–171. ISSN: 2096-0654 06/06
2. Pawar CV, Patni SS, Wale SK, Chemate HB, Dasgupta A (2015) India exploring agriculture sector using Crowdsourcing predictors (IJRASET). Department of Information Technology, Amrutvahini College of Engineering, Sangamner, Maharashtra, Apr 2015
3. USAID (2013) From the American people, briefing paper Crowdsourcing application for agricultural development in Africa, pp 1–6
4. Racine JS (2012) RStudio: a platform-independent IDE for R and sweave. J Appl Econom 27(1):167–172
5. Keser SB, Yayan U (2016) A case study of optimal decision tree construction for RFKON database. In: Proceedings of 2016 international symposium innovations in intelligent systems and applications (INISTA), Sinaia, Romania, pp 1–6
6. Peter Triantafillou Department of Computer Science (2018) UK data-less big data analytics (towards intelligent data analytics systems). In: 2018 IEEE 34th international conference on data engineering. University of Warwick
7. Melnik S, Gubarev A, Long JJ, Romer G, Shivakumar S, Tolton M, Vassilakis T (2011) Dremel: interactive analysis of web-scale datasets. Commun ACM
8. Engle C, Lupher A, Xin R, Zaharia M et al (2012) Shark: fast data analysis using coarse-grained distributed memory. In: Proceeding of ACM SIGMOD

9. Anagnostopoulos C, Triantafillou P (2015) Learning set cardinality in distance nearest neighbours. In: Proceeding of IEEE international conference on data mining (ICDM15)
10. Anagnostopoulos C, Triantafillou P (2015) Learning to accurately count with query-driven predictive analytics In: Proceeding of IEEE international conference on big data
11. Anagnostopoulos C, Triantafillou P (2015) Efficient scalable accurate regression queries in in-dbms analytics. In: Proceeding of IEEE international conference on data engineering (ICDE17)

Optimized Database Using Crowdsourcing

Vignesh Balakrishnan and N. Bhaskar

Abstract RDBMS is the most normal and antiquated way to deal with database arrangements. The data is kept in an extremely organized methodology in style of tables or relations. With appearance of Big Data in any case, the organized methodology misses the mark to serve the needs of monstrous data frameworks that are basically unstructured in nature. Expanding ability of SQL, however, allows huge amount of data to be overseen, and it does not generally make a difference as a response to Big Data frameworks that anticipates brisk reaction and quick speedy adaptability. To comprehend this disadvantage, a sensibly new database framework suggested to as NoSQL was presented. NoSQL framework is acquainted which give the fast adaptability and unstructured stage for Big Data application.

Keywords Crowdsourcing · MySQL · NoSQL · SSIS

1 Introduction

As the technology is being evolved, human too evolved with the technology. They always want things to be done in a most efficient and simple manner. The main objective of this approach is to showcase the throughput time variation between MySQL and NoSQL databases in form of retrieving same data from both databases. In the existing system, uploading large amount of data is slow and time consuming. In proposed system, uploading large amount of data is fast and time reducing. The proposed system is to show an optimized database by the performance comparison using throughput time variation between the MySQL and NoSQL databases using crowd sourcing application. Deduplication, which can save storage cost by enabling us to store only one copy of identical data, becomes unprecedentedly significant with the dramatic increase in data stored in the databases.

V. Balakrishnan (✉) · N. Bhaskar
Department of Information Technology, KCG College of Technology, Chennai, India
e-mail: bvignesh253@gmail.com

N. Bhaskar
e-mail: bhaskar@kcgcollege.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_118

2 Overview

2.1 SQL Server Integration Services

Performance task of uploading large amount of data in database is increased. If error occurred in the insertion of data or the column left null, SSIS indicates about these things to the user to rectify it. It is a programmable object model that allows the developer to write their own piece of code. Deduplication operation is adopted for eliminating duplicate copies of redundant data [1].

2.2 Service-Level Agreement

A service-level agreement is a formal contract concerning a given service between two parties: the admin and the user. The SLA explicitly defines the concerned service using measurable metrics such as the service availability and performance. If the user violates the agreement, the SLA indicates to the admin regarding the violation. And also used to guarantee the satisfaction of the service quality expected by the customer. An administration-level ascension (SLA) is an agreement between a specialist co-op and its inward or outside clients that archives what benefits the supplier will outfit and characterizes the administration models the supplier is committed to meet [2].

3 Related Work

Recent crowdsourcing systems, such as CrowdDB and Qurk and Deco, provide an SQL-like query language as a declarative interface to the crowd. The query that works as indicated by our necessity is not constantly valuable for us, for example, on the off chance that information is refreshing on non-endurable time. We have to advance question for better execution. Each inquiry gives same outcome yet the question with best time normal is the thing that we need and use expertly. The database query optimizer to choose efficient implementations using indices to evaluate predicates or selecting join algorithms. The user has to submit an SQL query and the system takes the responsible for compiling the query, generating the execution plan.

Advantages

In paper [3], develops an efficient algorithm for optimizing selection queries, join queries, and complex selection-join queries and the second stage validates our approach.

Challenges

In crowdsourcing concept, there is a slight difficulty in dealing with a large amount of data processing. Lack of a quantitative decision support process to identify better concepts [3].

4 Proposed System

Crowdsourcing allows large-scale and flexible invocation of human input for data gathering and analysis. With the help of this, admin gathers information from the employee and manager and produces an output to the user as per their request. Admin designed those menus with some restrictions involved in it. The menus are provided as an instant template when they login their page within a second. And then, the optimized tables are stored as a report in a dynamic query table. Using key deduplication, duplicate data are avoided while storing in the databases.

The crowdsourcing Web application has been designed in a way for the user to show the performance comparison between the two different databases. So, to check the comparison, the graphical image is designed to see the variation throughput time from the given input. User can check the comparison efficiency between MySQL and NoSQL databases. As we are introducing service-level agreement algorithm in this crowdsourcing application, privacy is also maintained between each user and the admin. SSIS method, is a platform to creates efficient data integration solutions.

Thus, the following table will show the different process of execution in different databases (Table 1).

Efficiency: The capacity, calculation and correspondence overheads related with the enormous information deduplication ought to be as little as could be allowed, and the expense of seeking for copied information ought to likewise be limited [5].

Confidentiality of data: Security analysis demonstrates that key duplication ensures data confidentiality and convergent key security, and well protects the ownership privacy simultaneously [2].

Result: The final result will be performance variation between two different databases is shown in Fig. 1.

5 Conclusion

Hence, by our approach, performance variation between two different databases are shown in the form of graph. It helps the user to choose right database regarding the

Table 1 Basic queries in two different databases [4]

Query	MySQL database	NoSQL database
Create query	CREATE TABLE table_name (column_name1 datatype, column_name2 datatype)	No need for defining schema
Insert query	INSERT INTO table_name (column_name1, column_name2) VALUES(value1,value2)	db.collection_name. insert ({name1: value1,name2: value2})
Delete query	DELETE FROM table_name WHERE (condition)	db.collection_name.remove ({condition})
Import query	BULK INSERT table_name FROM file_name WITH {FIELDTERMINATO R =',', ROWTERMINATOR ='\n'} GO	mongoimport–db database_name -collection collection_name–type csv–file "file_name"
Select query	SELECT column_name FROM table_name	db.collection_name({}, {condition})

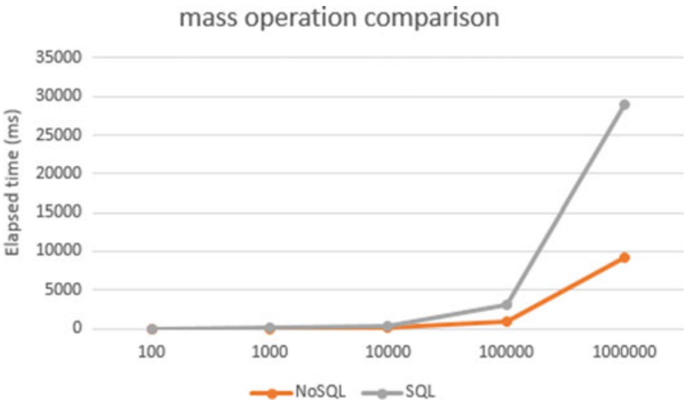


Fig. 1 Performance comparison graph between MySQL and NoSQL

process. The future research should include many databases with proposed system and brings out the throughput time variation among those databases.

References

1. Chauhan D Using the advantages of NOSQL: a case study on MongoDB. Department of Computer Science, Himachal Pradesh University, Summerhill, Shimla, India
2. ETL Function Realization of Data Warehouse System Based on SSIS Platform Tong Wu College of Computer Science and Information Technology, Guizhou University Guiyang, China 550025. wtxx@citiz.net

3. Forbes HL, Schaefer D (2018) Crowdsourcing in product development: current state and future research directions. In: International design conference, design 2018
4. Chandra AK, Merlin PM (1977) Optimal implementation of conjunctive queries in relational data bases. In: Published in the proceedings of ninth annual ACM symposium theory of computing (STOC)
5. Liu L, Zhang Y, Li X (2018) KeyD: secure key-deduplication with identity-based broadcast encryption. IEEE Trans Parallel Distrib Syst 26(5):1206–1216

Anti-Counterfeit on Medicine Detection Using Blockchain Technology

R. Anand, Khadheeja Niyas, Sorjeeta Gupta and S. Revathy

Abstract The goal of this project is to find whether a given medicine is fake or original using blockchain technology. Blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but also has the potential to disrupt other markets. It removes the need for trusted intermediaries, can facilitate faster transactions and add more transparency. A medical product is counterfeit when there is false representation in relation to its identity or source. In the case of medicines, the implications are more severe. This technology stops the entry of fake drugs into the supply chain, mainly the part between the manufacturer and consumer. The technology uses digital signature where each block gets a unique crypto id. This digital signature is provided for each block and it gives a strong control of ownership.

Keywords Blockchain · Supply chain · Healthcare

1 Introduction

Nowadays, for any transaction to take place between two parties, there is always a trusted intermediary in between. But using blockchain, there is no need of a middle party between the consumer and supplier. Blockchain technology is a new and rapidly growing technology. This technology was first introduced in 1991 and they considered assigning a time period to digital documents and so, it is not possible

R. Anand (✉) · K. Niyas · S. Gupta · S. Revathy
Department of Information Technology, KCG College of Technology, Chennai, India
e-mail: nowhereanand@yahoo.com

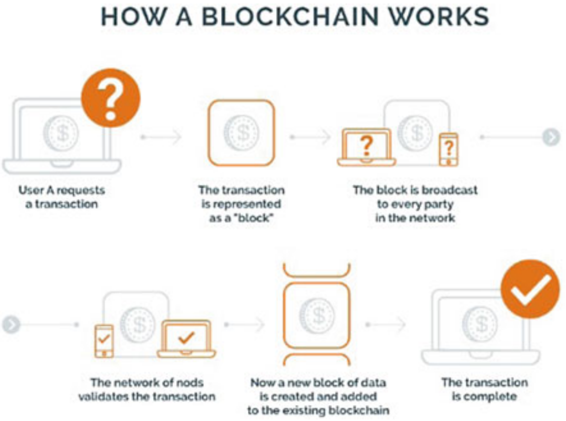
K. Niyas
e-mail: khadheejaniyaz123@gmail.com

S. Gupta
e-mail: get2sorjeeta@gmail.com

S. Revathy
e-mail: rey.revathy16@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_119

to make any changes just like an agreement. Using this technology, we can handle the data, manage the exchange or transaction between any two parties, and store the details about any new product. Implementation of this technology in many industries leads to its massive success. Blockchain is a distributed network and it is a write-once-read-only record of details. The data are stored in peer-to-peer network where information about any product can be viewed by anyone that is in the network. The chain stores information about any transaction or exchanges that occur in the network. It is similar to all other network but what makes blockchain technology different is that no data can be deleted or altered by anyone in the network. No changes can be made in the network until it is validated by all the authorized users of the network.

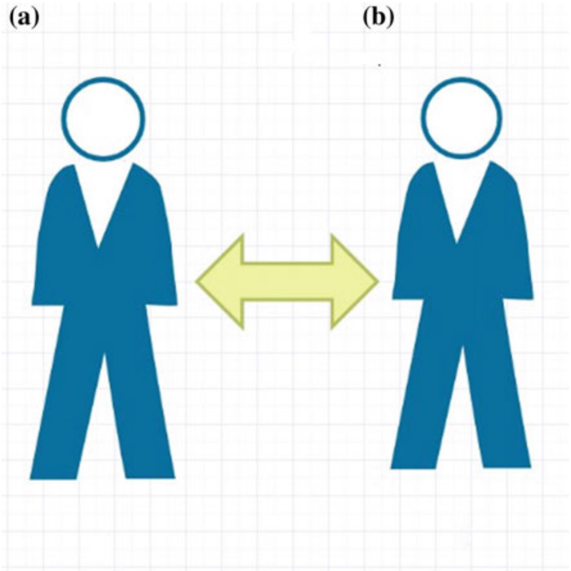

HOW A BLOCKCHAIN WORKS
User A requests a transaction
The transaction is represented as a "block"
The block is broadcast to every party in the network
The network of nods validates the transaction
Now a new block of data is created and added to the existing blockchain
The transaction is complete

Blockchain is a chain of blocks and each block contains information. A block is a set of data and is identified with a cryptographic hash and timestamp. Each block contains the newly entered data, unique hash value, and the previous hash value. When a new block is added, it contains the previous hash values so that there will be an order from the first block that was first ever generated in the chain. This first block is called genesis block. The same process is repeated again and again to grow and maintain the block. The blocks of data are stored in a linear chain fashion. It is a continuously growing list of digital records which are linked and secured using cryptography.

A block is just a collection of information that is needed by the organization for the purpose of keeping track of the processes or to identify the addition or removal of products from the chain (Fig. 1).

Two people wish to interact with each other for transaction purpose or for exchange of data. Suppose A wants to send money to B in a network, the transaction takes places through the blocks that are interconnected in the chain. This transaction takes a block and that block is broadcasted to every other party in the network. Those in the network check whether the block is valid or not. If it is valid, then they approve for the transaction to occur. The block can then be added to the chain to be used for future references. The money moves from A to B.

Fig. 1 Block working process



In blockchain technology, there are two keys: private key and public key. The main purpose of these keys is to create a secure unique identity. Identity is based on the private and the public cryptographic keys. The combination of a private and a public key generates a highly secure digital signature. This digital signature is provided for each block, and it gives a strong control of ownership.

In the future, many industries will use blockchain technology. Some industries already using blockchain technology are:

Banking and payments

Banks access financial services and it connects billion of people from different countries in the world, like bitcoins allow anyone to transfer money, banks also increasingly allow anyone to do the payments. Banks are now investing in blockchain; the BARCLAYS is the bank which is already using the technology.

- Cyber security

Allowing the blockchain ledger public, the data is encrypted using cryptography and this may lead the data to be less hacked and it cannot be changed. It also eliminates the need of a middleman system and makes it more efficient, this allow only the authorized user to access the data.

- Supply chain management

With blockchain technology transaction, the supply chain can be documented in a permanent decentralized record, and it also monitored securely and transparently. This helps to reduce the time delay, loss of data, and human mistakes. It also verifies the authenticity of a product by tracking them from the origin, and it also understands the environmental impact of the products.

- Healthcare

One of the challenges healthcare faces is the lack of a secure platform to store and share data and they are often victims of hacking because of outdated infrastructure. This technology allows hospitals to safely store data like medical records and share it with authorized professionals or patients. Gem and Tierion are the two companies that are working on disrupting the current healthcare data space.

- Insurance

The global insurance market is based on trust management. Blockchain is a new way of managing trust, and it is used to verify many types of data in insurance contract, like the insured person's identity.

2 Proposed System

This project helps to track the manufacturing process of the medicines, right from the raw materials to the retailers and consumers, using blockchain technology. This ensures that there is no tampering in important information about the medicines. The proposed system uses blockchain technology because by this technology, the network can be open to everyone. All users of the network are aware of the transactions that take place. If a new user has to enter the network, then it has to validate with all the other users in the network. The network is open to everyone; it is a peer-to-peer network. Using a simple web application, every end user can easily find out the correct details of the medicine and find out whether the medicine is original or not.

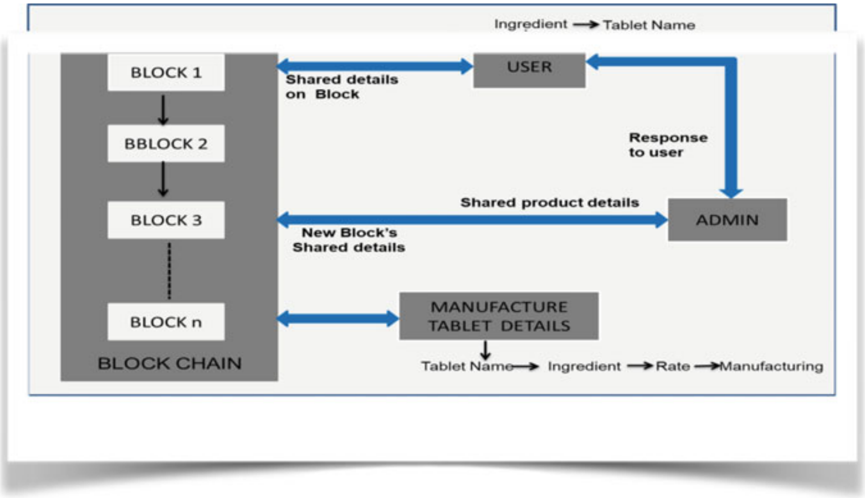
3 Problem Formulation

The use of counterfeit medicine can be harmful to health. Their use may result in treatment failure or death. They also undermine confidence in health service. Solving the counterfeit drugs problem is important to ensure that the patients do not lose faith in the benefits of pharmaceuticals and become non-adherent with their treatments. Controlling the availability of counterfeit drugs is not easy, but it is necessary, given the tremendous public health issues concerning counterfeit drugs, which can harm or kill people.

4 Existing System

Detecting a substandard drug is not an easy task. Some are entirely fake while some are potentially dead (does not produce a desired result or ineffective). Consumption of fake medicine can lead to consequences ranging from delayed treatment to dangerous side effects. Consumers do not have testing equipment at home, but there are ways by which counterfeit medicines can be identified and avoided such as checking the packaging, checking the tablets/dosage form, physical attributes of tablets, verifying medicines by online or SMS but by this way, information is not open to everyone, only the user is aware of the transactions that take place and is not secure; so, we are making use of blockchain technology which is the network that is open to everyone and is secure.

5 Architectural Design



Counterfeit medicines are difficult to track and test. To detect the counterfeit drugs before they reach the customers through the global supply chain, there must be enough systems that can detect counterfeit medicines. To find out whether the medicine is counterfeit or not, we need regulators to properly check its pharmaceutical ingredients. Regulators also analyze the packaging, the medicines serial number, and also the inserts in order to determine the originality. Therefore, the process of finding out the counterfeit medicines is a time-consuming and difficult task. Counterfeit medicine results in major financial issue. In the case of medicines, the implications are more severe because the products might not contain the right active ingredients and therefore be useless to harmful. Using blockchain technology, we can reduce the possibilities of counterfeit. This technology stops the entry of fake drugs into the supply chain, mainly the part between the manufacturer and consumer.

The diagram illustrates the algorithm used by the counterfeit drug detection network. When the manufacturing company manufactures a new medicine, they assign a unique serial number to each new medicine. For that, a unique protocol asset called hash is used. Then these medicines are added into the supply chain. Each medicine is added as blocks to the chain. The samples are split into subset. To find out whether the medicine is original or fake, we have to carry out package inspection where the medicines ingredients are checked. From the added ingredients first, we identify each ingredient. Then we check the amount of each ingredient added. From those added ingredients, we see if there are any toxic substances such as chalk or flour, or even toxic, made from rat poison or antifreeze. Or sometimes, a counterfeit medicine does not contain the expected dose of whatever active ingredient they are supposed to deliver, or they are expired. If any of these situations are found, then that medicine is said to a fake one. If it is proved to be not fake, then the medicines are distributed to the wholesale distributor and then to the users. Solving the counterfeit medicine problem using blockchain technology is important to ensure that patients do not lose faith in the benefits of pharmaceuticals and become non-adherent with their treatments. The expansion of the internet has made the controlling of counterfeit medicines very difficult.

6 Algorithm

- User enters the medicine details in the system.
- Admin responses to the user and sends the details or request to the network and ensures authentication.
- In the blockchain, the details of particular medicine are entered from the manufacturer while creating blocks.
- Only one block which has the same ingredient will response at a time.
- Each time the user's crypto will generate for each transaction that is private key.
- The detail shared by the user is compared with the datasets already present.
- Admin will verify the details.
- Sends the notification to the user whether the medicine is fake or not.

7 Implementation

7.1 Tablets

7.1.1 Tablet Name: Paracetamol

Ingredient: The ingredients are maize, starch, potassium sorbate, purified talc, povidone, and soluble starch.

Manufactures.

7.1.2 Tablet Name: Vic Vicks

Ingredient:

Each uncoated tablet contains ingredients:
Paracetamol I.P. 500 mg,
Diphenhydramine HCl I.P. 25 mg,
Phenylephrine HCl I.P. 5 mg,
Caffeine (anhydrous) I.P. 30 mg.
Excipients q.s. Color: Lake Brilliant Blue FCF.

Dosage:

One tablet every 4–6 h does not exceed more than four doses in 24 h.

Caution:

Do not use with other Paracetamol products. Taking more daily dose of Paracetamol may cause serious liver damage or allergic reactions (e.g., swelling of face, mouth, difficulty in breathing, itching, or rash). In the case of overdose, consult a doctor eventually even if no symptoms appear.

Manufactures:

Product Description:

Vicks Vapo Rub medicated vapor begin to work fast to relieve our cough. Use on chest and throat temporarily relieves cough. Also, great use as a topical analgesic to relief minor aches and pains in our muscles and joints.

Manufacturer:

Soothing vapor prevents cough. Vapo Rub is applied on the chest or throat so it does not interact with other medication the way pills are and does not to cause drowsiness or side effects. Vapo Rub may be used for oral decongestant for people who suffer from tension and may be suited for diabetics who are looking for a sugar-free cough suppressant. Vicks Vapo Rub can also be rubbed on sore muscles to relieve aches and pains.

7.2 Blockchain Client

Blockchain:

A system in which a record of transactions made in bitcoin maintained across several computers that are linked in a peer-to-peer network.

The blockchain network has no central authority. It is an independent system. It is a shared and immutable ledger so information inside it is open for everyone to see. Hence, anything that is built on the blockchain is visible to everyone involved and is accountable for their actions.

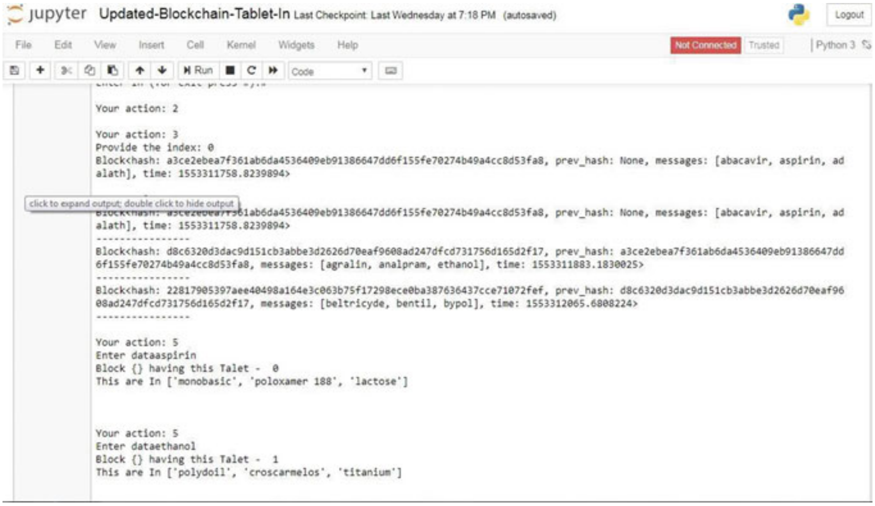
- Multiple nodes can be added to the blockchain.
- Proof of work (PoW).
- Simple conflict resolution between nodes.
- Transactions with RSA encryption.
- Blockchain client can be the user as well as manufactures.
- According to network, the user also receives the request and response as well as manufactures.
- Both of them share their requirement in the network if they having the public key of them means they can able to access the transaction and can respond to the user.
- It can be managed by the admin side.

7.3 Blockchain Admin

- History immutability.
- Un-hackability of the system.
- Data persistence.
- No single point of failure.

– Transactions can be managed using the admin or block miner.
– The admin will manage the transaction between the manufactures as well as users.
– User would not know the manufactures public key as well as manufacture also do not know the users public key.
– The transaction can be done by the admin so that It will be secure one.
– Every "post" can also be called a "transaction" (it is all simply data at the end of the day).
– The transactions are packed into blocks.
– A block can contain one or more transactions.
– The blocks containing the transactions are generated frequently and added into the blockchain.
– Each block should have a unique id (because every block should be uniquely identifiable).

8 Implementation


jupyter
Updated-Blockchain-Tablet-In Last Checkpoint: Last Wednesday at 7:18 PM (autosaved)
Logout
File
Edit
View
Insert
Cell
Kernel
Widgets
Help
Not Connected
Trusted
Python 3
Run
Code
click to expand output; double click to hide output

```
Your action: 2

Your action: 3
Provide the index: 0
Block<hash: a3ce2ebea7f361ab6da4536409eb91386647dd6f155fe70274b49a4cc8d53fa8, prev_hash: None, messages: [abacavir, aspirin, ad
alath], time: 1553311758.8239894>

Block<hash: a3ce2ebea7f361ab6da4536409eb91386647dd6f155fe70274b49a4cc8d53fa8, prev_hash: None, messages: [abacavir, aspirin, ad
alath], time: 1553311758.8239894>
----------------
Block<hash: d8c6320d3dac9d151cb3abbe3d2626d70eaf9608ad247dfcd731756d165d2f17, prev_hash: a3ce2ebea7f361ab6da4536409eb91386647dd
6f155fe70274b49a4cc8d53fa8, messages: [agralin, analpram, ethanol], time: 1553311883.1830025>
----------------
Block<hash: 22817905397aee40498a164e3c063b75f17298ece0ba387636437cce71072fef, prev_hash: d8c6320d3dac9d151cb3abbe3d2626d70eaf96
08ad247dfcd731756d165d2f17, messages: [beltricyde, bentil, bypol], time: 1553312065.6808224>
----------------

Your action: 5
Enter dataaspirin
Block {} having this Talet -  0
This are In ['monobasic', 'poloxamer 188', 'lactose']


Your action: 5
Enter dataethanol
Block {} having this Talet -  1
This are In ['polydoil', 'croscarmelos', 'titanium']
```

9 Conclusion

In blockchain-based applications and experiments, faith on the longevity of blockchain technology is increasing. Scalability and consensus algorithms are areas of growing research in order to make blockchain more adaptable for businesses of larger scale. Areas like taxation, education, and insurance are yet to see a major overhaul via blockchain adoption and these can be the focus areas of future research in blockchain. Acceptance of cryptocurrency by governments and establishment of regulations governing them are very important to ensure ethical use of cryptocurrency. The public blockchains also provide an opportunity of mining interesting patterns of cryptocurrency usage, user behavior, and monetary networks across the globe.

Bibliography

1. Barbora Hornáčková BC (2018) Using Blockchain smart contracts in the DEMO Methodology. Czech Technical University in Prague Faculty of Information Technology, Jan 2018
2. Nakasumi M (2017) Information sharing for supply chain management based on block chain technology. In: 2017 IEEE 19th conference on business informatics (CBI), Thessaloniki, pp 140–149

3. Cui G, Shi K, Qin Y, Liu L, Qi B, Li B (2017) Application of block chain in multi-level demand response reliable mechanism. In: 2017 3rd international conference on information management (ICIM), Chengdu, pp 337–341
4. Xu Y, Wu M, Lv Y, Zhai S (2017) Research on application of block chain in distributed energy transaction. In: 2017 IEEE 3rd information technology and mechatronics engineering conference (ITOEC), Chongqing, pp 957–960
5. Judmayer A, Stifter N, Krombholz K, Weippl E, Bertino E, Sandhu R (2017) Blocks and chains: introduction to bitcoin, cryptocurrencies, and their consensus mechanisms. Morgan & Claypool
6. Ewen H, Mönch L, Ehm H, Ponsignon T, Fowler JW, Forstner L (2017) A Testbed for simulating Semiconductor Supply Chains. IEEE Trans Semicond Manufact 30(3):293–305
7. Ro YK, Liker JK, Fixson SK (2007) Modularity as a strategy for supply chain coordination: the case of U.S. Auto. IEEE Trans Eng Manage 54(1):172–189

Fault Detection in an Indoor Wireless Sensor Network Using RSSI-Based Machine Learning Technique

R. Pradheepa, M. Bhuvaneshwar, S. Ajay Kumar, B. Ajay Raj and K. S. Anusha

Abstract WSN plays a significant role in various fields like in communication, military, etc., and as it is being applied in various fields, the faults in it have to be taken seriously. There were different approaches taken to detect these faults. But, there were very less number of approaches of detection of faults through RSSI. There can be many reasons for change in the measured value of a node. But, change in RSSI can only be limited to distance, disturbance or due to the health of the node. Due to this reason, we are motivated that detection of fault in WSN using RSSI can be reliable than other methods in suitable scenarios. Also, a suitable machine learning technique has been implemented to reduce human involvement in the detection process.

Keywords Wireless sensor networks (WSN) · RSSI · Neural networks

1 Introduction

Wireless sensor network (WSN) is defined as the network of self-governing sensors, which are dispersed spatially across a region that is to be monitored, and that records physical or environmental conditions and communicates the gathered information through wireless links with each other are called wireless sensor networks. Wireless

R. Pradheepa · M. Bhuvaneshwar (✉) · S. Ajay Kumar · B. Ajay Raj · K. S. Anusha
Department of Electronics and Communication Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India
e-mail: bhuvander@gmail.com

R. Pradheepa
e-mail: pradheeparamasundaram@gmail.com

S. Ajay Kumar
e-mail: ajayk0077@gmail.com

B. Ajay Raj
e-mail: ajayraj98b@gmail.com

K. S. Anusha
e-mail: ks_anusha@cb.amrita.edu

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_120

sensor networks (WSNs) have its application on various fields such as healthcare (less invasive patient monitoring), environmental monitoring such as continuous monitoring of air, water, soil, structural monitoring for buildings and bridges, animal farm conditioning, forest fire detection, air pollution or radiation level detectors, traffic congestion control, adaptive street light control and various military and wildlife monitoring.

Since WSNs are mostly applied in hostile and harsh conditions, they are susceptible to node failures and damage which can impact the efficiency of monitoring. Some of the faults can be offset faults, battery faults, hardware faults, etc. [1].

RSSI is chosen as our fault detection parameter as it is directly related to the battery level of the nodes.

Objective of paper:

- To detect faults in a wireless sensor network
- To apply machine learning technique to detect the faults

Reminder of the paper will be presented as follows: Sect. 2 will be related works where summary of various papers is discussed. In Sect. 3, problem statement and project methodology have been discussed where the algorithm has been explained briefly. In Sect. 4, the final results have been discussed.

2 Related Works

In this paper [1], various kinds of faults and its error reduction techniques have been discussed. Author is trying to emphasize the importance of error reduction because increase in demand of WSN has made the system very accurate that even error in small quantity is considered to be intolerable. Errors were classified on the basis of its locality as data-centric and system-centric. The fault reduction has three main approaches as follows: centralized approach, distributed approach and hybrid approach.

In previous works on finding faults in WSN was done using a machine learning tool called SVM [2]. Support vector machine (SVM) is considered to be the most powerful machine learning tools used in many of practical applications. SVM method is used to detect the sensor received data and to identify the faults. Kernel function has excellent adaptation threshold for nonlinear classification in case of fault detection. Initially, faults in WSN were discussed, and as fault detection kernel function was used. SVM is a statistical approach where a nonlinear model was introduced in order to reduce the faults. Here, humidity is taken as the parameter for detecting faults in WSN.

RSSI is another type of parameter which can be used for detecting faults in WSN. Through RSSI, battery faults can be detected as RSSI, and the module's battery level is interrelated [3]. This paper is based on the performance, design and implementation parameters in autonomous energy monitoring and cultivating irrigation system through Internet. This prototype, due to its least cost and user-efficient interface through Internet application, could be deployed by the farmers into practice very easily and effectively, and this is an introductory-level application without investing in new technologies. This system is developed using tools like programming languages, software and hardware due to which a cost efficient and user-friendly practices could be made possible. This prototype by exploring through wireless sensor network may give different benefits in terms of crop yield. This checking subsystem empowers precise observation of each and every condition within the development, and this web application would provide us a convenient model for crop protection and thus by helping the farmers to face adverse situation.

Machine learning can be used to reduce human involvement in the fault detection process [4]. The overall idea behind most of the machine learning techniques is that a computer learns from training datasets to perform a task. Machine learning has two methodologies that are supervised machine learning and unsupervised machine learning. In supervised machine learning, the training dataset consists of desired output of the task along with that data. Supervised machine learning includes a set of classification algorithms/methods, which takes input in the form of dataset and the classifications of each data set so that the computer can efficiently learn how to identify and classify new data. In unsupervised machine learning, the training dataset contains data but with no solutions, so the system creates a solution of its own. Unsupervised machine learning includes clustering algorithm, which takes input as a dataset that covers various part and converts it into clusters in order to process the task in a effectively manner.

A statistical way of approach towards the detection of faults in wireless sensor networks [5].

The proposed method in this paper learns the possible outcome effectively without any training data set. So, this method can be used in the identification and classification of data and system faults by considering the structural relationship between two kinds of hidden Markov model (HMM). The main focus at present lies on the effective calibration on data and system faults.

HMM is a statistical model in which the system being modelled is assumed to be Markov processed with unknown parameter, and determining the hidden parameters from the overall observable parameters. In an HMM, the hidden state is not directly identified, but the state variables used in the detection are directly observable. Each state has a probability distribution function over all the possible output observation.

3 Problem Statement and Methodology

WSN plays a significant role in various fields like in communication, military, etc., and as it is being applied in various fields, the faults in it have to be taken seriously.

There were different approaches taken to detect these faults. But, there were very less number of approaches of detection of faults through RSSI. There can be many reasons for change in the measured value of a node. But, change in RSSI can only be limited to distance, disturbance or due to the health of the node. RSSI values are directly related to battery level of the node which makes detection of battery fault in WSN simple.

As mentioned above, the process of detecting faulty nodes is found monitoring the RSSI values of each node. Since there is a direct relationship between RSSI and distance, we have designed a model with the help of this relationship. The topology considered here is a mesh network as all the nodes are interconnected to each other which helps us to detect the faulty nodes effectively.

The coordinates of each node are obtained from the data of Intel Berkeley WSN [1]. It contains data for about 54 sensors that were deployed in Intel Berkeley Research Lab. It contains the *X* and *Y* coordinates of 54 sensors places in an experimental setup in the lab and also measured parameters like moisture, temperature, humidity and light. Here, only the *XY* coordinate is used.

The *XY* coordinates from the excel sheet are imported into MATLAB, and they are plotted in a graph. With the sensor coordinates, a distance matrix was developed as follows (Fig. 1):

Distance between each node with each other node is obtained with this matrix. Distance between two nodes is found by the equation:

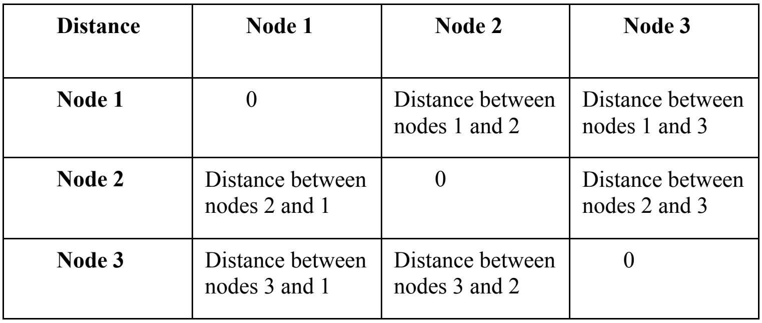
$$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \tag{1}$$

Friis equation gives us the direct relation between distance and RSSI,

$$P_r = \frac{P_t G_t G_r \lambda^2}{4\pi R^2} \tag{2}$$

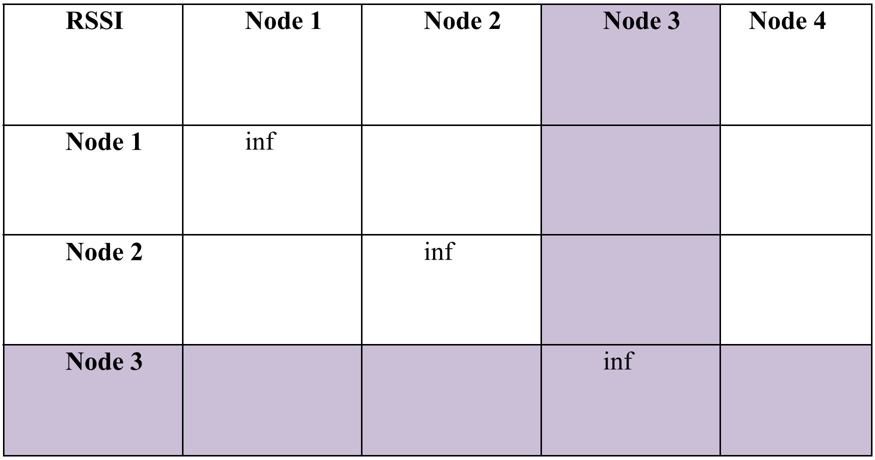
Since the obtained received power is in mW, we converted those mW values to dBm using the following equation:

$$\text{RSSI} = 10 * \log\left(\frac{P_r}{1\,\text{mW}}\right) \tag{3}$$



Distance	**Node 1**	**Node 2**	**Node 3**
Node 1	0	Distance between nodes 1 and 2	Distance between nodes 1 and 3
Node 2	Distance between nodes 2 and 1	0	Distance between nodes 2 and 3
Node 3	Distance between nodes 3 and 1	Distance between nodes 3 and 2	0

Fig. 1 Matrix for node in mesh network



RSSI	Node 1	Node 2	Node 3	Node 4
Node 1	inf			
Node 2		inf		
Node 3			inf	

Fig. 2 Matrix for diagonal elements in mesh network

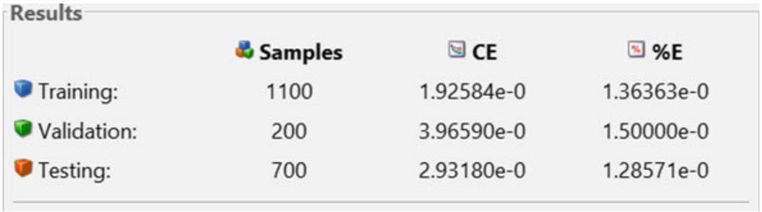
In our project, we considered the characteristics of an XBee module. From the datasheet, it can be found that the maximum range of the XBee modules can range up to 40 m. Hence, we found out the RSSI value for the maximum range to be −90 dBm and hence can be said as the maximum RSSI value that can be available in this sensor. Any value beyond which has to be faulty. Using this **−90 dBm** as threshold for good functioning, the RSSI matrix has been analysed.

If anyone node **(here node 3)** loses its both transmission and receiving capability, the RSSI matrix will be affected as follows (Fig. 2):

Here, in this table, rows are considered for reception, and column is for transmission.

When a sensor node goes faulty, practically all the values in the highlighted area might not exceed the threshold value. Similarly, in a good functioning node, not all values in the highlighted area need to be within threshold due to some unpredictable events. Hence, a node is said to be faulty only if all the node's RSSI values exceed the threshold value. A value of either 0 or 1 is assigned to each node depending on if the corresponding node is faulty or not. '0' is assigned to healthy nodes, and '1' will be assigned to the faulty ones.

A supervised neural network is trained to detect the faulty nodes in a wireless network. To train a neural network, one would need an input and output training dataset. We have trained the machine learning model with an input dataset of 40,000 samples and an output dataset of 2000 samples (i.e. for every 2000 input samples, one output sample is mapped to it). After training the dataset, we get the following error percentage which will be displayed in the results section.



Results

	Samples	CE	%E
Training:	1100	1.92584e-0	1.36363e-0
Validation:	200	3.96590e-0	1.50000e-0
Testing:	700	2.93180e-0	1.28571e-0

Fig. 3 Error percentage after training the model using training dataset from neural networks

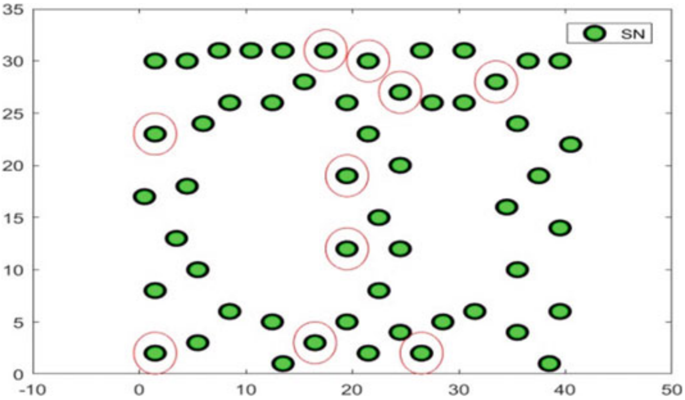


Fig. 4 Final output (faulty nodes are encircled with red circles)

4 Results and Conclusion

Even though this model gives us an accuracy of 98.8%, testing with hardware will give us the concrete proof which can be done in future. Here, free space is considered, and for future scope, obstruction can be considered (see Figs. 3 and 4).

References

1. Muhammed T, Shaikh RA (2017) An analysis of fault detection strategies in wireless sensor networks. J Netw Comput Appl 78:267–287
2. Zidi S, Moulahi T, Alaya B (2018) Fault detection in wireless sensor networks through SVM classifier. IEEE Sens J 18(1):340–347
3. Georgios M, Christos G (2015) Web based monitoring and irrigation system with energy autonomous wireless sensor network for precision agriculture. In De Ruyter B, Kameas A, Chatzimisios P, Mavrommati I (eds) Ambient intelligence. AmI 2015. Lecture notes in computer science, vol 9425. Springer, Cham
4. Louridas P, Ebert C (2016) Machine learning. IEEE Softw
5. Warriach EU, Tei K (2013) Fault detection in wireless sensor networks: a machine learning approach. In: 2013 IEEE 16th international conference on computational science and engineering, Sydney, NSW, pp 758–765

Image Description Generation Using Deep Learning

Neha Supe, Deepti Patil, Revathi Mahadevan, Tanvi Pandhre and Bharti Joshi

Abstract Over the years, various attempts have been made to make social media and devices more disabled friendly. Screen readers and other assisting technologies have made it easier for people with visual disabilities like low vision and blindness to interact with social media. However, images on the social network are still inaccessible to them. Developing the description of an image in natural language is an upcoming problem which is at the intersection of disciplines of artificial intelligence, computer vision, and natural language processing. The image captioning task, also known as visual captioning, makes the technical chassis of many important applications of semantic visual search and visual questioning, photo and video sharing in social media, visual intelligence in chatting robots, and aid for visually impaired people to perceive surrounding objects and happenings. To describe an image effectively, it involves the detection of objects in images, identifying scenes and attributes of the objects. Then, these labels are used to construct semantically meaningful sentences to generate paragraphs which describe the images. Our research makes an attempt to carry out the task to produce a paragraph like a description of images.

Keywords YOLO · CNN · LSTM · Deep learning · Image description

N. Supe · D. Patil · R. Mahadevan (✉) · T. Pandhre · B. Joshi
Ramrao Adik Institute of Technology, Navi Mumbai, Maharashtra 400706, India
e-mail: revathim15@gmail.com

N. Supe
e-mail: neha_supe@yahoo.com

D. Patil
e-mail: deepti4597@gmail.com

T. Pandhre
e-mail: tanvippandhre@gmail.com

B. Joshi
e-mail: bharti.joshi@rait.ac.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_121

1 Introduction

The task of describing the contents of the image is a complex one. Screen readers which are available now can only read the text on the screen of the device to the user. A visually disabled user must rely on text read out aloud by the screen reader to understand what the image is about. People with cognitive disabilities have difficulty in interpreting images, but they can understand the text. Therefore, the proposed system aims to tackle these challenges by generating a description of the image in natural language.

Describing an image is an easy problem for a human who has a perfect vision, but it is a difficult task for a machine as it involves both understanding the content of an image and then translating the information that is generated into natural language. The task of image description generation involves generating a multi-line paragraph of text which will describe the objects and actions in the image. A great deal of research is already available in this domain.

The image description framework can be divided into two modules logically, one is an 'image-based model' [1] which extracts the features and nuances out of our image, and the other is a 'language-based model' [1] which translates the features and objects given by our image-based model to natural sentences. The steps involved are as follows:

1. Scene Detection
2. Object Detection
3. Attribute Classification
4. Sentence Generation

The usual approach is to use CNN and RNN [2, 3]. The object detection and attribute classification are done by CNN [2–4], whereas the RNN generated sentences [5–7].

The proposed framework will be used in social media to describe the contents of the images in the user's feed. Our approach would enable the relationships and attributes between the objects that are detected by the object detector and classifier be described in detail. A multi-lined description is generated to describe the happenings in the image in a detailed understandable manner.

2 Related Work

Johnson et al. [2] proposed model generates detailed captions by creating and localizing regions in images. They used fully convolutional localization network (FCLN), recurrent neural network (RNN), and long short-term memory (LSTM). The architecture processes each image with a single, efficient forward pass and does not need external regions proposals. This image can be trained with only one round of optimization.

In [3], a technique is used to adjust weights of various samples, and it uses a two-stage optimization approach for missing concepts mining. This method detects added semantic concepts, and high accuracy is obtained. The methodology employed by them is RNN, CNN-RNN, Online Positive Recall and Missing Concepts Mining (OPR-MCM). Semantic concepts are identified, and high accuracy is achieved.

In the research [4], InstaPIC-1.1M method tries to solve personalized image captioning problem using YFCC100M data sets. It produces a describing sentence for a user image, computing for prior knowledge such as users active vocabulary or writing pattern in users previous documents. The methodologies used are natural language processing with convolutional neural networks (CNN). They have performed two tasks: the hashtag prediction helps in predicting a series of hashtags for an image, and the post-generation generates a natural sentence of normal words, emoji, and hashtags.

In another paper [8], scene graphs are generated using the objects detected in an image with their pairwise relationship predicted, while region captioning creates a natural language description of the objects, their attributes, relations, and other context information. The methodology used is Multi-level Scene Description Network (MSDN) which depends on the convolutional layers of VGG-16 and an LSTM-based language model to prepare natural sentences to interpret the region. In MSDN, given an input image, a graph is dynamically built up to form the relationship among regions with different linguistic meaning. The graph gives an innovative approach to allineate features from different tasks.

In [5], VGG-16 is used for object detection and scene classification, and a hierarchial recurrent neural network of two levels is used for sentence generation. The output produced by this model is in a paragraph and is detailed compared to the previous CNN models.

When we compare the existing projects with the proposed system, it is clear that there has been extensive research done towards the improvement in efficiency of generating image captions by combining different techniques and applying them on different types of data sets.

The system proposed is inclined towards applying object detection, scene recognition, attribute extraction, and sentence generation using CNN and LSTM. Therefore, we use YOLO [9] as an object detection algorithm as it is faster, accurate, and more efficient than CNN. It is also real-time. Detailed paragraphs are generated using two-level hierarchical RNN as it has shown to generate more descriptive sentences.

3 Proposed Methodology

3.1 Object Detection

You only look once (YOLO) model processes the image and predicts the class of object and bounding boxes in a single evaluation. Initially, we give the image as input to this model, it divides the image in $S \times S$ grid. Each grid predicts B bounding boxes with the confidence score. The probability that the object detected belongs to a particular class (*Dog*, *cat*, *banana*, *car*, etc.) is its confidence score. Each bounding box being evaluated takes five elements under consideration: x, y, w, h, and a box confidence score. We consider x and y as offset values, the height and width of the bounding box are normalized with respect to those of the image, so the values for x, y, w, and h are between 0 and 1.

The ideal size of images for YOLO is 416 × 416, but as it is made up of only convolutional and pooling layers, it can resize images on the fly. YOLO divides the image into the grid size like $S \times S$, and each cell of the grid predicts five bounding boxes with different aspect ratios and size. YOLO generates a tensor for every bounding box, which tensor will give its location within the grid, the height and width of the grid, with respect to that of the image, and the confidence score. It is possible that every bounding box may not contain an object. If centre of an object falls in the grid cell, then that cell is responsible for predicting that object. Bounding boxes give confidence score, which reflects the confidence of model that the bounding box contains an object and accuracy of its prediction.

Formula for the confidence score is $\mathrm{Pr(Object)} \times \mathrm{IOU}_{\mathrm{pred}}^{\mathrm{truth}}$. Confidence score is zero for boxes containing no objects, else it is equal to Intersection over Union (IOU) between prediction and ground truth.

Grid cells also detect the C class of the object using conditional class object probabilities, Pr (ClassilObject). Only one class per grid cell is predicted irrespective of the number of bounding boxes. At the time of testing, conditional class probabilities are multiplied by individual box confidence prediction, $\mathrm{Pr(Classi|Object)} \times \mathrm{Pr(Object)} \times \mathrm{IOU}_{\mathrm{pred}}^{\mathrm{truth}} = \mathrm{Pr(Classi)} \times \mathrm{IOU}_{\mathrm{pred}}^{\mathrm{truth}}$ this value gives class-specific prediction for each bounding box. For finding the final bounding boxes, we need to do the following two steps:

Remove the bounding boxes which have no object and also those that predict a confidence score less than a threshold of 0.24.
From the bounding boxes which claim to have an object, using Non-Max Suppression and Intersection over Union remove the redundancy of identifying the same object.

3.2 Scene Detection

Modern deep learning methods focus on using semantic context for smoothing or regularizing the predicted label maps while ignoring another rich semantic context available in the data sets. The data set uses class names of scenes in the images, and image patches' label map statistics for supervision signals for learning deep feature representations. The data set images are categorized according to classes.

