

Lecture Notes in Networks and Systems 8

H. S. Saini

Rishi Sayal

Sandeep Singh Rawat *Editors*

Innovations in Computer Science and Engineering

Proceedings of the Fourth ICICSE 2016

 Springer

Lecture Notes in Networks and Systems

Volume 8

Series editor

Janusz Kacprzyk, Polish Academy of Sciences, Warsaw, Poland
e-mail: kacprzyk@ibspan.waw.pl

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.

Advisory Board

Fernando Gomide, Department of Computer Engineering and Automation—DCA, School of Electrical and Computer Engineering—FEEC, University of Campinas—UNICAMP, São Paulo, Brazil

e-mail: gomide@dca.fee.unicamp.br

Okyay Kaynak, Department of Electrical and Electronic Engineering, Bogazici University, Istanbul, Turkey

e-mail: okyay.kaynak@boun.edu.tr

Derong Liu, Department of Electrical and Computer Engineering, University of Illinois at Chicago, Chicago, USA and

Institute of Automation, Chinese Academy of Sciences, Beijing, China

e-mail: derong@uic.edu

Witold Pedrycz, Department of Electrical and Computer Engineering, University of Alberta, Alberta, Canada and

Systems Research Institute, Polish Academy of Sciences, Warsaw, Poland

e-mail: wpedrycz@ualberta.ca

Marios M. Polycarpou, KIOS Research Center for Intelligent Systems and Networks, Department of Electrical and Computer Engineering, University of Cyprus, Nicosia, Cyprus

e-mail: mpolycar@ucy.ac.cy

Imre J. Rudas, Óbuda University, Budapest Hungary

e-mail: rudas@uni-obuda.hu

Jun Wang, Department of Computer Science, City University of Hong Kong Kowloon, Hong Kong

e-mail: jwang.cs@cityu.edu.hk

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

H.S. Saini · Rishi Sayal · Sandeep Singh Rawat
Editors

Innovations in Computer Science and Engineering

Proceedings of the Fourth ICICSE 2016

 Springer

Editors

H.S. Saini
Guru Nanak Institutions
Ibrahimpattam, Telangana
India

Sandeep Singh Rawat
Guru Nanak Institutions
Ibrahimpattam, Telangana
India

Rishi Sayal
Guru Nanak Institutions
Ibrahimpattam, Telangana
India

ISSN 2367-3370 ISSN 2367-3389 (electronic)
Lecture Notes in Networks and Systems
ISBN 978-981-10-3817-4 ISBN 978-981-10-3818-1 (eBook)
DOI 10.1007/978-981-10-3818-1

Library of Congress Control Number: 2017932092

© Springer Nature Singapore Pte Ltd. 2017

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

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, express 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.

Printed on acid-free paper

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

Preface

The volume contains 41 papers presented at the 4th International Conference on Innovations in Computer Science and Engineering (ICICSE 2016) held during 22–23 July, 2016 at Guru Nanak Institutions Campus in association with CSI Hyderabad Chapter.

The focus of the 4th ICICSE 2016 is to provide an opportunity for all the professionals and aspiring researchers, scientists, academicians and engineers to exchange their innovative ideas and new research findings in the field of computer science and engineering. We have taken an innovative approach to give an enhanced platform for these personnel, participants, researchers, students and other distinguished delegates to share their research expertise, experiment breakthroughs or vision in a broad criterion of several emerging aspects of computing industries. The conference received an overwhelming response in terms of number of submissions from different fields pertaining to innovations in the field of computer science in main tracks and special session. After a rigorous peer-review process through our program committee members and external reviewers, we accepted 41 submissions with an acceptance ratio of 0.38.

ICICSE 2016 was inaugurated by Dr. Anirban Basu, President, Computer Society of India. The guest of honors were Dr. A. Govardhan, Principal, JNTUCEH, Ms. G. Sandhya, Senior Program Manager Microsoft India, Mr. Raju Kanchibotla, Southern, Regional Vice President, CSI and Dr. Raghav Kune, Scientist, ADRIN and ISRO.

We take this opportunity to thank all keynote speakers and special session chairs for their excellent support to make ICICSE 2016 a grand success. We would like to thank all reviewers for their time and effort in reviewing the papers. Without their commitment it would not have been possible to have the important ‘referee’ status assigned to papers in the proceedings. The quality of these papers is a tribute to the authors and also to the reviewers who have guided any necessary improvement. We are indebted to the program committee members and external reviewers who have contributed towards excellent reviews and in a very short span of time. We would also like to thank CSI Hyderabad Chapter having coming forward to support us to organize this mega event.

We would also like to thank the authors and participants of this conference. Special thanks to all the volunteers for their tireless efforts. All the efforts are worth and would please us all, if the readers of these proceedings and participants of this conference rate the papers and the event inspiring and enjoyable.

Finally, we place our special sincere thanks to the press, print and electronic media for their excellent coverage of this conference.

Ibrahimpattam, India

H.S. Saini
Rishi Sayal
Sandeep Singh Rawat

Organizing Committee

Patrons

Sardar Tavinder Singh Kohli
Sardar Gagandeep Singh Kohli

Conference Chair

Dr. H.S. Saini

Conference Co-Chairs

Dr. Veeranna
Dr. D.D. Sharma
Dr. S. Sreenatha Reddy
Dr. Rishi Sayal

Convenors

Dr. S. Masood Ahamed
Prof. V. Deva Sekhar
Dr. K. Madhusudana
Dr. Sandeep Singh Rawat
Ms. Thayyaba Khattoon

Co-Convenors

Dr. V. Sathiyasuntharam
Mr. S. Madhu
Mr. Lalu Nayak
Mrs. Subbalakshmi
Mrs. D. Sirisha
Mr. D. Saidulu
Mr. Ch. Ravindra

Conference Committee

Dr. Rishi Sayal
Mr. B. Sudhakar
Mr. M. Bharath
Mr. B. Nandan
Mr. Manikrao Patil

Publicity Chair International

Dr. D.D. Sharma
Mr. Imran Quereshi
Ms. E. Swetha Reddy
Ms. Thayyaba Khatoon
Mr. V. Poorna Chandra
Mr. B. Venkateswarlu

Publicity Chair National

Prof. V. Deva Sekhar
Mr. Y. Ravi Kumar
Ms. Kanchanlatha
Mr. D. Kiran Kumar
Ms. B. Mamatha

Program and Publication Chair

Ms. Thayyaba Khatoon
Mr. T. Ravindra
Mrs. K. Prasunna
Mr. K. Suresh
Mr. Devi Prasad Mishra
Mr. Nusrath Khan

Accommodation Committee

Dr. S. Masood Ahamed
Mr. A. Ravi
Mr. A. Vinay Sagar
Mr. B. Sudhakar
Mr. A. Srinivas
Mr. A. Ugendar

Advisory Board-International/National, Technical Program Committee

Dr. San Murugesan, Australia
Dr. Hemant Pendharkar, USA
Dr. Chandrashekar Commuri, USA
Dr. Muzammil H. Mohammed, Saudi Arabia
Dr. William Oakes, USA
Dr. Sartaj Sahni, USA
Dr. Jun Suzuki, USA
Dr. Prabhat Kumar Mahanti, Canada
Mrs. Sunitha B., Melbourne, Australia
M. Siva Ganesh, USA
Dr. Maliyanath Sundaramurthy, USA
Dr. Raj Kamal, India
Prof. Bipin V. Meheta, India
Dr. A. Damodaram, India
Dr. Amirban Basu, India
Dr. P.S. Avadhani, India
Dr. D.C. Jinwala, India
Dr. Aruna Malapadi, India
Mr. Ravi Sathanapalli, India

Dr. Sohan Garg, India
Dr. C. Shoba Bindu, India
Mr. Raju Kancibhotla, India
Prof. Rajkumar Buyya, Australia
Dr. Anuj Sharma, USA
Dr. Stephanie Farell, USA
Dr. Arun Somani, USA
Prof. Pascal Lorenz, France
Dr. Vamsi Chowdavaram, Canada
Mr. M. Kiran, CTS, New Jersey, USA
Dr. Lakshmivarahan, USA
Dr. S.R. Subramanya, USA
Dr. Sitalakshmi Venkataraman, Australia
Prof. Avula Damodaram, India
Dr. A. Govardhan, India
Dr. V. Kamakshi Prasad, India
Mr. H.R. Mohan, India
Dr. D.V.L.N. Somayajulu, India
Dr. Naveen Kumar, India
Dr. Uday Bhaskar Vemulapati, India
Dr. R.B.V. Subramanyam, India
Dr. Vijaylakshmi, India
Dr. K.P. Supreethi, India
Mr. Ramanathan, India

A Note from the Organizing Committee

Welcome to the 4th International Conference on Innovations in Computer Science & Engineering, India. On behalf of the entire organizing committee, we are pleased to welcome you to ICICSE-2016.

ICICSE, as the conference in the field, offers a diverse program of research, education, and practice-oriented content that will engage computer science engineers from around the world. The two-day core of the meeting is anchored by the research paper track. This year, the research paper track received 151 submissions. The papers underwent a rigorous two-phase peer-review process, with at least two program committee members reviewing each paper. The program committee selected 41 papers. All members of the program committee attended the meeting. These papers represent world-wide research results in computer science engineering.

Planning and overseeing the execution of a meeting of ICICSE is an enormous undertaking. Making ICICSE-2016 happen involved the combined labor of more than 50 volunteers contributing a tremendous amount of time and effort. We offer our sincere thanks to all the committee members and volunteers, and encourage you to take the opportunity to thank them if you meet them here. We would also like to thank all our sponsors who helped in making this event accessible to the Computer Science Engineering community.

Finally, we would like to thank the editorial board of Springer for agreeing to publish the proceedings and the staff at the editorial office for all their help in the preparation of the Proceedings.

Dr. H.S. Saini
Professor and Managing Director

Dr. Rishi Sayal
Professor and Associate Director

Dr. Sandeep Singh Rawat
Professor and Head-CSE

Contents

Comparative Study of Techniques and Issues in Data Clustering	1
Parneet Kaur and Kamaljit Kaur	
Adaptive Pre-processing and Regression of Weather Data	9
Varsha Pullabhotla and K.P. Supreethi	
A Comparative Analysis for CBIR Using Fast Discrete Curvelet Transform	15
Katta Sugamya, Suresh Pabboju and A. Vinaya Babu	
Compute the Requirements and Need of an Online Donation Platform for Non-monetary Resources Using Statistical Analyses	29
Surbhi Paltani, Saru Dhir and Avi Bhardwaj	
Enacting Segmentation Algorithms for Classifying Fish Species	39
Madhulika Bhatia, Madhulika Pandey, Neeraj Kumar, Madhurima Hooda and Akriti	
Pattern Based Extraction of Times from Natural Language Text	51
Vanitha Guda and Suresh Kumar Sanampudi	
Evaluating the Performance of Tree Based Classifiers Using Zika Virus Dataset	63
J. Uma Mahesh, P. Srinivas Reddy, N. Sainath and G. Vijay Kumar	
SaaS CloudQual: A Quality Model for Evaluating Software as a Service on the Cloud Computing Environment	73
Dhanamma Jagli, Seema Purohit and N. Subash Chandra	
A Survey on Computation Offloading Techniques in Mobile Cloud Computing and Their Parametric Comparison	81
Sumandeep Kaur and Kamaljit Kaur	
A Proposed Technique for Cloud Computing Security	89
Kanika Garg and Jaiteg Singh	

Optimizing Job Scheduling in Federated Grid System	97
Akshima Aggarwal and Amit Chhabra	
A SDE—The Future of Cloud	105
N. Leelavathy, D.S.M. Rishitha and M. Sushmitha	
Cloud Security-Random Attribute Based Encryption	113
V. Havisha, P.V. Padmavathi and S.V. Ramanamurthy	
Cloud VM/Instance Monitor Phase-II (CIM-PII) Subsystem of eCloudIDS	121
Madhan Kumar Srinivasan, P. Revathy and Keerthi Balasundaram	
A Review on Big Data Mining in Cloud Computing	131
Bhaludra R. Nadh Singh and B. Raja Srinivasa Reddy	
Implementation of Fuzzy Logic Scheduler for WiMAX in Qualnet	143
Akashdeep	
A Survey of Evolution of IEEE 802.16 Certification and Standardization	151
Akashdeep	
Mutual Trust Relationship Against Sybil Attack in P2P E-commerce	159
D. Ganesh, M. Sunil Kumar and V.V. Rama Prasad	
Adaptive Block Based Steganographic Model with Dynamic Block Estimation with Fuzzy Rules	167
Mohanjeet Kaur and Mamta Juneja	
Secure Geographical Routing Using an Efficient Location Verification Technique	177
S.L. Aruna Rao and K.V.N. Sunitha	
Time-Efficient Discovery of Moving Object Groups from Trajectory Data	185
Anand Nautiyal and Rajendra Prasad Lal	
Impact on Wave Propagation in Underground to Above Ground Communication Through Soil for UWB Buried Antenna at 3.5 GHz	193
Vandana Laxman Bade and Suvarna S. Chorage	
A Comprehensive Architecture for Correlation Analysis to Improve the Performance of Security Operation Center	205
Dayanand Ambawade, Pravin Manohar Kedar and J.W. Bakal	

Systematic Approach to Intrusion Evaluation Using the Rough Set Based Classification 217
 R. Ravinder Reddy, Y. Ramadevi and K.V.N. Sunitha

Host-Based Intrusion Detection System Using File Signature Technique 225
 G. Yedukondalu, J. Anand Chandulal and M. Srinivasa Rao

Intra and Inter Group Key Authentication for Secure Group Communication in MANET 233
 G. Narayana, M. Akkalakshmi and A. Damodaram

Performance of Efficient Image Transmission Using Zigbee/I2C/Beagle Board Through FPGA 245
 D. Bindu Tushara and P.A. Harsha Vardhini

Modified Probabilistic Packet Marking Algorithm for IPv6 Traceback Using Chinese Remainder Theorem 253
 Y. Bhavani, V. Janaki and R. Sridevi

Taxonomy of Polymer Samples Using Machine Learning Algorithms 265
 Kothapalli Swathi, Sambu Ravali, Thadisetty Shravani Sagar and Katta Sugamya

A Comprehensive Analysis of Moving Object Detection Approaches in Moving Camera 277
 Neeraj and Akashdeep

Innovative Approach for Handling Blackouts in the Transmission Grid Through Utilization of ICT Technology 287
 Gresha S. Bhatia and J.W. Bakal

A Comparative Analysis of Iris and Palm Print Based Unimodal and Multimodal Biometric Systems 297
 Yakshita Jain and Mamta Juneja

Fairness Analysis of Fuzzy Adaptive Scheduling Architecture 307
 Akashdeep

A Novel Approach for Emergency Backup Authentication Using Fourth Factor 313
 K. Sharmila, V. Janaki and A. Nagaraju

Automated Cooling/Heating Mechanism for Garments 325
 Akash Iyengar, Dhruv Marwha and Sumit Singh

Anatomization of Software Quality Factors: Measures and Metrics 333
 Aditi Kumar, Madhulika Bhatia, Anchal Garg and Madhurima

Dynamic Scheduling of Elevators with Reduced Waiting Time of Passengers in Elevator Group Control System: Fuzzy System Approach	339
Malan D. Sale and V. Chandra Prakash	
Level Skip VLSI Architecture for 2D-Discrete Wavelet Transform	347
G. Kiran Maye and T. Srinivasulu	
On the Construction and Performance of LDPC Codes	355
B.N. Sindhu Tejaswini, Rajendra Prasad Lal and V. Ch. Venkaiah	
Performance Evaluation of Hysteresis Fed Sliding Mode Control of PMLDC Motor	363
M. Senthil Raja and B. Geethalakshmi	
A Selective Data on Performance Feature with Selective Algorithms	369
M. Bharat, Konda Raveendra, Y. Ravi Kumar and K. Santhi Sree	
Author Index	377

About the Editors

Dr. H.S. Saini, Managing Director of Guru Nanak Institutions, obtained his Ph.D. in Computer Science. He has over 24 years of experience at university/college level in teaching UG/PG students and has guided several B.Tech., M.Tech., and Ph.D. projects. He has published/presented high-quality research papers in international, national journals and proceedings of international conferences. He has two books to his credit. Dr. Saini is a lover of innovation and is an advisor for NBA/NAAC accreditation process to many institutions in India and abroad.

Dr. Rishi Sayal, Associate Director of Guru Nanak Institutions Technical Campus, has done B.E. (CSE), M.Tech. (IT), Ph.D. (CSE), LMCSI, LMISTE, MIEEE, MIAENG (USA). He has completed his Ph.D. in Computer Science and Engineering in the field of data mining from prestigious and oldest Mysore University of Karnataka state. His research work is titled “Innovative Methods for Robust and Efficient Data Clustering”. He has published 22 research papers in international journals and conferences to support his research work (one paper being awarded the best paper in ICSCI 2008 supported by Pentagram Research Centre, India). He has over 25 years of experience in training, consultancy, teaching, and placements. His major accomplishments: Coordinator of professional chapter including IEEE, reviewer of IJCA (International Journal of Computer Association, USA). He is member of international association of engineers and guided more than 20 PG students. His current areas of research interest include data mining, network security, and databases.

Dr. Sandeep Singh Rawat obtained his Bachelor of Engineering in Computer Science from National Institute of Technology, Surat (formerly REC, Surat) and his Masters in Information Technology from Indian Institute of Technology, Roorkee. He was awarded Doctorate in Computer Science and Engineering by University College of Engineering, Osmania University, Hyderabad in 2014. He has been working at Guru Nanak Institutions Hyderabad since 2009 and he has 12 years of teaching and 2 years of industrial experiences. His current research interests include data mining, grid computing and data warehouse technologies. He is a life member of technical societies like CSI, ISTE, and member of IEEE.

Comparative Study of Techniques and Issues in Data Clustering

Parneet Kaur and Kamaljit Kaur

Abstract Data mining refers to the extraction of obscured prognostic details of data from large databases. The extracted information is visualized in the form of charts, graph, tables and other graphical forms. Clustering is an unsupervised approach under data mining which groups together data points on the basis of similarity and separate them from dissimilar objects. Many clustering algorithms such as algorithm for mining clusters with arbitrary shapes (CLASP), Density peaks (DP) and k-means are proposed by different researchers in different areas to enhance clustering technique. The limitation addressed by one clustering technique may get resolved by another technique. In this review paper our main objective is to do comparative study of clustering algorithms and issues arising during clustering process are also identified.

Keywords Data mining · Database · Clustering · k-means clustering · Outliers

1 Introduction

Data mining is used for analyzing huge datasets, finds relationships among these datasets and in addition the results are also summarized which are useful and understandable to the user. Today, large datasets are present in many areas due to the usage of distributed information systems [1]. Sheer amount of data is stored in world today commonly known as big data. The process of extracting useful patterns of knowledge from database is called data mining. The extracted information is visualized in the form of charts, graphs, tables and other graphical forms. Data

P. Kaur (✉) · K. Kaur

Department of Computer Engineering and Technology, Guru Nanak Dev University,
Amritsar, India
e-mail: parneetbriar23@yahoo.in

K. Kaur

e-mail: kamal.aujla86@gmail.com

© Springer Nature Singapore Pte Ltd. 2017

H.S. Saini et al. (eds.), *Innovations in Computer Science and Engineering*,
Lecture Notes in Networks and Systems 8, DOI 10.1007/978-981-10-3818-1_1

mining is also known by another name called KDD (Knowledge Discovery from the Database). The data present in database is in structured format whereas, data warehousing may contain unstructured data. It is comparatively easier to handle static data as compared to dynamically varying data [2]. Reliability and scalability are two major challenges in data mining. Effective, efficient and scalable mining of data should be achieved by building incremental and efficient mining algorithms for mining large datasets and streaming data [1]. In this review paper our main objective is to do the comparative study of clustering algorithms and to identify the challenges associated with them.

2 Clustering in Data Mining

Clustering means putting objects having similar properties into one group and the objects with dissimilar properties into another. Based on the given threshold value the objects having values above and below threshold are placed into different clusters [1]. A cluster is group of objects which possess common characteristics. The main objective in clustering is to find out the inherent grouping in a set of unlabeled data [2]. Clustering is referred to as unsupervised learning technique because of the absence of classifiers and their associated labels. It is a type of learning by observation technique [3]. Clustering algorithm must satisfy certain requirements such as, it should be scalable, able of dealing with distinct attributes, capable of discovering arbitrary shaped clusters, and must possess minimal requirements for domain knowledge to determine input parameters. In addition, it should deal with noise and outliers [4–6].

2.1 Partitioning Clustering

In partitioning methods the instances are relocated and are moved from one cluster to another by starting the relocation from initial partitioning. The number of clusters to be formed is user defined. Examples of partitioning algorithms include Clustering Large Datasets Algorithm (CLARA) and k-means [7].

2.2 Density Based Clustering

These methods are based upon density and the cluster grows till the time the density does not exceed some threshold value. Density Based Spatial Clustering of Applications with Noise (DBSCAN) approach is a density based technique which is based on the idea that the least number of data points (Minpts) must be present around a point in its neighbourhood with radius (ϵ) [2].

2.3 Model Based Clustering

Model based approaches exaggerate the fit among the dataset and few mathematical models. The mathematical model generates data and then the original model is discovered from the data. The recovered model defines clusters and assigns documents to clusters [8].

2.4 Hierarchical Clustering

In such methods the data set is decomposed into a hierarchy. The decomposition can be done in agglomerative or divisive manner. Agglomerative approach is a bottom up technique where initially each data object is present in a single group whereas divisive is top down approach in which initially all the clusters are present in one cluster and then with every iteration this cluster is splitted into tiny clusters and the process continues until each data point is present within a single cluster. This kind of decomposition is represented by a tree structure called as dendrogram [9].

3 Literature Survey

Different types of mining algorithms have been proposed by distinct researchers. Selecting appropriate clustering algorithm however, depends on the application goal and algorithm's compatibility with the dataset. This section illustrates issues that may arise during the formation of clusters and different approaches to tackle with these problems.

3.1 Identification of Formation of Clusters

Very few techniques are available which can automatically detect the number of clusters to be formed. Some of the techniques rely on the information provided by the user while some use cluster validity indices which are very costly in terms of time required for computation. Some statistics such as Pseudo-F statistic and the Cubic Clustering Criterion (CCC) are used for identifying the cluster number [3]. Hao Huang et al. [4] designed an approach which is used for clustering clusters having arbitrary shapes (CLASP) that shrinks the size of dataset. CLASP is very effective and efficient algorithm which automatically determines the number of clusters and also saves computational cost. Zhensong Chen et al. [10] presented an

approach for image segmentation, based on density peaks (DP) clustering. This method possesses many advantages in comparison to current methods and can predict the cluster number, based on the decision graph and defines the correct cluster centers. Christy et al. [6] proposed two algorithms, detection of outliers on the basis of clusters and on the basis of distance, which uses outlier score for the detection and then removal of the outliers.

3.2 Clustering Large Datasets

Significant accuracy in clustering can be achieved by using Constrained Spectral Clustering (CSC) algorithms. However, to handle large and moderate datasets the existing CSC algorithms are inefficient. Clustering Large Applications (CLARA) is the best partitioning technique designed for large datasets which has less computation time [7]. Ahmad Chih-Ping Wei et al. [7] gives the comparative study of algorithms which cluster complex datasets. As the number of clusters increase, Clustering Large Applications based on Randomized Search (CLARNS) performs best in case of execution time and produces good quality clusters. In large datasets, CLARA gives better clustering results whereas Genetic Algorithm based clustering-Random Respectful Recombination (GAC-R) performs efficient clustering only in case of small datasets.

3.3 Large Computational Time

As compared to the traditional clustering algorithms like k-means, hierarchical clustering algorithms have many advantages but such algorithms may suffer from high computational cost [1]. Density based outlier detection algorithms also suffer from the problem of large computation time. High computation time is a major barrier in case of density based outlier detection algorithms although, they have number of advantages. Such algorithms have a less obvious parallel structure. So to resolve the problem of time and cost some algorithms are proposed by different researchers. Spectral clustering algorithms can easily recognize non-convex distribution and are used in segmentation of images and many more fields. Such clustering often costs high computation time when they deal with large images. So to solve this problem Kai. Li et al. [5] proposed an algorithm based on spectral clustering which performs segmentation of images in less computational time.

3.4 Efficient Initial Seed Selection

K-means algorithm is the crucial clustering algorithm used for mining data. The centers are generated randomly or they are assumed to be already available. In seed based integration, small set of labeled data (called seeds) is integrated which improves the performance and overcome the problem of initial seed centers. Iurie Chiosa et al. [11] has proposed novel clustering algorithm called Variational Multilevel Mesh Clustering (VMLC) which incorporates the benefits of variational algorithms and hierarchical clustering algorithms. The selection of seeds to be selected initially is not predefined. So to solve this problem, a multilevel clustering is built which offers certain benefits by resolving the problems present in variational algorithms and performs the initial seed selection. Another problem that the clusters have non optimal shapes can be solved by using greedy nature of hierarchical approaches.

3.5 Identification of Different Distance and Similarity Measures

For measuring the distance some standard equations are used in case of mathematical attributes like Euclidean, Manhattan and other maximum distance. These three special cases belong to Minkowski distance. Euclidean distance (ED) is the measure which is usually used for evaluating similarity between two points. It is very simple and easy metric, but it also possesses some disadvantages like it is not suitable in case of time series application fields and is highly susceptible to outliers and also to noise [12]. Usue Mori et al. [12] has proposed a multi-label classification framework which selects reliable distance measure to cluster time series database. Appropriate distance measure is automatically selected by this framework. The classifier is based on characteristics describing important features of time series database and can easily predict and discriminate between different set of measures.

4 Summary of Clustering Approaches

This section summarizes the clustering approaches which are reviewed in the above section. It is very clear from the table that the limitation addressed by one technique may get resolved by another (Table 1).

Table 1 Clustering techniques

Author (Year)	Clustering technique	Benefits	Limitations
Hao Huang (2014)	Algorithm for mining clusters with arbitrary shapes (CLASP)	Less computational cost	Efficiency reduces while clustering large datasets
Zhensong Chen (2015)	DP clustering algorithm	Defines correct cluster centres	More computational time
Chih-Ping Wei (2000)	Clustering large datasets (CLARA)	Produce small, distinct and symmetric clusters	Overlapping of clusters
A. Christy (2015)	Cluster based outlier detection, distance based outlier detection	Removes noise	Poor feature selection
Kai Li (2012)	Image segmentation algorithm based on spectral clustering	Recognize non convex distribution in images	High computation time
Iurie Chiosa (2008)	Variational multilevel mesh clustering	Produces clusters having optimal shape	More complexity and overhead

5 Conclusion

This paper describes the comparative study of clustering techniques such as CLARA, K-means, CLASP and SHRINK which are used by researchers in different application examined at different levels of perception. This paper highlights the concerned issues and challenges present in different clustering algorithms. The issue arising in one approach is resolved by other approach. Fuzzy logic is good for handling uncertainties and due to parallel nature, neural networks are good at handling real time applications. By doing hybridization of neural networks and fuzzy techniques we can obtain efficient results in detection of outliers. We have concluded that algorithms like CLARA are used for clustering large datasets efficiently, but some asymmetric clustering algorithms like CLASP, efficiently cluster simple datasets but do not give expected outputs in case of mixed and tightly coupled datasets. They are less accurate and efficient for clustering large datasets. Therefore, the technique based on the neural networks should be proposed to improve clustering and for increasing the efficiency in the asymmetric clustering algorithms.

References

1. R. Mythily, Aisha Banu, ShriramRaghunathan, Clustering Models for Data Stream Mining, Procedia Computer Science, Volume 46, 2015, Pages 619–626, ISSN 1877-0509.
2. Amineh Amini, Teh Ying, Hadi Saboohi, On Density-Based Data Streams Clustering Algorithms: A Survey, Journal of Computer Science and Technology, January 2014, Volume 29, Issue 1, pp 116–141.

3. Parul Agarwal, M. Afshar Alam, Ranjit Biswas, Issues, Challenges and Tools of Clustering Algorithm, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 1, May 2011.
4. Hao Huang, Yunjun Gao, Kevin Chiew, Lei Chen, Qinming He, "Towards effective and efficient mining of arbitrary shaped clusters", ICDE, 2014, 2014 IEEE 30th International Conference on Data Engineering (ICDE), 2014 IEEE 30th International Conference on Data Engineering (ICDE) 2014, pp. 28–39.
5. Kai Li, Xinxin Song, "A Fast Large Size Image Segmentation Algorithm Based on Spectral Clustering," 2012 Fourth International Conference on Computational and Information Sciences, pp. 345–348.
6. A. Christy, G. Meera Gandhi, S. Vaithya subramanian, Cluster Based Outlier Detection Algorithm for Healthcare Data, Procedia Computer Science, Volume 50, 2015, Pages 209–215, ISSN 1877-0509.
7. Chih-Ping Wei, Yen-Hsien Lee and Che-Ming Hsu. Department of Information, Empirical Comparison of Fast Clustering Algorithms for Large Data Sets, Proceedings of the 33rd Hawaii International Conference on System Sciences – 2000.
8. Zhang Tie-jun, Chen Duo, Sun Jie, Research on Neural Network Model Based on Subtraction Clustering and Its Applications, Physics Procedia, Volume 25, 2012, Pages 1642–1647, ISSN 1875-3892.
9. Pedro Pereira Rodrigues, Joao Gama, Joao Pedro Pedroso, "Hierarchical Clustering of Time-Series Data Streams," IEEE Transactions on Knowledge and Data Engineering, vol. 20, no. 5, pp. 615–627, May, 2008.
10. Zhen-song Chen, Zhi-quan Qi, Fan Meng, Limeng Cui, Yong Shi, Image Segmentation via Improving Clustering Algorithms with Density and Distance, Procedia Computer Science, Volume 55, 2015, Pages 1015–1022, ISSN 1877-0509.
11. Iurie Chiosa, Andreas Kolb, "Variational Multilevel Mesh Clustering," Shape Modeling and Applications, International Conference on, pp. 197–204, 2008 IEEE International Conference on Shape Modeling and Applications, 2008.
12. Usue Mori, Alexander Mendiburu, and Jose A. Lozano, Member, Similarity Measure Selection for Clustering Time Series Databases, IEEE Transactions on Knowledge and Data Engineering, 2015.

Adaptive Pre-processing and Regression of Weather Data

Varsha Pullabhotla and K.P. Supreethi

Abstract With the evolution of data and increasing popularity of IoT (Internet of Things), stream data mining has gained immense popularity. Researchers and developers are trying to analyze data patterns obtained from various devices. Stream data have several characteristics, the most important being its huge volume and high velocity. Although, a lot of research is being conducted in order to develop more efficient stream data mining techniques, pre-processing of stream data is an area that is under-studied. Real time applications generate data which is rather noisy and contain missing values. Apart from this, there is the issue of data evolution, which is a concern when dealing with stream data. To deal with the evolution of data, the proposed solution offers a hybrid of preprocessing techniques which are adaptive in nature. As a result of the study, an adaptive preprocessing and learning approach is implemented. The case study with sensor weather data demonstrates the results and accuracy of the proposed solution.

Keywords Stream mining • Data evolution • Adaptive pre-processing

1 Introduction

In the present day scenario, there are many applications in our day to day lives ranging from social networks, health monitors, telecommunications, network monitoring tools, sensor devices (in manufacturing, industrial pumps etc.) and such which continually generate huge volume of data at high velocity. These data streams evolve over time. Thus, there is a need for adaptivity of predictive models

V. Pullabhotla (✉) · K.P. Supreethi
Computer Science and Engineering Department,
Jawaharlal Nehru Technological University Hyderabad, Hyderabad, Telangana, India
e-mail: varshapull28@gmail.com

K.P. Supreethi
e-mail: supreethi.pujari@jntuh.ac.in

to adapt to the evolution and change in environment of data streams. Recently, a lot of research and study is being carried out for such adaptive learning [1–3].

In real applications, pre-processing of data is a very important step of the data mining process as real data often comes from complex environments and can be noisy and redundant. In adaptive learning literature, the data pre-processing gets low priority in comparison to designing adaptive predictors. As data is continually changing, adapting only the predictor model is not enough to maintain the accuracy over time.

A good way to approach the above problem would be to tie the adaptivity of the preprocessor with the predictor. This can be accomplished in two ways. The first approach is to put aside a validation set, and use this validation set to optimize the pre-processing parameters and keep the pre-processing fixed in the model. The other approach would be to retrain the preprocessor afresh every time the learner is retrained. This approach requires the preprocessor to be synchronized with the learner.

In this paper, the aim is to present an implementation that can achieve adaptive pre-processing to get accurate output from adaptive learning. The pre-processing algorithm used is the “Multivariate Singular Spectrum Analysis”. The learner algorithm used is the “K Nearest Neighbor” algorithm. These algorithms coupled with the Fixed window strategy [4] produce the adaptive pre-processing and learner framework.

The remainder of the paper is structured as follows: Sect. 2 presents the surveyed related work. Section 3 presents the proposed method for adaptivity. Section 4 shows the experimental results and performance evaluation. Finally, in Sect. 5, the conclusions drawn are presented.

2 Related Work

There has been a considerable amount of research and study conducted to address the issue of adaptive pre-processing along with adaptive learning. The issue of adaptive pre-processing while learning from a continuously evolving stream of data was raised in [4]. A framework that connects adaptive pre-processing to online learning scenarios was proposed. A prototype was developed to enable adaptive pre-processing and learning for stream data.

There has been the use of Genetic algorithm (GA) proposed by Wei Li to improve adaptive pre-processing to accomplish better results from adaptive learning [5].

Adaptive pre-processing of data streams has also been used with clustering algorithms. A pre-processing technique called equi-width cubes splits data space into a number of cubes, depending upon the data dimension and memory limit [6]. The new data which arrives is incorporated into one of the cubes. The algorithm computes a cluster center from previous chunk to create a new chunk. This new chunk is then sent to the clustering algorithm. This algorithm makes sure that the

data will not occupy all the available memory space and prevents loss of data due to the rate at which it arrives.

Adaptive pre-processing has been addressed in stationary online learning [7] for normalization of the input variables in neural networks. This was carried out so the input variables would fall into the range $[-1, 1]$. This proposed approach relates scaling of input features with scaling of the weights. However, the pre-processor is not adaptive.

3 Proposed Method

The framework of the proposed method is described in Fig. 1. The proposed Multivariate Singular Spectrum Analysis (MSSA) and K Nearest Neighbor approaches are applied to streaming weather data. Streaming weather data for the city of Hyderabad, India is used. The approach is carried out in two stages. In the first stage the MSSA algorithm which is used for pre-processing is trained with historical weather data for the city. The K-Nearest Neighbor algorithm is used for prediction. This model is trained using the output generated by the pre-processing algorithm. A stream of weather data is passed to this model, however, the results are not satisfactory.

The second stage involves applying the Fixed window strategy to the stream of weather data and retrain the preprocessor from scratch using the results obtained. The output obtained from the preprocessor results in the decomposition of the original time series into a stream of data without any noise. This output is passed to two K-nearest neighbor learner models: A model which is already trained using historical weather data and the other which is trained using the output obtained after retraining the pre-processor.

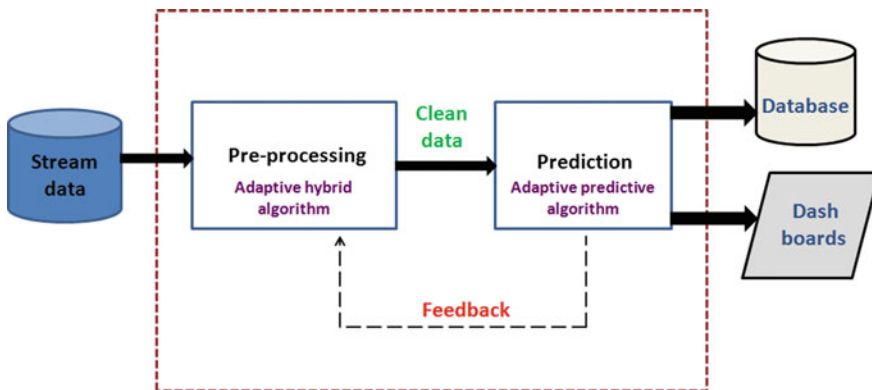


Fig. 1 Proposed system

4 Experimental Results

The proposed method is applied to streaming weather data for the city of Hyderabad, India. The performance measurement used to determine the accuracy of the prediction is the Root Mean squared error. This measure is meant to be used to understand how accurate the weather prediction for the next hour will be.

In this study, $m = 3$ and $N = 10$ are used, where N represents the sample size of the stream and m is the number of lags considered where the covariance is positive (this is determined using the autocorrelation function. We see a positive correlation at lag 3). The Root mean square error for the adaptive pre-processing and non-adaptive predictor is 0.29154. This error isn't considered too high and thus prediction is considerably accurate.

In the case of adaptive pre-processing and adaptive prediction, the RMSE is relatively low (0.014) and thus results in accurate prediction. However, this predictor is not trained by historical data as it is adaptive in nature. Thus this adaptive predictor has to be periodically re-trained for every 10 historical values to ensure that the predictor maintains its accuracy.

5 Conclusion and Future Scope

In this study, it has been demonstrated that the proposed approach, adaptive MSSA-KNN, could yield significantly higher prediction accuracy of weather data variables such as Temperature and Humidity than that of the non-adaptive KNN method. Adaptive MSSA-KNN results in a significant improvement prediction of weather data with RMSE of 0.014 and non-adaptive method results in RMSE of 0.29.

Future work would be focused on applying an incremental model instead of using a replacement model for adaptive pre-processing. Another area to work on would be to focus on passing multiple streams of weather data from different cities at once (Table 1).

Table 1 Prediction accuracies with adaptivity

Data	Adaptive pre-processing	Adaptive learning	RMSE
Stream weather data	No	No	4.008
Stream weather data	Yes	No	0.29154
Stream weather data	Yes	Yes	0.014

References

1. A. Bifet, G. Holmes, B. Pfahringer, R. Kirkby, and R. Gavaldà.: New Ensemble Methods for Evolving Data Streams. In: Proc. 15th ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining (KDD '09), pp. 139–148, 2009
2. E. Ikonomovska, J. Gama, and S. Dzeroski.: Learning Model Trees from Evolving Data Streams. In: Data Mining Knowledge Discovery, vol. 23, no. 1, pp. 128–168, 2011
3. P. Kadlec and B. Gabrys.: Architecture for Development of Adaptive on-Line Prediction Models. In: Memetic Computing, vol. 1, no. 4, pp. 241–269, 2009
4. Indrè Žliobaitė and Bogdan Gabrys.: Adaptive Pre-processing for Streaming Data. In: IEEE Transactions On Knowledge And Data Engineering, Vol. 26, No. 2, February 2014
5. Ketan Desale and Roshani Ade.: Preprocessing of Streaming Data using Genetic Algorithm. In: International Journal of Computer Applications (0975–8887) Volume 120–No.17, June 2015
6. Piotr Duda, Maciej Jaworski, and Lena Pietruczuk.: On Pre-processing Algorithms for Data Stream, L. Rutkowski et al. (Eds.): ICAISC 2012, Part II, LNCS 7268, pp. 56–63, 2012. Springer-Verlag Berlin Heidelberg 2012
7. H. Ruda.: Adaptive Preprocessing for on-Line Learning with Adaptive Resonance Theory (Art) Networks. In: Proc. IEEE Workshop Neural Networks for Signal Processing (NNSP), 1995

A Comparative Analysis for CBIR Using Fast Discrete Curvelet Transform

Katta Sugamya, Suresh Pabboju and A. Vinaya Babu

Abstract A Content Based Image Retrieval is proposed using two techniques in order to show a comparative analysis. The comparative analysis points out it's overall performance depends on the type of techniques used to extract multiple features and similarity metrics between the query image and images database. The first method uses colour histogram to extract colour features and the second method uses the Fast Discrete Curvelet Transform (FDCT) for the same process. In the first method, based on the colour features the query and database images were compared by using chi-square distance. Colour-histograms for both images were obtained and the images with most similarities are displayed (five images in this case). In the second method, instead of one feature (colour in the first case), a set of features are taken into consideration for calculating the feature vector. Once computation of feature vector is done, database and query images are compared to find out the top five similar images and results are displayed to the user.

Keywords Fast discrete curvelet • Transform (FDCT) • Inverse fast fourier transform (IFFT)

1 Introduction

With the enormous growing of digital data, it has become one of the active research area in the field of machine learning. The usage of multimedia caused an explosively growing of digital data giving people more ways to get those data.

K. Sugamya (✉) • S. Pabboju
Department of IT, Chaitanya Bharathi Institute of Technology, Hyderabad, India
e-mail: sugamya.cbit@gmail.com

S. Pabboju
e-mail: plpsuresh@gmail.com

A. Vinaya Babu
Department of CSE, JNTU, Hyderabad, India
e-mail: avb1222@jntuh.ac.in

An efficient technique in searching and retrieving of images from the huge collection of data is emphasized.

Approaches using manual text annotations for retrieving and indexing image data have several problems. First, it is tricky to find out the contents of an image using a keywords. Second, the manual annotation process was ambiguous, deficient and subjective. The problems were complex and in great demand to solve. Second, an approach based on low level contents is known as content-based image retrieval (CBIR). Most of the CBIR [1] techniques use low-level image features [2] such as color [3], texture, shape, edge, etc., for image indexing and retrieval. Features can be computed automatically by using low level contents.

1.1 Content Based Image Retrieval (CBIR)

A technique that searches apparently similar range of images as that of query image using low level features. Comparing the feature vectors of image database with query image using pre-selected similarity measure, and then sorting out the results. A reduced set of images which have the same features as that of the query image is obtained. After obtaining the set of images, they are sorted based on their similarity values.

One of the important part in content-based image retrieval (CBIR) is Feature extraction. The literature gives multiple texture feature extraction techniques, using statistic and spectral methods. So far there is no efficient technique which accurately capture the edge information as it is the most important texture feature in an image retrieval. The present works on multiple feature [4] analysis, particularly the Curvelet method [5], provide a good opportunity to extract most accurate texture feature for image retrieval. Curvelets were initially proposed for image de-noising [6] and has shown a promising performance. For capturing the edge information accurately, Fast Discrete Curvelet Transform (FDCT) [7] is used. Edge detection using Fast Discrete Curvelet Transform [8] is more useful for multi feature point of view than texture based DCT [9] analysis.

2 Fast Discrete Curvelet Transform

Fourier samples have less computational complexity in Fast Fourier transform based on complex ridgelet transform instead of FDCT. The wrapping of curvelet transform reduces data redundancy in the frequency domain. Curvelets are variable in width and length that represents more anisotropy than ridgelets that have a fixed length which is equal to the image size of a variable width. The promising approach is based on FDCT using wrapping. Which is simpler, less redundant and faster in computation than ridgelet based curvelet transform, and intend to use for texture representation in the CBIR research. A 2-D image as input will take wrapping of

Fourier samples in curvelet transform in the form of an array $f[u, v]$ such that $0 \leq u < M$, $0 \leq v < N$ and generates a number of curvelet coefficients indexed by a scale s , an orientation l and two spatial location parameters (t_1, t_2) as output. To form the curvelet texture descriptor, statistical operations are applied to these coefficients. Discrete curvelet coefficients can be defined by:

$$C^D(s, l, t_1, t_2) = \sum_{\substack{0 \leq u < M \\ 0 \leq v < N}} f(u, v) \phi_{s,l,k_1,k_2}^D[u, v] \quad (1)$$

Here, each ϕ_{s,l,t_1,t_2}^D is a digital curvelet waveform. The curved edges of an image will be captured by Curvelet transform that implements the parabolic scaling on the sub-bands in the frequency domain more effectively. These Curvelets in an oscillating behaviour in the direction perpendicular to their orientation in frequency domain. A pyramid structure consisting of many orientations at each scale were obtained in wrapping based curvelet transform which is as a better performer for multiple feature [4] analysis of images. The pyramid consists of several sub-bands at distinguishable range of high and low frequency levels at different orientations and positions. The curvelet is a wedge like a needle shaped element at high scales, whereas, it is non directional at the coarsest scale. Curvelet becomes finer and smaller in the spatial domain and more sensitivity to curved edges with increased resolution levels. This enables an effective capture of the curves of an image by few coefficients, and curved singularities can be approximated.

The distinction between images can be found by High frequency components, and edges can be effectively represented by texture features of the curvelet coefficients. The frequency responses at different scales and orientations were combined; hence a rectangular frequency tiling that covers the whole image in the spectral domain will be obtained. Curvelet transforms are usually implemented in the frequency domain will be able to achieve better efficiency. Hence, using fourier transformations curvelet coefficients and image feature coefficients are transformed and then multiplied in the frequency domain. By applying Inverse fast fourier transform to the result the curvelet coefficients were obtained. The process can be described as

$$\text{Curvelet transform} = \text{IFFT}[\text{FFT}(\text{Curvelet}) \times \text{FFT}(\text{Image})] \quad (2)$$

From Eq. (2) the result of a product is a wedge. In spectral domain, the trapezoidal form of edge is not suitable to use in the inverse Fourier transform which is the next step in collecting the curvelet coefficients using IFFT. Directly data cannot be accommodated into a rectangle of size $2^j \times 2^{j/2}$. To surmount this setback, a wedge wrapping process i.e. a parallelogram with sides 2^j and $2^{j/2}$ is chosen to support the wedge data. Inside the wedge periodic tiling of the spectrum and then collecting the rectangular coefficient in the center area is done by the wrapping. And then successfully collects all the information in the parallelogram of size $2^j \times 2^{j/2}$ from the center of the rectangle.

2.1 Curvelet Computation

Discrete curvelet transform is better option to represent the curved edges of an images more efficiently than wavelet and Gabor filters. It can give better discriminatory texture patterns of an image. Discrete curvelet transform can be applied to an image to obtain coefficients with faster and less redundant manner. These coefficients are then used to form the texture descriptor of that image. Curvelet coefficients of a 2-D Cartesian coefficients $f[u, v]$, $0 \leq u < M$, $0 \leq v < N$ are given as follows:

$$C^D(j, l, k_1, k_2) = \sum_{\substack{0 \leq u < M \\ 0 \leq v < N}} f(m, n) \phi_{j,l,k_1,k_2}^D[u, v] \quad (3)$$

where ϕ_{j,l,k_1,k_2}^D is the curvelet waveform. This transform generates an array of curvelet coefficients indexed by their scale j , orientation l and location parameters (k_1, k_2) .

3 Implementation

3.1 General Idea

In a content based image retrieval system, any combination of features can be used to generate the feature vector and use that to compare the input query with the database images. In the proposed work, colour feature is extracted using colour histogram, texture and edge features were extracted using fast discrete curvelet transform. The proposed paper consists of two sub-modules: one for extracting only colour feature and other for extracting edge and texture feature.

Module 1: Shows the basic steps involved in the first module which deals with color feature extraction using color histogram.

Module 2: The second module of the proposed system consists of extracting edge and texture features using Fast Discrete Curvelet Transform (FDCT).

The Fig. 1 shows the major steps involved in the proposed system.

The overall system can be summarized as below:

- Step 1: Creating and loading feature database: A database consisting of 600 images are taken. The feature vector for module 1 and module 2 are calculated separately and stored.
- Step 2: Query image selection: A query image is provided to the system, some feature vectors were calculated for the query as well as database image.

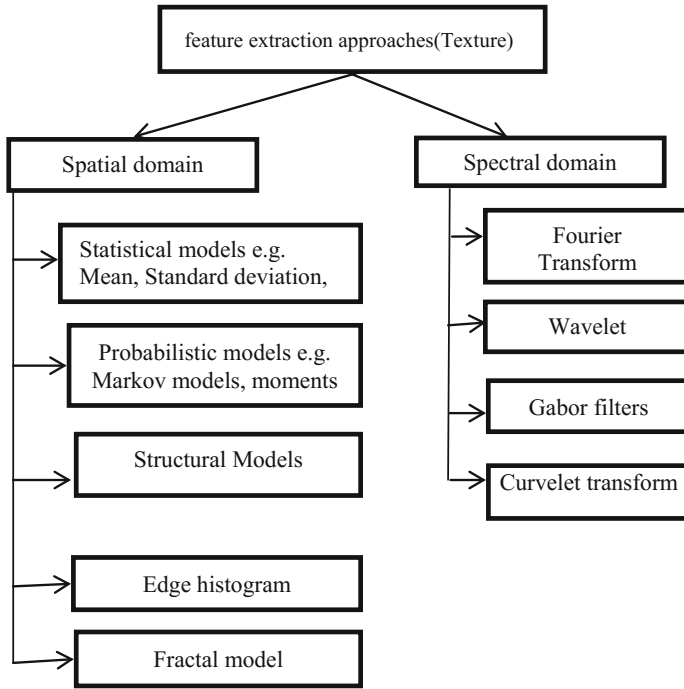


Fig. 1 Approaches for texture feature extraction

- Step 3: Calculation of similarity value: For the first module, the similarity is calculated using Eq. 4. For the second module, the similarity value is calculated using Eq. 5.
- Step 4: Similarity matching and indexing of database images: Once the similarity values are calculated for all the database images, the images of the database are then organized in ascending order with respect to the similarity value. A mapping is performed in order to relate the indexes of the image in the database to its corresponding similarity values.
- Step 5: Retrieve similar images and store them in the increasing order of their similarity values. Out of these images, the first ‘n’ images are taken and displayed to the user.

3.2 Detailed Description

Module 1: The first module is about taking the query image, calculating its colour histogram. Same colour histograms are calculated for image database. Then, comparison of colour histogram of query with the database images is performed.

For the first module, Fig. 2 shows some of the images present in the database of 600 sample images with different datasets. For all these images, colour histogram is computed and stored as the feature database.

The user inputs a query to the system. A 2D histogram of the HSV values is calculated for both the input and database images. The histograms of the input image and database images are compared. For each image 'i', distance 'D' is

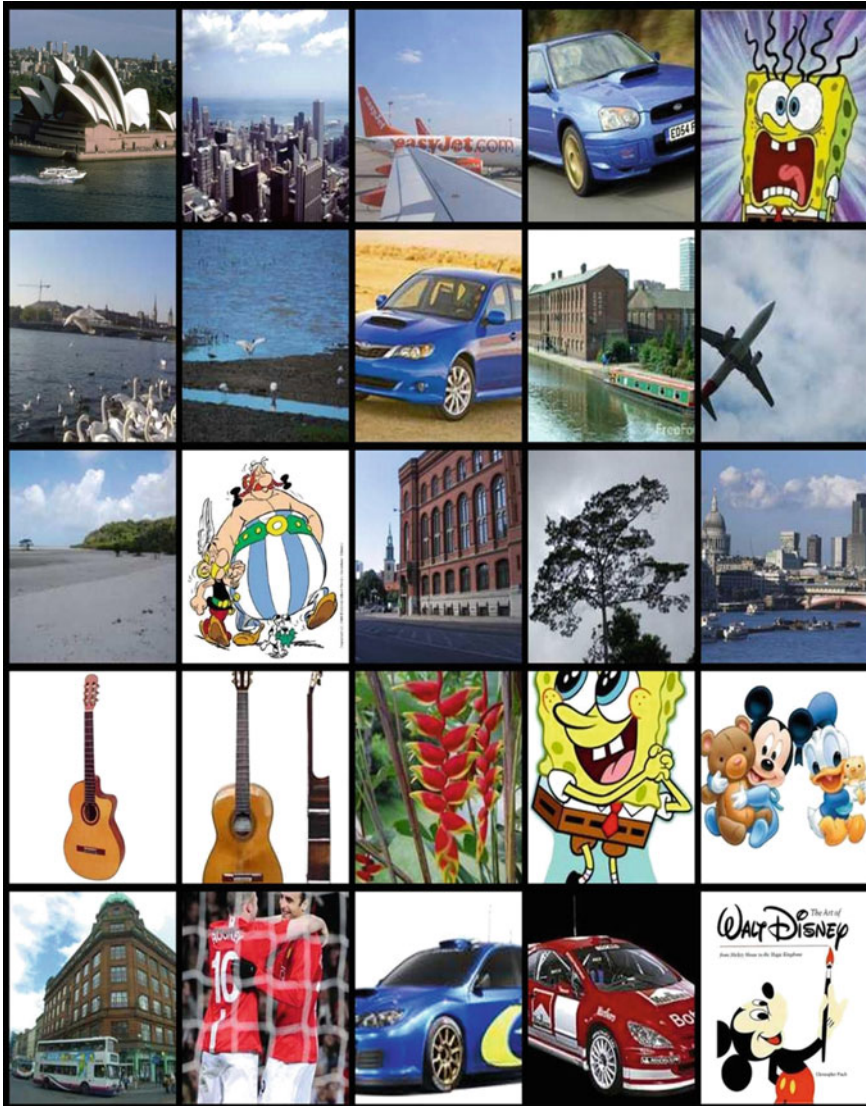


Fig. 2 Sample images from the image database

calculated between the histogram of the query image and each database image histogram using chi-square distance:

$$D_{chisquare}(H, G) = \sum_{i=1}^L \frac{\left(H(i) - \frac{H(i) + G(i)}{2}\right)^2}{\frac{H(i) + G(i)}{2}} \quad (4)$$

Only distances D_2 among D are kept, which are greater than the predefined threshold T ($= 0.01$). Let L_2 be the number of the above distances.

A smaller set D_3 out of these distances, is calculated which are greater than a second threshold T_2 ($= 0.8$). Let L_3 be the number of D_3 distances. Then, the similarity between the query image and the image 'i' is calculated as:

$$S_i = \frac{L_2 * D_3(i)}{L_3^2} \quad (5)$$

The 'n' images with smallest S_i values are shown as output. The number of images given as output can be changed. In the results and analysis part, the 'n' value is taken as 5.

Module 2: The proposed system is about taking the input query image and then extracting the edge and texture features using fast discrete curvelet transform (FDCT). First an image is taken. That image is then subjected to a filter, which filters the pixels representing the rough edges present in the image.

Then, this filtered image is divided into 'n' small squares in order to make the processing easy. Once the image is divided into tiny squares, these squares are elongated up to a level where each and every square contains a straight line (if it contains anything at all). The elongation procedure is done to elongate the curved edges of image boundaries, so that they become straight lines. This ensures that the edge irregularities are captured properly and accurately without missing any significant detail. After the elongation (also called smooth partitioning), the squares are separated into individual units. Out of all the individual squares, only those squares containing the edges (i.e. the straight lines) are kept and the rest of the blank squares are discarded.

For the remaining squares (with the edges), FDCT coefficients are calculated. With these coefficients, mean and standard deviations are calculated which is later used to calculate the similarity value. Once the similarity values are calculated, the database images are sorted and indexed accordingly. Out of the sorted results, most relevant images are displayed to the user. Once the curvelet coefficients are generated and stored. The mean and standard deviation coefficients associated with each sub-band are computed. Generally, these mean and standard deviation are then used as the texture feature vector elements of the image. Thus, for each curvelet, two texture features were obtained. If n Curvelets were applied to the transform, $2n$ texture feature will get. This results a $2n$ dimensional texture feature vector for each image in the feature database. These feature descriptors are then used to index images in the feature database, which is also known as the image 'indexing

scheme'. An internal mapping is generated to make links between images in database to the corresponding features in feature database.

Once the feature database images are indexed then, search and retrieval is performed on the basis of these features. To obtain feature vector, query image is subjected to feature descriptor generation process. Using similarity measures, the database image are compared to the query image features vectors.

4 Results and Analysis

4.1 Outputs

The Fig. 3 shows the Graphical User Interface (GUI) for the proposed system. In the GUI, there are four buttons. The 'Query Image' button is used to select the input image from a directory. The 'Load Database' button is to select and load the database of 600 images. Once the query image is selected and the database is loaded, the next step is to press the 'Color Histogram' button which does multiple functions. First, it computes and plots all the histograms for the query and the database images. After computing the histograms, it computes the similarity values. According to these values, it performs the sorting and indexing then displays the relevant images at the end.

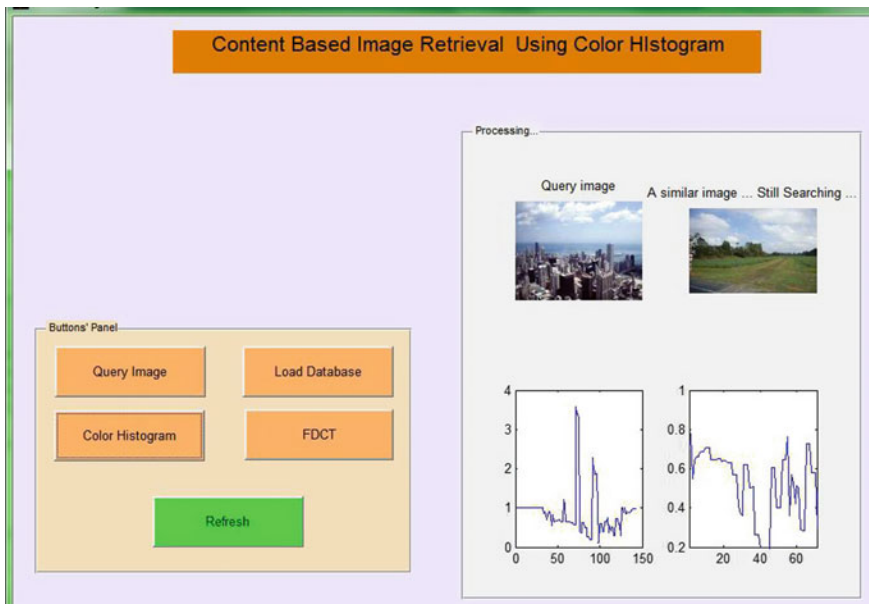


Fig. 3 An instance of the histogram computation

As mentioned earlier, the number of retrieved images is denoted by 'n' and it can be changed. For demonstration purpose, 'n' is assigned a value of 5 and the results are displayed accordingly. Figure 3 Retrieved images for the input query image when database contains the query image already. The Fig. 3 has total 6 images displayed. The first one is the query image as labelled. The remaining five images are the retrieved images whose similarity values were the smallest. The relationship of similarity values and the relevance is inversely proportional i.e. lesser the similarity value, more relevant the image is. The similarity values corresponding to the images are displayed on top of them. The similarity value of the first image in Fig. 4 is 0.000. The reason behind this is that the query image has an exact match in the database. When the image is an exact match (a duplicate, in other words) then the similarity is 0.000 which clearly means that they are not different at all. But when an image which does not have an exact match in the database, as shown in Fig. 4, then the similarity values will be sorted accordingly and only 5 images with the smallest similarity values will be retrieved.

Figure 5 shows the output obtained after pressing the 'FDCT' button in the initial GUI shown in Fig. 3. This is a sub-GUI which is initialized after the 'FDCT' button press. This sub-GUI has two buttons: 'Load Image' and 'Search'. The 'Load Image' button is to load the same image that was selected as query image by the user initially in Fig. 2. After successfully loading that query image, the 'Search' button is pressed. Once the 'Search' button in Fig. 3 is pressed, a number of computations are done in the background. On pressing the button, the first thing that

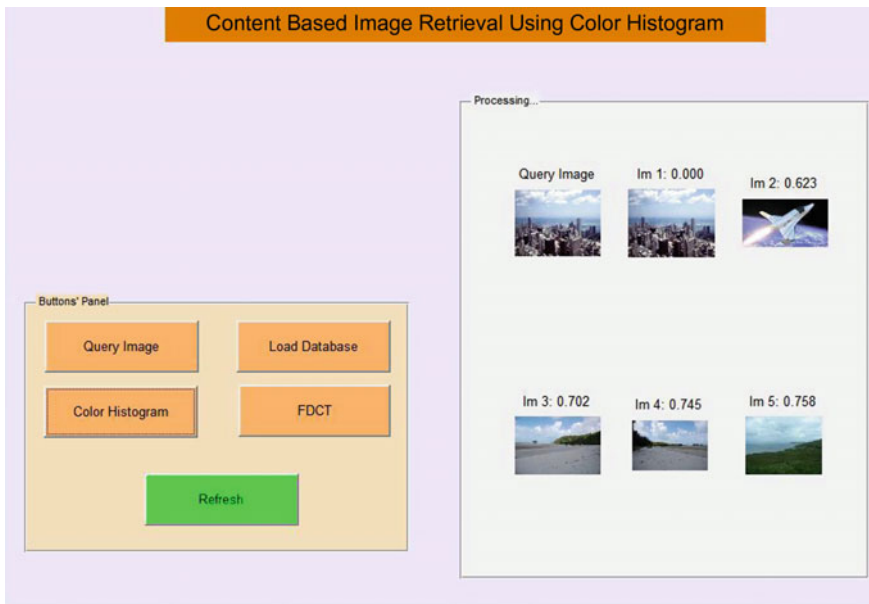


Fig. 4 shows the retrieved set of images for the query image

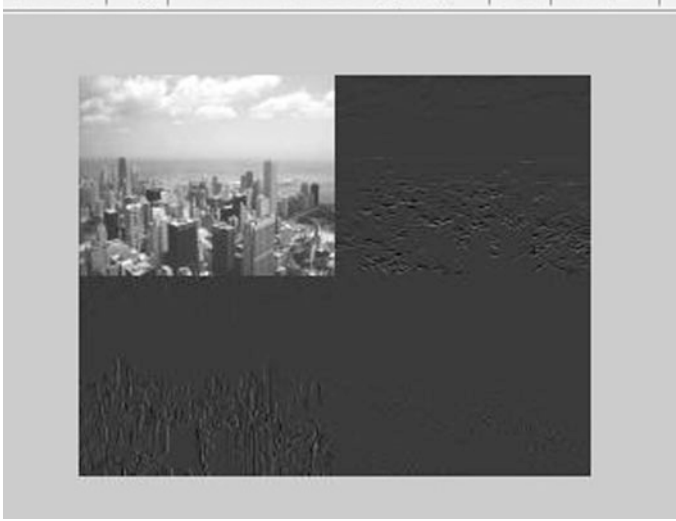


Fig. 5 The detected edges of the query image

happens if that the edges of the image are identified using a filter and displayed as in Fig. 5.

In the above Fig. 5 have four components. The first one is the gray scale image obtained from the original query image. The top right component shows the horizontal edges i.e. the edges obtained when the filter is applied horizontally. The bottom left component is the result obtained when a vertical filter is applied to get the edges. The last component is the combined result of both the horizontal and vertical edge detection process.

Figure 6 shows the different curvelet sub-bands of the input query image. These sub-bands were obtained by applying fast discrete curvelet transform at various scale as demonstrated in Fig. 5.

Figure 7 shows the final set of retrieved images obtained after applying the fast discrete curvelet transform on the query image.

4.2 Analysis

In the proposed paper two sub-systems have been implemented: One using colour histogram to extract colour feature of an image and using the histograms to retrieve relevant images. And the other, using Fast Discrete Cosine Transform to extract texture and edge features for input image. By using these features, retrieve relevant images from the database.

Figure 8 shows the comparison of the two sub-systems based on the similarity values. As the figure clearly shows that the results are better when FDCT is used.

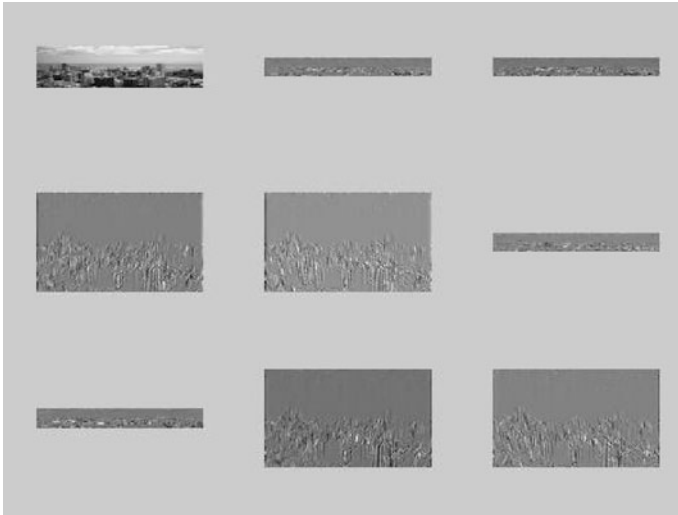


Fig. 6 Curvelet sub-bands of the query image

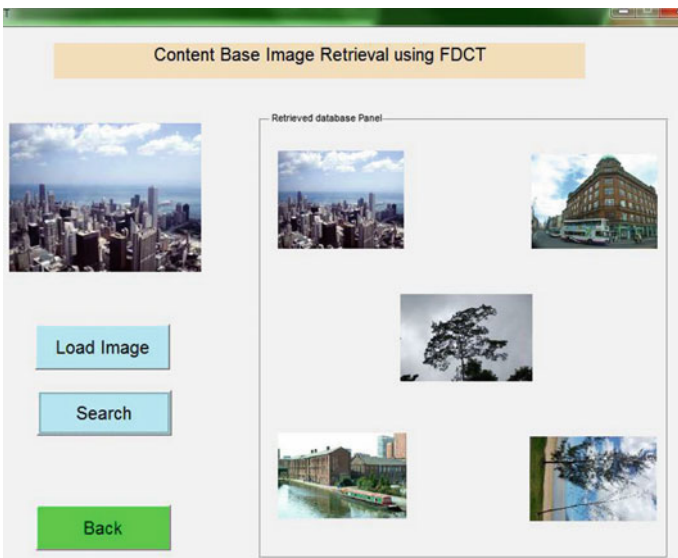
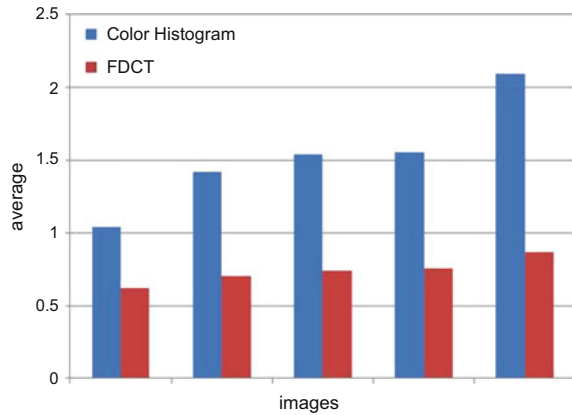


Fig. 7 Retrieved set of images on applying FDCT

The bar graph is constructed using similarity values in case of ten query images and the average of these similarity values are taken to plot the bar graph. The five separate groups represent the average similarity values (Y-axis) for five output images (X-axis) that are retrieved at the end. The leftmost group represents the

Fig. 8 Comparison of similarity values for color histogram and FDCT



average of the most similar images and the rightmost group represents the least similar images out of the five images retrieved in each case.

5 Conclusion and Future Scope

An approach to CBIR is proposed using colour histogram and fast discrete curvelet transform but any CBIR system has endless scope to work with. By using different approaches it has been seen that retrieval ratio depends upon image class, for some images it gives good retrieval ratio while poor for some other. From results it is proved that the proposed work gives a very good image retrieval accuracy. The system performance is quite reasonable as per the similarity bar graph shown above.

This approach concentrates only on retrieval of image based on the calculated feature vector which can lead to retrieval of images that a user might find completely irrelevant. To improve that, relevance feedback can be used to improve the system so that the results are satisfactory to the user.

References

1. Arnold W. M. Smeulders, IEEE Marcel Worring, Simone Santini, Amar nath Gupta, and Ramesh Jain (2000), "content based image retrieval at the end of early years", IEEE Transactions on pattern analysis and machine intelligence, vol. 22, page no. 12.
2. R.Venkata Ramana Chary, Dr. D. Rajya Lakshmi and Dr. K.V.N Sunitha, "Feature extraction Methods for Color Image Similarity", Advanced Computing: An International Journal (ACIJ), Vol.3, page No.2, March 2012.
3. Hamid A. Jalab, "Image Retrieval System Based on Color Layout Descriptor and Gabor Filters", IEEE Conference on Open Systems (ICOS2011), Langkawi, Malaysia, September 25–28, 2011.

4. Young Deok Chun, Nam Chul Kim, and Ick Hoon Jang “Content-based Image Retrieval using Multi-resolution Color and Texture Features”, *Multimedia, IEEE Transactions on* Oct. 2008, vol. 10, Issue no. 6, pg no:1073–1084.
5. Mohamed Elhabiby, Ahmed Elsharkawy, Naser El-Sheimy, “Second Generation Curve let Transforms vs. Wavelet Transforms and Canny Edge Detector for Edge Detection from WorldView-2 data”, *International Journal of Computer Science & Engineering Survey (IJCSES)* Vol. 3, No. 4, August 2012.
6. Jean-Luc Starck, Emmanuel J. Candès, and David L. Donoho, “The Curve let Transform for Image De-noising”, *IEEE transactions on Image Processing*, Vol. 11, page No. 6, June 2002.
7. Ishrat Jahan Sumana, “Image Retrieval Using Discrete Curve let Transform”, Thesis, Monash University, Australia, November 2008.
8. B. Sravani, B. Ramesh Reddy, “An Enhanced Glaucoma Identification using FDCT Classified by Multi SVM”, *International Journal of Engineering Research & Technology*, Vol. 3–Issue 9, September 2014, ISSN: 2278-0181.
9. Yu-Len. Huang, “A Fast Method for Textural Analysis of DCT-Based Image,” *Journal of Information Science and Engineering*, Vol. 21, pp. 181–194, 2005.

Compute the Requirements and Need of an Online Donation Platform for Non-monetary Resources Using Statistical Analyses

Surbhi Paltani, Saru Dhir and Avi Bhardwaj

Abstract NGOs in India face a lot of challenges that differ from place to place. Some of these challenges include insufficient funds, inadequate public participation, insufficient non-monetary donations, people confusing donation with waste disposal and depreciation in the extent of volunteerism. In this paper, we have analyzed an efficient and technological way to overcome such scenarios. This paper also focuses on the deep understanding of the donor behavior, strategies that can be used to influence their perceptions and the results of the survey conducted to determine the preferences of the donors. It explains how all this knowledge can be implemented as features on a web platform to gain the maximum benefit for NGOs. The results were derived using statistical analysis and conducting t-test and one way ANOVA test using Statistical Package for the Social Sciences (SPSS) software.

Keywords Web platform • Non-monetary requirements • Donor behavior • Survey • SPSS • T-test • ANOVA

1 Introduction

These days NGOs encounter a lot of obstructions in achieving their motives. This paper is intended to analyze donor behavior (to understand the donor decision process), their responses, both offline and online so as to figure out the right strategies that can be used for an NGO while making an online platform for both donors and organizations. This study also analyses whether there is any requirement for the online presence of these organizations from the donors' point of view and to

S. Paltani (✉) · S. Dhir · A. Bhardwaj
Amity University, Noida, Uttar Pradesh, India
e-mail: surbhipaltani09@gmail.com

S. Dhir
e-mail: sdhir@amity.edu

A. Bhardwaj
e-mail: avibhardwaj.mvm@gmail.com

what extent the donors are willing to use this online platform to make donations as required by the organization. The survey, conducted among the donors helped to analyze a better solution in the form of an online platform. This platform can offer the NGOs to state their actual requirements of resources and then map their requirements with what the donors are willing to donate, so as to establish a contact between the donors and the organization. This will lead to a win-win situation in which the donor is able to donate what he wants to and the organization receives what is required by them. It would help the NGOs to convey the organization goals to a number of potential donors. Usage of various tools can help to insert the features customized in accordance with their needs. In addition, various tools specific for this platform that provide online donation database management, free services for fund raising and creating donation forms can play a great role in enhancing the usage of the platform. Initially a research based methodology, should be adopted to comprehend the actual meaning of donation and the services/features that can be provided to the organizations through this platform. The act of donating is best characterized 'as a voluntary surrender of resources to a resource starved beneficiary' by Bajde [1]. It is important for NGOs maintain good relations with volunteers and donors so that they continue to donate in the future for their cause. In order to achieve this, a strong online communication method that enables them to easily be in touch with their donors is required. Surveys depicted that there are still a lot of NGOs that have not established their web presence due to the lack of funds or the technical knowledge as a result of which their requirements for resources and the staff apt for the people of their organizations aren't fulfilled.

The advantage of this study is that it will help to examine the donors' perspective so that features of an online platform can be identified that would support the NGOs through the lowest level and will serve as a way to reduce complications. Statistical test (T test and one way ANOVA) is applied to determine the actual result of the survey with respect to the goal. T test is done to conduct statistical analysis on two questions to compare them. One way ANOVA compares the mean in between two or more groups, where one variable is independent [2].

2 Literature Review

2.1 Existing Frameworks Regarding Donor Behavior

There are different research methodologies are used to enhance the knowledge among community [3]. Guy's & Patton's research (1989) was initial and one of the most important in the area of the donor decision process. Their findings include that the realization of the fact that another person requires support and is in the situation of unpleasant outcomes should be provoked in the donors. After analyzing the situation they might recognize their responsibility for helping and their reaction of

whether they want to donate or not would solely depend on how they perceive the situation and how it was portrayed before them [4].

The model demonstrated donor behavior as an input-output process. Input represents the request presented in front of the donor. Several factors that affect their comprehensiveness to the input given to them include charity appeal, images, facts and the mode of ask. Output represents the response of the donor which is usually regulated by various factors such as judgmental criteria and donor's past experience which are identified as processing determinants [5]. In 2007, Sargeant & Woodliffe examined the monetary donations to extend this model and depicted that the fundraising is associated with the good reputation of nonprofits [6].

Bajde's research (2006) laid emphasis on promoting the non-profit organization that in turn would motivate the donors. Research has depicted that there are two groups of variables that influence donor's response. The first group includes the factors that can be controlled by the non-profit organization such as cause of need, images appeals, message, nature and size of request. The second group includes the donor and non-donor variables like mood, attention, government policies, media exposure etc. [1].

Later, the findings have shown that donor's behavior is affected by incentives, empathetic nature, extrinsic variables like gender, age, marital status, earnings, etc. A study suggested that if the sum is lowered down and the number of asks from the donor is increased then it'll aid in fundraising since it increases donor's compliance.

2.2 Marketing Activities of NGO Influencing Donor's Perception

Benett and Barkensjo (2005) explained three types of relation marketing, namely relationship advertising, database marketing and two-way marketing contacts. They defined relationship marketing as a form of advertising with the purpose of keeping the donors informed about any upcoming event or charity and making them realize about the organization's need. Two-way marketing contacts include using communication systems in order to sustain a two way relationship with the donors. It can be achieved by using a website, posts, email and the organizations can reply to them and keep them updated about the forthcoming events [7].

These three types/factors play an important role in changing donor's perception about the organization. It totally depends on what marketing strategy is used by the organization to lure the donors. If used in a right manner, a positive perception is generated in the mind of donors regarding the NGO [7].

2.3 Applying the Donor Knowledge to an Online Solution

The behavioral study of the donors should be applied to the web application and considered as a part of the requirements. The various facilities that are associated with the web application can be of great advantage to the small NGO's and can ensure their firm web presence. Sargeant identified some vital factors of Internet which can help these NGO's to promote themselves. These include person to person conversation, search engine optimization (SEO), web applications, online communities, news groups, email and advertising. Implementing all these provisions in a single web application can play a vital role in providing a platform for the marketing of non-profits [8]. Studies show that majority of NGO's either attains web presence and have no specific publicizing goal or just present information to existing donors.

Darja Leskovec's research describes how the inferences of their research can be implemented to the online provision of information, goods and also how the existence of these non-profit organizations totally depend on the individual donations [9].

Some major points were identified to make the content of NGO's websites more attractive. These include (1) Approachability-how easier it is for the application to offer support (2) Accurately specified reasons, while seeking support (3) Effective Communication with donors (4) Transparency-ways to analyze how donated funds are used (5) Information-letting donor learn everything about NGO's cause (6) Tailoring-letting donors customize things according to their interest (7) Specifying the extent to which a donor can be a part of the cause [6].

3 Result Analysis

Two surveys were conducted and statistical analysis was done for completing the research of donor preferences. The first survey was conducted amongst 85 people to compare monetary and non-monetary donations and to know how much of the population believe in the concept of donation. Results depicted that 75.3% people have made some sort of donations and strongly believe in the concept of donation while on the other hand 24.7% have still kept themselves away from making donations. So, most of the people feel that the concept of donating to an NGO is for a good cause and is right. Also, it was found that only 44.7% have approached NGO or any other organization to donate. Not many of the people, voluntarily went to the NGO to donate.

3.1 T-Test

A t-test was conducted in Statistical Package for the Social Sciences (SPSS) [10] for comparing two questions and getting the result for donation preferences. This test was conducted for two of the survey questions. The purpose was to analyze whether the donors prefer making monetary donations or the non-transparent and unclear monetary system restricts them from making monetary donations. The questions were:

Q1-“Would you like to make non-monetary donations if you find an online platform for it?”

Q2-“Do you feel that the process of NGO is transparent for the monetary donations that you make?”

For both of the above questions, option values were set as 1 for “yes” and 2 for “no” in SPSS while conducting the statistical analysis. Tables 1 and 2 represents the results for the T-test to compare monetary and non-monetary donations. In Table 1, statistics for the paired sample are revealed. For the first question, mean value is 1.1059 which is close to the option 1(yes) whereas for the second question, mean value is 1.7059 which is close to the option 2(no). In Table 2, paired samples test result is depicted and the mean value is negative which means that the first variable (donate_if_platform) is preferred more. The significant value for the test is calculated as 0.000 which is less than 0.05. This implies that there is a very low probability that the null hypothesis is true. Hence, there is a severe inclination towards the non-monetary donations and donor’s responses conveyed that they are ready to make non-monetary donations if they find a platform for it. Since, most of the people felt that the money process of the NGO is not transparent and they do not get the evidence of how their donated money was utilized for the cause of NGO we can conclude that they might not consider making donations associated with money. They would prefer making non-monetary donations like food, books, clothes, etc. The survey also depicted 64% donation preference for clothes, 57% for food, 50% for books, 30.2% for toys and 10.5% other non-monetary donation.

Table 1 T-test paired sample statistics

	Mean	N	Standard deviation	Standard error mean
Pair 1 donate_if_platform	1.1059	85	0.30951	0.03357
Ngo_process_transparent	1.7059	85	0.45835	0.04971

Table 2 Paired sample test

	Paired differences					t	df	Sig. (2-tailed)
	Mean	Std. deviation	Std. error mean	95% Confidence interval of the difference				
				Lower	Upper			
Pair 1 Donate_if_platform-Ngo_process_transparent	-0.60000	0.56061	0.06081	-0.72092	-0.47908	-9.867	84	0.000

3.2 ANOVA Test

After finding out the preferences from the first survey another survey was conducted. The purpose of this survey was to analyze the utility of an online platform meant for donations from donors’ point of view. The survey was conducted comparatively on a bigger scale amongst 152 people who varied in terms of how frequently they make donations. It included people who donate weekly, monthly, yearly, those who donate whenever they feel like, some who donate only during disasters and those who do not make donations at all. One-way ANOVA test was conducted to analyze the opinion of these groups of people regarding the requirement for an online platform like a website that would ease the process of making non-monetary donation. The survey question was:

“Is there any requirement for an online platform like a website that enables you to make non-monetary donations easily and free of cost?”

The option values for this question were 1 for “yes” and 2 for “no”. 79.6% people felt the requirement for an online web platform that enables them to make donations. Table 3 shows the frequently the donors make donations. The descriptive results conveyed that those donate weekly, those who do not make donations and those who donate only during disasters feel the requirement for this web platform the most since the value is closer to 1.

In Table 4, variances between the groups and within the groups are represented. The sum of Squares between the groups is 1.926 and within groups is 22.752. df represents a degree of freedom and total df is calculated as the number of responses-1 i.e. $152 - 1 = 151$. df between groups is calculated as the number of groups (in this case 6)-1 i.e. $6 - 1 = 5$. Mean Square is Sum of Squares divided by the degree of freedom and the final F statistic is calculated by dividing Sum of Square between and within groups. Now, since significant value is 0.035 (less than 0.05) the null hypothesis can be rejected and the difference between both groups is proven significant.

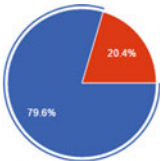
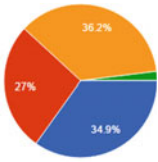
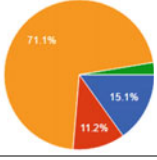
Table 3 Descriptive analysis

	N	Mean	Std. deviation	Std. error
Donate weekly	7	1.0000	0.00000	0.00000
Donate monthly	16	1.1875	0.40311	0.10078
Donate yearly	14	1.4286	0.51355	0.13725
Donate whenever you feel like	74	1.2568	0.43983	0.05113
Donate only during disasters	9	1.1111	0.33333	0.11111
Do not make donations at all	32	1.6025	0.24593	0.04348
Total	152	1.2039	0.40426	0.03279

Table 4 One-way ANOVA

	Sum of squares	df	Mean square	F	Sig.
Between Groups	1.926	5	0.385	2.472	0.035
Within Groups	22.752	146	0.156		
Total	24.678	151			

Table 5 Statistics

Question	Objective	Results
Would you like to make non-monetary donation if you find an online platform in which you do not need to voluntarily go to an NGO to donate?	To about the utility of the online platform once it is created	 <ul style="list-style-type: none"> ● yes ● no
How would you prefer to donate?	To know whether people would prefer and online platform or they would still stick to the offline methods	 <ul style="list-style-type: none"> ● through a website ● by downloading an application in your phone ● by voluntarily going to an NGO ● won't donate at all
When would you prefer to donate?	To know the situations in which the online platform will be utilized	 <ul style="list-style-type: none"> ● if you receive an online request for non-monetary donation from an NGO ● only during disasters ● in both the above cases ● won't donate at all

3.3 Summary of Results

Table 5 depicts the results for a few questions regarding the utility of the online platform, the conditions in which the donors will use the platform to donate and to know the preferences amongst the platforms available.

4 Conclusion

This research examined the real life behavior of the donors towards the process of making donations to NGOs in order to draw results and conclusion. Multiple tests and research methods were adopted to reach the results. Statistical results for various survey questions were analyzed. T-test was used in order to compare the responses for monetary and non-monetary donations and analyzing the reason for inclination towards non-monetary donations. ANOVA Test was used to determine,

which groups feel the requirement for an online platform the most. These groups were segregated on the basis of how frequently they make donations. Results suggested that a lot of people feel the need for an online platform which enables them to donate non-monetary resources possessed by them since they hesitate to make monetary donations due to the in transparency of NGO's money process. Only 36.2% people responded that they would prefer going to an NGO voluntarily for donation purposes. People's responses also conveyed that they are willing to donate in both the situations of disaster and the situation in which they receive an online request from the NGO through this platform. Collectively, these outcomes suggest that an online donation platform for non-monetary resources will turn out to be in favor of NGOs and support their existence by reducing the donation related complications.

References

1. Bajde, D.: Altruism and its relevance to consumer behavior and marketing: exploring the meaning of donation to charity: doctoral dissertation. Ljubljana: Ekonomska Fakulteta (2006).
2. Dhir, S., Kumar, D.: Agile Software Development in Defiance of Customary Software Development Process: A Valuation of Prevalence's and Challenges. *Advance Science Letters*, 21(11), 3554–3558 (2015).
3. Garg, A., Madhurima, Madhulika, Dhir S., “Hubbubs Of Research Terminologies: Let Cat Out Of Bag”, *IJHEPS*, 2015, ISBN:978-81-909047-9-7, Year-5/Vol-1/Issue-9, page 1–10.
4. Guy, B., Patton, W.: The marketing of altruistic causes: understanding why people need help. *The Journal of Consumer Marketing*. 6(1), 19–30 (1989).
5. Sargeant, A.: Charitable Giving: Towards a Model of Donor Behavior. *Journal of Marketing Management*. 15, 215–238 (1999).
6. Sargeant, A., West, D. C., Jay, E.: The Relational Determinants of Nonprofit Web Site Fundraising Effectiveness: An Exploratory Study. *Nonprofit Management & Leadership*. 18 (2), 141–156 (2007).
7. Bennett, R., Barkensjo, A.: Causes and Consequences of Donor perceptions of the quality of the relationship marketing activities of charitable organisations. *Journal of Targeting, Measurement and Analysis for marketing*. 13(2), 122–139 (2005).
8. Sargeant, A.: Web Based Fund Raising: Is Anyone Making Any Real Money? *Fund Raising Management*. 32(8), 20–23 (2001).
9. Leskovec, D.: How to Collect Donations: Conceptual Review and Implications For Online Non-Profit Information Goods Providers. *Akademija*. 55–68 (2010).
10. Vyomkesh, Madhurima, Dhir, S., Garg, A., “Statistical Analysis of Indian E-Commerce Market, “International conference on soft computing techniques and implementations, ICSCA2015, IEEE.
11. Martin, R., Randal, J.: How is donation behavior affected by the donation of others? *Journal of Economic Behavior & Organization*. 67, 228–238 (2008).
12. Basil, D.Z., Ridgway, N.M., Basil, M.D.: Guilt and Giving: A Process Model of Empathy and Efficacy. *Psychology & Marketing*. 25(1), 1–23 (2008).
13. Sargeant, A., Hudson J.: Donor Retention: What Do We Know and What Can We Do About It? *International Journal of Nonprofit and Voluntary Sector Marketing*. 13, 89–101 (2008).

14. Hagenbuch, D.: Easy Ways to Turn Your Supporters into Fundraisers. *Nonprofit World Magazine*. 25(1), 22–23 (2007).
15. Bennett, B.: Giving to the Giver: Can Charities Use Premium Incentives to Stimulate Donations? *Journal of Promotional Management*. 13(3–4), 261–280 (2008).
16. Bennett, R.: Impulsive donation decision during Online browsing of charities websites. *Journal of Consumer Behavior*. 8, 116–134 (2009).
17. Carroll J.: Net makes giving easier. *CA Magazine*. 136(8), 12 (2003).
18. Winterich, K.P. Mittal, V., William T. Ross Jr.: Donation Behavior toward In-Groups and Out-Groups: The Role of Gender and Moral Identity. *Journal of Consumer Research*. 36, 199–214 (2009).
19. Mayo, J.W., Tinsley, C.H.: Warm glow and charitable giving: Why the wealthy do not give more to charity? *Journal of Economic Psychology*. 30, 490–499 (2009).
20. Regner, T., Barria, J.A.: Do consumers pay voluntarily? The case of online music. *Journal of Economic Behavior & Organization*. 71, 395–406 (2009).

Enacting Segmentation Algorithms for Classifying Fish Species

Madhulika Bhatia, Madhulika Pandey, Neeraj Kumar,
Madhurima Hooda and Akriti

Abstract The fundamental feature of Computer vision involves consolidating image processing, pattern recognition and classification procedures. Extricating data from a digital picture relies on upon first distinguishing essential objects or dividing the picture into homogenous sectors or objects termed as segmentation and afterward allotting out these sectors or objects to specific classes termed as classification procedure. The term homogeneous may allude to the shade of the region or an object, however it additionally may utilize different characteristics, for example, composition and shape. This study concentrates on implementing image segmentation and classification on six different fish species using the watershed and the nearest neighbor classifier (kNN) algorithm.

Keywords Image segmentation · Classification · Watershed algorithm · Nearest neighbor algorithm

M. Bhatia (✉) · M. Hooda
Noida, India
e-mail: mbhadauria@amity.edu

M. Hooda
e-mail: 10madhurima@gmail.com

M. Pandey · N. Kumar · Akriti
New Delhi, India
e-mail: madhulika.pandey02@yahoo.in

N. Kumar
e-mail: neerajkumar1989@gmail.com

Akriti
e-mail: aakriti1495@gmail.com

1 Introduction

Dividing an image into region of areas which are same or homogeneous can be termed as image segmentation [1]. The process of segmentation is divided into various categories on the basis of parameters like intensity of pixel, homogeneity, discontinuity, clusters of data, topology etc. The meaning of Classification is to give every segment in an image a certain class, and the classes are decided beforehand. Segmentation and classification are inter-related in a way that a classifier implicitly segments an image, and segmentation implies a classification [2]. In past many algorithms related to segmentation of images have been proposed. There are three classes in which techniques of segmentation can be classified (1) characteristic feature threshold or clustering, (2) edge detection, and (3) region extraction [3]. This is generally used to locate objects and other significant information in digital images. The whole image is segmented into different portions called segments as result. Each and every pixel in an area matches with respect to certain characteristic property or a property that has been computed earlier. Regions that are close to each other are significantly different with respect to the same characteristics [4].