We create a two-level label hierarchy for each of the original classes by exploiting semantic context, and CNN is fine-tuned with the proposed label hierarchies.

The representations of features learned by the model are more descriptive and distinguishable and provide accurate classification into classes. On the other hand, the label map statistics of image patches also provide crucial prior information on the appearance of patches since they specify the spatial layout of the semantics in the surrounding region.

During the training period, we adopt stochastic gradient descent (SGD) with minibatch sizes of 64, 64, and 10 to optimize the three CNN models, respectively The learning rate is initialized as 10^{-3} and decreased by a factor of 10, and step size is 2×10^4. During testing, the efficient pixel-wise forward-propagation algorithm was adopted for the Clarifai and the OverFeat models.

3.3 Sentence Generation

It is a complex task to generate paragraphs for images which require the model to understand fine-grained images and also develop long-term language reasoning. The generated paragraphs of multiple sentences to describe images should be detailed and also form coherent stories. The paragraph result for an image has to be informative and complex linguistically compared to single sentence description.

For our method, we will use the data set which comprises paragraph annotations, region-wise annotations, corresponding images. We will use data from MS COCO [10] and Visual Genome [11] which have images annotated with a multi-line sentence description.

In this paper, we are using long short-term memory (LSTM) network. It produces one word at each time step based on previously generated word, hidden state, and context vector.

The first level of LSTM: It is a single-layer LSTM. It will be given the pooled region vector as input, and the result produced will be a sequence of vectors where each vector will be used to generate one sentence each to form a paragraph. Each vector will give the topic the sentence is about.

The second level of LSTM: The second level of LSTM is a two-layer LSTM. The output of the first level of LSTM which is topic vectors, one for each sentence will be the input for the second level of LSTM. These vectors are combined to form one pooled vector and will be used to generate words of the sentences. The hidden state of the previous LSTM layer will be used to predict the words of the sentence at every time step. After an "end" token has been encountered, all the topics will be used to predict words to form sentences and will form a paragraph.

4 Results

We evaluated our generated image descriptions with METEOR [5]. METEOR is used for automatic metric evaluation which takes human judgement into account. It is used to evaluate a machine generated translation by calculating a score based on word to word matches comparison between the translation from model and a reference translation by human. It produces good correlation with human judgement at the sentence and segment level. The METEOR score evaluated for our model is 12.35.

5 Conclusion

The visually impaired is not able to access and interpret images. The existing technologies enable screen readers which do not interpret images itself. There is a lack of systems which would generate such descriptions in a comprehensive way. Therefore, the proposed system aims to tackle these challenges by generating a descriptive caption of the image. The system would generate a natural language description of an image in real time. Above research shows that the descriptions generated are accurate and semantically correct. This output would be in the form of speech so as to enable the visually impaired to comprehend the image. Some modifications or possible upgradation like describing GIFs and videos can be pursued in future.

References

1. Kinghorn P, Zhang L, Shao L (2017) Deep learning based image description generation. In: 2017 IEEE
2. Johnson J, Karpathy A, Fei-Fei L (2016) DenseCap: fully convolutional localization networks for dense captioning. In: IEEE conference on computer vision and pattern recognition
3. Zhang M, Yang Y, Zhang H, Ji Y, Shen HT, Chua T-S (2018) More is better: precise and detailed image captioning using online positive recall and missing concepts mining. IEEE Trans Image Process
4. Li Y, Ouyang W, Zhou B, Wang K, Wang X (2017) Scene graph generation from objects, phrases and region captions. In: IEEE international conference on computer vision
5. Krause J, Johnson J, Krishna R, Fei-Fei L (2017) A hierarchical approach for generating descriptive image paragraphs. In: IEEE conference on computer vision and pattern recognition
6. Gu J, Wang G, Cai J, Chen T (2017) An empirical study of language CNN for image captioning. In: IEEE international conference on computer vision
7. Feng Y, Lapata M (2013) Automatic caption generation for news images. In: IEEE transactions on pattern analysis and machine intelligence
8. Mao J, Huang J, Toshev A, Camburu O, Yuille A, Murphy K (2016) Generation and comprehension of unambiguous object descriptions. In: IEEE conference on computer vision and pattern recognition
9. YOLO9000 Better, faster, stronger [Online]. Available https://pjreddie.com/media/files/papers/YOLO9000.pdf
10. Lin T-Y, Maire M, Belongie S, Hays J, Perona P, Ramanan D, Dollar P, Zitnick CL (2014) Microsoft coco: common objects in context. In: ECCV
11. Krishna R, Zhu Y, Groth O, Johnson J, Hata K, Kravitz J, Chen S, Kalantidis Y, Li L-J, Shamma DA, Bernstein M, Fei-Fei L (2016) Visual genome: connecting language and vision using crowdsourced dense image annotations. arXiv preprint: arXiv:1602.07332

Multi-agent-Based Interference Mitigation Technique in Wireless Communication System

P. Aruna and A. George

Abstract The popularity of agents in artificial intelligence (AI) can be seen almost everywhere in the form of effective decision making, predictive analysis, expert systems, and so on. In parallel, wireless communication systems in the form of wireless local area networks (WLANs) and wireless personal area networks (WPANs) are also providing tremendous support for data communication. Exploring and utilizing the benefits of artificial intelligence and wireless communication systems together in an environment are still in the nascent stage due to the divergent characteristics of the respective domain. One of the major drawbacks in the existing wireless communication system is interference in 2.4 GHz band. This work proposes a multi-agent-based interference mitigation technique to mitigate the interference issues in wireless communication system and aims to enhance the communication process in terms of packet delivery ratio. This work is implemented as a pilot project in an educational institution for teaching students in wireless communication environment, the result shows that technology has added new dimensions to teaching–learning process, and performance of the wireless communication system is also increased in terms of packet delivery ratio.

Keywords Artificial intelligence · Agents · Wireless local area network · Wireless personal area network · Interference · 2.4 GHz

P. Aruna (✉)
Department of Software Engineering, Periyar Maniammai Institute of Science and Technology, Thanjavur, India
e-mail: rparuna.mca@gmail.com

A. George
Department of Mathematics, Periyar Maniammai Institute of Science and Technology, Thanjavur, India
e-mail: amalanathangeorge@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_122

1 Introduction

The emergence and advancement of communication technologies for flexibility among applications, virtual communities, and Web services are increasing day by day. This technological development accelerated a lot in the wireless communication devices, and these communication devices can be broadly classified into wireless personal area network devices and wireless local area network devices. Each device in WPAN and WLAN is having its own characteristics and restrictions. When both WPAN and WLAN mobile communication devices coexist in a particular environment, there arises interference due to the usage of unlicensed ISM band of 2.4 GHz.

In wireless communication, the frequency-hopping spread spectrum (FHSS) and direct-sequence spread spectrum (DSSS) are used by WLAN and WLAN. Transmission can be initiated [1] either by FHSS or DSSS. When the receiver detects the unwanted signal in the received signal along with original signal or it receives corrupted signal, then it is termed as interference or noise. When there is the best performance between data transmission among Bluetooth and Wi-Fi devices, then there is less interference [2]. If there is interference among the devices, then there might be a need to resend data among the communications which leads to worst or poor performance. Following are the foremost negative effects of interference.

- A decrease in the wireless range between devices;
- A decrease in data throughput;
- Intermittent or complete loss of the connection;
- Difficulty pairing between device's discovery phase.

Some of the positive aspects of wireless communication such as distribution, cooperation, decentralization, and mobility can be interrelated to the characteristics of agents. In addition to these common attributes, agents offer more intelligence and autonomy to act on its own in the environment. The main contributions of this work are as follows: (1) use of agent technology in the domain of wireless communication, (2) agents are used to mitigate the interference issues among the WPAN and WLAN devices, and (3) use of agents to increase the throughput and packet delivery ratio. This work is designed using Java Agent Development Framework [3].

The remainder of this paper is organized as follows. Section 2 provides the underlying motivations for this proposed work. Section 3 discusses related works on agent-based technologies for wireless communication systems. Section 4 represents the proposed work in detail. Section 5 represents the implementation of proposed work with a case study to measure the performance of wireless communication systems, and finally, Sect. 6 concludes the paper with a brief summary of the work and also gives an outline for the future work.

2 Motivations

A multi-agent-based approach is presented in this proposed work to deal with interference in wireless communication systems. An agent technology solution is proposed since agent characteristics have the ability to perceive the environment and act accordingly. This will be used to enhance the performance of the wireless communication systems in terms of resource optimization. Concerning the choice and the usage of agent technology to come up with new interference mitigation technique for wireless communication system, it is simply admired by the dynamic characteristics of agents such as mobility, interactivity, autonomy, and intelligence. Indeed, the proposed work can be used to significantly enhance the performance of wireless communication system and particularly the elimination of interferences, by moving the data collected by the proposed agents in the wireless communication devices.

3 Related Work

It can be observed that researchers [4–6] have already proposed agent-based technologies for the wireless communication systems, but serves different purposes. Our foremost objective is to design and develop a multi-agent-based system to support wireless communication system in the 2.4 GHz band with low interference among the devices.

4 Proposed Approach

This approach is based on the usage of multi-agents in the wireless communication environment. This work mainly used two kinds of dynamic topologies namely network topology and agent topology. Network topology describes physical layout and the relationship among the devices in the environment. Agent topology describes logical organization of various agents in the environment. To generate network topology and agent topology, this system utilizes various agents. The role of agents in this approach is to detect the list of devices in the environment, to classify the devices based on their characteristics, to perform the routing activities among the devices, and to mitigate the interference among the devices in the environment.

4.1 Architecture

The multi-agent architecture is illustrated by Fig. 1. This work reveals that users along with WPAN and WLAN devices are working in specific locations and it is monitored by the environment agent. WLAN and WPAN agents, hold details information about

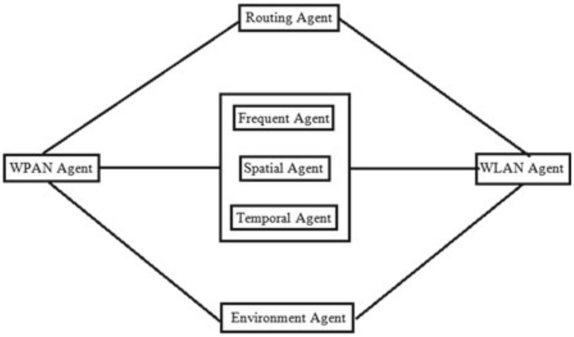


Fig. 1 Multi-agent architecture for wireless communication

the WLAN and WPAN devices in the environment. Routing agent: this agent holds the routing information between the transmitter and receiver devices. This routing agent supports both the unipath and multipath routing protocols [7] to disseminate information to all the devices in the environment. When a source node has to send data packets to a destination node, it searches its route table to find if the route already exists. If no route exists, then the source node initiates a route discovery process by broadcasting route request (RREQ) packet to all its neighbors. When a RREQ reaches a mobile node and if it is not the destination node, it adds its ID to the next node and forwards/multicasts to its neighbors and broadcasts a route reply (RREP) packet to the sender along the reverse path in network. This continues until the RREQ packet reaches the destination node or the TTL reaches a threshold value. If a path is discovered, then the path is stored in the routing table along with a time stamp value *T*. Frequent agent, spatial agent, and temporal agent play a vital role mitigating interference among the WLAN and WPAN devices to ensure enhanced performance of the wireless communication system. The role of frequent agent is to monitor the frequency of communication between the transmitter and receiver, and priority is given to the most frequent communication devices based on ranking mechanism. The role of spatial agent is to keep Wi-Fi and Bluetooth devices logically separately with certain distance along with their respective antennas. Insulating material can also be used to separate the devices. Bluetooth/Wi-Fi spatial isolation is impossible when both radios share a common transmission medium which may be an antenna, transmitter, and receiver.

The role of temporal agent in the proposed architecture is to offer the Bluetooth and Wi-Fi radios that are embedded in the same device but takes time slice between them in transmitting or receiving information. It is one of the coexistence methods. This kind of isolation can be implemented between Wi-Fi and Bluetooth with a support of printed circuit board which informs all the connected devices other than transmitting device to refrain from sending data during this time.

4.2 Proposed Interference Mitigation Algorithm

To overcome interference in the wireless communication system, this work proposes the following FST (frequent spatial, temporal) algorithm mechanism in the agents.

Proposed Algorithm

1. Detecting list of devices accessing the system and its neighborhood with the support of environment agent;
2. Monitoring each device performance using WPAN and WLAN agent;
3. Routing agent is deployed for each and every category of WPAN and WLAN agent to route data among the devices and its uses frequent spatial and temporal agent to overcome the interference with the devices and sharing of data.
4. Classifying the devices based on its category/signal strength using frequent, space, and/or time.
5. Each agent is interrelated to overcome the isolation error, and cooperation is achieved with the support of agent communication language.

The above proposed algorithm mitigates interference issues in the heterogeneous wireless communication network.

5 Performance Measure

To evaluate the efficiency of the proposed multi-agent-based system for wireless communication, the proposed work is implemented in JADE environment and the data communication and transmission are selected from the learning management system (LMS) of an educational institution. Various types of data from the LMS such as audio, video, text, and animation are taken into account as packets, and the performance of these packets is measured in terms of packet delivery ratio.

Packet delivery ratio is defined as the ratio of data delivered packets to the corresponding destinations to those generated in terms of constant bit rate. Illustration of the experiment setup is shown in Fig. 2.

The experiment was conducted with two cases with the support of same set of twenty-five users and data packets from different locations: the first one with the support of multi-agent-based wireless communication system exclusively for WPAN devices, WLAN devices and with the coexistence of WLAN and WPAN devices and the second one was without the support of multi-agents for WPAN devices, WLAN devices and along with the coexistence of WLAN and WPAN devices. Tables 1, 2, 3 and Fig. 3 give the packet delivery ratio for the experiment setup with UDP transmission. Tables 4, 5, 6 and Fig. 4 give the packet delivery ratio for the experiment setup with TCP transmission. It can be observed that the multi-agent-based wireless communication systems perform better in terms of packet delivery ratio for all the WPAN communication, WLAN communication and for the coexisted WLAN and WPAN communication in both UDP and TCP transmission.

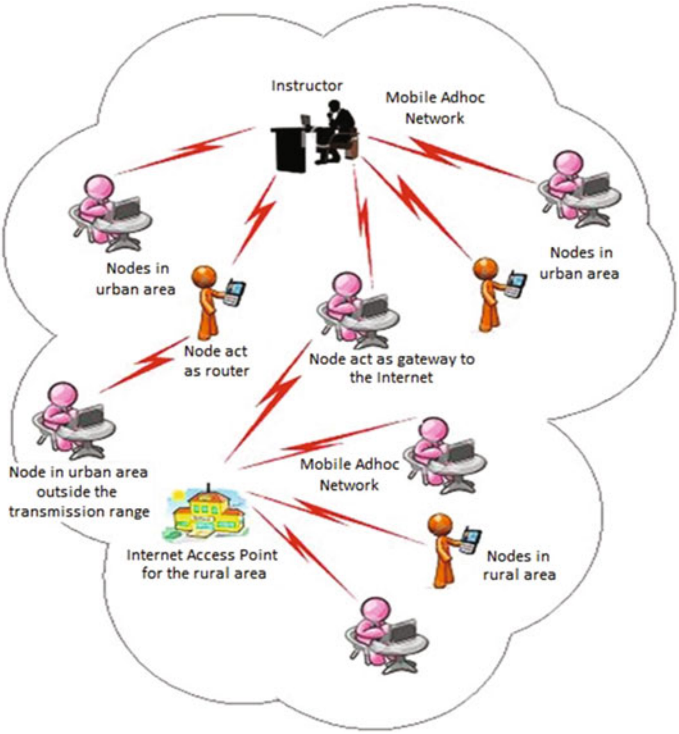


Fig. 2 Illustration of the experimental setup

Table 1 Packet delivery ratio for the experiment setup WPAN devices for UDP

	Wireless personal area network (WPAN)
Wireless communication without multi-agents	s:4306 r:2139 r/s Ratio:0.4967 f:0
Wireless communication with multi-agents	s:4336 r:2639 r/s Ratio:0.6086 f:0

Table 2 Packet delivery ratio for the experiment setup WLAN devices for UDP

	Wireless local area network (WLAN)
Wireless communication without multi-agents	s:4287 r:4282 r/s Ratio:0.9988 f:1737
Wireless communication with multi-agents	s:4387 r:4385 r/s Ratio:0.9995 f:1737

Table 3 Packet delivery ratio for the experiment setup WPAN and WLAN devices for UDP

	WPAN + WLAN
Wireless communication without multi-agents	s:4311 r:2445 r/s Ratio:0.5672 f:0
Wireless communication with multi-agents	s:4341 r:2885 r/s Ratio:0.6672 f:0

Fig. 3 Packet delivery ratio—UDP for the experiment setup

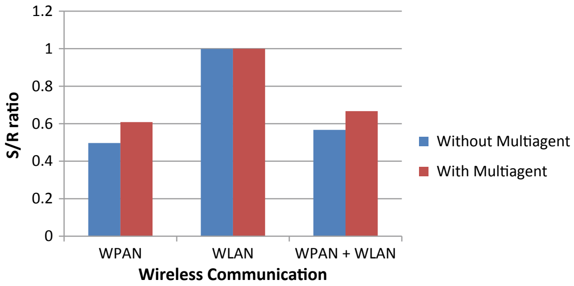


Table 4 Packet delivery ratio for the experiment setup WPAN devices for TCP

	Wireless personal area network (WPAN)
Wireless communication without multi-agents	s:20 r:16 r/s Ratio:0.8000 f:2
Wireless communication with multi-agents	s:20 r:18 r/s Ratio:0.9000 f:4

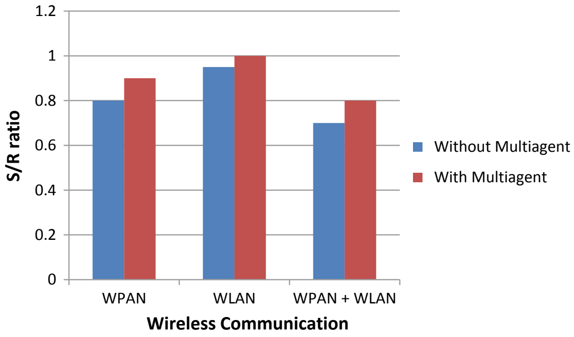
Table 5 Packet delivery ratio for the experiment setup WLAN devices for TCP

	Wireless Local area network (WLAN)
Wireless communication without multi-agents	s:20 r:19 r/s Ratio:0.9500 f:2
Wireless communication with multi-agents	s:20 r:20 r/s Ratio:1.0000 f:2

Table 6 Packet delivery ratio for the experiment setup WPAN + WLAN devices for TCP

	WPAN + WLAN
Wireless communication without multi-agents	s:20 r:14 r/s Ratio:0.7000 f:0
Wireless communication with multi-agents	s:20 r:16 r/s Ratio:0.8000 f:2

Fig. 4 Packet delivery ratio—TCP for the experiment setup



6 Conclusion

The underlying interference issues between WPAN and WLAN devices in the wireless communication systems must adapt themselves to a dynamically changing environment and devices; also, the performance should be increased in the wireless communication in terms of throughput and packet delivery ratio. With these objectives, this paper proposed multi-agent-based interference mitigation technique in wireless communication system, and this study deploys the agent technology for the communication between devices and to mitigate the interference issues among the WPAN and WLAN.

From the case study implementation, it is noted that the proposed model is having technology agnostic, friendly to legacy technologies, extensible, scalable (over a broad range of dimensions), dynamic and adaptive, resilient and trustworthy.

References

1. Qureshi A, Guttag J (2005) Horde: separating network striping policy from mechanism. In: MobiSys
2. Barford P, Crovella M (1998) Generating representative web workloads for network and server performance evaluation. In: SIGMETRICS
3. Bellifemine FL, Caire G, Greenwood D (2007) Developing multi-agent systems with JADE, vol 7. Wiley, Hoboken
4. Harrabi S, Chainbi W, Ghedira K (2013) A multi-agent approach for routing on vehicular ad-hoc networks. Procedia Comput Sci 19:578–585
5. Cicirello V, Peysakhov M, Anderson G, Naik G, Tsang K, Regli W, Kam M (2004) Designing dependable agent systems for mobile wireless networks. IEEE Intell Syst 19(5):39–45
6. RoyChoudhuri R, Bandyopadhyay S, Paul K (2000) Topology discovery in ad hoc wireless networks using mobile agents. In: Mobile agents for telecommunication applications, pp 531–542
7. Choudhury RR, Paul K, Bandyopadhyay S (2004) MARP: a multi-agent routing protocol for mobile wireless ad hoc networks. Auton Agent Multi-Agent Syst 8(1):47–68

Implementing Machine Learning on Edge Devices with Limited Working Memory

A. Harish, Saksham Jhawar, B. S. Anisha and P. Ramakanth Kumar

Abstract The architecture is aimed at pushing the computing towards the edge. When most of the computation occurs towards the edge device where the data is generated, the processing becomes faster and more efficient. This improves the user's wait time and delivers results faster to the user. Machine learning techniques are implemented in the edge devices. While one can process data at the sensor, what one can do is limited by the processing power available on each IoT device. Data is at the heart of an IoT architecture, and one needs to choose between immediacy and depth of insight when processing that data. The more immediate the need for information, the closer to the end devices your processing needs to be. We propose an architecture to use machine learning algorithms in the limited memory of the edge device.

Keywords Edge device · Fog layer · Working memory · Thin client

1 Introduction

Edge computing is a technique that introduces a new computation layer between the cloud and end-users. The motivation behind developing this layer is to overcome the flaws present in cloud computing. Cloud computing suffers various problems ranging from processing of huge amounts of data (network congestion) to security issues arising from physical distance between the cloud and its end-user. As the physical distance increases, latency in data communication increases. To counter

A. Harish (✉) · S. Jhawar · B. S. Anisha
Information Science and Engineering, R.V. College of Engineering, Bengaluru, India
e-mail: it.is.harish.a@gmail.com

S. Jhawar
e-mail: sj.sakshamjhawar@gmail.com

B. S. Anisha
e-mail: anisha@rvce.edu.in

P. Ramakanth Kumar
Department of Computer Science and Engineering, R.V. College of Engineering, Bengaluru, India
e-mail: ramakanthkp@rvce.edu.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_123

these problems, edge computing devices store and process some amount of data in the newly introduced layer. This layer is present physically closer to end-users, lowering the latency problems.

Traditional edge computing machine learning models are based on the concept of training classifiers present on a single edge device. However, this results in excessive load on edge devices. To increase the efficiency and reliability of these devices, another system that acts as a server can be used to train classifiers based on existing dataset. The model parameters generated on the server can be sent to edge device to assist with the decision-making process. This would significantly decrease the load on edge devices and would enable them to take quick actions.

2 Related Work

A team comprising of individuals from the city of Antwerp, Belgium and the Flemish region collaborated to develop large-scale living laboratory to test smart city applications [1]. The team worked with local government to put their anomaly detection approach to test. The process included mounting air quality sensors on the vehicles used by Bpost (postal service of Belgium). These vehicles covered almost every corner of the city while delivering goods and at the same time provided the team with real-time air quality data. This in turn eliminated the need of using static sensors for data collection. The objective of the test was to alert civilians about the air pollution and observe huge amounts of organic compounds present in the atmosphere.

Conventionally, data from sensor is sent to the centralised cloud layer, where it is processed. This approach suffers from latency flaws and network congestion. To counter this, the team designed their system in such a way that most of the computation takes place at computation nodes, also called as fog resources. These nodes are positioned in close proximity of the sensor to provide enhanced data transmission. The team used BIRCH algorithm to cluster data samples. The parameters related to air quality aberration were identified using robust covariance algorithm. As a result, in the case of anomaly detection, computation nodes notified the centralised server and IoT sensors.

To conclude, introducing fog resources enabled faster response time [2–6] and showcased wide view of network behaviour [7–10].

3 Architecture and Implementation

To overcome the latency in transferring the data to server for adequate action and the error rate in taking actions based on simple constraints, we propose a model that inculcates the swiftness of edge computing and accuracy of machine learning models trained by the resource-rich server.

The proposed model has two stages of operation that happens in different physical locations on different devices. The division of the system into stages further eases the process and implementation. The two stages are:

3.1 Training the Model in the Server/Cloud

We deal with a heavy server system in this model. The server system has resources like RAM size and features like multithreading that compensate for the lighter client edge node. The majority of the training occurs on the server where high processing speed is available.

The data collected for the specific use case is used to train the machine learning model. Different models such as neural networks, linear logistic regression and polymorphic logistic regression are trained and tested over the cross-validation dataset. The model that provides the most accuracy and is the most suitable for the given use case is chosen for the application.

The model is now trained using the dataset collected from various sources and is used for further processing.

3.2 Computation/Decision-making on the Edge Device

The edge device is a very thin client. This paper concentrates on getting the edge to work using a very small working memory. This is suitable for devices that are embedded circuits and have limited working memory to function on.

Noting that the training of the machine learning model is already complete on the server, the edge device inherits the parameters of the model from the server. The edge device now collects the required and agreed upon data from the environment.

Following this, the edge device is ready to be put to use. The parameters obtained from the server and the newly obtained environmental values are used to compute the appropriate result for the given situation.

In a dynamic system with real-time data, the cycle of this process can be used to obtain relevant results from time to time.

For the purpose of simplicity, we have used the theory logistic regression [11] with a linear graph to discuss the model. However, we can use other more complicated models such as neural networks, support vector machines, etc., and obtain results accordingly without much variation in the model or the latency incurred.

Further, we provide details about the implementation of a fire detection system that we implemented. The system uses logistic regression model to detect the presence of fire with the usage of physical parameters such as temperature, relative humidity, etc. (Figs. 1 and 2).

The machine learning model to be implemented is chosen considering the merits and demerits of various models. The model is trained using the data previously collected. Once the model achieves its required efficiency, it is ready to undertake connection requests from edge devices.

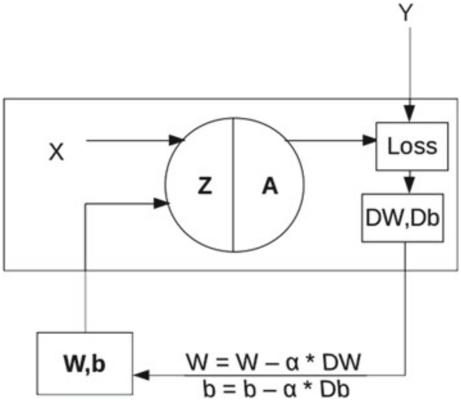


Fig. 1 Training the machine learning model in the server

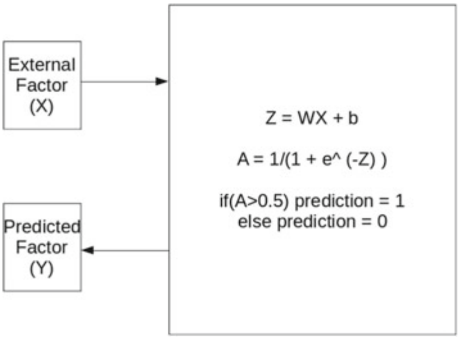


Fig. 2 Computation using machine learning at the edge

The edge device connects with the server and obtains the parameters of the machine learning model that was trained. Now, the device is ready to function to its needs. The edge device senses the external environment and computes the result according to the machine learning system, thus giving better and faster results and moving the analytics towards the edge device (Fig. 3).

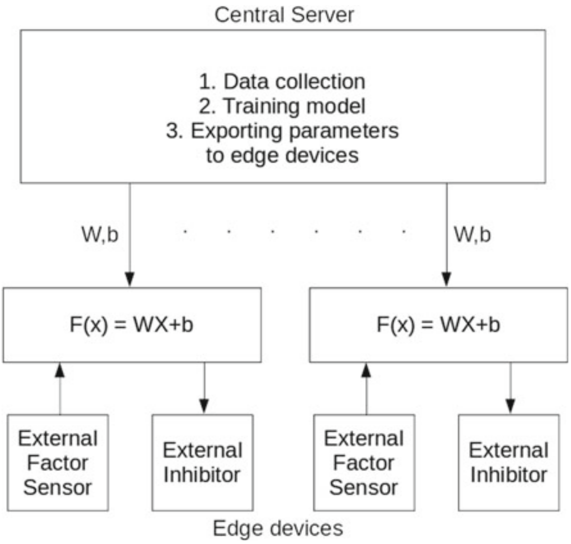
The traffic towards the server is now reduced. The edge device performs a part of the computing and thus reduces the load on the server.

Further, the model can be modified to send feedback to the server to improve the performance of the machine learning model developed.

4 Experimentation and Results

The proposed model was implemented, and the application was put to test. We implemented the server using a HP laptop with 8 GB of RAM. We chose a device with light computational capabilities because it is easier and cheap to access and program. The added advantage of cost was on our side.

Fig. 3 Architecture of the complete system



The application we chose to implement was that of a fire detection model in a normal household. We chose this application for two reasons.

4.1 *Ease of Obtaining Data*

The input data needed for the training of the machine learning model at the server was easily available for different sources such as the nist.gov site and our own data sources from various locations across the city of Bengaluru.

Temperature and relative humidity were used in the initial trial runs. Other factors such as atmospheric pressure, SO_2 and NO_2 levels of the air were used to experiment with the model. The model gave similar results as that of the results specified here.

4.2 *Ease of Implementation and Testing*

The proposed model could be easily implemented for the application. We implemented logistic regression [11] with the available data to classify the situations of existence of fire and the non-existence of fire for the input read from the sensors.

We noticed that the proposed architecture includes the goodness of server training with that of edge device decision-making. We compared the results of this hybrid model with that of a simple constraint-based decision system. In this system, the edge device made decisions based solely on the fixed constraints of the physical environment. For example, say temperature >35 °C and relative humidity greater than 50%.

Table 1 The test results

Type of model	Type of input	
	Positive (112 test samples)	Negative (112 test samples)
Simple constraints	101	105
Proposed architecture	111	112

The results were in favour of the proposed architecture.

The positive samples represent the test scenarios where there was an existence of fire, whilst the negative samples represent the absence of fire.

From Table 1, it is clear that the proposed model outperforms the simple constraint model that has been used historically [12] for edge computing.

5 Conclusion

The concept of edge computing is still young, and the research to explore this domain is evolving exponentially. In essence to the points discussed in this paper, edge computing proposes a solution to solve problems related to network congestion and latency by reducing the physical distance between centralised cloud and end-user devices. As per the results obtained, introducing edge nodes between centralised cloud and end-user devices has proven to be more efficient than the traditional systems. The proposed method which incorporates a machine learning model not only improves the scalability but also increases adaptability and the ease of maintenance. Processing raw data in edge nodes and passing on the relevant information to cloud expedite the overall communication process.

References

1. Santos J, Leroux P, Wauters T, Volckaert B, De Turck F (2018) Anomaly detection for smart city applications over 5G low power wide area networks. April, 2018
2. Shi W, Cao J, Zhang Q, Li Y, Xu L (2016) Edge computing: vision and challenges. October, 2016
3. Villari M, Fazio M, Dustdar S, Rana O, Rajan R (2016) Osmotic computing: a new paradigm for edge/cloud integration. December, 2016
4. Yi S, Li C, Li Q (2015) A survey of fog computing: concepts, applications and issues. June, 2015
5. Ai Y, Peng M, Zhang K (2017) Edge computing technologies for internet of things: a primer. July, 2017
6. Gao Y, Hu W, Ha K, Amos B et al (2015) Are cloudlets necessary? October, 2015
7. Mach P, Becvar Z (2017) Mobile edge computing: a survey on architecture and computation offloading. September, 2017

8. Dinh HT, Lee C, Niyato D, Wang P (2011) A survey of mobile cloud computing: architecture, applications, and approaches. October, 2011
9. Luan TH, Gao L, Li Z, Xiang Y, Wei G, Sun L (2015) Fog computing: focusing on mobile users at the edge. February, 2015
10. Tong L, Li Y, Gao W (2016) A hierarchical edge cloud architecture for mobile computing. April, 2016
11. Peng J, Lee KL, Ingersoll GM (2002) An introduction to logistic regression analysis and reporting. September, 2002
12. Sen K, Sarkar J, Saha S, Roy A, Dey D, Baitalik S, Nandi CS (2015) Automatic fire detection and controlling system. May, 2015

Smart Transportation: An Edge-Cloud Hybrid Computing Perspective

Aashish Jaisimha, Salman Khan, B. S. Anisha and P. Ramakanth Kumar

Abstract Internet of things is enhancing various industries by connecting all devices to the Internet to solve key challenges. Transportation is a huge sector where extensive research and development is undergoing. The current developments by various independent corporate research companies use the power of cloud computing for storage and processing of data. With the need for quicker decision-making in critical services, a new paradigm, called edge computing is under research, where latency is tackled. Since, each has its own limitations, a new approach is given that involves both these paradigms—called hybrid computing. We would like to discuss the merits and demerits of each of these paradigms and propose two variants of hybrid computing with respect to smart transportation and smart tires in specific.

Keywords Internet of things · Cloud computing · Edge computing · Edge analytics · Hybrid computing · Centralized architecture · Distributed architecture · Embedded systems-on-a-chip

1 Introduction

Transportation, being an ever-challenged sector due to the rapid increase in its customer base poses lots of technological challenges. The need to design smarter solutions is now more than ever. Of the total sector, the major percentage is accounted by road transport. Tires are the only points of contact between the vehicle surface

A. Jaisimha (✉) · S. Khan · B. S. Anisha
Information Science and Engineering, R.V. College of Engineering, Bengaluru, India
e-mail: aashishcool99@gmail.com

S. Khan
e-mail: salmank123417@gmail.com

B. S. Anisha
e-mail: anisha@rvce.edu.in

P. Ramakanth Kumar
Department of Computer Science and Engineering, R.V. College of Engineering, Bengaluru, India
e-mail: ramakanthkp@rvce.edu.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_124

and the road. With every vehicle, there are multiple tires associated which need to function in a synchronized manner for the vehicle to run smoothly. Thus, the success of road transport is largely dependent on the tires and the lack of maintenance is a primary reason for failure of the system, and hence contributes to major accidents. Yet, it is one of the least explored domains under transportation. Tire bursts are commonly caused due to improper inflation, tire-aging, overloading, low quality of tires, and over-speeding.

Internet of things (IoT) connectivity is redefining today's world in a vast spectrum of applications such as smart-watches, smartphones and every possible appliance to build smart-homes and smart-cities. Thus, by incorporating IoT connectivity and using the power of sensors and data, smart tires can be developed to improve road safety, tire life, and fuel efficiency.

Multiple paradigms can be approached for the storage and processing of data. The most common in use is the cloud computing paradigm, which is the centralized architecture. The newer and the fast advancing paradigm is the edge computing paradigm, which is the distributed architecture. Most of the current development in smart tires are using cloud computing. It has not been explored much in the direction of edge computing. We discuss how the mixture of both of these paradigms can be useful. The goal is to bring the right balance between performance and speed.

Organization: The remaining research paper is structured as follows: In Sect. 2, we discuss the existing technology and the developments made in the field using IoT connectivity. In Sect. 3, we discuss and differentiate the various data computation paradigms. In Sect. 4, we propose two variants of hybrid architecture derived from both edge and cloud computing. Section 5 poses the key challenges in implementing our proposed architecture. We conclude the paper in the final section.

2 Existing Technology

2.1 Conventional Identification Technique

In the conventional days, there used to be a 'retread' mark on the tires. The wearing up of that particular mark used to be an indication to either change the tire or subject it to retreading process. This was a naïve approach to observe the normal aging of the tire and did not consider the other aspects leading to tire bursts (Fig. 1).

Another measure that helps to determine the aging of the tire is minimum legal tread depth. Tread wear indicators in the groove must not be let to align with the tire [1, 2].

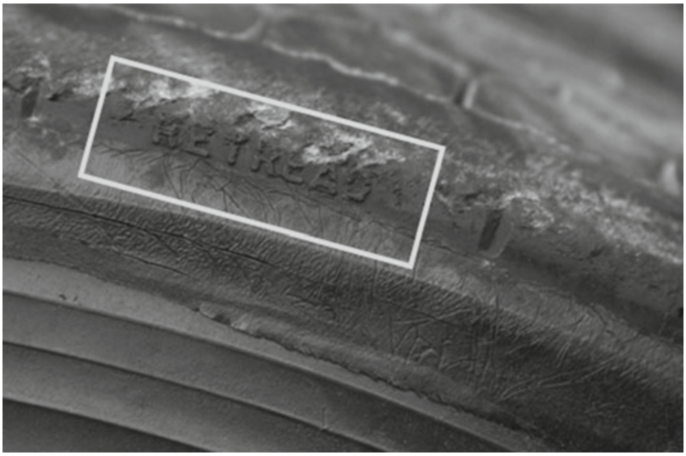


Fig. 1 Conventional identification of tire wearability

2.2 *IoT Connectivity*

Based on the requirements, various kinds of sensors have been deployed into the tires, most of which are to serve the common purpose of safety. Inflation pressure is an important quantity that is a good warning for most abnormalities in the tire. The pressure sensor is responsible for indicating when the internal pressure decreases or increases than a certain threshold. This data is useful to notify the owner to get the tires inflated. There are multiple contributing factors to changes in pressure, viz. temperature, speed, load, etc. Thus, the monitoring of tire parameters can be done by collecting the data. Another common observation that can be made on highways is the burning of tires. This can be detected either by the temperature sensor or the odor sensor (since tire burns cause a typical rubber burning odor). A transportation technology company, continental has developed its product called ContiConnect for digital tire monitoring [3, 4].

In the present scenario, the data that is collected is transferred onto a server or a cloud for processing. The traditional cloud architecture for processing of data has its own limitations, such as high network traffic, data management cost, and most importantly latency. In life-critical scenarios, latency plays a huge role and near-instantaneous decisions are of utmost importance. For example, tire design and purpose would be a lot different in the case of autonomous vehicles. The decision that needs to be taken would be based on more complex scenarios, such as driver behavior, pothole detection, and automatic breaking. Hence, pushing all data onto the cloud for processing will consume a lot of time and does not serve the service concerned.

3 Computation Approaches

3.1 *Cloud Computing*

In a cloud computing paradigm [5, 6], the data is sent from the tires, which is our edge node to the server for processing. The need for cloud is justified by the low processing power and the storage capability of the tire as the edge node. However, it causes issues such as network congestion and latency when there are continuous data and low response time required. In the process, availability and decision-taking time are compromised. Thus, in real-time delay-sensitive applications, where a decision has to be taken extremely quickly, it is not feasible to send the data to the server, provided the data can be processed locally (Fig. 2).

3.2 *Edge Computing*

When cloud computing was introduced, the end-devices had limited computing capacity and the devices were only capable of data collection. But with the rapid advancements in embedded systems-on-a-chip, it is now possible to perform complex computations on small end-devices. The edge computing paradigm proposes the processing of the data to be done locally. Therefore, it solves the issue of latency posed in the cloud architecture, where the processing can be done in the tire, which is the edge node itself. By this, the decision can be taken quickly. Another important advantage of edge computing over cloud computing in the transportation space

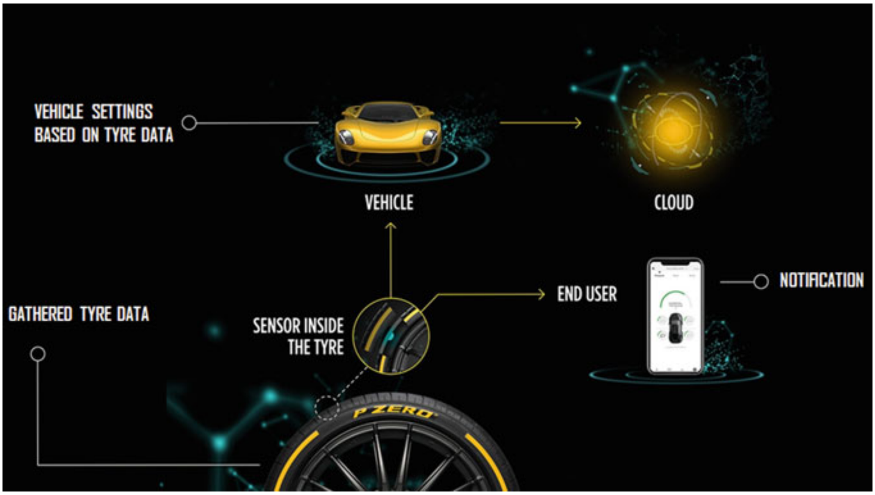


Fig. 2 Cloud interaction with tire and vehicle. *Source* Pirelli

would be the lack of need of network connection to work. In many situations, such as mountainous terrain, forest area, or rural area for that matter, the network connectivity cannot be expected to be flawless. Thus, in low bandwidth conditions, the edge computing is the appropriate approach.

Further, distributed clouds in the local server called a cloudlet can be used for processing of data with each such cloudlet being a part of the vehicle software [6, 7]. The research has also been in the direction of introducing more layers in between the edge and the cloud where computation can be distributed, giving rise to fog computing [8].

Edge Analytics

The primary reason for data to be sent to the cloud in IoT is to gather insights from the data; take a decision and strike an action. With rapid advancements in embedded systems-on-a-chip (SoC) has resulted in powerful and resourceful devices that are capable enough to run a full-fledged operating system or a complex algorithm. Edge analytics [9, 10] can be used for the computational analysis of the data gathered locally on the edge device, i.e., the tire. The time taken is drastically improved for taking data-driven decisions at real time. Edge analytics involves developing the analytics model, deploying and executing it on the edge. The complexity of analytics model is largely dependent on the processing power and the storage capacity of the device in the tire.

4 Hybrid Computing

With cloud computing and edge computing paradigms, both having its own advantages and disadvantages, it is best to bring about the right balance. Thus, both the paradigms can be incorporated based on the type of data and the service required with the data. We would like to propose two variations of hybrid architecture [6].

4.1 Non-interleaving Edge-Cloud Architecture

In this variation, the services direct the computation approach which is dependent on the criticality of the said tire services. A highly critical service would require low latency and high response time and would therefore process the data at the edge. The criticality of the service should be decided by the developer or manufacturer. Therefore, for every service, the analytical model must be designed at its target computation facility. For example, to determine the wearing of the tires, the cloud computing approach is more suitable, whereas, for auto-braking system, edge computing is more suitable. The primary goal would be to classify what data needs to be processed in the cloud and what data must be processed in situ (Table 1).

Table 1 Service and their appropriate computation paradigm based on criticality

Service	Criticality	Paradigm
Inflation detection	Medium	Cloud
Automatic braking	High	Edge
Life-cycle assessment	Low	Cloud
Tire burst detection	High	Edge
Hump alert	High	Edge
RFID vehicle identification	Medium	Cloud

Figure 3 shows hybrid non-interleaving edge-cloud architecture. It is important to know when the data needs to be processed locally, which is dependent on the type of service being demanded.

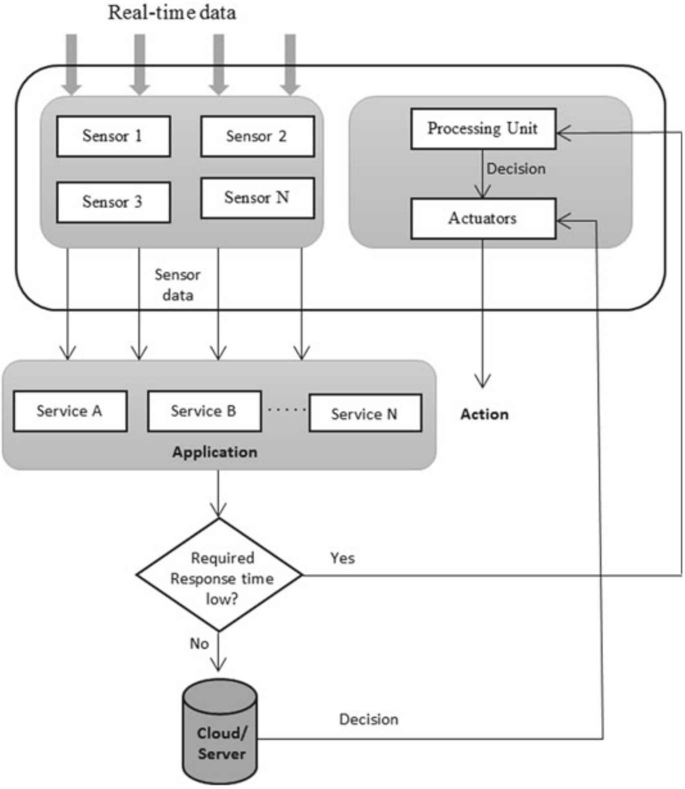


Fig. 3 Decision flowchart for non-interleaving edge-cloud architecture

4.2 Interleaving Edge-Cloud Architecture

The first variation discussed above affiliates one paradigm approach to a service of an application and the computation is carried out. But, for a service, to improve the performance, the edge-cloud paradigms can both be applied, provided the communication between the edge and the cloud is minimized efficiently. For improving the data-driven decisions taken by the edge device, machine learning could be applied which improves the accuracy drastically. But, most machine learning algorithms are computationally intensive and cannot be done at the edge without the aid of external modules. This problem can be solved by the interleaving edge-cloud architecture that we propose.

In this architecture, edge and cloud act as two different modules interacting with each other. Training being the most computationally intensive task of machine learning, the model can be trained at the server with predefined data for the service. The trained parameters could be passed onto the edge device. The edge device would be responsible for data collection and taking decisions using the gathered data and the parameters obtained from the server. In order to make the model more robust and the service dynamic, the edge device would also have the role of calculating the variance of incoming real-time data. If there is considerable fluctuation in the data detected, some historical data can be passed onto the server for retraining the model. This provides for updating of the parameters that can be sent back to the edge.

This architecture distributes the tasks between the edge and the server, with computation-intensive tasks done at the server end and lighter tasks done at the edge, thereby reducing the workload on the server. The interactions between edge and server are not completely cut out, but are minimized by a large extent. Thus, network traffic is reduced and hence latency is reduced to the maximum extent. This architecture could be expected to work really well for classification problems (Fig. 4).

Table 2 summarizes the difference between the two-hybrid models on various distinguishing aspects.

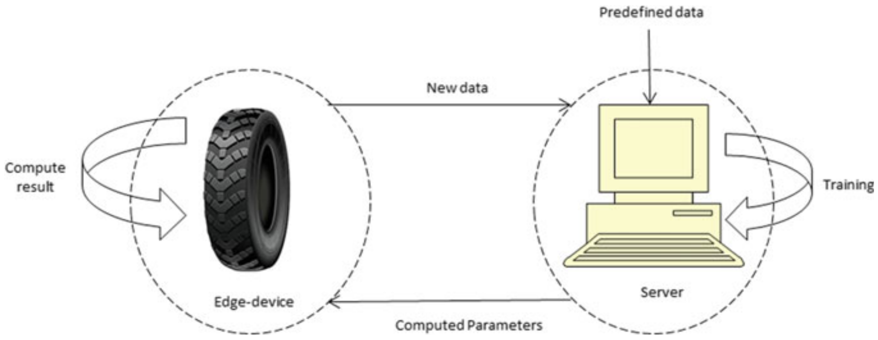


Fig. 4 Interleaving edge-cloud architecture

Table 2 Distinguishing aspects of the two-hybrid models proposed

Hybrid models	Non-interleaving	Interleaving
1. Data processing point	Depends on the service	Computation intensive—At server Lighter task—At the edge
2. Key features	• Processing happens at a single facility • Depends on criticality of service	• Interaction between edge and cloud • Task distribution based on computation intensity
3. Low bandwidth performance	Cloud: Availability is compromised Edge: Works effectively	The system should completely rely on edge until network is restored

5 Key Challenges

The hybrid computing approach, though takes the aid of both the paradigms, has issues related to integrating both the paradigms. This is because the technological advancements in the two approaches are not proportionate. Cloud computing has been researched for a long time and a lot of progress has been made, whereas edge computing is relatively new and still under exploration. For the best results from the hybrid approach, substantial advancements must be done in the areas of edge computing.

Further, in the interleaving edge-cloud hybrid model, since there is communication between the edge and the cloud, network connectivity affects the system. The communication will be disrupted under low bandwidth conditions and the processing can take place only on the edge.

6 Conclusion

The transportation industry is largely dependent on the tire manufacturing sectors. The progress toward intelligent tires gives a total new dimension for smart transportation. With autonomous transportation under huge research and development, the prime focus should be on to reduce the latency in decision-making and communication. A pure cloud computing or a pure edge computing approach, both have its own merits and demerits. Thus, the hybrid approach discussed in the paper throws light on exploiting the better of the existing two approaches and working toward the synchronization of working between the two approaches.