To implement image segmentation and classification, two basic techniques namely nearest neighbor of pixel-based segmentation and watershed algorithm of region-based segmentation were used. The pixel based segmentation aims at classifying the image mainly on the basis of the gray level of the image. Region based segmentation starts with a seed pixel and then split the seed until the original image is made of only homogeneous regions [5]. The approach used is to segment dataset with the help of two algorithms and differentiate between the two segmented images to state the comparison between two algorithms. Existing segmentation and classification algorithm implemented using watershed and kNN algorithm. The dataset is acquired from the internet from dani20294 at word press. The brief description regarding the techniques used is been discussed below.

1.1 *Nearest Neighbor Classifier*

NN classifier algorithm is a lazy-learning image segmentation process. The most common non-parametric methods rely on Nearest-Neighbor (NN) distance estimation, referred to here as “NN-based classifiers”. “Nearest-Neighbor-Image” classifier can classify an image by the class of its nearest that means the most similar image in the database [6]. The output generated by the algorithm is basically a class membership. The object gets assigned to the class that is most common to its k neighbors and the object is classified by the majority votes of its neighbors [7].

1.2 Watershed Algorithm

The word watershed is defined as a ridge that segregates regions drained by different river basins. On the basis of morphological concepts, points can be classified into three categories [8]: (1) points falling into a regional minimum; (2) points where if a drop of water is placed at the any location of those points it would invariably fall to a single minimum; (3) points where water would equally fall to more than one such minimum [9]. The algorithm imagines that a hole is punched in each regional local minimum and the whole topography is submerged in water, the water begins to fill all catchment basins and minimum of which are under the water level. The pixel that is below the water level at a certain period of time is marked as flooded [10]. Water level arises to a certain level where the two flooded regions from separate catchment basins merge. When this happens algorithm builds a 1-pixel thick dam that segregates the two regions and the watershed line is represented by the dam. The flooding continues till the whole image gets segmented into different catchment basins separated by watershed ridge lines [11].

2 Implementing Watershed Algorithm

For image segmentation [12, 13], firstly RGB image is been converted Gray image and then morphological transformation is applied to it. After calculating B and W, watershed algorithm is applied to it as shown in Fig. 1.

2.1 Load Image

The dataset has been acquired from internet [14]. The dataset is converted to grey image using `rgb2gray` (RGB) and the grey image is considered as the topographical surface.

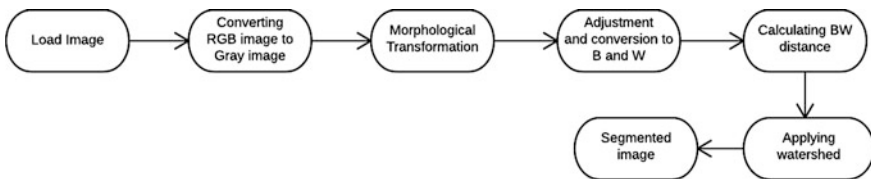


Fig. 1 Watershed segmentation methodology

2.2 *Morphological Transformation*

Tophat is a morphological transformation used for subtracting the background from an image. Tophat is the elimination of the opened image from the original.

2.3 *Adjustment*

imadjust function maps the intensity values in grayscale image y to new values in z such that 1% of data is saturated at low and high intensities of y [15].

2.4 *Converting Image to Black and White*

Using the ‘‘Otsu’’ segmentation method, a correct threshold level is selected where the image gets converted into two modes. Then the image is converted to a black and white image using `im2bw(z, level)` working on the z image with the threshold specified by the `graythresh(image)` function. After getting the black and white image, the image is complemented to get black images and a white background. The black and white image is depicted in Fig. 2.

2.5 *Calculating BW Distance*

`bwdist` calculates the distance transform. The distance transform of an image is the distance from every pixel to the nearest non-zero value pixel. Next infinity is assigned to the values of A inside the O image. Modification of the image is done so that the background pixels and the extended minima pixels are the only local minima of the image. This allows the local minima to be inside the image and then the water is filled and watershed is determined.

Fig. 2 Black and white



2.6 Applying Watershed

The watershed transformation is the transformation that changes the image into some other image in which the catchment basins tend to be the objects to be identified [16]. In Fig. 3 we have made the fishes or the regions to be classified as black and the background as white. Now label2rgb is used to convert the labels to RGB according to the colour map specified which in this case is given as 'hot'. This allows the ridges to be filled with hot colours as shown in Fig. 4.

3 Implementing Nearest Neighbor Classifier

For nearest neighbour classifier technique, methodology is depicted in Fig. 5.

3.1 Load Image

The function imread is used to read the image and imshow will display the image.

Fig. 3 Compliment

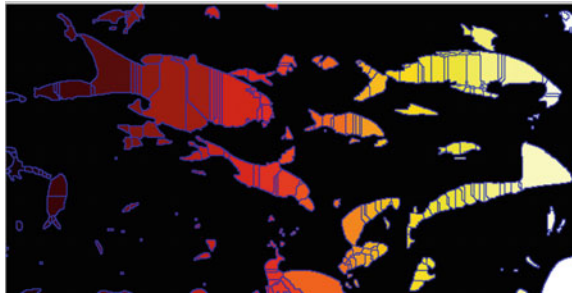


Fig. 4 Applying watershed



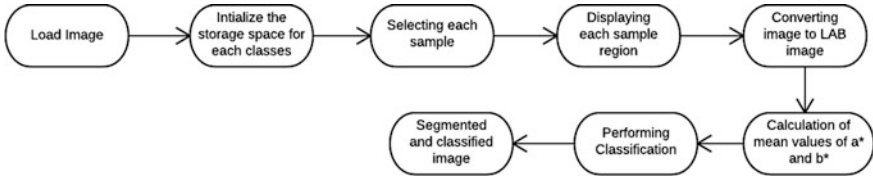


Fig. 5 Nearest neighbour classifier methodology

Fig. 6 Class selection one (Gold Fish)



Fig. 7 Class selection two (Silver Fish)



3.2 Initialize the Storage for Each Sample

The storage for each sample region is selected. We are trying to classify 6 objects in the dataset hence, 6 sample regions have been initialised as goldfish, silverfish, stingray, angel fish, yellow tang fish and sea grass. A variable “nC” is selected that denotes the number of classes which will be 6 in this case. Next a matrix is initialised for the sample regions having zero values. The 6 classes’ selection is shown in Figs. 6, 7, 8, 9, 10 and 11.

3.3 Selecting Each Sample Region

Now, using the ‘roipoly(image)’ function in MATLAB sample regions for 6 classes are selected. The 6 classes’ selection is shown in Figs. 6, 7, 8, 9, 10 and 11.

Fig. 8 Class selection three
(Star Fish)



Fig. 9 Class selection four
(Yellow Tang Fish)



Fig. 10 Class selection five
(Angel Fish)



Fig. 11 Class selection six
(Sea grass)



3.4 Converting rgb to l*a*b* Image

'Lab' image basically has a mix of one channel with no color (L), plus two channels with a dual color combination that have no contrast. 'Lab' format gives two channel values as a1 and b1 which helps in identifying labels for the new pixels we are iterating through. Makecform is an inbuilt function in MATLAB which makes transformation from the color names to color space coordinate system. We are transforming the standard computer monitor RGB values to lab. Now we apply the transformation using apply form function to the image y.

3.5 Calculation of Mean a* and b* Values

Now the mean values for a and b is calculated for each ROI area. First two variables a1 and b1 is defined and then colour marker matrix is made to tell the values of a1 and b1 rgb to l*a*b* image.

3.6 Performance Classification

The next step is performing the classification using the nearest neighbour classifier. We now have the mean values of a1 and b1. For the classification of each pixel in the new image Euclidean distance between the pixel and each colour marker is calculated. The values a1 and b1 is changed to double to perform mathematical calculations. Next we assign value and label (l) as minimum of the distance. Colour labels are assigned from 0 to 5 as there are 6 classes. Then labels are assigned the values of colour labels for each colour marker.

3.7 Clearing Value Distance

Now 6 different colours are declared. Then a matrix is made having the same size as the input image. Labels are converted to double. Then iterating through pixels we assign these pixels the colours according to the labels they have derived from the minimum distance. After the loop ends the imshow command is used to display the segmented image.

4 Results and Discussions

4.1 Watershed Algorithm

We have found that the after applying watershed algorithm final image has black outlines for the ridge lines as shown in Fig. 12. Fishes are getting segmented based on the ridge lines. Watershed produces a complete division of the image in separated regions even if the contrast is poor, thus avoiding the need for any kind of contour joining.

4.2 Nearest Neighbor Classifier Algorithm

After segmentation, the yellow tang fish is shown using cyan colour, gold fish is having red colour, silver fish has a green and blue distinction, the star fish is blue at the bottom, angel fish is yellow and the seagrass is reddish blue in the segmented image. Then a scatter plot is made using the scatter plot parameters according to the pixels of the classes we chose as the objects to be separated as shown in Fig. 13. Scatter plot for the KNN is shown in Fig. 14.

Fig. 12 Segmented image



Fig. 13 Segmented image

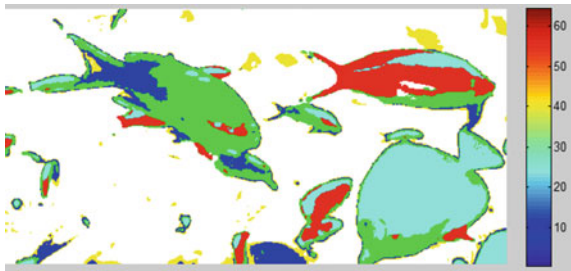
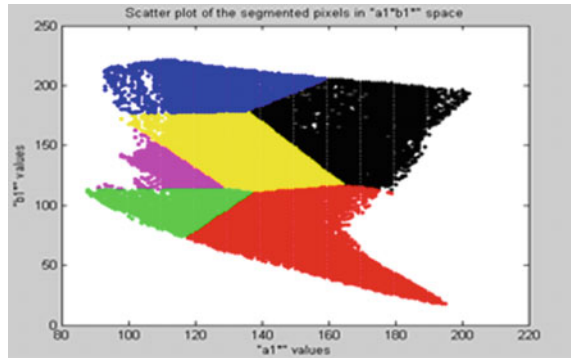


Fig. 14 Scatter plot

5 Conclusion

The main purpose of this work is to implement segmentation process and to get region of interest in an image which helps in notation of the object scene [17]. On the basis of some characteristics fish species are segmented into the partitions set of visually different and homogeneous regions and are further classified [18]. The result includes a segmented image in which six species can be classified according to the region where it is present in the image on the basis of pixel positioning and the second image is the watershed segmented image in which the fishes are separated from the background by black ridge lines. In region based segmentation, it needs gradient information, so the noise in original image will lead to lots of fake regional minimums, which ultimately will result in over-segmentation [9]. We can conclude that since image segmentation deals with and gets affected by type of image, color, texture and even level of noise, different techniques are specialized for a particular application in order to achieve better performance results and this identification and selection of an appropriate approach to a segmentation problem can be a difficult task [1].

References

1. Khan, A. M., & Ravi, S. (2013). Image Segmentation Methods: A Comparative Study.
2. Pandey, Madhulika. "An Amalgamated Strategy for Iris Recognition Employing Neural Network and Hamming Distance." *Information Systems Design and Intelligent Applications*. Springer India, 2016. 739–747.
3. Fu, K. S., & Mui, J. K. (1981). A survey on image segmentation. *Pattern recognition*, 13(1), 3–16.
4. Bhatia, M., Yadav, D., Gupta, P., Kaur, G., Singh, J., Gandhi, M., & Singh, A. (2013, September). Implementing edge detection for medical diagnosis of a bone in Matlab. In *Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on* (pp. 270–274). IEEE.

5. W.X Kang, R.R Liang. “The comparative research on image segmentation algorithms”, IEEE conference on ETCS, 2009.
6. Boiman, O., Shechtman, E., & Irani, M. (2008, June). In defense of nearest-neighbor based image classification. In *Computer Vision and Pattern Recognition, 2008. CVPR 2008. IEEE Conference on* (pp. 1–8). IEEE.
7. Harini, R and C. Chandrashekhar. “Image Segmentation using nearest neighbor classifier on kernel formation”, International conference on pattern recognition Informatics and Medical engineering”, 2012.
8. Rafael C. Gonzalez, Richard E Woods. Digital Image Processing (Second Edition). Beijing: Publishing House of Electronics Industry, 2007.
9. Yang, Q., & Kang, W. (2009). General research on image segmentation algorithms. *International Journal of Image, Graphics and Signal Processing (IJIGSP)*, 1(1), 1.
10. Agarwal, Rashi: Image Processing: [<http://www.learningsquare.com>].
11. Bhatia, M., Bansal, A., Yadav, D., & Gupta, P. (2015). A Proposed Stratification Approach for MRI Images. *Indian Journal Of Science And Technology*, 8(22). doi:[10.17485/ijst/2015/v8i22/72152](https://doi.org/10.17485/ijst/2015/v8i22/72152).
12. Wang, L., Shi, J., Song, G., & Shen, I. F. (2007). Object detection combining recognition and segmentation. In *Computer Vision–ACCV 2007* (pp. 189–199). Springer Berlin Heidelberg.
13. Tsai, A., Yezzi Jr, A., Wells, W., Tempny, C., Tucker, D., Fan, A.,.... & Willsky, A. (2003). A shape-based approach to the segmentation of medical imagery using level sets. *Medical Imaging, IEEE Transactions on*, 22(2), 137–154.
14. [Unattributed]: Fish species: [<https://dani20294.wordpress.com/>].
15. Bhatia, M., Bansal, A., Yadav, D., & Gupta, P. (2015). Proposed Algorithm to Blotch Grey Matter from Tumored and Non Tumored Brain MRI Images. *Indian Journal Of Science And Technology*, 8(17). doi:[10.17485/ijst/2015/v8i17/63144](https://doi.org/10.17485/ijst/2015/v8i17/63144).
16. Bansal, A. (2013). Implementing Edge Detection for Detecting Neurons from Brain to Identify Emotions. *International Journal of Computer Applications*, 61(9).
17. Dr. (Mrs.) G. Padmavathi, Dr. (Mrs.) P. Subashini and Mrs. A. Sumi “Empirical Evaluation of Suitable Segmentation Algorithms for IR Images”, *IJCSI International Journal of Computer Science Issues*, Vol. 7, Issue 4, No 2, July 2010.
18. X. Munoz, J. Freixenet, X. Cuf_1, J. Mart, “Strategies for image segmentation combining region and boundary information”, *Pattern Recognition Letters* 24, page no 375–392, 2003.

Pattern Based Extraction of Times from Natural Language Text

Vanitha Guda and Suresh Kumar Sanampudi

Abstract Nowadays data sources are producing huge amount of data everywhere namely news data, wikis, web crawlers and many other databases, data needs to be analyze and exploited to obtain the required information to build several knowledge databases. In this context time is an essential component of information space and it is a real phenomenon which makes a continuous change through which we live. The information which is associated with time is termed as temporal information and the process of identifying and retrieving times are called as temporal information extraction (TIE). The temporal information extraction is useful in many natural language processing (NLP) applications like information extraction for generating better text summaries and temporal question answering (Q.A) systems for time related searches, and information retrievals etc. Times are also useful to order the events in the text, the ordering can be from the past through the present into the future and this will helpful to measure the durations of an event occurrence and find outs the relation between them. In this paper we present our work for extraction of various forms of times from natural language by using pattern rules. The results obtained from the experiments found to have better precision value when compared with existing methods.

Keywords Times extraction • Temporal information extraction • Natural language processing

V. Guda (✉)

JNTUH, Chaitanya Bharathi Institute of Technology, Gandipet, Hyderabad 500075, India
e-mail: vanithaguda@gmail.com

S.K. Sanampudi

JNTUHCEJ, Nachupally, Karimnagar, India
e-mail: sureshsanampudi@jntuh.ac.in

© Springer Nature Singapore Pte Ltd. 2017

H.S. Saini et al. (eds.), *Innovations in Computer Science and Engineering*,
Lecture Notes in Networks and Systems 8, DOI 10.1007/978-981-10-3818-1_6

1 Introduction

Web is the primary source for language processing applications like question answering, information extraction, and document summarization etc. There is a serious need to extract the temporal information from the given text, for example, consider Q.A system of news domain, if we want to know who was the Prime Minister (P.M) of India in the month of *February 1991*, system need to result the document set that tell us about the P.M from 1990 to 1995. In this context a temporally aware system will helps the Q.A system to infer about the P.M during February 1991. Next to project the importance of temporal information in medical domain, consider a patient's record that the doctors maintains the information about patient's medical observations. The information delivered in the record need not be in chronological order, extracting a temporal structure of the medical record will help practitioner to understand the patient's medical history easily. Extracting temporal information will benefit to the other applications of NLP like legal domain, and other times based searches. But most of the earlier research works on temporal information processing was carried out on the data collected from the news domain because of the availability of large corpora and presence of temporal expressions.

The remaining part of the paper is organized as follows, Sect. 2 describes an overview of existing works for temporal information extraction, Sect. 3 presents a framework for times extraction and its components description, in Sect. 4 describes an algorithm of pattern based rules for times extraction and lastly Sect. 5 explains results and conclusion of the paper in Sect. 6.

2 Existing Works

The dynamic facts of the information are called as events [1] these events are all kinds (Example, wedding, joined, natural, cultural, sports, political). Mostly events occur within a timeline thus extracting the time related information is a challenging task because time exist in many forms. Time expressions in natural language text can be expressed as a point in time i.e., implicit or explicit form, duration or a frequency. Temporal information extraction extracts the times which are connected with events or depending on the document creation time (DCT). Most of the existing works carried out in domain specific, initially temporal expressions are treated as a type of named entities and their identification is also a part of the named entity recognition task. But in recent works of TIE has been applied to various domains like medical [2], legal [3] etc. The existing systems [4, 5] provides times as outputs and the identifications of times as annotations for further interpretations. Here in Table 1 we are presenting detailed study on existing methods for temporal information.

Table 1 Study on existing systems for times extraction

Name of the system	Technique	Description
Temporal algebra systems [6]	Qualitative and quantitative temporal models and temporal logics	Only based on temporal logic, No specification for the explicit time interval
Time calculus [16]	Encodes the natural language based on the constraints, in this derived temporal logic yields under specification and granularity information of times	Quantitative duration easily captured. Basic vocabularies required for the composition of time expression are temporal units and values
Time graphs [17]	Recognizes the temporal variables like points or interval, and different classes of constraints (temporal relations) namely that are qualitative and quantitative relations	The relative durations between time intervals are represented in a separate network. By using Time graph relations between events and times can be identified
Rule Based methods or knowledge driven methods [18]	HeidelTime as a UIMA component, SuTime as a Temporal Tagger, TempEx first temporal tagger with TIMEX2 tags.GUTimeperl temporal tagger	Knowledge is encoded in the form of patterns that expresses the rules to extract the times. Information will be extracted from corpora by using predefined or discovered linguistic patterns
Statistical methods [19]	Hidden Markov models (HMM) for NER, and Temporal tagging [20], conditional random field (CRF) as a statistical model for pattern recognition	These algorithms are modelled by training samples, this can be called as a class of supervised learning algorithms
Feature engineering [21]	(1) Maximum entropy models based on the weights of the features (2) Based on the syntactic and semantic features of the system (3) SVM based models support vector machines to find the features	Essential component for all classifiers in this feature descriptors words recognition with nominal values. It also works based on word features digit features domain features
Unified model	Handles both qualitative and quantitative temporal information through PDNs	The problem is identifying the consistency of PDN is NP-hard
Time ML [12]	Temporal mark-up language is a Representation or mark-up language used to capture temporal information. It consists of a collection of tags inserted into a text, intended to mark explicit temporal relations among events reported in the text	It's only a mark-up language can only represents the language cannot performs reasoning of the generated events with times

Table 1 presents the overview of the existing systems, the columns in the table are, first column is existing system names, second column describes the method used in that corresponding systems and last column explains description about the system. In above overview the first three systems are traditional approaches based on Allen’s interval algebra [6] next three systems are machine learning algorithm based [7], and the last two systems are annotations based systems.

3 Frame Work for Times Extraction

The Fig. 1 presents the proposed framework model for extraction of times from natural language text and the major components are input source, Normalization, and pattern based rules for identifying the times.

3.1 Components Description

- (i) **Input text:** Natural language text, text document or pool of documents can be the Input for the work and text is not in structured form.
- (ii) **Normalization:** This component is the basic step in NLP, normalization means text needs to undergo some pre-processing steps to prepare the text for further processing. Normalization involves finding the Lexical, Morphological, Syntactic and Formatting features these are also called as tokenization. The features are:
 - Lexical: Forming of basic token means word itself removing all other letters from the token (e.g., 5 for “5pm”) and also involves removal of unwanted symbols, stop word elimination from text these to identify proper token.

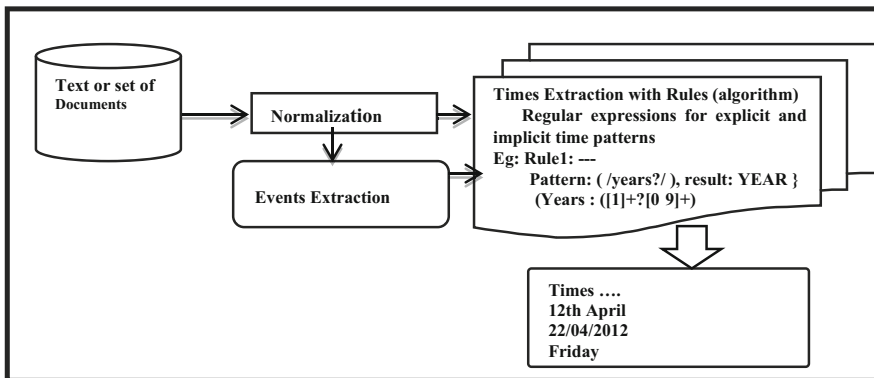


Fig. 1 Proposed model for times extraction

- Morphological: The Parts Of Speech (POS) tagging can be implemented for identified token (e.g., noun with NN, adjective as JJ) by using Stanford OpenNlpParser [8].
 - Syntactic: Basic tag of token forms a syntactic chunk which the token belongs to (e.g., I-IPP for inside proper pronoun, VBD- verb in ing form).
 - Formatting features: These are some set of flag indications where text needs to be formatted (Example, if the text all in is all Caps like “FRI” is all Dots “F.C.I”, is all Digits like “2012” or initial Caps “March” or any of all these combinations).
- (iii) **Events Extraction:** Event extraction component extracts the events from the text with the help of the tagged entities. Events are generally expressed by means of verbs, nominalizations, adjectives, predicative clauses or prepositional phrases. Event extraction explained in our previous work [9] identified events can also be the input for times extraction component.
- (iv) **Times Extraction with Rules:** This is the major component of our work for the extraction of times. Here we have written pattern rules for times extraction, before that identifying various types of time expression and recognition of it is must. The temporal information refers to different types of time expressions that can be a timestamp or duration. The following are the types of time expression:
- (a) **Types of Time Expressions:** Time expressions can be date, time, duration or set frequency time, that are:
- **Date Expressions:** A date expression refers to a point in time of the granularity day “e.g., April 22, 2013” or any other coarser granularity, like month “e.g., April 2013” or year “2013”. Most of the date expressions can be calendric dates (e.g., “January 4”) and other verbal expressions which can be mapped to calendar dates (e.g., this week, last month, next Friday, or this time etc.).
 - **Time Expression:** Time expression can refer to a point in time and time granularity smaller than day such as a part of a day (e.g., Friday morning) or time of a day (e.g., “5:50pm”). In other words TIME is used to represent specific time points within a day e.g., 4.05am or can be relative time 20 min ago etc.
 - **Duration Expression:** A duration expression provides information about the length of an interval. The amount of intervening time between the two end-points of a time interval. Examples for Duration expressions like “last two months onwards”, “two hours”.

Table 2 Times classification

Temporal expression	Type	Normalized
December 3, 1884	Explicit time and type as a DATE	1884-12-03
From 1952 to 1962	RANGE	1952/1962

- **Set Frequency or Range Expression:** A set expression refers to the periodical aspect of an event, e.g., “every Friday, or thrice a day”. Medical Documents like discharge summaries have various frequency terms and most of them are represented by latin abbreviations such as tid (thrice a day)”, \q4 h (every four hours)”.
- **Implicit and Explicit Times:** Most of the times classifications [10] are described in the form of explicit and implicit form of representations in the above mentioned types of Date, Time expressions are said to be *explicit form* and the duration like points, intervals are called as *implicit form* representation.

Example 1: Dr. Rajendra Prasad (Born on 3rd December 1884) was the first President of the Republic of India from 1952–1962. Prasad, from Bihar, was the first President of independent India, and also he is the longest-serving President for 12 years. Prasad was the only president to serve two terms in office.

In above Example 1, extraction of *temporal information about when was Dr. Rajendra Prasad born? And in which year he was president can be represented in the following Table 2.*

Time exist in text any of the above mentioned types, for the extraction it is necessary to identify the type and its context. By using the above stated classification of time expressions in our work our pattern based rules are formed to extract the times from text explained in Sect. 4.

4 Pattern Based Rules for Times Extraction

Two popular methods [11] for times extraction are TIMEX3 Tag from TimeML [12] and other is by using Java library SuTime [13]. The major limitation of TimeML is purely annotation based only represents time expressions. SuTime is another method, it extracts all types of time expressions which exist in text, but specific time based holiday events (like Independence day, Mother’s day etc.), and durations are not recognized by Suntime. In our work we considered the limitations of SuTime and TimeML and extended our work. We implemented the work in two ways one is by using SuTime and the other is without using SuTime that are:

- Using SuTime: After the normalization task, in Rules component by using SuTime we are extracting time in all formats and to overcome the limitation of SuTime we are adding a specific holiday package to SuTime (explained sample rules of holiday package in algorithm).
- Without using SuTime: For this task we have written complete pattern based rules for recognition of all types of times including holidays package, the algorithm stated below:

Input: Set of normalized tokens

Output: identified time expressions (T_d) from text

Terms: (T_e : explicit time; T_i : implicit time; T_h : holiday time)

1. Initialize RESULT Set as empty = {}
2. for each normalized token t in corpus do {
3. if ($t.timestamp \in (T_e)$) { // map the T_eRules for explicit times
4. } else if ($t.timestamp \in (T_i)$) { // map the T_iRules for implicit times
5. } else if ($t.timestamp \in (T_h)$) { // map the T_hRules for specific holiday times
6. } else if (Timestamp of token $t \rightarrow T_e$ or T_i or T_h called as token t_d and $t_d \in (T_t, D_a, D_u, C_o)$ { // (T_t : times, D_a : dates, D_u : duration/ intervals, C_o is composite time)
// Sample rules for T_e, T_i and T_h stated below in note }
7. RESULT t_d // the derived t_d can be mapped to any one of the rules
8. Add t_d to RESULT
9. } else non temporal word $t \notin t_d$

```

}
```

Note: Sample Pattern Rules

T_e Rules: a token that matches the regular expression for explicit times "years"

```
{ruleType: "token  $t_e \in T_e$ ", Pattern:(/years?/), result:
YEAR}: (Years: ([1]+?[0-9]+)
```

```
{ruleType: "token  $t_e \in T_e$ ", Pattern explicit:( /times?/ ),
result: times} (Years:[1]+?[0-9]+)
```

T_i Rules : mapping from a token that matches the regular expression for "implicit times"

```
{ruleType: "token  $t_e \in T_i$ ", pattern: (( $\$num$ )/ to|- /
( $\$num$ )["- NODE)), result: Duration ( $\$1, \$2$ )} // can be
extended to find the with  $\$3$  and uses Allen's algebra
```

T_h Rules: mapping the token for specific holiday times

```
{ruleType: "token  $t_e \in T_i \wedge t_e \in T_i$ ", "filter", pattern
({word:/Independencyday|spring|Good Friday |march| may/
& !{ tag:/NN.*/ } ])}
//Some set of sample rules for specific events from
holiday package
```

```
1. {(/new//year/ $\$POSS?$ /eve/)=>IsoDate(NIL,12,31)}//New
year Event
```

```
2. {(/new//year/ $\$POSS?$ /day/?)=>IsoDate(NIL,1,1)}//January1st
3. {(/republic/ /day/)=>IsoDate(NIL, 1, 26)}// Republic Day
4. {(/independence//day/)=>IsoDate(NIL, 8, 15)}
//Independence Day
```

```
5. {(/st.?.|saint/?/valentine/ $\$POSS?$ /day/)=>IsoDate(NIL,2,14
)} // Valentains Day
```

```
6. {(/good//friday/)=>IsoDate(NIL, 3,25) } // GoodFriday
7. {(/dr.b.r.ambedkar//jayanti/?)=>IsoDate(NIL, 4,14)}//
AmbedkaJayanthi
```

```
8. {(/gandhi//jayanthi/)=>IsoDate(NIL, 10, 2) } //Gandhi
Jayanthi
```

```
9. {(/x-?mas|christmas//eve/)=>IsoDate(NIL,12, 24)}//X-mas
Eve
```

```
10. {(/x-?mas|christmas//day/?)=>IsoDate(NIL,12, 25)}
//Christmas
```

In the above algorithm token t maps to T_e , T_i and T_h maps the pattern rules and returns the time expressions. Date, time, duration and specific holiday time everything has to be written in the form of regular pattern of the defined categories. In above note sample rules for explicit, implicit and holiday times and c is for holiday specific times. In step 7 after c point sample holiday times are presented. The normalized text token matches with the rules mentioned that will be added to result set, otherwise it is not temporal event.

5 Results

To obtain the results, the data set for our experiment was collected from Wikipedia articles. We selected the three representative categories of articles Warfare [14], and Celebrities [14], and news data [14]. Summing over all articles yields a total 2000 sentences. We randomly sampled 30 documents with 1200 sentences, within this test set there are total 268 events identified by Evita [1, 15] and total times are 148 hand coded manually the extracted times with the methods presented in Table 3.

By using the above designations Precision, Recall and F-measure are calculated these measures are the quality measures to find the relevance and accuracy of the methods. In Table 4 total number of times present in the given input are 148, second row consists of retrieved times after executing the methods, third row consist of relevant items from the retrieved, and last three rows consists of accuracy measures. The values are computed as follows:

- A = Number of relevant records retrieved,
 - B = Number of relevant records not retrieved, and
 - C = Number of irrelevant records retrieved.
- Precision = $A / (A + C) * 100$
 Recall = $A / (A + B) * 100$

$$F - \text{Measure} = 2 * \frac{\text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}}$$

Example 1: For Using Suntime Calculation: A = 63, B = 148 - 63 = 85 and C = 100 - 63 = 37 substitute these values for Precision = $63 / (63 + 37) * 100 = 63\%$, Recall = $63 / (63 + 85) = 42.5\%$, similarly compute for the remaining, calculated values represented in Table 4.

Table 4 Shows obtained results for the comparing the three method’s accuracies, using SuTime with holiday package obtained better precision that is 94 and 85% f-measure and our proposed algorithm for times is achieved equivalent f-measure with SuTime with holiday package results. With the above comparisons the results of our approach also obtained noticeable precision.

Table 3 Results obtained for the methods

Test sources/articles	Number of events	Times retrieved from the input data		
		Using SUTIME	Using our pattern rules algorithm	SUTIME + holiday package of our algorithm
Warfare	102	28	30	32
Celebrities	78	15	39	32
News data	88	39	69	61

Table 4 Accuracy of the results (with precision, recall, F-measure)

	Using SUTIME	SUTIME + holiday package of our algorithm	Using our pattern rules algorithm
Total number of times in the given input	148	148	148
Total retrieved times	100	125	138
Number of relevant times from retrieved	63	118	122
Precision (%)	63	94	89
Recall (%)	43	79	82
F-measure (%)	51	85.8	85.3

6 Conclusion and Future Work

In this paper we presented an approach to extract the times from the text, observed the results with the existing methods. Work explained in two methods for the extraction of times With SuTime and without SuTime by adding our holiday package. The proposed algorithm with SuTime library provides better precision with low recall rate. Modelling of the times information, time related events increasingly apparent in natural language applications such as temporal summarization, time based QA systems related and to the legal domain also. Scalability is the one major issue of our approach in future work will be focuses on scalability and also by using this times extraction component as one sub module temporal event information can be retrieved efficiently.

References

1. Roser Sauri, Robert Knippen, Marc Verhagen, and James Pustejovsky. Evita: a robust event recognizer for QA systems. In HLT '05: Proceedings of the conference on Human Language Technology and Empirical Methods in Natural Language Processing, pages 700–707, Morristown, NJ, USA, 2005.
2. SunghwanSohn, Kavishwar B Waghlikar, Dingcheng Li, Siddhartha R Jonnalagadda, Cui Tao, Ravikumar Komandur Elayavilli, and Hongfang Liu. Comprehensive temporal information detection from clinical text: medical events, time, and tlink identification. Journal of the American Medical Informatics Association, pages amiajnl-2013.
3. Yan Xu, Yining Wang, Tianren Liu, Junichi Tsujii, I Eric, and Chao Chang. An end-to-end system to identify temporal relation in discharge summaries: 2012.
4. Schilder, F., and Habel, C. From temporal expressions to temporal information: Semantic tagging of news messages. In Proceedings of the ACL-2001.
5. Verhagen, M.; Mani, I.; Saur'1, R.; Knippen, R.; Littman, J.; and Pustejovsky, J. Automating Temporal Annotation with TARSQI-2005.
6. Allen, J. Maintaining knowledge about temporal intervals. C. ACM 26(11):832–843, 1983.
7. Matthew Richardson and Pedro Domingos. Markov logic networks. Machine Learning, 2006.

8. <http://nlp.stanford.edu/software/eventparser.shtml>.
9. Vanitha Guda, Suresh Kumar Sanampudi.: Rule based Event Extraction in Natural Language Text, In Proceedings of IEEE international conference of Recent Trends in ISBN 978-1-5090-0773-5/16/\$31.00 © 2016 IEEE, pp. 47–51, May 2016.
10. N. Chambers, S. Wang, and D. Jurafsky. Classifying temporal relations between events. Proceedings of the ACL 2007.
11. B. Boguraev and R. K. Ando. Time Bank-Driven TimeML analysis. In Annotating, Extracting and Reasoning about Time and Events, Dagstuhl Seminar Proceedings. Dagstuhl, Germany, 2005.
12. Pustejovsky, J., Castano, J., Ingria, R. Saurí, R., Gaizauskas, R., Setzer, A., Katz, G., and Radev, D., TimeML: Robust specification of event and temporal expressions in text. In IWCS-5 Fifth Intl. Workshop on Computational Semantics-2003.
13. Angel X Chang and Christopher D Manning. Sutime: A library for recognizing and normalizing time expressions. In LREC, pages 3735–3740, 2012.
14. <http://www.cs.washington.edu/ai/iwp/tie.html>.
15. Verhagen, M.; Mani, I.; Saurí, R.; Knippen, R.; Littman, J.; and Pustejovsky, J., Automating Temporal Annotation with TARSQI. In Demo Session. Proceedings of ACL, 2005.
16. Bramsen, P.; Deshpande, P.; Lee, Y.; and Barzilay, R. Inducing temporal graphs. In Procs. of EMNLP, 189–198, 2006.
17. Mani, I.; Schiffman, B.; and Zhang, J. Inferring temporal ordering of events in news. In Procs. of HLT-NAACL, 2003.
18. JannikStrotgen and Michael Gertz. Heideltime: High quality rule-based extraction and normalization of temporal expressions. In Proceedings of the 5th International Workshop on Semantic Evaluation, pages 321–324. Association for Computational Linguistics, 2010.
19. Daniel M. Bikel, Richard Schwartz, and Ralph M. Weischedel. An algorithm that learns what is I in a name. Mach. Learn., 34(1–3):211–231, ISSN0885-6125. [10.1023/A:1007558221122](https://doi.org/10.1023/A:1007558221122), feb 1999.
20. J. Poveda, M. Surdeanu and J. Turmo. A Comparison of Statistical and Rule-Induction Learners for Automatic Tagging of Time Expressions in English. In Proceedings of the International Symposium on Temporal Representation and Reasoning, 2007.
21. Corinna Cortes and Vladimir Vapnik. Support-vector networks. In Machine Learning, pages 273–297, 1995.

Evaluating the Performance of Tree Based Classifiers Using Zika Virus Dataset

J. Uma Mahesh, P. Srinivas Reddy, N. Sainath and G. Vijay Kumar

Abstract Data mining have been used in real time applications due to its artificial intelligence nature. Data mining is highly used in medical domain as it helps in making better predictions and supports in decision making. It also supports physicians in developing better diagnostic treatments. We have used Data mining to analyze Zika virus disease which leads to many deaths in South Africa and America. Zika virus is very fatal and spreads due to virus transmitted primarily by Aedes Mosquito. In this research work we have worked on tree based mining algorithms and further improvement is done by using filters which removes noise from the dataset. In this we worked on J48, decision tree, SVM and Random forest algorithms and indicate Experimental results.

Keywords Data mining · Classification · Tree based classifier · WEKA · Zika virus dataset · Decision tree

J. Uma Mahesh (✉)

Department of Computer Science & Engineering, Geethanjali College
of Engineering & Technology, Hyderabad, Telangana, India
e-mail: umamaheshshalini@gmail.com

P. Srinivas Reddy · N. Sainath

CSE, Bharat Institute of Engineering & Technology, Hyderabad, Telangana, India
e-mail: psrinu570@gmail.com

N. Sainath

e-mail: nsainath@gmail.com

G. Vijay Kumar

ECM, K L University, Guntur, India
e-mail: gvijay_73@kluniversity.in

© Springer Nature Singapore Pte Ltd. 2017

H.S. Saini et al. (eds.), *Innovations in Computer Science and Engineering*,
Lecture Notes in Networks and Systems 8, DOI 10.1007/978-981-10-3818-1_7

1 Introduction

Data mining is the process of getting interesting and relevant information from huge data which is stored in repositories. Data mining process is used to discover, examine and mine useful data using various algorithms [1].

In healthcare organizations, data mining is highly used so as to extract useful information from patient’s raw data which helps in intelligent discussion making and helps the physicians in diagnosis of disease [2, 3] likewise in this paper we have depicted the spread of Zika virus and its symptoms for the disease, generated few graphs for purpose of vizualisation and the statistics obtained serves the purpose of obtaining knowledge from the processed data by applying the concepts of Data mining.

Data mining can be consequently branching off into sub processes that consist of selecting data preprocessing, transformation, data mining and finally interpreting data. Data Mining is also known as Knowledge Discovery of Data (KDD) [4].

Steps involved in the Data mining process can be depicted by Fig. 1.

Steps followed in Data mining process:

- Step 1 Data selection in this data which is required for our application domain is selected. Relevant data is retrieved from data repositories. Medical data can gathered from various health records of patients also it can be frequently obtained from various health care centers [5].
- Step 2 After selecting the data, Data preprocessing is done in which ambiguous data is handled; data is converted into specific formats and deals with missing values [6].
- Step 3 Transformation of data in which unstructured data is handled and data is converted into structured and in numeric form. And data is mined using various functions and algorithms to extract hidden information.
- Step 4 After mining results are evaluated, and visualized in form of graphs which helps in making better interpretations [7] In health care, mining is all about extracting and analyzing.

The patient’s conditions which helps in making assured predictions so as to raise the accuracy of diagnosis [8].

Fig. 1 Data mining process

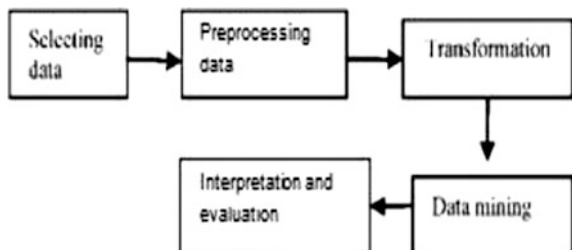
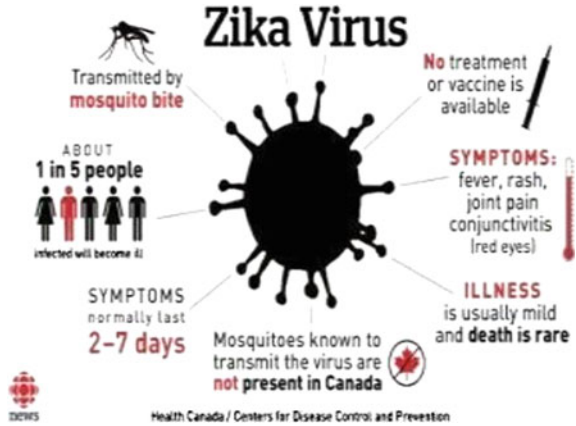


Fig. 2 Causes for Zika virus



In medical domain, classification technique is widely used. Classification gives step by step guide to build a classifier model using on training data, and the model is tested using the test data and helps in making predictions [9]. In this we compare the classification of various tree based algorithms (SVM, Random forest and J48).

Classification is process examining the attributes of each instance and assigning it to one of a predefined class label [10]. In this classification is done based on the symptoms and other factors and predict either patient is died of Zika virus, it has widely spread in areas around the rain forests of Central Africa. Zika virus has been the leading cause of death in South European countries. In 2014, there was 90% death rate due to this virus. There is great need of mining, as handling patients in these situations is very difficult and to get efficient results mining is very helpful. The virus transmits primarily through the Aedes mosquitoes infecting persons.

Vaccines for the cure of Zika virus are under progress but variety of blood, immunological and therapies are given to infected person. Also supportive cares with rehydration, symptomatic treatments are given [11, 12]. Data mining methods applied to the datasets to find out relations and patterns that are useful in understanding the evolution of disease [13]. In this paper, we evaluated the performance measures using tree based classification algorithms. The aim is to evaluate the performance of various classifiers and improvement is made by using unsupervised filters and further fusion of algorithm is done so as to make better prediction. In this research work we worked on machine learning WEKA tool we generated the decision tree (Fig. 2).

2 Related Works

Rahman and Hasan [2] classified Zika affected patients into various categories according to their health conditions. And various decision tree models are developed and compared and predictions are made using the efficient decision tree

model. Robu and Hora [9] have analyzed medical data using various data mining algorithms on 4 different datasets and improvements are made so as to make better predictions.

Datasets include:

1. Spread of Zika virus across countries of North America.
2. Symptoms of Zika virus affected cases.

Amin et al. [1] have discussed data mining and analyzed the Zika affected patients. In, this paper we have discussed and compared various data mining algorithms and performances of these algorithms are evaluated. Solutions [4] used various classification algorithms to predict Zika on basis of gene expression data. And performance is evaluated when worked against 2 different Zika virus datasets. Nookala et al. [8] worked on real datasets using various classification algorithms and performance is evaluated on basis of various parameters like accuracy, precision and recall and various techniques in order to improve the results. Jarrett et al. [3] presented decision support framework in health care domain. Meng and Yang [14] has proposed hybrid algorithm in order to enhance the accuracy of classifiers and worked on 10 real datasets. Mohamed et al. worked on various classification algorithms and performance is evaluated. Farid et al. [13] has presented general data mining framework.

3 Methodology

Step 1: Information Gathering (ZIKA Virus)

Zika virus disease (Zika) is a disease caused by Zika virus that is spread to people primarily through the bite of an infected *Aedes* species mosquito. The most common symptoms of Zika are fever, rash, joint pain, and conjunctivitis (red eyes). The illness is usually mild with symptoms lasting for several days to a week after being bitten by an infected mosquito. People usually don't get sick enough to go to the hospital, and they very rarely die of Zika. For this reason, many people might not realize they have been infected. Once a person has been infected, he or she is likely to be protected from future infections. Zika virus was first discovered in 1947 and is named after the Zika forest in Uganda. In 1952, the first human cases of Zika were detected and since then, outbreaks of Zika have been reported in tropical Africa, Southeast Asia, and the Pacific Islands. Zika outbreaks have probably occurred in many locations. Before 2007, at least 14 cases of Zika had been documented, although other cases were likely to have occurred and were not reported. Because the symptoms of Zika are similar to those of many other diseases, many cases may not have been recognized.

Symptoms:

Most people infected with Zika virus won't even know they have the disease because they won't have symptoms. The most common symptoms of Zika are fever, rash, joint pain, or conjunctivitis (red eyes). Other common symptoms include muscle pain and headache. The incubation period (the time from exposure to symptoms) for Zika virus disease is not known, but is likely to be a few days to a week. Areas with active mosquito-borne transmission of Zika virus: Prior to 2015, Zika virus outbreaks occurred in areas of Africa, Southeast Asia, and the Pacific Islands.

In May 2015, the Pan American Health Organization (PAHO) issued an alert regarding the first confirmed Zika virus infections in Brazil.

Currently, outbreaks are occurring in many countries. Zika virus will continue to spread and it will be difficult to determine how and where the virus will spread over time.

Step 2: Framing of Dataset (ZIKA Virus)

Symptoms and countries of spread of ZIKA virus are taken as attributes and data is collected then designed data in excel sheet by retrieving as (.csv extension) pie charts, box plots are designed (Fig. 3).

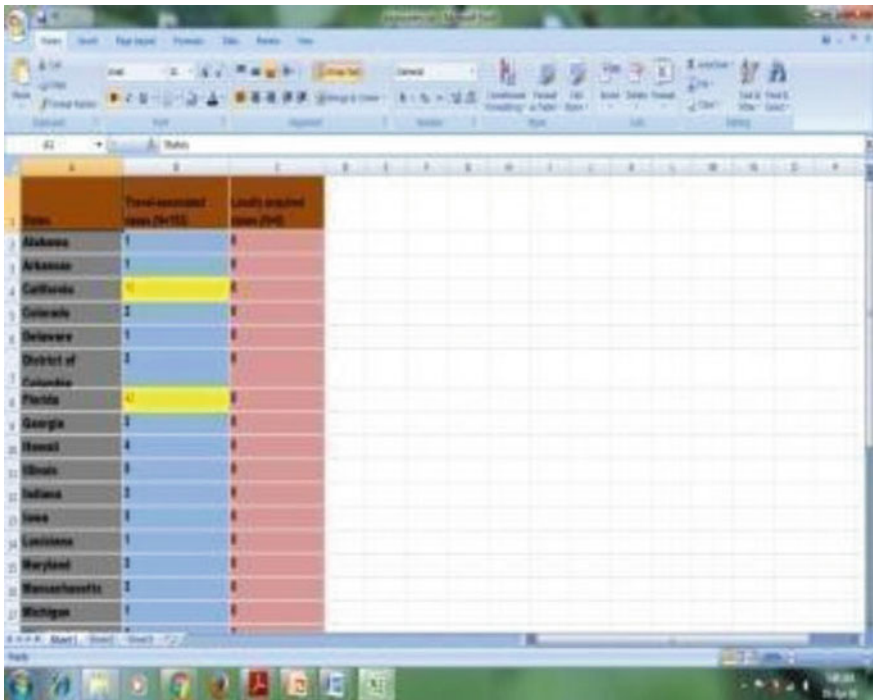


Fig. 3 Spread of "ZIKA" virus across countries of North USA

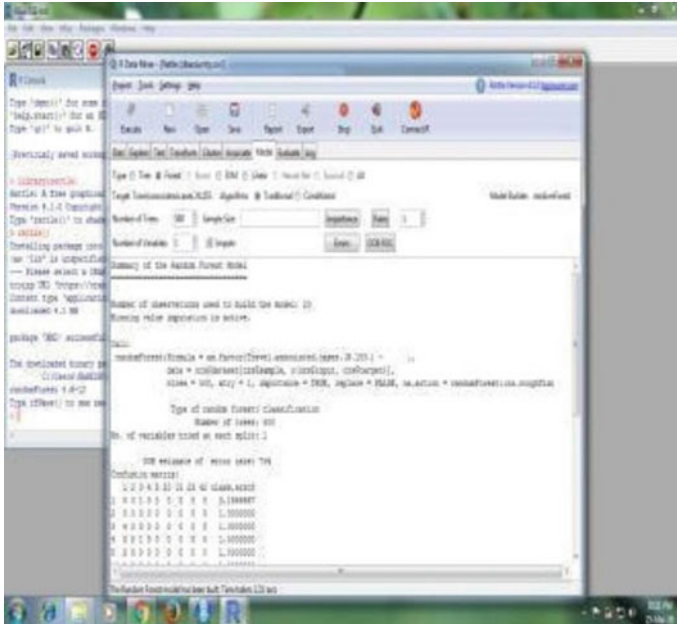


Fig. 4 Generated confusion matrix

The above dataset comprises of data regarding spread of zika virus across various countries of North America that happens by 2 modes, they are:

- 1. Locally transmitted cases
- 2. Travel associated cases

Step 3: Applying Algorithms on ZIKA Dataset

Various algorithms like Random forest is been applied on the Zika virus dataset collected in this paper. The outcomes obtained are:

Generated Confusion matrix.

Time taken for generating the Random forest (Fig. 4).

To create confusion matrix following steps are followed:

```
#create ZIKA dataset obs = c(sample(c(0, 1), 20, replace = TRUE), NA); obs = obs[order(obs)] pred = runif(length(obs), 0, 1); pred = pred[order(pred)] #calculate the confusion matrix confusion.matrix(obs, pred, threshold = 0.5)
```

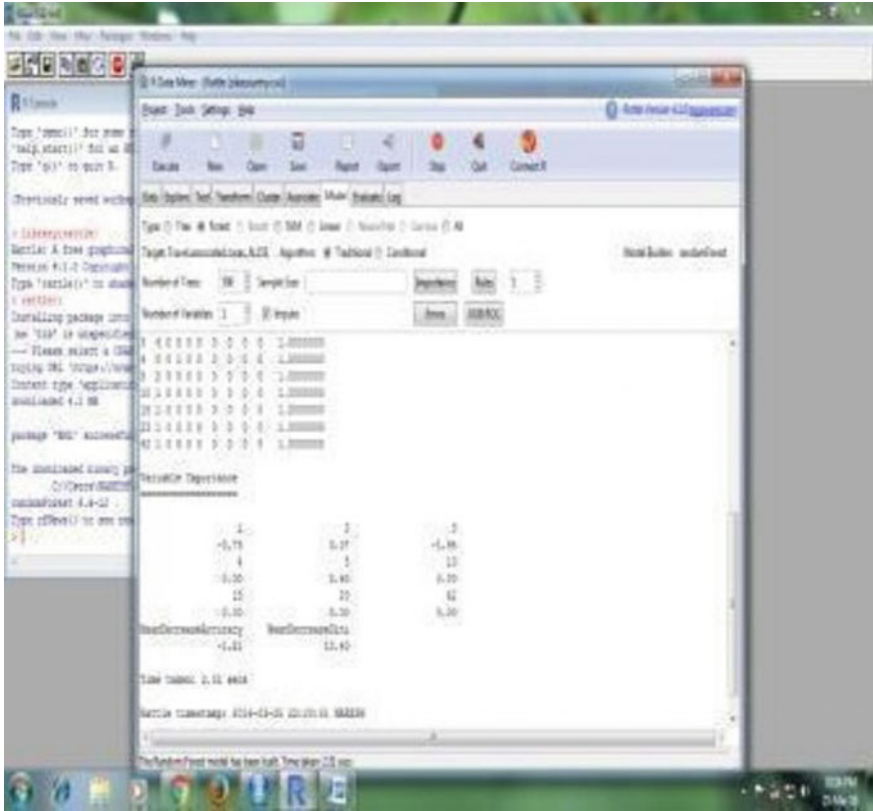



Fig. 5 Computing confusion matrix

where the parameters are described as:

obs a vector of observed values which must be 0 for absences and 1 for occurrences pred a vector of the same length as obs representing the predicted values. Values must be between 0 and 1 pre presenting a likelihood.

Returns a confusion matrix (table) of class 'confusion matrix' representing counts of true and false presences and absences (Fig. 5).

Table 1 Events predicted from dataset

Predicted	Event	No event
Event	A	B
No event	C	D

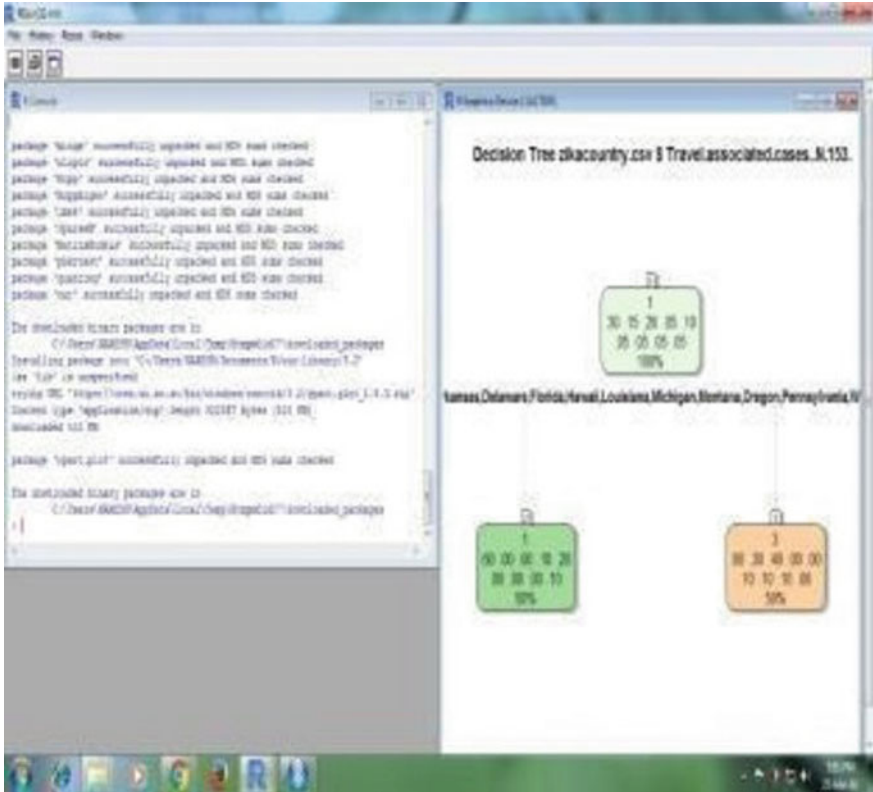


Fig. 6 Decision tree

Confusion matrix with a 2×2 table with notation (Table 1).
 The formulas used to compute the confusion matrix are:

$$\begin{aligned}
 \text{Sensitivity} &= A / (A + C) \\
 \text{Specificity} &= D / (B + D) \\
 \text{Prevalence} &= (A + C) / (A + B + C + D) \\
 \text{PPV} &= (\text{sensitivity} * \text{Prevalence}) / ((\text{sensitivity} * \text{Prevalence}) + ((1 - \text{specificity}) * (1 - \text{Prevalence}))) \\
 \text{NPV} &= (\text{specificity} * (1 - \text{Prevalence})) / (((1 - \text{sensitivity}) * \text{Prevalence}) + ((\text{specificity}) * (1 - \text{Prevalence}))) \\
 \text{Detection Rate} &= A / (A + B + C + D) \\
 \text{Detection Prevalence} &= (A + B) / (A + B + C + D)
 \end{aligned}$$

Balanced Accuracy = (Sensitivity + Specificity)/2.

Step 4: Obtaining decision tree for ZIKA country travel associated cases basing on frequency (Fig. 6).

Creating, Validating and Pruning Decision Tree in R To create a decision tree in R, we need to make use of the functions rpart(), or tree(), party(), etc. rpart() package is used to create the tree. It allows us to grow the whole tree using all the attributes present in the data.

4 Conclusion

Data Mining is gaining its popularity in almost all applications of real world. One of the data mining techniques i.e., classification is an interesting topic to the researchers as it is accurately and efficiently classifies the data for knowledge discovery. Decision trees are so popular because they produce human readable classification rules and easy to interpret than other classification methods. Frequently used decision tree classifiers are studied and the experiments are conducted to find the best classifier for Zika Diagnosis. The experimental results show that SVM is the best algorithm for classification of Zika virus dataset. It is also observed that SVM performs well for classification on medical data sets of increased size.

References

1. Amin, Syed Umar, Kavita Agarwal, and Rizwan Beg. "Genetic neural network based data mining in prediction of heart disease using risk factors." *Information & Communication Technologies (ICT), 2013 IEEE Conference on*, pp. 1227–1231. IEEE, 2013.
2. Rahman, Rashedur M., and Fazle RabbiMdHasan. "Using and comparing different decision tree classification techniques for mining ICDDR, B Hospital Surveillance data." *Expert Systems with Applications* 38, no. 9 (2011): 11421–11436.
3. Jarrett, Anna. "Ebola: A Practice Summary for Nurse Practitioners." *The Journal for Nurse Practitioners* 1\, no. 1 pp. 16–26, (2015).
4. Solutions. In *DEXA Workshops*, pp. 90–94. 2013.
5. Weitschek, Emanuel, Giovanni Felici, and Paola Bertolazzi. "Clinical Data Mining: Problems", Pitfalls.
6. Xuexia, Dou. "Application of data mining algorithms in the analysis of financial distress early warning model of listed company." In *Computer Research and Development (ICCRD), 2011 3rd international Conference on*, vol. 4, pp. 287–290. IEEE, 2011.
7. Gupta, Shelly, Dharminder Kumar, and Anand Sharma. "Performance analysis of various data mining classification techniques on healthcare data." *International journal of computer science & Information Technology (IJCSIT)* 3, no. 4 (2011).
8. Nookala, Gopala Krishna Murthy, Bharath Kumar Pottumuthu, Nagaraju Orsu, and Suresh B. Mudunuri. "Performance analysis and evaluation of different data mining algorithms used for cancer classification".
9. Robu, R., and C. Hora. "Medical data mining with extended WEKA." *Intelligent Engineering Systems (INES), 2012 IEEE 16th International Conference on*, pp. 347–350. IEEE, 2012.
10. Yu, Hong, Xiaolei Huang, Xiaorong Hu, and HengwenCai. "A comparative study on data mining algorithms for individual credit risk evaluation." In *Proceedings of the 2010 international Conference on Management of e - Commerce and e-Government*, pp. 35–38. IEEE Computer Society, 2010.
11. *International Journal of Advanced Research in Artificial Intelligence (IJARAI)* Vol. 2, no. 5, pp. 49–55, (2013).
12. <http://www.who.int/mediacentre/factsheets/fs103/en/>.
13. Farid, Dewan Md, Li Zhang, Chowdhury Mofizur Rahman, M. A. Hossain, and Rebecca Strachan. "Hybrid decision tree and naive Bayes classifiers for multi-class classification tasks." *Expert Systems with Applications* 41, vol. 4, pp: 1937–1946, 2014.

14. Meng, Jianliang, and Yanyan Yang. "The application of improved decision tree algorithm in the electric power marketing." In World Automation Congress (WAC), 2012, pp. 1–4. IEEE, 2012.
15. Zandi, Faramak. "A bi-level interactive decision support framework to identify data mining-oriented electronic health record architectures." *Applied Soft Computing* 18 (2014) pp: 136–145.
16. <https://github.com/mirador/ebola-dataireleases>.
17. Zhao, Jitao, and Ting Wang. "A general framework for medical data mining." In Future Information Technology and Management Engineering (FITME), 2010 International Conference on, vol. 2, pp. 163–165. IEEE, 2010.

SaaS CloudQual: A Quality Model for Evaluating Software as a Service on the Cloud Computing Environment

Dhanamma Jagli, Seema Purohit and N. Subash Chandra

Abstract The cloud computing is a key computing approach adopted by many organizations in order to share resources. It provides Everything As-A-Service (XaaS). Software-As-A-Service is an important resource on the cloud computing environment. Without installing any software locally, service user can use software as a utility. And enjoy the benefits of SaaS model. Hence SaaS usage is increased drastically, the demand for selecting quality is also increased. This paper presents a novel quality model intended for evaluating software as a service (SaaS), depending on the key features of Software as a service. Because SaaS key features are playing critical role in the quality and differentiating from conventional software quality.

Keywords Cloud computing • Software-As-A-Service (SAAS) • Service quality • Software quality

1 Introduction

The cloud computing as a sophistication in computing epitomizes vigorously scalable and regularly virtualized resources, which are delivered as a service through a web browser via Internet. In the cloud computing environment, everything such as network, infrastructure, platform, software or application is available as a service. The unique type of cloud service is Software-As-A-Service (SaaS).

D. Jagli (✉) · S. Purohit · N. Subash Chandra
JNTU Hyderabad, Hyderabad, India
e-mail: dsjagli.vesit@gmail.com

S. Purohit
e-mail: supurohit@gmail.com

N. Subash Chandra
e-mail: subhashchandra_n@yahoo.co.in

S. Purohit
Kirti College, University of Mumbai, Mumbai, India

It stands commonly used service by many customers and service providers to provide benefits to service their customers. In order to understand these benefits, evaluating the quality of SaaS on cloud has become extremely essential due the increased demand. This quality model further helps to manage quality at the top level as per the evaluation results. Existing conventional quality models are not competent enough for providing all Software service-specific features [1]. In this paper, initially, the description of conventional quality model for software and service is given separately. Further the paper describes about the proposed model followed by results and discussion. Finally, it concludes with future scope.

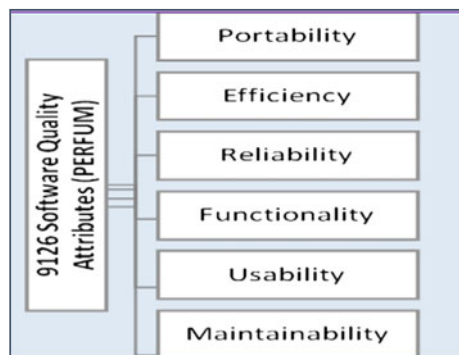
2 Proposed Quality Model

In this paper an innovative quality model is suggested to assess quality of software as a service on cloud, produced around quality attributes.

(a) Software Quality Model-ISO/IEC 9126 (25010): (PERFUM)

The ISO/IEC standard quality models are of two types: product quality model and quality in use model. Based on the static and dynamic properties a product quality model is further subdivided as internal product quality and external product quality model. Quality in use model is a system model used to relate the usage of a product to the context of the use. The ISO/IEC Standard quality model later modified as 25010 quality model to know software products quality. This model has identical internal and external quality characteristics and sub characteristics. The variance is in the quality measures. Quality in use has no sub characteristics [2]. According to ISO/IEC 9126 standards, software quality can be assessed using six characteristics. The software product quality model has six characteristics and 24 sub characteristics. In this paper, proposed quality model evaluates software product, the metrics or measures of the software product quality similar to ISO/IEC 9126 [3]. The standard attributes have been shown in the Fig. 1.

Fig. 1 ISO/IEC9126 quality model



Due to the gap between conventional and clouding computing paradigms, the traditional quality models, based on ISO 9126 standards, are inadequate for assessing quality of SaaS [1]. They do not support efficient and effective evaluation of cloud computing explicit quality features. A quality model which can completely evaluate the needs of SaaS on cloud yet to arise [1]. Hence, rigorous efforts are being made at developing a quality model needed for measuring Software-As-A-Service on the cloud computing environment.

(b) Service Quality Model: (RATER)

In 1988, Parasuraman and his team introduced a standard quality model for service evaluation with five dimensions were used in order to evaluate the service quality provided to any service users. That quality method is called as SERVEQUAL, which has become a very popular model for service quality. “The service qualities emphasized are reliable, assurance, responsiveness, empathy and tangible” [4] as shown in the Fig. 2. Service user satisfaction is an increasing worry of any businesses all through the world [5]. In order to Evaluate SaaS quality, it also required to evaluate service quality.

(c) Key Features of Software-As-A-Service(SaaS)

The quality of SaaS includes quality software product plus quality of service. The key features of SaaS are critical and play an important role while describing quality of software as a service [6]. Identified Seven key features of SaaS are identified as shown in the Fig. 3.

- *Multi-tenant*: Multi-tenant means acceptable to the proposal which has profitable clarifications to multiple end user. The Software as a service essentially attains multi-tenancy. That is it has a capability to fulfil multiple end-users in parallel built on a solitary application instance. The service users want same functionality. Generally, multi-dimensional QoS parameters are response time, throughput and availability [7].

Fig. 2 Service quality model

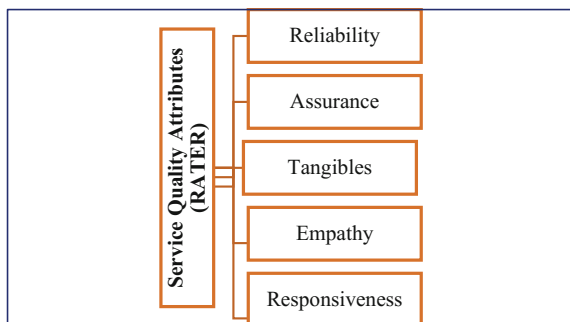
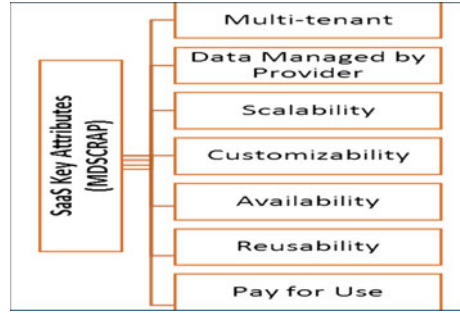


Fig. 3 Key features of SaaS

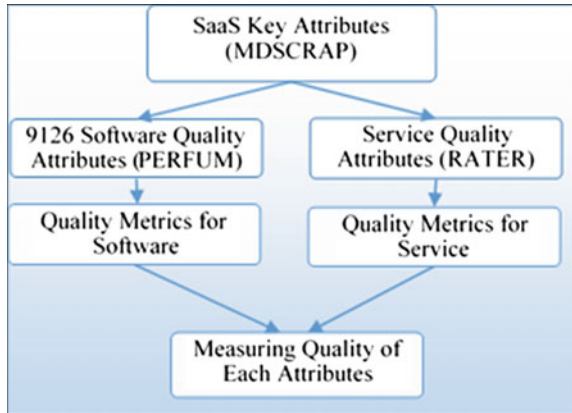


- *Data Maintained by Service Provider*: SaaS model of software arrangement provides service suppliers authorization solicitations anywhere to service users on demand. So that service suppliers will be additionally responsible for installation and data management. Hence, maximum data of clients are stored in the service provider's data center and maintained by them.
- *Scalability*: It is a desirable feature of the cloud services. Scalability means ability to handle increasing quantities of tasks or workloads. Service users can not have the control over resources. Service suppliers are solely liable for expanding services as per customer requests.
- *Customizability*: It is a capability used for services to be altered through service users, so that service users can utilize services effectively.
- *Availability*: The service users are capable of using SaaS in the cloud computing environment from a Web browser through the Internet. The customers are not having proprietorship to use the SaaS. That means the software have to be installed and run on the service supplier's server. This feature is one of the most critical in the SaaS usage.
- *Reusability*: This defines a capability of reuse of software essentials for building various applications. The main principle of cloud computing is to use again and again several kinds of services available on the internet. In cloud computing reusability is an essential feature of SaaS.
- *Pay-per-use*: The expenses of Software-as-a-services are purely based on the usage of service and are not related to purchase of ownership [1].

(d) SaaS Cloud Quality Model

Proposed quality model of SaaS is based on the two important aspects of SaaS: software quality and service quality. SaaS quality model is also involved with the key feature of SaaS. In this model all key features of SaaS are identified and are mapped to software product quality model as well as service quality model. Further some metrics to measure quality of SaaS are derived. The work flow of the model is shown in the Fig. 4.

Fig. 4 Proposed quality model work flow



3 Results and Discussion

(1) Mapping Software Quality Attributes

The proposed quality model is used to map the SaaS key features with standard software product quality attributes as per ISO/IEC 9126. Mapping relationship between the key features of Software-as-a-service plus quality attributes of ISO 9126 standard are shown in the Fig. 5. The goal of this mapping is to empower the capacity of each key feature of SaaS and to have metric to measure its software product quality. Similarly the key features of SaaS are mapped with each quality attribute of software product quality model and derived related metrics as shown in the Fig. 7. This enables to measure the quality of each attribute of SaaS with respect to software.

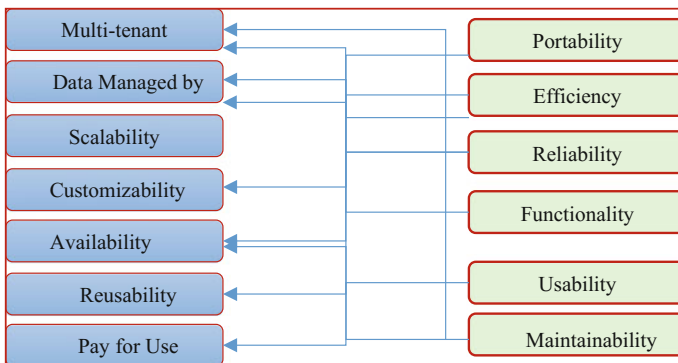


Fig. 5 Mapping software quality attributes

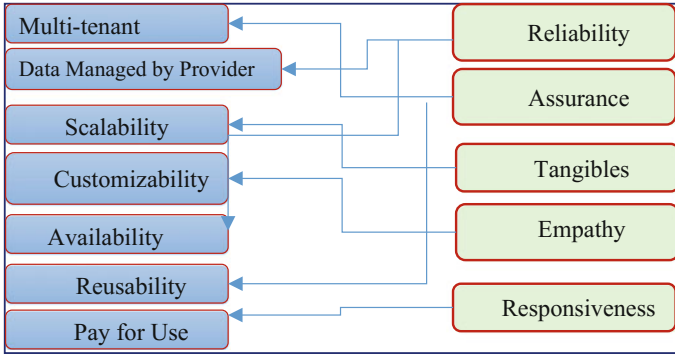


Fig. 6 Mapping service quality attributes

(2) Mapping Service Quality Attributes

The SERVQUAL is a widely accepted evaluation model of service quality which is used as the basic framework [8] for service quality on the cloud computing environment so that all key features of SaaS are mapped with service quality attributes as shown in the Fig. 6.

(3) Derived Metrics

The goal of this mapping is to empower the capacity of each key feature of SaaS to have a metric to measure its service quality. Similarly for all key features of SaaS when mapped with each quality attribute of the service quality model and derived related metrics gives a good measure of quality. This facilitates the best possible way to measure the overall quality as well as quality of each attribute of SaaS with respect to its service. Many metrics are derived to measure software and service quality of SaaS as shown in the Fig. 7.

- Maturity: Occurrence of failure of the software [9].
- Interoperability: Capability of software element towards interacting with further components [10].
- Suitability: Correctness to arrangement of purposes of software [9].
- Accurateness: Rightness of the functions [9].
- Recoverability: Capacity towards to revert back unsuccessful system to complete working system, including data plus network links [9].
- Understandability: Standardizes the effortlessness system functions can be understood and communicates to human being perceptual model to use easily [9].
- Changeability: Characterizes the amount of effort needed for code modification [9].
- Install ability: Illustrates struggle necessary to install software [9].

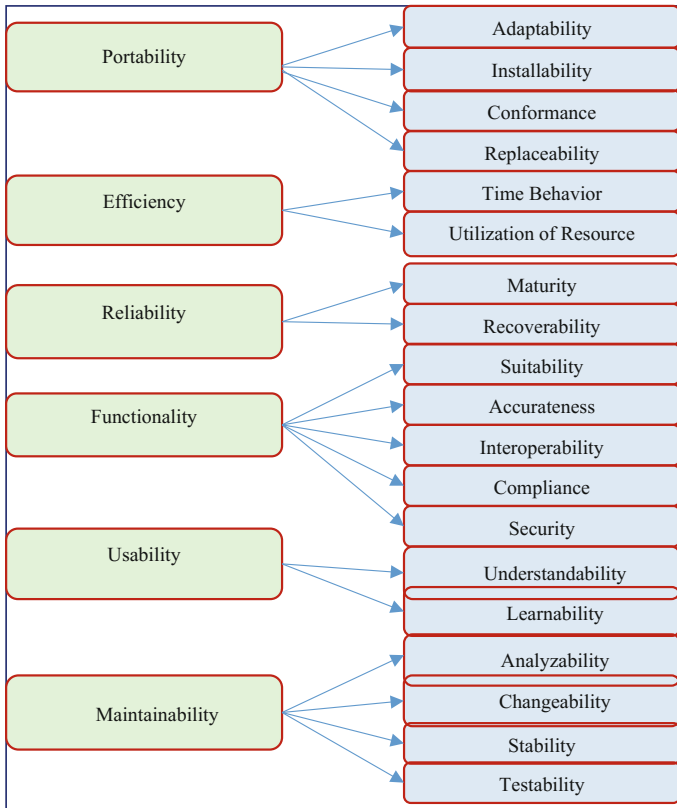


Fig. 7 Derived metric for software quality attributes

4 Conclusion and Future Scope

The new proposed model has been introduced based on the key features of SaaS. All identified key features have been mapped with standard quality attributes of software product and service, as SaaS is the combination of both software products as well as service. With the help of mapping quality metric had been derived to evaluate a quality of SaaS. Further, it is also intended to implement automated tool by using this model to evaluate SaaS quality.

References

1. J. W. J. Y. Lee, "A Quality Model for Evaluating Software-as-a-Service in Cloud Computing," in Software Engineering Research, Management and Applications, 2009. SERA '09. 7th ACIS International Conference on, 2009, pp. 261–266.
2. J. -M. Desharnais, "Analysis of ISO/IEC 9126 and 25010," 2009.

3. P. X. Wen and L. Dong, "Quality Model for Evaluating SaaS Service," in 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies, 2013, pp. 83–87.
4. Gajah, S. N. R. Sankranti, S. A. Wahab, N. J. A. Y. Norazira Abas, and S. N. A. M. Rodzi, "Adaptive of SERVQUAL Model in Measuring Customer Satisfaction towards Service Quality Provided by Bank Islam Malaysia Berhad (BIMB) in Malaysia," *Int. J. Bus. Soc. Sci.*, vol. 4, no. 10, pp. 189–198, 2013.
5. A. Parasuraman, V. A. Zeithaml, and L. L. Berry, *SERVQUAL: A Multiple-Item scale for Measuring Consumer Perceptions of Service Quality*, vol. 64. 1988, p. 28.
6. Dhanamma Jagli, Dr. Seema Purohit, Dr N. Subhash Chandra "SAASQUAL : A Quality Model for Evaluating SaaS on The Cloud," pp. 1–6, 2015.
7. Q. He, J. Han, Y. Yang, J. Grundy, and H. Jin, "QoS-driven service selection for mul-ti-tenant SaaS," *Proc. - 2012 IEEE 5th Int. Conf. Cloud Comput. CLOUD 2012*, pp. 566–573, 2012.
8. Z. Wang, N. Jiang, and P. Zhou, "Quality Model of Maintenance Service for Cloud Computing," 2015 IEEE 17th Int. Conf. High Perform. Comput. Commun. (HPCC), 2015 IEEE 7th Int. Symp. Cybersp. Saf. Secur. (CSS), 2015 IEEE 12th Int. Conf Em-bed. Software, pp. 1460–1465, 2015.
9. F. Beringer, "Software quality metrics and model," 2009.
10. IEEE Computer Society, "IEEE Standard for a Software Quality Metrics Methodology - IEEE Std 1061TM-1998 (R2009)," vol. 1998, 2009.

A Survey on Computation Offloading Techniques in Mobile Cloud Computing and Their Parametric Comparison

Sumandeep Kaur and Kamaljit Kaur

Abstract Mobile Cloud Computing (MCC) is a distributed computing model which outspreads the idea of utility computing of the Cloud Computing to the Smart Mobile Devices (SMDs). Outsourcing intensive applications of the SMDs to the remote servers is the key idea of Mobile Cloud Computing. Many techniques have been developed for offloading computation intensive application code on the cloud servers for execution for saving scarce resources of the mobile devices such as battery life, network bandwidth, device's storage memory, processing unit's performance etc. This paper presents review on techniques for computational offloading. Computation offloading is relocating some computation concentrated part of an application code to a cloud server for execution to fulfil the source requirements. A comparative study on the techniques for computational offloading has been shown on the basis of parameters such as bandwidth, network latency, cost, energy consumption, execution time etc.

Keywords Cloud computing · Mobile cloud computing · Computation offloading · Application partitioning · Application deployment · Network-aware computation offloading

1 Introduction

Cloud Computing is a type of distributed model which offers access to the sharable resources over the internet; that resides on the cloud, on request basis. Resources like storage, computing, services etc. Mobile Cloud Computing is a distributed computing model that enables Smart Mobile Devices (SMDs) to access the services

S. Kaur (✉) · K. Kaur
Department of Computer Engineering and Technology,
Guru Nanak Dev University, Amritsar, India
e-mail: suman.goraya22@gmail.com

K. Kaur
e-mail: kamaljit.aujla86@gmail.com

provided by the Cloud providers through cloud data centers. Mobile device uses internet networks such as wireless, 3G etc. for connecting to the cloud server. The applications like GPS, Image Processing, Speech recognition, Sensor Data Applications, Multimedia search, Natural Language Processing need high computing power and large number of resources. In Computation offloading resource-intensive and computation-intensive components of mobile applications are migrated to the cloud servers for execution. Cloud servers are selected with sufficient amount of resources available [1].

2 Literature Work

2.1 Offloading in Mobile Cloud Computing

Offloading in Mobile Cloud Computing is migrating computation to cloud servers which are rich in resources. Offloading accesses servers for short duration through network (wired or wireless). These servers use concept of *Virtualization* to provide the offloading services. Enormous amount of research has been performed on computation offloading in MCC and number of frameworks has been developed. Kosta et al. [2] presented a framework for MCC named *ThinkAir* for dynamic resource provisioning and parallel execution in the cloud for mobile application code offloading. *ThinkAir* removes the input, output and environmental restrictions. It supports scalability and parallelism. It provides method level offloading and supports virtualization for performing parallel executions.

Folino and Pisani [3] presented a framework for offloading of mobile applications code using Genetic Programming (GP). Fitness function is used for evaluating the user's requirements, the network, the data and the application code. Magurawalage et al. [4] presented a system design for computation offloading in mobile cloud computing. They included a middle layer in the MCC architecture which is a composition of cloudlets and it is termed as cloudlet layer. An algorithm has been developed to decide whether to offload the computation to the cloudlet layer or to the mobile clone taking into consideration the turnaround time.

Komnios et al. [5] proposed a framework named Cost-Effective Multi-Mode Offloading (CEMMO) that improves the computation offloading in MCC with multi-hop peer-assisted communication. CEMMO offloads the mobile traffic irrespective of its content. Mukherjee and Debashis De [6] presented an offloading scheme for low power for femto-cloud mobile network that emphasis on the decision making standards that is whether to offload the code to the cloud server or to execute the code on the mobile device. Khan et al. [7] presented a context-aware application model named as *MobiByte*. *MobiByte* uses multiple types of computation offloading techniques. This model improves performance of the applications by improving the energy efficiency, execution time.

Year Ref.	Description	Environment	Parameters				Limitations	
			Bandwidth	Network Latency	Execution Time	Energy Consumption		Cost
2012 [3]	ThinkAir: framework for dynamic resource allocation and parallel execution	Xen			Offloads only if execution time is improved	Offloads only if energy consumption is improved using energy estimation model.	Privacy-sensitive applications need more security	
2014 [5]	Energy efficient and network-aware framework: uses middle layer termed as cloudlet layer to improve the network efficiency	CloudSim 2.0	Network medium reduces with the use of the cloudlet layer	Less network delay	Use of cloudlet layer benefits in term of execution time	For CPU of 500 MIPS the energy consumption is 0.9W	Subjective to network and data security threats	
2015 [6]	Cost Effective Multi Mode Offloading (CEMMO) framework	Opportunistic Network Environment (ONE) simulator				31% better energy consumption	Less cost	Scalability, security
2015 [7]	Low power offloading strategy: femto-cloud architecture	Cloud Servers of WBUT (West Bengal University of Technology)		Reduces network latency to 4-31% approx.	Less network latency reduces execution time	Energy consumption can be reduced to 3-32% approx.		No support for energy efficient job scheduling and resource management
2015 [8]	MobiByte: a context-aware application model for computation offloading in MCC	Android platform, Eclipse, Sony Xperia S smartphone, GoogleApp Engine, JDK, JRE			Does not depend on clones thus reduces service startup delays and runtime	Results show offloading to virtual cloud consumes less energy than real cloud		Communication overhead

Fig. 1 Comparison of frameworks for computation offloading in MCC

Lack of compatibility of MCC frameworks with standard technologies & techniques for dynamic performance estimation and relocation of program components makes it harder to adopt MCC at large to overcome the limitations of mobile devices. Most of the MCC frameworks rely on full cloning of the code. They also focus on the less execution time. Figure 1 shows the parameters based comparison of frameworks for computation offloading in MCC.

2.2 Application Partitioning

Computational offloading in Mobile Cloud Computing uses the application partitioning to separate different operational logics of the application code which can be executed independently in the distributed environment of cloud computing. Runtime Profiling and Partitioning of application is one of the challenging aspects of computational offloading in MCC which requires additional computing resources

utilization in SMDs. Lie Yang et al. [8] proposed a framework which partitions application at runtime and executes them distributive on the cloud optimizing the throughput. March et al. [9] had proposed a model named μ Cloud which partitions applications as a graph of components deployed onto cloud servers and mobile devices for execution. Liu et al. [10] have proposed a taxonomy and review on Application Partitioning Algorithms (APAs) in Mobile Cloud Computing. Three types of partitioning models have been used by the application partitioning applications; graph-based model, Linear Programming (LP) model, and hybrid approach (combination of graph based and LP). Chun et al. [11] proposed an elastic offloading framework named CloneCloud. It performs static and dynamic profiling of the application code for the partitioning. Abdelminaam et al. [12] talk about computation offloading in mobile cloud computing and propose a model which carefully partitions the application code using an elastic partition algorithm and offload it to the cloud clone for the execution. Figure 2 shows the parameters based comparison for Application partitioning in MCC.

Year Ref	Description	Environment	Parameters			Limitations	
			Bandwidth	Network Latency	Execution Time		Energy Consumption
2012 [9]	A Framework for partitioning and execution of data stream applications in MCC	Genetic Algorithms			More benefit in terms of execution time when the application size rises up	Larger computation cost as the application graph size increases	Load balancing and scheduling problem
2011 [10]	μ Cloud: partitions applications as a graph of components	Java, SL4A (Scripting Languages for Android)		Less Network latency			Subjective to security threats
2011 [12]	CloneCloud Framework: elastic offloading framework	Android Platform, Dell Desktop, Ubuntu				Automatic static and dynamic analysis of running code to improve the energy consumption	Less Scalable, considers limited input/output conditions
2013 [13]	An Elastic Computation partitioning framework for augmenting the performance of mobile applications	Android 4 OS, Samsung Galaxy Grand, 1.2 GHz Dual Core CPU		Less Network latency		Computing cycles are available for less power consumption	Energy efficiency is less

Fig. 2 Comparison of frameworks for application partitioning in MCC

Year Ref.	Description	Environment	Parameters				Limitations
			Bandwidth	Network Latency	Execution Time	Energy Consumption	
2013 [15]	Graph-based Application Partitioning Algorithms for optimized s/w deployment in MCC	Eppstem power law generator	Focus is on minimizing bandwidth between Software components		Execution Time is lower than SA (Simulated Annealing) but much higher than MLKL (Multilevel graph Partitioning)		No Focus on Execution time
2015 [16]	Energy Efficient Computational Offloading framework (EECOF)	Android OS platform, Samsung Galaxy S2 mobile devices, Open Stack Cloud OS	Network medium reduced up to 84%			Energy Consumption Cost reduced to 69.9%	Lack of seamless application execution

Fig. 3 Comparison of frameworks for application deployment in MCC

2.3 Application Deployment

In MCC, it is important to choose the VM machine for application deployment so that the execution time and energy consumption is minimum and performance of the mobile device remains high. Verbelen et al. [13] have designed graph-based APAs that allocate software components to the machines in the cloud so that bandwidth is minimized. They have discussed three heuristics: Multilevel graph partitioning (MLKL), Simulated Annealing (SA), Hybrid (combination of MLKL and SA). Drawback of these algorithms is that they do not focus on the execution time and energy consumption. Shiraz et al. [14] proposed an Energy Efficient Computational Offloading Framework (EECOF) in MCC. This framework stresses on the overhead of relocation of components at runtime to lessen the energy consumption. Results shows that energy consumption cost has been reduced 69% and the size of the data transmission has been reduced by 84%. Lee et al. [15] talks about energy conscious scheduling for distributed computing systems under different operating systems. List scheduling is an effective method to solve several scheduling problems. Figure 3 shows the parameters based comparison of frameworks for application deployment in MCC.

3 Conclusion and Future Work

The main issue in MCC is to decide what part of the application code to offload, how to offload and where to offload. We surveyed the various application partitioning techniques, application deployment techniques. Also a comparative table of

these techniques shows the comparison between them on the basis of parameters like execution time, bandwidth, energy consumption, network latency and cost. Future work consists of developing frameworks for automatic partitioning and profiling. To develop software deployment frameworks that automatically deploys software components over distributed environment. Lightweight frameworks need to be developed for reducing communication overheads during computation offloading.

References

1. Fernando, N., Loke, S.W., Rahayu, W.: Mobile Computing: A survey. In: Future Generation Computer Systems 29 (2013), doi:[10.1016/j.future.2012.05.023](https://doi.org/10.1016/j.future.2012.05.023), pp. 84–106. Elsevier (2013).
2. Kosta, S., Aucinas, A., hui, P., Mortier, R., Zhang, X.: ThinkAir: Dynamic resource allocation and parallel execution in the cloud for mobile code offloading. In: IEEE INFOCOM, pp. 945–953. IEEE (2012).
3. Folino, G., Pisani, F.S.: Automatic offloading of mobile applications into the cloud by means of genetic programming. In: Applied Soft Computing 25 (2014), pp. 253–265. Elsevier (2014).
4. Magurwalage, C.M.S., Yang, K., Hu L., Zhang J.: Energy-efficient and network-aware offloading algorithm for mobile cloud computing. In: Journal of Computer Networks 74 (2014), Elsevier, pp. 22–33. Elsevier (2014).
5. Komnios, I., Tsapeli, F., Gorinsky, S.: Cost-Effective Multi-Mode Offloading with peer-assisted communications. In: Ad Hoc Networks 25 (2015), doi:[10.1016/j.adhoc.2014.07.028](https://doi.org/10.1016/j.adhoc.2014.07.028), pp. 370–382. Elsevier (2015).
6. Mukherjee, A., De, D.: Low power offloading strategy for femto-cloud mobile network. In: Engineering Science and Technology, an International Journal, doi:[10.1016/j.jestch.2015.08.001](https://doi.org/10.1016/j.jestch.2015.08.001), pp. 1–11. Elsevier (2015).
7. Rehman Khan, A.R., Othman, M., Khan, A.N., Abid, S.A, Madani, S.A.: MobiByte: An Application Development Model for Mobile Cloud Computing. In: J Grid Computing (2015) 13, pp. 605–628. Springer (2015).
8. Yang, L., Cao, J., Tang S., Li, T., Chan, A.T.S.: A Framework for Partitioning and Execution of Data Stream Applications in Mobile Cloud Computing. In: IEEE Fifth International Conference on Cloud Computing, pp. 794–802. IEEE (2012).
9. March, V., Gu, Y., Leonardi, E., Goh, G., Kirchberg, M., Lee, B.S: μ Cloud: Towards a New Paradigm of Rich Mobile Applications. In: 8th Conference on Mobile Web Information Systems (MobiWIS), pp. 618–624. ScienceDirect (2011).
10. Liu, J., Ahmed, E., Shiraz, M., Gani, A., Buyya, R., Qureshi, A.: Application partitioning algorithm in mobile cloud computing: Taxonomy, review and future direction. In: Journal of Network and Computer Applications 48 (2015), doi:[10.1016/j.jnca.2014.09.009](https://doi.org/10.1016/j.jnca.2014.09.009), pp. 99–117. Elsevier (2015).
11. Chun, B.G., Ihm, S., Maniatis, P., Naik, M., Patti, A.: Clonecloud: elastic execution between mobile device and cloud. In: 6th Conference on Computer Systems, EuroSys '11, pp. 301–314. ACM (2011).
12. AbdElminaam, D.S., Kader, H.M.A., Hadhoud, M.M., El-Sayed, S.M.: Elastic Framework for Augmenting the Performance of Mobile Applications using Cloud Computing. In: Proceedings of IEEE, pp. 134–141. IEEE (2013).
13. Verbelen, T., Stevens, T., Turk, F.D., Dhoedt, B.: Graph partitioning algorithms for optimizing software deployment in mobile cloud computing. In: Future Generation Computer Systems 29 (2013), doi:[10.1016/j.future.2012.07.003](https://doi.org/10.1016/j.future.2012.07.003), pp. 451–459. Elsevier (2013).