References

1. Tyre industry going IoT, https://rainrfid.org/wp-content/uploads/2017/10/9-Voyantic_Partanen_RAIN_Tire_Industry_Going_IoT_PUBLIC_2017.pdf
2. Johnson S, Schmeitz A (2014) Study on some safety-related aspects of tyre use, 10–22, May 27, 2014. https://ec.europa.eu/transport/road_safety/sites/roadsafety/files/pdf/tyre10062014/discussion_document.pdf
3. ContiConnect. Digital tyre monitoring, anytime, anywhere, https://www.continentaltyres.com/transport/tyre-monitoring/conticonnect
4. Reinventing the wheel: why smart tyres give the IoT real grip, https://internetofbusiness.com/reinventing-the-wheel-smart-tyres-and-the-iot
5. Atlam HF, Alenezi A, Alharthi A, Walters RJ, Wills GB (2017) Integration of cloud computing with internet of things: challenges and open issues. In: 2017 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData), Exeter, pp 670–675
6. Cloud, edge or hybrid IoT solutions: which computing model is best suited for your IoT application?, https://www.embitel.com/blog/embedded-blog/cloud-edge-or-hybrid-iot-solutions-which-computing-model-is-best-suited-for-your-iot-application
7. Hassan N, Gillani S, Ahmed E, Yaqoob I, Imran M (2018) The role of edge computing in internet of things. In: IEEE communications magazine, vol 56, no 11, pp 110–115, Nov 2018
8. Bermbach D et al (2018) A research perspective on fog computing. In: Braubach L et al (eds) Service-oriented computing—ICSOC 2017 workshops. Lecture notes in computer science, vol 10797. Springer, Cham
9. A guide to edge IoT analytics, https://www.ibm.com/blogs/internet-of-things/edge-iot-analytics/
10. Moor insights and strategy: IOT analytics at the edge, Aug 2016. http://www.moorinsightsstrategy.com/wp-content/uploads/2016/08/IoT-Analytics-at-the-Edge-by-Moor-Insights-and-Strategy.pdf

A Low-Cost Ideal Fish Farm Using IoT: In the Context of Bangladesh Aquaculture System

Md. Kalim Amzad Chy, Abdul Kadar Muhammad Masum, Mohammad Emdad Hossain, Md. Golam Rabiul Alam, Shahidul Islam Khan and Mohammed Shamsul Alam

Abstract This paper presents an IoT-based low-cost aquaculture system for automatic monitoring of fish firms to increase the production of fishes in order to meet the protein demand. A microcontroller is employed in measuring several essential parameters of the water like pH, temperature, water level, oil layer, and to monitor the fish behavior to understand their hunger level that is directly affect in the growth of firm fishes. A mobile application and an interactive Web interface are designed to notify the measured parameters value and necessary recommendation. Bluetooth and ESP8266 Wi-Fi module are integrated with the system to deliver the data to the mobile app and Web interface. In case of any abnormality, the system informs the concerned authority to take the immediate steps. In addition, the forecasting of the several water parameters in the following day to take an earlier preventive action makes the proposed framework more exceptional. Therefore, the system will assist the fish farmer to enhance the production of quality fishes, which may help to meet the protein challenges for the large population.

Md. Kalim Amzad Chy · A. K. M. Masum (✉) · S. I. Khan · M. S. Alam
Department of Computer Science and Engineering, International Islamic University Chittagong, Chittagong, Bangladesh
e-mail: akmmasum@yahoo.com

Md. Kalim Amzad Chy
e-mail: kalim.amzad.chy@gmail.com

S. I. Khan
e-mail: nayeemkh@yahoo.com

M. S. Alam
e-mail: alam_cse@yahoo.com

M. E. Hossain
Department of Business Administration, International Islamic University Chittagong, Chittagong, Bangladesh
e-mail: mehapstat@gmail.com

Md. Golam Rabiul Alam
Department of Computer Science and Engineering, BRAC University, Dhaka, Bangladesh
e-mail: rabiul.alam@bracu.ac.bd

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_125

Keywords Smart fish farm · pH sensor · Oil layer detection · Support vector regression (SVR) · Random forest regression

1 Introduction

Ocean is a great source of protein. So, we are increasing stress on the ocean that creates natural imbalance. To meet the protein demand, alternate sources should be explored. Aquaculture-based fish farming is one of the solutions to this crucial problem. Fish farming is very cheap as only 1.5 lb feed is needed to produce 1 lb fish while in case of meat from cow its 8–9 lb feed and 8000 L water [1]. In respect to financial gain, a significant difference between Internet of things (IoT)-based fish farm and non IoT-based fish farm has been found in earlier research [2].

The primary objective of this work is to develop a low-cost smart fish monitoring and controlling system that can measure different important water characteristics like pH, temperature, oil level, water level, and fish hungry level by observing the fish behavior. Several low-cost sensors are equipped with the system to accomplish the assigned task. To develop the system only $50–$55 is required. This amount is such a low cost that a fish farmer can easily adapt.

2 Related Work

Nowadays, IoT makes a revolutionary change in diverse fields [3]. Consequently, IoT improves the fish farming system that resolves a large portion of the nutrition problem for more growing population. Conventional fish farming faces a lot of difficulties in a change of the climate like heavy rainfall, extreme weather, limited water in a farm, and high temperature. Food and Agriculture Organization (FAO) highly recommends that modern technologies should be integrated with traditional farming to overcome the challenges. SK telecom developed an IoT-based fish farm system that observes pH, temperature, dissolved oxygen, and notifies the fish farmer in real time through their smartphones [4]. To test the water quality, the conventional method takes several samples from various locations and process in the laboratory. To smart this method, Shareef et al. [5] presented an IoT-based decisions support system using wireless sensor network (WSN) technologies that determine various physio-chemical characteristics of water and inform the end user through smart mobile. Simbeye and Yang [6] also developed a fish farm monitoring system to examine water quality based on WSN technology. Their equipped sensors collect temperature, oxygen level, pH, the water level of the fish farm, and transfer the data to the mother server via ZigBee protocol. If any water parameter exceeds its threshold level than an auto-generated message will be sent to the user. They utilized LabView software to show the gathered information. But the high cost is the main drawback of this system.

Besides, most of the work does not identify which sensors they have employed or equipped high-cost sensors that make the system tough to cope up in the fish farm [7]. Moreover, most of the system supply the fish feed after a certain period ignoring feeding when they required. Prediction of the amount of next week fish feed is missing in most of the system.

In the context of Bangladesh aquaculture system, lots of fisheries follow the traditional methods to cultivate the fish. As a result, the cost becomes high, but the output is not the expected level. To the best of our insight, this is the first attempt to develop a low-cost fish farm monitoring and understanding when fish require feed by analyzing their movement. Also, the forecasting features of the next week fish farm parameters will help the fish farmer to take a preventive step in advance.

3 Methodology

The IoT-based fisheries monitoring and controlling system are presented in Fig. 1. The figure depicts how the fisheries information will be gathered and transferred to the end users of the system. The system estimates several parameters of the water like pH, temperature, oil layer, water level, and the movement of the fish that directly affect on the quick growth of a fish. Firstly, to measure the targeted water parameters and fish movement, the system takes a few moments to initialize the equipped sensor. As pH sensor does not give a proper reading at a static situation, it needs to shake slightly to measure the pH of the water appropriately. The system uses a servo motor to perform this task that rotates the pH sensor 30° in one direction and 30° in reverse direction. For more accuracy and lower the amount of power consumption of the system, it takes an average of five pH value where each value is read in every 3 min. By using Eq. 1, this average value is calculated where P is the value of pH in every 3 min and pH is the desired result.

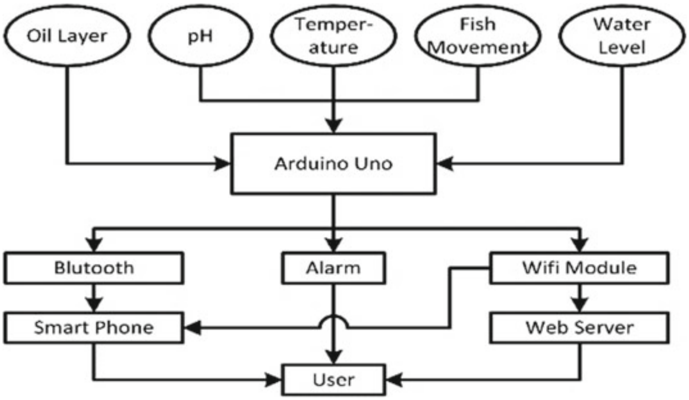


Fig. 1 Block diagram of IoT-based aquaculture system

$$\mathrm{pH} = \left(\sum_{i=1}^{5} P_i\right)/5 \tag{1}$$

IR optical sensor measures the density of the oil layer and stores the data in memory. For pH value measuring, the value of the oil layer is calculated using Eq. 2, where D is the value of the oil layer in every 3 min and Oil_layer is the ultimate result.

$$\mathrm{Oil\_layer} = \left(\sum_{i=1}^{5} D_i\right)/5 \tag{2}$$

Usually in a fishery, after a certain period, fish food is supplied to the fishes. The system can determine either the fishes are extreme hungry or medium hungry or not so that enough fish food is supplied. The abnormal movement, i.e., not a frequent movement of the fish can help us to understand the fish hunger level. Three ultrasonic sensors (a, b, c) are deployed in this purpose where each ultrasonic sensor takes six values after every 10 s. For each sensor, the average value is calculated using Eqs. 3, 4, and 5 where a is a location of a fish measured by sensor a and b and c are like a. Then, RMS value is calculated for each sensor using Eqs. 6, 7, and 8. a_rms is measured RMS value by sensor a and b_rms and c_rms are like a_rms. From these three RMS value of the sensor, we can determine the hungry level easily. If three RMS value exceeds the threshold value, then the hungry level is extreme, if two values exceed then medium hungry level, if one value exceeds then normal hungry level.

$$a = [a_1, a_2, \ldots a_6] \quad b = [b_1, b_2, \ldots b_6] \quad c = [c_1, c_2, \ldots c_6]$$

$$\mathrm{a\_avg} = \left(\sum_{i=1}^{6} a_i\right)/6 \tag{3}$$

$$\mathrm{b\_avg} = \left(\sum_{i=1}^{6} b_i\right)/6 \tag{4}$$

$$\mathrm{c\_avg} = \left(\sum_{i=1}^{6} c_i\right)/6 \tag{5}$$

$$\mathrm{a\_rms} = \sqrt{(a_1 - \mathrm{a\_avg})^2 + \cdots + (a_6 - \mathrm{a\_avg})^2} \tag{6}$$

$$\mathrm{b\_rms} = \sqrt{(b_1 - \mathrm{b\_avg})^2 + \cdots + (b_6 - \mathrm{b\_avg})^2} \tag{7}$$

$$\mathrm{c\_rms} = \sqrt{(c_1 - \mathrm{c\_avg})^2 + \cdots + (c_6 - \mathrm{c\_avg})^2} \tag{8}$$

Too hot and too cold temperature is a great reason of the slow growth of a fish. The system gets the current temperature of fisheries through temperature sensor. In similar to pH and oil_layer value measuring, the system measures the temperature of the fishery using Eq. 9 where T is the temperature in every 3 min and temperature is the estimated value.

$$\text{Temperature} = \left(\sum_{i=1}^{5} T_i\right)/5 \tag{9}$$

Similarly, too high and low water level is not suitable for the fishes. A liquid level sensor can measure the water level but costly. To make the system more cost-effective, a low-cost ultrasonic sensor is equipped to measure the water level. In Eq. 10, W is the water level in every 3 min and water_level is the outcome of the right-hand side calculations

$$\text{Water\_level} = \left(\sum_{i=1}^{5} W_i\right)/5 \tag{10}$$

Through two communication medium, the microcontroller sends the gathered data to the end user. A mobile application and Web interface are integrated with the system to operate it easily. Bluetooth module sends the data in a mobile app so that local fishery supervisor can easily gain the necessary information. ESP8266 Wi-Fi module sends the data to the Web interface so that one can monitor the fishery remotely. In the Web interface, the data is plotted graphically and stored in the database that will help the supervisor of the fishery to check the previous data when necessary.

3.1 Circuit Design and Softwares

The proposed system is developed by following the designed circuit. The ground and VCC pin of every sensor are connected to the ground and 5 V pin of Arduino Uno. The pH sensor relates to the analog pin of Arduino. From the analog output of the pH sensor, the value of pH is calculated using the formula of pH calculation. Servo motor, buzzer, temperature sensor, IR optical sensor, ultrasonic sensor, Bluetooth module, and Wi-Fi module is connected to the Arduino UNO microcontroller board according to the developed circuit diagram. Arduino IDE and language is used to write the code and burnt into the system that is easy to understand and reliable.

3.2 Algorithm

The entire flowchart of an IoT-based ideal fishery system appears in Fig. 2. Primarily, all sensor values are initialized. To measure the pH value, servo motor rotates 30° left and 30° right as pH sensor needs to shake for proper value. By using pH formula, pH is determined 5 times in every 3 min. Average of the pH value is calculated for 15 min duration. As optimal pH value for speedy growth of fishes is 7–8.5, the system turns on the alarm if it exceeds this range [8]. IR optical sensor engages to measure the oil layer of the water. By removing the heat and noise value form the entire value received from IR optical sensor, the system gets the actual value. If the oil layer value less than 500 than pH sensor notifies the user and turns on the alarm. To estimate the fish moving rate, every 10 s is taken in 1 min duration. 4.5 cm RMS value of the sensor act as a threshold value to determine the hungry level of the fishes. Average value of the water level and temperature within 15 min is calculated like the pH sensor. [9] says that 22–27 °C is the optimum temperature for the rapid growth

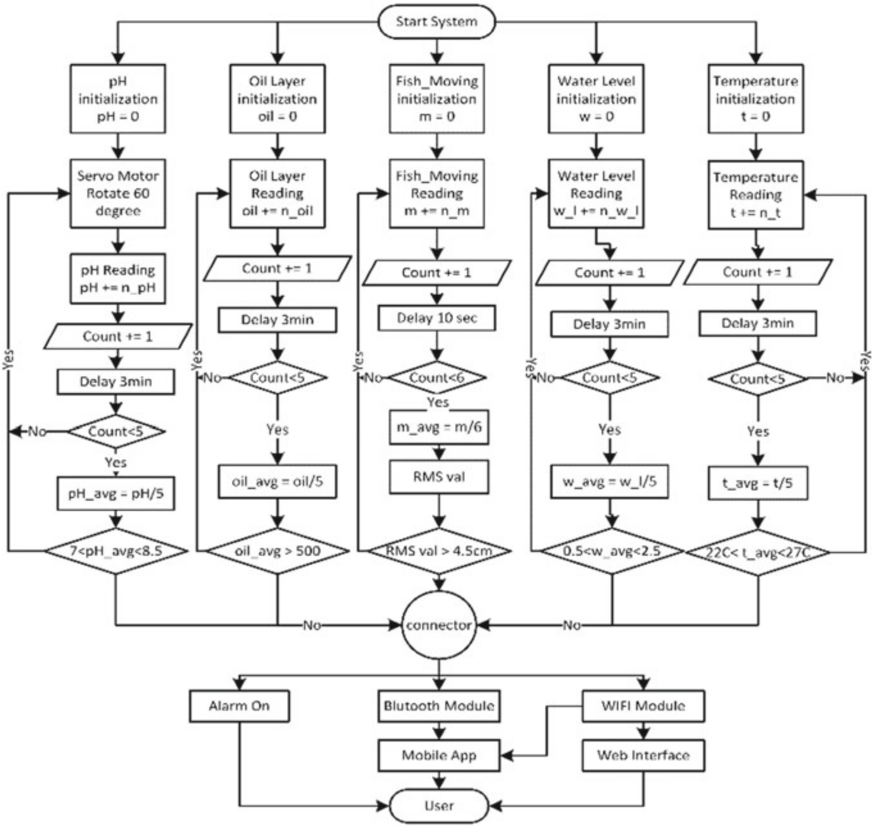


Fig. 2 Working process of the proposed system

of the fish. So, in case of exceeding this range, the system informs the owner of the fishery through mobile app and Web interface. The flow of the data from the device to the mobile app and Web is performed through the Bluetooth and Wi-Fi module.

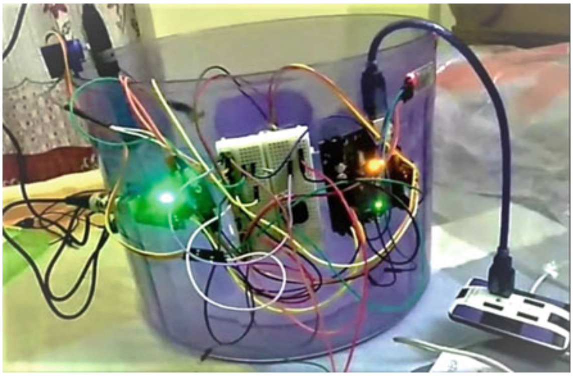
3.3 Predicting the Following Day Fish Feed Consumption

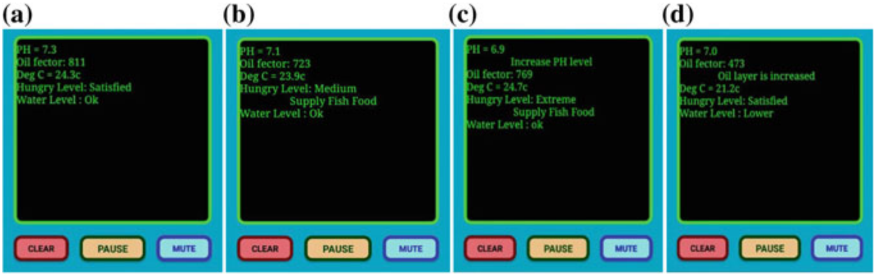
The system can forecast the various essential parameters and notifies the user. For simplicity, here, we have considered just forecasting of the probably required fish feed in next day. The system can predict other parameters. We have recorded about 200-day data of fish feed and used the data to train our model. Dataset is split into 70% and 30% where 70% data is for training and 30% data is reserved for testing the model. Through different kinds of machine learning regression algorithms such as linear regression (LR), decision tree regression (DTR), polynomial regression (PR), support vector regression (SVR), and random forest regression (RFR), we fit the training data to prepare the model to forecast the amount of the fish feed in the following day. After finishing the model training part with training data, the model is examined by testing data. Then, the mean absolute error and accuracy level are calculated to evaluate the model. From these results, we have found RFR gives better outcomes than other regression models.

4 Experimental Results and Discussion

A prototype of the proposed system is shown in Fig. 3. The pH, temperature, oil layer, water level, and fish hungry level are the outcomes of the system. The essential parameters of the water are sent to the mobile app through Bluetooth module for local user, and data is sent to the Web server through the ESP8266 Wi-Fi module for the remote user. Also, data is saved to the cloud storage for further analytics.

Fig. 3 Photograph of the prototype





(a)

PH = 7.3
Oil fector: 811
Deg C = 24.3c
Hungry Level: Satisfied
Water Level : Ok

(b)

PH = 7.1
Oil fector: 723
Deg C = 23.9c
Hungry Level: Medium
Supply Fish Food
Water Level : Ok

(c)

PH = 6.9
Increase PH level
Oil fector: 769
Deg C = 24.7c
Hungry Level: Extreme
Supply Fish Food
Water Level : ok

(d)

PH = 7.0
Oil fector: 473
Oil layer is increased
Deg C = 21.2c
Hungry Level: Satisfied
Water Level : Lower

Fig. 4 **a** A sample of everything ok, **b** an example of fish hungry notification, **c** a sample of pH and hungry level notification, **d** an example of oil layer notification

In Fig. 4, some sample outcomes of the system taken at different time and different situation. In Fig. 4a, all parameter is ok while at the time of medium hungry level the system notifies it successfully (Fig. 4b) and inform the user. In case of pH level decreasing the system informs the user, shown in Fig. 4c while in the oil layer exceeding the threshold value case the system successfully determines the situation (Fig. 4d).

In the Web interface, the system sent the measured data and visualized it graphically to make it more interactive with the user. In Fig. 5, the system visualizes the pH data over time and store it into the server for further analytics. Like the pH data visualization, the system also visualizes the temperature data (Fig. 6), oil layer data (Fig. 7), and water level data (Fig. 8) graphically into the Web interface for the remote user.

Some forecasted data are displayed in Table 1 where the first column "Date Test" refers to the forecast of the power consumption of that date. "MonthDate" format is used to represent a date where the last two digits refer to data and remainder value to month. For example, "218" implies second-month 18th day, "717" implies seventh–month 17th day, and so forth.

Accuracy level and mean absolute error are considered to judge the model that is shown in Tables 2 and 3, respectively. Shifting the degree of PR analysis provides

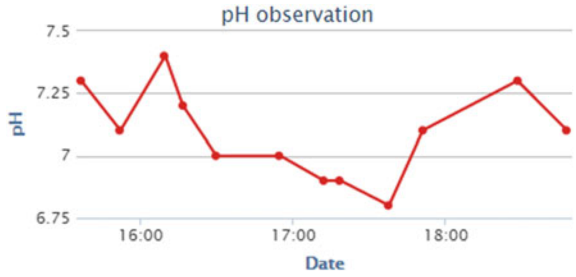


Fig. 5 pH observation

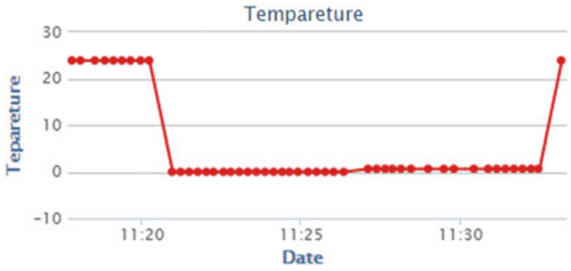


Fig. 6 Temperature observation

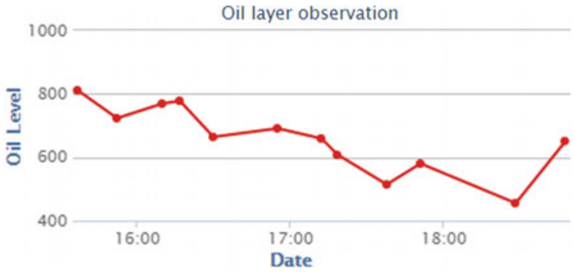


Fig. 7 Oil layer observation

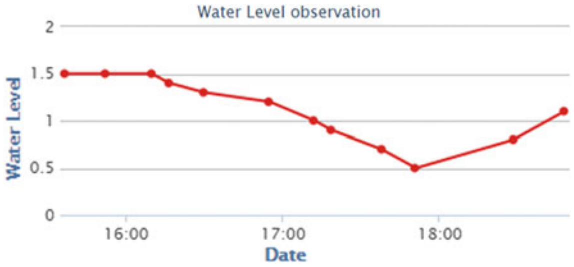


Fig. 8 Water level observation

Table 1 Testing data

Date test	Fish feed (g)	LR	PR	SVR	DTR	RFR
113	10096.59	10101.15	10101.31	10294.05	10602.16	10524.65
218	10173.3	10176.01	10178.49	10294.79	10693.29	10418.38
303	10235.84	10236.61	10237.68	10294.44	10732.53	10593.94
515	10394.56	10387.76	10383.78	10295.23	10561.82	10582.49
717	10572.98	10531.77	10539.52	10295.58	10732.19	10689.75

Table 2 Accuracy comparison

Accuracy	LR	PR	SVR	DTR	RFR
Training set	85.45	85.49	87.49	92.09	95.75
Testing set	84.76	84.85	86.05	90.94	94.24

Table 3 Output observations

Evolution of the linear model		LR	PR	SVR	DTR	RFR
Mean absolute error	Training set	44.2489	44.2063	29.2189	26.3687	23.0747
	Testing set	43.6042	43.2575	35.5301	30.2692	23.8518

a good result than LR. RFR gives a better result than DTR and other models. So, it can be decided that the RFR-based model is more suitable to forecast the water parameters.

5 Conclusion

The traditional fish cultivation method fails to meet the demand of protein because of the lacking in real-time monitoring the adverse aqua environment of fishes. The proposed framework is more cost-efficient and smarter than existing traditional and smart systems. The design and development of low-cost autonomous and smart fishery monitoring system while integrating state-of-the-art sensors and technologies to determine ideal environment for aquaculture is our future research direction. The integration of the proposed IoT-based smart fishery monitoring system assists fish farming to increase the fish production.

Acknowledgements All author states that there is no conflict of interest. No animals (fishes) and humans are not involved in this work.

References

1. Ruan J, Wang Y, Chan FTS, Hu X, Zhao M, Zhu F et al (2019) A life cycle framework of green IoT-based agriculture and its finance, operation, and management issues. IEEE Commun Mag 57:90–96
2. Zhang Y, Hua J, Wang YB (2013) Application effect of aquaculture IOT system. In: Applied mechanics and materials, pp 1395–1401
3. Vernandhes W, Salahuddin NS, Kowanda A, Sari SP (2017) Smart aquaponic with monitoring and control system based on IoT. In: 2017 second international conference on informatics and computing (ICIC), pp 1–6
4. Sharma R (2014) SK telecom starts pilot operation of IoT-based fish farm management system. Available: http://en.c114.com.cn/576/a855896.html

5. Shareef Z, Reddy SRN, Delhi IGDTUW (2016) Design and development of IOT based framework for aquaculture. In: National conference on product design (NCPD 2016)
6. Simbeye DS, Yang SF (2014) Water quality monitoring and control for aquaculture based on wireless sensor networks. J Netw 9:840
7. Beardmore JA, Porte J (2003) Genetically modified organisms in aquaculture
8. Y. E. Corporation (2016) pH in fish farming. Available: https://www.yokogawa.com/library/resources/application-notes/ph-in-fish-farming/
9. Hobbyist TF (2019) Temperature control. Available: http://www.tfhmagazine.com/aquarium-basics/temperature-control.htm

IoT-Based Smart Monitoring System to Ensure Worksite Safety—A Context of Garment Industry in Bangladesh

Abdul Kadar Muhammad Masum, Ahmed Shan-A-Alahi, Abdullah Al Noman, Mohammad Nazim Uddin, Khairul Islam Azam and Mohammed Golam Sarwar Rakib

Abstract In this paper, we have proposed and designed a hybrid system that is able to detect fire breakout, gas leakage and noise pollution as well as providing location of the affected area and opening fire extinguish system. Raspberry Pi is integrated with MQ-5 sensor, humidity sensor, flame sensor, sound sensor and camera module. A 360° servo motor is accumulated with camera module to capture affected location even at any angle. To increase the reliability of this system, an authorized person is assigned to assess the real situation. If fire is detected, camera module takes a snapshot of affected region and sends it to admin's email through 802.11n LAN wireless module. Different sensors' value also transmits to server through that module in one-minute interval. Moreover, a buzzer is activated in control room when data and picture is sent to admin. If admin confirms the incident, the system will raise the alarm in whole workplace, uncover the water valve of affected region and send message to the owner and nearby fire brigade. Thus, a garment can secure the workplace for its workers.

Keywords Raspberry pi · Sound intensity · Fire detection · Garment industry

A. K. M. Masum (✉) · A. Shan-A-Alahi · A. Al Noman · M. N. Uddin · K. I. Azam ·
M. G. S. Rakib
Department of Computer Science and Engineering, International Islamic University Chittagong,
Chittagong, Bangladesh
e-mail: akmmasum@yahoo.com

A. Al Noman
e-mail: alnomancse143@gmail.com

M. N. Uddin
e-mail: nazimuddinasifiiuc@gmail.com

K. I. Azam
e-mail: khairulislam.azam@gmail.com

M. G. S. Rakib
e-mail: rakibsarwar3@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_126

1 Introduction

In Bangladesh economy, ready-made garments (RMG) industry has acquired a substantial facet in comparison with any other sectors for foreign exchange earnings and growth. According to the world trade organization (WTO), Bangladesh is the second-largest apparel supplier that holds 6.5% market share in the world in 2017 [1]. In every year, nearly about $5 billion earned from this sector which is around two-third of total exports. Around 2,500 garment factories are in Bangladesh, on which ten million livelihoods are indirectly or directly depend on it [2]. This sector also participates significant contribution in exporting which is almost 80% of total export of country [3]. Unfortunately, nowadays, this sector is under threat because of security risk of garment factories.

The best precedent is Tazreen Garment's fire, which is the deadliest fire incident in the country's history. It was November 24, 2012, a tragic fire incident was experienced by Tazreen Garment's Factory, where 117 people were dead [4]. On December 14, 2010, in Ashulia, Dhaka, "That's It Sportswear Ltd" garment factory was affected by fire where at least 28 more people had died, and also huge number of workers was grimly injured. Again at the "Garib and Garib" factory, situated at Dhaka, 21 peoples lost their lives in the deadly fire broke out [5]. In garment industry, the pollution level is increased along with the advent of the technology. There are many reasons for pollution: intense sound, temperature and humidity. It can cause hearing problem, heat illness, fatigue, heatstroke and cold-related medical conditions. So, we need to maintain a reasonable range of sound, temperature and humidity to control the pollution level. Consequently, worker feels less comfort to work. Therefore, these terrible incidents demonstrate that an early warning system is crying need to handle the risky situation in the garment factory.

Our proposed system is assuring the early warning in a factory's workplace. In this system, we used an intelligent algorithm to decide when to warn for fire breakout and gas leakage. If fire breakout and gas leakage are detected via flame and gas sensor, then their value sends to the controller office with snapshot of affected region and activates the buzzer in the office. The camera module is placed in the middle of the workplace and positioned at zero degree. If an incident is occurred, the system will start firing suppression system using uncovered water valve and also stop electricity and gas supplies. At the same time, GSM module sends the SMS to the owner and nearby fire service station for informing this incident. The system also collects the noise level using sound sensor and temperature and humidity level using humidity sensor to make the workplace comfortable for the workers. The main aim of this paper is to develop IoT-based smart early warning system in workplace. To the best of our knowledge, smart warning system in workplace is not implemented in Bangladesh yet. Moreover, operating the proposed system is more comfortable than other existing related systems.

2 Literature Review

The garment industry of Bangladesh is the largest manufacture sector which has a great impact on the socio-economic development of Bangladesh. Unfortunately, different types of sufferings in the workplace of factories are incredibly increasing nowadays that badly effects on this sector. At least 1,601 workers died in garment factories in last 2005–2016 where 280 workers in fire breakout, 1,221 in building collapse and 100 in gas leakage [6]. So, a smart warning system is essential to save valuable lives and growth of this sector.

Imteaj et al. [7] implemented a system for fire detection in workhouse using Raspberry Pi 3. They used gas and light intensity sensor to sense any indicators of fire and gas leakage. The system can extinguish fire breakout using water valves and can notify by SMS with location. But, they did not work on noise level also did not explain how to extinguish fire breakout. Moreover, Fuzi et al. [8] used Zigbee wireless module to sense signs of fire. The system composed of temperature sensor, Arduino Uno microcontroller, buzzer and operating software. To detect fire, they used only temperature sensor. Similarly, Islam et al. [9] also used Zigbee and localization technique to find the distance and position of fire which is cost expensive. Again, Sowah et al. [10] developed a system to sense fire using fuzzy logic in vehicle. They can put out fire breakout using air-conditioning system of vehicle.

For alerting an fire occurrence in any industrial premises, Sathishkumar [11] worked on automated fire voice alert system. They used automatic voice recorder to extinguish fire and GSM inside the system to send up-to-date information of surrounding area to the company's IP. The Yu et al. [12] proposed video processing based on fire alarming system. To detect the possible fire breakout, they adopted smoke color and its spreading features. But, detection of fire via video processing is time consuming.

So, our motive is to design an intelligent and early warning system to detect the fire breakout, gas leakage and noise pollution in the worksite which has to overcome the defect observed in the earlier system.

3 System Description

3.1 System Architecture

The system we designed consists of IoT and wireless technology that equipped in a room to monitor symptom of fire, gas leakage and noise pollution. We use Raspberry Pi 3 as our main device and use a series of sensors and module which are flame sensors, gas sensors, sound sensors, humidity sensors, servo motor, GSM module, camera module, two-channel relay module and water valve. The flame sensor can detect the fire in particular place. The existence of gas is detected by gas sensor. The camera module is used for taking the snap of affected area with the help of servo motor. The sound sensor is used to detect the noise level of industry. The output of the flame sensor, gas sensor and sound sensor is a digital value. We use a converter to get the analog value from flame, gas and sound sensor.

Data transmits from sensors to cloud server and picture sends to email through 802.11n LAN wireless module which is built in Raspberry Pi 3. When the certain condition is true, then the relay module activates the alarm and uncovers the water valve. At the same time, GSM module notifies owner and nearby fire station by sending SMS after admin confirmation. To measure the level of noise pollution, we use sound sensor. Humidity sensor is used for measuring temperature and humidity of workplace. By these sensors, we can see the situation of pollution level by cloud. In the flow chart, flame sensor is denoted as F, and Gas sensor is denoted as G. To detect the fire breakout and gas leakage, we used four pairs of flame and gas sensors and also used a camera module which is embedded with servo motor for rotating 360°. Camera module is placed in the middle of the room. Initially, we set the direction of the camera module at 0°. If the value of F1 and G1 is true, then the camera rotates 45° angle with the help of servo motor and takes a snap of the first quadrant. Similarly, it rotates 135°, 225° and 315° angles for second, third and fourth quadrant, respectively, for taking a snap of these quadrant.

3.2 Blog Diagram and Flow Chart

After giving power supply, the Raspberry Pi 3 gets power, and the input–output port gets ready as shown in Fig. 1. Flame sensor, gas sensor, sound sensor and humidity sensor transmit data to Raspberry Pi 3, and camera module also sends snap through it. Raspberry Pi 3 used it's built in 802.11n LAN wireless module for sending data and snapshot to the admin. When certain condition is satisfied, then buzzer is activated, and GSM module is used for sending SMS to owner and fire service. The implementation of our proposed system is followed by this flow chart which is shown in Fig. 2, and circuit diagram is shown in Fig. 3.

3.3 System Implementation

The code for total device is written in Python. Python program checked every part individually and set threshold value for flame sensor and MQ-5 sensor. If the threshold exceeded, then Raspberry Pi Infrared Camera Module takes snap of this. A sim is placed in GSM to communicate with administration and send location of specific affected area.

Each sensor is connected to Raspberry Pi 3. Where, Flame and MQ-5 sensors have four pins. We used ADS 1115 16-Bit I2C ADC module to get the analog value from sensors. The signal pin of flame is connected with ADC module pin A1, and MQ-5 is connected with ADC module pin A2. SCL and SDA pin of ADC module

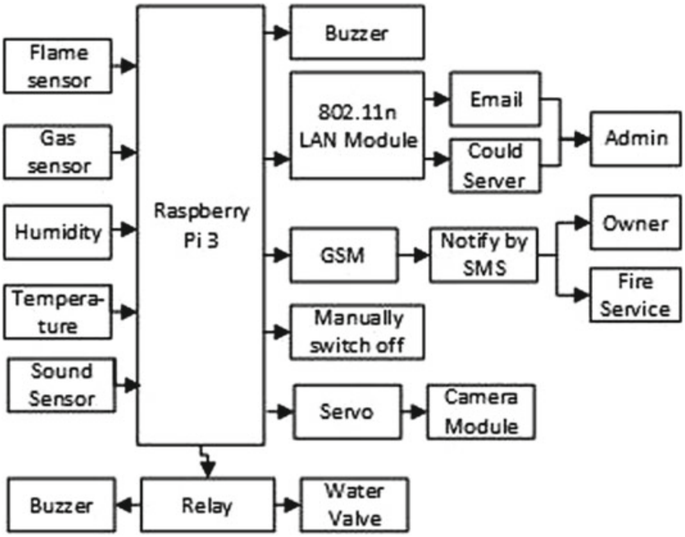


Fig. 1 Block diagram of the proposed systems

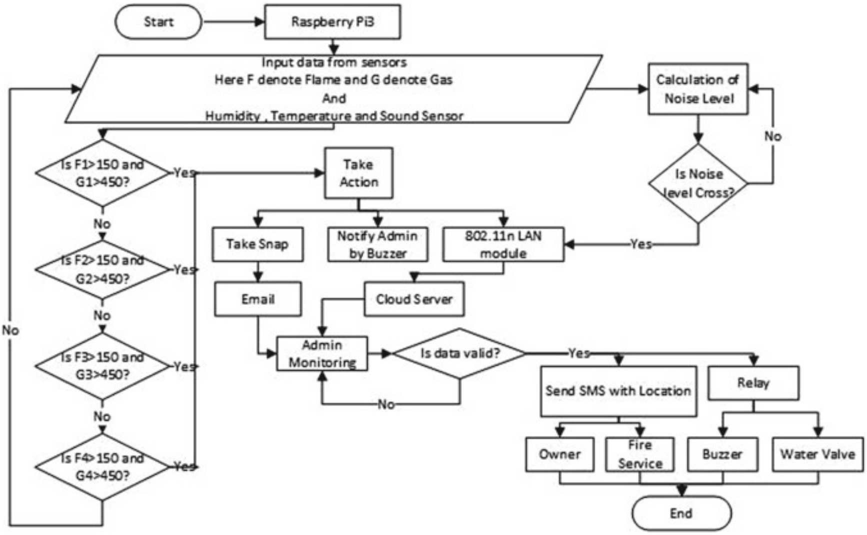


Fig. 2 Flowchart of the designed system

is connected to GPIO2 and GPIO3 of Raspberry Pi 3. DHT11 and RKI-3103 sound sensor has three pins. Where, signal pin of RKI-3103 sound sensor is connected with ADC module pin A0. Signal pin of DHT11 is connected with GPIO18 pin of Raspberry Pi 3. VCC and GND pins of all sensors are connected with 5 V and GND of Raspberry Pi 3. The servo motor and relay module have digital pin. Signal pin

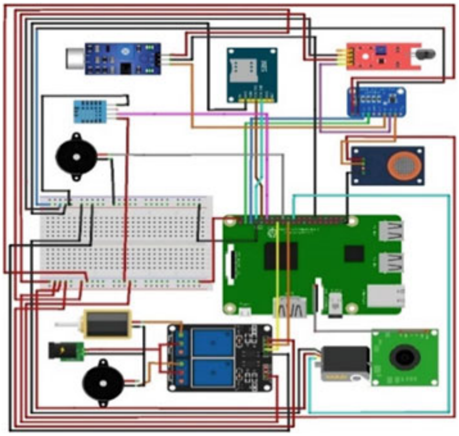


Fig. 3 Circuit diagram

of relay is directly connected with pin GPIO22 and GPIO10 of Raspberry Pi 3. The signal pin of servo motor is connected with GPIO25 pin of Raspberry Pi 3. VCC and GND pin is connected with 5 V and GND of Raspberry Pi 3 in both sensors. The ribbon of camera module is connected to Raspberry Pi 3's CSI camera port.

Then, we enable the camera module by raspi-config. A Python script is written to take snap when flame and gas are detected. A servo motor is used to rotate the camera. The servo motor and relay module have digital pin. Signal pin of relay is directly connected with pin GPIO22 and GPIO10 of Raspberry Pi 3. The signal pin of servo motor is connected with GPIO25 pin of Raspberry Pi 3. VCC and GND pin is connected with 5 V and GND of Raspberry Pi 3 in both sensors. We use SIM800 GSM/GPRS to send SMS. Where RX pin of SIM800 is connected to GPIO14 TX pin, and TX pin of SIM800 is connected to GPIO15 RX pin of Raspberry Pi 3. The ground pin of SIM800 and Raspberry Pi 3 is connected to each other. In our system, the Raspberry Pi 3 is connected with an external 5000 mAh power bank. A 2 A power supply adapter is used to operate SIM800 GSM/GPRS.

4 Experiments and Results

Flame sensor, gas sensor, camera module, sound and humidity sensor based on a smart warning system can measure symptom of fire breakout, gas leakage, pollution of noise, humidity and temperature level of workplace. The camera module takes the snap after satisfying required value of flame and gas sensor. A prototype of our proposed system is shown in Fig. 4. Humidity, sound, flame and gas sensor send data to the server through 802.11n LAN wireless module which has built in Raspberry Pi. At the server, the gas and flame sensors' data are presented graphically in Figs. 5 and 6. Representation of noise level and temperature level is shown in Figs. 7 and 8. Camera module sends the snapshot of affected area through this module in admin's

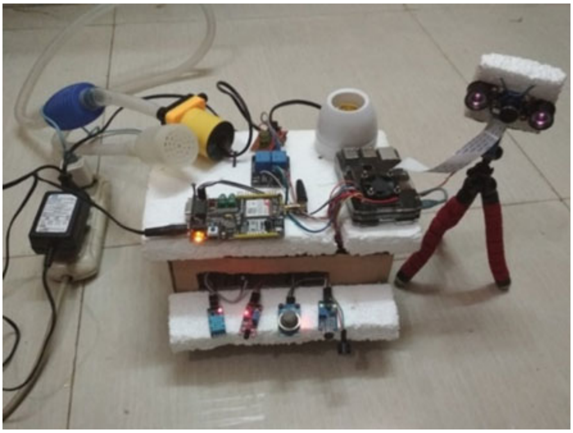


Fig. 4 Prototype of our proposed system

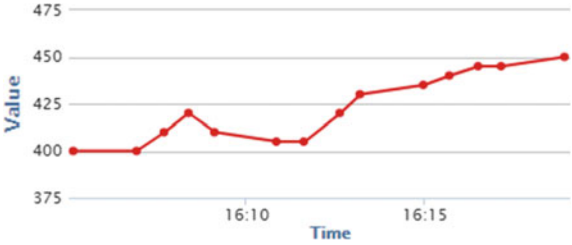


Fig. 5 Gas sensor's data representation

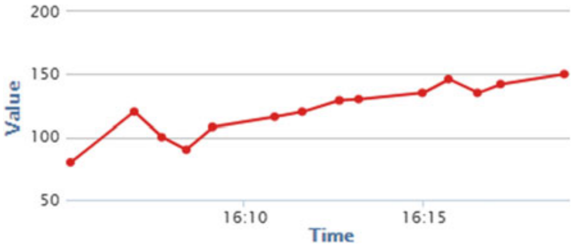


Fig. 6 Flame sensor's data representation

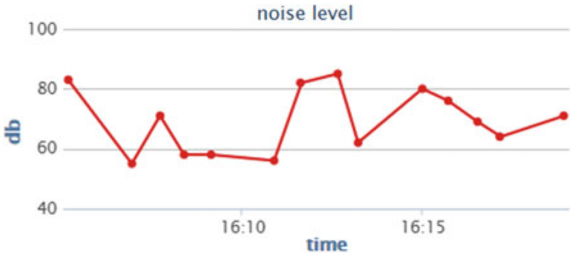


Fig. 7 Representation of noise level

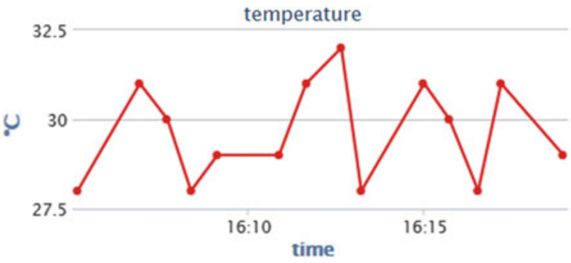
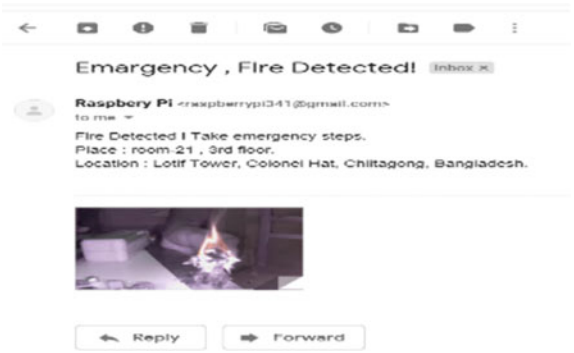


Fig. 8 Temperature representation

email as shown in Fig. 9. Controller office checked it and activated the buzzer alarm, uncovered the water valve and shut off the power circuit if data is exceeded. The system also sends SMS to owner and nearest fire service station as shown in Fig. 10.

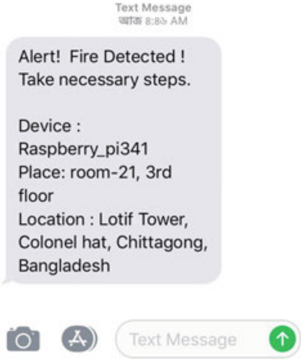


Emargency , Fire Detected!

Raspbery Pi <raspberrypi341@gmail.com>
to me

Fire Detected ! Take emergency steps.
Place : room-21 , 3rd floor.
Location : Lotif Tower, Colonel Hat, Chittagong, Bangladesh.

Fig. 9 Email from Raspberry Pi



Text Message
আজ 8:৪৬ AM

Alert! Fire Detected !
Take necessary steps.

Device :
Raspberry_pi341
Place: room-21, 3rd floor
Location : Lotif Tower, Colonel hat, Chittagong, Bangladesh

Fig. 10 SMS alert

5 Conclusion

To provide the safety of workstation, traditional system is not sufficient and also has many limitations. This paper designed a smart warning system to monitor workstation efficiently and effectively. By investigating sensor data, our system gives the authentication of incident and warns at real time. Cloud server is used for presenting sensor data graphically and storing purpose. This is a remarkable idea in context of developing nations, particularly Bangladesh. The entire framework is cost effective than existing system. If our designed system can be successfully implemented in every factory, then it is expected that the damage of life and wealth because of the fire and gas accidents and noise pollution will minimize remarkably, and the nation's economy won't be faltered by such heartbreaking accidents. When data gets massive, some features like Hadoop HDFS, MapReduce are initiated to handle big data. So, our proposed system should integrate into every factory to change the current terrible situation of the workstation of Bangladesh.

References

1. Bhuiyan MSA (2019) Sustainable economic growth: a challenge to embrace for Bangladesh. Glob J Hum-Soc Sci Res 4(2):34–39
2. Islam S, Roman RI (2019) Assessment of fire hazard on the readymade garment industry in Chittagong City, Bangladesh. Indonesian J Environ Manage Sustain 3(4):20–28
3. Rahman MA (2015) Impact of garments industry in Bangladesh economy, Aug 20, 2015. Available: http://dspace.ewubd.edu/handle/123456789/1651
4. Dhaka Bangladesh clothes factory fire kills more than 100, Nov 25, 2012. Available: https://www.bbc.com/news/world-asia-20482273
5. At least 28 more garment workers die in Bangladeshi factory fire, Apr 4, 2013. Available: https://cleanclothes.org/news/2010/12/14/at-least-28-more-garment-workers-die-in-bangladeshi-factory-fire
6. Alamgir F, Banerjee SB (2019) Contested compliance regimes in global production networks: insights from the Bangladesh garment industry. Hum Relat 72(2):272–297
7. Imteaj A, Rahman T, Hossain MK, Alam MS, Rahat SA (2017) An IoT based fire alarming and authentication system for workhouse using Raspberry Pi 3. In: 2017 international conference on electrical, computer and communication engineering (ECCE), pp 899–904
8. Fuzi MFM, Ibrahim AF, Ismail MH, Ab Halim NS (2014) HOME FADS: a dedicated fire alert detection system using ZigBee wireless network. In: 2014 IEEE 5th control and system graduate research colloquium, pp 53–58
9. Islam T, Rahman HA, Syrus MA (2015) Fire detection system with indoor localization using ZigBee based wireless sensor network. In: 2015 international conference on informatics, electronics & vision (ICIEV), pp 1–6
10. Sowah R, Ampadu KO, Ofoli A, Koumadi K, Mills GA, Nortey J (2016) Design and implementation of a fire detection and control system for automobiles using fuzzy logic. In: 2016 IEEE industry applications society annual meeting, pp 1–8
11. Sathishkumar R (2016) Design and development of automatic fire detection using sms and voice alert system. Int J Sci Eng Res 7:114–117
12. Yu L, Wang N, Meng X (2005) Real-time forest fire detection with wireless sensor networks. In: Proceedings 2005 international conference on wireless communications, networking and mobile computing, pp 1214–1217

Evading Gratuitous Energy Consumption Due to Activation of Superfluous Nodes in WSN

Alok Misra and Divakar Singh Yadav

Abstract In the recent period, wireless sensor networks are mostly used in diverse applications of sensing that includes medical, armed forces, civil, adversity management, environmental and commercial applications. Wireless sensor networks typically comprise a hefty amount of sensors. Sensors are device that produces a measurable response in changing the environmental conditions like temperature, humidity, pressure, etc. As the sensor has the limited energy, to boost the duration of network and maintaining coverage preservation, we necessitate an approach that involves least sensors in communication of sensed data to base station. In this research work, we amalgamate the conception of genetics and extended search to evade gratuitous energy consumption which is due to activation of superfluous nodes. We aim to prepare a schedule in which least number of sensors are stimulated and cover each point of concerns.

Keywords Energy-efficiency · Full coverage preservation · Network life span addition · Sensor scheduling

1 Introduction

Wireless sensor network consists of a assortment of sensor nodes and running on limited magnitude of battery power. Each sensor node of WSN can sense, process and transmit data to base station (BS). If all the packets are passed to BS straightforwardly by sensor nodes, the nodes which are far away from BS will depart untimely. Alternatively, among sensor nodes transmitting packets via a couple of hops, sensors nodes which are in close proximity to the BS are inclined to depart untimely. Thus, some areas of network become totally un-examined, and network partitions are created. Lifetime of sensor nodes is required to be extended by minimum consumption

A. Misra (✉)
Dr. A.P.J. Abdul Kalam Technical University, Lucknow, India
e-mail: alokalokmmm@gmail.com

D. S. Yadav
Institute of Engineering and Technology, Lucknow, UP, India

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_127

of power in transmission [1]. Thus, to curtail the power consumption, we aim to cover each point of concern (POC) at least by one sensor. Typically, the superfluous sensor nodes, which are chosen by scheduling policies [2–4], should be kept in sleeping mode for energy preservation. As soon as the lively node loses its entire energy, there is urgent need to wake up one or more sleeping nodes to reinstate that dying node. As a consequence, the coverage control is assured, and original coverage is preserved after switching off superfluous nodes. To discover the most optimal schedule, in which we decide which sensor to stimulate and which sensor to be deactivated, we exploit the conception of genetic algorithm.

1.1 Genetic Algorithm

In genetic algorithms, we have a set or a populace of feasible solutions to the given hitch. These solutions are then subjected to recombination and mutation (as in natural genetics). Fitness value is determined for each candidate solution, and the greater suit persons are given a larger likelihood to breed superior "vigorous" individuals. This is driven by theory of Darwinian that is "Survival of the fittest". In this way, we proceed to "evolve" with higher individuals or solutions over generations, until we attain a criterion of detention. In the genetic algorithm, we repeat selection, crossover and mutation procedure unless a pre-defined criterion is fulfilled.

1.2 Sensing Coverage Representation

Consider target area A in which set of sensor nodes is delineated as $S = \{s_1, s_2, s_3, \ldots, s_M\}$, where s_i is located at coordinates $\{a_i, b_i\}$, where i varies from 1 to M and M be the total nodes which are deployed in area A. Each sensor has sensing radius Ra.

Let P be set of POCs distributed over the area A. If N is number of POCs, then $P = \{p_1, p_2, \ldots, p_N\}$, where POC p_j is situated at $\{a_j, b_j\}$, where j varies from 1 to N. A binary coverage variable $C_{i,j}$ which signifies whether sensor s_i covers the POC p_j is delineated as follows:

$$C_{i,j} = \begin{cases} 1 \text{ if} (a_i - a_j)^2 + (b_i - b_j)^2 < \mathrm{Ra}^2 \\ 0 \qquad\qquad \text{Otherwise} \end{cases}$$

2 Literature Review

Currently, many academicians have investigated the optimization algorithm for the coverage and location of nodes in wireless sensor networks. Cardei's TianD algorithm [5], Wang's CCP algorithm [6] and Liang's Huang algorithm [7] are some effective approaches in this context.

Chen et al. [8] proposed a fusion memetic scaffold (Hy-MFCO) for optimizing coverage. From real-world experimentations and computer simulations, they produced the outcomes that specify that Hy-MFCO is proficient in maximizing detection coverage and, at the same moment, attaining energy effectiveness.

Liang et. al. [7] proposed a method that uses the adaptive group head communication method to guarantee that power burning is unprejudiced throughout the network and can perk up the network time phase. Cardei et al. [5] designed a scheme to ascertain a "maximum separation set coverage problem". In this scheme, the nodes that are incorporated in the utmost separation coverage area are in operation, while residual nodes remain in dormant state. Thus, much energy is saved, and life cycle of the network is enhanced. Jia et al. [9] presented a weighted genetic algorithm and optimization coverage mechanism based on the genetic restriction algorithm. According to the fitness function generated to perform the operation of the genetic algorithm, a complete coverage province is needed for the guessing the finest set of nodes and the absolute assortment of the work node, thus prolonging the endurance of the network. Han [10] proposed a scheme anchored in a genetic algorithm coverage programming and evolutionary inclusive search techniques to monitor all the targets and that can discover the optimum coverage set, extending the life span of the network.

3 Proposed Approach

3.1 Problem Formulation

In this study, the focal point of our work is to manage the POC coverage with least energy efficiently. Consequently, our endeavor is to locate such specific set of sensor nodes such that each POC is covered by at least one node. This hitch can be devised mathematically as follows:

Optimization Model:

$$\begin{aligned}
&\mathrm{Min} \sum \mathrm{cost}_{\mathrm{i}}.a_{\mathrm{i}} \quad i = 1,\ 2,\ 3,\ 4 \ldots M \\
&\text{Subject to :} \\
&\quad \sum C_{\mathrm{i,j}}\ a_{\mathrm{i}} \geq 1,\ j = 1,\ 2,\ 3,\ 4 \ldots N \\
&\quad x_{\mathrm{i}} = 1 \text{ or } 0, \quad\ i \in [1, M]
\end{aligned}$$

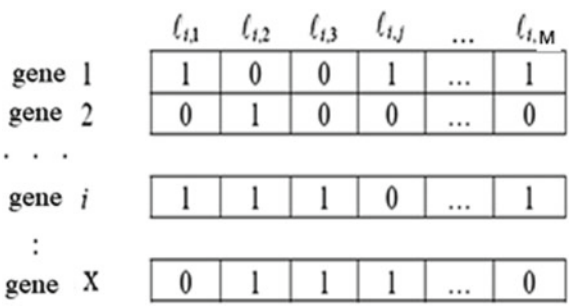
where Cost_i is the outlay of stimulating ith sensor node; a_i's are the key assessment variables which are determined by proposed approach. The proposed approach decides the value of a zero if it should be inactive otherwise a is set 1. The objective function diminishes the total number of nodes required to be activated such that each POC in sensing vicinity is covered.

3.2 Absolute Sensing-Area Coverage Using Extended Genetic Algorithm

The proposed "Absolute sensing-Area Coverage Using extended Genetic Algorithm" (ASCeGA) comprises two optimization strategies: an extended GA approach for schedule determination for sensor nodes and a stir-up proposal. The foremost scheme deactivates superfluous nodes in clustered WSN in accordance with the proposed schedule for nodes. The working of proposed approach is exemplified in Fig. 2. The subsequent stir-up proposal handles the energy-proficient coverage optimization every time. The initial populace is usually produced in random manner. Selection, crossover and mutation are genetic operations, which are used in evolutionary process.

In the ASCeGA, we use the fitness function to evaluate the rectitude of every individual solution (gene). After completion of genetic operations, we apply the extended search to further improve the rectitude of the solutions. After extended search, a novel populace of superior genes is produced. Individuals in the novel populace are h in the vicinity of to the overall finest solution. Additionally, when termination criterion is satisfied, it will be assumed that finest solution has been found, and thus the evolutionary process will be ended.

Figure 1 depicts the genetic representation for the power-proficient coverage optimization. There is X number of genes, and allele $l_{i,j}$ denotes whether sensor node s_j in gene i is active or not. As there are M nodes, the length of each gene is M. Here, we take fixed size of populace size for every populace generated in each generation. With the aim to preserve power and attain the finest coverage ratio, a best schedule



	$l_{1,1}$	$l_{1,2}$	$l_{1,3}$	$l_{1,j}$	…	$l_{1,M}$
gene 1	1	0	0	1	…	1
gene 2	0	1	0	0	…	0
. . .						
gene i	1	1	1	0	…	1
:						
gene X	0	1	1	1	…	0

Fig. 1 Genetic representation used in the ASCeGA

for sensor nodes is included into the ASCeGA to dormant these superfluous nodes (Fig. 2).

We also propose a coverage vector CV to characterize the coverage of each POCs. By using the sensing coverage model (Sect. 3.1), we delineate the coverage vector of s_i as $CV_i = [C_{i,1}, C_{i,2}, \ldots, C_{i,N}]$, where $s_i \in S$. In the similar way, for another

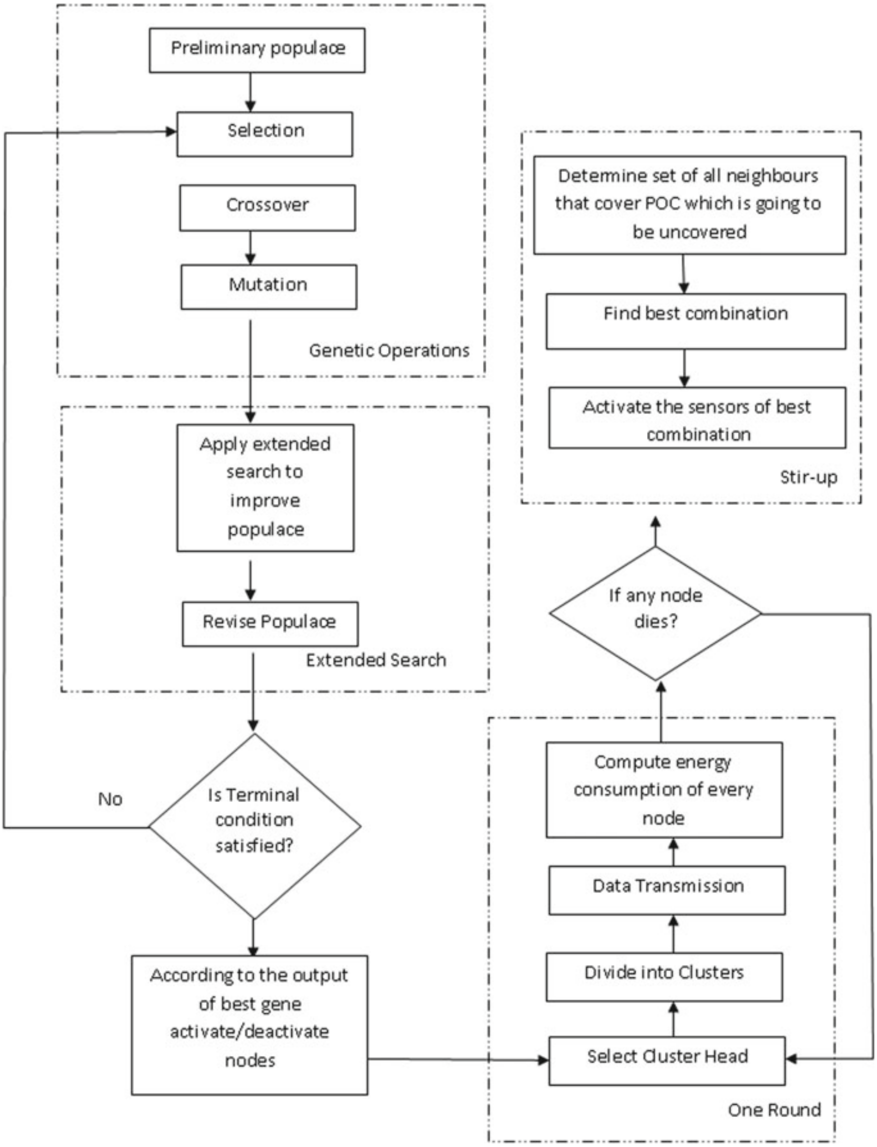

Preliminary populace
Selection
Crossover
Mutation
Genetic Operations
Apply extended search to improve populace
Revise Populace
Extended Search
No
Is Terminal condition satisfied?
According to the output of best gene activate/deactivate nodes
Determine set of all neighbours that cover POC which is going to be uncovered
Find best combination
Activate the sensors of best combination
Stir-up
If any node dies?
Compute energy consumption of every node
Data Transmission
Divide into Clusters
Select Cluster Head
One Round

Fig. 2 Flowchart of the ASCeGA

sensor node $s_{\text{ j}} \in S$, the coverage vector is would be $\text{CV}_{\text{j}} = [C_{\text{j, 1}}, C_{\text{ j, 2}}, \ldots, C_{\text{ j, N}}]$, where $i \neq j$. By using binary model, following synthetic coverage vector (SCV) can be delineated for s_{i} and s_{j} to symbolize whether a specified POC is covered by these sensors.

$$\text{SCV}\big(s_{\text{i}}, s_{\text{j}}\big) = \text{CV}_{\text{i}} \vee \text{CV}_{\text{j}} = \big[C_{\text{i,1}} \vee C_{\text{j,1}},\ C_{\text{i,2}} \vee C_{\text{j,2}}, \ldots, C_{\text{i,N}} \vee C_{\text{j,N}}\big]$$

where SCV designates a synthetic coverage vector, which determines whether s_{i} and s_{j} cover every POC in combined manner or not. Consequently, the SCV for a gene k is delineated as follows:

$$\text{SCV}(k) = \big(l_{\text{k, 1}}.\text{CV}_1\big) \vee \big(l_{\text{k, 2}}.\text{CV}_2\big) \ldots \vee (l_{\text{kM}},\ \text{CV}_{\text{M}})$$

As the coverage assessment procedure is made simpler into binary operations, the working of ASCeGA can be enhanced significantly. Additionally, we can establish the coverage ratio (CoR) for the gene k by:

$$\text{CoR}_{\text{k}} = \frac{\|\text{SCV}(k)\|}{N}$$

where $\|\text{SCV}(k)\|$ represents the number of POC covered by gene k. The utility ratio (UR*)* of nodes for gene k is computed by:

$$\text{UR}_{\text{k}} = \frac{\sum\limits_{p=1}^{N} l_{\text{k, p}}}{M}$$

where $\sum_{p=1}^{N} l_{\text{k, p}}$ represents total nodes that have been chosen to be stimulated. We delineate fitness function f_{k} as the goodness of gene k and devise it as:

$$\text{f}_{\text{k}} = \text{CoR}_{\text{k}} - \text{UR}_{\text{k}}$$

Substituting CoR_{k} and UR_{k}:

$$\text{f}_{\text{k}} = \frac{\|\text{SCV}(k)\|}{N} - \frac{\sum\limits_{p=1}^{N} l_{\text{k, p}}}{M}$$

The constrained boundaries are $0 \leq \text{CoR}_{\text{k}} \leq 1$, $0 \leq \text{UR}_{\text{k}} \leq 1$ and $1 \leq f_{\text{k}} \leq 1$. Thus, the solution encoded in gene k is considered better if it has higher value of $f_{\text{k.}}$

Genetic Operations

Selection, crossover and mutation are the operations generally used in genetic algorithms. For selection, we have numerous strategies but proportional fitness, roulette wheel and fixture selections are mostly used. The fixture assortment strategy has been exploited in proposed ASCeGA. We have opted for this just because it gives the best fitness of each generation more powerfully. In the fixture assortment approach, a competition is organized among arbitrarily selected individuals and then chooses the conqueror for crossover. In proposed ASCeGA, every allele signifies the state of a sensor which is kept 1 for active and 0 for dormant. The gene with elevated fitness value implies that the clustered WSN has an improved schedule for sensor nodes while applying ASCeGA. The result of selection procedure is used for crossover. A single-point crossover is used in crossover task.

After the crossover, we apply the mutation operation which changes one or more values in any probable gene allele. It supports the whole GA to thwart the populace from being ensnared in a local best solution. Therefore, the newly constructed individual (gene) is added to the original gene pool. The concluding offspring have an elevated fitness because of iterative operations of crossover as well as mutation.

Extended Search Scheme

In this research work, an extended exploration plan is derived so that proposed ASCeGA converges rapidly thus further perk up the righteousness of the populace computed by genetic operations. In this approach, we alter the value of every allele from one to zero and keep the updated gene if the fitness value of new gene is greater than the fitness value of original gene.

In this way, gene can be polished to an improved one if superfluous nodes are found. Contrasting the traditional genetic approaches, the proposed ASCeGA gives superior outcome by performing the extended search process. Using the developed extended exploration scheme, the ASCeGA converges swiftly.

The ASCeGA keeps sprouting until a extinction condition is fulfilled. Here, the evolutionary process is finished when its optimal result is unaffected for η subsequent generations.

Stir-up

Our stir-up mechanism comes into picture when active node looses its entire energy. When such situation occurs, some POC becomes uncovered. Thus, some dormant nodes are required to be stimulated to recover the coverage of uncovered POCs.

After each transmission, each active sensor of gene is checked whether it is still active or exhausted its whole energy. If one sensor s_{i} drains its entire energy, the BS will re-examine the coverage of network and find the uncovered POCs $\left(\mathrm{CV}_{\mathrm{uncovered}}^{S_{\mathrm{i}}}\right)$ by taking exclusive OR between the original SCV of all sensor nodes including sensor s_{i}, and the SCV without sensor s_{i}.

Let node $s_{\mathrm{i}} \in S$, where S is the set of all sensor nodes, and i =1, 2, 3 … M. The ui signifies the set of all adjacent sensors of s_{i}, where i =1, 2, 3 … M. If SCV (synthetic coverage vectors) of some sensors which belong to ui, have overlapped with $\mathrm{CV}_{\mathrm{uncovered}}^{S_{\mathrm{i}}}$, let $\mathrm{OP_i}$ be the set of such sensors. Additionally, let $S_{\mathrm{OP_{i,k}}}$ characterize the k-th probable subset of $\mathrm{OP_i}$, and w is total number of subsets in $\mathrm{OP_{i.}}$

Process of the stir-up proposal

```
best_comb, best_value = 0;
map=[0, 0, …,0], res = [0, 0, …,0], length = $N$;
```

If (sensor s_i has exhausted its energy and cannot work acceptably) then

```
{  Loop k =1 to w
   { Loop every element d of $S_{OP_k}$
      { map =$CV_d$ ∪ map ;}
      res=map∩ $CV_{uncovered}^{S_i}$
      if $\sum_{a \in res} a + \frac{1}{size(S_{OP_k})+1}$ > best_value then
      best_value= $\sum_{b \in res} b + \frac{1}{size(S_{OP_k})+1}$

      best_comb= $S_{OP_k}$ ;
   }
output = best_comb;
}
```

Stir-up proposal spawns a best schedule to stimulate and makes some sensors in a dormant mode. As mentioned above, some dormant nodes will be activated by BS according to the finest schedule of nodes generated by the stir-up method at the commencement of the next round. If any sensor loses its complete energy yet again, the sit-up method will re-examine the coverage and resolve to stimulate some other sensor nodes to convalesce the uncovered POCs. In this way, we succeed to preserve the coverage of POCs in effective manner.

4 Experimental Evaluation

We simulated our proposed approach in a field with dimensions 100 m × 100 m where 10 POCs and 100 nodes disseminated randomly in a sensing field. All the POCs are also deployed randomly. MATLAB is used to implement the simulations. The sensing range Ra is assumed as 12.61 m considering 20% active nodes. Nodes with space less than 12.61 m are delineated as neighbors. Number of generations to which the optimization carried out is 30. Crossover rate (Rc) is 0.8, and mutation rate (Rm) is 0.006. Transmit/receive energy (*Eelec)* is 50 nJ/bit, amplification energy (*Eamp)* is 100 pJ/bit/m^2, and data aggregation energy *EDA* is 5 nJ/bit/report. Location of base station is (50, 200). Data packet size is 400 bits. Initial energy of each node is 0.5 J.

Figure 3 depicts the deployment of nodes and coverage for POCs after applying the proposed optimal schedule.

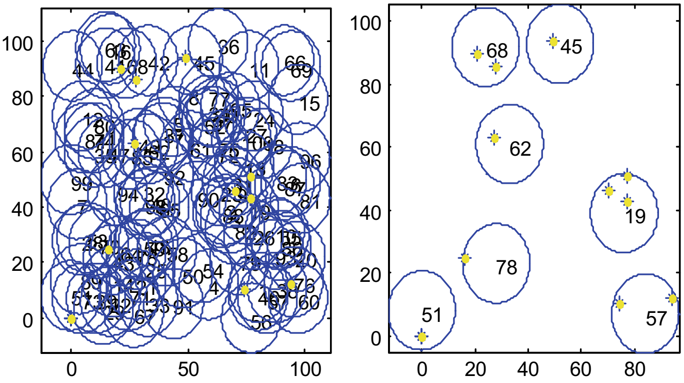


Fig. 3 Unvarying deployments of sensors and POCs

We evaluate our proposed approach with VP-NL [11] and FDA [12] and *K* coverage GA [13]. We conducted simulations using the identical network mentioned previously where nodes and POCs are deployed randomly.

Sensing coverage ratio is exemplified in Fig. 4 against number of rounds. This figure noticeably designates that VP-NL and FDA provide meager capabilities in maintaining coverage ratio (CoR). While the ASCeGA reaches to 0% sensing coverage ratio at round number approx 4000 which is greater than all other compared approaches.

Figure 5 shows the comparison of life span of propose and other approaches. We detect that the sensors loose entire energy rapidly using VP-NL and FDA methods because of lack of efficiency in scheduling strategy. Conversely, the *K* coverage

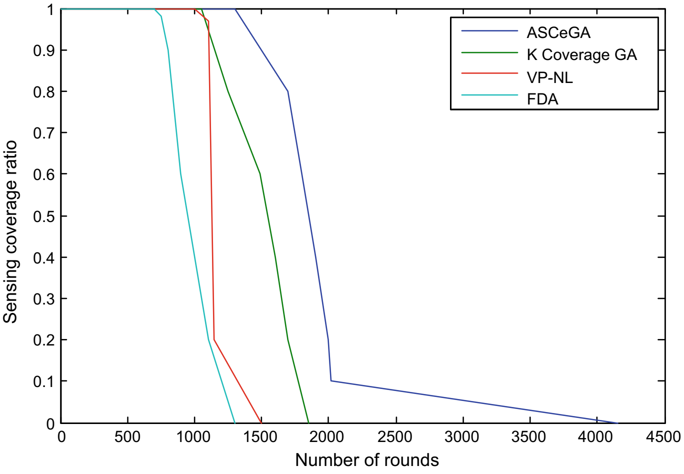


Fig. 4 Rounds verses sensing coverage ratio versus

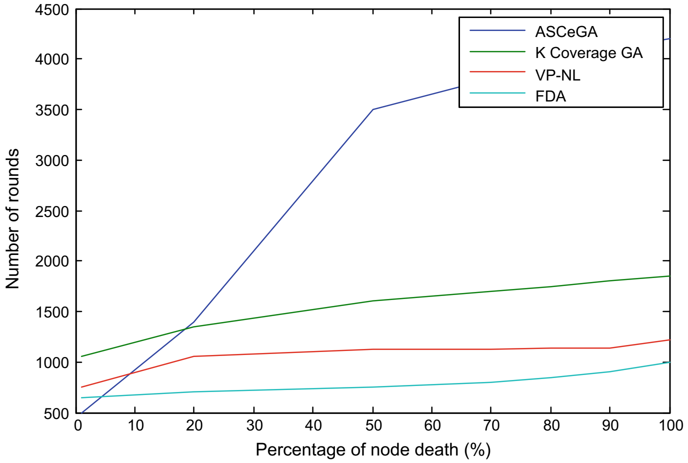


Fig. 5 Number of rounds versus percentage of dead nodes

GA and ASCeGA can deactivate the superfluous sensor nodes via node-scheduling strategy that accumulate a large amount of energy, so the network life span can be enhanced.

5 Conclusion

As sensor partakes in the network operations only for the time they have energy, then energy competence in the blueprint of every aspect of such nodes is required. Energy burning in sensors occurs chiefly due to computational processing. In this paper, we designed an energy-proficient approach by exploiting the genetic algorithm so that only minimum nodes should be active at any time and participate in communication. If any active node dies, any sleeping node to recover the network coverage is woken. Our experimental evaluation shows that by using the extensive genetic algorithm, we attained the better network life span and coverage.

References

1. Biswas S, Das R, Chatterjee P (2018) Energy-efficient connected target coverage in multi-hop wireless sensor networks. Industry interactive innovations in science, engineering and technology, Springer, Singapore, pp 411–421
2. Liu Y, Pu J, Zhang S, Liu Y, Xiong Z (2009) A localized coverage preserving protocol for wireless sensor networks. Sensors 9:281–302
3. Bellur U, Jaiswal N (2006) Power aware duty scheduling in wireless sensor networks. Lect Note comput Sci 4308:546–551

4. Boukerche A, Fei X, Araujo RB (2007) An optimal coverage-preserving scheme for wireless sensor networks based on local information exchange. Comput Commun 30:2708–2720
5. Cardei M, Du DZ (2005) Improving wireless sensor network lifetime through power aware organization. Wirel Netw 11:333–340
6. Wang XR, Xing GL, Zhang YF, Lu CY, Pless R, Gill CD (2003) Integrated coverage and connectivity configuration in wireless sensor networks. In: Proceedings of the 1st ACM conference on embedded networked sensor systems (SenSys'03), Los Angeles, CA
7. Liang Y, Zeng P, Yu H (2006) Energy adaptive cluster-head selection for wireless sensor networks. Inf Control 35:141–146
8. Chen CP, Mukhopadhyay SC, Chuang CL, Lin TS, Liao MS, Wang YC, Jiang JA (2015) A hybrid memetic framework for coverage optimization in wireless sensor networks. IEEE transactions on cybernetics 45(10):2309–2322
9. Jia J, Chen J, Chang J, Zhao L, Wang G (2007) Optimal coverage scheme based on genetic algorithm in wireless sensor networks. Control Decis 1(22):1289–1292
10. Gil JM, Han YH (2011) A target coverage scheduling scheme based on genetic algorithms in directional sensor networks. Sensors 11:1888–1906
11. Yang Q et al. (2015) Variable-power scheduling for perpetual target coverage in energy harvesting wireless sensor networks. In: International symposium on wireless communication systems (ISWCS), IEEE, pp 281–285
12. Wan X, Wu J, Shen X (2015) Maximal lifetime scheduling for roadside sensor networks with survivability. IEEE Trans Veh Technol 64(11):5300–5313
13. Elhoseny M et al. (2017) K-coverage model based on genetic algorithm to extend WSN lifetime." IEEE Sens Lett 1.4:1–4

Detection of Phishing Websites Using Machine Learning

Ahmed Raad Abbas, Sukhvir Singh and Mandeep Kau

Abstract Phishing is defined as imitating a creditable company's website aiming to take private information of a user. These phishing websites are to obtain confidential information such as usernames, passwords, banking credentials and some other personal information. Website phishing is the act of attracting unsuspecting online users into revealing private and confidential information which can be used by the phisher in fraud, blackmail or other ways to negatively affect the users involved. In this research, an approach had been proposed to detect phishing websites by applying a different kind of algorithms and filters to achieve a reliable and accurate result. The experiments were performed on four machine learning algorithms, e.g., SMO, logistic regression and Naïve Bayes. Logistic regression classifiers were found to be the best classifier for the phishing website detection. In addition, the accuracy was enhanced when the filter had been applied to logistic regression algorithm.

1 Introduction

Online phishing is considered a criminal way to deceive users to reveal their important information, like username, password, as it mentioned in Fig. 1, credit card detail, etc., by pretending to be a trustworthy entity in the online communication. They get the users trust by claiming that they are from a legitimate party, like well-known services providers or financial institution such as bank or PayPal, etc., and then they misguide the users to a fraudulent website to grab their credentials. Phishing was considered a crime for the industrial economy, due to the massive loss which they suffered [1].

The number of the phishing attempts according to APWG is getting higher and expanding.

A. R. Abbas (✉) · S. Singh · M. Kau
Department of Information Technology Development (IT), University Institute of Engineering and Technology (UIET), Punjab University, Chandigarh 160015, India
e-mail: ahmedalani.sa@yahoo.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_128

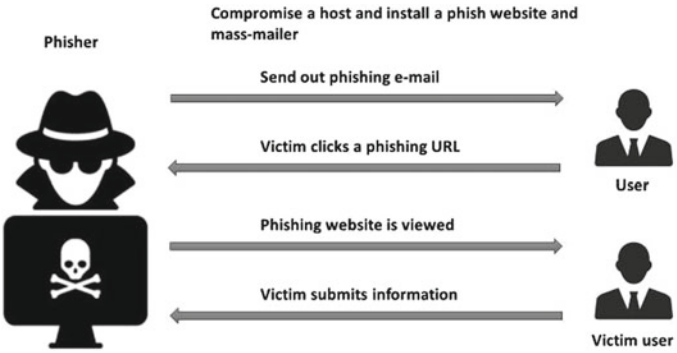

Phisher
Compromise a host and install a phish website and mass-mailer
Send out phishing e-mail
Victim clicks a phishing URL
Phishing website is viewed
Victim submits information
User
Victim user

Fig. 1 An example of phishing

The statistic reports have displayed that the entire phishing attack was enlarged significantly from 180.577 to 263.538 cases from the last quarter of 2017 until the first quarter of the year 2018. As for the monetary losses, it was massive [2].

A lot of users without realizing click on phishing domain daily. The hackers did not just target the clients yet the companies as well. In the 3rd Microsoft Safer Index Report, which was out on 2014, the phishing attacks can influence very high a 5 billion dollar. The lack of awareness of the users is the main reason behind this huge lost [3]. So, security protectors must take an action for clients not to face any harmful sites. The protectors mostly attempt to rise to awareness of the company against phishing to prevent any damage and build immune security system which can confront phishing and prevent it.

2 Literature Review

A new methodology [4] was proposed to detect phishing websites, by utilizing arbitrary forests, for example, the sorting algorithm with the aid of RStudio. Therefore, they were able to extract eight features which they have found it to be the best and work it out to achieve an overall accuracy as they claimed 95%.

A new system was introduced by Sahingoz [5] which involves using seven different algorithms, for example, the Decision Tree, Ad boost, K-star, KNN ($n = 3$), Random Forest, SMO and Naïve Bayes. And 3 kinds of properties, and present them as NLP based features, word vectors, and hybrid features. Meanwhile, they have constructed their individual dataset with 73,575 URLs. This set comprises 36,400 legitimate URLs and 37,175 phishing URLs. Moreover, they have found that the NLP-biased features have performed the best among the other features' types. Moreover, the utilization of NLP grounded properties and word vectors jointly similarly will increase the functioning of the phishing detection structure. Authors use [6] a nonlinear regression approach to detect if the website is phishing or not. They have used harmony search and support vector machine metaheuristic algorithms to train the system. And as they have claimed, harmony search preforms an improved exactness percentage of 94.13% and 92.80% for training process, respectively, by utilizing about 11,000 web pages has proposed [7] an anti-phishing method, which utilizes machine learning by selecting nineteen different properties in the user's part to differentiate between phishing website and legitimate. They have used 2141 phishing pages from Phish Tank and Open phish, and 1918 genuine web pages from Alexa popular websites, some online payment gateways, and some top banking websites. By means of the machine learning, their anticipated method achieved 99.39% accurate percentage.

In other studies, such as [8], the researcher uses a hybrid technique by merging machine learning methods with image checking. A significant drawback of the image/visual grounded phishing discovery was around the requirement of a preliminary image database or previous familiarity (web history) of that web page; nevertheless, the given method is unrestricted of these barriers. They have implemented three featured groups: hyperlink-based features, third-party grounded features, and URL obfuscation features. Despite the have used third-party services, they manage to achieve high accuracy with 99.55%.

In [9], a classifier model was adopted which is able to detect phishing sites in a smart and computerized method by utilizing a dataset freely available. The used random forest algorithm has achieved 97.36% accuracy, and as they claimed that their outcomes exhibited that RF is quicker, strong and more precise than the rest of the classifiers.

The authors of [10] studied specific features which can increase the accuracy efficiency to detect the phishing websites. As they claimed in their study that (URL-grounded features, domain-grounded features, page-grounded features and content-grounded features) are the best features for machine learning-grounded discovery of phishing sites.

The authors of [11] in their study have recommended three new features which were measured with the current features. The investigational findings show that the new features are very powerful in contrast with the current features. The new features should be recognizable among the phishing and non-phishing websites.

3 Detection of Phishing Websites

The proposed approach architecture is shown in Fig. 2. This proposed work starts with investigating the accuracy the phishing detection system with complete set of features. Then, applying different algorithms on the divided or grouped features is investigated.

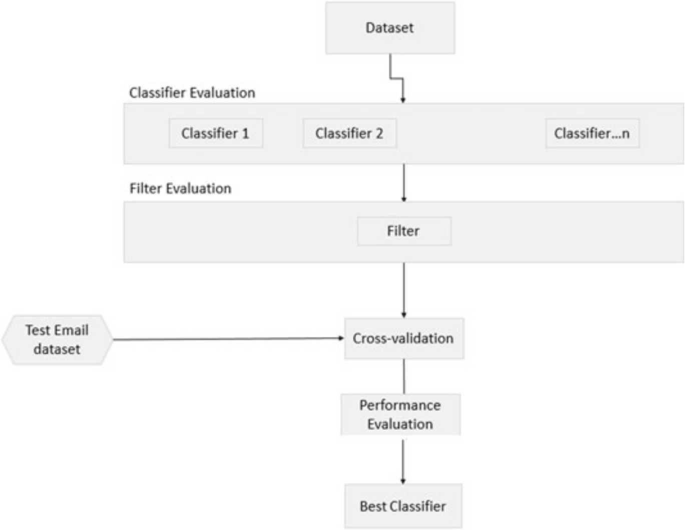


Fig. 2 Proposed approach architecture

3.1 Pre-processing

In the pre-processing stage, phishing website data was gathered from UCI repository website. Features have then been taken out from each website, all the features for all websites are given by rows, and each row presents the possibility of the website whether being legitimate, suspicious or phishing. By presenting different kind of features which in return they were chosen very carefully to fulfill the gaps in the phishing websites. Approximately, 30 features are presented, they were divided into subgroups to cover all area of website phishing, and each group can deal with specific and different area. The set of features were categorized into four collections: address bar-based features (contains 12 features), abnormal-based features (contains 6 features), HTML, JavaScript-based features (contains 5 features) and domain-based features (consists of 7 features).

3.2 Selection of Features

As it was discussed before, the making of four groups is grounded on the structure and the content of the website. This creates the collections as shown in Table 1.

Merged Groups Feature Selection:

Table 1 Groups of the features for phishing website detection

S. no	The features group	Number of features
1	Address bar-based features	12
2	Abnormal-based features	6
3	HTML, JavaScript-based features	5
4	Domain-based features	7
5	All the features	30

Table 2 Merged groups

S. no	The features group	Number of features
1	Group (1 + 2)	18
2	Group (1 + 3)	17
3	Group (1 + 4)	19
4	Group (2 + 3)	11
5	Group (2 + 4)	13
6	Group (3 + 4)	12

All these groups had been combined in Table 2, where each group presents a combination of two groups from the four features groups. The aim is finding the best group of features to apply in area of phishing detection for more accuracy.

3.3 The Used Algorithms

Four supervised ML algorithms were used, to prepare and examine the overall exactness with the grouped features for phishing websites detection. They were preferred and selected because of their different training strategy they can be used to figure out the mechanism and the rules of testing and learning, and the selected algorithms are well-known and listed below:

NAÏVE BAYES
SMO
Logistic Regression

3.4 Resample Filter

Resample filter adds instances to a class. This is understood by merely adding instances from the class which has only few instances multiple times to the result dataset. Produces a random subsample of a dataset using either sampling with replacement or without replacement. It balances the dataset by generating new data for the minor class [12].

4 Experimental Results on Features Selection

The results show that the three algorithms have achieved almost same accuracy in our test scenarios. However, the SMO classifier algorithm has the lowest mean of accuracy in both feature selection and groups selection as it is plotted in Table 3.

The logistic regression has achieved overall the best/highest accuracy at almost all the scenarios and features that had been tested. The logistic regression algorithm has shown that when it comes to websites phishing detection with use of the WEKA platform can detect the phishing attempts, and it can be considered as a reliable algorithm. On the other hand, the algorithms SMO and Naïve Bayes their results were in some cases very close but according to our dataset and our tests has shown that the performance for both of these algorithms were not best results and SMO algorithm consume a long time to process one test, this withdraw can affect the detecting process.

5 Conclusion

This work principally comprises machine learning-based techniques to recognize phishing websites. The used dataset contains 30 features, for more investigation and analysis, the features of dataset had been divided into four groups, each group contains related features, and then, their accuracy had been examined (precision and recall). The groups merged, finally, six different groups had been obtained as a result of this merging, and these groups had been analyzed to get the best results. All the groups were tested with three classifiers, the logistic regression was found to be the best regarding accuracy comparing with other classifiers. Then, a resample filter had been added to balance the dataset, which in return helped to enhance the result of logistic regression with accuracy rate of 93.8%.

Table 3 Overall accuracy

Algorithm	All	Address	Abnormal	HTML, JAVA	Domain	Group					
						G1	G2	G3	G4	G5	G6
Naïve Bayes	92.9	89.5	87.2	55.3	70.6	92.7	89.6	90	86.9	87.9	71.2
SMO	93.9	89.5	86.6	55.2	69.5	92.8	89.5	89.5	87.5	88.7	69.5
Logistic regression	93.8	89.5	87.3	55.9	70.8	93.1	89.6	91	87.3	88.8	71.1

References

1. Kirlappos I, Sasse MA (2012) Security education against phishing: a modest proposal for a major rethink. IEEE Secur Priv 10(2):24–32
2. APWG (2017) APWG Reports| APWG. https://www.antiphishing.org [Online]. Available https://www.antiphishing.org/resources/apwg-reports/
3. Katz J, Aspden P (1997) Motivations for and barriers to internet usage: results of a national public opinion survey. Internet Res 7(3):170–188
4. Parekh S, Parikh D, Kotak S, Sankhe S (2018, April) A new method for detection of phishing websites: URL detection. In: 2018 second international conference on inventive communication and computational technologies (ICICCT). IEEE, pp 949–952
5. Sahingoz OK, Buber E (2018) Machine learning based phishing detection from URLs. Expert Syst Appl. p 1–32
6. Rao RS, Pais AR (2018) Detection of phishing websites using an efficient feature-based machine learning framework. Neural Comput Appl. 1–23
7. Subasi A, Molah E, Almkallawi F, Chaudhery TJ (2017, November) Intelligent phishing website detection using random forest classifier. In: 2017 international conference on electrical and computing technologies and applications (ICECTA). IEEE, pp 1–5
8. Buber E, Demir Ö, Sahingoz OK (2017, September) Feature selections for the machine learning based detection of phishing websites. In: 2017 international artificial intelligence and data processing symposium (IDAP). IEEE, pp 1–5
9. Abunadi A, Akanbi O, Zainal A (2013, December) Feature extraction process: a phishing detection approach. In: 2013 13th international conference on intellient systems design and applications. IEEE, pp 331–335
10. Domingos P, A general method for making classifiers cost-sensitive. Artificial Inelligence Group, Instituto Superior Técnico, Lisboa, 1049–001
11. Babagoli M, Aghababa MP, Solouk V (2018) Heuristic nonlinear regression strategy for detecting phishing websites. Soft Comput 1–13
12. Jain AK, Gupta BB (2018) Towards detection of phishing websites on client-side using machine learning based approach. Telecommun Syst 68(4):687–700

Smart Drip Irrigation Using IOT

Smita Deshmukh, Swati Chavan, Prajakta Zodge, Pooja Dalvi and Akshaykumar Jadhav

Abstract As we can see in today's world, only some devices like PCs and mobiles are connected to the Internet. Nowadays, the world is copiously surpassed by the Internet and the internet of things. The Internet is used for the rudimentary need of all human beings [3]. IoT represents the concurrence of advances in minimization, wireless connectivity, enhances batteries and data storage capacity, and without sensors, IoT is not possible. It simply means to monitor a physical device or machine, or it is inter-networking of physical devices which is entrenched with electronics, sensors, software, and network connectivity to facilitate it to achieve greater value and services by swapping data with the producer [1]. IoT permits objects to be sensed or controlled remotely across the network infrastructure. The result improves accuracy, economic benefits, efficiency and reduces the intervention of a human. In this paper, we are going to deal with rudimentary and imperative perceptions of IoT and its scope in the forthcoming future. This paper studies the need for IoT in day-to-day life for different applications and gives fleeting information about IoT. IoT contributes significantly toward revolutionary farming approaches. So, we are trying to demonstrate IoT in the automatic watering system [2]. An automatic watering system monitors and preserves the approximate moisture gratified in the soil. Raspberry Pi is used as a microcontroller to implement the control unit. The setup uses the temperature sensor, moisture sensor and humidity sensor which measure the approximate temperature, moisture and humidity in the land. This value empowers the system to use belonging quantity of water which avoids over/under irrigation.

S. Deshmukh · S. Chavan (✉) · P. Zodge · P. Dalvi · A. Jadhav
IT Department, Terna Engineering College, Mumbai University, Plot no. 12, Sector-22, Phase 2, Nerul(W), Navi Mumbai, Maharashtra 400706, India
e-mail: Swati98tc@gmail.com

P. Zodge
e-mail: Prajaktazodge21@gmail.com

P. Dalvi
e-mail: Dalvipoojav25@gmail.com

A. Jadhav
e-mail: Aj773144@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_129

Keywords IoT · Moisture · Temperature · Humidity

1 Introduction

Agriculture is and will be the backbone of Indian economy [3]. Irrigation scheduling is one of the solutions of the questions of "When do I water?" [4]. In our country, monsoon rainfall is irregular and uneven. We have only 4% of the world's freshwater resources to satisfy the agricultural needs for our 1.324 billion population, and improper method of irrigation is the primary reason for water wastage in agriculture [5]. Automatic irrigation is easy to configure, and it helps to save energy and resources. To make sustainable agriculture and prevent water wastage, smart drip irrigation using IoT is proposed [6]. Sensors are physical device which converts device parameter to electric signal on which we control whole system [6]. The objective of this system is to render a reliable, robust, efficient and intelligent drip irrigation controller device-based system which is smart enough to analyze distinct parameters of a field like moisture, temperature, humidity, etc., and provides a water delivering schedule in a targeted manner near the root zone of the crop to ensure all the crops get enough water for their healthy growth, thereby reducing manual intervention of farmer [7]. Sensors measure the field parameter which helps to reduce wastage of water than other systems [8]. The system analyzes the soil quality to avoid soil erosion [9]. It provides capability to farmer for control system through Android application. The system uses emitter lines with different nozzles that can control water flow so that plants like succulents can get less water, while plants with high water requirements can get more and keep a check on the amount of water used for irrigation [8]. The system gathers local weather information and some even factors in the field landscape (types of plants, soil quality, slopes, etc.) to make irrigation run-time adjustments, so the crops always receive the appropriate amount of water [7]. In order to inform the farmer about exact field condition and provide manual control over the system, system incorporates the concept of IoT (internet of things) via mobile app [10]. The Android application has a user interface (UI) which will show all the data to user in graphical format [11]. System provides benefit of both reduction of labor cost and water wastage.

2 Existing System

The prior system consists of mainly two parts hardware and software [8]. In that, software is a web page designed by using PHP, and soil content monitored by hardware part [8]. The existing system consists of Arduino along with sensors which monitor the soil moisture content and accordingly irrigating the fields as when needed [8]. This system introduced a GSM-SMS secluded measurement and control system for farms based on PC-based database system which are connected with the base station, which is developed by using a microcontroller, GSM module, actuators and sensors. Many conditions like the status of electricity, running status of a motor, increased/decreased temperature, changing a level of moisture will be informed to the users via SMS on GSM network or by Bluetooth [8]. The system receives and sends messages through GSM module, and parameters like temperature, air humidity and moisture which are set by the central station are measured in every base station. Parameter is exchanged between a far end and designed system via SMS on GSM network. A SIM with 3G data pack inserted into a system which provides IoT features to the system. This system sets the irrigation time depending on reading from sensors and type of crop, and it can automatically irrigate the field when needed. The sensor parameters regularly updated on a web page by using the GSM-GPRS SIM900A parameter.

3 Proposed System

Features of Smart Drip Irrigation Using IOT:

1. Automated drip system collects real-time data of the water content in the root zone of the crop as an input argument, correlates it with other parameters such as temperature, humidity, insolation, light-intensity, barometric pressure of environment and outputs the precise amount of water/fertilizers required for the crop.
2. Water Source: The water level in the water reserve is kept in check by the SDIS, and the farmer is informed accordingly.
3. Real-time monitoring: System comprises a mobile app and GSM messaging facility which enable the farmer to remotely monitor the status of the field by knowing the sensor values.
4. Customization: A farmer can monitor and control the valve/motor status and set the desired crop moisture level by operating a mobile app or through GSM messaging service.
5. Set Preferences: Through the mobile app, a farmer can select the crop type, soil type preferences to adjust the system for a specific type of crop.

This is smart drip irrigation using IoT is the system which is designed to minimize water wastage in agriculture. It is cost effective, any farmer can use it in farm fields, and it increases productivity and saves water resources.

4 Working:

The smart drip irrigation using IoT comprises four major sections which are as follows:

Sensor section: System collects real-time data of the water content in the root zone of the crop as an input argument, correlates it with other parameters such as temperature, humidity, insolation, light-intensity, barometric pressure of environment and outputs the precise amount of water/fertilizers required for the crop. The water level in the water reserve is kept in check by the system, and the farmer is informed accordingly. **Control section:** Raspberry Pi monitors the system based on approximate parameter calibrated by various sensors. It defines the threshold value based on which it takes decisions whether to irrigate or not irrigate the field. SIS provides offline communication via GSM Module, an online communication via mobile app to notify the user exact condition of field.

GSM module (offline):

- Control the motor/valve status via SMS.
- Set the desired crop moisture level.
- Monitoring different parameters of the crops like moisture, temperature, humidity, soil fertility, insolation, light-intensity, barometric pressure of the environment.
- Monitor the status of water reserve and weather patterns.

Android application (via the Internet):

A farmer monitors and controls the valve/motor status and sets the desired crop moisture level by operating the mobile app.

IoT section:

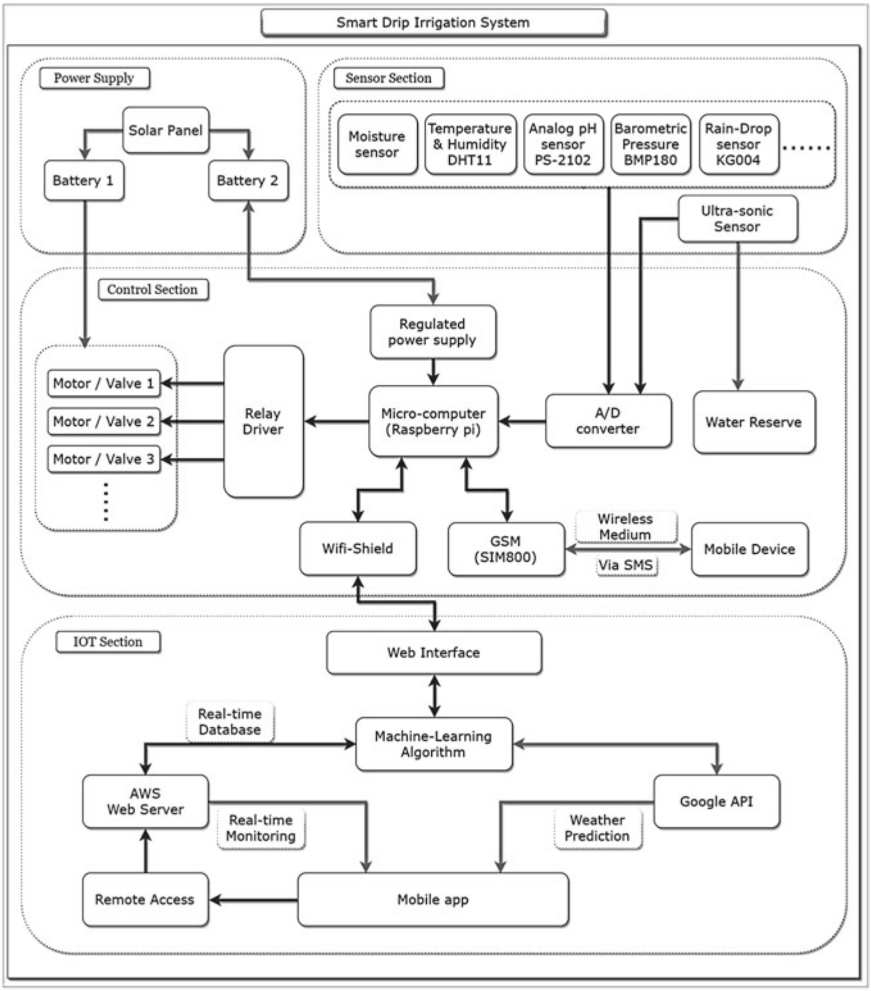
Machine learning algorithm:

- Monitors different parameters of the crop, water reserve, weather patterns and supervises the irrigation.
- Maintains records of different crop parameters and corresponding weather conditions.
- Performs analysis on historical data to predict the performance and watering needs of crop and recommends optimum practices to avoid any damage to the crops.
- Notifications to the farmer via mobile app and GSM.

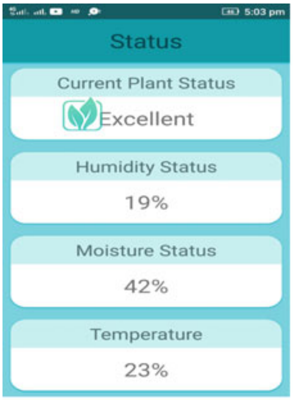
E-Plant: (Mobile app)

- Controlling the motor/valve status.
- Set the desired crop moisture level if necessary.
- Monitoring different parameters of the crop, water reserve and weather patterns.
- Selection of plant type, soil type as per farmer requirement.
- Day-wise graphical analysis of crop data.
- Predictions and recommendations based on the performance of the crop.

Block Diagram



Screenshot



Status

Current Plant Status

Excellent

Humidity Status

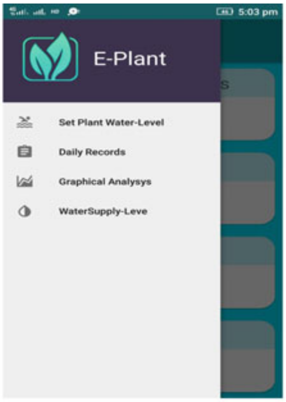
19%

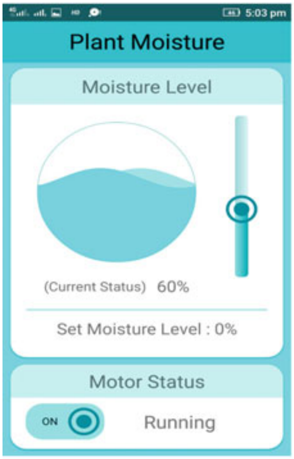
Moisture Status

42%

Temperature

23%





Plant Moisture

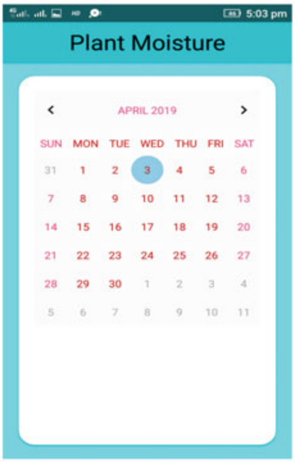
Moisture Level

(Current Status) 60%

Set Moisture Level : 0%

Motor Status

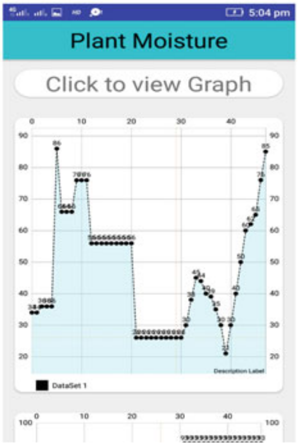
ON Running



Plant Moisture

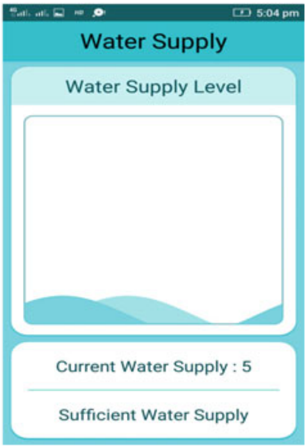
‹ APRIL 2019 ›

SUN	MON	TUE	WED	THU	FRI	SAT
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4
5	6	7	8	9	10	11



Plant Moisture

Click to view Graph



Water Supply

Water Supply Level

Current Water Supply : 5

Sufficient Water Supply

5 Conclusion

In our India, most of the water is consumed in agriculture activity. The methodology was designed in the way such that it monitors temperature, humidity, moisture in the soil, and the project provides an occasion to learn the existing systems, along with their topographies and downsides. The approach can be used to switch the motor depending on the favorable condition of plants, i.e., sensor values, thereby systematizing the process of irrigation, which helps to anticipate over or under irrigation of soil, thereby avoiding crop damage which is one of the most time-efficient activities in farming. The farm owner can observe the development online through an Android app. This research work determined that there can be a significant advancement in farming with the use of IoT and automation.