14. Shiraz, M., Gani, A., Shamim, A., Khan, S., Ahmad, R.W.: Energy Efficient Computational Offloading, Framework for Mobile Cloud Computing. In: J Grid Computing (2015) 13, doi:[10.1007/s10723-014-9323-6](https://doi.org/10.1007/s10723-014-9323-6), pp. 1–18. Springer (2015).
15. Lee, Y., Zomaya, A.: Energy conscious scheduling for distributed computing systems under different operating conditions. In: IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 8, pp. 1374–1381. IEEE (2011).

A Proposed Technique for Cloud Computing Security

Kanika Garg and Jaiteg Singh

Abstract This paper proposes a security technique called Encrypted Data Flow Mechanism (EDFM) based on the concept of Fog computing. EDFM primarily is proposed to secure cloud data storage from unauthorized/illegal access. The EDFM prototype was developed utilizing virtual machine(s), hosted hypervisor (VMware), Zentyal server and PHP. This simulated environment depends on a Fog Data Center called Broker, to hide actual cloud storage underneath it. To escalate cloud storage security, the simulated cloud communication paradigms make use of encrypted channels. This technique also tries to fool the intruder by providing fake document, in case he fails to prove his authenticity or he tries to access some document to which he is not entitled/permitted to access.

Keywords Blowfish · Encryption · Fog computing · Cloud computing

1 Introduction

Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and system software to run datacenters offering those services. Cloud platforms offer a variety of web services to its users. Cloud storage is suitable and accessible technology that gives access to our data anywhere on multiple devices. But if cloud computing has some advantages than it has some disadvantages too [1, 2]. As cloud is a composition of diversified domains like networking, varying platforms, integrated applications and storage etc. hence there is a high risk of events like information leakage, data theft and unauthorized access [3]. In this paper an attempt has been made to fortify the security of cloud storage. Most of the time data stored over a cloud based data center became vulnerable to

K. Garg (✉) · J. Singh
Chitkara University, Rajpura, Punjab, India
e-mail: gargkanika17@gmail.com

J. Singh
e-mail: jaiteg.singh@chitkara.edu.in

attacks, when transmitted/communicated over a network. These attacks can be classified based on domain of the attackers, or the techniques used in attacks. Thus, one of the biggest disadvantages is lack of security. Thus there is a need to secure data stored in cloud [4].

The successor of cloud computing is considered to be Fog Network. We assume fog networks as local network where all needful and common data is stored in servers of Fog network [5]. Fog services are able to increase the cloud's experience by placing the data close to the end user as per his requirements. Thus the data transmission time is reduced and speed of the overall system is increased. Another advantage of Fog network over cloud network is high level of secured data communication [6]. In this research one of the techniques called EDFM is implemented to secure cloud storage using the concept of fog computing.

Only end-to-end encryption can provide the security necessary to prevent any kind of attack. The selected cryptographic algorithm should take less processing time as it ensures speed [7]. In this research one of the symmetric key algorithms called Blowfish algorithm is used as its speed is fast and it takes less time to encrypt the data as compared to other symmetric key algorithms [8].

2 Implementation

The mechanism to implement manifold security for secure access to cloud data center using Fog Computing is shown in Fig. 1 and the name given to it is Encrypted Data Flow Mechanism (EDFM). So here is brief information about all units shown in Fig. 1 to enhance security:

2.1 Proxy Server

Proxy server used in Fig. 1 act as an intermediate between the client and the Cloud server to prevent from attacks and unexpected access to Cloud server. Proxy as per its functionality can be categorized as forward proxy and reverse proxy. In our EDFM mechanism, reverse proxy is used to secure cloud data.

2.2 Fog Server or Broker Server

The Broker Server(s) are intermediary independent unit(s) working between Proxy server and the Cloud Server. Role of these Broker units is to authenticate the identity of the client devices and the validity of requests. After authenticating the

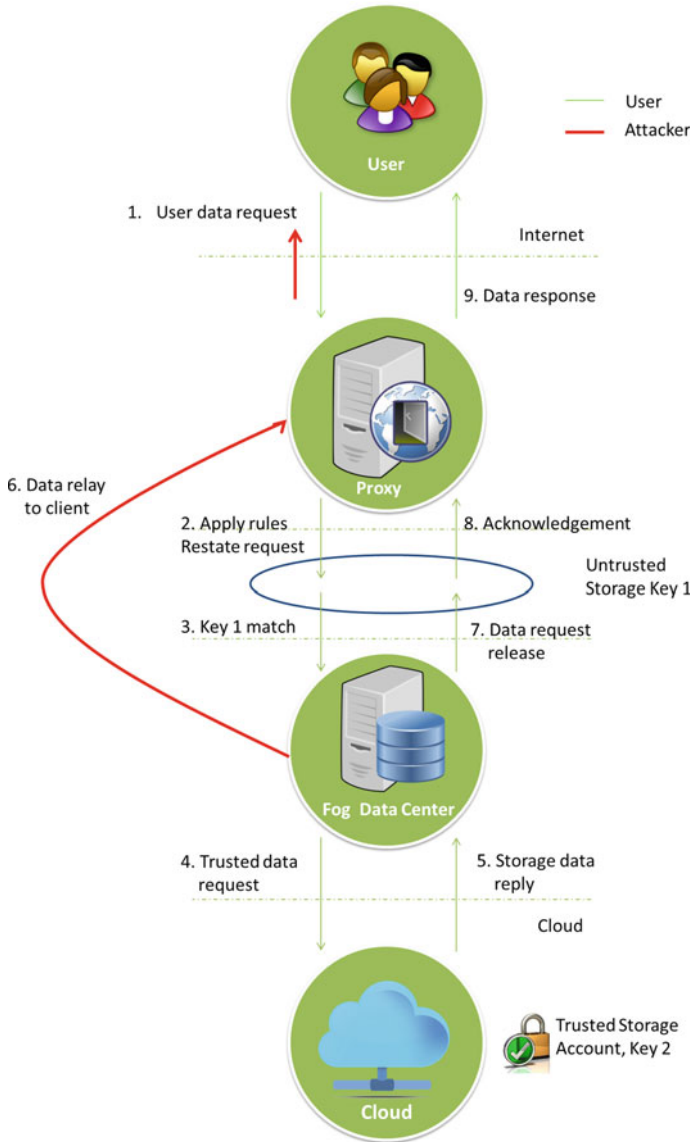


Fig. 1 Encrypted data flow mechanism (EDFM)

client device and request format, Broker will encrypt the request sent by the client and forward it to cloud data center. The requests is in encrypted form, hence it will be difficult for the attacker to decode those requests and to decode the identity of the clients as well [6].

2.3 *Cloud Data Center*

To avoid misuse of its resources Cloud will receive the requests in encrypted form. The request received will be decrypted using private key of broker as cloud will be having private keys of all the broker servers. Cloud server will verify the identity of Broker server. If it finds that the request is being forwarded by the valid Broker then only the request is processed.

2.4 *Devices as Authenticated Clients*

Client devices will be registered using the simple device authentication mechanism. This mechanism can be developed to uniquely identify these devices. It can be any network enabled device. These all devices are in fog network and are allocated a uniquely identified client ID. Request received by server using these client IDs will be processed. If request to the server comes from any other client without having client ID or invalid client ID, then the request will be rejected by the server. Once a client device is validated by the server only then it can avail the services of the cloud server.

2.5 *Users Authentication*

To enhance overall security of this system, users will be authenticated using username and password combination.

For doing server software implementation of this mechanism we have used PHP as a core programming language having MySQL connectivity to store log of requests. To display these request logs we have created user interface using HTML, JavaScript and cascading style sheets (CSS). We have also built a Hybrid Mobile Application called Cloud File Manager using ionic framework for clients.

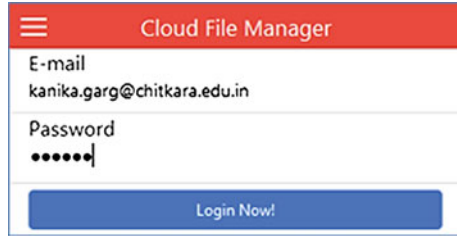
Mechanism: Firstly, this mechanism ensures that users and client devices should be registered with the system. We have developed Ionic Mobile Application hence users can register using their Android mobile, iPhone or any other mobile platforms supported by Ionic.

Internet connected devices in fog network are allocated a client ID, this way we got registered client devices.

The client device will request the server using its client id.

Till now client devices have been registered, now we have to authenticate users using our Mobile application called Cloud File Manager as shown in Fig. 2. Basic functionalities that a user can do using this application are uploading files, downloading files and listing files. Clients will send requests to the proxy as shown in Fig. 1 by considering it an actual server (cloud). Proxy will redirects requests to the

Fig. 2 Login screen of cloud file manager



Request History

Received	Forwarded
client_secret 8dfdc1ffafdc039b9fa7b3e25ce9be1d user_id 3 action download download_token +/X4TTwkLebM+fX7lwD809 KAcNUGGvm5cL5mvjxlShl= source 127.0.0.1	3s4Has/RQ5ACLYViXmd1KK/GzNhd7iISC03Lmb6bJikQ= 3s4Has/RQ5ACLYViXmd1KAtmywNy4Wo8NSxgDPC9I8: 3s4Has/RQ5ACLYViXmd1KFah2eJWWW6kDc3kf+oDfYY- 3s4Has/RQ5ACLYViXmd1KJcUQ17pksqqjYvsRMwfGtM= 3s4Has/RQ5ACLYViXmd1KMTRccwqNjft/KSm/bYdc/s= 3s4Has/RQ5ACLYViXmd1KCyWL3iNjse8XpefgH8F6ro= 3s4Has/RQ5ACLYViXmd1KN9caGSQT9odDmcP5KEv4D(3s4Has/RQ5ACLYViXmd1KNUkl mXlwLcy7D3wXIEidZjZ7P+P+dwN28LvswRio8rIVX2sjAm5C public_key 3s4Has/RQ5ACLYViXmd1KLZbXiwerfBx9cMRWJXu0cBg1

Fig. 3 Screenshot of request received and forwarded by broker server

fog data center. Proxy used in this research is Zentyal server. All internet connected devices in Fog network are managed by Fog Data center also known as Broker server as per its functionality. Broker server has all the information about client IDs which it will use for device verification purpose. So broker will verify clients using its client ID. Requests will be forwarded to the cloud server only if the client is verified. For going to proxy and proxy will further forward it to broker server. Now broker will verify client's ID and format of the request sent by client. After all authentications, request will be sent to the cloud server. This mechanism is done as follows:

Broker server will generate a public key by initializing its encryption algorithm using its private key. This public key will be sent along with the encrypted request to the cloud. The request history of broker server window is shown in Fig. 3. In this Fig. 3, it is visible that the request forwarded to the cloud server is encrypted.

After receiving request from broker server, Cloud server will take out public key of broker from request packet and will decrypt it. The request history of cloud server window is shown in Fig. 4; it shows that requests received by the cloud server are encrypted.

Request History

Received	Decrypted
<pre> 3s4Has/RQ5ACLYViXmd1KK/GzNhd7iSC03Lmb6bJikQ= 3s4Has/RQ5ACLYViXmd1KAtmywNy4Wo8NSxgfDPC9I8= 3s4Has/RQ5ACLYViXmd1KFah2eJWWW6kDc3kf+oDFYY= 3s4Has/RQ5ACLYViXmd1KJcUQ17pksqqlYvsRMwfGtM= 3s4Has/RQ5ACLYViXmd1KMTccwqNjft/KSm/bYdc/s= 3s4Has/RQ5ACLYViXmd1KCylWL3iNjse8XpefgH8F6ro= 3s4Has/RQ5ACLYViXmd1KN9caGSQT9odDmcP5KEv4D0= 3s4Has/RQ5ACLYViXmd1KNUkl mXlwLcy7D3wXIEidZJZ7P+P+dwN28Lv swRio8rfVX2sjAm50lmzRrjQbMAxlg== public_key 3s4Has/RQ5ACLYViXmd1KLZbXiwe fBx9cMRWJXu0cBg1tqImBP9tVsZpuRmSApI9 source 127.0.0.1 </pre>	<pre> user_id 3 action download source 127.0.0.1 download_token +X4TTwkLebM+fx7IwD809 KAcNUGGvm5cL5mvjxlShI= </pre>

Fig. 4 Screenshot of request received and decrypted by cloud server

Reponse to Client
<pre> status Success message Files retrieved! client_secret 3d379ea2f20df1983a1ff0daccdc64a16 actual_reponse {"GodplHQWr9twJE908KwwzSsUzqtypOiKs6fyrV3ajU=":"GodplHQWr9twJE908Kww5W1PC VrFeOompJU":"GodplHQWr9twJE908Kww3OzNYclivfMfam1S57v4dJ4sox7OLSXvJCfpgwXyek Vy+jbRwPIEywV6du6+CNITPuzNbrAaTPoLJQ5yCpRhAjoHSi+INT2jCaJHsnEPToD7Vn1TT3b cloud_reponse {"status":"success","message":"Files r retrieved","broker_secret_hash":"8dfdc1fffa7c039b9fa7b3 </pre>

Fig. 5 Screenshot of response sent back to client by cloud server

After decrypting the request packet cloud server will check source of request, by verifying broker’s identity as cloud server has information about authentic brokers. In request packet cloud will also get a public key which can be decrypted by same private key from which it was generated. Once the cloud server will know the private key from which decryption has done, a reply will be sent to the broker server after encrypting it with the same private key. Response sent by the cloud server to the broker server is also encrypted thus providing security to the data in transit.

The Fig. 5 shows the response sent by cloud server back to the client via broker and proxy server.

Thus by this EDFM mechanism, secure communication is established between client and the cloud server, making it difficult for the attacker to access the sensitive data stored on cloud. Also, as shown in Fig. 1, Fog data center is relaying the data to the client back (shown in red). This is the case when one user wants to access the data of another user. Then if that user has access rights to access that data item, then permission is granted to download or access that data item. But if the data item is view only and still some other user tries to access or download it, then fake document will be provided to that user.

3 Conclusion

In this research, a security mechanism is thus developed to secure the cloud data center using the concept of Fog computing. All the devices in Fog network are connected to secured data center called broker, from which reply is received/sent from the cloud server in an encrypted way which is further forwarded to the client device thereby increasing security.

References

1. Suo H, Liu Z, Wan J, Zhou K.: Security and privacy in mobile cloud computing. In: 9th International Wireless Communications and Mobile Computing Conference (IWCMC), IEEE, Jul 1, pp. 655–659, (2013).
2. Pearson S, Benameur A.: Privacy, security and trust issues arising from cloud computing. In Cloud Computing Technology and Science (CloudCom), IEEE Second International Conference on Nov 30, pp. 693–702 (2010).
3. Singh, Jatinder, et al.: Twenty security considerations for cloud-supported Internet of Things. (2015).
4. Puthal D, Sahoo BP, Mishra S, Swain S.: Cloud computing features, issues, and challenges: a big picture. In Computational Intelligence and Networks (CINE), IEEE International Conference on Jan 12, pp. 116–123 (2015).
5. R. Raut, M. Waje, S. Kulkarni and A. Gupta: Security for Cloud using Fog Computing. IJRIT International Journal of Research in Information Technology, Volume 2, pp: 98–101, (2014).
6. Aazam M, Huh EN. Fog computing and smart gateway based communication for cloud of things. In Future Internet of Things and Cloud (FiCloud), International Conference IEEE on Aug 27, pp. 464–470 (2014).
7. Devi TR.: Importance of Cryptography in Network Security. In Communication Systems and Network Technologies (CSNT), IEEE International Conference on Apr 6, pp. 462–467 (2013).
8. Alabaichi A, Ahmad F, Mahmood R.: Security analysis of blowfish algorithm. In Informatics and Applications (ICIA), Second International Conference on Sep 23, IEEE, 12–18 (2013).

Optimizing Job Scheduling in Federated Grid System

Akshima Aggarwal and Amit Chhabra

Abstract Parallel computing is a type of computation in which jobs are executed by the parallel servers. Jobs are further distributed into number of tasks by checking the availability of server. Federated Grid System is a system consists of number of heterogenous clusters which are associated with number of servers. Comparison with existing work on the basis of parameters such as makspan, flow time and energy. The time taken by a single job to accomplish its task is flow time and the time taken by all the jobs to accomplish its task is the makespan of that jobs. DVFS levels are considered in a system to reduce the power consumption during the execution of parallel jobs. In our proposed system we have used DVFS based genetic algorithm so that the job acquired by parallel processors provide optimal results.

Keywords Parallel computing · Makespan · Flow time · Federated grid structure

1 Introduction

Parallel computing is operating on the principle that large problems can often be divided into smaller ones, which are then solved at the same time. In this type of computation many jobs are performed simultaneously on different servers. There are several types of parallel computing: bit-level, instruction-level, data, and task parallelism. To get high performance computation parallelism is utilized from many years. In our proposed system by using parallel computing we can achieve optimal result in short span of time. It is closely related to concurrent computing—they are frequently used together, and often conflated, though the two are distinct: Paral-

A. Aggarwal (✉) · A. Chhabra
Department of Computer Engineering, Guru Nanak Dev University, Amritsar, India
e-mail: akshimaaggarwal2009@gmail.com

A. Chhabra
e-mail: amit.cse@gndu.ac.in

lelism without concurrency (such as bit-level parallelism), and concurrency without parallelism (such as multitasking by time-sharing on a single-core CPU) is also possible. A task is typically broken down in several, very similar subtasks that can be processed independently and whose results are combined afterwards, upon completion in parallel computing. The tasks in parallel computing can be classified according to the level at which the hardware supports parallelism, with multi-core and multi-processor computers having multiple processing elements within a single machine, while clusters, MPPs, and grids use multiple computers to work on the same task.

Parallel programming models [1] and tools are suitable for high-performance computing. So we will use shared and distributed memory approaches, as well as the current heterogeneous parallel programming model. The availability of multi-core CPUs has given new impulse to the shared memory parallel programming approach. In addition, the hybrid parallel programming is the current way of harnessing the capabilities of computer clusters with multi-core nodes.

Parallel job scheduling [2] is to run the tasks on parallel basis on different machines. For this purpose to share the resources of the parallel machine among a number of competing jobs, provides the required level of service to each machine.

The federated grid system [3] follows a technique which attains the best possible makespan. This strategy is based on anticipating the specifications of all resources in a system and approaches towards non-coordinated workflow scheduling.

Performance of Federated Grid system [4] which saves time and utilizing communication bandwidth to reduce the number of job migrations. It is a self adjusting resource sharing policy which maintains the systems complete autonomy and improves its resource performance.

Parallel Jobs [5] schedule the tasks according to the requirement. The online jobs can be required by number of peoples to perform their tasks simultaneously. There should be requirement of a machine or group of machines to perform those tasks simultaneously, which give high performance to user. Federated Grid structure is a collection of different servers to reach a common goal. It is distributed system that involves a large number of files with non-interactive workloads. A cluster computing in that grid computers have each node set to perform a different task/application. Grid computers also tend to be more heterogeneous and geographically dispersed than cluster computers. For computationally intensive tasks, clusters of computers have emerged as cost-effective parallel or distributed computing systems. These clusters which are composed of high performance computational nodes linked together by low-latency/high-bandwidth interconnection networks are utilized in federated grid. These clusters can be federated to yield systems considered tightly-coupled. A genetic algorithm is the method using which the jobs which are running on parallel computers can help in achieving optimal results. A fitness function will be used to achieve those goals. Fitness function is combination of make span and flow time. A genetic algorithm (GA) is method for solving optimization problems based on a natural selection process that provides better results.

The basic concepts of Genetic Algorithms [6] is developed for finding the minimum make span of the n number of jobs, m number of machine permutation flow shop sequencing problem [7]. Genetic algorithm applied to scheduling in multi-cluster environments to perform the jobs in short span of time. This algorithm helps the clusters of federated grid structure to achieve optimal results [8]. This paper provides an efficient and reliable evolutionary programming algorithm for solving the optimal power flow (OPF) problem. The class of curves used to describe generator performance does not limit the algorithm.

In it different phases of migration [9] are described and it relates energy cost with power consumption. They observe that power consumption increase as there is increment in utilized bandwidth and as increase in VM size the migration time will also increase. It is critical for a power system to [10] estimate its operation state based on meter measurements in the field and the configuration of power grid networks.

In federated Data Grids, [11] individual institutions share their data sets within a community to enable collaborative data analysis. Data access needs to be provided in a scalable fashion since in most e-science communities; data sets do not only grow exponentially but also experience an increasing popularity.

2 Proposed Work

In our proposed algorithm by using genetic algorithm the jobs will be allocated to different clusters of Federated grid structure. This allocation of job is based on the criteria of fitness function. The server which is free or have less load of work will take that job and execute it. Firstly the job is distributed according to the availability of clusters in federated grid structure. Each federated grid structure is group of heterogenous clusters. These clusters perform set of similar tasks. Genetic algorithm helps the jobs to choose the server which is free to serve him. By using the fitness function the server will produce the optimal results.

The proposed system is divided into the parts. We first describe various job allocation strategies within the proposed system. Second we will describe the genetic algorithm used to select optimal result and finally we use result section to describe the result produced through the proposed system.

In the job allocation strategy we will choose the jobs from different set of pools. The pools like

$$\begin{aligned} J_1 &= \{J1, J2, J3 \dots Jn\} \\ J_2 &= \{J1, J3, J5 \dots Jn\} \\ &\vdots \\ J_n &= \{J2, J4, J6 \dots Jn\} \end{aligned}$$

Now we will select the jobs from these pools randomly on the very first time with the help of Genetic Algorithm. Now put that job to pool where selected jobs of all the pools will be served for processing.

$$C = \{J_1, J_2, J_3, J_4 \dots J_n\}$$

By using genetic algorithm these jobs will be selected from the pool C and allocated on the basis of load of server. The server with fewer loads will get that job and perform it. The fitness function i.e. makespan, flow time are considered to get optimal results.

Genetic Algorithm is building block used for a number of different application areas. An example of this would be multidimensional optimization problems in which the character string of the chromosome can be used to encode the values for the different parameters being optimized. The genetic algorithm will be used in this paper to select the optimal values out of legion of values. The genetic algorithm continues until the desired goal is met or after the completion of number of iterations. The pseudocode used in the proposed GA based Energy Efficient algorithm is elaborated as follows.

Step 1: Create structure including Grid and Power

Step 2: Set the machines to operate at highest values of voltage and frequency

Step 3: Select the jobs and partition the jobs into tasks with predefined burst time

Step 4: Perform allocation
Case1: Intra-Grid

$$Exe_T = Burst_{Time} / Power_{of_grid} \quad \text{Eq. 1}$$

Case2: Inter-Grid

$$Exe_T = Burst_{Time} / Power_{of_Sl_grid} \quad \text{Eq. 2}$$

Step 5: $Power = ac * v^2 * F$ where ac is constant having value 1. V and F are voltage and frequency

Step 6:

$$Energy = Power * \sum Exe_T + \sum Idle_t \quad \text{Eq. 3}$$

Calculating Energy consumed by each job

Step 7: Defining Fitness Function

$$Fitness = \alpha * Makespan + (1 - \alpha) * Flowtime \quad \text{Eq. 4}$$

Where α is constant having value 0.5

Step 8: Perform Selection through Random Sampling

Jobs = Random(Jobs)

Step 9: Apply crossover

Case 1 Uniform crossover

Case 2 Arithmetic crossover

Step 10: Perform mutation

Case 1 Bit Inversion without power alteration

Case 2 Bit Inversion with power alteration

The considered steps used to determine the optimal allocation policy in case of federated grid. The steps considered in the pseudocode involve creating structure for the system considering Grids including the varying levels of power consumption.

The machine is set to operate at high values of DVFS level. When decided jobs are allocated then analysis is made whether the task is allocated to intra-grid or inter-grid. The execution time calculations have distinct formulas for the same. The time consumption is calculated as

Intra-Grid Allocation

$$Exe_T = Burst_{Time} / Power_of_grid \quad (1)$$

Inter-Grid Allocation

$$Exe_T = Burst_{Time} / Power_of_SL_grid \quad (2)$$

The power consumption is calculated after the execution time is determined. The formula used for this purpose is

$$Power = ac * v^2 * F \quad (3)$$

The power consumption has to be minimized in the proposed technique. Once calculated, further calculation about the energy consumption will be made. The energy calculation will also involve energy of the idle machine. The formula to accomplish this is given in terms of methodology as

$$Energy = Power * \sum Exe_T + \sum Idle_t \quad (4)$$

The fitness function is then evaluated to determine the minimum possible cost encounter. The fitness function is given as

$$Fitness = \alpha * Makespan + (1 - \alpha) * Flowtime \quad (5)$$

The value of α is lies between 0 and 1. For our convenience α is taken to be 0.3. The selection operation is performed to select the jobs randomly for first time processing.

Jobs = Random(Jobs)

The mutation and crossover will be performed after the selection. Different possible combination of mutation and crossover is possible. In our case we utilized

Uniform crossover

Arithmetic crossover

The mutation which is considered in distinct case is Bit inversion with and without power alteration (Tables 1, 2 and Figs. 1, 2).

Table 1 Chromosome structure for case 1

Grids	Computation power	Number of machines
1	2	5
2	3	5
3	4	5

Table 2 Chromosome structure for case 2

Grids	Computation power	Number of machines	DVFS-level
1	2	5	4
2	3	5	4
3	4	5	4

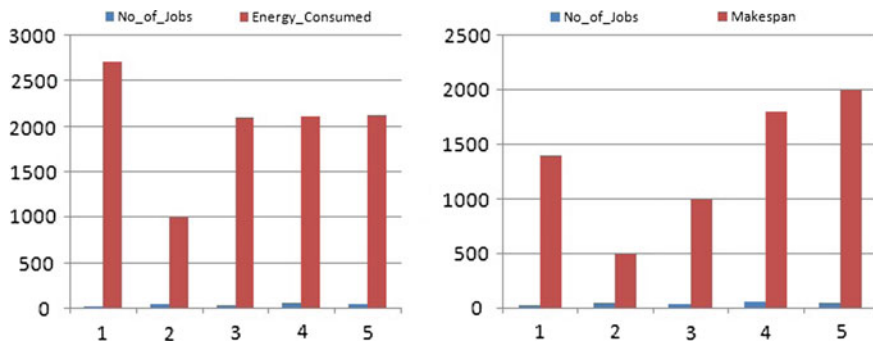


Fig. 1 Results of energy consumption and makespan without DVFS capability

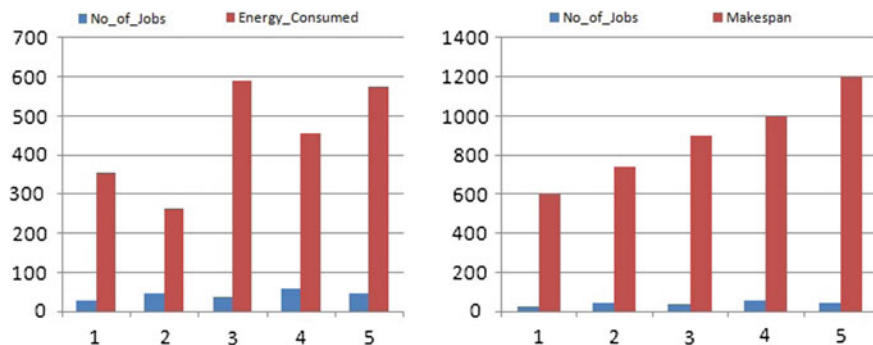


Fig. 2 Results of energy consumption and makespan with DVFS capability

3 Results

Comparison takes place by taking same number of jobs and iterations, varying DVFS levels through mutation. In the first case we have taken the values of Energy Consumption and Makespan by taking high value of DVFS level. In the Second case we have taken the values by varying the DVFS levels to attain optimal results of Energy Consumption and Makespan.

4 Conclusion and Future Directions

In the proposed system we achieve optimal results of different jobs which are performed by different servers in federated grid system. The fitness function of genetic algorithm helps us to reach this goal. Comparison with the existing work on the basis of Energy consumption and makespan, achieved to get optimal results for Energy consumption but the makespan of the jobs get slightly increased due to the time required in changing the DVFS values but due to introduction of DVFS level, power consumption reduces and then energy consumption values reduces. As according to the comparison from the existing work energy is reduced by 40%. Communication time is not considered in this case. As we only consider the optimality in our proposed system, in future we will also consider the distance of jobs from current machine to server allocated.

References

1. Diaz J, Munoz-Caro C, Nino A.: A Survey of Parallel Programming Models and Tools in the Multi and Many-Core Era. *IEEE Trans Parallel Distrib Syst* [Internet]. 2012 Aug [cited 2016 Mar 25]; 23(8):1369–86. In: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6122018>.
2. Dror G, Feitelson LR, Feitelson DG, Rudolph L.: Parallel Job Scheduling: Issues and Approaches. *Jsspp* [Internet]. 1995; 949:1–18. In: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.47.545>.
3. Katia Leal.: Self-adjusting resource sharing policies in Federated Grids. *Future Generation Computer Systems*, vol. 29, pp. 488–496, 2013.
4. Katia Leal.: Anticipating resource saturation in Federated Grids. *Future Generation Computer Systems*, vol. 45, pp. 114–122, 2015.
5. Sgall J.: On-line scheduling of parallel jobs. *Proc 19th Symp Math Found Comput Sci*. 1994; 841:159–76.
6. Reeves CR.: A genetic algorithm for flowshop sequencing. *Comput Oper Res* [Internet]. 1995 Jan [cited 2016 Apr 27]; 22(1):5–13. In: <http://www.sciencedirect.com/science/article/pii/0305054893E0014K>.
7. Gabaldon E, Lerida JL, Guirado F, Planes J.: Multi-criteria genetic algorithm applied to scheduling in multi-cluster environments. *J Simul* [Internet]. Nature Publishing Group; 2015; 9(4):287–95. In: <http://www.palgrave-journals.com/doi/10.1057/jos.2014.41>.

8. Yuryevich J.: Evolutionary programming based optimal power flow algorithm. IEEE Trans Power Syst [Internet]. IEEE; 1999 [cited 2016 May 3]; 14(4):1245–50. Available from: <http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=801880>.
9. Strunk, A. and W. Dargie.: Does Live Migration of Virtual Machines Cost Energy? pp. 514–21 in 2013 IEEE 27th International Conference on Advanced Information Networking and Applications (AINA). In: <http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6531798>.
10. Q. Yang et al.: On False Data-Injection Attacks against Power System State Estimation: Modeling and Countermeasures. IEEE Transactions on Parallel and Distributed Systems 25 (3):717–29. In: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6490324>. 2014.
11. Scholl, Tobias, Richard Kuntschke, Angelika Reiser, and Alfons Kemper.: Community Training: Partitioning Schemes in Good Shape for Federated Data Grids. Pp. 195–203 in Third IEEE International Conference on e-Science and Grid Computing (e-Science 2007). In: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4426888>.

A SDE—The Future of Cloud

N. Leelavathy, D.S.M. Rishitha and M. Sushmitha

Abstract The probe of Internet has made the digital civilization possible, where everything is interconnected and can be accessed from everywhere. However, the complexity of traditional IP networks is high which makes its management difficult in spite of their widespread acceptance. It is both difficult for network configuration as per the present policies, and reconfiguring it whenever required for faults, load and changes made dynamically. The present technology uses the data and control planes together in routers. Software-Defined Environment (SDE) is an emerging prototype that uses vertical integration, i.e., separating the network's intelligence from the physical devices like hardware switches or routers, endorsing logical centralization of controlling the network. It introduces the ability to adapt, program the network which can optimize the entire computing infrastructure namely, compute—storage—network resources, so that it can adapt to the type of application or protocol required. The separation of control and data planes in its implementation of switching hardware, and the forwarding of traffic between different networks with different defined policies, is the key to the desired flexibility. Hence, SDN makes it easier to create by simplifying the network control problem into manageable pieces which is a present business demand with more agility and flexibility through virtualization. Understanding SDN paradigms are the key for enterprises trying to properly position cloud services. SDN is appropriately accepted as more efficient “Cloud Networking,” i.e., the revolutionary growth in network usage and its services support the cloud computing on a large scale. This paper discusses various tasks and technology models of SDNs which are typically needed for proper utilization of cloud services and appreciate its advantages.

N. Leelavathy (✉) · D.S.M. Rishitha · M. Sushmitha
Department of Computer Science & Engineering, Pragati Engineering College,
Surampalem, Andhra Pradesh, India
e-mail: drnleelavathy@gmail.com

D.S.M. Rishitha
e-mail: malikarishi@gmail.com

M. Sushmitha
e-mail: maddiralasushmitha@gmail.com

Keywords Software-defined environment • Control plane • Data plane • Cloud computing

1 Introduction

In the present technology of computing, the products provided by vendors such as DEC and IBM are completely integrated, with a trademarked hardware and operating system and/or with some application software. Hence, customers tend to be locked by one vendor, use only those applications which are offered by that particular vendor. It makes migration from one vendor’s hardware platform to another platform difficult, rather it may be impossible. It is very important to develop applications that are compatible to run on different platforms. Moreover, the traditional network architectures cannot meet the demands of high volume and various variety of traffics.

The idea behind the concept of SDN is to separate the switching function between data plane and control plane on separate hardware devices as described in Fig. 1. One device simply performs switching function and the other has “intelligence” to provide best routes to destination keeping the QoS and QoE requirements of dynamic environments.

OpenFlow or other open APIs are used in SDN to control the data in the switches of the data plane. The routing decisions are taken at a logically placed

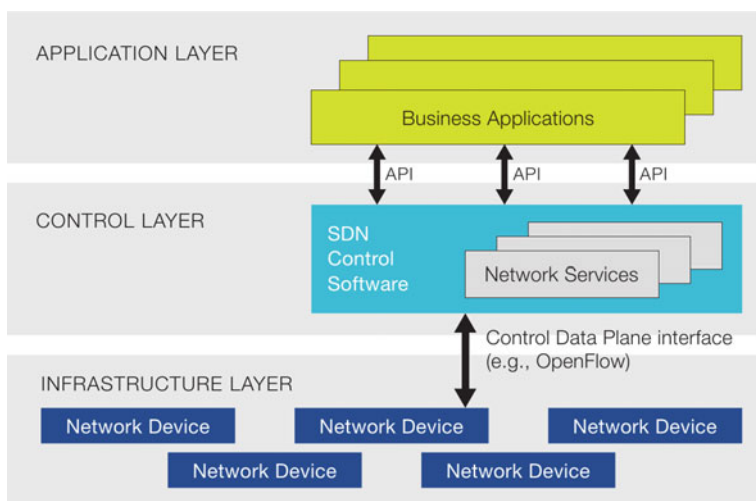


Fig. 1 Architecture of SDN

centralized device called controller whereas the forwarding of packets is done by a physical device called a switch or hub. Moreover, the controllers take the information about dynamic demands and capacity variations obtained from the networking equipment through which the traffic is flowing. SDN applications are nothing but simple software programs that uses an abstract view of the network for making their decisions. The SDN controllers are designed as per the applications that convey their network requirements.

The characteristics of Software-Defined Networking is as follows:

- SDN separates the data plane from its control plane. Then the data plane devices become simple hardware devices that does packet-forwarding.
- The control plane is realized in a set of centralized controllers or a single centralized controller. It has a centralized understanding of the networks under its control.
- A portable software can be used in the controller that can run on readily available product servers. It is also capable of programming the forwarding devices, may be switches based on the overall view of the network.
- Open interfaces are defined between the controllers and the devices in the data plane.
- The applications running on top of the SDN controllers can program the network topology.
- The SDN controllers have an abstract view of network resources which are presented to the required applications.

Hence, the benefits of SDN are that it is directly Programmable with centralized management. It delivers agility and flexibility so that SDN enables organizations to create new types of services, applications, and business models that can offer more revenue streams from the network.

SDN with cloud would give better applications [1]. Cloud computing is to use data centre software and servers in networks to dynamically allocate resources and run applications for remote end users. Cloud computing is for infrastructure and computing services that have traditionally been deployed on premise that are now offered as a service on typically large scale shared infrastructure. Cloud is typically divided into three categories—public, private, and hybrid. Cloud deployments have higher flexibility and cost savings over traditional private data centres.

Virtualization is crucial for cloud computing. By allowing physical servers to run one or more virtual machines on demand, cloud architectures offer rapid scaling and efficient allocation of server resources dynamically. SDN aims to customize this by making the underlying physical layer with a generic switch and all other applications like firewalls, routing, load balancing, etc. be implemented in software on top of these generic hardware.

2 Models of SDN

Techniques used for computing has taken a significant revolution when compared to the earlier decade. The virtualized cloud data centers are replacing the dedicated static servers, which offers better flexibility with lower costs. The design of automated computing resources in cloud data centers are instantiated and work at a faster rate may be, in a matter of minutes. Typically, the network management is performed manually by a human often is much slower. The dynamic behavior of network has wide impact, and its changes are complex to predict.

There are three models of SDN described below which explains the basic mechanisms, benefits goals, and shortcomings of each.

2.1 *The Network Virtualization Model*

One of the simple models of SDN that the market considers is the network virtualization model. Virtualization is nothing but an accurate and faithful reproduction of the physical network that is fully isolated. It provides both location and physical network state independence. Moreover, a virtualized network is one which can be reconfigured by instantiating, operating and removing without physical asset interaction by the network manager.

Virtualization is changing the rules of networking. The initial goals of the network virtualization are to decouple the underlying hardware of local area network (LAN). Network Virtualization solves a lot of the networking challenges, provision of the network on-demand, without having to physically touch of the underlying infrastructure. To achieve this, the network virtualization platforms starts a software element—generally the hypervisor. Therefore, thousands of virtual networks can be created in this way without affecting the network operations.

The greatest advantage of network virtualization is defeating vendor-locking and supporting multi-tenant clouds without making any changes to the network itself. And therefore, it becomes simpler to combine network provisioning with cloud services.

The drawback is that the virtual networks appear as traffic to the network devices above network layer. These devices can't prioritize individual virtual networks unless deep packet inspection is used to recognize the virtual network header. At last, as the software is part of the cloud server stack it establishes the virtual networks and these can only be linked with the virtual machines not the devices.

Mobility, Big data and the necessity for agility are the trends motivating the business entrepreneurs to adopt virtualized, cloud-based IT infrastructures. Anytime, anywhere access of services is placing implausible demands on the network. To maintain good profits with high productivity in this competition, business need efficient, cost-effective ways to deliver simple and easy accessible applications to

users. Virtualization technologies along with cloud architectures is directly addressing those requirements, making them significant to the modern data center.

2.2 The ‘Evolutionary’ Approach

Another model of SDN is the “Evolutionary” model. The goal of this model is to design the software control plane of the network along with its operations using the current networking technologies available. To obtain this, the networking users have to support the specific standards like GRE, VXLAN, BGP and MPLS. With the help of this standards the network is developed to maintain low traffic with good quality of services. It gives opportunity to the vendors to merge their solutions into a set of interfaces available through cloud.

Network devices utilize this SDN model, for making it fully integrated with network operations. Traditional traffic engineering policies can be exerted, and the virtual networks can hypothetically extend from server to client when the devices can support the required standards.

Centralization in SDN means that the controller must fully control all network devices within the strategy domain. The network devices must offer APIs may be implemented through cloud, for the controller to develop the topology, and also implement the monitoring and control of network resources across various multiple devices.

Most of the SDN vendors are implementing all the network standards described above. The major problem is that the evolutionary model when used may not fully support the standards specified by other vendors. This model also requires integration among the management systems, cloud virtual networking, and sometimes the human operator has to manage the task manually.

2.3 The OpenFlow Model

The final and most widely used model is the OpenFlow model which is most popular and related to SDN. OpenFlow protocol is a standardized protocol for interacting with the forwarding behavior of switches from multiple vendors. This provides us a way to control the behavior of switches throughout our network dynamically and programmatically. OpenFlow substitutes the conventional, discovery-based forwarding table updates in switches and routers with programs written in devices providing centrally controlled forwarding tables. The controller takes complete control over the network the way it is segmented or virtualized, to manage traffic efficiently. Any combination of switches and controllers that support OpenFlow can be used in this model of SDN.

OpenFlow is implemented over TCP/IP model, which enables the use of any network topology between the controller and the network device. It also provides

the ability for the controller to send and as well as receive packets on each switch port, this may be used to do topology discovery and emulate existing protocols. The newer versions of this OpenFlow model may also include enhanced improvements to meet the needs and demands that can truly satisfy the customer [2].

3 Future Scope of SDN

3.1 Fault Tolerance

In SDN, the controllers that are logically centralized manages the topological services, inventory services, statistical services, host tracking services, etc. Regardless of the use of logically centralized control concept, a single controller results in a single point failure. This leads to fatal service disruptions only at that network. An alternative solution for this is to model each controller as a replicated state machine and instead consistently replicate the set of inputs to each controller. But this is only solving a part of the problem and so we make sure that at the time of controller failures, we have the state of the switch which is being consistent, also the interactions between the switches and controllers is complex and hence the existing systems do not use this and hence forth, we use “Ravana” a SDN controller platform [3], that offers a fault free centralized controller in which we handle the entire event processing life-cycle. Here the event processing on controllers and command execution takes place as a transaction where in the total process is to be either executed or left unprocessed. This leads to a one-time execution of the entire system so that there are no repetition or execution of commands.

3.2 Congestion Control

TCP is designed to operate on a many to one communication pattern where data is sent to receiver from multiple senders simultaneously. This many to one communication pattern appears in the case of data center networks which store the data at multiple servers. With SDN the centralized control methods and global view of the network can be handled in an effective way with this congestion control mechanisms [4]. TCP enables the controller to select a long lived flow by adjusting the TCP window size to reduce the sending rate of data packets which in turn reduces the flow and hence forth preventing the data from being overlapped or mislead. In this paper, the congestion control mechanisms is implemented with SDTCP and Open TCP as a TCP adaptation framework in SDNs. The benefit of SDTCP is that it can accurately decelerate the flow of packets to ensure the improvement in the performance.

Open TCP is presented as a system for dynamic adaptation of TCP based on network and traffic conditions in Software defined networks. It mainly focuses on the internal traffic in the SDN based datacentres. We use this technique to simplify the adaptation process towards network and traffic conditions. Open TCP based on link utilization leads up to 59% reduction in flow completion time. Congestion control leads to zero packet loss and high performance.

3.3 *Quality of Service (QoS)*

In SDN, a logically centralized software program is used to control the behaviour of entire network. This is done by decoupling the routing decision tier from the forwarding layer [5].

The OpenFlow protocol is used for the communication between the control and data plane. But the main problem in network is the lack of efficient management of resources to provide good Quality of Service (QoS). This usually happens in a network where there is a delay and packet loss. Hence to eradicate this we came up with the solution called the ICP (Inter Linear Program) where the shortest path is chosen. This decision taken also considers both network requirement and service requirement in terms of packet loss and delay. Moreover, the QoS architecture gives the possibility to map the optimal solution, we also use multiple path topology composed of wired or wireless network.

4 Conclusions

Traditional networks are complex and tedious to manage due to vertically integrated control and data planes. Also, networking devices are strictly tied to the products and versions. Hence, came up the Software Defined Networks which can solve long standing problems. The major aspects of SDN are dynamic programmability of forwarding devices which increases flexibility and decoupling of data and control plane and viewing the network as a single logically centralized network. Applications that run above the controller are easily deployed and developed as compared to that of the traditional networks. SDN introduces a new pace of innovation in the networking infrastructure [6].

We started with comparing the traditional networks with the upcoming paradigm which has overcome the drawbacks of the age old networks. The paper also includes the use of cloud with SDN which provides us with improvised results. This paper provides an overview on SDN with cloud computing and network virtualization for an absolute working of the SDN we have also discussed the facets: fault tolerance, congestion control and quality of service (QoS). Finally, SDN has successfully gave rise to the next generation networking and promoting advances in

several areas such as evolution of scalability and performance of devices and architectures, promotion of security and dependability, emerging topics that further require research are realization of network as a service cloud computing paradigms.