Reference

1. https://www.pwc.com/us/en/increasing-it-effectiveness/assets/future-of-the-internet-of-things.pdf
2. http://www.ewaterautosys.com/water-automation-system.html
3. http://www.wplawinc.com/agricultural-irrigation-blog/the-most-common-problems-with-farm-irrigation-systems
4. Sahu CK, Behera P (2015) A low cost smart irrigation control system. In: IEEE sponsored 2nd international conference on electronics and communication system (ICECS)
5. Kansara K et al. (2015) (IJCSIT) Int J Comput Sci Inf Technol 6(6):5331–5333. https://www.researchgate.net/publication/296396429_Sensor_based_Automated_Irrigation_System_with_IOT_A_Technical_Review
6. Bhagyashree KC, Rana JG (2016) Smart irrigation system using raspberry pi In IRJET 03(05)
7. Automated Irrigation System Using a Wireless Sensor Network and GPRS Module Article (PDF Available). In: IEEE transactions on instrumentation and measurement
8. https://www.ijcaonline.org/archives/volume159/number8/rawal-2017-ijca-913001.pdf
9. Tararani G, Shital G, Sofiya K, Gouri P, Vasekar SR, (IRJET) Smart drip irrigation system using IOT. https://www.irjet.net/archives/V5/i10/IRJET-V5I10124.pdf
10. Sahu T, Automated smart irrigation system using raspberry pi. MTech CSE Gyan Ganga Institute of Technology and Sciences Jabalpur, India. https://www.ijcaonline.org/archives/volume172/number6/sahu-2017-ijca-915160.pdf
11. Nemali KS, van Iersel MW (2006) An automated system for controlling drought stress and irrigation in potted plants. Sci Hortic 110(3):292–297, Nov 2006

An Efficient Scheduling Algorithm for Sensor-Based IoT Networks

M. Deva Priya, T. Suganya, A. Christy Jeba Malar, E. Dhivyaprabha, Prajith Kesava Prasad and L. R. Vishnu Vardhan

Abstract Internet of Things (IoT) based networks with sensors are energy and delay stringent. Efficient scheduling algorithms for IoT-based networks are the need of the hour. Nodes with selfish behavior degrade the performance of the network. Hence, a scheduling algorithm that schedules packets based on their emergencies and priorities yields better results. In this paper, M/M/1 and M/M/N scheduling scheme to schedule Emergency packets (E-packets) and Regular packets (R-packets) is proposed. The next-hop nodes are chosen based on the trust value of nodes. It is seen that the proposed scheme yields better results in terms of Packet Delivery Ratio (PDR), end-to-end delay, throughput and routing overhead.

Keywords IoT networks · Wireless sensor network (WSN) · Scheduling · Backpressure scheduling · Emergency packets (E-packets) · Regular packets (R-packets)

M. Deva Priya (✉) · T. Suganya · A. Christy Jeba Malar · E. Dhivyaprabha · P. K. Prasad ·
L. R. Vishnu Vardhan
Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India
e-mail: m.devapriya@skct.edu.in

T. Suganya
e-mail: suganya.t@skct.edu.in

A. Christy Jeba Malar
e-mail: a.christyjebamalar@skct.edu.in

E. Dhivyaprabha
e-mail: e.dhivyaprabha@skct.edu.in

P. K. Prasad
e-mail: 15tucs144@skct.edu.in

L. R. Vishnu Vardhan
e-mail: 18tucs253@skct.edu.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_130

1 Introduction

Internet of Things (IoT) is a technology in which devices including sensors are connected through the Internet. It comprises of a large network including people and things which accumulate and share data depending on the surrounding environment and their usage [1]. IoT systems are versatile and find their applications in diverse fields due to their flexibility in adapting to any environment. It is a powerful technology with devices that are capable of supporting data collection, automation, operations, etc.

A Wireless Sensor Network (WSN) includes several hundreds and thousands of tiny sensors that sense, monitor, measure, process and communicate the values of real-world parameters such as heat, humidity and weather [2]. These networks are more economical in contrast to traditional wired networks with sensors. The sensors are energy stringent and have limited lifetime. The sensors are equipped with transceivers involving less power that aid in collecting data. To preserve the cost effectiveness of WSNs, they are made of small batteries. This becomes a challenge as energy is a factor that determines the lifetime of a network [3, 4].

1.1 Selfish Node Attack

In WSN, nodes forward data packets to their neighbors consuming bandwidth, energy and memory. Selfish nodes maintain communication with desired nodes and forward packets, but decline to collaborate with other nodes. They do not share resources with others but use them only for their own necessity. They conserve their own resources, but drain others'. They do not forward or retransmit packets leading to loss of communication and degradation of performance of network [5].

2 Related Work

In this section, the scheduling schemes proposed by various authors for WSNs are discussed. Backpressure Scheduling (BS) is not suitable for Emergency IoT (EIoT) as the queueing model is inefficient for scheduling Emergency packets (E-packets).

Tassiulas and Ephremides [6] have propounded a traditional BS scheme which was later extended to Mobile Ad hoc Networks (MANETs) [7], cellular networks [8], WSN [9], energy stringent sensor networks [10], WSNs for multimedia [11] and multi-hop wireless networks.

Sridharan et al. [12] have designed a protocol for rate control based on the BS scheme. The throughput in a network is improved by the propounded data aggregation scheme. The overall network stability is maintained by conserving energy in a network [13].

Moeller et al. [9] have proposed a BS scheme different from path-based schemes. In path-based schemes, loops are absent and packets are transmitted through shorter paths. In the modified BS scheme, the delay of BS is reduced and unnecessary long path and loop problems are circumvented. These issues can be avoided by computing the weights based on the difference in queue backlog.

Similarly, Dvir and Vasilakos [14] have proposed a hop count-based scheme wherein packets are transmitted to a controlled area. Ying et al. [15] have designed a clustering-based BS scheme wherein two types of queues namely, inter-cluster queues and intra-cluster queues are maintained in each node.

The number of queues and the end-to-end delay are reduced when the traditional BS scheme uses Last in First Out (LIFO) queue instead of First in First Out (FIFO) queue. Alresaini et al. [16] have pre-computed the queue backlogs, enabling the network to generate backlog difference gradients on low network loads. The end-to-end delay is acceptable as the per-neighbor queue replaces the traditional backpressure queue model.

Huang et al. [17] have examined the tradeoff between LIFO and FIFO queue models. It is seen that the average energy consumption of BS scheme converges gradually. They have not dealt with queuing emergency packets.

Ji et al. [18] have focused on reducing the forwarding packet delay by employing a computation method for weighted queues. To deal with the packets at the end of the queue, packet delay-based link weight assignment is done.

Hu and Gharavi [19] have found paths using a greedy approach. The hop count is based on the lengths of the shortest paths.

It is seen that, in the recent past, BS schemes have gained much attention [20]. A distributed gradient-based backpressure framework [21] is proposed for WSNs to deal with optimization of energy and throughput. Venkataraman et al. [22] have designed a BS scheme that incorporates trust factor into link weights. Zheng et al. [23] have propounded a network model, wherein the scheduling is dealt in the task layer. Each task comes with a scheduling policy, followed by an application-dependent transmission.

3 Existing System

Two existing schemes are discussed in this section namely, Last in First out (LIFO) Backpressure Scheduling (BS) scheme and Event-Aware Backpressure Scheduling (EABS) scheme.

3.1 Last in First Out (LIFO) Backpressure Scheduling (BS) Scheme

Packets in a network may be regular or important. Some packets may be important as they pertain to emergency events and demand faster transmission.

LIFO BS scheme focuses on changing the traditional FIFO queue to LIFO [9]. Routing decisions are based on the difference in queue backlogs which is acceptable for network with low loads. This may lead to longer and loop path problem. The packets transmitted in a network can either be Emergency packets (E-packets) or Regular packets (R-packets). The end-to-end delay increases with the increase in the number of packets. If a common scheduling scheme is proposed to handle both the packet types under LIFO BS scheme, E-packets will not be effectively serviced [12].

The E-packets are scheduled through shortest paths in a non-congested network. They are delivered to the destination at the earliest. However, long paths, even paths with loops may be selected in the traditional BS scheme. As the network load increases, the numbers of loops also increase, leading to more end-to-end delay. Guaranteeing the performance of a scheduling algorithm for E-packets is challenging [13].

3.2 Event-Aware Backpressure Scheduling (EABS)

Event-Aware Backpressure Scheduling (EABS) scheme chooses the next-hop node by integrating shortest path selection with the BS scheme. The E-packets are sent through shortest paths. The difference in queue backlogs is considered to circumvent congestion. The end-to-end delay is reduced with an increase in the forwarding percentage [14]. E-packets are to be delivered to the destination within the stipulated time. For example, in case of fire, packets with temperature details should be forwarded quickly. The number of E-packets is limited. Distance-weighted method reduces the end-to-end delay of packets. E-packet is given priority and forwarded to the nodes closer to the destination. When multiple E-packets are to be forwarded, the one with the least deadline is chosen to be forwarded [24].

4 Proposed System

Selfish nodes degrade the performance of a network. The proposed Secure Event-Aware Backpressure Scheduling (SEABS) scheme considers the E-packets in a network that is prone to selfish node attacks and assigns more weight to them. In EABS, though the queuing delay is reduced for E-packets, the dropping of packets is not taken into consideration. The proposed SEABS scheme deals with the selfish node attack.

Assume that some intermediate nodes act as selfish nodes and drop the Route Request (RREQ) packets. The E-packets should be capable of traversing through the network and reaching the destination quickly. In the proposed scheme, two queues namely, M/M/1 or M/M/n are used. The RREQs that are broadcast are put into the M/M/n queue, and the Route Responses (RREPs) are scheduled in an M/M/1 queue, as the E-packets are unicast when selfish node behavior is sensed in the network.

The scheduler is supported by a packet classifier, which classifies the packets as R-packets and E-packets. The E-packets are given priority, and the scheduler forwards the packets through the nodes with better trust value.

The E-packets are scheduled using higher priority M/M/1 queue. R-packets are scheduled using M/M/n Queue.

The backlog of queue 'Q' at a node at time slot '$t + 1$' is given by '$Q_{\mathrm{BT}}(t + 1)$'.

$$Q_{\mathrm{BT}}(t+1) = Q_{\mathrm{TR}}(t) + \mathrm{Reg}_{\mathrm{DES}}^{Q}(t) + \mathrm{Emg}_{\mathrm{DES}}^{Q}(t) \qquad (1)$$

where

$Q_{\mathrm{BT}}(t)$ Queue backlog at time slot 't'
$Q_{\mathrm{TR}}(t)$ Queue transmission rate at time slot 't'
$\mathrm{Reg}_{\mathrm{DES}}^{Q}(t)$ Number of R-packets arriving at a queue
$\mathrm{Emg}_{\mathrm{DES}}^{Q}(t)$ Number of E-packets arriving at a queue

The selected queue 'q_{sel}' is given by,

$$q_{\mathrm{sel}} = \left\{ Q_{\mathrm{TR}}^{\mathrm{SRC}}(t) - \frac{\mathrm{HC}_{\mathrm{DES}} - \mathrm{HC}_{\mathrm{SRC}}}{\mathrm{HC}_{\mathrm{SRC}}} . Q_{\mathrm{TR}}^{\mathrm{DES}}(t) \right\} \qquad (2)$$

where

$Q_{\mathrm{TR}}^{\mathrm{SRC}}(t)$ Queue backlog at source at time slot 't'
$Q_{\mathbf{TR}}^{\mathbf{DES}}(t)$ Queue backlog at destination at time slot 't'
$\mathrm{HC}_{\mathrm{SRC}}$ The hop-count at source
$\mathrm{HC}_{\mathrm{DES}}$ The hop-count at destination

The trustworthiness of node 'y' by node 'x' is given by the following equation.

$$\mathrm{Trust}_{x}^{y} = \frac{m_c + \mu\, m_s}{m_t + \mu\, m_a} \qquad (3)$$

where

μ Probability that the link remains active and correct
m_c Transmitted message found to be correct
m_s Successful transmissions
m_t Total number of messages not destined but transmitted by 'x' to 'y'
m_a Total number of attempted transmissions

After selecting the forwarding queues, the distance weight 'w' can be expressed as,

$$w = \frac{\left(\mathrm{HC}_{\mathrm{DES}}^{q_{\mathrm{sel}}} - H_{\mathrm{SRC}}^{q_{\mathrm{sel}}}\right)}{H_{\mathrm{SRC}}^{q_{\mathrm{sel}}}} \tag{4}$$

where

$\mathrm{HC}_{\mathrm{DES}}^{q_{\mathrm{sel}}}$ The hop-count at the source for the selected queue
$H_{\mathrm{SRC}}^{q_{\mathrm{sel}}}$ The hop-count at destination for the selected queue

Weighted queue backlog difference '$w(t)$' is given by,

$$w(t) = \mathrm{Trust}_x^y \cdot \left\{\left(Q_{\mathrm{BT}}^{q_{\mathrm{sel}}}(t) - w * Q_{\mathrm{BT}}^{q_{\mathrm{sel}}}(t)\right)\right\}. \tag{5}$$

where

$Q_{\mathrm{BT}}^{q_{\mathrm{sel}}}(t)$ Queue Backlog at time slot 't' of the selected queue

The node with maximum '$w(t)$' is selected as the next-hop node.

5 Performance Evaluation

Network Simulator-2 (Ns-2) is used for simulations. A total of 50 mobile nodes are randomly deployed in a rectangular area 1000 m × 1000 m.

The capacity of the wireless channel capacity is taken as 2 Mbps. The simulation period is taken as 50 sec.

The performance is analyzed by varying the number of selfish nodes. The packet size is fixed to 512 bytes. The random waypoint model is used.

The performance of the proposed Secured Event-Aware Backpressure Scheduling (SEABS) scheme is compared with the existing Last in First out (LIFO) Backpressure Scheduling (BS) scheme and Event-Aware Backpressure Scheduling (EABS) scheme. The performance is analyzed in terms of Packet Delivery Ratio (PDR), throughput, end-to-end delay and routing overhead. It is seen that the proposed SEABS offers better PDR and throughput, involving less end-to-end delay and routing overhead in contrast to the existing BS and EABS schemes (Figs. 1, 2, 3, 4).

The proposed SEABS offers 1.5 times and 1.2 times better PDR in contrast to the existing BS and EABS scheduling schemes respectively. Similarly, it yields 3 and 1.8 times better Throughput when compared to BS and EABS scheduling schemes respectively. The existing schemes BS and EABS schemes respectively involve 2 and 1.5 times more delay when compared to the proposed SEABS scheme. Similarly, they involve 1.8 and 1.6 times more routing overhead in contrast to SEABS.

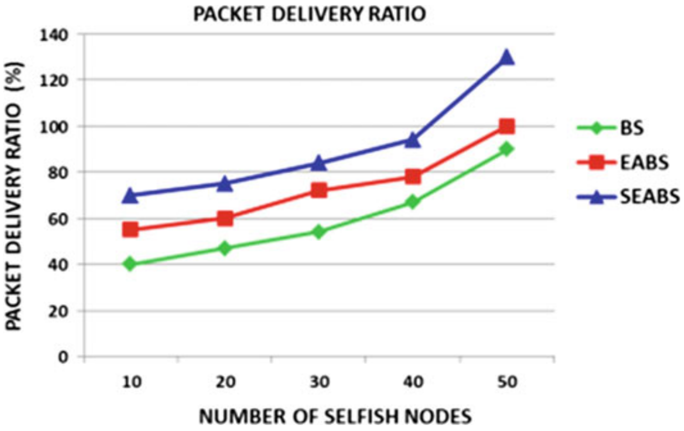


Fig. 1 Packet delivery ratio

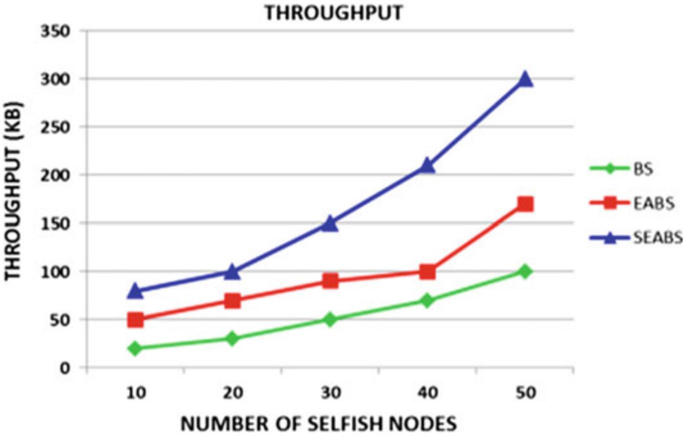


Fig. 2 Throughput

6 Conclusion

In this paper, a Secured Event-Aware Backpressure Scheduling (SEABS) scheme is propounded. The performance of the proposed system is compared with Last in First out (LIFO) Backpressure Scheduling (BS) scheme and Event-Aware Backpressure Scheduling (EABS) scheme. As the next-hop nodes are selected based on the weights computed by taking the trust value and the weighted queue backlog difference, the proposed scheme outperforms the existing schemes.

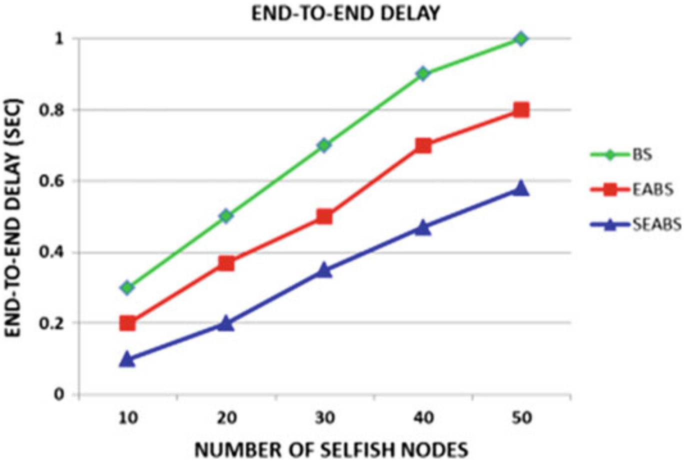


Fig. 3 End-to-end delay

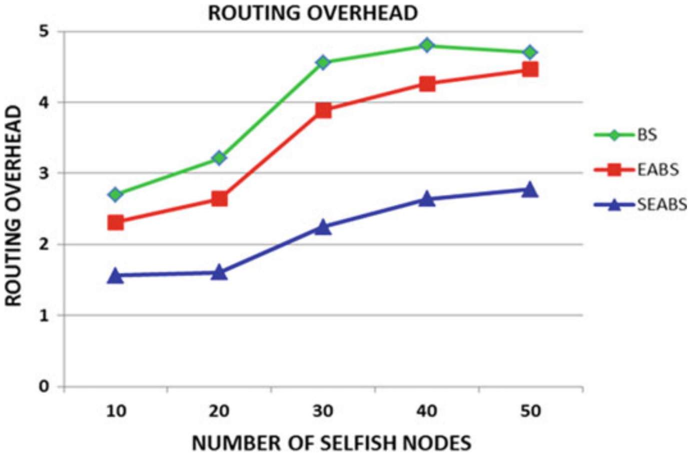


Fig. 4 Routing overhead

References

1. Chen H, Jia X, Li H (2011) A brief introduction to IoT gateway. In: Proceedings of the IET International Conference on Communication Technology and Application, ICCTA, pp 610–613
2. Ian I, Su W, Sankarasubramaniam Y, Cayirci E (2002) Wireless sensor networks: a survey. Comput Netw 38(4):393–422
3. Abbasi AA, Younis M (2011) A survey on clustering algorithms for wireless sensor networks. Comput Commun 30(14–15):2826–2841
4. Boyinbode O, Le H, Takizawa M (2011) A survey on clustering algorithms for wireless sensor networks. Int J Sp-Based Situat Comput 1(2–3):130–136

5. Das SK, Saha BJ, Chatterjee PS (2014) Selfish node detection and its behavior in WSN. In: Proceedings of the IEEE International Conference on Computing Communication and Networking Technologies, ICCCNT, pp 1–6
6. Tassiulas L, Ephremides A (1992) Stability properties of constrained queueing systems and scheduling policies for maximum throughput in multihop radio networks. IEEE Trans Autom Control 37(12):1936–1948
7. Neely MJ, Modiano E, Rohrs CE (2005) Dynamic power allocation and routing for time-varying wireless networks. IEEE J Sel Areas Commun 23(1):89–103
8. Andrews M, Kumaran K, Ramanan K, Stolyar A, Vijayakumar R, Whiting P (2000) CDMA data QoS scheduling on the forward link with variable channel conditions. Bell Lab Tech Memo 4:1–45
9. Moeller S, Sridharan A, Krishnamachari B, Gnawali O (2010) Routing without routes: the backpressure collection protocol. In: Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Network, pp 279–290
10. Liu L, Jiang J, Shu L, Hancke G (2017) Analysis of energy-efficient connected target coverage algorithms for industrial wireless sensor networks. IEEE Trans Industr Inf 13(1):135–143
11. Majidi A, Mirvaziri H (2014) BDCC: backpressure routing and dynamic prioritization for congestion control in WMSNs. Int J Comput Netw Inf Secur 6(5):29
12. Sridharan A, Moeller S, Krishnamachari B (2005) Investigating backpressure based rate control protocols for wireless sensor networks, vol 7. USC EE CENG technical report, CENG-2008
13. Neely MJ, Urgaonkar R (2009) Optimal backpressure routing for wireless networks with multi-receiver diversity. Ad Hoc Netw 7(5):862–881
14. Dvir A, Vasilakos AV (2010) Backpressure-based routing protocol for DTNs. ACM SIGCOMM Comput Commun Rev 40(4):405–406
15. Ying L, Srikant R, Towsley D, Liu S (2011) Cluster-based back-pressure routing algorithm. IEEE/ACM Trans Netw (TON) 19(6):1773–1786
16. Alresaini M, Sathiamoorthy M, Krishnamachari B, Neely MJ (2012) Backpressure with adaptive redundancy. In: Proceedings of the IEEE International Conference on Backpressure with Adaptive Redundancy, pp 2300–2308
17. Huang L, Moeller S, Neely MJ, Krishnamachari B (2013) LIFO-backpressure achieves near-optimal utility-delay tradeoff. IEEE/ACM Trans Netw 21(3):831–844
18. Ji B, Joo C, Shroff NB (2013) Delay-based back-pressure scheduling in multihop wireless networks. IEEE/ACM Trans Netw 21(5):1539–1552
19. Hu B, Gharavi H (2014) Greedy backpressure routing for smart grid sensor networks. In: Proceeding of the 11th IEEE Consumer Communications and Networking Conference, pp 32–37
20. Jiao Z, Yao Z, Zhang B, Li C (2014) A distributed gradient-assisted anycast-based backpressure framework for wireless sensor networks. In: Proceedings of the IEEE International Conference on Communications (ICC), pp 2809–2814
21. Jiao Z, Zhang B, Gong W, Mouftah H (2015) A virtual queue-based back-pressure scheduling algorithm for wireless sensor networks. EURASIP J Wirel Commun Netw 1(35)
22. Venkataraman R, Moeller S, Krishnamachari B, Rao TR (2015) Trust–based backpressure routing in wireless sensor networks. Int J Sensor Netw 17(1):27–39
23. Zheng X, Cai Z, Li J, Gao H (2017) A study on application-aware scheduling in wireless networks. IEEE Trans Mob Comput 16(7):1787–1801
24. Qiu T, Qiao R, Wu DO (2018) EABS: an event-aware backpressure scheduling scheme for emergency Internet of Things. IEEE Trans Mob Comput 17(1):72–84

Cost-Based Meta-Task Scheduling Algorithm for MultiCloud Computing (CBMTSA)

B. J. Hubert Shanthan and L. Arockiam

Abstract MultiCloud plays vital role in providing the heterogeneous types of resources to the user on-demand with minimum cost and time. Resource management and scheduling act as an influential aspect in the improvement of the performance of the MultiCloud environment. Scheduling deeds a considerable challenge in the distributed heterogeneous multiple cloud systems. The existing min-min algorithm is suitable for smaller number of tasks. The tasks are allocated to the VMs with high-processing speed. The proposed cost-based meta-task scheduling algorithm (CBMTSA) is feasible for the passive autonomous task-based scheduling for MultiCloud systems. Scheduling and rescheduling are two stages involved in this algorithm. Scheduling stage is used to allocate the tasks to the high-speed VMs. Makespan value is computed in the scheduling stage. The computed makespan is an outset value for rescheduling the tasks. The rescheduling stage is used to reschedule the tasks from high-speed VMs to low-speed VMs. The CBMTSA surpasses the existing min-min algorithm. Makespan, execution cost, and cloud server utilization ratio are the metrics considered in this algorithm.

Keywords MultiCloud · CBMTSA · Makespan · Execution cost · Scheduling stage · Rescheduling stage

1 Introduction

A cloud is an inevitable technology which provides the storage, computation, and communication resources to the users connected to the Internet [1]. In MultiCloud the cost is charged based on the usage of the VMs [2]. Platform as a Service (PaaS) [3], Software as a Service (SaaS) [4] and Infrastructure as a Service (IaaS) are three major models in the cloud [5]. The SaaS model is designed for the end users to access

B. J. Hubert Shanthan (✉) · L. Arockiam
Department of Computer Science, St. Joseph's College, Trichy, India
e-mail: hshanthan@gmail.com

L. Arockiam
e-mail: larockiam@yahoo.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_131

through simple Web browser. IaaS service model is used for storage, computation, and communication process among the virtual machines [6]. PaaS model is used for the programmers to deploy and create their applications [7]. In the MultiCloud, there are heterogeneous types of service providers with different pricing schemes based on the SLA terms between CSPs and CSUs. MultiCloud is an advancement of the cloud and it offers different types of cloud services from other cloud service providers [8]. The resource scheduling in MultiCloud is a tedious process. The solutions obtained from the existing heuristics-based approaches do not reduce both cost and time simultaneously [9]. The failure rate is comparatively less in the static scheduling, when compared with the dynamic scheduling algorithms [10].

The main purpose of this article is to propose a cost-Based meta-task scheduling algorithm (CBMTSA) curtails the execution rate of the virtual machines in the MultiCloud environment and increase the resource utilization of the cloud server. Section 2 narrates the existing literature works of the algorithm. Section 3 elucidates the propounded CBMTSA. The Sect. 4 gives results and discussions and Sect. 5 concludes with research findings and list out the future directions of research.

2 Related Works

Lucas-Simarro et al. [11] proposed an optimized service deployment scheduling strategy for MultiCloud environment. The modular broker architecture was suggested based on cost optimization criteria. The user constraints such as budget, performance, VM placement, and load balancing under different environmental conditions such as static and dynamic were considered in their approach.

Kokilavani and Amalarethinam [12] articulated an independent and load-balanced scheduling algorithm to dwindle the makespan and to use the underutilized cloud servers. The algorithm comprised of two stages namely scheduling and rescheduling. The scheduling stage was used to allocate and execute the tasks to the VM with minimum execution time. The computed makespan value in the scheduling stage was used as a threshold value.

Tang et al. [13] developed a mechanism for sharing the service provider resources. The mechanism was designed to analyze the demands of the user and the pricing policy was designed for the anticipating users. Nash equilibrium was a strategy based on the game theory developed to solve the bidding problem among the users.

Amalarathinam et al. [14] enlightened a customer-oriented cost-based task scheduling algorithm for cloud. The algorithm was designed with economical cost of the user. The price was computed based on the duration the tasks were executed in the virtual machines. Monetary cost and makespan were used to improve the performance of the cloud systems.

Panda et al. [15] proffered a scheduling algorithm for allocation of the tasks in the MultiCloud environment. Makespan and rate of utilization of the cloud server are the parameters considered in this algorithm. Allocation, matching, and scheduling are the stages used in that algorithm. The VMs with minimum competition time are selected in the matching stage. The first-come-first-serve (FCFS) basis mechanism was followed in the matching stage. The allocation stage acted as an intermediate layer between matching and scheduling stage.

Elkader [16] expressed a novel computation-based load balance aware scheduling algorithm for cloud. The algorithm comprised of two stages namely fill and spill. The fill scheduler was used to schedule the task based on the VM capabilities in each cloud. The spill scheduler was used to execute tasks with the VM.

Mei et al. [17] analyzed a mechanism to increase profit among the cloud service providers. The pricing model was designed for short-term and long-term users. The existing pricing model was emphasized on long-term users. The cloud broker acted as a MultiCloud agent between service provider and the cloud clients. The optimized multi server M/M/N/n queuing model was used to configure the VM for the user-defined tasks. The queuing model helped to analyze the factor that affects the profit in the cloud service providers.

Ali and Alam [18] suggested a mechanism for the allocation of the tasks with minimum length to the VM with minimum completion time. The algorithm was developed based on the standard min-min algorithm. The algorithm emphasized on the smaller tasks and the waiting times for larger tasks were increased exponentially.

Mihailescu and Teo [19] extended dynamic pricing scheme for the MultiCloud environment. Dynamic pricing scheme increased the efficiency of resource usage by the customers. The pricing strategies were decided based on the resource demand of the customers. The VMs in the cloud are charged high when the customer requests are peak on demand. The VMs are charged with less cost when the customer requests are low.

Ibrahim et al. [20] enlightened a task-based scheduling algorithm for the MultiCloud. The pricing model for MultiCloud is designed in this algorithm. The algorithm was designed to decrease the makespan and minimize the execution time and cost. The pricing models of the companies such as Google Cloud and Amazon EC2 were used in this algorithm.

3 Cost-Based Meta-Task Scheduling Algorithm (CBMTSA)

Figure 1 depicts the working mechanism of CBMTSA algorithm.

Scheduling and rescheduling are vital stages involved in this algorithm.

The input values are given in the form of ETC matrix for the scheduling stage.

The ETC matrix comprises of execution time of the tasks given by the user to the virtual machines.

The formula for ETC calculation is given by the Eq. (1)

$$\mathrm{ETCij} = \mathrm{ISi/PSj} \tag{1}$$

where ISi denotes millions of instructions (MI) which is also known as task length and PSj denotes millions of instructions per second (MIPS) also known as virtual

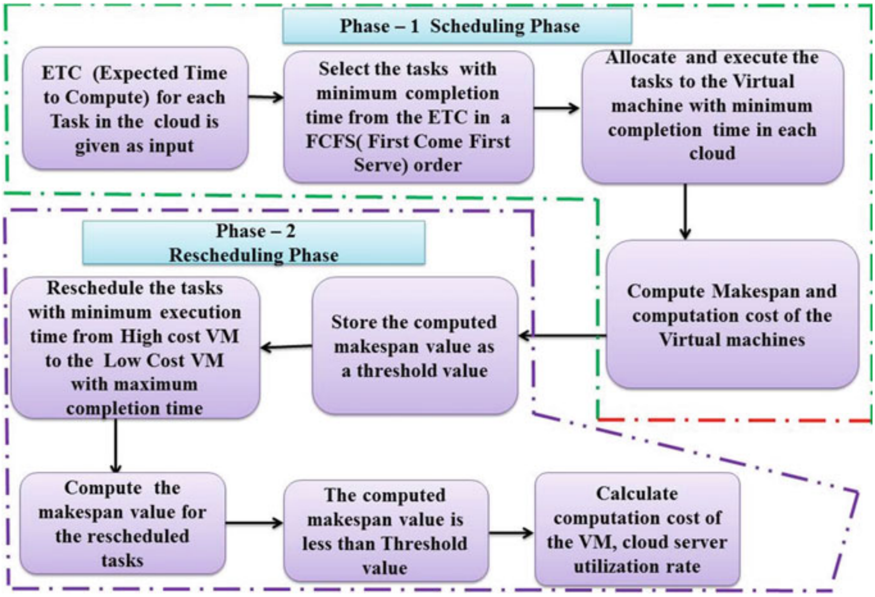

Phase – 1 Scheduling Phase
ETC (Expected Time to Compute) for each Task in the cloud is given as input
Select the tasks with minimum completion time from the ETC in a FCFS(First Come First Serve) order
Allocate and execute the tasks to the Virtual machine with minimum completion time in each cloud
Compute Makespan and computation cost of the Virtual machines
Phase – 2 Rescheduling Phase
Store the computed makespan value as a threshold value
Reschedule the tasks with minimum execution time from High cost VM to the Low Cost VM with maximum completion time
Compute the makespan value for the rescheduled tasks
The computed makespan value is less than Threshold value
Calculate computation cost of the VM, cloud server utilization rate

Fig. 1 Methodological diagram of CBMTSA algorithm

machine processing speed. The completion time of each task is computed by the sum of expected execution time and the virtual machine ready time. The formula for completion time is given below in the Eq. (2).

$$\mathrm{CTij} = \mathrm{ETCij} + \mathrm{Rti} \tag{2}$$

where ETCij denotes the ETC matrix and RTi denotes the ready time of each virtual machine available in the MultiCloud.

The tasks from the ETC matrix are scheduled based on their minimum completion time. The tasks with minimum execution time are allocated to the VM with minimum completion time. Cloud manager acts as a centralized controller between cloud user and cloud service provider. Cloud manager selects tasks from the ETC matrix based on the first-come-first-serve (FCFS) order.

The manager computes the completion time of all the VMs in the MultiCloud environment. After the computation process, cloud manager selects the VMs that give minimum earliest completion time and assign the task to the VMs of the corresponding cloud. The ready time for all VMs in the clouds is updated after the allocation of the tasks. The makespan value of VMs in each cloud is computed. The makespan value is obtained from the scheduling stage of each VM and stored as an outset value. The cost computed is based on the processing speed of the VMs. The VMs with high-processing speed requires more cost and it completes the tasks within minimum time. The low-speed VMs require very low cost and their completion time is extremely high when compared to the high-speed VM.

The cloud VMs server utilization ratio is given below in the Eq. (3).

$$\Pr\left(\mathrm{VM}_j\right) = \sum_{j=1}^{n} \mathrm{VM}_j * \mathrm{Cost} \tag{3}$$

where VMj denotes the computation time of the *j*th virtual machine. Cost denotes the price of the accessing VMs in the cloud. In the scheduling stage, the high-speed VMs are emphasized and they are too expensive. It is not suitable for the users who demand low-cost resources. So, to overcome this conflict, rescheduling stage is introduced to reduce the execution cost of the VM and to increase the idle utilization of VMs. The cloud manager selects the tasks with minimum execution time from the high-speed VMs. The selected task is rescheduled to low-speed VMs with maximum completion time. The computed makespan value in the rescheduling stage must not exceed the threshold value computed in the scheduling stage. The rescheduling stage balances the load among the virtual machines in the cloud and also reduces the overall maximum completion time of the tasks. The formula for cloud resource utilization ratio calculation is given by the Eq. (4)

$$\mathrm{CRU}_{ij} = \frac{\mathrm{suc}_i}{\mathrm{Num\_T}} * 100 \tag{4}$$

where Suc_i denotes the successive completion of tasks in each cloud, Num_T represents the number of tasks available in the clouds.

3.1 Proposed CBMTSA Algorithm for MultiCloud Computing

```
Input: Total Number of tasks, VMs, Clouds
Output: Makespan, Cost, Average Resource Utilization
Step 1: Start
Step 2: Input the VMs, clouds, processing speed, and task
Step 3: CALL CB SCHEDULE
Step 4: CALL CB RESCHEDULE
Step 5: Stop
CB-SCHEDULE
Step 1: Check the condition whether the queue lengths of the tasks are not empty
Step 2: Check the total number of VMs and clouds are not left empty
Step 3: Arrange the tasks in the increasing order
Step 4: The tasks with minimum completion time are selected and executed in the VMs from each cloud
Step 5: Compute Makespan and execution cost of the Virtual machines in the clouds.
Step 6: Stop
```

CB-RESCHEDULE

Step 1: The condition whether the Meta tasks and Virtual machines are not empty
Step 2: Compute the completion time of the tasks
Step 3: Arrange the tasks in decreasing order
Step 4: The tasks with Maximum Execution time are selected and executed in VMs with high processing speed
Step 5: Reallot the selected task from high processing speed VM to low capacity VMs
Step 6: The ready time of the VMs are updated frequently
Step 7: Calculate the Makespan and execution cost of VMs
Step 8: Calculate Cloud server utilization ration
Step 9: Stop

4 Results and Discussion

Table 1 represents the sample ETC matrix for 10 tasks, 4 virtual machines, and 2 clouds. The cloud C1 represents Amazon EC2 cloud and the cloud C2 represents Google Cloud Console.

Table 2 details the scheduling stage of the CBMTSA algorithm. The stage uses batch mode of scheduling mechanism where all the tasks are executed parallely in the available virtual machines.

Table 3 shows the rescheduling stage of the CBMTSA algorithm. The rescheduling process reduces the makespan, computation cost of the VMs, and also increases the cloud server utilization.

Table 4 illustrates the makespan value of the rescheduling stage. The makespan value in the rescheduling stage is 28.96. The total cost incurred in the rescheduling stage is 191.13$.

5 Conclusion

A cost-based meta-task scheduling algorithm (CBMTSA) articulated to schedule the independent tasks. The algorithm focuses mainly to reduce the computation cost of the virtual machines. The existing min-min algorithm is suitable for smaller number of tasks and it merely schedules the tasks to the VMs with high-processing power. The min-min algorithm gives more importance to the high-speed VM cloud service providers and it also costs high for the cloud consumers. The low-speed VM or the virtual machine with minimum processing speed is not utilized in the existing algorithm. To overcome the challenges, the proposed CBMTSA algorithm is developed and the importance is given for both the low-speed VMs and the high-speed VMs of the MultiCloud environment. The proposed CBMTSA comprised of

Table 1 Expected time to compute (ETC) matrix

Cloud	Virtual machines (seconds)	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10
Cloud C1	VM1	11.6	6.92	0.61	6.01	1.99	15.63	72.7	16.17	1.2	12.66
	VM2	8.21	4.82	0.43	4.18	1.4	10.87	50.86	11.44	0.84	8.78
Cloud C2	VM3	9.82	5.77	0.51	5	1.67	13.1	61.45	13.68	1.02	10.49
	VM4	6.73	1.23	0.18	1.28	0.09	7.78	18.4	8.11	0.42	4.29

Table 2 Scheduling phase

Cloud	Virtual machines (seconds)	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10
C1 (Amazon)	VM1 (1S)				6.01						
	VM2 (3S)		4.82							0.84	8.78
C2 (Google cloud)	VM3 (2S)			0.51		1.67			13.68		
	VM4 (4S)	6.73					7.78	18.4			

Table 3 Rescheduling phase

Cloud	Virtual machines (seconds)	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10
C1 (Amazon)	VM1 (1S)	11.6			6.01					1.2	
	VM2 (3S)		4.82								8.78
C2 (Google cloud)	VM3 (2S)			0.51		1.67	13.1		13.68		
	VM4 (4S)							18.4			

Table 4 Makespan results in the rescheduling phase

Clouds	C1		C2	
Virtual machines	VM1	VM2	VM3	VM4
Makespan values (seconds)	18.81	13.6	28.96	18.4

two stages, namely scheduling stage and rescheduling stage. The scheduling stage uses min-min scheduling algorithm. The rescheduling stage is introduced to underrate the VMs computation cost and the makespan value of the VMs. The rescheduling stage selects the task-VM pair with minimum execution time and it is rescheduled to the task-VM pair with maximum completion time. The experimental results from the simulator prove that the proposed algorithm surpasses the existing min-min algorithm in terms of metrics such as computation cost, makespan, and cloud server utilization rate. This algorithm enables the consumer to access the cloud resources at minimum cost and time.

References

1. Mell P, Grance T (2009) The NIST definition of cloud computing. National Institute of Standards and Technology, Information Technology Laboratory, Technical Report Ver. 15
2. Munteanu VI, Sandru C, Petcu D (2014) MultiCloud resource management: cloud service interfacing. J Cloud Comput 3(1):1–23
3. Buyya R, Broberg J, Goscinski A (2012) Cloud computing principles and paradigms. Wiley
4. Lahmar F, Mezni H (2018) Multicloud service composition: a survey of current approaches and issues. J Soft Evolut 1–24 (Wiley)
5. Shanthan BJH, Arockiam L (2018) Resource based load balanced min min algorithm (RBLMM) for static meta task scheduling in cloud. In: International conference on advances in computer science and technology. Int J Eng Technol Spec Issue 1–8
6. Jane VA, Shanthan BJH, Arockiam L (2018) Survey of algorithms for scheduling in the cloud: in a metric perspective. Int J Comput Sci Eng 6(2):66–70
7. Shanthan BJH, VinothKumar DA, Karthigai Priya G, Arockiam L (2017) Scheduling for Internet of Things applications on cloud: a review. Imp J Inter Discip Res (IJIR) 1(3):1649–1653
8. Shanthan BJH, Arockiam L (2018) Spell aware meta task scheduling algorithm (SAMTSA) for MultiCloud. Int J Sci Res Comput Sci Appl Manag Stud 7(4):1–5
9. Stephen A, Shanthan BJH, Ravindran D (2018) Enhanced round Robin algorithm for cloud computing. Int J Sci Res Comput Sci Appl Manag Stud 7(4):1–5
10. Shanthan BJH, Arockiam L (2018) Rate aware meta task scheduling algorithm for MultiCloud computing (RAMTSA). IOP conference series. J Phys Conf Ser 1142:012001, pp 1–10. https://doi.org/10.1088/1742-6596/1142/1/012001
11. Lucas-Simarro JL, Moreno-Vozmediano R, Montero RS, Llorente IM (2012) Scheduling strategies for optimal service deployment across multiple clouds. Future generation computer systems, Elsevier, pp 1431–1441
12. Kokilavani T, Amalarethinam DD (2011) Load balanced min-min algorithm for static meta-task scheduling in grid computing. In: Int J Comput Appl 20(2):43–49
13. Tang L, He S, Li Q (2016) Double-sided bidding mechanism for resource sharing in mobile cloud. IEEE J Cloud Comput 1–11
14. Amalarathinam DIG, Beena TLA (2015) Customer facilitated cost-based scheduling (CFCSC) in cloud. Procedia, Elsevier, pp 660–667

15. Panda SK, Gupta I, Jana PK (2015) Allocation-aware task scheduling for heterogeneous MultiCloud systems. In: Second international symposium on big data and cloud computing challenges, Procedia computer science, Elsevier, pp 176–184
16. Elkader AA (2017) Enhancing the minimum average scheduling algorithm (MASA) based on makespan minimizing. Artifi Intell Mach Learn J 17(1):9–13 (Delaware)
17. Mei J, Li K, Tong Z, Li Q, Li K (2018) Profit maximization for cloud brokers in cloud computing. IEEE Trans Parallel Distrib Sys 1–18
18. Ali SA, Alam M (2018) Resource-aware min-min (RAMM) algorithm for resource allocation in cloud computing environment. arXiv:1803.00045
19. Mihailescu M, Teo YM (2010) Dynamic resource pricing on federated clouds. In: 2010 10th IEEE/ACM international conference on cluster, cloud and grid computing, IEEE, pp 513–518
20. Ibrahim E, El-Bahnasawy NA, Fatma A (2017) Task scheduling algorithm in cloud computing environment based on cloud pricing models. In: IEEE 2016 world symposium on computer applications and research, pp 65–71

Implementation of Low-Cost Mobile Robot for Rescue Challenges

Rajesh Kannan Megalingam, Shree Rajesh Raagul Vadivel, Prasant Kumar Yadav, Katta Nigam, Ravi Teja Geesala and Ruthvik Chanda

Abstract One of the biggest challenges in today's world in the field of robotics is rescue robotics. This paper aims in the design and implementation of mobile robot for the search and rescue operations in natural calamities such as earthquakes. These rescue robots reduce the response time as compared to humans and help in getting information to the rescue teams using sensors. The main issues concerned with the present rescue robots are modularity, mobility, durability, and robustness. The robot is designed considering all the required parameters in SOLIDWORKS CAD and simulated in Rviz with the control interface as Robot Operating System (ROS). The robot is designed in such a way that it can do all the mobility tasks like climbing stairs, moving on uneven terrains, step fields, sand, and gravel, as well as exploring tasks like finding the injured victims and hazardous signs.

Keywords Multi-terrain robot · Robot Operating System (ROS) · Graphical user interface (GUI) · Solidworks · Tele-operated

R. K. Megalingam · S. R. R. Vadivel · P. K. Yadav · K. Nigam · R. T. Geesala (✉) · R. Chanda
Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India
e-mail: ramsrimanasi@gmail.com

R. K. Megalingam
e-mail: rajeshkannan@ieee.org

S. R. R. Vadivel
e-mail: shreerajgul@gmail.com

P. K. Yadav
e-mail: yprasant0@gmail.com

K. Nigam
e-mail: 123nigam.k@gmail.com

R. Chanda
e-mail: ruthvikchanda1999@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_132

1 Introduction

The first use of the rescue robots was actually during the World Trade Center (WTC) collapse in 2001 though research was going on this field in the past for many years. The main goal of these robots is to reduce the number of deaths during disasters by surveying the areas which humans are not permitted until the fire is off. Effective communication without delay and errors between the rescue team and the robot plays a key role in these situations. The rescue robot presented in this research has both wired connectivity and wireless connectivity. Robot Operating System (ROS) establishes both wired and wireless connectivities through master–slave protocol between the control system and the rescue robot. Both wired and wireless systems have its own advantage and disadvantage in rescue operations. Wired connection provides reliable connection and does not provide any interference as in wireless communication. The advantage of this is that it provides constant and faster speed compared to wireless connection because of one-to-one connection. But the disadvantage of wired connectivity is that they may not be so effective in disaster scenarios because their reliability is not so good as compared to wireless. For example, if the cables are damaged, the re-installation process would be difficult in those disaster areas. This rescue robot carries several cameras, lidar, kinect, and other sensors. Several sensors are used in this robot to know the environmental conditions of the unknown disaster area. The sensors like IMU and encoders used are for locating or identifying the robot motion. The robot is tele-operated from the controller station with a user interface and a controller.

The innovative idea of the mechanical design with the flipper mechanism and main drive mechanism is an advantage for this robot. The center of mass is well adjusted so that it does not topple while climbing stairs and any other uneven rough disaster terrain. The compactness and small size of the design allow the robot to enter small voids and collect useful information where humans cannot enter. The agility of the robot also holds an important aspect during these disaster situations where even seconds of time is valuable.

2 Related Works

The paper [1] presents the development of crawler rescue robot with two flipper arms which has the capability to move in all the four directions, i.e., not only up and down (pitching motion) but also left and right (yawning motion). The flipper arm in this robot is 2DOF. Paper [2] proposes the new design of the mobile robot which aims to perform on different types of terrains and disaster areas in a balanced way. This robot has the capability to run on any rocky and sandy area and to climb the stairs. The paper [3] discusses an exploration algorithm for the rescue robots in which it automatically maps the unknown environment while driving. Paper [4] presents the method for multi-hop communication in robots, i.e., in detail, a method by which GUI using ROS can be constructed to operate the robot is introduced. Paper [5] describes the machine learning techniques for quick training of robots for navigational tasks and facilitating remote operations. In paper [6], the authors described the design and control of the four-flipper tracked robot. They even described the control mechanisms and the multifunctionality capabilities of the robot. Paper [7] describes the fixed path algorithm and the behavior of the autonomous wheelchair using simulation technique. In paper [8], they proposed the gesture-based wheel chair and its unconventional methods of navigation which are simple and cost-effective. The two methods include Line Following Navigation (LFN) and Location Aware and Remembering Navigation (LARN). Paper [9] describes about the Interactive Remote Robot Operation (IRRO) for reducing the ambiguities and abstracting them. The authors used iterative closest points (ICP) algorithm for the results of collision detection in the reconstructed 3D map. In paper [10], the authors developed a dummy robot for the evaluation of the safety measures and features of the robot. With this testing using the dummy robot, the safety concerns that exist with the humans are removed. Paper [11] describes the study of risk assessment of the rescue robot which helps to improve the reliability of the rescue robot. The assessment is done by considering each subsection in the robot and then combining everything together. Paper [12] proposes the configuration of sensors to be used in the robot which is used to measure the environmental conditions of the disaster areas like CO_2 sensor, temperature sensor, and smoke particle density.

3 Architecture

Figure 1 gives the detailed process on how Robot Operating System (ROS) acts as the main platform to control the robot. The ROS forms the base for the architecture of our robot. Through ROS nodes and topics, the required data is exchanged. The user can control the robot from workstation wirelessly. The control station system is the master, and the robot is slave. The control is divided into different blocks.

3.1 User Interface

The user interface block consists of a graphical user interface. The GUI is built on ROS plug-in RQT.

The GUI consists of two camera view blocks which give a good perception of the robot surroundings from the cameras fixed on the robot. For establishing communication between the robot and control station, the computers should be connected to an external router through ethernet cables. By running both the systems under fixed ROS_MASTER_URI with an IP address, we can establish a bridge between

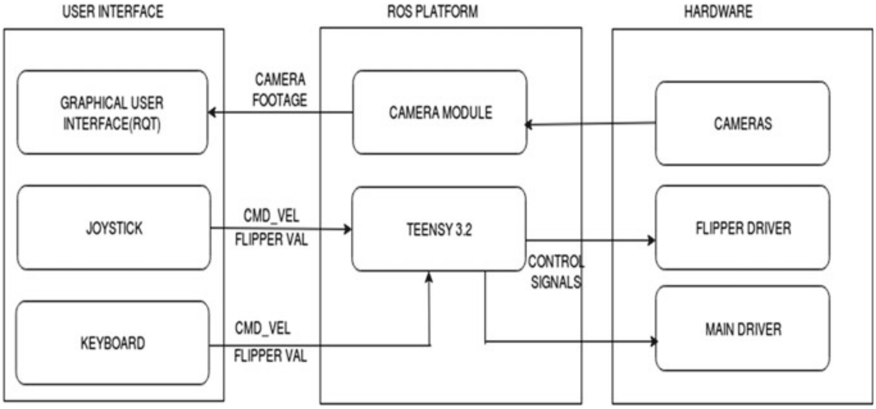


Fig. 1 Architectural diagram of the system

the control station and the robot. By this bridge, data communication takes place. A customized joystick is designed for the control of robot. The user can also control the robot through keyboard.

3.2 ROS Platform

ROS platform deals the transmission of data through nodes. Nodes are processes that perform computation. Our robot control system usually comprises many nodes. Nodes exchange data through ROS-defined messages. These messages are routed via a transport system with publish/subscribe semantics through topics. We used USB_CAM ROS package to transmit camera data. These transmitted data are seen in GUI. And the user input values through joystick are published by JOY_NODE in topic names CMD_VEL and FLIPPER_VAL. These transmitted messages are subscribed by SERIAL_NODE, and by establishing serial communication between PC and Teensy, the received data is transmitted to Teensy board. Further computation of data takes place in Teensy board which produces the corresponding PWM values and drive signals to the motor drivers and flipper drivers.

3.3 Hardware

One of the most important aspects of navigating mobile robots is perception. The robot was remotely operated with the help of cameras (logitech c310), encoders, and IMU data. We placed a camera at the front end of the robot with a rotary base made of servo to get a 180° view, +90° to the right and −90° to the left, while the robot is in motion. We had one camera each at the corner end, at the back placed horizontally, mounted over a moving servo base with possible rotation of 90° (45° to each side). This arrangement covers all the possible views around all the sides of the robots, and most importantly, we can also view the positioning of the flippers. The camera live feed was streamed back to the operating station with the help of ROS nodes and ROS usb_cam package. Since the bandwidth required for the data was huge, there was a delay in the communication network so we had to compress the video data to reduce the video latency. The video data was compressed by a node written in C++ which dropped some of the unnecessary features of the images of each frame in a way that the video quality is maintained to a standard.

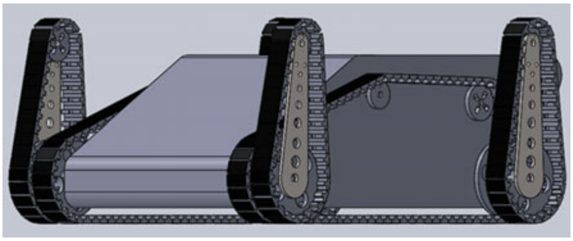
The encoder data and IMU were used to keep track of the motion and the distance moved by the robot in the GUI. The IMU data was used to measure if we have a rolling on a inclined surface. The encoder data also helped to maintain our differential drive of the main drive without any error. The data was transmitted from the Teensy 3.2 through a topic/odom to the GUI node to keep a note of the sensor (IMU, encoders) readings.

The flippers were designed to perform a movement of 360° around the center position of the main drive motor shaft. To enable an easy control of the flippers, they were assigned with some poses. The first pose consists of all the four flippers pointing vertically up and 90° from the ground. This pose was used to move it quickly through the plane surfaces since the area of contact is minimum in this pose. The second pose was where the front two flippers were vertically inclined at an angle 45° from the ground, and others were vertically 90° from the ground. This position was mostly used for climbing up inclined surfaces. The third position was where all the flippers laid horizontally to the ground making an angle of zero degree. This position was fully stretched position of the robot.

4 Design and Implementation

Body as shown in Figs. 2 and 3 was designed on SOLIDWORKS platform with two drive wheels and four flippers, and mild steel was the material used in manufacturing the robot. Chain sprocket power transmission mechanism is followed in robot mobility where electrical power of the motor was converted into momentum which was essential for the body movement. The dimensions of the robot body are 60 ×

Fig. 2 Left corner view



30 × 25 cm (length × width × height); the electronics for the body are placed from opening designed to and fro of the robot. The center of the mass of the body was sustained with care to avoiding the toppling of the robot; two E-bike motors with 24 V input supply and 350 W power help to drive the body. The shaft of the E-bike motors was replaced with 10-mm shaft which was further coupled with 50-mm pitch circle sprocket (Fig. 4). Worm-geared window motors (Fig. 5) with 12 V voltage supply were used for the flipper movement, and 12-mm shaft was passed through these motors which is coupled to 5 mm thickness and 150-mm-long flipper plate. Two sprockets of 100 mm pitch circle diameter are coupled through welding concentrically to maintain common axis of rotation around the shaft that has been passed through the center for the flipping mechanism. One sprocket was mated with main drive chain where the other was mated for flipper chain. Main sprocket is parallel to two more sprockets; one of them was attached to drive sprocket which was coupled to E-bike motor, and the other sprocket was coupled to rotary encoder. The side plate of body which was manufactured with 5 mm MS had the PCD of the E-bike and encoder to couple. Sprocket-to-sprocket distance for the center chain was 54 cm, and the length of the flipper was 15 cm (distance between main sprocket and dummy sprocket of flipper). Flipper adjusting mechanism is taken care by the flipper plate which was designed and manufactured with the PCD for the center shaft and 50-mm pitch circle flipper dummy sprocket axis. Lidar placement and mountings for pan and tilt for camera were taken care during the manufacturing. 1-mm metal sheet was used for body cover of the robot, 3 cm ground clearance for the robot, and the 380 cm × 320 cm area for placements of components (camera, lidar) above the body.

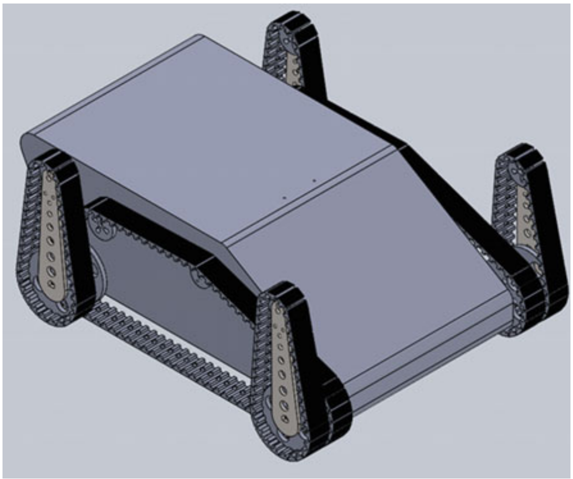


Fig. 3 Right-top corner view

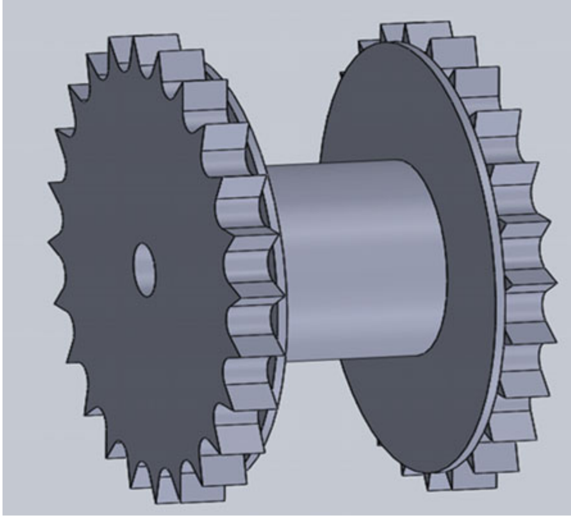


Fig. 4 Coupled sprockets

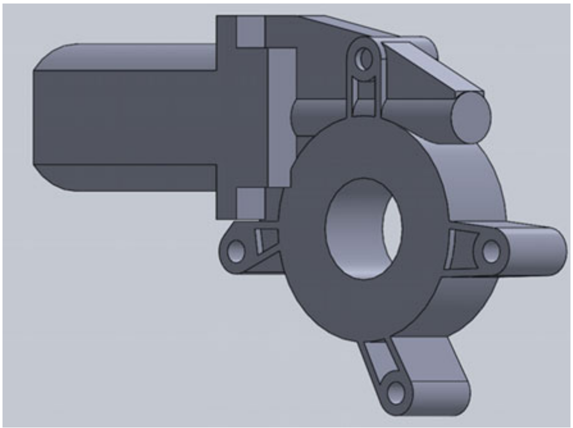


Fig. 5 Worm-geared window motor

5 Experiments and Results

The robot was tested in an arena which resembles the real-world scenario. The operator controls the robot using a customized joystick board. The operator controlled wirelessly through the video visual from the cameras fixed on the robot. The design and solid metallic body gave extra stability. To inspect the feasibility of the proposed design, we tested the robot under different terrain scenarios, A. 25° ramps, B. uneven terrain, C. 45° steep terrain, and D. parallel rail bars.

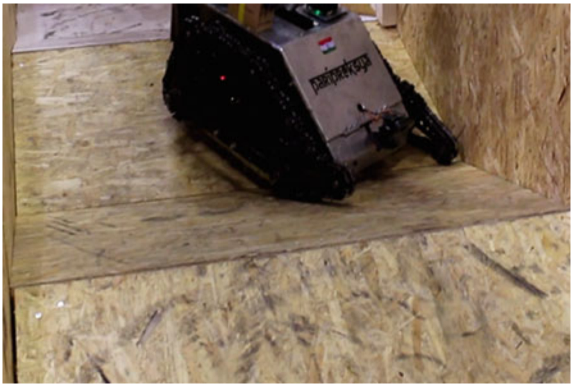


Fig. 6 Robot tested on rail bars

5.1 25° Ramps

This test scenario contains 25° continuous ramps. According to the tested results, the robot was able to drive freely as shown in Fig. 6. The flipper mechanism gave extra support to modify the pose to the altered terrain environments.

5.2 Uneven Terrains

This test scenario consists of varied angles and dimensions of ramps on the trot continuously. Despite these harsh terrains, the robot drives freely.

5.3 45° Steep Terrain

The arena consists of a 45° steep track. With the high torque E-bike motor and the flipper mechanism, it will be to go up the 45° steep track.

5.4 Parallel Rail Bars

This test consists of two parallel rail bars of breath equal to the dimension of the main track width of the robot. With the PID control, speed parameter of the robot is controlled by which we were able to drive the robot on the parallel rails without deviating its path as shown in Fig. 7.

These scenarios will test the robustness and flexibility of the robot in harsh environments.

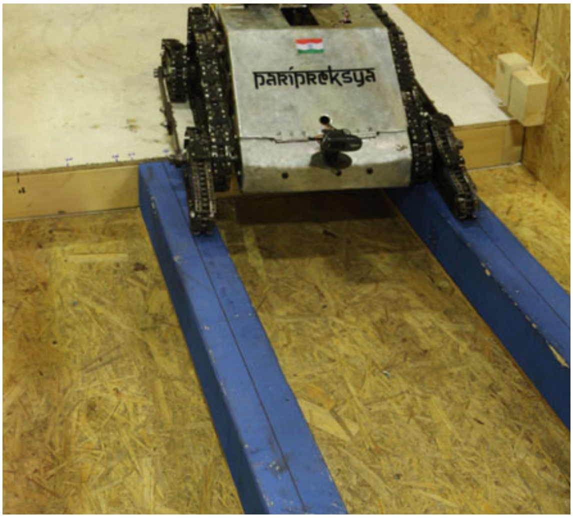


Fig. 7 Robot tested on ramps

6 Future Works

Robot flipper mechanism needs to be modified so it adds more stability to reach steepy terrains too. Gearbox should be redesigned to meet the required torque for flipper. The drive chain mechanism needs to be modified since axial motion of the main sprockets causing the chain to slip from the sprocket. This problem can be restrained by installing cross-roller bearing mechanism. Efficiency of power transmission through sprocket chain mechanism is way less than direct coupling of the motor to sprocket so it is necessary to avoid chain drive mechanism. Chassis material needs to be fabricated with aluminum to diminish the weight issues. Track belt needs to be installed with nylon pulley instead of direct chain and sprocket since robot is lacking friction in few situations. This also reduces the weight of the robot. As the robot runs many modules, processor speed of the microprocessor needs to be improved to decrease delay in transmission of camera footage. Communication range of the robot also needs to be improved for extending the exploration limits of the robot, needs to extend research on autonomous navigation which maps the surrounding and navigate itself, and needs to include image-processing module for detecting hazard signs and victims.

7 Conclusion

Although there is an enormous amount of research in the field of search and inspection robotics, this paper provides the working and design of a low-cost mobile robot which can be used for search and inspection in disaster-hit areas. The mobility of the robot through rough terrains or through debris left in the disaster hit areas is impactful and considerable because of its flipper mechanism. The body design developed is very suitable for disaster sites because of its rigidity and durability. The power consumption of the robot is also less compared to other robots used for exploration purposes. The paper also acknowledges the fact that during disaster situation, we need a reliable communication network between the operator and the robot. Thus, the Ubiquiti antenna deployed near the controller station provides strong and reliable connection between the master and slave interface. The Wi-Fi adapter used is configured with an operating bandwidth of 5 GHz so that we do face a transmission delay in the network. We also focus on the setup time for the robot which is considerably small in our case. Setup time needs to be very small for these rescue robots.

Acknowledgements We thank Amrita University and Humanitarian laboratory for providing us this wonderful opportunity to direct our thoughts into a real prototype. We thank Dr. Rajesh Kannan Megalingam for providing us space and infrastructure needed to complete this project. We thank all the people who have helped us to accomplish this project in time.

References

1. Sato N, Torii K, Morita Y (2013) Development of crawler type rescue robot with 2 DOF flipper arms. In: IEEE/SICE international symposium on system integration
2. Gupta VK, Gupta AK (2013) Design and development of six-wheeled multi-terrain robot. In: International conference on control, automation, robotics and embedded systems (CARE)
3. Wirth S, Pellenz J (2007) Exploration transform: a stable exploring algorithm for robots in rescue environments. In: IEEE international workshop on safety, security and rescue robotics
4. Shin S, Yoon D, Song H, Kim B, Han J (2017) Communication system of a segmented rescue robot utilizing socket programming and ROS. In: 14th international conference on ubiquitous robots and ambient intelligence (URAI)
5. Moridian B, Kamal A, Mahmoudian N (2018) Learning navigation tasks from demonstration for semi-autonomous remote operation of mobile robots. In: IEEE international symposium on safety, security, and rescue robotics (SSRR)
6. Kovačić Z, Cukon M, Brkić K, Vasiljević G, Mutka A, Miklić D, Vuglec F, Rajković I Design and control of a four-flipper tracked exploration and inspection robot. In: 21st mediterranean conference on control and automation
7. Megalingam RK, Vishnu GB, Pillai M (2015) Development of intelligent wheelchair simulator for indoor navigation simulation and analysis. In: IEEE international women in Engineering (WIE) conference on electrical and computer engineering 2015 (WIECON-ECE 2015), BUET, Bangladesh
8. Megalingam RK, Manoj PS, Nammily NR (2011) Unconventional indoor navigation: gesture based wheelchair control. In: International conference on indoor positioning and indoor navigation (IPIN'2011), Guimarães, Portugal
9. Shin YD, Park JH, Jang GR, Yoon JS, Baeg MH (2013) Interactive remote robot operation framework for rescue robot. In: IEEE International symposium on safety, security, and rescue robotics (SSRR)
10. Nallathambi DJ (2018) Comprehensive evaluation of the performance of rescue robots using victim robots. In: 4th international conference on control, automation and robotics (ICCAR)

11. Phuengsuk R, Suthakorn J (2016) A study on risk assessment for improving reliability of rescue robots. In: IEEE international conference on robotics and biomimetics (ROBIO)
12. Ferreira NL, Couceiro MS, Araújo A, Rocha RP (2013) Multi-sensor fusion and classification with mobile robots for situation awareness in urban search and rescue using ROS. In: IEEE international symposium on safety, security, and rescue robotics (SSRR)

Smog Detection and Pollution Alert System Using Wireless Sensor Network

Manita Rajput, Mrudula Geddam, Priyanka Jondhale and Priyanka Sawant

Abstract Air pollution is a primary concern for humankind, causing asthma attacks, wheezing, shortness in breath, etc. In the Indian subcontinent, air quality decreases, increasing smog due to the burning of crops to prepare for the harvest and emissions from the vehicles, etc. Driving becomes difficult due to this blinding smog. To overcome these problems, a wireless network of sensors is proposed along the expressways and in public places to measure the smog. A personal area network (PAN) network of motes is set up. Using MQ135 and DSM501a sensors, smog pollutants are measured. Contiki OS and Cooja simulator are used to analyze the performance of network by emulating nodes using Tmote Sky. The nodes in this PAN are mounted over the lamp posts on the bridge to collect information of various pollutants and send the acquired data to a mote. This mote acts as a central node in the wireless sensor network (WSN) and transmits data over user datagram protocol (UDP). Finally, the parameters with warning messages are displayed at the entrance of bridges for the drivers to create a safety alert. The future aspect of this project may lead to displaying the messages at short intervals along the whole bridge with updated values. Also, the recorded data can be stored on the server and after a certain period of time, the data can be analyzed to observe the number of pollutants being emitted, and measures can be taken accordingly.

Keywords Smog · TmoteSky TelosB motes · Cooja simulator · Contiki OS · AQI

M. Rajput · M. Geddam · P. Jondhale (✉) · P. Sawant
Department of Electronics and Telecommunication Engineering, Fr. C.R.I.T, Vashi, Navi, Mumbai, India
e-mail: priyankajondhale12@gmail.com

M. Rajput
e-mail: manita.rajput@fcrit.ac.in

M. Geddam
e-mail: mrudula17geddam@gmail.com

P. Sawant
e-mail: piyasawant10@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_133

1 Introduction

Smog is a form of air pollution that mainly consists of ozone, along with harmful substances like sulfur dioxide, nitrogen dioxide, carbon monoxide, and PM10s, which can find their way deep into the lungs. Smog is a harmful mixture of fog, dust and air pollutants such as nitrogen oxides and volatile organic compounds which combine with sunlight to form a dense layer of ground-level ozone. Ozone when present high in the atmosphere is beneficial, but when nearer to the ground, it can cause irritating health effects. The name was constructed by putting together the words ‘smoke’ and ‘fog’ [1]. Smog can be caused by

- Large amounts of coal burning in an area.
- Slash-and-burning of crops (a major source in Delhi).
- Smog-forming pollutants generated from automobile exhausts, power plants, fireworks, even paint, hair spray, charcoal starter fluid, and plastic popcorn packaging.
- The formation of smog is also closely linked with temperature, sunshine, and calm winds [2]. The most affected people by smog are children, infants, the elderly, those with cardiac and respiratory problems like asthma, emphysema, chronic bronchitis, those who stay outdoors for long periods of time, and people with unusual susceptibility to ozone. Smog can cause minor issues like eye and throat irritation, headaches. But when exposed to it over a long period of time, smog can have a much worse effect on the body [3]. The basic structure of a WSN [4] is shown in Fig. 1. It shows a cluster node to which many sensors are connected. The data fetched by sensors is collected by the cluster node. It is then sent to the sink node which can be a mote, Raspberry Pi, or an Arduino, etc. This sink node collects, packetizes, and sends the data to the monitoring system (microprocessor). It processes the data packets and displays them for the specified application.

In order to achieve the aim of the project, a detailed block diagram of the proposed solution is shown in Fig. 1b which shows the actual interconnection of various components. Motes collect and transfer data using four stages: collecting the data, processing the data, packaging the data, and communicating the data. Each mote

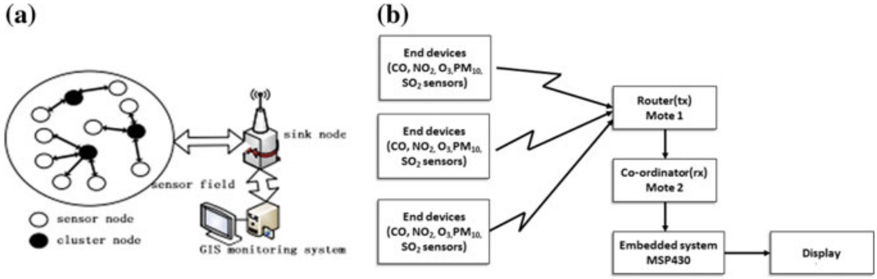

(a)
sink node
sensor field
sensor node
cluster node
GIS monitoring system
(b)
End devices (CO, NO$_2$, O$_3$, PM$_{10}$, SO$_2$ sensors)
End devices (CO, NO$_2$, O$_3$, PM$_{10}$, SO$_2$ sensors)
End devices (CO, NO$_2$, O$_3$, PM$_{10}$, SO$_2$ sensors)
Router(tx) Mote 1
Co-ordinator(rx) Mote 2
Embedded system MSP430
Display

Fig. 1 **a** Basic structure of a WSN [5]. **b** Implemented block diagram of system collects data using various types of sensors connected to it. A network of sensors which can measure the smog contents is proposed for the measurement of smog and alerts the crowd along the expressways and public places.

2 Motivation

In India and its neighboring countries, air quality decreases just about every year at the onset of winter as farmers begin burning their crops to prepare for their new harvest and emissions from the vehicles, etc. The air quality index in Delhi—which measures the concentration of toxic particulate matter in the air—had shot up to 451 in the year 2017, as compared to the ideal value of 100. This led to the motivation to think about developing a system hoping to address this problem at an affordable price and alert the drivers and pedestrians about the current environmental conditions.

3 Literature Review

3.1 Present Smog Detection Devices in India

Many devices are available in the market presently, to measure the level of smog. Some of them were studied by us. Described below are the present smog detection devices available in the market. A brief description of them and drawbacks, as to why they cannot be used effectively, accompanies them.

(1) Air Pollution and Fog Detection through Vehicular Sensors: This paper demonstrates that LIDAR technology, already onboard for the purpose of autonomous driving, can be used to improve the weather condition recognition when compared with a camera-only system. System has the combination of a front camera and a LIDAR laser scanner used as a sensor instrument set for air pollution and fog recognition [6].

(2) Air Pollution Detection Based On Head Selection Clustering And Average Method From Wireless Sensor Network: The proposed method mainly focus on longer sustain time period of sensor network, effective processing of collected information, and less overhead in routing information between sensor nodes [7].

(3) Smart Environment Monitoring Beacon-Cluj Napoca University, Romania: The purpose of Smart Environment Monitoring Beacon is to present a beacon created for monitoring the environmental conditions, like weather parameters, air

pollution, sound levels, and UV radiation index using GSM module [8].

(4) 6LoWPAN Network Using Contiki Operating System: This paper focuses on the working of 6LoWPAN network using Contiki tool with Cooja simulator and various WSN's simulation tools [9].

(5) Wireless Sensor Network-Based Pollution Monitoring System in Metropolitan Cities [10]: This study proposes air pollution and monitoring model which detects pollution in the air on the basis of data mining algorithm [11]. Bluetooth module is used to connect the controller with client, and the client connects with the server via web services. Wireless sensors are used to the amount of gases [12].

(6) Urban Air Pollution Monitoring System with Forecasting Models: A system for monitoring and forecasting urban air pollution is presented in this paper. The system uses low-cost air quality monitoring motes that are equipped with an array of gaseous and meteorological sensors [13].

(7) Into the SMOG: Stepping Stone to Centralized WSN Control: This paper illustrates that wireless sensor networks (WSNs) can lead to improve network lifetime, benefit reliability, help to diagnose and localize network failures. A complete network topology model that scales and reacts to the network dynamics that occur in low-power wireless networks is proposed [14].

3.2 Census Data

According to the World Health Organization (WHO) global air pollution database released in Geneva, India has 14 out of 15 most polluted cities in the world—Kanpur being the worst with a PM 2.5 concentration of 173 $\mu g/m^3$. Soot, dust, ozone, and sulfur oxides are a growing threat for billions of people around the world. A whopping nine in ten people on Earth breathe highly polluted air, and more than 80% of urban dwellers have to endure outdoor pollution that exceeds health standards, according to the WHO's World Global Ambient Air Quality Database. The measurements and calculations as of 2016 revealed that 11 of the 12 cities with the highest levels are located in India. Figure 2 shows Kanpur, India, population 3 million, tops the list with a yearly average of 319 $\mu g/m^3$ of PM 2.5, the most hazardous particle commonly measured [15].

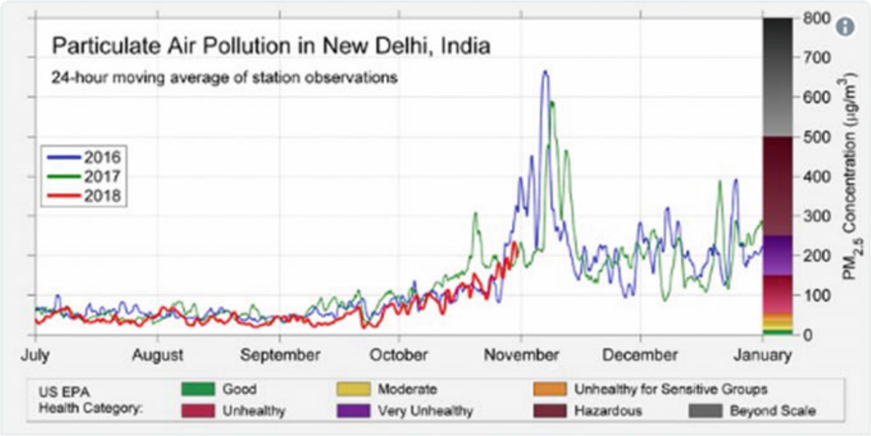


Fig. 2 Air pollution in Delhi, India, with PM 2.5 calculation, Survey 2016 [15]

4 Software Implementation Using Cooja

4.1 Simulated Results of InBuilt Sensors

The Tmote Sky MTM-CM5000 consists of inbuilt temperature, light, and humidity sensors. SHT-11 sensor measures both humidity and temperature. Initially, the sensors are activated, and then the current temperature and humidity values are fetched. The obtained values are then displayed on an LCD display.

Using the above flow process shown in Fig. 3, we implemented the software model for measuring temperature and humidity by setting up two nodes in Cooja software, and the obtained results are shown in Fig. 4a, b.

4.2 Simulated Results of External Sensor Interfacing

For measuring levels of PM10 and CO_2 pollutants, external sensors, namely DSM501a and MQ135 are interfaced with the mote. These sensors are powered using the VCC and GND pins of motes itself. The sensor senses the analog values and gives it to the mote via ADC 0/1 pin. The acquired measures are voltage values, are later converted to ppm or µg/m^3, and are then displayed as the sensor output. The values are updated after a particular delay provided in the code. Figure 5 shows the flowchart for interfacing external sensors with the motes. It illustrates the port configuration and the way to proceed with this interfacing. The software model for the same and obtained results are given in Fig. 6a, b where CO_2 pollutant is measured by implementing a software representation.

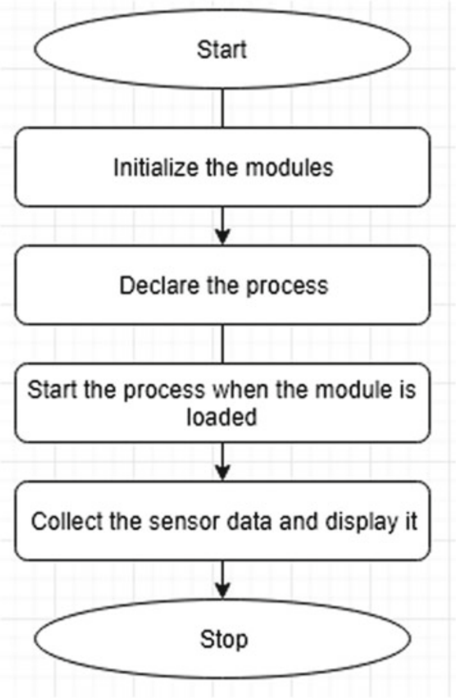
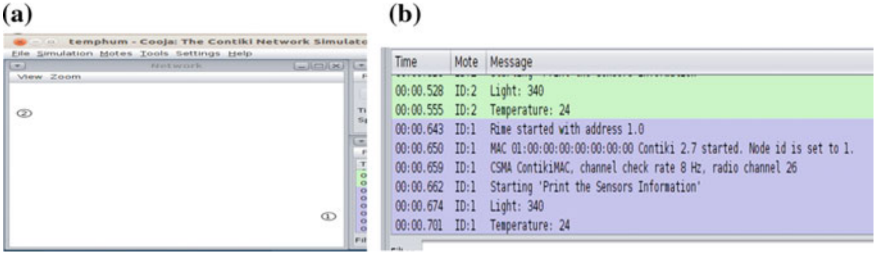

Start
Initialize the modules
Declare the process
Start the process when the module is loaded
Collect the sensor data and display it
Stop

Fig. 3 Flowchart for temperature and humidity measurement using inbuilt sensors


(a)
temphum - Cooja: The Contiki Network Simulato
File Simulation Motes Tools Settings Help
Network
View Zoom
2
1
(b)

```
Time       Mote  Message
00:00.528  ID:2  Light: 340
00:00.555  ID:2  Temperature: 24
00:00.643  ID:1  Rime started with address 1.0
00:00.650  ID:1  MAC 01:00:00:00:00:00:00:00 Contiki 2.7 started. Node id is set to 1.
00:00.659  ID:1  CSMA ContikiMAC, channel check rate 8 Hz, radio channel 26
00:00.662  ID:1  Starting 'Print the Sensors Information'
00:00.674  ID:1  Light: 340
00:00.701  ID:1  Temperature: 24
```

Fig. 4 a Setting two nodes in Cooja to check temperature and humidity. b Obtained node output showing ideal temperature and light values

In Figure 7a, b, PM_{10} pollutant's software simulation is done using Cooja simulator.

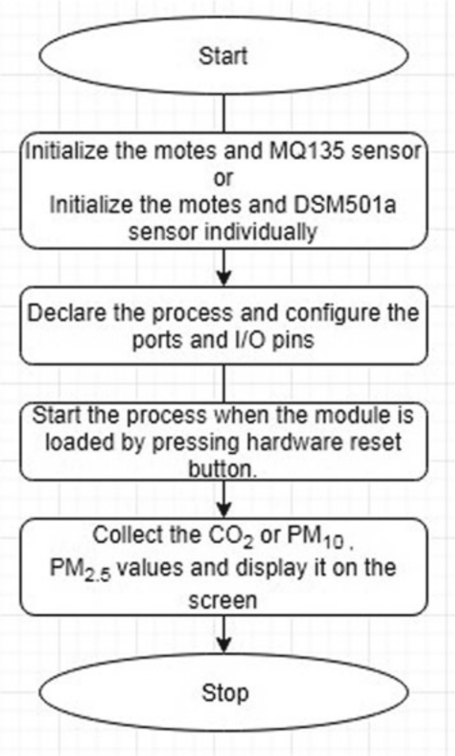
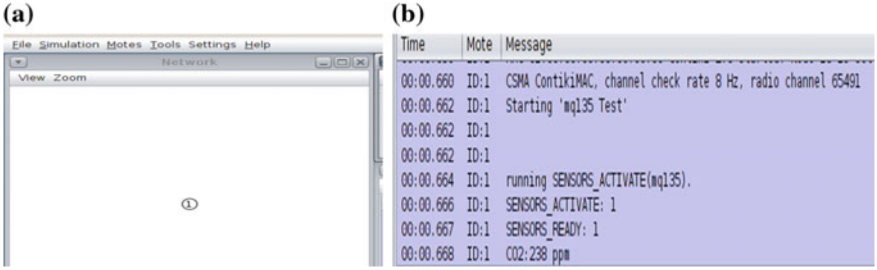

Start
Initialize the motes and MQ135 sensor or Initialize the motes and DSM501a sensor individually
Declare the process and configure the ports and I/O pins
Start the process when the module is loaded by pressing hardware reset button.
Collect the CO_2 or PM_{10}, $PM_{2.5}$ values and display it on the screen
Stop

Fig. 5 Flowchart for measuring pollutants values from external sensors (MQ135 and DSM501a)

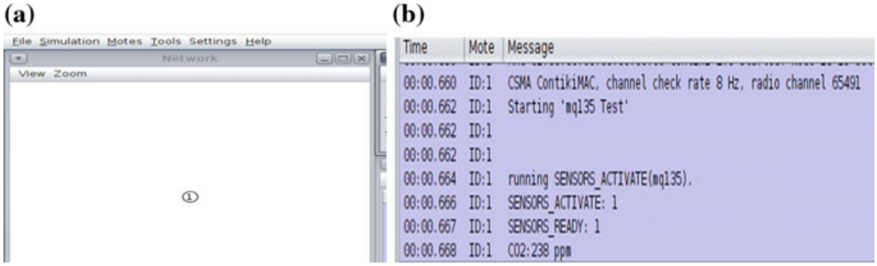


```
Time       Mote  Message
00:00.660  ID:1  CSMA ContikiMAC, channel check rate 8 Hz, radio channel 65491
00:00.662  ID:1  Starting 'mq135 Test'
00:00.662  ID:1
00:00.662  ID:1
00:00.664  ID:1  running SENSORS_ACTIVATE(mq135).
00:00.666  ID:1  SENSORS_ACTIVATE: 1
00:00.667  ID:1  SENSORS_READY: 1
00:00.668  ID:1  CO2:238 ppm
```

Fig. 6 **a** Setting up a node in Cooja for measuring CO_2. **b** Node output showing CO_2 value in ppm

4.3 *Creation of a PAN Network in Cooja*

After obtaining the measured values, they are required to be transmitted to the central mote in order to get displayed. For this data transmission, a PAN network of two or more motes is created, and using unicast or multicast routing, the obtained data packets are routed in the network. In this case, a network of only two motes is



```
Time        Mote  Message
00:00.660   ID:1  CSMA ContikiMAC, channel check rate 8 Hz, radio channel 65491
00:00.662   ID:1  Starting 'mq135 Test'
00:00.662   ID:1
00:00.662   ID:1
00:00.664   ID:1  running SENSORS_ACTIVATE(mq135).
00:00.666   ID:1  SENSORS_ACTIVATE: 1
00:00.667   ID:1  SENSORS_READY: 1
00:00.668   ID:1  CO2:238 ppm
```

Fig. 7 **a** Setting up a node in Cooja for measuring PM_{10} pollutant value. **b** Node output showing PM_{10} value in $\mu g/m^3$

created, and so unicasting is used. Figure 8a shows the flowchart for creating a virtual simulation of motes and sensors in PAN configuration. In this configuration, all the pollutant values are obtained simultaneously.

The two motes work in client–server configuration, their PAN arrangement is done in VMware software, and the obtained simulated results are shown in Fig. 9a, b.

4.4 Hardware Implementation with Motes and Sensors

Taking the analog output from the sensor nodes, we got the following results. We considered various real-life inputs that may be received by the sensors under different weather conditions. Mote1 is working as a client while Mote2 is working as a server; their individual transmissions and PAN configuration outputs with internal as well as external sensors are provided in Fig. 10.

Figure 10a depicts the function of one of the motes as a client sensing and transmitting data packet to the mote at other end while Fig. 10b shows another mote working as a server receiving all the data packets from the client and routing them in the PAN configuration.

Figure 10c shows the MQ135 sensor's measured CO_2 output when interfaced with the mote. Its obtained results are shown in ppm while Fig. 10d gives DSM501a sensor's real-time measured PM_{10} pollutant value in $\mu g/m^3$. This arrangement itself gave fairly reliable output and creates a PAN configuration with two motes in it, one sending data packets and the other receiving it making a client–server configuration. These sensors send their data to mote via the ADC pin available on MTM-5000 mote and are processed with the help of MSP430 microprocessor's timers and counters utilities.

We have actually implemented the real-time PAN configuration of two Tmotes and sensors powered using USB slots of laptop. Figure 10a shows the real-time hardware implementation of the same. In this implementation, Mote1 acts as a client and has MQ135 and DSM501a sensors interfaced with it. Sensors collect the data and give data packets to client mote. These packets are then processed by onboard

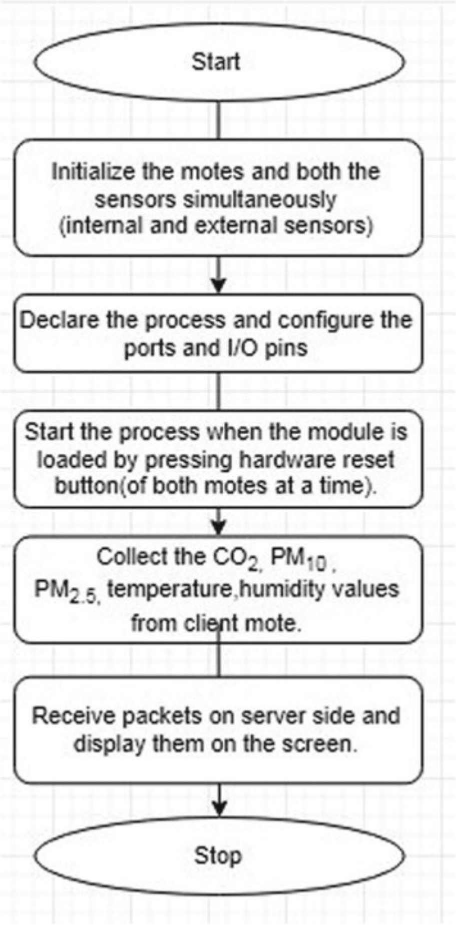
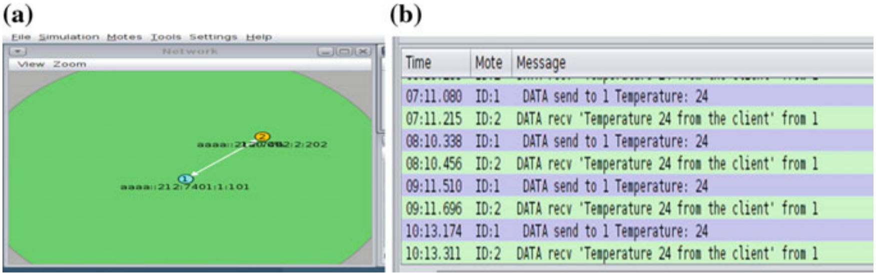
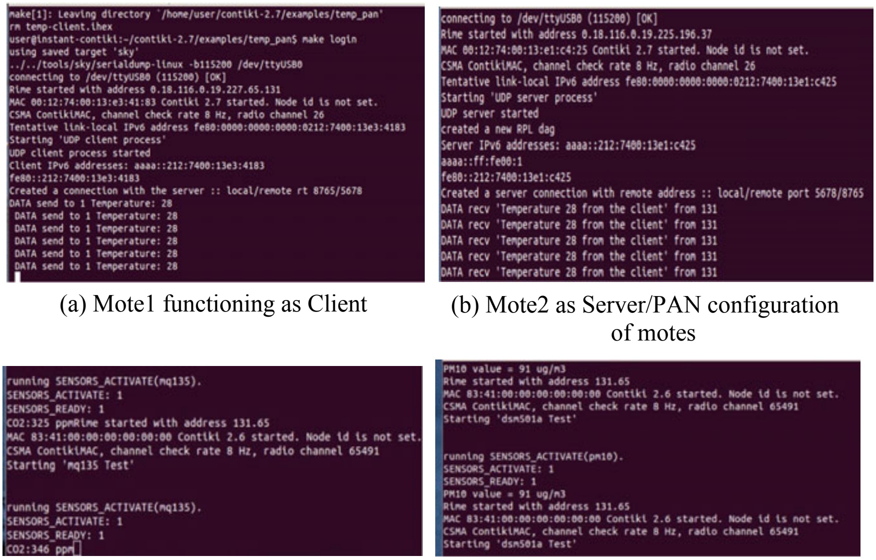

Start
Initialize the motes and both the sensors simultaneously (internal and external sensors)
Declare the process and configure the ports and I/O pins
Start the process when the module is loaded by pressing hardware reset button(of both motes at a time).
Collect the CO$_2$, PM$_{10}$, PM$_{2.5}$, temperature,humidity values from client mote.
Receive packets on server side and display them on the screen.
Stop

Fig. 8 Flowchart for creating a PAN consisting of motes and sensors



```
Time       Mote  Message
07:11.080  ID:1   DATA send to 1 Temperature: 24
07:11.215  ID:2  DATA recv 'Temperature 24 from the client' from 1
08:10.338  ID:1   DATA send to 1 Temperature: 24
08:10.456  ID:2  DATA recv 'Temperature 24 from the client' from 1
09:11.510  ID:1   DATA send to 1 Temperature: 24
09:11.696  ID:2  DATA recv 'Temperature 24 from the client' from 1
10:13.174  ID:1   DATA send to 1 Temperature: 24
10:13.311  ID:2  DATA recv 'Temperature 24 from the client' from 1
```

Fig. 9 **a** Setting up two motes in PAN configuration using Cooja software. **b** Data transmission and reception between both the motes in Cooja output window



```
make[1]: Leaving directory `/home/user/contiki-2.7/examples/temp_pan'
rm temp-client.ihex
user@instant-contiki:~/contiki-2.7/examples/temp_pan$ make login
using saved target 'sky'
../../tools/sky/serialdump-linux -b115200 /dev/ttyUSB0
connecting to /dev/ttyUSB0 (115200) [OK]
Rime started with address 0.18.116.0.19.227.65.131
MAC 00:12:74:00:13:e3:41:83 Contiki 2.7 started. Node id is not set.
CSMA ContikiMAC, channel check rate 8 Hz, radio channel 26
Tentative link-local IPv6 address fe80:0000:0000:0000:0212:7400:13e3:4183
Starting 'UDP client process'
UDP client process started
Client IPv6 addresses: aaaa::212:7400:13e3:4183
fe80::212:7400:13e3:4183
Created a connection with the server :: local/remote rt 8765/5678
DATA send to 1 Temperature: 28
 DATA send to 1 Temperature: 28
 DATA send to 1 Temperature: 28
 DATA send to 1 Temperature: 28
 DATA send to 1 Temperature: 28
 DATA send to 1 Temperature: 28
```

(a) Mote1 functioning as Client

```
connecting to /dev/ttyUSB0 (115200) [OK]
Rime started with address 0.18.116.0.19.225.196.37
MAC 00:12:74:00:13:e1:c4:25 Contiki 2.7 started. Node id is not set.
CSMA ContikiMAC, channel check rate 8 Hz, radio channel 26
Tentative link-local IPv6 address fe80:0000:0000:0000:0212:7400:13e1:c425
Starting 'UDP server process'
UDP server started
created a new RPL dag
Server IPv6 addresses: aaaa::212:7400:13e1:c425
aaaa::ff:fe00:1
fe80::212:7400:13e1:c425
Created a server connection with remote address :: local/remote port 5678/8765
DATA recv 'Temperature 28 from the client' from 131
DATA recv 'Temperature 28 from the client' from 131
DATA recv 'Temperature 28 from the client' from 131
DATA recv 'Temperature 28 from the client' from 131
DATA recv 'Temperature 28 from the client' from 131
```

(b) Mote2 as Server/PAN configuration of motes

```
running SENSORS_ACTIVATE(mq135).
SENSORS_ACTIVATE: 1
SENSORS_READY: 1
CO2:325 ppmRime started with address 131.65
MAC 83:41:00:00:00:00:00:00 Contiki 2.6 started. Node id is not set.
CSMA ContikiMAC, channel check rate 8 Hz, radio channel 65491
Starting 'mq135 Test'


running SENSORS_ACTIVATE(mq135).
SENSORS_ACTIVATE: 1
SENSORS_READY: 1
CO2:346 ppm
```

(c) MQ135 sensor output measuring CO_2

```
PM10 value = 91 ug/m3
Rime started with address 131.65
MAC 83:41:00:00:00:00:00:00 Contiki 2.6 started. Node id is not set.
CSMA ContikiMAC, channel check rate 8 Hz, radio channel 65491
Starting 'dsm501a Test'


running SENSORS_ACTIVATE(pm10).
SENSORS_ACTIVATE: 1
SENSORS_READY: 1
PM10 value = 91 ug/m3
Rime started with address 131.65
MAC 83:41:00:00:00:00:00:00 Contiki 2.6 started. Node id is not set.
CSMA ContikiMAC, channel check rate 8 Hz, radio channel 65491
Starting 'dsm501a Test'
```

(d) DSM501a sensor output measuring PM_{10} value

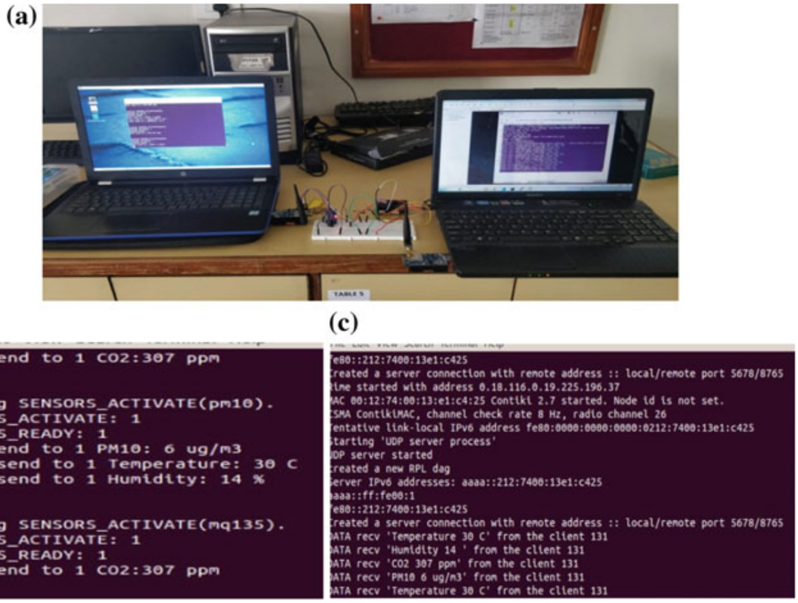
Fig. 10 Hardware sensor and mote's output in VMware workstation terminal window

MSP430 microcontroller and sent to the server Mote2 at the other end over UDP. The acquired data is then displayed.

Figure 10b shows the output window of client mote which sends the data packets to the server mote. It first fetches the server data, packetizes them, and then routes the packets over UDP. Figure 10c describes the operation of server mote which receives the data packets sent by client mote and displays them on the terminal window as shown in Fig. 11.

5 Conclusion

Overall, the development for this project has been discussed covering hardware design and software development. This project demonstrated the possibility of implementing a system that will help in monitoring the pollutant level in the atmosphere, thus creating a social alert. The project is developed especially keeping in mind the vehicle accident prevention application, and hence, emphasizes the creation of a driver alert system with system information being displayed on the big displays along highways. The idea to implement the system on street light poles has made it cost-effective by cutting off the installation costs, and also the usage of motes has incorporated the use of wireless communication for data transmission and increased



```
DATA send to 1 CO2:307 ppm

running SENSORS_ACTIVATE(pm10).
SENSORS_ACTIVATE: 1
SENSORS_READY: 1
DATA send to 1 PM10: 6 ug/m3
 DATA send to 1 Temperature: 30 C
 DATA send to 1 Humidity: 14 %

running SENSORS_ACTIVATE(mq135).
SENSORS_ACTIVATE: 1
SENSORS_READY: 1
DATA send to 1 CO2:307 ppm
```

```
fe80::212:7400:13e1:c425
reated a server connection with remote address :: local/remote port 5678/8765
ime started with address 0.18.116.0.19.225.196.37
AC 00:12:74:00:13:e1:c4:25 Contiki 2.7 started. Node id is not set.
SMA ContikiMAC, channel check rate 8 Hz, radio channel 26
entative link-local IPv6 address fe80:0000:0000:0000:0212:7400:13e1:c425
tarting 'UDP server process'
DP server started
reated a new RPL dag
erver IPv6 addresses: aaaa::212:7400:13e1:c425
aaa::ff:fe00:1
fe80::212:7400:13e1:c425
reated a server connection with remote address :: local/remote port 5678/8765
ATA recv 'Temperature 30 C' from the client 131
ATA recv 'Humidity 14 ' from the client 131
ATA recv 'CO2 307 ppm' from the client 131
ATA recv 'PM10 6 ug/m3' from the client 131
ATA recv 'Temperature 30 C' from the client 131
```

Fig. 11 **a** Actual implementation of PAN configuration with motes and sensors

node connectivity limit. Powering motes using batteries leads to increased efficiency, less power consumption, and long system life.

References

1. Corbalan P, Marfievici R, Cionca V, O'Shea D, Pesch D (2016) Into the SMOG: the stepping stone to centralized WSN control. In: 2016 IEEE 13th international conference on mobile ad hoc and sensor systems (MASS)
2. Kampa M, Castanas E (2007) Human health effects of air pollution–laboratory of experimental endocrinology. University of Crete, School of medicine, Heraklion, Greece, 10 June 2007
3. Online: Effects of smog–India today available: http://www.indiatoday.in/fyi/story
4. Online: www.scribd.com
5. Genc S (2012) The adverse effects of air pollution on the nervous system. J Toxicol 23. Article ID 782462
6. Sallis P, Dannheim C, Icking C, Maeder M (2015) Air pollution and fog detection through vehicular sensors [16]. In: IEEE Xplore conference on 06 April
7. Goel AK, Ray S, Agarwal P, Chandra N (2012) Air pollution detection based on head selection clustering and averaging method from wireless sensor network. In: IEEE Xplore 2012 2nd international conference on advanced computing and communication technologies (SICACCT), 7–8 Jan 2012
8. Alexandru P, Andrei M, Cristina-Madalina S, Stan O (2018) Smart environment monitoring beacon. Cluj Napoca University, Romania—IEEE international conference on automation, quality and testing, robotics (AQTR)—05 July 2018

9. Kavyashree ED (2018) 6LoWPAN network using contiki operating system. In: 3rd national conference on image processing, computing, communication, networking and data analytics (NCICCNDA 2018), 28 April 2018
10. Ayele TW, Mehta R (2018) Air pollution monitoring and prediction using IoT. In: 2018 second international conference on inventive communication and computational technologies (ICICCT)
11. Raipure S, Mehetre D (2015) Wireless sensor network based pollution monitoring system in metropolitan cities. In: International conference on communications and signal processing (ICCSP)
12. Raipure S, Mehetre D (2015) Wireless sensor network based pollution monitoring system in metropolitan cities. In: IEEE international conference on communications and signal processing (ICCSP) November 2015, Melmaruvathur, India
13. Shaban KB, Kadri A, Rezk E (2016) Urban air pollution monitoring system with forecasting models. In: IEEE xplore IEEE sensors journal conference on 15 April 2016
14. Corbalan P, Marfievici R, Cionca V, O'Shea D, Pesch D (2016) Into the SMOG: the stepping stone to centralized WSN control. In: IEEE 13th international conference on mobile ad hoc and sensor system
15. Online: The times of india available: https://timesofindia.indiatimes.com/india/india-tops-world-in-bad-air-quality-kanpur-delhi-among-top-15-mumbai-4th-most-polluted-megacity/articleshow/63997130.cms

IoT-Based Women Security System

Megalingam Rajesh Kannan, K. Jyothsna, T. S. Aparna, T. Anjali, M. Meera and S. D. Amrutha

Abstract In the current global scenario, the prime question in every woman's mind is about her safety and security. The only thought haunting every women is when they will be able to move freely on the streets even in odd hours without worrying about their security. This work suggests a new perspective to use technology to protect women. The wearable system resembles a normal watch with a button. Women can press the button when they feel discomfort and activate the system. The system can also be activated by changes in sensor setup output which is part of the system. When activated, the system tracks the location of the woman using Global Positioning System (GPS) sensor and sends an emergency email to the person who can help or save her. The system also incorporates a screaming alarm that uses real-time clock, to call out for help. The main advantage of this system is that the user does not require a smartphone unlike other applications that have been developed earlier. The use of sophisticated components ensures accuracy of the system and makes it reliable. Uneven terrains, step fields, sand and gravel, as well as exploring tasks like finding the injured victims and hazardous signs.