References

1. Kreutz, Diego, Fernando Ramos, Paulo Verissimo, Christian Esteve Rothenberg, Siamak Azodolmolky, and Steve Uhlig. "Software-defined networking: A comprehensive survey." arXiv preprint [arXiv:1406.0440](https://arxiv.org/abs/1406.0440) (2014).
2. Tourrilhes, Jean, Puneet Sharma, Sujata Banerjee, and Justin Pettit. "The Evolution of SDN and OpenFlow: A Standards Perspective." *IEEE Computer Society* 47, no. 11 (2014): 22–29.
3. Katta, Naga, Haoyu Zhang, Michael Freedman, and Jennifer Rexford. "Ravana: Controller fault-tolerance in software-defined networking." In *Proceedings of the 1st ACM SIGCOMM Symposium on Software Defined Networking Research*, p. 4. ACM, 2015.
4. Ghobadi, Monia, Soheil Hassas Yeganeh, and Yashar Ganjali. "Rethinking end-to-end congestion control in software-defined networks." In *Proceedings of the 11th ACM Workshop on Hot Topics in Networks*, pp. 61–66. ACM, 2012.
5. Ongaro, Francesco, Eduardo Cerqueira, Luca Foschini, Antonio Corradi, and Mario Gerla. "Enhancing the quality level support for real-time multimedia applications in software-defined networks." In *Computing, Networking and Communications (ICNC), 2015 International Conference on*, pp. 505–509. IEEE, 2015.
6. Medved, Jan, Robert Varga, Anton Tkacik, and Ken Gray. "Opendaylight: Towards a model-driven SDN controller architecture." In *2014 IEEE 15th International Symposium on*, pp. 1–6. IEEE, 2014.

Cloud Security-Random Attribute Based Encryption

V. Havisha, P.V. Padmavathi and S.V. Ramanamurthy

Abstract Cloud computing, to reduce the capital and operational costs, shares computing resources rather than establishing local servers to handle applications. But Cloud computing could not take off because of security issues. Major challenges in building a secure and trustworthy cloud system are: Outsourcing (don't know where your servers are, how many copies of your data are kept and who all have access to your data physically and programmatically), Multi-tenancy (What type of programs are running along with your program on the same virtual machine), and massive shared physical and logical storage, computing power and bandwidth over internet. The traditional security mechanisms like PKI, RSA, DES etc. are not suitable for Cloud data as the keys can be deciphered (The minimum key length has increased from 32 bits to 512 bits today). This paper proposes a novel encryption technique where the key for each segment (row or tuple) of data is changed to a part (attribute value) of the data itself. This mechanism makes sure that no person can decrypt the data without having access to the Key Attribute Table, which is stored on a local server or in a different cloud.

Keywords Cloud PKI • RSA • DES • Encryption • Security

V. Havisha (✉) • P.V. Padmavathi • S.V. Ramanamurthy
Department of Computer Science & Engineering, Pragati Engineering College,
Surampalem, Kakinada, Andhra Pradesh, India
e-mail: havisha96vedula@gmail.com

P.V. Padmavathi
e-mail: paddu1996.p@gmail.com

S.V. Ramanamurthy
e-mail: saripalli@ieee.org

1 Introduction

Cloud computing relies on sharing computing resources through internet. Cloud Service Providers (CSPs) (e.g. Microsoft, Google, Amazon, etc.) have commercialized cloud computing by leveraging virtualization technologies and self-service capabilities for providing computing resources (CPU, Memory, Network bandwidth, external storage) via the Internet. Virtual machines of several clients are co-located on the same physical server, leading to specific security issues like, virus threats, side channel attacks etc. CSPs must ensure that their customers' applications and data are secure to retain their customer base and competitiveness. Enterprises want to reduce their local infrastructure and go on to cloud, but are afraid of the security of their applications and data [1].

2 Cloud Security

Security has become the most significant barrier of the development and widespread use of cloud computing. The major tasks involved in Cloud Security are (Fig. 1):

- **Governance:** The data security desecrations mostly initiate within the organization itself. An organization's board is responsible (regulators, customers and liable to shareholders) for the framework of standards, processes and activities that together ensure the security of data in cloud. To maintain and execute the Cloud governance framework, in-house procedures, access matrices, the security mechanisms must be developed.
- **Compliance:** In order to protect the intellectual properties and corporate assets of their own companies, most organizations have established security and compliance policies and procedures, especially in the IT space. But in practice these principles and procedures are not considered due to issues like: lack of time, training and oversight. There should be a proper observation of these procedures (vigilance cell) or a mechanism to report non-compliance.
- **Data security:** Associated with Cloud data services, there are numerous concerns, traditional security concerns, e.g., network eavesdropping, data access

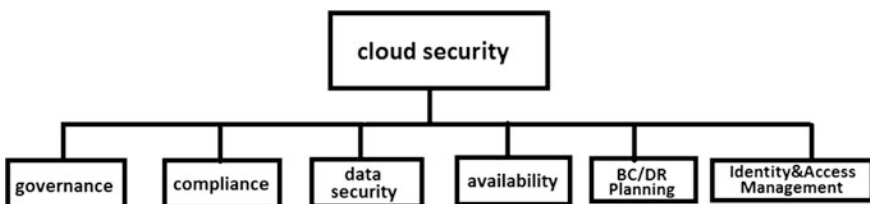


Fig. 1 Major tasks in cloud security

controllability, denial of service attacks and illegal invasion, and specific cloud computing concerns like side channel attacks, virtualization vulnerabilities, and abuse of cloud services. Certain security requirements are to be met in a cloud data service to avoid the concerns: Data Confidentiality, Data Integrity and Data Access Controllability. Cloud Data centers can be checked by a third party and certify to induce confidence in the cloud customers.

- **Availability:** For most of the organizations taking up cloud computing high availability is the major task to be considered. The Cloud Service Providers ensure almost 100% availability because this is one of crucial areas where security of the cloud is judged. They back up the data in different datacenters located in different continents to accomplish this.
- **BC/DR planning:** Business Continuity/Disaster Recovery planning is one of the greater challenges in cloud security. Cloud Service Providers not only backup the data in different data centers (across continents), but also can provide the users with the necessary computing power and network (bandwidth) access to that data. Business Continuity means giving continuous access to functional applications, servers and data. DR planning in the cloud environments is extremely cumbersome because there are many hardware failures than in traditional environments.
- **Identity and Access management:** IAM (Identity and Access Management) is one of the methods used by cloud service providers for grant of access to data in the cloud. The casual username/password mechanism may be too simple for confidential data. Either OTP or Email confirmation have become the normal method to grant approval at a transaction level. More complicated access mechanisms are being used and are being provided as a service by third parties.

Main challenges for building a secure and trustworthy cloud system: (Fig. 2)

- **Outsourcing**—In outsourcing, one doesn't know where your servers are, how many copies of your data are kept and who all have access to your data physically and programmatically. The loss of control is a greater concern of security.
- **Multi-tenancy**—In multi-tenancy, one can know what type of programs are running along with your program on the same virtual machine. Multiple customers can share and utilize the same cloud platform. Multi-tenancy means processes belonging to other users (competitive customers, hackers) run on the

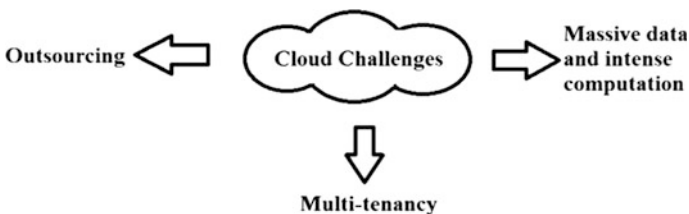


Fig. 2 Major challenges in cloud

same physical HW, in different virtualized environments controlled by hypervisor SW. As hypervisors are SW, they are vulnerable to leakages and virus threats.

- **Massive data and intense computation**—Massive data storage and high performance computing tasks are handled by cloud computing. Because of the high computing power and/or high bandwidth overhead, traditional security mechanisms may not be suitable to store massive data. For example, hashing techniques are not suitable to verify the integrity of remote data. New strategies and protocols are expected [2].

3 Security Techniques

We have about 34 security techniques among which identity based authentication, RSA algorithms, TLS handshake, public key homomorphic, a novel cloud dependability model, Attribute based encryption etc. are included.

- **DES:** DES (Data Encryption Standard) is the most widely used encryption algorithm in the world. The input to DES is plaintext block of a given size (64-bits) and the output is encrypted text block of the same size.
- **RSA:** RSA is an algorithm for public-key cryptography, involves two keys a public key and a private key. The message encrypted one key is decrypted by another key. Normally public key is used for encrypting and the private key is used for decrypting. User data is protected and it includes encryption prior to storage, making the transmission secure.

3.1 What Is Encryption?

To safeguard the data in cloud computing, strong encryption with key management is used. Access to protected resources is empowered by key management while resource protection is provided by encryption.

4 Attribute Based Encryption (ABE)

Attribute based encryption is more suitable for accessing cloud data. The main objective is to offer security and access control. Flexibility, scalability and fine grained access control are some of the aspects of this approach.

Types of ABE

There are many types of ABE namely

1. Cipher text ABE
2. Key-policy ABE
3. ABE with non-monotonic access structures
4. Hierarchical ABE

4.1 Ciphertext Attribute Based Encryption

CP-ABE is the standard and customized model of ABE. The users are assigned with an access tree structure over the data attributes. Threshold gates are the nodes of the access tree where the leaf nodes are attributes. To replicate the access tree structure, the user is defined with a secret key. Secret keys are associated with monotonic access structures and set of attributes are assigned with cipher text (Fig. 3).

In CP-ABE, secret keys are generated which are accessible only to the authorized users. Access tree structure is generated and if the secret key matches with the access tree structure then it allows the customer to decrypt the data. Further, cipher text is generated and if it satisfies the access tree structure it returns the message.

4.2 Key-Policy Attribute Based Encryption

One-to-many interactions can be possible through this type of encryption. The sender identifies the Cipher-texts with a group of descriptive attributes. The attribute authority which is well-believed gives the user’s private key. The schemes that involves the decryption of the data depends on the type of the cipher text. Well-formed group of companies with set of laws about who may read certain documents use this ABE schemes. Protected forensic study and secure transmission of data uses KP-ABE (Fig. 4).

In KP-ABE, to encrypt the data public key and the master key are used by the message senders which are authorized. A secret key is returned which allows the user to decrypt the data encrypted only if it matches with access tree structure. If the user’s access structure is satisfied by the attribute set then the message is returned.

Fig. 3 Mechanism of CP-ABE [3]

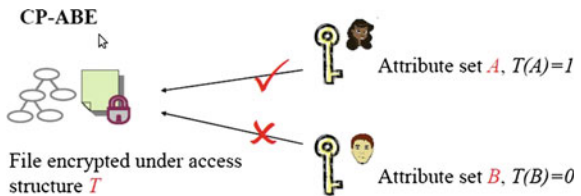
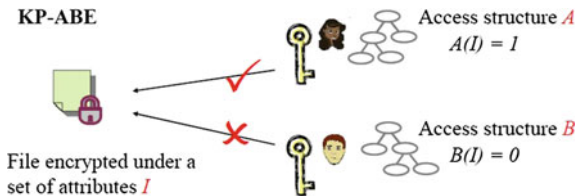


Fig. 4 Mechanism of KP-ABE [3]



4.3 ABE with Non-monotonic Access Structure

Monotonic access structures cannot be used for negative constraints in a key’s access formula. In 2007, Ostrovsky proposed an attribute-based encryption with non-monotonic access structure to solve this problem. In ABE with Non-Monotonic access structure, it states the number of attributes the cipher text has. The user is able to decrypt the encrypted message whenever a key R is generated if and only if it satisfies the access structure ATS with the attributes of that cipher text. If the access structure is satisfied the private key E is used to generate the actual message.

4.4 Hierarchical Attribute-Based Encryption

Wang et al. obtained this technique. There are few parameters involved in H-ABE model. They are: the root master (RM), the domain master (DM), the users and the attributes. The role of the root master is to tend to the third member or a group while that of the domain master is to tend to a group or a multiple number of the users. To create the keys, this scheme utilized the principle of the hierarchical creation of the keys (Fig. 5).

In the H-ABE algorithm, the domain master is created directly using the system parameters and their respective master keys. If the eligibility of the user to the attribute is confirmed then the user attribute and the identity keys which are secure are created for the user else “NULL” is generated. Cipher text is also generated. To recover the plain text the parameters, the cipher text, the user attributes and the

Fig. 5 Mechanism of H-ABE [4]

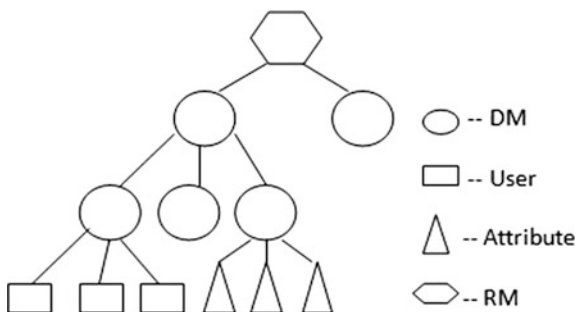
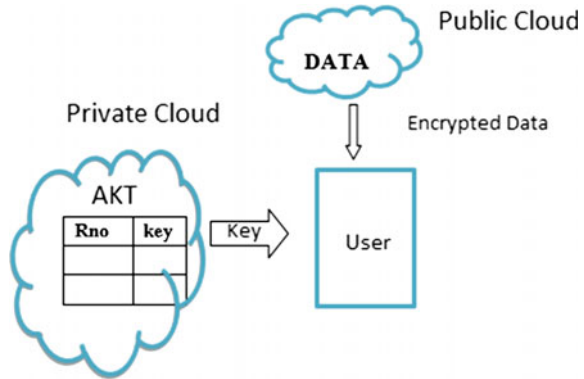


Fig. 6 Mechanism of R-ABE



identity keys which are secure on all attributes in the conjunctive clause are taken. This may not be applicable in few scenarios.

5 Random Attribute Based Encryption

Apart from all the techniques of Attribute based Encryption, we put forth a novel encryption technique in which data can be secure in a different way. In this technique, the data is stored in a public cloud and the attribute key table (AKT) is stored in a private server or a different cloud. The attribute key table consists of record no, (Rno) and a key (Key) value which is unique because it is one of the attribute values of that row. The key changes for every record stored in the public cloud and the plain data never travels on the net (Fig. 6).

The data is decrypted with the key. The data from the public cloud is in the form of encrypted data and from the attribute key table the key is derived. The user can decrypt the data only if these are available (i.e. Encrypted data and the key) with the user. The key size is of 32 bits to 512 bits (due to large no. of combinations, decryption of data is difficult).

6 Conclusion

It is well known that security is the key determinant for the success of cloud technologies. In this paper we discussed some of the best security methods and proposed a different methodology. The advantage of the proposed method is that the key varies for every transmission over the network randomly and the plain text never travels on the public network. We are still in the process of finalizing the details of this method and we are very hopeful that this method will benefit the cloud community.

References

1. Krešimir Popović, Željko Hocenski “Cloud computing security issues and challenges” Institute of Automation and Process Computing.
2. Mohit Marwaha, Rajeev Bedi “Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing” IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013.
3. Parmar Vipul Kumar J, RajaniKanth Aluvalu “Key Policy Attribute Based Encryption (KPABE): A Review” International Journal of Innovative and Emerging Research in Engineering Vol. 2, Issue 2, 2015.
4. Minu George, Dr. C. Suresh Gnanadhas, Saranya. K “A Survey on Attribute Based Encryption Scheme in Cloud Computing” International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 11, November 2013.

Cloud VM/Instance Monitor Phase-II (CIM-PII) Subsystem of eCloudIDS

Madhan Kumar Srinivasan, P. Revathy and Keerthi Balasundaram

Abstract Today cloud computing has established itself as a paradigm in delivering day-to-day on-demand solutions for most of the world's IT corporates making it undoubtedly the most cost efficient method to use, maintain, and upgrade. Apart from the technical features, the corporate world is strongly driven by the striking 'pay-as-you-go' service model. Though the cloud has its advantages, organizations are apprehensive in migrating to a public cloud owing to its severe security challenges. Considering the fact that in present business world, data being an important enterprise asset, it needs to be protected with the highest priority. eCloudIDS, a next-generation security framework designed with a hybrid innovative two-tier expert engine is poised to be one of the most suitable security solution for cloud computing environments. The aim of eCloudIDS is to secure the environment of VMs on which the customers' applications and data are deployed. One of the subsystem of eCloudIDS is the 'CIM—Cloud VM/Instance Monitor' responsible for monitoring the user events on the user specified VMs and instances. CIM is accountable for observing all the events of both authorized and unauthorized users (hackers) and advances them further for an instant capture of each and every activity for the configured VMs. In its initial phase (CIM-PI), the design and implementation of CIM was a successful prototypical experimentation that achieved the monitoring functionality at cloud virtual machine on an open source cloud computing software CloudStack enabled private test-bed. This work bolstered by the research findings and progress made subsequent to CIM-PI, describes the

M.K. Srinivasan (✉)

Indian Institute of Management Calcutta (IIM-C), Kolkata, India
e-mail: madhankrs@gmail.com

P. Revathy

Hindustan University, Chennai, India
e-mail: revamadhankr@gmail.com

K. Balasundaram

The University of Texas at Dallas, Richardson, USA
e-mail: bskeerthi7390@gmail.com

© Springer Nature Singapore Pte Ltd. 2017

H.S. Saini et al. (eds.), *Innovations in Computer Science and Engineering*,
Lecture Notes in Networks and Systems 8, DOI 10.1007/978-981-10-3818-1_14

phase-II design and implementation of eCloudIDS architecture's 'Cloud VM/Instance Monitor (CIM-PII)' with an enhanced monitoring and administration capabilities at VM operating system level including support of heterogeneity in logs.

Keywords Cloud security · eCloudIDS · iCloudIDM · CIM-PII · State-of-the-art cloud computing security taxonomies · Cloud security framework

1 Introduction

Cloud computing is definitely a win-win model for all the enterprises and its stakeholders. But the numerous security concerns associated to it prevents the enterprises from migrating to the cloud paradigm [1–3]. Thus understanding these several security lacunas, and addressing all of them is the top most necessity especially when accounting the user's privacy and sensibility of the data positioned in public (and hybrid) cloud environments.

eCloudIDS [2] is a next-generation generic cloud security framework designed with a hybrid, innovative two-tier expert engines. eCloudIDS addresses the top 3 state-of-the-art cloud computing security taxonomies [1] namely logical storage segregation and multi-tenancy security issues (taxonomy #1) [4–7], identity management issues (taxonomy #2) [8–10], and insider attacks (taxonomy #3) [11]. In our previous effort, the architecture of eCloudIDS [2] along with the implementation of the uX-Engine [4], proposal and implementation of iCloudIDM's layers I [9] and II [10] subsystems were described. Further the experimentation continued with [12], which was a prototypical implementation that achieved an appropriate result on monitoring functionality at cloud virtual machine deployed in a private cloud test-bed using CloudStack. The work here discovers furthermore with the design and implementation of proposed eCloudIDS architecture's monitoring subsystem 'Cloud VM/Instance Monitor (CIM)' Phase II by the research findings and progress inherited from the earlier works. In general, CIM is responsible for observing the events occurring on the user specified VMs or instances running on the infrastructure of eCloudIDS.

2 Related Work

It is ironical that though the existing CSP's assure securing the privacy of data from all aspects, clients are still ambivalent in trusting the CSP's data security as CSP's are considered to be an outsider to their confidence circle [1, 2, 4]. CSP's would not

be adhering to provide the particulars of their executives who would be authorized to the client's data and may not disclose any process involved in watching their access to this data. In [1, 4], it is conspicuous that "Malicious Insider" is one among the top 3 threats in the cloud environment. The white paper by Juniper Networks in [6] points that companies which migrated to public cloud suffer vast number of breaches on the security front than they suffer with their outdated IT infrastructure.

In addition to the above, the data breach report by Verizon [13] highlights a 26% surge in malicious insiders' breaches amounting to a total of 48% of data breaches by them. In the work [14], the authors have proposed an IDS model in which every individual user is monitored by a mini instance of IDS. This model doesn't focus on protecting customer data which is very essential. In [15], the authors have proposed a cloud security model that identifies, collects provenance data from the logs and uses a rule based collection framework that allows for selective filtering of relevant information from the logs. This model would face challenges in a cloud environment where there would be a requirement to consolidate logs from different modules and hosts. CIM implementation will face this challenge in its implementation using intelligent logging and machine learning techniques.

In the work of [16], a framework named "Intrusion Detection System as a Service (IDSaaS)" is introduced that allows users to defend their public cloud instances. This implementation works with a single public cloud currently and this framework should be generalized to work in a distributed environment and have capability to work in diverse or even in heterogeneous clouds. In [17], authors considered two methods, one that is performance approach where the system can generalize to new types of vulnerability and help detect abuse of privileges attacks. But it gives a high false alarm rate. The second method being the information approach notices known trails left by attacks, have potential for low false alarm rates. The CIM implementation focused on performance approach using the techniques of AI. C. Mazzariello et al. [18] explored the advantages of distributed, and centralized approaches to find and prevent the outbreaks originated by customers or external nodes. Although it is a fast and cost effective solution, it can only detect known attacks as only Snort is involved. From our work in [19, 20], we analysed the supervised learning techniques in detail to apply to the eCloudIDS architecture.

In extension to the eCloudIDS proposal [2], the work [4] explores implementation of eCloudIDS architecture's Tier-1 uX-Engine subsystem's implementation. In another work, the architectural implementation of iCloudIDM's layers I [9] and II [10] subsystems were explained. Further in [12], a prototype that achieved the monitoring functionality at cloud virtual machine appropriate result on the deployment of cloud in a private environment using CloudStack. This paper describes the phase-II design and implementation of eCloudIDS architecture's CIM (CIM-PII) subsystem that intends to enhance the monitoring and management capabilities of CIM by using enhanced algorithms on additional logs that are heterogeneous in nature.

3 Cloud VM/Instance Monitor (CIM) in eCloudIDS

Cloud VM/Instance Monitor (CIM) subsystem is accountable for monitoring the events occurring in the user specified VMs/instances. Since it is important to decide which one to log and not to, CIM is designed to monitor the VM in an uninterrupted manner on the directories used by user's applications, files, and even the tables in the database as designed in C3 by the user. CIM monitors all the events of hackers, unauthorized, and legit users and report it to H-log-H for instant capturing of each and every action for the configured instances.

Based on the nature of the resources accessed in the virtual machines by any user, the output of CIM might produce heterogeneous audit logs. A primitive approach followed is to build a parser for every type of log subjected to study and later structured into a single unified unit. This system tends to overcome traditional IDS limitations by employing self-learning capabilities (machine learning techniques) which will assist in tolerating small performance deviations. CIM scrutinizes the performance of virtual servers, applications running on them and even the best resources they share. These auditing tools designed for each logs will amass a huge amount data and discover patterns which may be difficult to identify otherwise.

3.1 *Cloud Instance Monitor—Phase I*

The Phase-I implementation of CIM focused on a primary log called as auth.log file that is omnipresent in any Linux based operating systems. CIM monitors auth.log and extracts significant fields such as Timestamp, login user, login module, ruser, rhost, USER, CMP, PWD, message from it. These fields have all the information required to authenticate an authorized or an unauthorized access. CIM then parses it to store into a separate log file named myauth.log which is advanced to the next subsystem (H-Log-H) of eCloudIDS for further analysis. CIM-PI implementation witnessed a proficient accomplishment in producing myauth.log file output as targeted.

3.2 *Cloud Instance Monitor—Phase II*

The research findings subsequent to the Phase-I implementation of CIM proved to be fruitful paving way for progressing in several aspects, out of which two of them are mainly taken into account, explored, and implemented in Phase II of CIM. They are:

- To extract information subjecting two more logs significant to the intrusion in VM.
- To prove the capability of CIM subsystem in handling heterogeneous logs.

4 Design and Implementation

The complete experimentation was on a private cloud infrastructure using CloudStack 3.0.0 and Citrix XenServer 6.0 hypervisor. One of the Cloud VM was booted with CentOS 6.0 32-bit. This will be henceforth mentioned as Instance-M in this paper. This VM was deployed with an application, i.e. a prototype deployed with MySQL database. CIM monitors the activities of a cloud VM through log files, given the fact that each activity of a virtual machine gets recorded in its operating system log files. It parses the log files to obtain the required fields separately and stores those fields in separate log files. Parsing is done with the help of customized algorithms designed for each log types.

Using the Zeitgeist service in Ubuntu OS, the log files were tracked down and were logically deployed for the implementation. The following are the list of system generated log files that were parsed for this investigation:

- Syslog—/var/log/syslog
- daemon.log—/var/log/daemon.log
- auth.log—/var/log/auth.log
- recently-used.xbel—/.local/share/recently-used.xbel

These parsed files are then sent to H-log-H and ALP subsystems, which manages and maintains these files and generates single final structured output for uX-Engine to process further. The log files specified in Table 1 with particular fields and modules were subjected for experimentation.

The main reason for subjecting the above four logs specifically is that they were heterogeneous nature both in semantics and in behaviour. These logs each provides information from multifarious levels in an operating system where data tampering is recorded such as actions at kernel, storage, access control and file levels. The syslog

Table 1 Logs, Modules and Fields in Ubuntu OS taken for eCloudIDS implementation

Logs	Modules	Fields
auth.log	sudo, su, gdm-session-worker, gnome-screensaver-dialog, polkitd	time, date, loginuser, module, ruser, rhost, PWD, CMD, USER, message
daemon.log	rtdkit-daemon, avahi-daemon, gdm-binary, NetworkManager, dhclient	Time, data, loginuser, module, DHCPDISCOVER, message
sys.log	rtdkit-daemon, avahi-daemon, gdm-binary, NetworkManager, dhclient, kernel	Time, data, loginuser, module, DHCPDISCOVER, message

typically contains the logs of kernel level activities. Apart from kernel level information, typically the syslog captures several other activities and the associated information which are not recorded by the other logs. This results in accession of numerous logs to monitor, some of which are extraneous to this experimentation.

The Daemon Log is generated by a program running in the background of the operating system that ensures proper functioning of the OS. Using daemon log even certain crucial information such as the file name, application name accessed and analysed. The CIM was configured to monitor and capture the entries of USB related activities. Similar to syslog, a dedicated daemon log parser was implemented specifically to capture only the necessary fields from daemon.log.

The Xbel log file i.e. recently-used.xbel file is primarily a part of the GTK + library. It can be inferred from the file name that the Xbel log records the list of the most recently used files. The main rationale for including Xbel logs for experimentation is to monitor the recent activities from heterogeneous applications. It is to be noted that unlike the other logs, the recently-used.xbel is in an XML format. This parsing is dealt by the H-log-H subsystem distinctly to translate it into a processed format. In the recently-used.xbel file, the elements are added according to creation date and not according to the modification date. Capturing the date modified was essential for the experimentation and thus the CIM Phase II subsystem was tweaked.

In the Ubuntu family, all authentication attempts are recorded in a discrete file known as auth log. The ironical reason to study the auth log for this experiment is to learn the user login patterns to understand the usage and control the user has over the sudo command so as to ascertain the level of severity to the message while subjecting to the experimentation of this system. Also to extract only the relevant logs pertaining to user login authentications, a dedicated auth log parser was implemented. Thus the four logs supervised for the CIM-PII covers the following breadth:

- Kernel level activities
- Application daemons/USBs
- Recently used files
- Authentication attempts

Thus the audit logs outputted by the CIM module is heterogeneous irrespective of its severity and authorization, and access by any user.

5 Results

This section analyses the result of the enhanced Phase II (CIM-PII) implementation of Cloud VM/Instance Monitor subsystem of our eCloudIDS security framework.

Phase-I implementation of CIM i.e. CIM-PI [12] was expected to work with minimum functionalities so as to prove its concept to be extended in future for

better integration, and result. Extending this implementation is the CIM-PII where the breadth of the experiment was expanded and three more logs of variant functionalities were put into processing. The approach of heterogeneous log by CIM monitoring module witnessed a proficient accomplishment as targeted. This output is further capable as compared to CIM-PI of going as input to eCloudIDS framework’s next subsystem namely H-log-H. The screenshots of the results obtained from this implementation is shown in this section. Figure 1 shows the Instance-M along with its experimental project complete package deployment using CloudStack. Figure 2 shows the monitored logs recorded with respect to various user

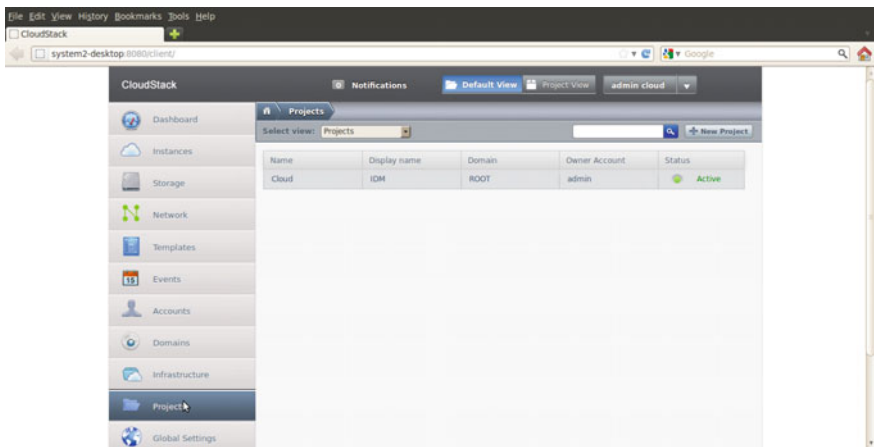


Fig. 1 Experimental project deployment in Instance-M

```

Apr 28 08:17:01 internsl-desktop CRON[2336]: pam_unix(cron:session): session opened for user root by (uid=0)
Apr 28 08:17:01 internsl-desktop CRON[2336]: pam_unix(cron:session): session closed for user root
Apr 28 09:17:01 internsl-desktop CRON[2347]: pam_unix(cron:session): session opened for user root by (uid=0)
Apr 28 09:17:01 internsl-desktop CRON[2347]: pam_unix(cron:session): session closed for user root
Apr 28 10:17:01 internsl-desktop CRON[2361]: pam_unix(cron:session): session opened for user root by (uid=0)
Apr 28 10:17:01 internsl-desktop CRON[2361]: pam_unix(cron:session): session closed for user root
Apr 28 11:17:01 internsl-desktop CRON[2373]: pam_unix(cron:session): session opened for user root by (uid=0)
Apr 28 11:17:01 internsl-desktop CRON[2373]: pam_unix(cron:session): session closed for user root
Apr 28 11:51:40 internsl-desktop gnome-screensaver-dialog: gkr-pam: unlocked login keyring
Apr 28 12:17:01 internsl-desktop CRON[2587]: pam_unix(cron:session): session opened for user root by (uid=0)
Apr 28 12:17:01 internsl-desktop CRON[2587]: pam_unix(cron:session): session closed for user root
Apr 28 12:53:32 internsl-desktop gnome-screensaver-dialog: pam_unix(gnome-screensaver:auth): authentication failure; logname= uid=1000 euid=1000 tty=/dev/rhosh+
rhost= users=internsl
Apr 28 12:53:36 internsl-desktop gnome-screensaver-dialog: gkr-pam: unlocked login keyring
Apr 28 12:54:58 internsl-desktop sudo: internsl : TTYpts/1 : PWD=/home/internsl : USER=root : COMMAND=/usr/bin/nautilus
Apr 28 13:04:34 internsl-desktop sudo: internsl : TTYpts/1 : PWD=/home/internsl : USER=root : COMMAND=/sbin/dmcclient
Apr 28 13:06:19 internsl-desktop sudo: internsl : TTYpts/1 : PWD=/home/internsl : USER=root : COMMAND=/sbin/dmcclient
Apr 28 13:06:22 internsl-desktop sudo: internsl : TTYpts/1 : PWD=/home/internsl : USER=root : COMMAND=/sbin/dmcclient
Apr 28 13:08:30 internsl-desktop sudo: internsl : TTYpts/1 : PWD=/home/internsl : USER=root : COMMAND=/sbin/dmcclient
Apr 28 13:11:21 internsl-desktop sudo: internsl : TTYpts/2 : PWD=/home/internsl : USER=root : COMMAND=/usr/bin/nano /etc/default/avahi-daemon
Apr 28 13:13:39 internsl-desktop sudo: internsl : TTYpts/1 : PWD=/home/internsl : USER=root : COMMAND=/sbin/dmcclient
Apr 28 13:17:01 internsl-desktop CRON[3611]: pam_unix(cron:session): session opened for user root by (uid=0)
Apr 28 13:17:01 internsl-desktop CRON[3611]: pam_unix(cron:session): session closed for user root
Apr 28 13:22:16 internsl-desktop polkit-agent-helper-1[3647]: pam_unix(polkit-1:auth): authentication failure; logname= uid=1000 euid=0 tty= ruser=internsl rhost=
user=internsl
Apr 28 13:22:21 internsl-desktop polkitd(authority=local): Operator of unix-session:/org/freedesktop/ConsoleKit/Session2 successfully authenticated as unix-
user:internsl to gain TEMPORARY authorization for action org.freedesktop.network-manager.settings.system.modify for system-bus-name=:1.80 [/usr/bin/nm-connection-
editor] [owned by unix-user:internsl]
Apr 28 13:23:19 internsl-desktop sudo: internsl : TTYpts/1 : PWD=/home/internsl : USER=root : COMMAND=/sbin/ifconfig eth0:avahi down
Apr 28 13:23:38 internsl-desktop sudo: internsl : TTYpts/1 : PWD=/home/internsl : USER=root : COMMAND=/sbin/ifconfig eth0 down
Apr 28 13:23:44 internsl-desktop sudo: internsl : TTYpts/1 : PWD=/home/internsl : USER=root : COMMAND=/sbin/ifconfig eth0 down
Apr 28 13:23:48 internsl-desktop sudo: internsl : TTYpts/1 : PWD=/home/internsl : USER=root : COMMAND=/sbin/ifconfig eth0 up
Apr 28 13:26:07 internsl-desktop sudo: internsl : TTYpts/1 : PWD=/home/internsl : USER=root : COMMAND=/usr/bin/nano /etc/network/interfaces

```

Fig. 2 CIM-PI’s auth.log with recorded user activities on Instance-M configured with Ubuntu 10.04 32-bit LTS OS

```

May 5 14:48:11 internsl-desktop gdm-session-worker[1419]
May 5 14:48:11 internsl-desktop gdm-session-worker[1419]
May 5 14:48:19 internsl-desktop gdm-session-worker[1419]      msg:Login successfull after logout
May 5 14:48:11 internsl-desktop gdm-session-worker[1419]
May 5 14:48:19 internsl-desktop gdm-session-worker[1419]      msg:Login successfull after logout
May 5 14:48:11 internsl-desktop gdm-session-worker[1419]
May 5 14:48:19 internsl-desktop gdm-session-worker[1419]      msg:Login successfull after logout
May 5 14:48:21 internsl-desktop polkitd(authority=local)
May 5 14:48:11 internsl-desktop gdm-session-worker[1419]
May 5 14:48:19 internsl-desktop gdm-session-worker[1419]      msg:Login successfull after logout
May 5 14:48:19 internsl-desktop gdm-session-worker[1419]
May 5 14:48:11 internsl-desktop gdm-session-worker[1419]
May 5 14:48:19 internsl-desktop gdm-session-worker[1419]      msg:Login successfull after logout
May 6 10:55:28 internsl-desktop gdm-session-worker[1352]
May 5 14:48:11 internsl-desktop gdm-session-worker[1419]
May 5 14:48:19 internsl-desktop gdm-session-worker[1419]      msg:Login successfull after logout
May 5 14:48:19 internsl-desktop gdm-session-worker[1419]
May 5 14:48:21 internsl-desktop polkitd(authority=local)
May 6 10:55:28 internsl-desktop gdm-session-worker[1352]
May 6 10:56:04 internsl-desktop gdm-session-worker[1352]      msg:Login successfull after logout
May 5 14:48:19 internsl-desktop gdm-session-worker[1419]
May 5 14:48:11 internsl-desktop gdm-session-worker[1419]
May 5 14:48:19 internsl-desktop gdm-session-worker[1419]      msg:Login successfull after logout
May 5 14:48:19 internsl-desktop gdm-session-worker[1419]
May 5 14:48:21 internsl-desktop polkitd(authority=local)
May 6 10:55:28 internsl-desktop gdm-session-worker[1352]

```

Fig. 3 CIM-PI's myauth.log output

activities on Instance-M in a log file. Figure 3 shows the processed CIM-PI result screen of the log file, which has the CIM-PII processed data with specific selected fields from different log files. This log will act as an input to H-log-H subsystem of eCloudIDS.

6 Conclusion and Future Directions

The architecture proposed with eCloudIDS aims to offer the maximum security assurance for enterprises which weights their data security over everything else in cloud computing environments (public and hybrid). This research work explores the extended implementation or Phase-II internal design particulars and implementation of eCloudIDS security framework's Cloud VM/Instance Monitor subsystem (CIM-PII) with VM-level Operating System monitoring capabilities. While this reveals different research concentrations in the cloud security arena, CIM-PII also provides future ways on exploring extended heterogeneous monitoring capabilities at cloud virtual machine level. In this paper, the CIM-PII implementation achieves the monitoring functionality at cloud virtual machine appropriate result on the private cloud test infrastructure set up using CloudStack. This result when compared to CIM-PI provides more monitoring and management capabilities so as to support heterogeneity logs as input to succeeding subsystem H-log-H in eCloudIDS security framework. CIM-PII will enable eCloudIDS to further enhance the performance of its core engines, i.e. uX-Engine and sX-Engine, to get overall superior accuracy result.

References

1. Madhan Kumar Srinivasan, K. Sarukesi, Paul Rodrigues, M. Saimanoj, P. Revathy, "State-of-the-art Cloud Computing Security Taxonomies – A classification of security challenges in the present cloud computing environment," ACM, Aug. 2012, pp. 470–476, DOI:[10.1145/2345396.2345474](https://doi.org/10.1145/2345396.2345474).
2. Madhan Kumar Srinivasan, K. Sarukesi, K. Ashima, P. Revathy, "eCloudIDS – Design Roadmap for the Architecture of Next-generation Hybrid Two-tier Expert Engine-based IDS for Cloud Computing Environment," Springer CCIS, Springer Verlag-Heidelberg, USA, Sep. 2012, pp. 358–371, Service Vol. 335, DOI:[10.1007/978-3-642-34135-9_36](https://doi.org/10.1007/978-3-642-34135-9_36).
3. Madhan Kumar Srinivasan, K. Sarukesi, K. Ashima, P. Revathy, "eCloudIDS Tier-1 uX-Engine Subsystem Design and Implementation using Self-Organizing Map (SOM) for Secure Cloud Computing Environment," Springer CCIS, Springer Verlag-Heidelberg, USA, Sep. 2012, pp. 432–443, Service Vol. 335, DOI:[10.1007/978-3-642-34135-9_42](https://doi.org/10.1007/978-3-642-34135-9_42).
4. "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1.," Cloud Security Alliance, 2009.
5. "Top Threats to Cloud Computing V1.0.," Cloud Security Alliance, 2010.
6. "Securing Multi-Tenancy and Cloud Computing," Juniper Networks, 2012.
7. H. Li, J. Sedayao, J. Hahn-Steichen, E. Jimison, C. Spence, S. Chahal, "Developing an Enterprise Cloud Computing Strategy," Intel Corporation, 2009.
8. M. Priyadharshini, R. Baskaran, Madhan Kumar Srinivasan, Paul Rodrigues, "A Framework for Securing Web Services by Formulating a Collaborative Security Standard among Prevailing WS-* Security Standards," Springer CCIS, Springer Verlag-Heidelberg, USA, Sep. 2012, pp. 269–283, Service Vol. 193, DOI:[10.1007/978-3-642-22726-4_29](https://doi.org/10.1007/978-3-642-22726-4_29).
9. Madhan Kumar Srinivasan, K. Sarukesi, P. Revathy, "eCloudIDS Tier-1 iCloudIDM Layer-I (iCloudIDM-LI) Subsystem Design and Implementation through User-centric Identity Management Approach for Secure Cloud Computing Environment," IEEE Computer Society, Italy, DOI:[10.1109/MDM.2013.95](https://doi.org/10.1109/MDM.2013.95).
10. Madhan Kumar Srinivasan, K. Sarukesi, P. Revathy, "Architectural Design for iCloudIDM Layer-II (iCloudIDM-LII) Subsystem of eCloudIDS Generic Security Framework," Proc. Of ICACCI 2013, IEEE, 2013.
11. M. Shiels, "Malicious insider attacks to rise," Technical report, BBC News, 2009.
12. Madhan Kumar Srinivasan, K. Sarukesi, Revathy P, "Design Roadmap for the Phase-I Implementation of Cloud VM/Instance Monitor (CIM-PI) Subsystem of eCloudIDS Security Framework," Elsevier, Aug. 2013, pp. 520–525, ISDN: 9789351071495.
13. W. Baker, A. Hutton, "2010 Data Breach Investigations Report, A study conducted by the Verizon RISK Team with cooperation from the U.S. Secret Service and the Dutch High Tech Crime Unit," Technical report, Verizon, New Jersey, 2010.
14. S. N. Dhage, B. B. Meshram, R. Rawat, S. Padawe, M. Paingaokar, A. Misra, "Intrusion detection system in cloud computing environment," ACM, New York, USA, 2011, pp. 235–239, ISBN: 978-1-4503-0449-8, DOI:[10.1145/1980022.1980076](https://doi.org/10.1145/1980022.1980076).
15. Devarshi Ghoshal, Beth Plale, "Provenance from log files: a BigData problem," ACM, New York, USA, 2013, pp. 290–297, ISBN: 978-1-4503-1599-9, DOI:[10.1145/2457317.2457366](https://doi.org/10.1145/2457317.2457366).
16. Turki Alharkan, Patrick Martin, "IDSaaS: Intrusion Detection System as a Service in Public Clouds," IEEE Computer Society Washington DC, USA, 2012, pp. 686–687, ISBN: 978-0-7695-4691-9, DOI:[10.1109/CCGrid.2012.81](https://doi.org/10.1109/CCGrid.2012.81).
17. Sanjay Ram M, Velmurugan N, Thirukumaran S, "Effective Analysis of Cloud Based Intrusion Detection System," International Journal of Computer Applications & Information Technology, Vol. I, Issue II, September, 2012, ISSN: 2278-7720.
18. Claudio Mazzariello, Roberto Bifulco and Roberto Canonico, "Integrating a Network IDS into an Open Source Cloud Computing Environment," IEEE, 2012, pp. 265–270, ISBN: 978-1-4244-7408-0/10.

19. B. Keerthi, Madhan Kumar Srinivasan, K. Sarukesi, Paul Rodrigues, "Implementation of Next-generation Traffic Sign Recognition System with Two-tier Classifier Architecture," Proc. ACM ICACCI 2012, ACM, Aug. 2012, pp. 481–487, DOI:[10.1145/2345396.2345476](https://doi.org/10.1145/2345396.2345476).
20. B. Keerthi, Madhan Kumar Srinivasan, K. Sarukesi, "iReSign – Implementation of Next-generation Two-tier Identity Classifier-based Traffic Sign Recognition System Architecture using Hybrid Region-based Shape Representation Techniques," Springer CCIS, Springer Verlag-Heidelberg, USA, Sep. 2012, pp. 408–421, Service Vol. 335, DOI:[10.1007/978-3-642-34135-9_40](https://doi.org/10.1007/978-3-642-34135-9_40).

A Review on Big Data Mining in Cloud Computing

Bhaludra R. Nadh Singh and B. Raja Srinivasa Reddy

Abstract Data mining has become indispensable in the wake of ever-growing data in enterprises. The IT departments of organizations have their data mining services. However, the size of data is increased exponentially in such a way that the existing mining algorithms are inadequate to handle such data. The rationale behind this is that the data has become big data with characteristics like volume, variety and velocity. The big data needs to be handled in a distributed environment. Such environment is provided by cloud computing with its rich pool of computing resources. Therefore it is important to understand the dynamics of big data and mining of big data. Aligning IT wings of organizations to handle big data and perform mining on the big data is time consuming and needs investment. For this reason, it is desirable to have a mining service in cloud that can cater to the needs of organizations at an affordable price. This is actually a paradigm shift in thinking of obtaining business intelligence required by organizations. Towards this end this paper reviews literature and provides useful insights that can help in comprehending the present state-of-the-art on big data and possibility of mining service in cloud computing.