Keywords IoT · Women security · GPS · Email alert

M. Rajesh Kannan · K. Jyothsna (✉) · T. S. Aparna · T. Anjali · M. Meera · S. D. Amrutha
Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India
e-mail: kjyothsnareddy117@gmail.com

M. Rajesh Kannan
e-mail: rajeshkannan@ieee.org

T. S. Aparna
e-mail: aparnats90@gmail.com

T. Anjali
e-mail: anjalitsuresh98@gmail.com

M. Meera
e-mail: meeramurali3498@gmail.com

S. D. Amrutha
e-mail: amruthasdevan17@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_134

1 Introduction

In this research work, we are developing a women security watch for helping woman in distress by using IoT. Using this device, women can send the details of location, an emergency mail and switch on the screaming alarm by simply pressing a button in the watch. Or the system can also be automatically activated by observing the variations in the sensors like the temperature sensor and heartbeat sensor. Even in the twenty-first century, women cannot step out of their house in night time as they cannot be assured of their physical safety. Now a days, the prime question in every girls mind, considering the ever rising increase of issues on women harassment in recent past, is mostly about her safety and security. This research work suggests a new perspective to use technology for women safety. Approximately, 848 Indian women are harassed, raped or killed every day. That is a way beyond huge number. We propose an idea which changes the way everyone thinks about women safety.

2 Motivation

An undeniable reality that has not changed and is still prevailing, not only in our country but all around the world, is the safety of women. Whether at home, working place or outside the home, safety of women matters a lot. Its a sad truth that every minute and every second some women, let it be mother, sister, wife, young girls, infants are getting harassed, assaulted and molested at various places all over the world. Even though there are many laws and worldwide organisations working for the welfare of women, the number of unlawful or illegal acts against women is rapidly increasing day by day. The fact is that there are cases which are not even filed or reported. Now, the situation has reached to a stage where parents are scared to allow their daughters to step out of the house. This has inherited a fear in every girl's mind and decreased the confidence level. This has become a matter requiring a resolution. Thus, it is indeed a need to call for a security system for the safety of women.

3 Related Works

A smart watch for women security based on IoT concept 'watch me' is proposed in [1]. It works automatically based on the heartbeat rate which triggers the sensor, produces a high pitch alarm sound and sends an alert signal to the nearby police station. The Personal Stun-A Smart device for women safety, when activated, sends GPS location, pulse rate and body temperature of the person to the ice contacts and police control room. The band which is part of this device when thrown with a force, the force sensor gets activated and sends the GPS location [2]. An innovative approach for women and children security-based location tracking system using

GPS and GSM is presented in [3]. Paper [4] proposes a system which sends message along with location to the family members, nearest police station and to people in near vicinity. In [5], the authors propose a tracking system that receives GPS signals, processes and transmits data to the tracking center.

A novel IoT access architecture for vehicle monitoring system is proposed in [6]. Even though this is not relevant to the problem we address, we can learn about the IoT and sensor integration. Paper [7] presents the design and implementation of an Ethernet-based Smart Home intelligent system for monitoring the electrical energy consumption based upon the real-time tracking of the devices at home. In paper [8], the authors present a system which gathers sensor data, translates, sends data to the server with 3G/4G network, stores and retrieves sensor data using IoT. An IoT smart home architecture for long-term care of people with special needs is presented in [9]. Paper [10] presents a system which sends alerts to the user about the health risks if any, ensures better utilization of energy and resources and sends an email notification to the user account if higher light intensity is detected in the room. We see that papers [6–10] are not related to women security but used IoT technology for the intended cause.

Paper [11] proposes a smart IoT-based agriculture system to control CO_2, soil moisture, temperature and light, based on the soil moisture. The objective is to increase the yield and to provide organic farming. A vehicle tracking system using GPS is proposed in [12]. Human tracking in certain outdoor and indoor areas by combining the use of RFID and GPS is proposed in [13]. A real-time GPS-based tracking system based on GSM mobile phone which tracks the location of the vehicle and its speed based on mobile phone is presented in [14]. A system that is used for parenting purpose to monitor the movement of children outside the home is proposed in [15]. In all these research papers, we see that either IoT or GPS or both technologies are used to achieve the goal. In our system, we propose to use IoT, GPS and Wi-Fi technologies to achieve our goal.

4 Design and Implementation

The architecture diagram of the system we designed and implemented is shown in Fig. 1. This section describes about each of the blocks in the architecture diagram.

4.1 Design Units

Sensor Unit. The sensor unit consists of a heart rate sensor to sense and monitor the heart rate of the user wearing the device. The heart rate signals are passed on to the Microcontroller Unit (MCU) to process and take a decision.

MCU. Microcontroller Unit is Arduino uno with Atmega328 microcontroller. Even though it is not the heart of the system, it can take some good decisions as to

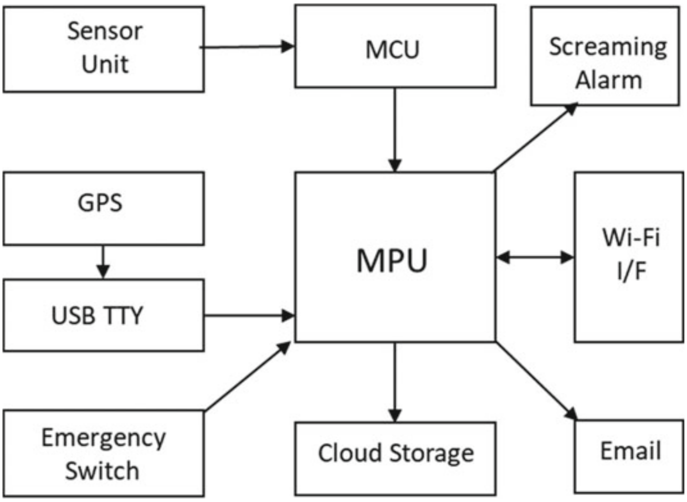


Fig. 1 Architecture diagram of the propose women safety system

find out irregular heart rates and report to the Microprocessor Unit (MCU). It works according to the program stored in its read-only memory (ROM). The Atmega328 is a 28 pin microcontroller.

MPU and Wi-Fi I/F. The microprocessor unit (MPU) is the heart of the system. It interacts with the MCU, Global Positioning System (GPS), Wi-Fi, email, cloud storage and emergency switch. This is the central controller and the algorithm to interact with all the above-mentioned modules are programmed into the MPU. The Raspberry Pi 2 board is used as the MPU. The programming is done in Python. The Raspberry Pi 2 board uses a powerful ARM Cortex-A7-based quad-core processor which runs at 900 MHz. The Wi-Fi I/F, i.e., the wireless LAN is part of the MPU which is supported by the Raspberry Pi 2. Using the wireless interface, the user can connect the proposed wearable device to the Internet via tethering with the smartphone Wi-Fi interface. By this way, the device gets continuous access to Internet thereby enabling the access to cloud storage.

GPS Module and USB TTL. The GPS module is connected to the MPU via USB TTL. USB TTL is used as level shifter to translate the 5 V signaling of USB signals to the TTL level and vice versa. The GPS tracks the location (latitude and longitude) of the user wearing the device. The MPU gets the location information of the user and passes it to the cloud. If the user is in distress (either abnormal heart rate or the emergency switch is pressed), the cloud will immediately send an emergency email to the relative or the caretaker of the user.

Emergency Switch. The user in distress, when presses the emergency switch which is directly connected to the MPU, the MPU will initiate the process of sending an emergency email to the relative or the caretaker of the user without any delay. The MPU gets the location of the user from the GPS data and sends to the cloud which will then initiate an email.

Cloud Storage (ThingSpeak). We used ThingSpeak for our project which is free to use for research purposes. For IoT environment, ThingSpeak enables communication capabilities. It is very helpful to design and build applications based on the data obtained from the sensors. Eight fields of data can be stored by each channel, and it allows to use 255 alphanumeric characters. The best thing is that it offers four dedicated fields for positional data which includes latitude, longitude, description and elevation. The data that is received at the ThingSpeak end and is time stamped with a sequential ID. For our purpose, we need to create one channel to pump our sensor data. Once the channel is created, ThingSpeak allows to publish the data with an API. It also creates a 'write key' for authentication.

Email. When the person or the user is in distress, it causes increase in heart rate, and the MPU can process this data and decide to send an emergency email to the user's relative. The latitude and the longitude coordinates of the user's location are collected via GPS and passed to ThingSpeak which in turn notified the user's relative. Alternatively, if the user presses the emergency switch, the MPU does repeat the same process to email the relative of the user, for help.

Screaming Alarm. The screaming alarm gets triggered whenever the user in distress presses the emergency switch or abnormal heart rate is detected by the MPU. Along with sending the email to the relative of the user, the screaming alarm will also be triggered so that nearby people can hear and notice and come to the rescue of the user in distress.

4.2 Functional Flow of the Proposed System

Figure 2 shows the work flow for the proposed security system for women. During a critical condition or accident, the user's heart rate increases. The sensor unit is continuously monitored by the MCU, and the sensor data is processed. The heart rate is determined, and this too is a continuous process.

The MCU passes the sensor data to the MPU. The Raspberry Pi-based MPU processes this data and can take a decision to contact the ThingSpeak if the heart rate is abnormal. A serial communication port is used between the MCU and the MPU to pass the information. Alternatively, if the user can press the emergency switch under stressful condition or distress, the MPU repeats the same workflow as when the heart rate increases. The heart rate condition is detected automatically by the system without the need for user intervention. The emergency switch press requires human intervention. Both modes of operation of the devices enhance the user-friendly nature of the device. Once the MPU decides that an email notification has to be sent, it collects the GPS data from the GPS module via USB TTL and passes this information to the IoT-based ThingSpeak. The ThingSpeak can then send an emergency email notification to the relative or any other person that was predetermined by the user and registered with the ThingSpeak. Along with sending email to the user, the screaming alarm will also be triggered.

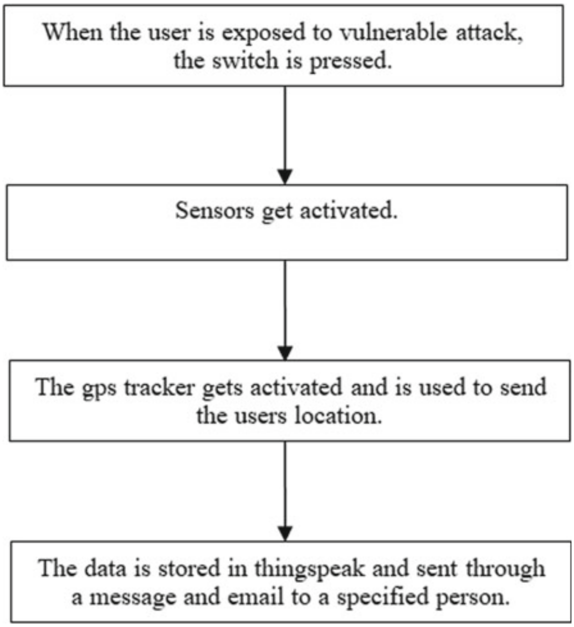

When the user is exposed to vulnerable attack, the switch is pressed.
Sensors get activated.
The gps tracker gets activated and is used to send the users location.
The data is stored in thingspeak and sent through a message and email to a specified person.

Fig. 2 Work flow diagram

4.3 MPU Algorithm

The algorithm that is implemented in Python programming and used in the Raspberry Pi MPU is shown as flowchart in Fig. 3. The program waits for trigger from either the emergency switch or the sensor unit which uses the heart rate sensor. Once triggered from either of these sources, the program immediately sounds the screaming along. Simultaneously, it gets the latitude and longitudinal values from the GPS via USBttl and passes these values to the IoT-based ThingSpeak. An email is immediately sent to the relative of the user. For this entire system to work, the MPU should be continuously connected to the Internet via mobile phone or smartphone. The email ID of the relative of the user is stored in advance in ThingSpeak.

Figure 4 shows the implementation of the system for women security. The figure clearly shows the MPU with Wi-Fi I/F, MCU, GPS, USBttl, screaming alarm and sensor unit.

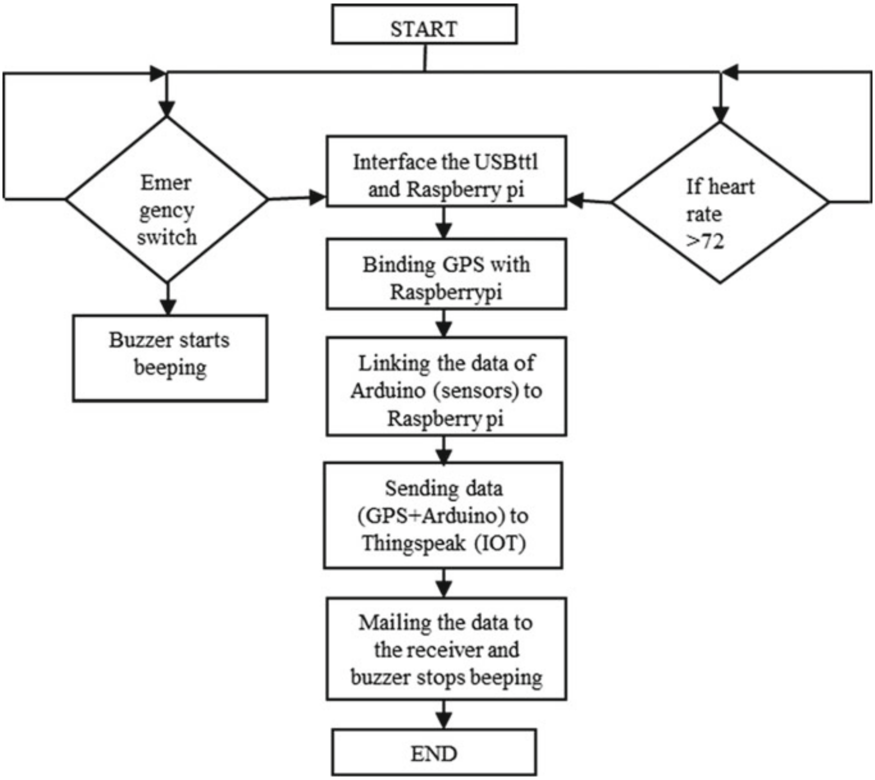

START
Emer gency switch
Buzzer starts beeping
Interface the USBttl and Raspberry pi
Binding GPS with Raspberrypi
Linking the data of Arduino (sensors) to Raspberry pi
Sending data (GPS+Arduino) to Thingspeak (IOT)
Mailing the data to the receiver and buzzer stops beeping
END
If heart rate >72

Fig. 3 Flowchart for the Python program implemented in Raspberry Pi

5 Experiment and Results

5.1 Experimental Setup

Seven users were chosen to test the device. Each of the users was given the device and asked to press the emergency switch from six different locations near to our Amrita Vishwa Vidyapeetham University (AVVU). Two users from Vallikavu near our university, one user at Mata Amritanandamayi Math, one user at Mata Amritanandamayi Math (MAM) bajan hall, another user at Mata Amritanandamayi Math hospital, one user at Amrita Vishwa Vidyapeetham university main gate and the last user at Amrita Vishwa Vidyapeetham university canteen pressed the emergency switch.

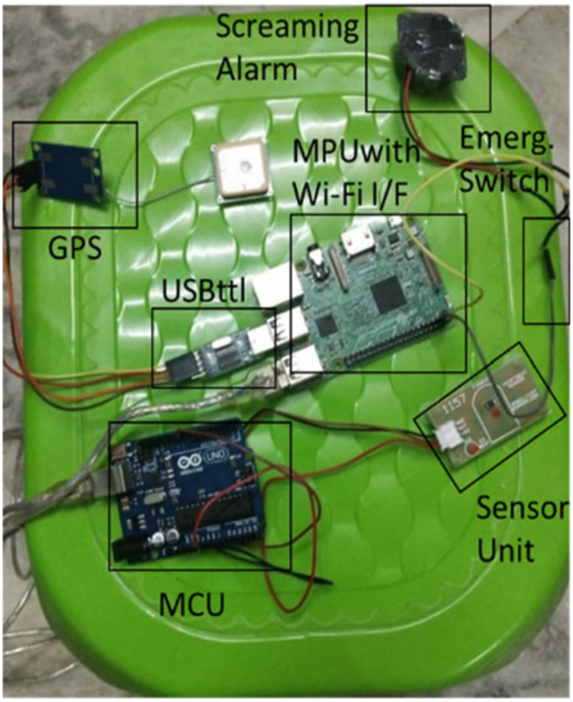


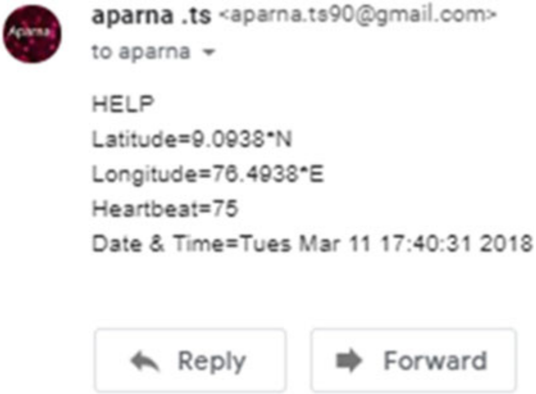
Fig. 4 Women security device

5.2 Test Results

Table 1 shows the latitude and longitude values of the each of the seven users along with their locations. While the second column in the table lists the latitude and longitudinal values obtained through GPS, the third column lists the latitude and longitudinal values obtained through Google map for the same locations. The last

Table 1 System tests carried out at various locations

Location	GPS receiver results		Actual location		Deviation (m)
	Latitude	Longitude	Latitude	Longitude	
Vallickavu	9.0940° N	76.4915° E	9.0960° N	76.4926° E	1.199
Vallickavu	9.0938° N	76.4915° E	9.0950° N	76.4925° E	2.028
MAM	9.0872° N	76.4915° E	9.0892° N	76.4871° E	2.462
MAM bajan hall	9.0895° N	76.4915° E	9.0897° N	76.4859° E	0.562
MAM hospital	9.0889° N	76.4915° E	9.0899° N	76.4849° E	2.521
AVVU main gate	9.0936° N	76.4915° E	9.0938° N	76.4917° E	0.6916
AVVU canteen	9.0932° N	76.4915° E	9.0939° N	76.4919° E	0.6908



aparna .ts <aparna.ts90@gmail.com>
to aparna

HELP
Latitude=9.0938°N
Longitude=76.4938°E
Heartbeat=75
Date & Time=Tues Mar 11 17:40:31 2018

Fig. 5 Sample email details sent to the relative

column lists the error in meters, i.e., the latitude and longitudinal values obtained through the GPS fitted with our system and the Google map. We can see that we were able to achieve the error as minimum as 0.5 m, and hence, can conclude that the proposed system could accurately pinpoint the location of the user in distress.

A sample email that was sent to the relative, when one of the users pressed the emergency button of the proposed women safety system at the location Vallikavu, is given in Fig. 5. In these emails, we can see the request for 'HELP' from the user, the latitude and the longitude values and the date and time at which the request was generated. These emails were sent using the IoT-based ThingSpeak.

6 Conclusion

This project analyzes the emergency response system which guards and helps the women to save herself when she is in danger. The main objective is to model a low-cost system which can accumulate the data of the lady and provide urgent alert in case of emergency. Our effort behind this project is to construct and formulate a gadget that acts like a compact weapon. It is certainly a precise and protective methodology which will probably be very useful for the women. The establishment of a hardware and software prototype has accomplished two objectives: affirmation of the design and verifying whether the idolized technology is suitable for the system. The device is easy to handle, highly responsive and assures safety to the user.

Acknowledgements We thank Amrita Vishwa Vidyapeetham University and Humanitarian Technology (HuT) labs for providing us this wonderful opportunity to direct our thoughts into a real prototype. We thank all the people who have helped us to accomplish this project in time.

References

1. Helen A, Fathila MF, Rijwana R, Kalaiselvi VKG (2017) Watch me. In: 2017 second international conference on computing and communication technologies (ICCCT), Chennai, India
2. Ahir S, Kapadia S, Chauhan J, Sanghavi N (2018) The personal stun—A smart device for women's safety. In: 2018 international conference on smart city and emerging technology (ICSEET), Mumbai, India
3. Velayutham R, Sabari M, Rajeswari MS (2016) An innovative approach for women and children security based location tracking system. In: 2016 international conference on circuit, power and computing technologies (ICCPCT), Nagarcoil, India
4. Harikiran GC, Menasinkai K, Shirol S (2016) Smart security solution for women based on IoT. In: 2016 international conference on electrical, electronics and optimization techniques (ICEEOT), Chennai, India
5. Dafallah HAA (2014) Design and implementation of an accurate real time GPS tracking system. In: 2014 third international conference on e-technologies and networks for development (ICeND), Beirut, Lebanon
6. Wang S, Hou Y, Gao F, Ji X (2016) Novel IoT access architecture for vehicle monitoring system. In: 2016 IEEE 3rd world forum on internet of things (WF-IoT), Reston, VA, USA
7. Gupta P, Chhabra J (2016) International conference on innovation and challenges in cyber security (ICICCSINBUSH), Noida, India
8. Suyama T, Kishine Y, Naya F (2014) Abstracting IoT devices using virtual machine for wireless sensor nodes. In: 2014 IEEE world forum on internet of things (WF-IoT)
9. Coelho C, Coelho D, Wolf M (2015) An Iot smart home architecture for long-term care of people with special needs. In: 2015 IEEE, 2nd world forum on internet of things (WF-IoT), Milan, Italy
10. Malche T, Maheshwari P (2017) Internet of things (IoT) for building smart home system. In: 2017 international conference on I-SNAC (IoT in Social, Mobile, Analytics and Cloud), Palladom, India
11. Pallavi S, Mallapur JD, Bendigeri KY (2017) Remote sensing and controlling of greenhouse agriculture parameters based on IoT. In: 2017 international conference on big data, IoT and data science, Pune, India
12. Kumar R, Kumar H (2014) Availability and handling of data received through GPS device: In tracking a vehicle. In: 2014 IEEE international advance computing conference (IACC), Gurgaon, India
13. Hutabarat DP, Hendry H, Pranoto JA, Kurniawan A (2016) Human tracking in certain indoor and outdoor area by combining the use of RFID and GPS. In: 2016 IEEE Asia Pacific conference on wireless and mobile (APWiMob), Bandung, Indonesia
14. AI Rashad MA, Ourmar OA, Singh D (2013) A real time GSM/GPS based tracking system based on GSM mobile phone. In: 2013 second international conference on future generations communication technologies (FGCT), London, UK
15. Bilgic HT, Alkar AZ (2011) A secure tracking system for GPS-Enabled mobile phones. In: Proceedings of fifth international conference on information technology and multimedia (ICIMU), Kuala Lumpur, Malaysia

IoT-based Wearable Micro-Strip Patch Antenna with Electromagnetic Band Gap Structure for Gain Enhancement

M. Ameena Banu, R. Tamilselvi, M. Rajalakshmi and M. Pooja Lakshmi

Abstract Wearable antennas used for various applications such as telemedicine, firefighting, and navigation purpose are integrated into fabrics. The antenna performance is described with the integration of Electromagnetic Band Gap (EBG) structure in which the micro-strip patch antenna (MSP) consists of flexible substrate material. The main goal of using EBG structure in micro-strip patch antenna is to overcome the limitations of patch antenna and to achieve better gain and efficiency, lower side lobes and back lobes level, better isolations among array elements, and by suppressing surface wave modes. The design of micro-strip patch antenna is proposed to resonate the antenna at 2.45 GHz using Jeans as substrate material for wearable applications which supports Industrial, Scientific and Medical (ISM) applications. The various characteristics of antenna such as return loss and VSWR are analyzed. The simulation of antenna is done by CST studio software. Internet of Things (IoT) may be used for the development of antennas, which supports multi-standard services within a single design.

Keywords Wearable antenna · Jeans · Electromagnetic Band Gap · ISM band · CST studio software · IoT

1 Introduction

A device that designed to transmit or receive electromagnetic waves in free space is known as antenna and also antenna called as a transducer. Comparing to all types of antenna, the micro-strip patch antenna has low profile, low cost, lightweight, and conveniently to be integrated with RF devices, because that is widely used in various applications. The micro-strip antennas can be designed to have many geometrical shapes and dimensions. The simplest configuration of micro-strip patch

M. Ameena Banu (✉) · R. Tamilselvi · M. Rajalakshmi · M. Pooja Lakshmi
Department of Electronics and Communication Engineering, Sethu Institute of Technology, Pulloor, Virudhunagar District 626115, Tamilnadu, India
e-mail: ameenabanuece@sethu.ac.in

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_135

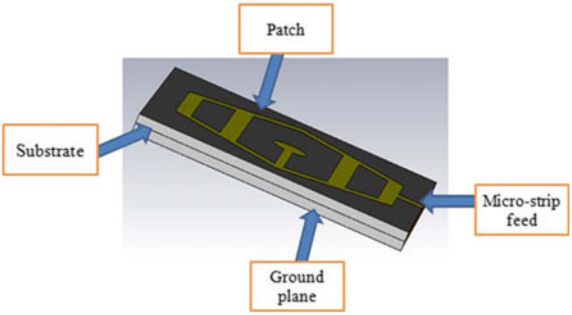


Fig. 1 Basic structure of micro-strip patch antenna

antenna consists of a radiating patch, dielectric substrate, and ground plane. The basic structure of micro-strip patch antenna is shown in Fig. 1.

Ground plane is called as lower conductor, the radiating patch is called as upper conductor, and the dielectric substrate is placed between the two conductors. In micro-strip patch antenna, the ground plane is a flat horizontal conducting surface, and it used to reflect the radio waves from the other antenna elements. The shape and size of the ground plane play a vital role in determining antenna radiation characteristics including return loss, gain, and VSWR.

The most aspect of designing micro-strip patch antenna is to choose the suitable dielectric substrate. For particular applications, the various types of substrates are available in the market that provides considerable flexibility in the choice of a substrate. The dielectric substrate characteristics including dielectric constant (permittivity) and dielectric medium are most considered to design a micro-strip patch antenna. The electrical characteristics of antenna are determined by substrate thickness and permittivity. The radiating patch is used to improve the performance of antenna. The micro-strip patch antenna consists of various shapes. The common shapes of patches are rectangular, circular, and triangular. Many shapes of patch design are combined to improve the antenna performance parameters [1, 2].

The drawbacks of micro-strip patch antenna are narrow bandwidth, low efficiency, and low gain. To overcome the drawbacks of micro-strip patch antenna, Electromagnetic Band Gap (EBG) is used. EBG structure is used to enhance the gain of the micro-strip patch antenna, reduce the backward radiation, and also achieve better radiation efficiency. The EBG technology plays a major role in the radio frequency and microwave applications because of their unique band gap characteristics at certain frequency ranges. The periodic arrangements of dielectric or metallic elements are known as EBG structure. The various EBG structures such as one-dimensional (1D), two-dimensional (2D), three-dimensional (3D), mushroom and uni-planar EBG may be used [3–5].

IoT is the network of physical devices and other appliances with embedded electronics, sensors, connectivity, software, and actuators, which is used to connect the device and exchange data. Data is transferred over a network without requiring human-to-computer or human-to-human interaction [6].

2 Literature Survey

Many researchers have designed the micro-strip patch antenna with flexible materials. Kumar et al. [7] developed the hexagonal shaped body wearable textile antenna on EBG substrate material, and they used felt as substrate material. The simulated antenna had achieved the return loss of −18.8526 dB and gain of 6.551 dB.

Researchers Purohit and Raval [8] developed the wearable textile patch antenna using jeans as substrate at 2.45 GHz. According to the simulated results, return loss is −32.57 dB at 2.45 GHz, and gain is 7.26 dB. But the fabricated antenna resonated at 2.4945 GHz with return loss of −30 dB.

Roland et al. [9] developed a patch antenna with EBG structure for WLAN applications using FR 4 as substrate. They used the mushroom structure for designing an EBG structure because of its high impedance characteristics. They achieved better return loss of −23.18 dB and gain of 14.2 dB at 2.42 GHz.

The above studies on design of micro-strip patch antenna with different substrate materials and different EBG structure techniques elaborated the advantages of use of flexible and multiple substrate materials. Hence, we authors are getting interested in designing an antenna with flexible substrate material which can extend its use for wearable applications and combination of different substrate materials as double substrate layer with EBG structure to enhance the performance of the antenna at the desired resonant frequency.

3 Antenna Design

The patch antenna, substrate, and ground layer dimensions are calculated as follows [10]:

1. To calculate width of the patch (W)

$$W = \frac{C}{2f_0\sqrt{\frac{(\varepsilon_r+1)}{2}}} \tag{1}$$

   where ε_r—relative permittivity
2. To calculate effective dielectric constant ($\varepsilon_{r\mathrm{eff}}$)

$$\varepsilon_r(\mathrm{eff}) = \frac{\varepsilon r+1}{2} + \frac{\varepsilon r-1}{4}\left(1+\frac{12h}{W}\right)^{-1/2} \tag{2}$$

where

h—height of the substrate
W—width of the patch

3. To calculate effective length of the patch (L_{eff})

$$L(\mathrm{eff}) = \frac{C}{2f0\sqrt{\varepsilon_{\mathrm{r}}(\mathrm{eff})}} \tag{3}$$

4. To calculate actual length of patch (L)

$$L = L(\mathrm{eff}) - 2\Delta L \tag{4}$$

where Δ—small deviation if required.

5. Substrate

For wearable antenna, the substrate material may be cotton, jeans, felt, teflon, etc. Two-layered substrates are used to design the micro-strip patch antenna. EBG elements are placed between the two-layered substrate to reduce the back radiations. In this work, the dielectric material jeans with dielectric constant $\varepsilon_{\mathrm{r}} = 1.6$ is used as substrate. The thickness of each substrate material is 1.6 mm for two-layered substrates with the dimensions of $54(L) \times 47(W)$ mm^2.

6. Ground

The copper material is used as ground plane with the dimension of $54(L) \times 47(W)$ mm^2 (Figs. 2, 3, 4).

All dimensions of different layers of micro-strip patch antenna are given in Table 1.

7. Electromagnetic Band Gap structure

EBG structures are always used as a part of microwave devices in order to improve the performance of devices especially to improve the radiation/gain patterns and to decrease the noise/losses in transmissions [11]. EBG structures are also known as

Fig. 2 Side view of antenna

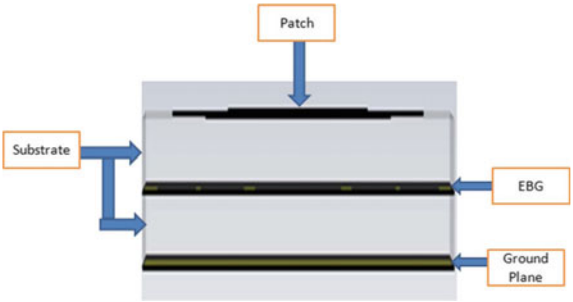


Fig. 3 Top view of antenna

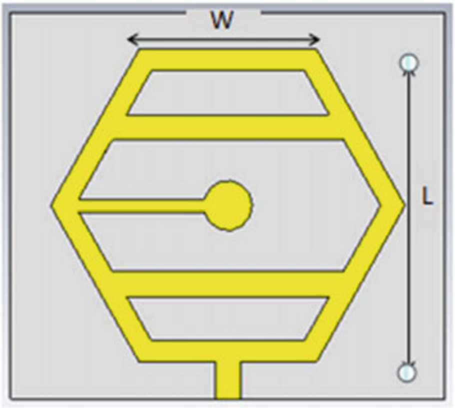
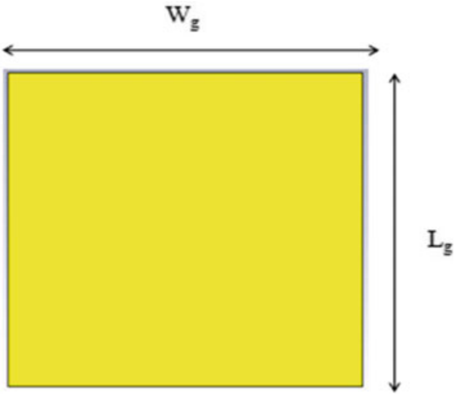


Fig. 4 Bottom view of antenna



high impedance surface due to their ability to suppress the surface wave at certain operational frequencies. In recent years, there has been rapid increase in the utilization of Electromagnetic Band Gap (EBG) structures in electromagnetic and antenna community [12]. In this proposed design, to achieve better gain and radiation efficiency, different EBG structures have been implemented as shown in Figs. 5, 6, 7, 8, and 9.

4 Results and Discussion

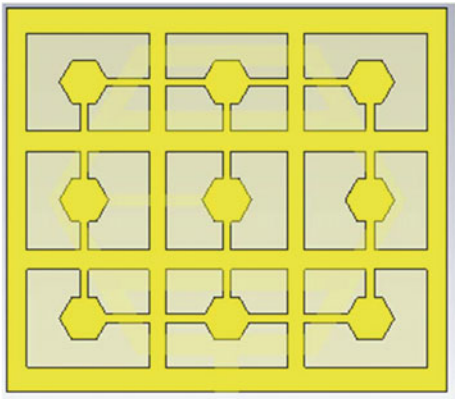
(i) Analysis of patch antenna without EBG structure

In this case, the micro-strip patch antenna with single substrate without EBG structure is considered where the thickness of the substrate material is 1.6 mm. While

Table 1 Dimensions of antenna

Parameters	Values (mm)
Patch length L	38
Patch width W	22
Patch height H	0.035
Ground length L_g	47
Ground width W_g	54
Ground height H_g	0.035
Substrate1 length	47
Substrate1 width	54
Substrate1 height	1.6
Substrate2 length	47
Substrate2 width	54
Substrate2 height	1.6
EBG layer length L_e	47
EBG layer width W_e	54
EBG layer height H_e	0.035

Fig. 5 EBG structure 1



simulating this design with the help of CST software, the following results shown in Figs. 10, 11, 12, and 13 are obtained.

(ii) Analysis of patch antenna with EBG structure

In order to improve the performance of the micro-strip patch antenna, the EBG structure is introduced in between the two substrate layers. The antenna parameters such as return loss, VSWR, gain, and directivity of designed patch antenna with different EBG structures are observed and compared. The proposed patch antenna performance with and without EBG is analyzed using CST Studio Suite software.

EBG structure 1

Fig. 6 EBG structure 2

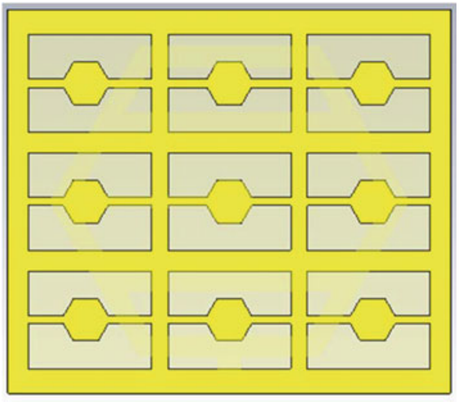


Fig. 7 EBG structure 3

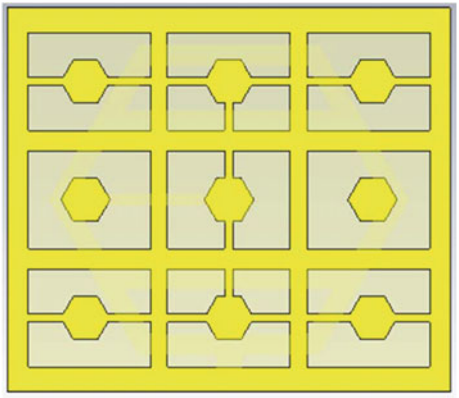
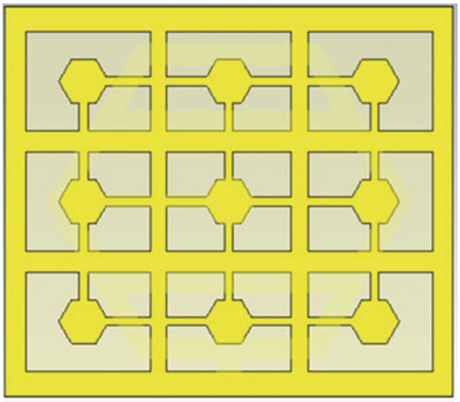


Fig. 8 EBG structure 4



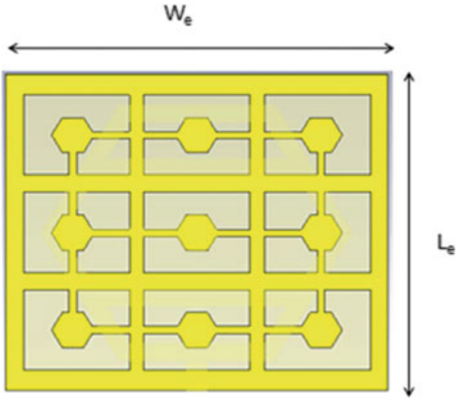


Fig. 9 EBG structure 5

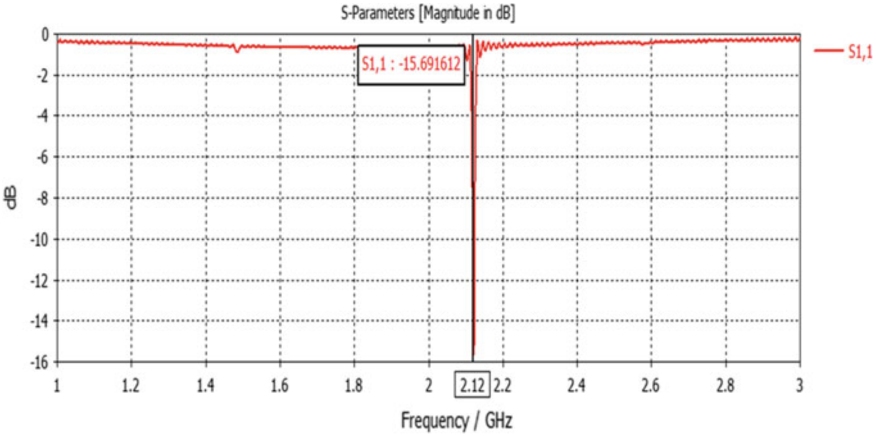


Fig. 10 Return loss plot without EBG

The designed micro-strip patch antenna has the linked hexagonal EBG structure as shown in Fig. 5, which has the gain and directivity of 5.225 dB and 6.802 dBi, respectively. The antenna parameters like return loss, VSWR, gain, and directivity are observed as depicted in Figs. 14, 15, 16, and 17.

EBG structure 2

The designed micro-strip patch antenna has modified EBG structure as shown in Fig. 6, which has the gain and directivity of 4.813 dB and 6.849 dBi, respectively. As compared with the previous design, the modified design produced high return loss with a frequency of 2.998 GHz. The performance parameters are shown in Figs. 18, 19, 20, and 21.

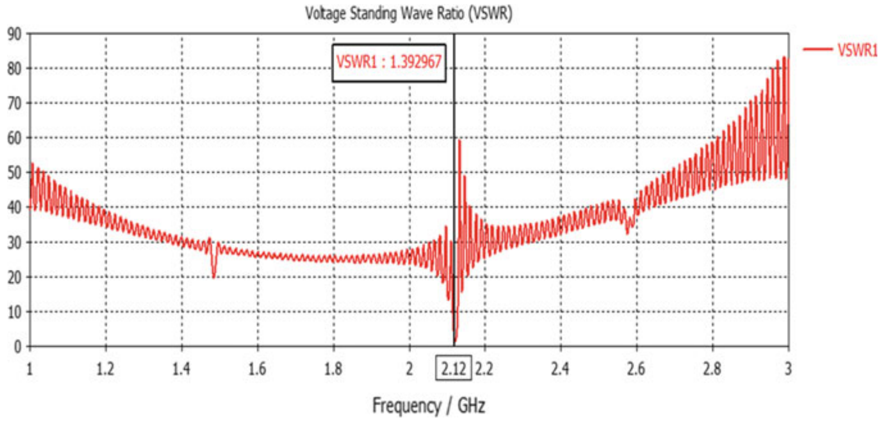
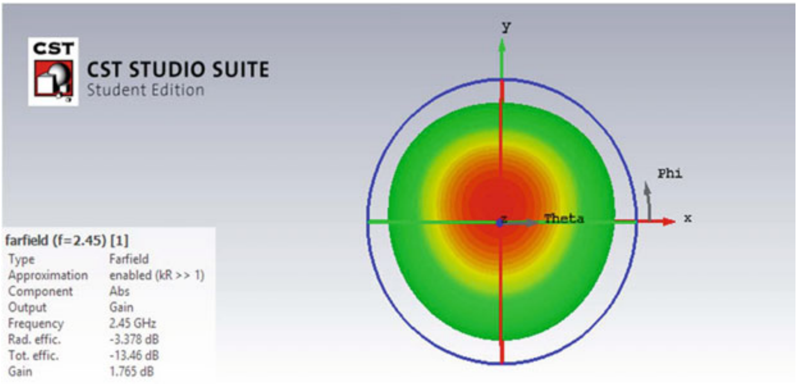


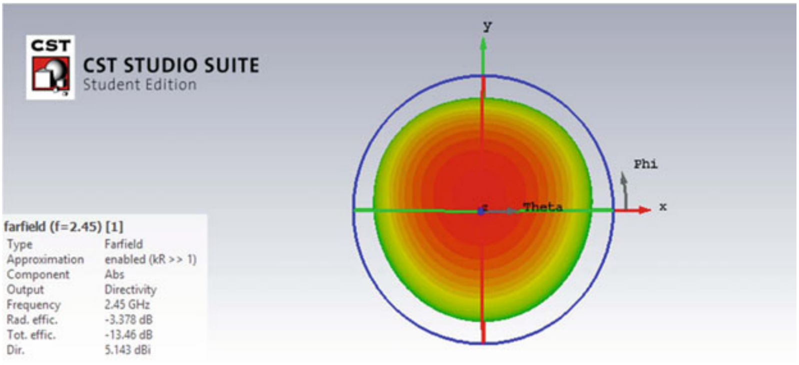
Fig. 11 VSWR plot without EBG



farfield (f=2.45) [1]

```
Type            Farfield
Approximation   enabled (kR >> 1)
Component       Abs
Output          Gain
Frequency       2.45 GHz
Rad. effic.     -3.378 dB
Tot. effic.     -13.46 dB
Gain            1.765 dB
```

Fig. 12 Gain without EBG



farfield (f=2.45) [1]

```
Type            Farfield
Approximation   enabled (kR >> 1)
Component       Abs
Output          Directivity
Frequency       2.45 GHz
Rad. effic.     -3.378 dB
Tot. effic.     -13.46 dB
Dir.            5.143 dBi
```

Fig. 13 Directivity without EBG

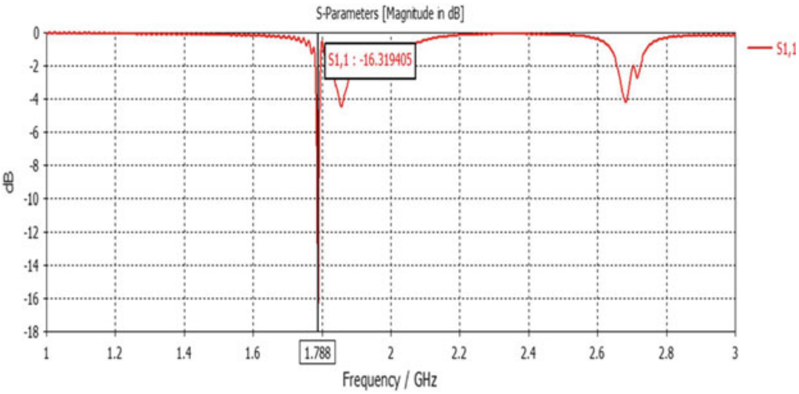


Fig. 14 Return loss plot with EBG structure 1

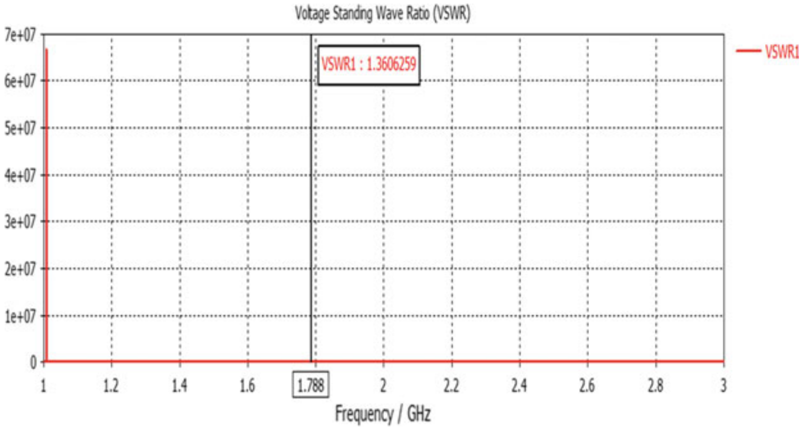
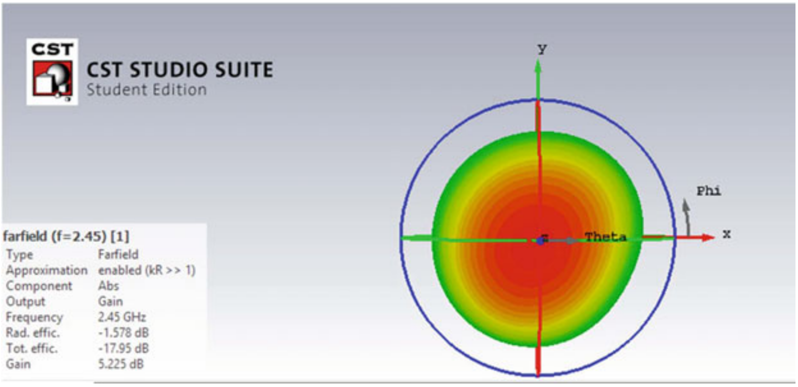


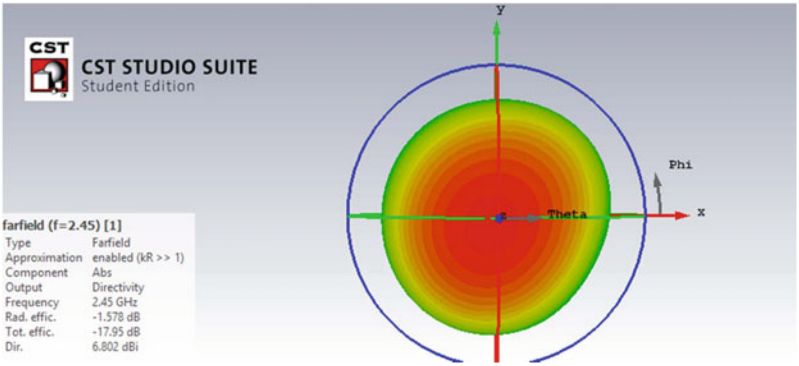
Fig. 15 VSWR plot with EBG structure 1



farfield (f=2.45) [1]

Type	Farfield
Approximation	enabled (kR >> 1)
Component	Abs
Output	Gain
Frequency	2.45 GHz
Rad. effic.	-1.578 dB
Tot. effic.	-17.95 dB
Gain	5.225 dB

Fig. 16 Gain with EBG structure 1



farfield (f=2.45) [1]

Type	Farfield
Approximation	enabled (kR >> 1)
Component	Abs
Output	Directivity
Frequency	2.45 GHz
Rad. effic.	-1.578 dB
Tot. effic.	-17.95 dB
Dir.	6.802 dBi

Fig. 17 Directivity with EBG structure 1

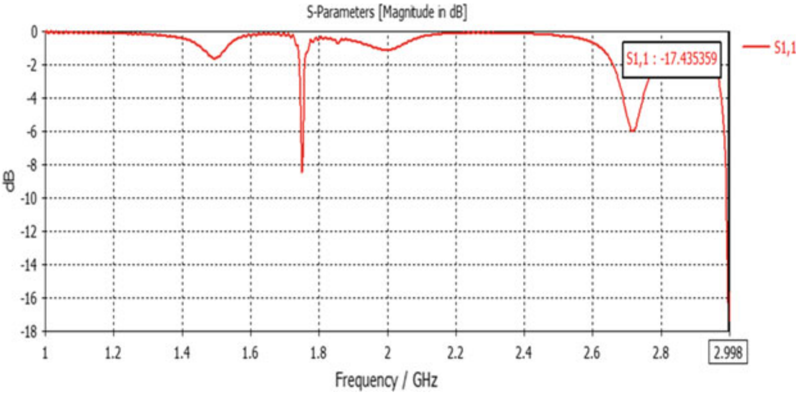


Fig. 18 Return loss plot with EBG structure 2

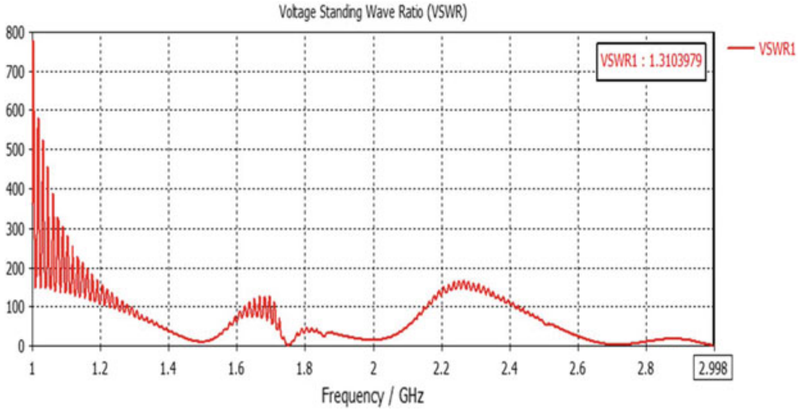
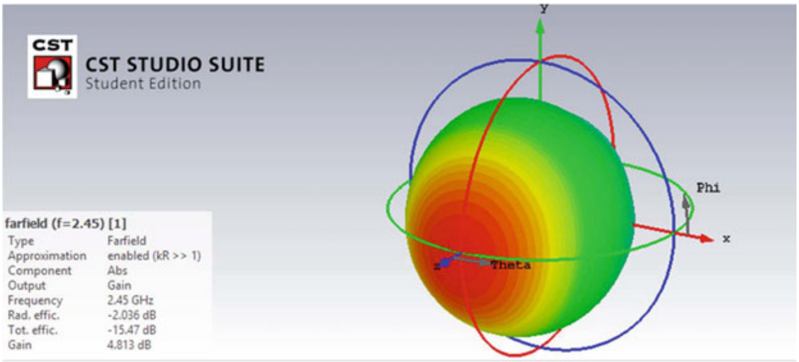


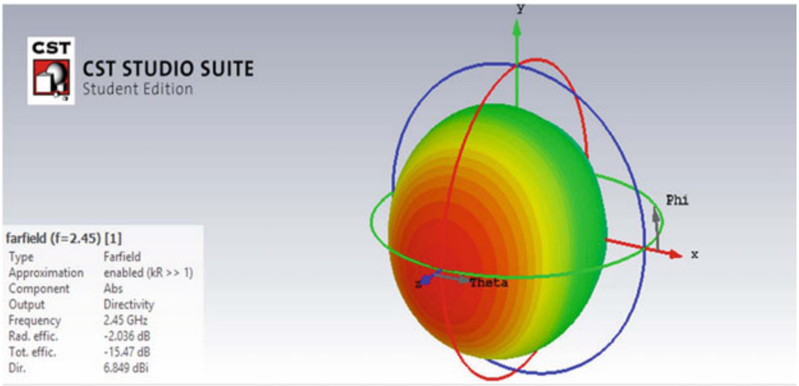
Fig. 19 VSWR plot with EBG structure 2



farfield (f=2.45) [1]

Type	Farfield
Approximation	enabled (kR >> 1)
Component	Abs
Output	Gain
Frequency	2.45 GHz
Rad. effic.	-2.036 dB
Tot. effic.	-15.47 dB
Gain	4.813 dB

Fig. 20 Gain with EBG structure 2



farfield (f=2.45) [1]

Type	Farfield
Approximation	enabled (kR >> 1)
Component	Abs
Output	Directivity
Frequency	2.45 GHz
Rad. effic.	-2.036 dB
Tot. effic.	-15.47 dB
Dir.	6.849 dBi

Fig. 21 Directivity with EBG structure 2

EBG structure 3

For the modified EBG structure 3 as shown in Fig. 7, gain and directivity are observed as 4.898 dB and 6.316 dBi, respectively, at the resonant frequency of 1.746 GHz. For this new MSP antenna, the performance parameters are shown in Figs. 22, 23, 24, and 25.