Keywords Big data • Cloud computing • Data mining • Mining as a service (MaaS)

B.R.N. Singh (✉)

Department of CSE, ANU, Nagarjuna Nagar, Guntur, Andhra Pradesh, India
e-mail: brn.singh@gmail.com

B.R.S. Reddy

ANU, Nagarjuna Nagar, Guntur, Andhra Pradesh, India
e-mail: brs_121@yahoo.com

© Springer Nature Singapore Pte Ltd. 2017

H.S. Saini et al. (eds.), *Innovations in Computer Science and Engineering*,
Lecture Notes in Networks and Systems 8, DOI 10.1007/978-981-10-3818-1_15

1 Introduction

Data plays significant role in the growth of any organization. When harnessed, data provides valuable insights that help in making strategies for business growth. Traditional approaches for analyzing data can be traced back to manual analysis and computerized analysis through data mining. Data mining is the process of discovering interesting facts from data sources. They are called trends or patterns. These are the discovered facts there were not known earlier. Many data mining algorithms came into existence to serve organizations in discovering actionable knowledge. Nevertheless, the data is growing exponentially and it has got characteristics like volume, velocity and variety. Such data is called big data. The existing data mining algorithms cannot handle big data efficiently for many reasons. First, the data is very huge and with different varieties. Second, the data mining algorithms were developed for serial processing and they cannot support parallel processing. Third, the existing algorithms are inadequate to perform their operations on big data. For this reason it is desirable to have new data mining algorithms that can work in distributed environment and cater to the big data processing required by organizations.

1.1 *Big Data*

Big data refers to the data with huge amount of data (volume), with structured and unstructured data (variety) and the data on transit (velocity). Enterprises in the real world are producing huge amount of data and that data is growing exponentially from time to time. Such data is called big data. Big data mining can provide opportunities and security issues to enterprises. In fact big data processing can add value to businesses when the data is mined and comprehensive intelligence is extracted.

1.2 *Volume*

This is one of the features that indicates huge amount of data. It also reflects exponential growth of data. Social networks and sensor networks are some of the examples where huge amount of data is generated. Recently there is unprecedented growth in the accumulation of data.

1.3 Velocity

Velocity refers to the moving nature of data. Data is steamed or accumulated constantly from different sources. For instance sense networks send data continuously to base station. The speed with which data is flown reflects the term velocity. Big data processing needs to deal with it.

1.4 Variety

This attribute refers to the fact that the big data has different varieties of data. As the data is arrived at the destination from different sources, the data is naturally of different kinds. The sources of data may be from news, emails, web logs, sensor networks and social networks. Handling such data which is in the form of structure, unstructured and semi-structured formats is very important requirement for processing big data.

1.5 Variability

This indicates that the data that comes from different sources many not be compatible with each other. Due to certain events data flow might have sudden increases that can have influence on the processing of big data.

1.6 Complexity

As data comes from different sources with different formats and the data is huge, it is naturally complex in nature. Such data needs to be correlated and processed.

1.7 Value

The ultimate purpose of maintaining and processing big data is its value to an enterprise. The value refers to the results of using business intelligence (BI) that helps in organic or inorganic growth of an organization. BI can help enterprises to make strategic decisions that lead to sustained growth in the competitive world.

2 Big Data Classification

There are many classes of big data. Stated differently there are many terms associated with big data. They are data processing, data staging, and data storing, content format and data sources. Each category has different aspects again. The classification of big data is visualized in Fig. 1.

The data sources available are IoT, transactions in different domains, social networking, sending, remote sensing, and World Wide Web (WWW). The data formats include structured, unstructured and semi-structured. The data stores are in the form of key-value pairs, graph based data, column or document-oriented data. The data staging is a process of normalization, data cleaning and data transformation. The data processing can be done using either real time process or batch processing.

3 Need for Big Data Mining

When there is exponential growth of data there is possibility of having very useful information hidden. Processing a portion of data may produce biased information that cannot be used to take accurate decisions. Sometimes big data contains cross organizational data. In other words, it is the data of a domain such as banking where data comes from different banks. Thus it is useful to get hidden trends in the data of the domain in order to have required business intelligence. Such BI can affect the whole domain instead of one or two players in the domain. Big data mining refers to considering the big data (whole data from different sources) for processing. Big

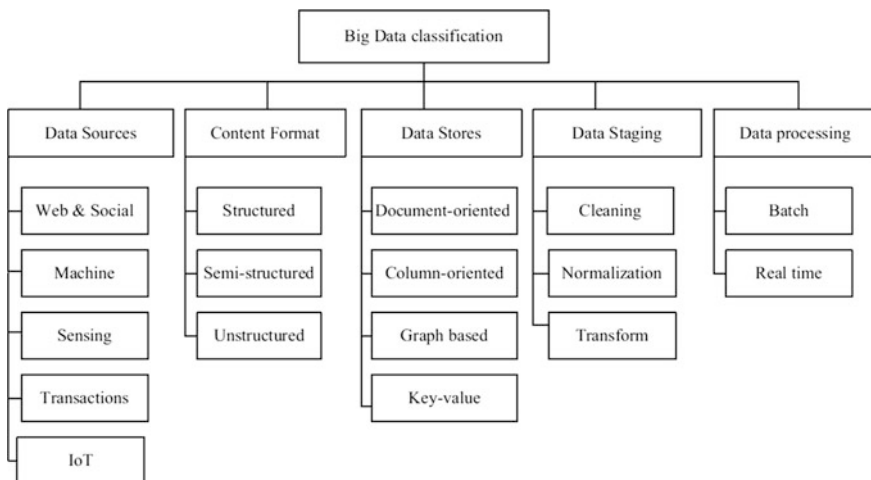


Fig. 1 Classification of big data [1]

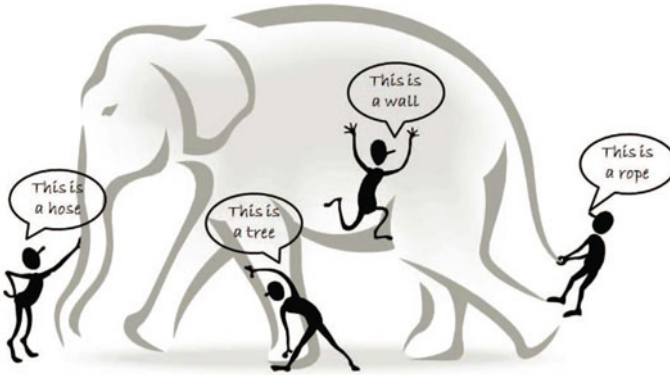


Fig. 2 Biased conclusions by processing portions of data [2]

data mining can provide comprehensive business intelligence which lacks if a portion of data is processed. As big data is different from traditional data with characteristics aforementioned, there should be different environment to process it. Processing voluminous data needs high processing power and a great deal of resources. Therefore it is essential to have big data mining to obtain very useful BI. Figure 2 shows why an organization should consider processing big data.

The blind men having limited view of sight on the data and made biased conclusions that are not accurate. This is clearly indicating the need for processing big data for comprehensive business intelligence. Since big data can add value to big business it is important to have such data mining strategy to make well informed decisions [3].

4 Big Data Platforms

Big data is relatively new research area. However, there are handful of frameworks or platforms that can be used to work with big data in different levels. The big data platforms are presented in Fig. 3. The big data platforms can support both real time processing and batch processing. They support parallel processing by leveraging GPUs in the cloud computing environment.

Big data platforms are the frameworks that support activities involved in processing big data. Right from storage to processing of big data there are many frameworks available. Apache Hadoop is one of the well known platforms that can provide built in infrastructure to store and process big data. In fact Hadoop is a distributed programming framework that supports MapReduce programming paradigm. MapReduce is the programming approach where Map and Reduce phases are involved. It is the programming approach that can process huge amount

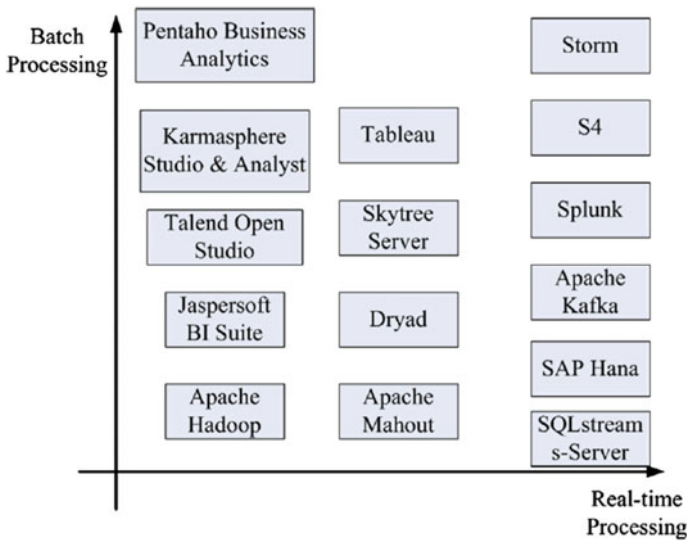


Fig. 3 Big data platforms [1]

of data or big data. Hadoop supports a distributed file system known as Hadoop Distributed File System (HDFS).

Dryad is another programming approach that exploits Dataflow Graph Processing (DGP). Apache Mahout is the platform that supports many pre-defined machine learning algorithms that can be used to process big data. It can be integrated with businesses so as to obtain business intelligence. Jaspersoft BI Suite on the other hand supports report generation automatically. Pentaho Business Analytics [1] is another tool for generating reports. Skytree server is the tool used to perform data analytics for big data mining. Tableau is another platform that can be used for processing big data. It supports three different tools like Server, Desktop and Public. For processing big data Karmasphere can also be used. Talend Open Studio is meant for providing graphical interface for big data processing.

For handling of streaming data S4 is the cloud platform specially designed. Real time processing and obtaining business intelligence is possible with Splunk. A messaging system is provided is known as Apache Kafka which achieves high throughput besides supporting in-memory analytics. SAP Hana is the big data platform that supports in-memory analytics though its scalable batch processing. Dremel is from Google for analyzing nested data in interactive fashion. A tool similar to Dremel from Apache is known as Apache Drill [1]. When big data is outsourced it there is possibility of privacy issues as explored in [4, 5]. In order to overcome these issues there is solution through l -diversity and k -anonymity in [6] in order to protect data from being abused. These techniques can effectively prevent identity disclosure attacks.

5 Distributed Programming Frameworks

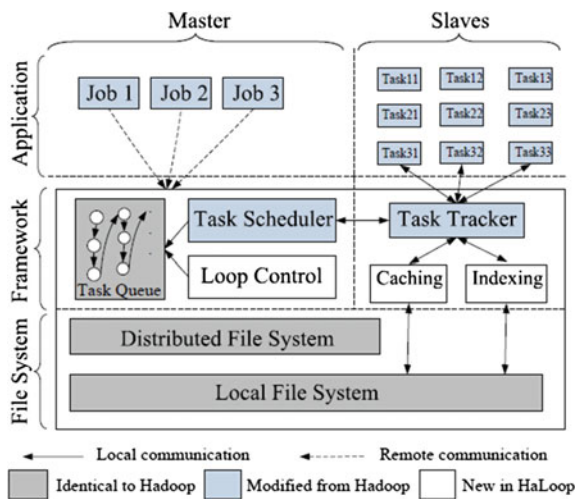
Distributed programming frameworks are the frameworks that work in cloud environment and they exploit parallel processing and data centres for efficient processing of big data. They support MapReduce programming paradigm that can help in processing large volumes of data. There are many distributed programming frameworks like Hadoop, Haloop, Hive, Mahout, Hbase, Pig, Spart, Twister, MAPR, Acro, Cassandra, and Chukwa [7]. In the same fashion, there are many databases that of NoSQL kind for supporting big data processing. They are SimpleDB, MangoDB, DynamoDB and so on [7]. DicCO [8] is the framework known for its ability to have collaborative aggregation for big data mining. Phoenix is a framework for distributed programming that can exploit the power of GPU [9]. Weka tool can also be integrated with MapReduce tool for processing big data. Stream mining is also possible with distributed programming frameworks as explored in [10].

5.1 Processing Big Data with Hadoop and Haloop

As explored in [11] Hadoop is MapReduce framework which is open source distributed programming framework. Haloop is a variant of Hadoop which extends the capabilities of Hadoop. Both can provide scalable programming solutions pertaining to big data. The Haloop architecture is shown in Fig. 4.

Haloop has many features such as loop aware scheduling of tasks, scheduling, indexing and caching. The architecture has three layers such as file system layer, framework layer and application layer. The file system layer has two kinds of file

Fig. 4 Overview of Haloop Architecture [11]



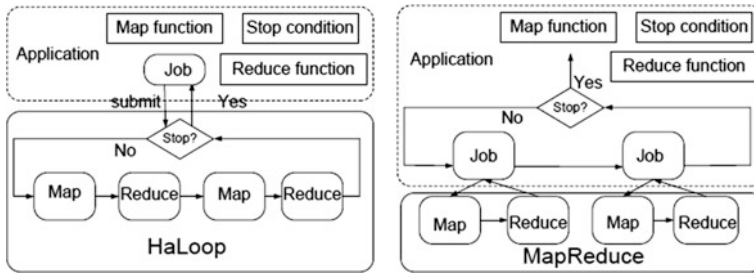


Fig. 5 Comparison of iterative process in Hadoop and HaLoop [11]

systems such as distributed and local file systems. The local file system shows the content of local system while the distributed file system reflects the files in distributed environment. The components present in the framework layer are task tracker, loop control and scheduler. The task scheduler schedules given jobs in loop aware fashion. The loop control coordinates to keep track of the given jobs. The caching and indexing are the features that can help to improve the speed of the processing. The slave and master nodes are in application layer that are meant for processing big data (Fig. 5).

The iterative processing in HaLoop and MapReduce frameworks function differently. The loop awareness is not supported in Hadoop while the HaLoop has support for it. HaLoop also supports caching and page rank algorithms in order to improve the processing and presentation of results.

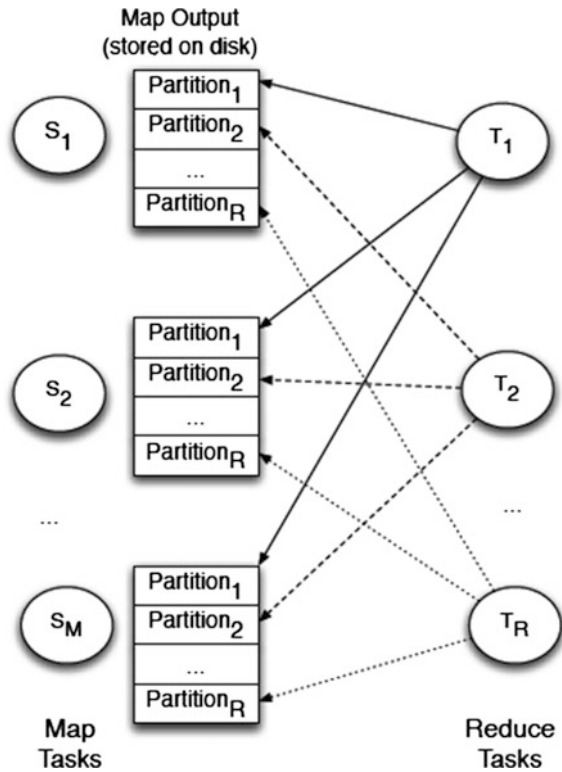
5.2 Large Scale Data Processing with Sailfish

Another framework named Sailfish was explored in [12] which is based on the new programming paradigm MapReduce. It has improved Map and Reduce parts of the programming model. When compared with Hadoop it exhibits 20% performance improvement. This is achieved through auto tuning feature.

As can be seen in Fig. 6, Sailfish has improved mechanisms for Map and Reduce. They are made flexible to work with huge volumes of data. They exploit the features such as auto-tuning for better processing. Its performance is evaluated using benchmark datasets provided by Yahoo. The parallel features of the environment are used by the framework with intermediate operations achieving high performance in terms of reducing computational overhead.

As shown in Fig. 7, the data is executed in batches. The framework uses this feature as and when required in order to reduce computational overhead. This is achieved by using efficient intermediate processing. It makes use of I files in order to support batch processing effectively.

Fig. 6 Map and Reduce tasks of Sailfish [12]



6 Relationship Between Big Data, Map Reduce and Cloud

Since big data is very huge and cannot be handled in the local machines due to limitations in the resources, cloud is the well known platform to handle such data. Therefore there is relationship between big data and cloud as cloud only can provide required resources for processing big data. Cloud can provide distributed programming frameworks, data centres and a pool of computing resources. The distributed programming frameworks are typically used to process huge amount of data. Especially they support MapReduce to handle huge amount of data. Virtualization is technology that makes the cloud computing easier. In fact cloud is on top of virtualization technology for scalable and available services. Big data utilizes the services rendered by cloud for efficient storage. Cloud based applications can be used to process big data [7]. The relationship between the MapReduce, cloud and big data can be understood by looking at Fig. 8.

The MapReduce programming model works in tandem with HDFS for processing big data which is stored in cloud. There are queuing engines like Mahout and Hive for effective processing of big data. HDFS is used to store and retrieve unstructured data. This is the file system that can cater to the file handling needs of

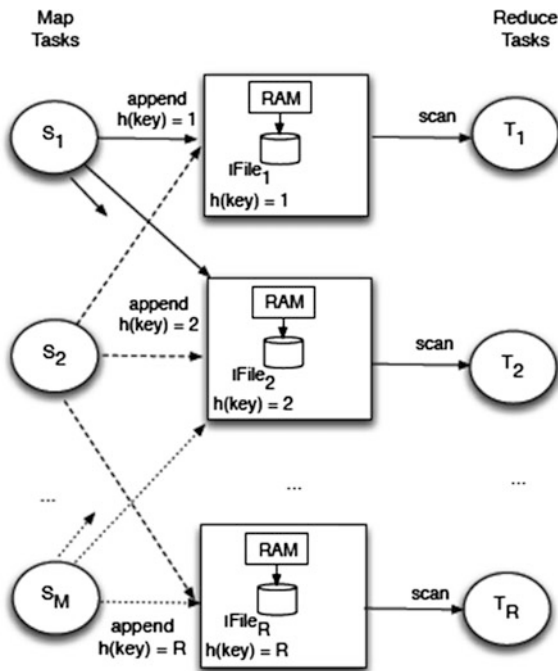


Fig. 7 Batch processing process in Sailfish [12]

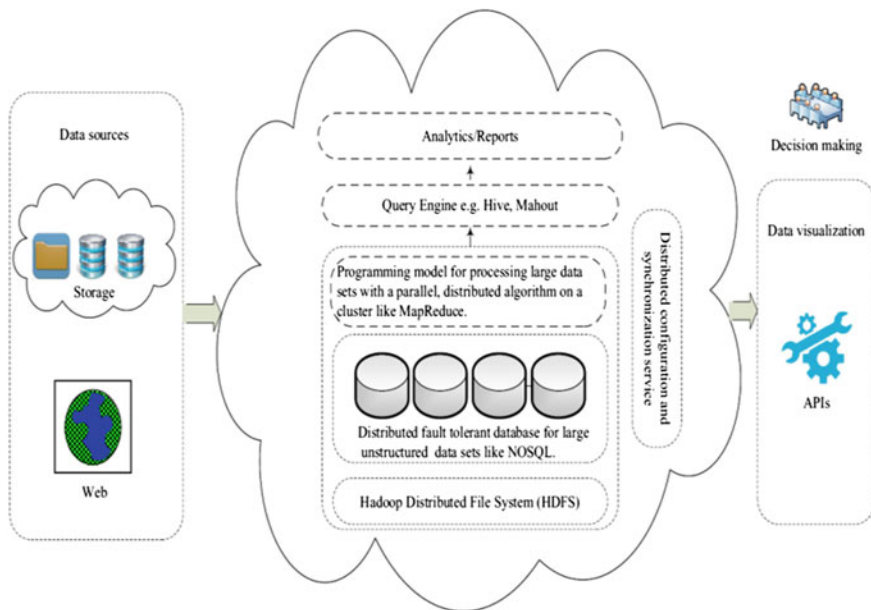


Fig. 8 Big data using cloud and MapReduce [7]

the distributed environment [7]. There are many cloud computing services provided by Google, Amazon, Microsoft and IBM. The frameworks like Elastic MapReduce, Azure, Hadoop and BigQuery are used to process big data. There are some case studies successfully exploited big data analytics. They include Alacer, Nokia, redbus, Swiftkey, and 343 Industries.

7 Conclusion and Future Work

In this paper a review is made on big data, distributed programming frameworks and MapReduce programming paradigm. This review provides basic level insights into cloud computing, big data, and need for big data mining. Traditional programming models cannot exploit GPUs available in pool of cloud resources. MapReduce can do this by utilizing parallel power of GPU. There are many distributed programming frameworks such as Sailfish, Hadoop and Haloop that support MapReduce programming. There is relationship between cloud computing, MapReduce programming paradigm and big data. As huge amount of data is outsourced to cloud and processed by distributed programming frameworks, there is natural relation between the cloud, MapReduce and big data. The review of frameworks in this paper can provide useful information besides relating them with programming model and cloud. In future we build a framework for providing a special big data mining service over cloud.

References

1. C.L. Philip Chen, Chun-Yang Zhang. (2014). Data-intensive applications, challenges, techniques and technologies: A survey on Big Data. ELsevier. p. 32–44.
2. Xindong Wu, Xingquan Zhu, Gong-Qing Wu. (2014). Data Mining with Big Data. IEEE. 26 (1), p. 97–107.
3. I. Kopanas, N. Avouris, and S. Daskalaki, “The Role of Domain Knowledge in a Large Scale Data Mining Project,” Proc. Second Hellenic Conf. AI: Methods and Applications of Artificial Intelligence, I.P. Vlahavas, C.D. Spyropoulos, eds., pp. 288–299, 2002.
4. J. Lorch, B. Parno, J. Mickens, M. Raykova, and J. Schiffman, “Shoroud: Ensuring Private Access to Large-Scale Data in the Data Center,” Proc. 11th USENIX Conf. File and Storage Technologies (FAST’13), 2013.
5. E. Schadt, “The Changing Privacy Landscape in the Era of Big Data,” Molecular Systems, vol. 8, article 612, 2012.
6. A. Machanavajjhala and J.P. Reiter, “Big Privacy: Protecting Confidentiality in Big.
7. IbrahimAbakerTargioHashem, IbrarYaqoob, NorBadrulAnuar, Salimah Mokhtar, Abdul-Gani, and SameeUllahKhan. (2015). The rise of “big data” on cloud computing: Review and open research issues. ELsevier. 47 (1), p. 98–115.
8. S. Papadimitriou and J. Sun, “Disco: Distributed Co-Clustering with Map-Reduce: A Case Study Towards Petabyte-Scale End-to-End Mining,” Proc. IEEE Eighth Int’l Conf. Data Mining (ICDM’08), pp. 512–521, 2008.

9. C. Ranger, R. Raghuraman, A. Penmetsa, G. Bradski, and C. Kozyrakis, "Evaluating MapReduce for Multi-Core and Multiprocessor Systems," Proc. IEEE 13th Int'l Symp. High Performance Computer Architecture (HPCA'07), pp. 13–24, 2007.
10. X. Zhu, P. Zhang, X. Lin, and Y. Shi, "Active Learning From Stream Data Using Optimal Weight Classifier Ensemble," IEEE Trans. Systems, Man, and Cybernetics, Part B, vol. 40, no. 6, pp. 1607– 1621, Dec. 2010.
11. Yingyi Bu, Bill Howe, Magdalena Balazinska and Michael D. Ernst. 2010. HaLoop: Efficient Iterative Data Processing on Large Clusters. USA: IEEE. p 1–12.
12. Sriram Rao, Raghu Ramakrishnan and Adam Silberstein. 2012. Sailfish: A Framework for Large Scale Data Processing. USA: Microsoft. p 1–14.

Implementation of Fuzzy Logic Scheduler for WiMAX in Qualnet

Akashdeep

Abstract IEEE 802.16 standard has not specified any algorithm for implementation of schedulers which has led to number of developments in recent past. Soft computing techniques like fuzzy logic based schedulers have also been proposed however integration of these schedulers into existing simulators is still a competing task. Although lot of help is available on web regarding integration of different algorithms in simulators but implementation of soft computing based algorithms in available simulators is still an open issue. This paper is an attempt to guide researchers towards implementation of fuzzy logic based scheduler in Qualnet simulator. Class diagram with sample code snippets are proposed to aid and guide researchers. The paper also discusses implementation of various quality of service mechanism for IEEE 802.16 networks.

Keywords IEEE 802.16 • Wimax • Growth of standard • Wimax forum

1 Introduction to WiMAX Scheduling

IEEE 802.16 is a series of Wireless Broadband standards written by Institute of Electrical and Electronics Engineers (IEEE) [1]. Current IEEE 802.16 standard does not specify any scheduler for WiMAX network and vendors are free to innovate and research with algorithms of their choice in this field. Scheduling in WiMAX is possible in both uplink and downlink directions. Scheduling decision in uplink are difficult to make as BS may have only limited or outdated information about current state of each uplink connection because of delay and likely collisions on the network. There are many schedulers available for WiMAX but adaptive and adequate schedulers are still in growing stage of development. Design of an adaptive approach for solving scheduling problem in WiMAX can be implemented using fuzzy uncertainty theories. Fuzzy logic based schedulers can be used to implement

Akashdeep (✉)
UIET, Panjab University Chandigarh, Chandigarh, India
e-mail: akashdeep@pu.ac.in

intelligent and adaptive algorithms. The readers may refer to studies of [2–4] for number of fuzzy logic based schedulers. Although theory and algorithm for fuzzy logic based method is widely available but implementation of any fuzzy scheduler in any of the simulators is not presented. This paper elaborates on implementation of dynamic scheduler for IEEE 802.16 networks that employs concepts of fuzzy logic in Qualnet 5.02 simulator. Scheduler based on authors own study has been taken as base for implementation.

2 Qualnet Simulator

To simulate IEEE 802.16 networks different options were available like ns-2 WiMAX patch from NIST [5], WiMAX module proposed by Freitag [6], CNG of University of Pisa [7], ns-3 simulator [8], OPNET [9], Omnet++ [10], MATLAB [11] but Qualnet [12], a simulator from Scalable Technologies provides easy GUI interface and object oriented architecture of its source code files. Qualnet is a proprietary simulator developed by Scalable Network Technologies, New York, USA. It is shipped with under mentioned libraries

- Developer Library
- Multimedia and Enterprise Library
- Wireless Library
- Advance Wireless Library
- Cellular Library
- Satellite Library
- Sensor Network Library
- UMTS (Universal Mobile Telecommunication System) Library
- Urban Propagation Library

2.1 *Advanced Library Structure*

Apart from providing support for above mentioned libraries Qualnet is shipped with Advanced Wireless Library that provides features for simulation of IEEE 802.16 WiMAX networks. The advanced wireless library for Qualnet 5.2 provides support for implementing features of IEEE 802.16 network. Implementation is divided into MAC and PHY layers. Advanced library ships in with some pre compiled header files for easy implementation of IEEE 802.16 features. PHY and MAC are implemented in header files `phy_dot16.h` and `mac_dot16.h` respectively. Implementation of MAC features and MAC sub layer features are further divided into number of independent files for their smoother interoperation and independent operations. Table 1 lists these files together with their purpose.

Table 1 Implemented files in Qualnet for IEEE 802.16 MAC

File(s)	Features available
mac_dot16.h	Main header file of implementation of IEEE 802.16 MAC. It includes structures for mac header, declarations for various timing signals, TLV values, generic parameters for ranging, request, intervals defined, declarations for service types etc.
mac_dot16_bs.h	Implementation of BS features of IEEE 802.16 MAC. Declarations of data structures together with supported operations for IEEE 802.16 BS
mac_dot16_cs.h	Implementation of convergence sub-layer feature for IEEE 802.16 MAC
mac_dot16_phy.h	Implementation of IEEE 802.16 MAC-PHY specific part
mac_dot16_qos.h	Implementation of IEEE 802.16 Quality of service implementation
mac_dot16_sch.h	Implementation of IEEE 802.16 scheduling functions
mac_dot16_ss.h	Implementation of features supported for IEEE 802.16 subscribers
mac_dot16_tc.h	Implementation of dot16 traffic conditioning and policing by remarking/dropping based bandwidth/delay policy
mac_dot16e.h	Implementation of IEEE 802.16e MAC as an extension of IEEE mac_dot16.h
mac_dot16_cs.h	Implementation of convergence sub layer of IEEE 802.16 MAC
phy_dot16.h	Implementation of IEEE 802.16 PHY features

3 Development of Fuzzy Logic Based Scheduler in Qualnet

Support for IEEE 802.16 in Qualnet 5.2 has been provided in Advanced Wireless Library but researchers need to have knowledge of wireless and developer library to understand its basic working. In spite of having a customized structure, scheduling library is not implemented as single API. Code for scheduling is scattered within various libraries and being proprietary software very little help about implemented classes is available on web. There is a dire need to narrow down this gap and this section provides an overview for implementation of scheduler in Qualnet. Figure 1 shows class diagram of developed fuzzy based scheduler for IEEE 802.16 networks together with some important variables or functions of other classes with which developed system interacts. WFQ algorithm has been implemented in *WfqScheduler* class with *FQScheduler* class as its base which further inherits some properties of *Queue* class. The *FQScheduler* class provides some common functionality to other weight-based schedulers also, so only specifics of insert and retrieve member functions (which are particular to WFQ) need to be implemented for our scheduler.

Implementation of common features for IEEE 802.16 standard has been provided in *MacDot16* class. This class acts as base for *MacDot16Bs* and *MacDot16Ss* classes which provides features for configuration of properties for base station and subscriber stations. The structure *MacDot16Qos* provides implementation of

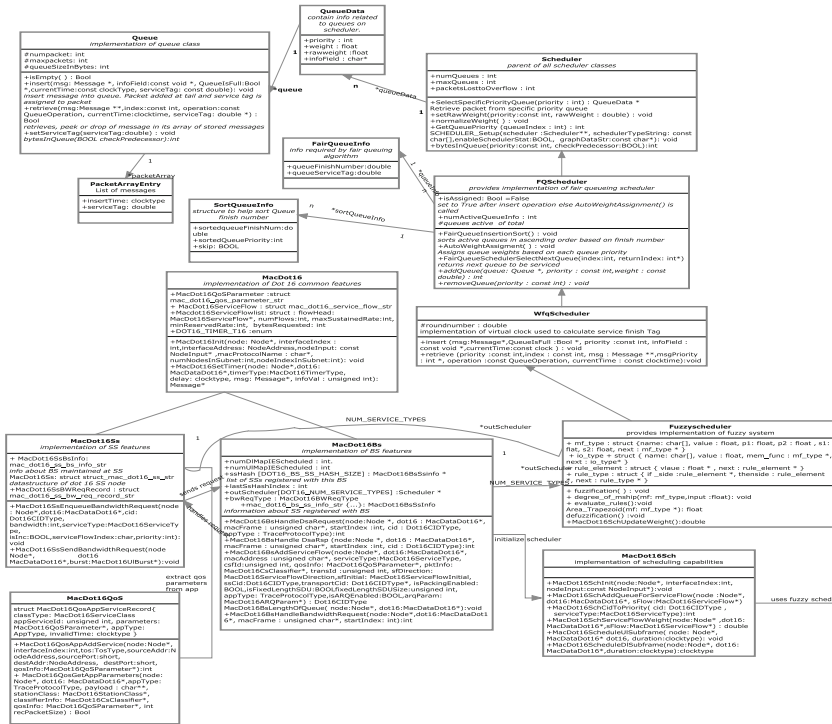


Fig. 1 Class diagram of fuzzy based scheduler

quality of service features for admitted applications. It also includes number of implemented functions like addition of new service class, updating of QoS parameters for various applications etc. The function *MacDot16QoSAppAddService* (...) helps to add service corresponding to the application being admitted. This function is called from application.h header file of wireless developer library. A service flow for application is created by calling function *MacDot16QoSAddServiceClass*(...). Implementation of service flows is core to process of scheduling and its facilities are tailored in *mac_dot16.h* file (header file for *MacDot16* class). A service flow provides unidirectional transport of packets either to uplink, transmitted by subscriber station or to downlink i.e. transmitted by Base Station. It is characterized by a set of parameters as service flow identifier (SFID), service class name (UGS, rtPS, ertPS, nrtPS, or BE), and QoS parameters (such as maximum sustained traffic rate, minimum reserved rate and maximum latency). QoS Parameters for any service flow are implemented by structure *MacDot16QoSParameter* and representation of service flow is provided using *MacDot16ServiceFlow* structure. Both are implemented in *MacDot16* class.

In order to code fuzzy logic principles in Qualnet suitable data structures to represent input/output variables, membership functions and fuzzy rules has been designed. Fuzzy logic scheduler has been implemented as an extension of WFQ

scheduler in class named as *Fuzzyscheduler*. The *Fuzzyscheduler* needs to interact with number of different entities and its interaction with these entities is shown. The class has implemented extended features of WFQ algorithm together with other fuzzy logic operations. There are three major transformations that are made to data before it is converted to output in any fuzzy system: Fuzzification, rule evaluation and defuzzification. These transformations have been implemented by designing functions *fuzzification(...)*, *evaluate_rules(...)* and *defuzzification()* respectively in *Fuzzyscheduler* class. Function *defuzzification()* is defined that calculates this value on the basis of strength of output rules. It makes further calls to *Area_Trapezoid()* function to calculate area under individual membership functions using centroid method. A function *MacDot16SchUpdateWeight (...)* has been defined in *Fuzzyscheduler* class. This function calls fuzzy inference system to find out new weight value based on input variables considered in this study at appropriate time intervals. Latency and throughput requirements for flow can be calculated from specific quality of service parameters of that flow. A function *MacDot16BsLengthOfQueue(...)* has been designed in *mac_dot16_bs.h* file for calculating amount of traffic present in queues. The function evaluates amount of data in queues of respective service classes of subscribers registered with base station by making calls to function *bytesInQueue(...)* defined in *if_scheduler.h* file. The function returns value of variable *bytesUsed* as sum of bytes stored in respective queue.

MacDot16 class contains structure named *MacDot16MacHeader* to simulate MAC header for IEEE 802.16 networks. This structure is used to implement various types of MAC header to be used by IEEE 802.16 standard for various purposes. Fields for this structure are defined as character (byte) types to prevent alignment of windows platform and different fields for generic type. This structure is used to build information about bandwidth request. Information from this structure is extracted by different functions based on which further actions are implemented by different entities of MAC layer. A number of macros are defined to gather information from this header like *MacDot16MacHeaderGetBR(header)*. It reads value for byte2, byte3 and three bits for byte 1, typecasts it to unsigned value in order to get information about bandwidth requirement. The first byte is used to find type of header i.e. whether header is generic or bandwidth request. Information in this header is utilized by scheduler to process bandwidth request at base station and by subscribers to indicate to basestation about its bandwidth requirements. Processing of bandwidth request at base station is done by function *MacDot16BsHandleBandwidthRequest(...)* defined in *MacDot16Bs* class. This function uses macros to extract details of bandwidth requirements sent by subscribers and depending on type of bandwidth requested, i.e. aggregate or incremental, it either adds it to previous requirement made by that service flow or assigns it as new aggregate requirement for that flow. Similar macros are used by SS to indicate about bandwidth requirements.

Allocation of bandwidth is done by functions defined in file *MacDot16Sch.cpp*. There is function named *MacDot16ScheduleUlSubframe(...)* that provides logic for bandwidth allocation in IEEE 802.16 networks. Function calculates value

of variable dataLen for different services based on maximum sustained rate for UGS and ertPS classes. Function makes use of technique discussed in previous chapter to make allocations to other classes. It then sets variable maxBwGranted to indicate about amount of bandwidth allocated to service flow. Information about bandwidth granted to different SS is conveyed by UL-MAP message which is a component of DL-subframe. The downlink subframe is built by function *MacDot16ScheduleDlSubframe(...)*. The function *ScheduleDlSubframe* calls data schedulers for each scheduling service to check for any queues requiring service. The weight calculated by function *MacDot16SchUpdateWeight (...)* are used by fuzzy scheduler to serve different queues based upon their new weights. This process is continued until all queues are served or scheduler runs out of slots.

4 Conclusion

The paper has presented implementation of a fuzzy logic based scheduler for IEEE 802.16 WiMAX network in world class simulator Qualnet 5.2. The implementation has been done by extending the existing structure of standard simulator. The extended class diagram together with implemented functions has been discussed. The paper also discusses technique to generate various applications and implement various features for IEEE 802.16 WiMAX networks. The paper may be lifeline to research scholars who are exploring the possibility to research and explore scheduling issues in WiMAX networks.

References

1. IEEE, 2010. Draft IEEE Standard for Local and metropolitan area networks Corrigendum to IEEE Standard for Local and Metropolitan Area Networks- Advanced Air Interface. IEEE P80216 m/D10, November 2010. 2010: 1–1132.
2. Sadri Y. and Mohamadi, S. K., 2013. *An intelligent scheduling system using fuzzy logic controller for management of services in WiMAX networks*. Journal of Super computers. 64, 849–861.
3. Alsahag, A. M., Ali, B. M., Noordin, N. K. and Mohamad, H. (2014), Fair uplink bandwidth allocation and latency guarantee for mobile WiMAX using fuzzy adaptive deficit round robin. Journal of Network and Computer Applications, 39, 17–25. URL:- <http://dx.doi.org/10.1016/j.jnca.2013.04.004>.
4. Akashdeep and Kahlon K. S., 2014. An embedded fuzzy expert system for adaptive WFQ scheduling of IEEE 802.16 networks. Expert Systems with applications. 41, 7621–7629. <http://dx.doi.org/10.1016/j.eswa.2014.05.048>.
5. NIST, “*The Network Simulator ns-2 NIST Add-on IEEE 802.16 Model (MAC+PHY)*,” 2007. URL:- http://www.nist.gov/itl/antd/emntg/upload/wimax_module.pdf.
6. Freitag J. and Fonseca, N., 2012. *WiMAX Module for the ns-2 Simulator*. IEEE 18th International Symp. on Personal, Indoor and Mobile Radio Communications, 1–6.

7. C. N. G. at the University of Pisa and B. W. N. L. at Georgia Institute of Technology. 2013. *ns2 Contributed Code: IEEE 802.16 Wireless Mesh Networks in ns-2*. URL:- <http://nslam.isi.edu/nslam/index.php/ContributedCode>.
8. https://www.nslam.org/doxygen/wimax-simple_8cc_source.html. last accesses May 7, 2016.
9. <http://www.riverbed.com/in/solutions/index.html>. last accessed May 7, 2016.
10. <https://omnetpp.org/omnetpp>. last accesses May 7, 2016.
11. <http://in.mathworks.com/matlabcentral/fileexchange/24369-wimax-physical-layer-simulation>. last accesses May 7, 2016.
12. <http://www.scalable-networks.com/pdf/QualNetTutorial.pdf> last accessed June 15, 2016.

A Survey of Evolution of IEEE 802.16 Certification and Standardization

Akashdeep

Abstract IEEE 802.16 is better known with the name of WiMAX as a future technology for communication networks. Most users are aware about technical details of IEEE 802.16 networks but very little has been discussed about progression and evolution of certification and standardization process. This paper is a novel attempt to trace this progression and will enlighten today's audience about process of WiMAX towards being one of popular technology. This paper is an attempt to summarize various activities that took place at IEEE for standardization and development of IEEE 802.16 as new standard. A comprehensive analysis of various projects and their timeline development is elaborated that reveals importance and incorporation of new ideas into already existing standards. Role of organizations like WiMAX forum is also elaborated.

Keywords WiMAX • Standard growth • WiMAX forum

1 Introduction to IEEE 802.16 and WiMAX

Wireless and mobile communications have changed communication systems over past decades. IEEE 802.16 is an internationally accepted standard [1] to provide up to 1 Gbit/s for fixed stations which is better than conventional cable modem and DSL connections. WiMAX facilitates various service providers to come across various challenges that they encounter due to growing customer demands since it has capability to flawlessly interoperate across different network types. Majority of articles and surveys being published on WIMAX [2–7] details only about technical details of technology. The contribution of various reports in listing offerings of various task groups is also limited. There have been some good books [8–11] listing growth of standard but related details have still been missing and only a list of various amendments is provided. One of study in this direction is available at [12]

Akashdeep (✉)
UIET, Panjab University Chandigarh, Chandigarh, India
e-mail: akashdeep@pu.ac.in

but there are few missing links. Authors in this study have tried to bring insight into various entities and processes involved in the standardization process. Role of WiMAX Forum organization in promoting, liaising with industry and certification of various devices is also specified. Organization of paper is as follows: Complete development process is portrayed in next section, role of WiMAX forum and use of system and certificate profiles is elaborated in next section. Conclusions and analysis are presented in the last section.

2 Advancements in IEEE 802.16 Standard

Many telcos initiated the idea to promote use of fixed broadband networks for providing Internet connectivity to businesses and individuals. The outcome of these findings led to formation of National Information Infrastructure and Local Multi-point Distribution Service (LMDS) bands with ranges 5–6 and 30 GHz. A need was felt by wireless community to standardize networks operating in such range that eventually paved way for IEEE 802.16 standard. Origin of standard and its growth is divided into four different stages covering entire life span of standard with different amendments and revisions.

2.1 Stage 1: Origin of Standard and Initial Years (1998–2003)

Project P802.16 was created by IEEE 802 Study Group established in 1998 to work on development of Broadband Wireless Access (BWA) and approved specification for interoperable LMDS in 1999. LMDS obtained consideration of investors as it provided broadband internet with other entertainment services but it failed as there was not any uniform standard for its access. Then IEEE 802.16 Working Group was erected by disbandment of this Software group (SG) to manage a new project, P802.16, on Broadband Wireless Access Standards. This project used a single carrier for air interface in 10–66 GHz and therefore was named Wireless MAC SC (single carrier). However it was renamed to P802.16.1 in 2000 so that consistency in numbering can be maintained with concurrent project, P802.16.2, developed by Task Group 2.

Project P802.16.3 which was targeted to develop air interface standard for 2–11 GHz got approval in 2000 and TG3 was constituted for its development. The project proposed three implementations for physical layer: Wireless MAN-SCa6 (Single Carrier), Wireless MAN-Orthogonal Frequency Division Multiplexing (OFDM) and Wireless MAN-Orthogonal Frequency Division Multiple Access (OFDMA). It was agreed to use a single MAC protocol running over different physical layer options therefore all air interface projects were intended to be

brought under one standard namely 802.16. A separate amendment was developed for each additional air interface specification. Goals of P802.16b were integrated in P802.16a and the former was withdrawn. Finally, IEEE Std 802.16-2001 was born in 2001 and was published in April 2002.

The standard was amended with IEEE 802.16-2001c “detailed system profiles for 10–66 GHz” and set of predefined parameters were included to provide interoperability support. It was the first amendment to IEEE 802.16-2001 which aimed for wireless networks operating on licensed radio frequency bands. A second amendment to current standard was made in form of IEEE Std 802.16a-2003. Certain modifications to MAC were made and additional physical layer specifications for 2–11 GHz were included. This standard was not affected by rain attenuation and operated in NLOS (Non-Line-of-Sight) environment which led to reduction in installation of antennas. IEEE 802.16a supported mesh network modes of operation that broadens basic 802.16 transmission range by passing single communication from one transceiver for providing guaranteed QoS to support voice and video messages.

2.2 Stage II: First Major Revisions to Standard (2003–2008)

In 2002, a new study group named as Mobile Wireless Metropolitan Area Network Study Group was established to pertain to issues of mobility. Group has to draft report on addition of mobility to existing standard considering scalability of users. This was implemented as project P802.16e as it was being handled by Task Group E. Project P802.16d was transformed into revision project to accommodate all revisions and renamed to P802.16-REVd. It led to approval of IEEE Std 802.16-2004 and IEEE 802.16-2001 and its two amendments were made obsolete. This standard offered OFDM (Orthogonal Frequency Division Multiplexing) with 256 carriers. It provides three different air-interfaces: (a) Wireless MAN-single carrier modulation (b) Wireless MAN-OFDM modulation with 256-point FFT with TDMA channel access (c) Wireless MAN-OFDMA with a 2048-point FFT. It includes two-way authentication for security purposes and supports “multihop” mesh networking to enable retransmission of packet from one node to another. Both TDD and FDD transmission mechanisms were supported by this extension.