EBG structure 4

For the modified EBG structure 4 as shown in Fig. 8, gain and directivity are observed as 5.063 dB and 6.728 dBi, respectively, with a resonant frequency of 1.884 GHz for which the characteristics are observed as depicted in Figs. 26, 27, 28, and 29.

EBG structure 5

The gain and directivity of 4.930 dB and 6.711 dBi, respectively, are obtained for the micro-strip patch antenna with EBG structure 5 which is resonated at the frequency of 2.848 GHz. The plots of various parameters are given in Figs. 30, 31, 32, and 33.

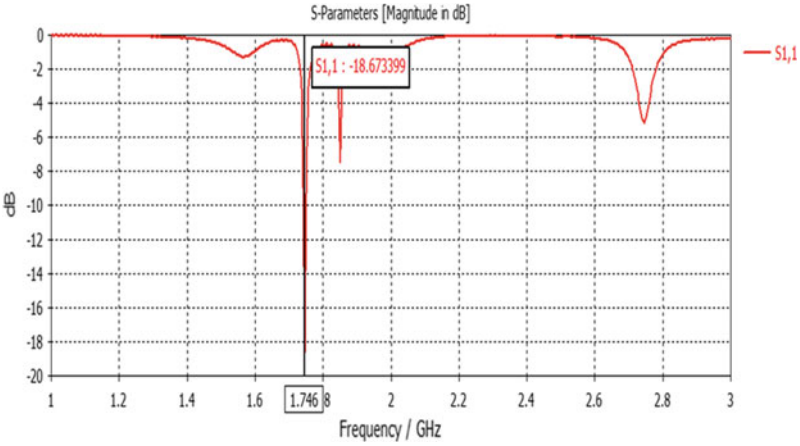


Fig. 22 Return loss plot with EBG structure 3

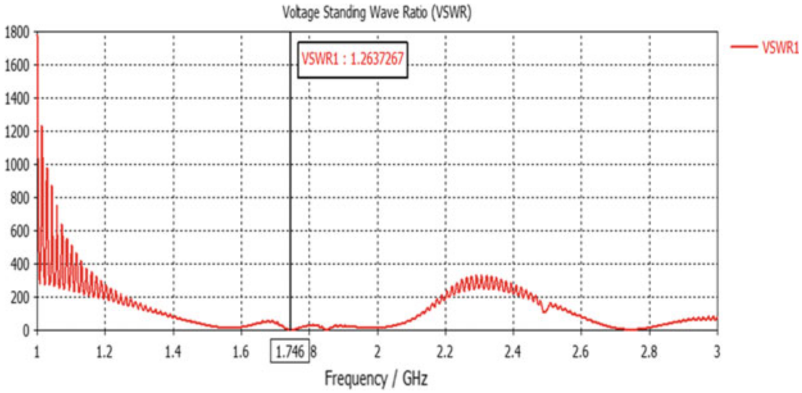
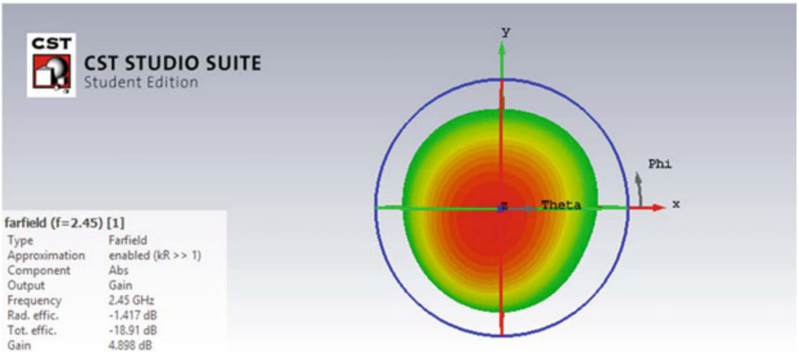
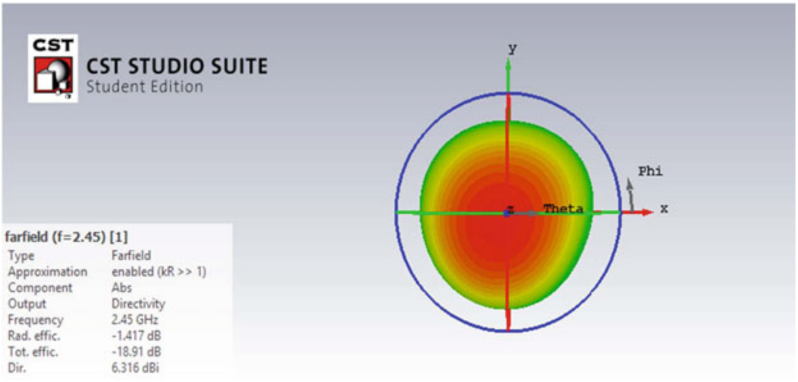


Fig. 23 VSWR plot with EBG structure 3



farfield (f=2.45) [1]
Type Farfield
Approximation enabled (kR >> 1)
Component Abs
Output Gain
Frequency 2.45 GHz
Rad. effic. -1.417 dB
Tot. effic. -18.91 dB
Gain 4.898 dB

Fig. 24 Gain with EBG structure 3



farfield (f=2.45) [1]

Type	Farfield
Approximation	enabled (kR >> 1)
Component	Abs
Output	Directivity
Frequency	2.45 GHz
Rad. effic.	-1.417 dB
Tot. effic.	-18.91 dB
Dir.	6.316 dBi

Fig. 25 Directivity with EBG structure 3

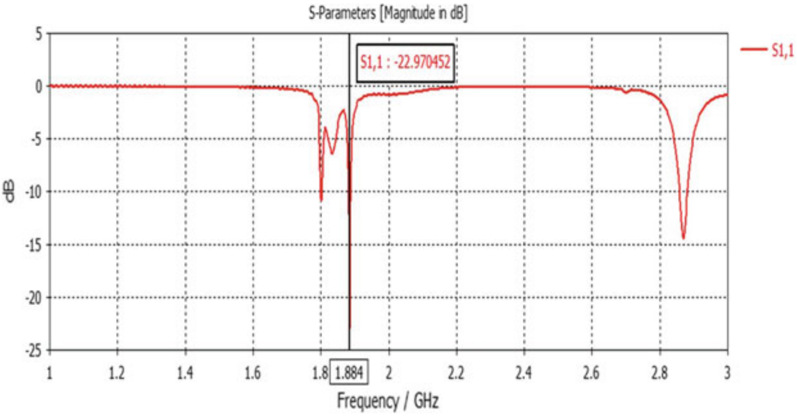


Fig. 26 Return loss plot with EBG structure 4

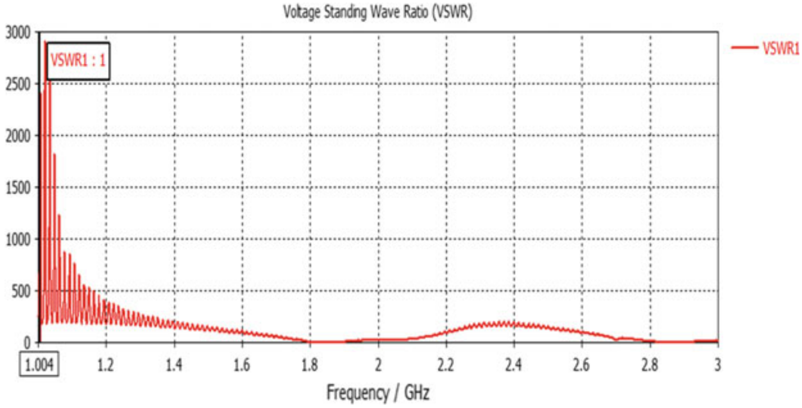
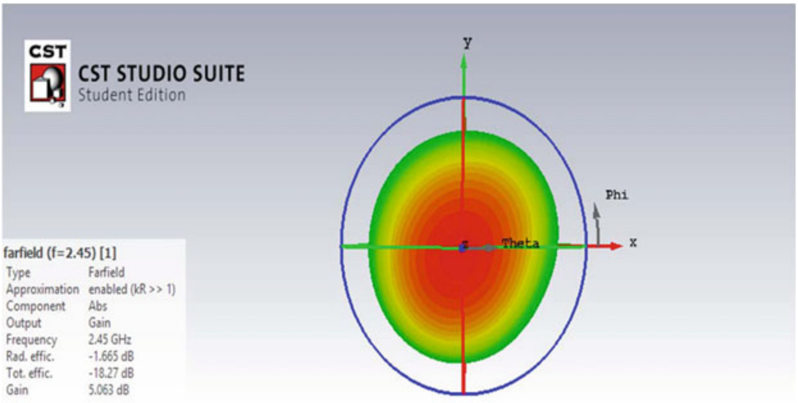
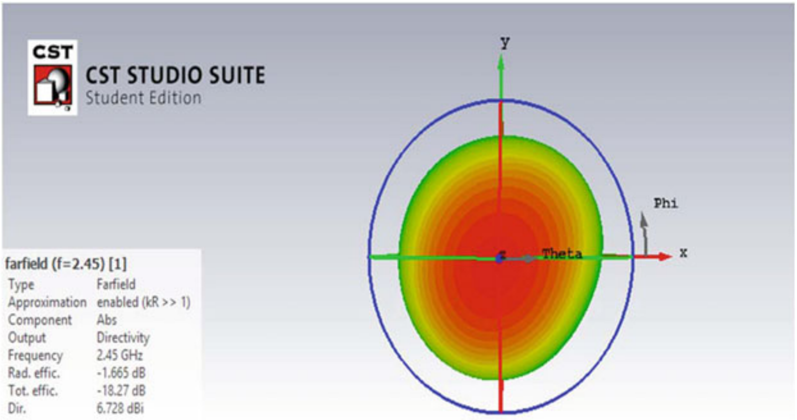


Fig. 27 VSWR plot with EBG structure 4



farfield (f=2.45) [1]
Type Farfield
Approximation enabled (kR >> 1)
Component Abs
Output Gain
Frequency 2.45 GHz
Rad. effic. -1.665 dB
Tot. effic. -18.27 dB
Gain 5.063 dB

Fig. 28 Gain with EBG structure 4



farfield (f=2.45) [1]
Type Farfield
Approximation enabled (kR >> 1)
Component Abs
Output Directivity
Frequency 2.45 GHz
Rad. effic. -1.665 dB
Tot. effic. -18.27 dB
Dir. 6.728 dBi

Fig. 29 Directivity with EBG structure 4

The performance parameters such as return loss, VSWR, gain, directivity, and resonant frequency observed for designed micro-strip patch antenna with different EBG structures are listed in Table 2 which is used to compare the performance of them.

5 Conclusion

While designing an antenna, the main consideration is its radiation characteristics. In this proposed design, the aim of introducing EBG structure is for improving the gain of the MSP antenna. When the performance parameters listed in Table 2 are

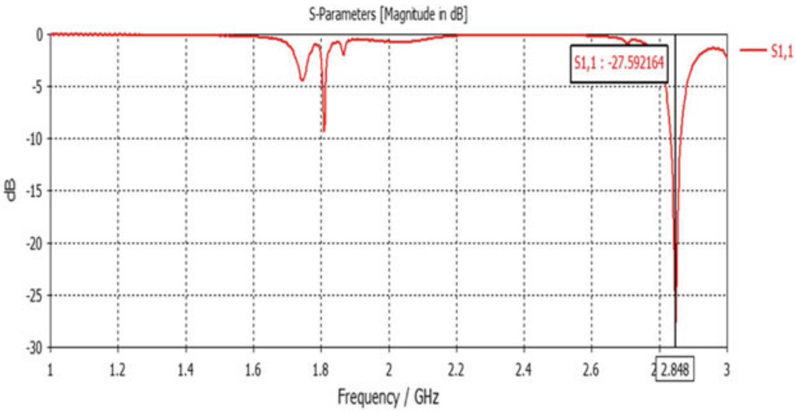


Fig. 30 Return loss plot with EBG structure 5

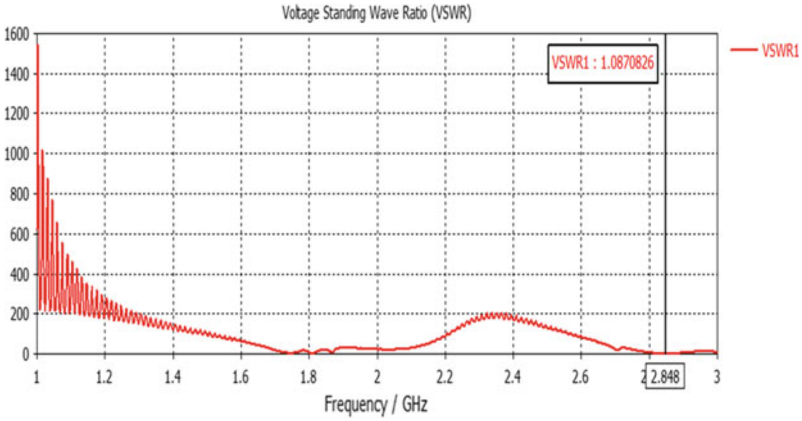
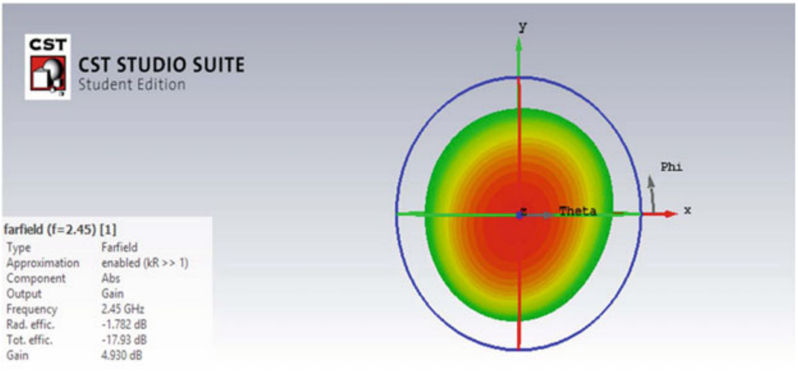


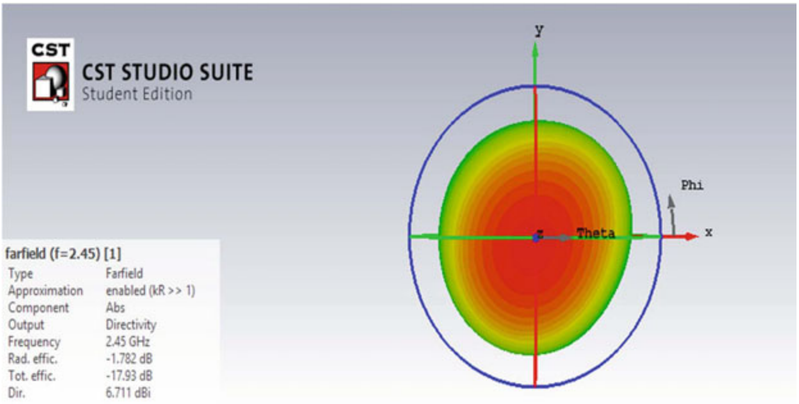
Fig. 31 VSWR plot with EBG structure 5



farfield (f=2.45) [1]

Type	Farfield
Approximation	enabled (kR >> 1)
Component	Abs
Output	Gain
Frequency	2.45 GHz
Rad. effic.	-1.782 dB
Tot. effic.	-17.93 dB
Gain	4.930 dB

Fig. 32 Gain with EBG structure 5



farfield (f=2.45) [1]

Type	Farfield
Approximation	enabled (kR >> 1)
Component	Abs
Output	Directivity
Frequency	2.45 GHz
Rad. effic.	-1.782 dB
Tot. effic.	-17.93 dB
Dir.	6.711 dBi

Fig. 33 Directivity with EBG structure 5

Table 2 Comparison of performance parameters of MSP with various EBG structures and without EBG

Parameters	Return loss S_{11} (dB)	VSWR	Gain (dB)	Directivity (dBi)	Frequency (GHz)
EBG structure 1	−16.319	1.360	5.225	6.820	1.788
EBG structure 2	−17.435	1.310	4.813	6.849	2.998
EBG structure 3	−18.673	1.263	4.898	6.316	1.746
EBG structure 4	−22.970	1	5.063	6.723	1.884
EBG structure 5	**−27.592**	**1.087**	**4.930**	**6.711**	**2.848**
Without EBG	**−15.691**	**1.392**	**1.765**	**5.143**	**2.12**

considered for analysis, it is obviously observed that the gain of the patch antenna with any of the EBG structure is more than the gain obtained without using EBG structure. While integrating different structures of the EBG layer, their resonances couple each other, and, as a result, a wider bandwidth will be generated and characteristics of the patch antenna such as return loss, gain, VSWR, and directivity vary. At the same time, if importance is given to return loss of the antenna which describes the radiating efficiency of the antenna, the MSP antenna with EBG structure 5 has improved return loss of −27.59 dB at the resonant frequency of 2.848 GHz. Right now, we have designed the antenna using EBG. In future, the proposed method may be further implemented using IoT for improving the overall performance.

References

1. Chougule JSA, Wali UV (2015) Design of flexible microstrip antenna for wearable application. Int J Res Emerg Sci Technol 2(6)
2. Rais NHM, Soh PJ, Malek F et al (2009) A review of wearable antenna. In: 2009 Loughborough antennas & propagation conference. https://doi.org/10.1109/lapc.2009.5352373
3. Tanaka M, Jae-Hyeuk J (2003) Wearable micro-strip antenna. In: The antennas and propagation society international symposium
4. Santas JG, Alomainy A, Yang H (2007) Textile antennas for on body communications: techniques and properties. In: The antennas and propagation, 2007. EuCAP 2007
5. Errifi H, Baghdad A, Badri A, Sahel A (2014) Improving micro-strip patch antenna directivity using EBG superstrate. Am J Eng Res 3(11):125–130 (e-ISSN: 2320-0847 p-ISSN: 2320-0936)
6. Nate K, Tentzeris MM (2015) A novel 3-D printed loop antenna using flexible NinjaFlex material for wearable and IoT applications
7. Kumar R, Singh J, Sohi BS (2016) Hexagonal shaped body wearable textile antenna on EBG substrate material. IJCSMC 5(6):260–266
8. Purohit S, Raval F (2014) Wearable-textile patch antenna using Jeans as substrate at 2.45 GHz. Int J Eng Res Technol 3(5). ISSN: 2278-0181
9. Karpagavalli S, Shaaru Nivetha R, Roland DS (2016) Enhancement of gain in micro-strip patch antenna using EBG structure for WLAN Application. Glob Res Dev J Eng. In: International conference on innovation in engineering and technology (ICIET)-2016, July 2016, e-ISSN:2445-5703
10. Balanis CA (2016) Antenna theory: analysis and design. Wiley
11. Amsaveni BM, Phavithra PJ (2018) Gain enhancement of a square patch antenna using EBG structure. Int J Innov Technol Explor Eng 8(2S). ISSN: 2278-3075
12. Shital L, Vaishali D (2017) Micro strip antenna array with square EBG structure. IOSR J Electron Commun Eng 12(6):58–62 e-ISSN: 2278-2834, p-ISSN: 2278-8735 (Ver. I (November–December 2017)

Design and Implementation of a 3 DOF Arm for Disaster Management

Rajesh Kannan Megalingam, Shree Rajesh Raagul Vadivel, Vamsi Gontu, Deepak Nagalla, Ravi Kiran Pasumarthi and Phanindra Kumar Allada

Abstract Current trend in technology has, in turn, necessitated the amelioration in automation and the ease of performing a task. Robotic arms are playing a decisive role in all aspects of human life irrespective of the application. Not only designing but also understanding them is strenuous. This paper discusses designing and implementation of a transparent 3-degree of freedom (DOF) arm which can be analyzed and controlled to perform divergent dexterity tasks with simple commands in a plain sailing way. The arm illustrated in this paper is mounted on a mobile robot and analyzed performing varied dexterity tasks with motley complexity. A lucid graphical user interface (GUI) is developed using Qt-designer to generate commands to control this arm. In discordance to heavy industrial or complex robotic arms, it can be shifted between places and can be mounted on any platform depending on the application.

Keywords Qt-designer · RQT · GUI · Robot operating system (ROS) · DOF · Universal robot description format (URDF) · Planar workspace

R. K. Megalingam (✉) · S. R. R. Vadivel · V. Gontu · D. Nagalla · R. K. Pasumarthi · P. K. Allada
Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India
e-mail: rajeshkannan@ieee.org

S. R. R. Vadivel
e-mail: shreerajgul@gmail.com

V. Gontu
e-mail: vamsi.gontu2308@gmail.com

D. Nagalla
e-mail: nagalla.deepak@gmail.com

R. K. Pasumarthi
e-mail: ravikiran.p3637@gmail.com

P. K. Allada
e-mail: alladaphanindrakumar@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_136

1 Introduction

Robotic arms are deployed in varied sectors like manufacturing, medicine, and many more. Major intention behind robotic arms is to replace human beings who are involved in dangerous work and also the work that need more accuracy and high precision. A robotic arm is expected to do tasks a human arm is capable of performing but with increased concentration and automation. By implementing robotic arms in different sectors, a task can be accomplished with high accuracy, reduced threat to human life, and in a short time span. In rescue operations, involving humans, the life of rescuer is also at risk as the affected area is unknown and just sending a mobile platform or a robot base is not an efficient way of rescuing. A robotic arm can be mounted on a mobile platform which can be used to clear debris and obstacles on its way and to interact with victims.

The triumphant deployment of a robotic arm needs a better understanding and precise analysis in first place. Several aspects like designing, fabricating, manufacturing, programming, and many more are involved in making a robotic arm work properly. The efficiency of arm is dependent on the workspace, accuracy, collision avoidance, ease of control, etc. More the DOF more is the work space and efficiency. Complexity in deployment increases simultaneously. Controlling the arm is also a key aspect as a task can be accomplished as expected only when it can be controlled with ease and when it responds as the controller expects it to respond.

2 Motivation and Problem Statement

A Robotic arm helps in the search and rescue operations. It helps us to locate victims in location where a person or a robot itself cannot enter in search and rescue operations. The robotic arm helps us in the cluttered areas during the natural disasters. But the problem of developing an arm with more degrees of freedom is, it is complex to design and build. It is also very expensive. It is risky for a human to save the life other in complicated situations. So in order to help the people in such type of situations, we can use the robotic arm. When the robotic arm is mounted on the robot it helps the controller to carry the rubble piles at the situation.

3 Related Works

Paper [1] discusses about developing of a mechanical design using CAD and simulating it using RoboAnalyzer software. It explains that the control of the robotic arm depends on the dexterity and manipulability of the arm. Paper [2] describes a new method for sliding mode control mechanism to reduce the disturbance in the control without affecting the performance or robustness of the system. It explains a law which adapts to the changes in the functionality of the system without affecting its performance. Paper [3] discusses about interfacing of a robotic arm using motion planning to control the arm to pick and place the objects using Robotic Operating System (ROS). Paper [4] explains about manually controlling of a robotic arm with a miniature version of the robotic arm using Bluetooth wireless technology controlled by human operator. Paper [5] discusses about controlling of a robotic arm by mimicking the human arm using "Kinect Skeletal Project" of Kinect SDK. It explains about controlling of the robotic arm using serial communication of Arduino microcontroller. Paper [6] discusses about the development of a robotic arm which is controlled using Bluetooth wireless interface that is attached to a pole, which can be used for pruning and harvesting fruits. Paper [7] describes about a new manipulation strategy to grasp various objects stably using a dual-arm robotic system in the ROS environment. To grasp an object, an operability index of the dual-arm robot (OPIND) has been defined. The manipulability index of both arms has been derived using the Jacobian matrix. Paper [8] discusses about a new approach with enough flexibility which can be potentially applicable for different scenarios in pick and place of objects using Robotic Operating System (ROS). Paper [9] presents Xinxin, an intelligent interaction service robot which can simultaneously localize and map the area using SLAM mapping which can be interacted with the robotic arm using voice command, remote control using ROS. Paper [10] describes about the design and implementation of a robotic arm on a wheel chair system to control it using teleoperation controls or voice command using ROS. Paper [11] describes about developing of a 6 DOF arm using counterbalance mechanism (CBM) to maintain high performance and reduce the torque required to move the arm. Paper [12] discusses about developing of a robotic arm using non-linear spring mechanism which reduces the torque on the joints thereby providing position accuracy and collision safety of the robotic arm.

4 Architectural Diagram

Robotic arm discussing in this paper follows the master–slave configuration. This is one of the finest configurations that helps. It means the slave performs the tasks as per the master commands that run the master system.

4.1 Control Station

Control station works as the ROS-master that refer to the controller and that communicates between the different nodes like joystick, keyboard, and GUI. These interfaces are used for different purposes in controlling the arm. The time instances of the published and the received data between ROS-master and ROS-slave should be in sync else the data will be ignored. These GUI values are published by the topics /cmd_vel and /joint_states.

Joystick. A customised Joystick is used for establishing a user friendly control of the arm. The signals from joystick are published over the /joint_state topic by the ROS-master running in the system on controller side. A topic is a virtual connection between two nodes, which acts as a link between them as the data is transferred.

Keyboard. Another mode of control is using a keyboard, where the characters on keyboard are used to control the arm. Each character clicked on the keyboard will be published to ROS-slave which is running on the robot via a topic named /cmd_vel.

GUI. GUI is designed to provide the user a visual feed from the camera on the arm. Qt-designer a package for designing GUI, integrated with ROS is used for displaying the received feed from cameras. The GUI can also be designed to send data to the ROS-slave for controlling the arm.

4.2 Base Station

From Fig. 1 base station refers to the robot. It includes both software and hardware. ROS-slave subscribes the topics from the ROS-master and they are sent to the

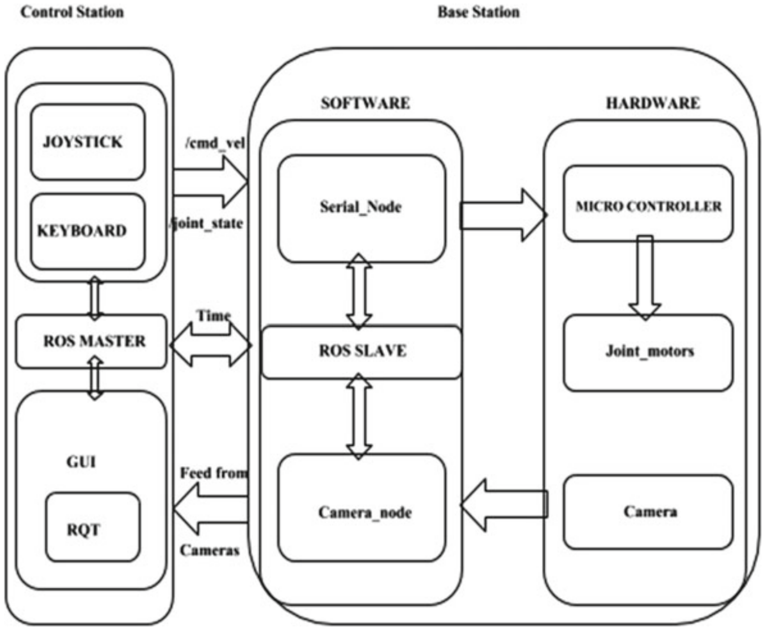


Fig. 1 Architectural diagram

microcontroller, joints, and the camera. When the camera and the microcontroller subscribe, they execute their tasks and send back the information to the ROS-master.

4.2.1 Software

Serial_node. Serial_node is a ROS node running as part of ROS-slave running in the base station. It establishes a serial communication with the microcontroller which controls the arm based on the commands sent from the control station. It also monitors the connection between microcontroller and base station throughout the run.

Camera Node. This node is responsible for initialising the camera and transmitting the feed to ROS-slave, which in turn publishes this to the GUI of ROS-master. The data from cameras is converted to different formats and the controller can choose any based on different factors like transmission power of antenna, transmission strength, noise in the transmission medium, and delay caused during transmission.

5 Design and Implementation

The robotic arm has a planar workspace in X–Z plane. Three linear actuators are used at all the three DOF's. The design is made in such a way that it had a vast planar workspace of −30° to 120° (Fig. 2). The first DOF is limited to 0°–125°, the second DOF is limited from 0° to 145°, and the third DOF is limited from 0° to 138°. The payload of the arm is 4–5 kg. Maximum reach length of the arm is 158 cm. It is very easy to fix the arm on a stable surface or on a movable wheeled robot; hence, it can also work as a spherical jointed robotic arm according to the base is mounted to. As the payload of the arm is of 5kgs and the reach length is 158 cm, this can act as a pick and place robotic arm. The design all can be manufactured by laser cutting and it is very easy to implement. The compressed dimension of the arm is very less that it can easily accommodate in the very less space of 15 × 80 × 8 cm (Fig. 3). The weight of the arm is 6 kg such that it can be carried easily.

5.1 Software

This paper is mainly concerted on the graphical user interface (GUI) that works on the Qt-platform which is an object-oriented application framework. This platform is used in many softwares in order to perform multiple applications that run on many of the desktops. Qt-designer is a GUI tool in Qt which forms a .ui file when widgets and objects are added to it. RQT is a software shell of ROS that enacts the various GUI tools in the form of plugins. When these plugins are enabled in the RQT, the respective package should run in order to work the GUI appropriately.

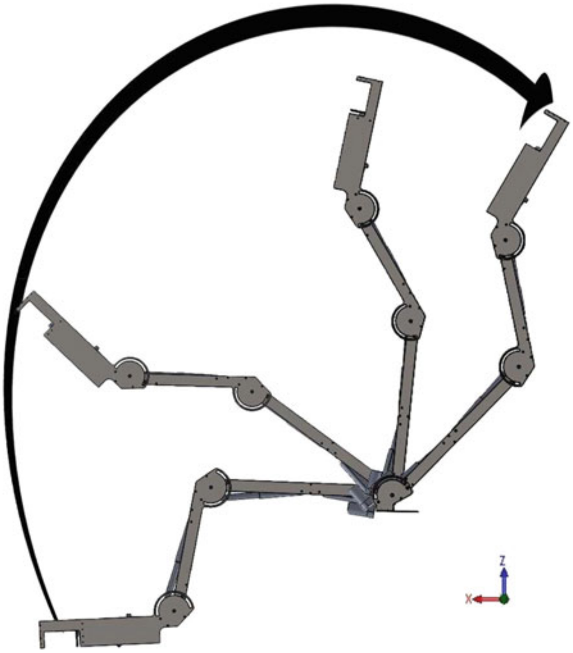


Fig. 2 Workspace of the arm

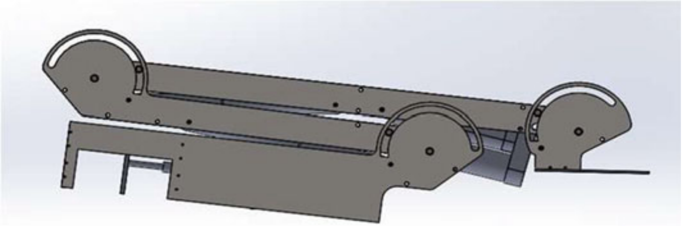


Fig. 3 Compressed position

The three DOFs of the robotic arm is a joint-by-joint control algorithm using multiple GUIs in different ways. Using sliders (Qslider) and radio buttons (Qradiobutton) widgets in a single GUI in Fig. 4, and the other GUI is an integration of line edit (Qlineedit) and a push button that can be seen in Fig. 5.

Figure 4 shows the control of the first three DOFs of the arm using sliders and the grippers are also being controlled by sliders. In Fig. 5, it was explained about the values of the angles that the respective DOF should rotate which can be given in the edit line that can be sent using the push button.

Arduino. The 3-DOF arm is programmed using the Arduino software. Since Arduino provides UART TTL serial communication, the whole arm is implemented

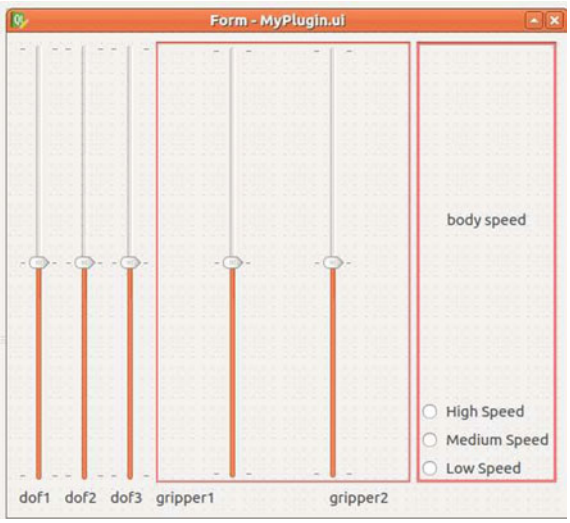


Fig. 4 Slider-based control

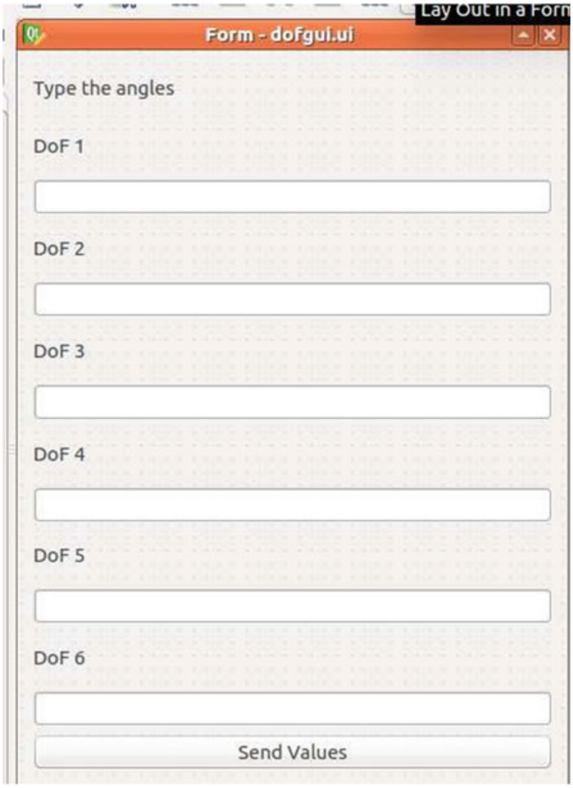
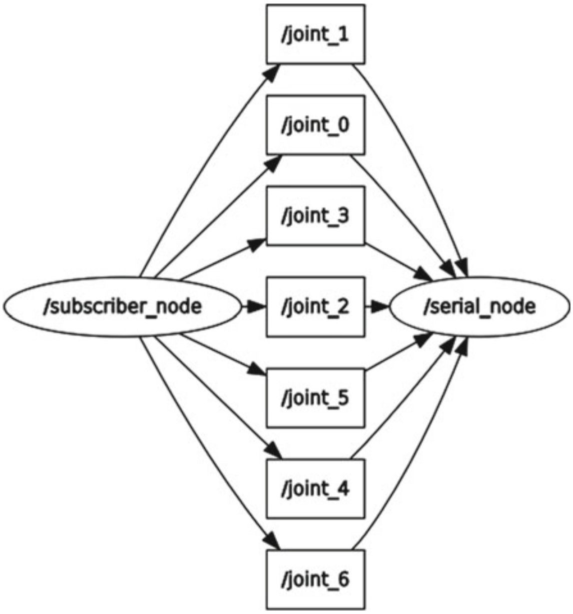


Fig. 5 Angle-based control

Fig. 6 ROS rqt_graph



using this communication. The actuators that used in this robotic arm work as same as the normal dc motor. End effector of the arm is also programmed using Arduino.

ROS Platform. ROS includes the mastering of nodes, multiplexing of data, and allows distributed performance over the multicore and multiprocessor. ROS lines are added to Arduino code to communicate between the nodes. These nodes publish and subscribe using different topics in order to establish the connections between the DOFs. In Fig. 6, it shows that the different topics have been published on the serial node. Here, the topics (/joint_0, /joint_1, /joint_2) are subscribed by the /subscriber_node and published on the /serial_node.

When camera is used to know the position of the gripper, camera node is also attached to Fig. 6 Usb_cam is the package used to run the camera on the arm. When RQT is launched, selecting the plugins icon → visualisation → image_view a window is popped on the GUI in which the usb_cam_compressed topic is being selected to the view the camera.

5.2 Hardware

The robotic arm that mentioned in the above context is employed with Arduino ATmega328 microcontroller using serial communication between the three motors. Two bullet and lact4 linear actuators had been used in the three DOFs. Dual motor drivers with 6–18 V compatible 20 capable specifications were used in this arm. A window shaft motor (wiper motor) is used to control the gripper. The position of

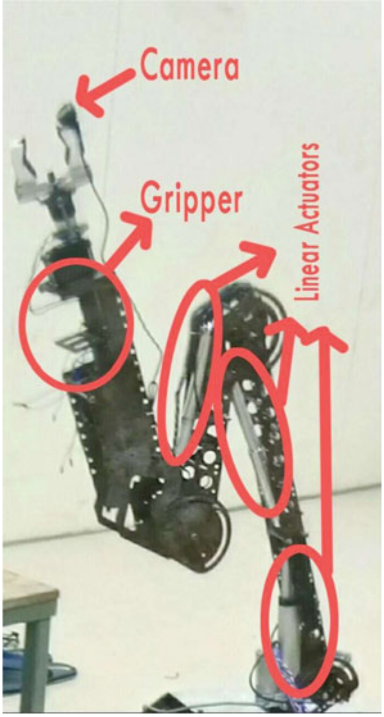


Fig. 7 Arm with gripper and camera

the gripper can be known from the camera attached to the end effector. There is an emergency switch that is attached at the gripper, if the gripper has extended to its maximum position it triggers and make the working of the gripper to stop.

In Fig. 7, it is shown how the actuators are mounted and assembled to one joint to another. It is also shown that the placement of camera on the gripper and how the gripper moves in Fig. 8.

Gripper. The griper of the above robotic arm is a unique one, which is capable of holding a block of 10 cm. The lever mechanism in Fig. 9 is used in this gripper. A high torque worm geared dc motor Fig. 10 (window lift motor) is used for the implementation of the lever mechanism. The holding torque of the gripper is 35 kg cm. There is very less backlash in the gripper and which is helpful in the precise working of gripper.

6 Experiments and Results

This section lists the results of experiments that we performed with the 3 DOF robotic arm.

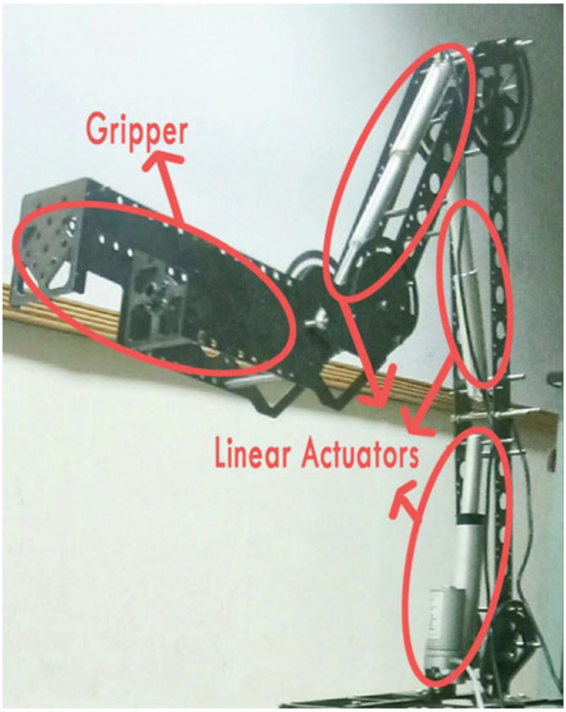


Fig. 8 Arm without camera mount

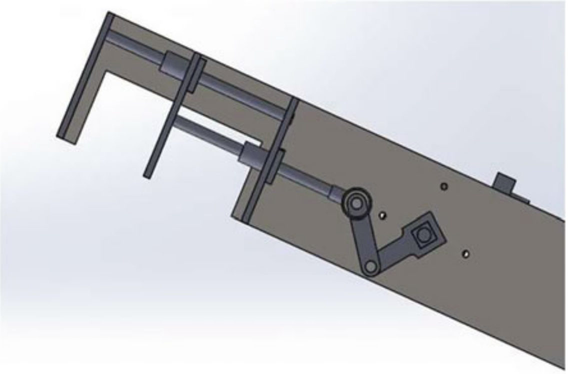
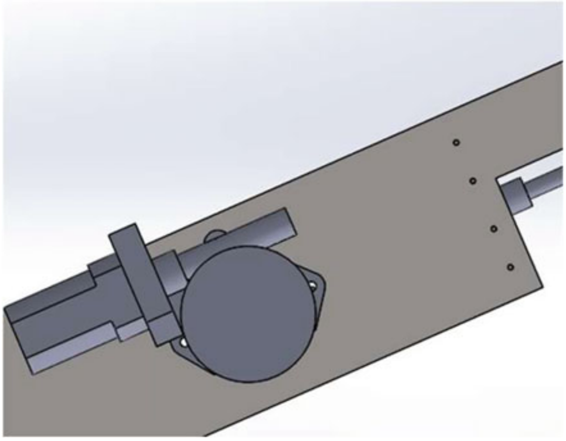


Fig. 9 Lever mechanism

Fig. 10 Motor used for gripper



In the first case, in Table 1, the base is free to move toward any direction; hence in that case, it can reach any point in the X–Y plane without any restrictions. But in the case toward the Z-axis which is normal to the arm it cannot extend more than

Table 1 X, Y, and Z positioning of the arm

Arena condition	Location			Test result
	X	*Y*	*Z*	
Free movement of base is allowed	0.1	0	0	Pass
	0.56	0	0	Pass
	1.68	0	0	Pass
	0	0.1	0	Pass
	0	0.56	0	Pass
	0	1.68	0	Pass
	0	0	0.1	Pass
	0	0	0.56	Pass
	0	0	1.68	Fail
Base is fixed at point of start	0.1	0	0	Fail
	0.56	0	0	Pass
	1.68	0	0	Fail
	0	0.1	0	Fail
	0	0.56	0	Pass
	0	1.68	0	Fail
	0	0	0.1	Fail
	0	0	0.56	Pass
	0	0	1.68	Fail

Table 2 Boundaries in *X*, *Y*, and *Z* axes

Axis	Boundaries of the arm	
	Min	Max
X-axis	0.48	1.42
Y-axis	0.48	1.42
Z-axis	0.54	1.63

the restricted value so the task has failed. In the second case, in Table 2, the base movement is restricted so the arm can only reach the points which are in its boundary. Hence, the arm fails to complete the tasks which are out of boundary.

7 Conclusion

The successful deployment of a 3 DOF robotic arm is described in this work. The arm is mounted on a mobile base which is tested for rescue operations in simulated arenas. The arm is able to do the dexterity check tasks like pick and place, turning valves, and few other. As the arm has planar workspace in *x*- and *z*-planes, an object in *y*-plane can be altered only by rotating the mobile platform. But, when the arena is narrow, and if the object is in *y*-plane, the task cannot be performed as the body cannot be moved. The complexity in deploying this arm is very less and it is well suited for running basic tests for evaluating the complexity of task.

Acknowledgements We express our gratitude and thankfulness to Humanitarian Technology Labs and the Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri Campus for helping us to complete this work.

References

1. Hussain SB, Kanwal F (2016) Design of a 3 DoF robotic arm. In: The sixth international conference on innovative computing technology (INTECH 2016) on 24–26 August in Dublin, Ireland
2. Fallaha C, Saad M, Kanaan H (2007) Sliding mode control with exponential reaching law applied on a 3 DOF modular robotic arm. In: Proceedings of the European control conference 2007 on July 2–5 in Kos, Greece
3. Hernandez-Mendez S, Maldonado-Mendez C, Marin-Hernandez A, Rios-Figueroa HV, Vazquez-Leal H, Palacios-Hernandez ER (2017) Design and implementation of a robotic arm using ROS and Moveit! In: IEEE international autumn meeting on power, electronics and computing (ROPEC) on 8–10 November 2017 in Ixtapa, Mexico
4. Megalingam RK, Boddupalli S, Apuroop KGS (2017) Robotic arm control through mimicking of miniature robotic arm. In: International conference on advanced computing and communication systems (ICACCS) on Jan 06–07 2017 in Coimbatore, India
5. Megalingam RK, Saboo N, Ajithkumar N, Unny S, Menon D (2013) Kinect based gesture controlled Robotic arm: a research work at HuT labs. In: IEEE international conference in

MOOC, innovation and technology in education (MITE) on 20–22 December 2013 in Jaipur, India

6. Megalingam RK, Vignesh N, Sivanantham V, Elamon N, Sharathkumar MS, Rajith V (2016) Low cost robotic arm design for pruning and fruit harvesting in developing nations. In: International conference on intelligent systems and control (ISCO) on 7–8 Jan 2016 in Coimbatore, India
7. Kim D-E, Park D-J, Moon J-H, Kim K-S, Park J-H, Lee J-M (2017) Development of a robot manipulation technology in ROS environment. In: IEEE international conference on multisensor fusion and integration for intelligent systems (MFI) on 16–18 November 2017 in Daegu, South Korea
8. Tavares P, Sousa A (2015) Flexible pick and place architecture using ROS framework. In: Iberian conference on information systems and technologies (CISTI) on 17–20 June 2015 in Aveiro, Portugal
9. Zhaohui Z, Xuesong M, Xu B, Hanghang C, Jian T (2016) Development of an intelligent interaction service robot using ROS. In: IEEE advanced information management, communicates, electronic and automation control conference (IMCEC) on 3–5 October 2016 in Xi'an, China
10. Tremblay T, Padir T (2013) Modular robot arm design for physical human–robot interaction. In: IEEE international conference on systems, man and cybernetics on 13–16 Oct 2013 in Manchester, UK
11. Lee W-B, Lee S-D, Song J-B (2017) Design of a 6-DOF collaborative robot arm with counterbalance mechanisms. In: IEEE international conference on robotics and automation (ICRA) on 29 May–3 June 2017 in Singapore
12. Park J-J, Kim H-S, Song J-B (2009) Safe robot arm with safe joint mechanism using nonlinear spring system for collision safety. In: IEEE international conference on robotics and automation on 12–17 May 2009 in Kobe, Japan

Correction to: A Semi-supervised Approach to Detect Malicious Nodes in OBS Network Dataset Using Gaussian Mixture Model

Md. Kamrul Hossain and Md. Mokammel Haque

Correction to:
Chapter "A Semi-supervised Approach to Detect Malicious Nodes in OBS Network Dataset Using Gaussian Mixture Model" in: G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89, https://doi.org/10.1007/978-981-15-0146-3_66

The original version of the book was published with incorrect corresponding author of Chapter "A Semi-supervised Approach to Detect Malicious Nodes in OBS Network Dataset Using Gaussian Mixture Model" "Muhammad Kamrul Hossain Patwary" (informal name) has been corrected to "Md. Kamrul Hossain" (official name). The chapter and book have been updated with the changes.

The updated version of this chapter can be found at
https://doi.org/10.1007/978-981-15-0146-3_66

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_137

Author Index

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3