In 2004 a new study group named as Network Management Study Group was created. This group was responsible for development of Management Information Base both mobile and fixed services. It resulted in creation of two projects P802.16f and P802.16g. The draft document proposed in P802.16f was approved as standard IEEE Std 802.16f-2005 in September 2005. IEEE 802.16-2004 underwent its first amendment that got published in December 2005. Progress made in project P802.16e which was started in 2002 eventually led to a new standard IEEE Std 802.16e-2005 that was second amendment made to standard. IEEE 802.16-2005 (IEEE 802.16e) was published in February 2006 by IEEE with frequency band of 2–6 GHz for mobility. It is also known as Mobile WiMAX. This technology adds

support for mobile subscriber stations. It would also support communication for users moving at vehicular speeds because of its technological advances of high speed signal handoffs. IEEE 802.16e has some clear advantages over 802.16-2004 as it provides support for multicast and broadcast service feature. It also supported enhanced techniques of Multiple-Input Multiple-Output (MIMO) and Adaptive Antenna System (AAS).

2.3 Stage III: Second Revision and New Amendments (2008–2013)

As P802.16-2004/Cor2 was merged into P802.16Rev2, merging of draft for P802.16Rev2 and P802.16i was also decided by IEEE working group in 2007. It led to withdrawal of project P802.16i in 2008. In Jan. 2008, an Adhoc group '16jm' was instated to study issues regarding repercussions of 802.16j and relay support. This AdHoc Group contributed to Task Group m in 2008. IEEE later in 2009 approved new revision of IEEE Std 802.16 known as IEEE Std 802.16-2009. IEEE Std 802.16-2004 was now ready to be replaced by new standard IEEE 802.16-2009. Support of single carrier physical layer no longer interested vendors, eventually leading to removal of Wireless MAN-SCa and inclusion of Wireless MAN-SC, Wireless MANOFDM and Wireless MAN-OFDMA. IEEE Standard 802.16j-2009 was approved as standard for draft developed by Relay Task Group and newly approved standard IEEE 802.16-2009 got its first revision immediately on its inception.

To improve robustness and reliability Network Robustness and Reliability (NRR) committee was approved in 2008 by 802.16 Working Group. The committee proposed creation of IEEE 802.16 GRIDMAN Study Group on 'Greater Reliability in Disrupted Metropolitan Area Networks' in 2009. The Study Group proposed an amendment to IEEE 802.16 on Higher Reliability Networks, which was approved in 2010 as project P802.16n. Work on license exempt TG was started in 2004 but no progress was made in this project even after four years of its inception which is the maximum life time period for any project assessment report. Two extensions were already granted to it and it was facing closure. However this licence exempt work group was able to develop project P802.16h and IEEE SASB approved it as standard 802.16h-2010 in 2010. In order to investigate future network challenges and possibilities, a new Project planning group was formed in November 2009. This Project Planning AdHoc group began drafting a machine-to-machine (M2M) Communications study report in 2010 and IEEE Project planning committee was formed on the basis of this group. IEEE Project Planning Committee proposed an amendment to existing IEEE Std 802.16 to enhance M2M communications. IEEE-SASB accepted it as project P802.16p. This amendment supports low power operations, small burst transmissions and was built on features in project P802.16m. Draft for project P802.16m by TG 'm' was completed as IEEE Std 802.16m-2011.

2.4 Stage IV: Current Standard and Ongoing Projects

The growth of IEEE 802.16 standard and its various amendments are shown in timeline diagram of Fig. 1. The figure shows development of various projects and evolution of standard on year wise time scale. Currently as on today (7th May 2016) following standards are active.

Active Standards

- IEEE 802.16-2012: Revision of IEEE Std 802.16, including IEEE Std 802.16h, IEEE Std 802.16j, and IEEE Std 802.16m
- IEEE Std 802.16p (First Amendment to IEEE Std 802.16-2012): Enhancements to Support Machine-to-Machine Applications; 2012-10-08
- IEEE Std 802.16n (Second Amendment to IEEE Std 802.16-2012): Higher Reliability Networks; 2013-03-06;
- IEEE Std 802.16q (Third Amendment to IEEE Std 802.16-2012): Multi-tier Networks; 2015-02-16;
- IEEE 802.16.1-2012: Wireless MAN-Advanced Air Interface for Broadband Wireless Access Systems, 2012-09-07
- IEEE Std 802.16.1b (First Amendment to IEEE Std 802.16.1-2012): Enhancements to Support Machine-to-Machine Applications; 2012-10-10
- IEEE Std 802.16.1a (Second Amendment to IEEE Std 802.16.1-2012): Higher Reliability Networks; 2013-06-25
- IEEE Std 802.16k-2007

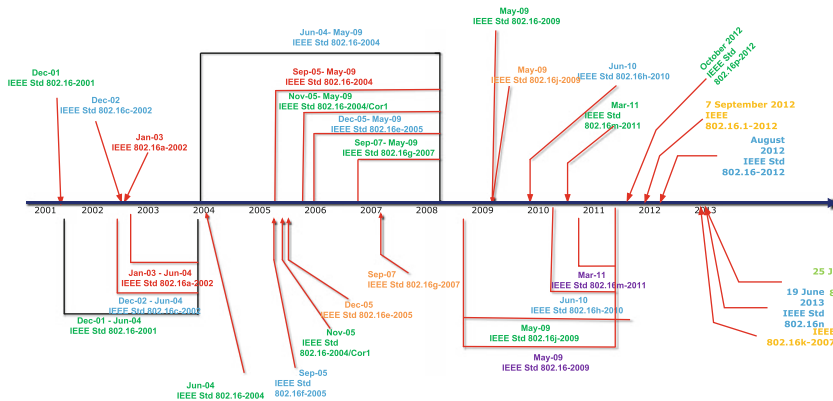


Fig. 1 Timeline for development of standard IEEE 802.16

3 WiMAX Forum

WiMAX forum is an organization with telecom operators and equipment manufacturers as its members looking after development of WiMAX and makes specifications for design of equipments. It issues ‘WiMAX Forum certified’ labels to products of equipment manufacturers developed in compliance with IEEE 802.16 standard. Technical Activities are organized with help of number of working groups within WiMAX Forum [13], Table 1 and harmonized by Technical Steering Committee.

3.1 Certification Process

WiMAX forum has established Test suites and testing laboratories to test vendor equipment and issue WiMAX Forum Certified Label to equipments. There are three WiMAX Forum Designated Certification Laboratories (WFDCL) [13] as compared to six listed by [11]. A vendor submits equipment with a certification profile and Protocol Implementation Conformance Statement (PICS) and a Protocol Implementation Extra Information for Testing (PIXIT). PICS is questionnaire defined by

Table 1 Working groups within WiMAX forum

Working group	Major role
Service Provider Working Group (SPWG)	Coordinate between ISP, WG and WiMAX Forum Board recommendation, requirement for network, air interface specifications
Aviation Working Group	Use of WiMAX in Air and Aviation Applications
Technical Working Group (TWG)	technical product specifications and certification test suites development for air interface based on OFDMA PHY
Smart Energy Working Group (SEWG)	<ul style="list-style-type: none"> – Promotion of WiMAX for smart energy applications like mining – Seek inputs from Oil, Gas and mining industry for development of WiMAX
Network Working Group (NWG)	– Create end-to-end networking and network interoperability (NWIOT) specifications for all WiMAX systems
Global Roaming Working Group (GRWG)	Assure availability of global roaming service for WiMAX technology in a timely manner as demanded by the marketplace
Regulatory Working Group (RWG)	To Influence worldwide regulatory agencies to promote WiMAX-friendly, globally harmonized spectrum allocations
Certification Working Group (CWG)	Manage WiMAX Forum Certification Program through selection and oversight of certification test labs

WiMAX Forum and is to be filled by vendor while PIXIT provides information on equipment configuration. Test suites and Certification Requirements Status List (CRSL) relevant to submitted product are identified. MAC, PHY layer capabilities are tested by RCT (Radio Conformance Testing), PCT (Protocol conformance testing), MIOT (Mobile Interoperability Testing) while NCT, IIOT are used to target upper layer capabilities with WiMAX Forum Network specification. Results are reviewed by WiMAX Certification Body to acknowledge product certification. It is also added to WiMAX Forum Certified Product Registry.

4 Conclusion

Study has presented an in depth coverage of evolution of projects, groups and progress of standard. The innovations in standard led to shift of interest from 10–66 to 2–11 GHz spectrum in early years. Adaption and addition of new features like mobility with multiple PHY layer technologies have been key elements in success of standard. Growth of standard is presented in four different stages describing additions and deletions made at appropriate time. Currently as of today, May 2016, IEEE 802.16-2012 which is revision of IEEE 802.16, including 802.16h, 802.16j, 802.16m is applicable. Working of WiMAX Forum and various working groups within it is also elaborated. The present paper is helpful to researchers and vendors looking to participate in certification or standardization process.

References

1. IEEE, 2010. Draft IEEE Standard for Local and metropolitan area networks Corrigendum to IEEE Standard for Local and Metropolitan Area Networks- Advanced Air Interface. IEEE P80216m/D10, November 2010. 2010: 1–1132.
2. Ahmadi, S. 2009. An overview of next-generation mobile WiMAX technology, *IEEE Communication Magazine*, 47(6), 84–98.
3. Etemad, K. 2008. Overview of mobile WiMAX technology and evolution. *IEEE Communication Magazine*, 46(10), 31–40.
4. Eklund, C., Marks, R., Stanwood, K., and Wang, S. 2002. IEEE standard 802.16: a technical overview of the Wireless MANTM air interface for broadband wireless access, *IEEE Communication Magazine*. 40(6), 98–107.
5. W. Kim.2009. Mobile WiMax, the leader of the mobile Internet era [WiMAX Report]. *IEEE Communication Magazine*, 47 (6), 10–12.
6. D. Pareek. *The business of WiMAX*. Wiley, 2006, ISBN-13 978-0-470-02691-5.
7. Akashdeep, Kahlon, K.S. and Kumar H., 2014. Survey of Scheduling Algorithms in IEEE 802.16 PMP networks. *Egyptian Informatics Journal*, 15(1), 25–36.
8. J. G. Andrews, A. Ghosh, and R. Muhamed, *Fundamentals of WiMAX: Understanding Broadband Wireless Networking*. Pearson Edu., 2007.
9. Nuaymi, L. *WiMAX: Technology for Broadband Wireless Access*. John Wiley & Sons, 2007.
10. Prasad R. and Velez, F. J. *WiMAX Networks - Techno-Economic vision and challenges*. Springer, 2010, ISBN 978-90-481-8751-5.

11. Bacioccola, Cicconetti, C., Eklund, C., Lenzini, L., Z. Li, and Mingozi, E.2010. IEEE 802.16: History, status and future trends. *Computer Communications*, 33 (2), 113–123.
12. <http://www.wimaxforum.org/about/working-groups>.
13. <http://www.wimaxforum.org/certification/designated-labs>.

Mutual Trust Relationship Against Sybil Attack in P2P E-commerce

D. Ganesh, M. Sunil Kumar and V.V. Rama Prasad

Abstract In recent years E-commerce has been developing rapidly. There are a huge number of areas where E-commerce can be used. There are also some peer to peer E-commerce applications that have been developed recently. These applications due to their openness, anonymity, decentralized nature, scalability is prone to huge variety of attacks that include both active and passive attacks. These attacks have been leading to the decrease of the reputation of the E-commerce organization and may also lead to financial loss or loss of information. One such attack is Sybil attack an active attack where a peer may try to forge its identity or obtain another identity by false means. With those Identities a peer can listen to the transactions of other peers and also he can manipulate the messages that are to be forwarded to the other peers in the peer to peer network. In this paper, we propose a mutual trust based network, thus diminishing the Sybil attacks.

Keywords Mutual trust relationship · Sybil attack · Peer to peer networks · E-commerce

1 Introduction

Peer to peer networks have wide range of applications. There can be communication systems, content rating systems, File sharing systems and also Ecommerce websites. These systems are user friendly and user can be able to use those applications easily. These peer to peer networks are popular for their openness, anonymity, self-organization, decentralized nature [1], scalability and fault

D. Ganesh (✉) · M. Sunil Kumar · V.V. Rama Prasad
Department of CSE, Sree Vidyanykethan Engineering College, Tirupati, India
e-mail: dgani05@gmail.com

M. Sunil Kumar
e-mail: sunilmalchi1@gmail.com

V.V. Rama Prasad
e-mail: vvrmaprasad@rediffmail.com

tolerance. Those activities will degrade the reputation of the system and also may lead to the damage to the peers in the network. These malicious peers can degrade the behaviour of the system. The cost of creating an identity in this type of systems is easy and so, malicious peers may use this opportunity to launch a Sybil attack. The number of identities that these attackers may create will depend on the computation power [2] of the peer as well as its band width. Forged identities or the identities obtained by a malicious peer are called Sybil peers. A Sybil identity [3] can be an identity owned by a malicious user, or it can be a bribed or stolen identity obtained through a Sybil attack. These identities can be used to obtain some kind of profit in any form by damaging a certain honest user. These Sybil peers can attack at both application level and overlay level. In this paper we propose a mutual trust based system which uses the trust of peers to determine a peer's trustworthiness. This will allow the peers to exist in groups based on interest thus making the neighbours more acquainted to each other. This will reduce the Sybil attacks in the system. Peers can identify each other based on the identifiers they obtained when they initially come into contact. Those identifiers may be used to digitally sign the transactions between those peers.

We further propose a centralized admission control as long as the peers have been partially admitted in a group. Our approach is based on mutual trust between the peers. This e-commerce system is based on interest among the peers. Peers are able to monitor each other using the historical behaviour of a peer. We propose mutual trust that can identify and eliminate Sybil peers. Sybil peers will have their trust cancelled and will be eliminated from the network.

2 Models

2.1 Network Model

We consider network of peers which have open and anonymous characteristics. Peers can take decisions on the trust to another peer [1] only if it is the member of the group. A graph G is a tuple $\langle V, E \rangle$, where V is the set of vertices and E is the set of edges. $V = \{v_1, v_2, v_3, \dots, v_x\}$ are the peers in the network and $E = \{e_1, e_2, e_3, \dots, e_y\}$ are the edges in the network. Only the neighbours of a peer can establish a link among them. If there is a link from v_i to v_j , it means there is also a link from v_j to v_i . If there is a link from v_i to v_j , then v_i is called trustor and v_j is called trustee.

Each peer maintains a set of identifiers to its neighbours which are unique for a neighbour. Peers can broadcast any packets in the network and the neighbours help it to spread those packets to all the peers in the network. Peers send messages to each other if they know the identifiers of each other. Each edge in the network represents a mutual trust in the network and will have a trust value $t(v_i, v_j)$ associated with it. Alternatively we can use the method in [2] where the adjacency is

determined the value of a_{ij} that is if the value of a_{ij} is equal to 1 then they v_i and v_j otherwise they are not adjacent.

2.2 Attack Model

In this paper, we focussed on the Sybil attack an active attack where an attacker will possess multiple identities and uses those identities to mislead other honest peers in the network. In this an attacker may obtain some personal information of the honest peers or may gain some financial profit from the honest peers. In this paper we focus on the peer to peer e-commerce. When a peer is compromised, all the information will be extracted. In this approach we use mutual trust between the interest peers to address these Sybil attacks. Mutual trust is scalable and efficient in peer to peer e-commerce network (Fig. 1).

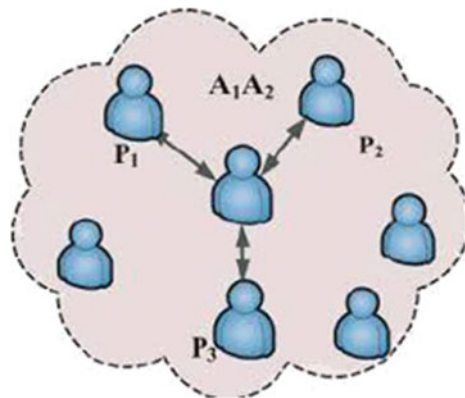
3 Preliminaries

For more details about the preliminaries, please refer to references.

4 Proposed Approach

In our approach there are two parts, one deal with the detection of Sybil attack and the other deals with the spreading of the trust among the peers in the network. Our algorithm will address the Sybil attack by using the mutual trust between the interest peers in the network. Peers can trade with each other even if are Sybil

Fig. 1 Detection of Sybil attack



or not. Peers will have identifiers that may uniquely identify a peer in the network. Our algorithm can be used to test the suspected peer whether it is a Sybil or not.

4.1 Computation Model

In this approach establishing a link between two peers will depend on the trust of the peers on the common neighbours of both peers. If trust of the two interested peers on a common neighbour has a lot of difference then we can assume that the peer can be a Sybil peer and so the link cannot be established between the peers with the Sybil peer as an intermediate node. Thus the edges in the network are keenly monitored and most of the edges that may result to Sybil attacks are not allowed in the group (Fig. 2).

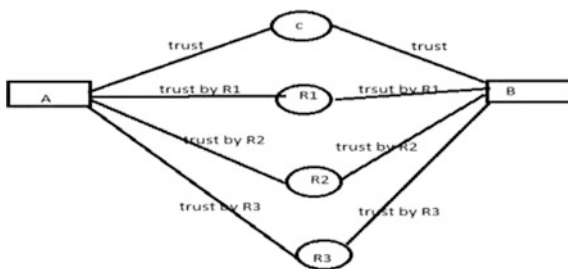
4.2 Dangers from the Compromised Peers

Sybil peers can compromise [4] the geographical routing in the group peer to peer network. Compromised peers may collude and can make an honest peer to appear as a Sybil peer by giving false recommendations or badmouth. Sybil peers may also modify the data that it has to forward to other peers in the network and can mislead the destination peer. Sybil attack peers can create more non-existing links in the network [5] by creating more bogus identities in the system. Sybil peers can obtain fair amount of private information of a honest peer by impersonating itself as some other honest peer.

4.3 Cooperation Among Neighbour Peers

Some peers may be malicious and selfish which will damage the normal functioning of the network. Peers must cooperate to communicate, discover, maintain the routes

Fig. 2 Mutual trust computational model



to other peers, and forward packets to their neighbours. In this cooperation some peers may collude and do malicious transactions.

4.4 Mutual Trust Relationship

Our approach is two-fold: Initially each peer acts as an identifier source which will help for the distribution of identifiers to the rest of the peers in the network and the second phase in which neighbours cooperation is used to detect a peer to be a sybil or not. Our method advocates peers can belong to many groups but has a base group which is the first group it joined unless it has decided to change, which is out of scope of our work. Mutual trust is derived from the similarity of the same set of neighbours based on interest in a pair of peers, i.e., p_i and p_j . We use the Jaccard metric in which the similarity of peer_i and peer_j is defined as follows:

$$mut(p_i, p_j) = \frac{|p_i \cap p_j|}{|p_i \cup p_j|} \quad (1)$$

where $|p_i \cup p_j| = 0$. If $mut(p_i, p_j)$ is not smaller than the similarity threshold S , then the interests of peer_i and peer_j are similar. The similarity relationship is symmetric, i.e., $mut(p_i, p_j) = mut(p_j, p_i)$. If N_i is the set of peer p_i 's neighbours, and N_j is the set of peer p_j 's neighbours. N_{ij} is the set of common neighbours of p_i and p_j assuming that the feedback is given by the peers which trade with that peer, hence $N_{ij} = p_i \cap p_j$, which are in the same or different groups [6] defined as $N_{ij} = p_i \cup p_j$. S_{ij} is the similarity between p_i 's and p_j 's trust value, about the same set of neighbours. It can be defined by the feedback of p_i 's and p_j 's trust value about the same neighbours. If $L(i, j)$ represents p_i 's local feedback about p_j , this also shows p_i 's behaviour in different transactions. Considering the set of common neighbours of p_i and p_j : $N_{ij} = (H_1, H_2, \dots, H_n)$. Assuming that $L(i, j)$ represents p_i 's feedback about p_j , and the p_i 's report about p_j 's behaviour, which equates as the trust value, then: $Q_i = L(i, H_1), L(i, H_2), \dots, L(i, H_n)$ is the p_i 's trust vector about neighbours; $Q_j = L(j, H_1), L(j, H_2), \dots, L(j, H_n)$ is p_j 's trust vector.

Suppose M_{ij} is the similarity between p_i and p_j trust values, about the same set of neighbours, and defined as the cosine angle between Q_i and Q_j , then M_{ij} is calculated as follows:

$$M_{ij} = \frac{\sum_{x \in N_{ij}} (nL)_{ix} \times (nL)_{jx}}{\sqrt{\sum_{x \in N_{ij}} (nL)_{ix}^2 \sum_{x \in N_{ij}} (nL)_{jx}^2}} \quad (2)$$

4.5 Detection of Sybil Attack Based on Mutual Trust Relationship

Malicious peer will create more forged identities which do not physically exist in the network, in order to mislead the honest peers. We assume there are three kinds of peers in the system. They are Sybil peers, honest peers and malicious peers. We compare the physical neighbours of a peer based on the ip address and if those identities have same set of neighbours then we determine those peers to be Sybil peers and will be expelled from the group.

When Sybil attack happens, A_1 and A_2 will both send messages.

$$\begin{array}{c} A_1 \quad A_2 \\ \frac{M_{P1}}{M_{P2}^{A1}} = \frac{M_{P1}}{M_{P2}^{A2}} \end{array} \quad (3)$$

$$\frac{M_{P1}^{A1}}{M_{P3}^{A1}} = \frac{M_{P1}^{A2}}{M_{P3}^{A2}} \quad (4)$$

If Eqs. (3) and (4) are correct, Sybil attack must have happened, for the exclusive geographical position with two Ids.

5 Trust Computation Among Neighbour Peers

Algorithm: Computation Cost

1. **Input:** Graph $G = (V, E)$, v_i, v_j , and the Trust
2. value $i, j, n, C(v_i, v_j)$
3. **Output:** $C(v_i, v_j)$
4. **For** $i \leftarrow 1$ **until** n **do** $C_{ii}^0 \leftarrow 1 + l(v_i, v_j)$;
5. **For** $1 \leq i, j \leq n$ and $i \neq j$ **do** $C_{ij}^0 \leftarrow l(v_i, v_j)$;
6. **For** $k \leftarrow 1$ **until** n **do**
7. **For** $1 \leq i, j \leq n$ **do**
8. $C_{ii}^k \leftarrow C_{ii}^{k-1} + C_{ik}^{k-1} \cdot (C_{kk}^{k-1})^* \cdot C_{ki}^{k-1}$
9. **For** $1 \leq i, j \leq n$ **do** $c(v_i, v_j) \leftarrow C_{ii}^n$
10. **end**

5.1 Eliminating Sybil Communities

In NP-complete problem we will find all subgraphs where as in neighbour similarity trust we will find the groups. So that relationship between two peers by neighbour similarity trust can be explained as NP-complete. This can be represented as neighbour similarity of peer $p_i \cap p_j$.

$$S(p_i, p_j) = \begin{cases} -1 & +ve \text{ test} \\ \frac{|p_i \cap p_j|}{\min\{|p_i|, |p_j|\}} & -ve \text{ test} \end{cases} \quad (5)$$

where -1 represents that \cap are distinct and \cap represents the set of common similarity peers $|.$ represents the size of a set or length.

5.2 Accepting Honest Peers

If the trust level decreases then other peers may loose confidence with the peer. Peers must offer benefits before doing any transactions in order to prove themselves as honest peers. If a random route visits the same peer more than once, the existing edges will be correlated. This is a feature in P2P e-commerce [7].

6 Security and Performance Analysis

6.1 Security Analysis

Here we are going to construct the SybilTrust which is the neighbour similarity trust by use of controller in the peers. The controller in the peers only admitted the honest peers. This SybilTrust illustrate that controller checks whether the peers had similarity or not. If peer doesn't have similarity it is said to be a Sybil attack peer. One more method is using in the SybilTrust is pairing method. It improves the authentication and trust worthiness of the system. So all neighbours are provided with authentication with the help of secret key. We evaluate the performance of the sybiltrust using two metrics namely Non-trustworthy rate and detection rate. Detection rate is the proportion of detected Sybil peers to total sybil peer communication cost.

We ran an experiment with 50 peers involving in 50 simulation runs resulting in total of 2500 interactions. So In this p2p e commerce group has a total 50 different categories of interest. The transaction between peers with similar interest can be defined as successful or unsuccessful, expressed as positive or negative. Hence, the

honest peers [18] are going to test more times, the chances that honest peers are erroneously determined as Sybil increases and finding the Sybil peers are also increased.

7 Conclusion

We presented Mutual trust relationship, a Sybiltrust which defence against Sybil attack in p2p e-commerce. Our approach is based on mutual relationship among peers in a group P2P e-commerce community by comparing all other approaches. This approach exploits the relationship among peers and results authenticate system. We also providing better defence mechanism. Mutual trust relationship helps to find out the Sybil peers and isolate the Sybil peers in honest groups.

References

1. J. Douceur, "The sybil attack," in Proc. Revised Papers 1st Int. Workshop Peer-to-Peer Syst., 2002, pp. 251–260.
2. A. Mohaisen, N. Hopper, and Y. Kim, "Keep your friends close: Incorporating trust into social network-based Sybil defenses," in Proc. IEEE Int. Conf. Comput. Commun., 2011.
3. H. Yu, C. Shi, M. Kaminsky, P. B. Gibbons, and F. Xiao, "DSybil: Optimal Sybil-resistance for recommendation systems," in Proc. IEEE Symp. Security Privacy, 2009, pp. 283–298.
4. B. Yu, C. Z. Xu, and B. Xiao, "Detecting Sybil attacks in VANETs," J. Parallel Distrib. Comput., vol. 73, no. 3, pp. 746–756, Jun. 2013.
5. A. Mislove, A. Post, K. Gummadi, and P. Druschel, "Ostra: Leveraging trust to thwart unwanted communication," in Proc. th USENIX Symp. Netw. Syst. Des. Implementation, 2008, pp. 15–30.
6. H. Yu, M. Kaminsky, P.B. Gibbons, and A. Flaxman, "SybilGuard: Defending against Sybil attack via social networks," IEEE/ACM Trans. Netw., vol. 16, no. 3, pp. 576–589, Jun. 2008.
7. J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis and defenses," in Proc. 3rd Int. Symp. Inf. Process. Sensor Netw., Apr. 2004, pp. 1–10.
8. K. Walsh and E. G. Sirer, "Experience with an object reputation system for peer to peer filesharing," in Proc. 3rd USENIX Conf. Netw. Syst. Des. Implementation, 2006, vol. 3.
9. K. Wang, M. Wu, and S. Shen, "Secure trust-based cooperative communications in wireless multi-hop networks," in Communications and Networking J. Peng, Ed., Rijeka, Croatia: InTech, Sep. 2010 ch. 18, pp. 360–378.
10. H. Yu, P. Gibbons, M. Kaminsky, and F. Xiao, "SybilLimit: A near optimal social network defense against Sybil attack," IEEE/ACM Trans. Netw., vol. 18, no. 3, pp. 3–17, Jun. 2010.
11. A. Tversky, "Features of similarity," Psychological Rev., vol. 84, no. 2, pp. 327–352, 1977.
12. F. Musau, G. Wang, and M. B. Abdullahi, "Group formation with neighbor similarity trust in P2P e-commerce," in Proc. IEEE Joint Conf. Trust, Security Privacy Comput. Commun., Nov. 2011, pp. 835–840.
13. G. Danezis and P. Mittal, "SybilInfer: Detecting Sybil attack peers using social networks," in Proc. Netw. Distrib. Syst. Security Symp., San Diego, CA, USA, Feb. 2009, pp. 1–15.

Adaptive Block Based Steganographic Model with Dynamic Block Estimation with Fuzzy Rules

Mohanjeet Kaur and Mamta Juneja

Abstract Steganography is a technique, which can be used for the purpose of hiding the data into similar form or other form of data to create the covert channel among the internet or intranet links to protect it from the various kinds of masquerading or snooping attacks. In this paper, we have proposed the dynamic fuzzifier for the robust image embedding. The dynamic fuzzifier module (DFM) is responsible for the segmentation, selection and fuzzy weight calculation among the input cover and secret image. The embedding algorithm has been designed with the spatio-temporal ability to embed the secret data in the block edges of the cover image, while utilizing the non-overlapping block-based division. The proposed method is able to achieve better PSNR than the existing algorithm while embedding the data into the cover image.

Keywords Dynamic fuzzy rule set determination (DFRSD) • Decision logic for embedding decision (DLED) • Fuzzy weight calculation algorithm • PSNR • MSE • Embedding capacity

1 Introduction

Steganography is derived from two Greek words stegano and graphic which means “covered writing”. It is a part of information security which is used to hide the data or any object from the intruder [1, 2]. It is the technique to hide the data into another data. It is the direct derivation of the watermarking methods used for the hiding the information. It can be performed on the various forms of data like text, video, audio, etc.

M. Kaur (✉) • M. Juneja
CSE Department, UIET, Panjab University, Chandigarh, India
e-mail: kaur.mohanjeet@gmail.com

M. Juneja
e-mail: mamtajuneja@pu.ac.in

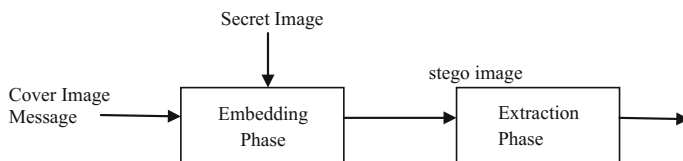


Fig. 1 Basic block diagram of steganographic system

In Fig. 1, cover image, secret image is embedded to generate the stego image and which is transformed to the receiver by using medium and then message is extracted from the stego image [2, 3].

2 Related Work

LSB based technique researched by Wang et al. [4], proposed an exhaustive search for optimal LSB substitution scheme and Canny [5], proposed a technique to substitute the same number of bits of each and every pixel of input host images for hiding the secret text or message. Then to improve the PSNR and robustness of the above method H.C. Wu et al. [6], proposed a method to use the combination of LSB and PVD approaches of steganography but in this approach there was always a need to send the Range width table at the receiver end for extraction of the original image. It was more prone to stego attacks and more distortion occurs at the receiver end during extraction.

To reduce the distortion at extraction phase for getting the original image Cheng-Hsing Yang [7], proposed steganography technique based on the adaptive LSB for the non-continuous areas of the image. PVD was used to define the continuous and non-continuous area in the image but it does not provide resistance to the attacks [7]. For providing more resistance towards the attacks Weiqi Luo et al. [8], proposed a technique of edge adaptive image steganography based on LSB matched revisited. This approach selects the embedding area, according to the size of the message which was embedded into the cover image and by PVD in two successive pixels in the original image.

Further to improve the robustness and imperceptibility, Santosh Arjun, N. and Atul Negi [9], proposed a method called adaptive steganography which uses both global feature (density, frequency, color and contrast) and local feature (pixel values) for data hiding. It was less prone to stego attacks and achieved the high embedding capacity but main disadvantage was that if order of the filter at the sender and the receiver end was not same during extraction than message decoding was not matched with the original image. Manglem Singh et al. [10], put forward a technique for hiding the encrypted data in the features of the image rather than embedding the secret data into the smooth area but the quality of the stego image was very poor. Chen et al. [11], suggested a method of high payload steganography

by using hybrid edge detection. In this method LSB substitution technique was combined with canny edge detection and fuzzy logic edge detection but implemented only at grey scale images.

Further to improve the PSNR and embedding capacity Hsien-Wen Tseng, Hui-Shih Leng [12], put forward a method of embedding data in the edge boundaries of the cover image using canny edge detection with their default threshold parameter with high PSNR. It provides more data hiding capacity at the boundaries of the image rather than embedding data at the smooth area of an image with high PSNR. It used the stego image as the native image for the object segmentation and feature extraction but provides low embedding capacity and used only for horizontal edge detection pixel boundaries.

To improve Chen et al. [11] payload capacity and PSNR Anastasia Ioannidou et al. [13], proposed a method based on high embedding capacity and hybrid edge detection for image steganography and Hussain M. and Hussain [14] suggested a method to improve the PSNR and embedding capacity using adaptive LSB technique for data hiding and fusion of canny edge detection and advanced Hough transforms used for edge pixel detection. Its embedding capacity was 60% for edge area and 50% for smooth areas and utilized 12 bits of RGB color image for embedding.

Mamta Juneja and Parvinder S. Sandhu [15], image steganography was done using high embedding capacity block based data hiding with minimum distortion using hybrid edge detection. This method used canny and fuzzy block based algorithm to embed the more covert data at the edge pixels rather than embedding at smooth area of the image but implemented it only at grey scale images. Deepali Singla and Mamta Juneja [16], in 2015 proposed a method for image steganography for color image using hybrid edge detection. LSB substitution was done by using 1-4-8 LSB and AES encryption algorithm was used.

3 Proposed Method

We have proposed the dynamic fuzzifier for the robust image embedding. The dynamic fuzzifier module (DFM) is responsible for the segmentation, selection and fuzzy weight calculation among the input cover and secret image. The DFM consists of primary two modules, where first deals with the segmentation of the input images (cover and secret), and the other evaluates the compatibility of the two segments for the data embedding. The embedding algorithm has been designed with the spatio-temporal ability to embed the secret data in the block edges of the cover image, while utilizing the non-overlapping block-based division (Fig. 2).

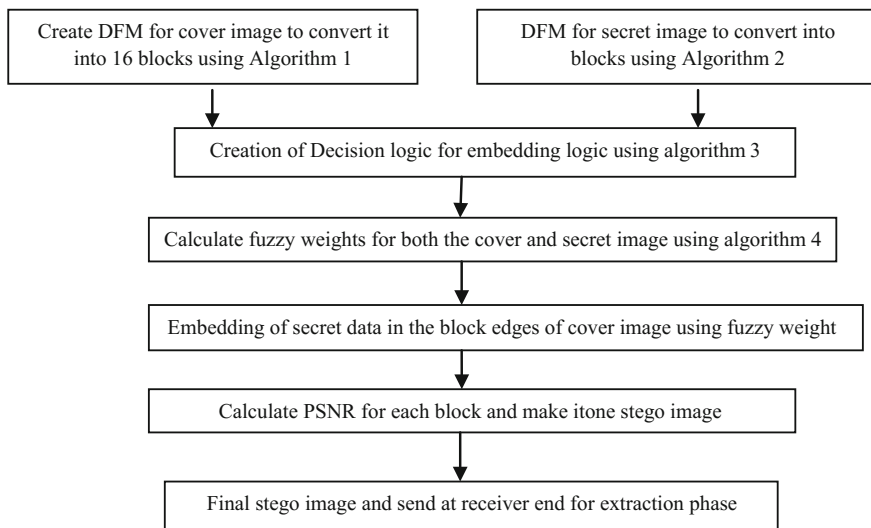


Fig. 2 Approach used embedding at sender end

3.1 Experimental Design

Dynamic fuzzy rule set determination is used for robust image embedding. The dynamic Fuzzifier module used for segmentation of cover and secret image into block and then selection of block of cover image for embedding it with secret image block using the calculation of fuzzy weight. Decision of Fuzzy weight is for embedding the block of cover image into secret image. The embedding algorithm has been designed with the spatiotemporal ability to embed the secret data in the block edges of the cover image, while utilizing the non-overlapping block-based division. In this we used four algorithms for embedding the block of the cover image with the secret image using the decision of fuzzy weight. It calculates the fuzzy weights of the blocks of cover image and fuzzy weights of the secret image then according to fuzzy weight embedding of cover and secret image done is:

Algorithm 1: Dynamic Fuzzy Rule Set Determination for Cover (DFRSD-Cover)

1. Input cover image matrix (IC_m)
 2. Calculate the image size in number of rows (C_r) and columns (C_c)
 3. Evaluate the number of rows and columns and return the estimated number of blocks
 - a. Return the horizontal dividend (CH_d) and vertical dividend (CV_d)
 - b. Return the horizontal pad value (CH_p) and vertical pad value (CV_p)
 4. Apply the padding pattern over the input image matrix according to CH_p and CV_p
 5. Initialize the 2-Level iteration counters
 6. Initialize the rotation counter and Input the round key value
 7. Calculate the vertical seed value
 - a. $vSeed=(diffV*(imx-1))+1$
 8. Calculate the vertical cap value
 - a. value $vCap=diffV*(imx)$
 9. Calculate the horizontal seed value
 - i. $hSeed=(diffH*(imy-1))+1$
 10. Calculate the horizontal cap value
 - i. $hCap=diffH*(imy)$
 11. Segment the smaller chunk from the cover image according to the $vSeed$, $vCap$, $hSeed$ and $hCap$
 - i. $CoverChunk=IC_m(vSeed:vCap,hSeed:hCap)$;
-

Algorithm 2: Dynamic Fuzzy Rule Set Determination for Secret (DFRSD-Secret)

1. Input secret image matrix (SC_m)
 2. Calculate the image size in number of rows (SC_r) and columns (SC_c)
 3. Evaluate the number of rows and columns and return the estimated number of blocks
 - a. Return the horizontal dividend (SH_d) and vertical dividend (SV_d)
 - b. Return the horizontal pad value (SH_p) and vertical pad value (SV_p)
 4. Apply the padding pattern over the input image matrix according to SH_p and SV_p
 5. Initialize the 2-Level iteration counters
 6. Initialize the rotation counter and Input the round key value
 7. Calculate the vertical seed value
 - a. $seeds=(diffV*(imx-1))+1$
 8. Calculate the vertical cap value
 - a. value $vCap=diffV*(imx)$
 9. Calculate the horizontal seed value
 - i. $hSeed=(diffH*(imy-1))+1$
 10. Calculate the horizontal cap value
 - i. $hCap=diffH*(imy)$
 11. Segment the smaller chunk from the secret image according to the $vSeed$, $vCap$, $hSeed$ and $hCap$
 - i. $secretChunk= SC_m(vSeed:vCap,hSeed:hCap,1)$;
-

 Algorithm 3: Decision Logic for Embedding Decision (DLED)

```

1. thresh1=fuzzy_weight(secretChunk);
2. thresh2=fuzzy_weight(coverChunk);
3. if thresh1<thresh2
   i. fw=thresh1/thresh2;
   ii. fw=fw*100;
4. else
   i. fw=thresh2/thresh1;
   ii. fw=fw*100;
5. end
6. if fw>fuzzyThresh
   i. Perform the embedding
7. Otherwise
   i. Embedding not permitted
   ii. Low Thresh Error. Fuzzy Logic Failed
  
```

 Algorithm 4: Fuzzy Weight Calculation Algorithm

```

1. Input the image matrix
2. Obtain the horizontal features (Hf)
3. Obtain the vertical features (Vf)
4. Perform Feature Amalgamation (Cf)
5. Obtain the constant values
6. Predict the fuzzy weight (Fw)
7. Return the fuzzy weight (Fw)
  
```

4 Results Analysis

To evaluate the performance of the steganography using three parameter [17]:

1. **Payload Capacity:** It is defined as the maximum amount of data that is embedded into the image.
2. **Robustness:** It is the message's ability to persist even after performing the operation like compression, rotation, cropping and filtering etc.
3. **Imperceptibility:** It is defined as the quality of the stego-image and which is measured using PSNR and MSE.

Peak Signal to Noise Ratio: Quality of images define by using PSNR

$$\text{PSNR} = 10 \log \left(\frac{C_{\max}^2}{\text{MSE}} \right) \dots [14]$$

Table 1 Image dataset based results of different 1 to 16 block of stego image PSNR and final PSNR of stego image have been described in the following table, Figs. 3 and 4



Cover image	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Stego image
	45.5	47	45.5	46.5	47	46	46.5	46	46.5	46.5	47.5	46	46	45.7	46	46.5	47
	45	46.5	47	46.3	47	46.7	46.8	46.9	46.4	47	45	46	45.5	46	46.5	45	46.4

Fig. 3 PSNR values for Lena image

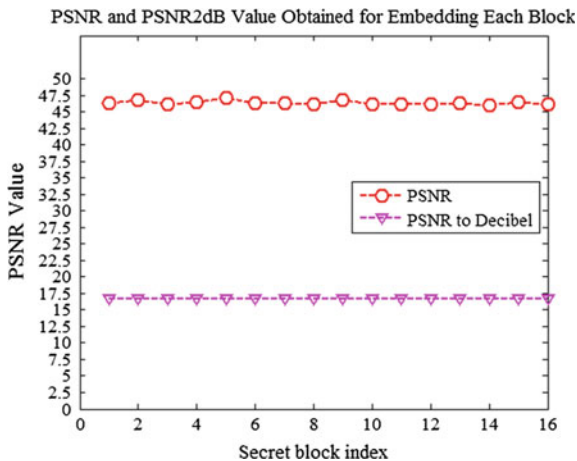
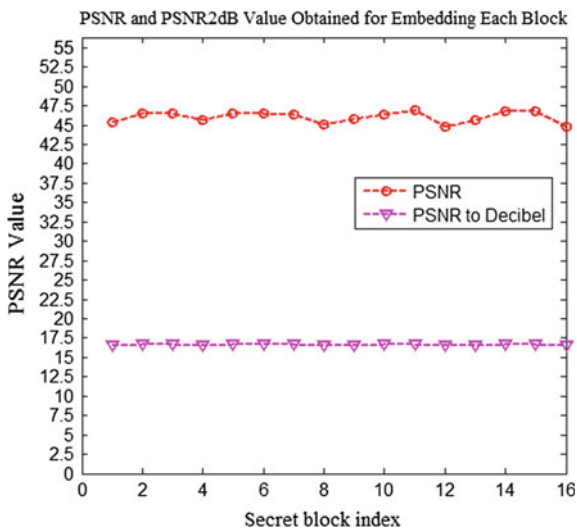


Fig. 4 PSNR values for Mandril image



Mean Square Error: This is represented by comparing error in data at received end with sender data before and after processing (Table 1).

$$MSE = \frac{1}{MN} \sum_{x=1}^M \sum_{y=1}^N (S_{xy} - C_{xy})^2 \dots [14]$$

5 Conclusion

In this paper, proposed approach achieved the goal of implementation of steganography based on dynamic fuzzy set (block based) for RGB images. In this proposed technique it contains two modules, first to convert the cover image into 16 different blocks and then the other module used to calculate the compatibility for embedding the one block of cover image to secret image block using the calculation of fuzzy weight. Further the, embedding algorithm is used to embed the secret data in the edges of block of cover image. It has achieved the target imperceptibility which is calculated using PSNR for each block of cover image and then merges the entire block after embedding it into secret image and creates the stego image. For each block, maximum 47 dB and minimum 45 dB PSNR calculated after embedding with secret data. The PSNR value of 47 dB has been recorded during the embedding of hidden object.

References

1. Artz, D.: 'Digital steganographic: hiding data within data', IEEE Int. Comput., 2001, 5, (3), pp. 75–80.
2. Lee, Y.K., Chen, L.H.: 'High capacity image steganography model', Proc. of IEEE on Vision, Image and Signal Process., vol. 147, no. 3, pp. 288–294, 2000.
3. Benlcouiri, Y., Ismaili, M., Azizi, A., and Benabdellah, M., "Securing images by secret key steganography," Applied Mathematical Sciences, vol. 6, no. 111, pp. 5513–5523, 2012.
4. Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin (2000), "Hiding Data in Images by Optimal Moderately Significant Bit Replacement" IET Electronics Letters, vol. 36, no. 25, pp. 2069–2070.
5. J. Canny, "A Computational Approach to Edge Detection," IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 8, pp. 679–687, 1986.
6. H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," Proceedings of 2005 Instrument Electric Engineering, Vis. Images Signal Process, vol. 152, no. 5 pp. 611–615, 2005.
7. Cheng-Hsing Yang, Chi-Yao Weng, Shiu-Jeng Wang, Hung-Min Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems". IEEE Transactions on Information Forensics and Security, Vol. 3, No. 3, pp. 488–497, 2008.
8. Weiqi luo, member, IEEE, fangjun huang, member, IEEE et al., "edge adaptive image steganography based on LSB matching revisited", IEEE transactions on information forensics and security, vol. 5, no. 2, June 2010.
9. Santosh Arjun, N. and Atul Negi, "A Filtering Based Approach to Adaptive Steganography," 10th Conference, TENCON 2006, IEEE, pp. 1–4, Nov 2006.
10. Manglem Singh, Birendra Singh, Shyam Sundar Singh, "Hiding Encrypted Message in the Features of Images", IJCSNS, VOL. 7, No.4. April, 2007.
11. Chen, W.-J., Chang, C.-C., and Le, T., "High payload steganography mechanism using hybrid edge detector," Expert Systems with Applications, vol. 37, no. 4, pp. 3292–3301, 2010.

12. Hsien-Wen Tseng, Hui-Shih Leng, "high-payload block-based data hiding scheme using hybrid edge detector with minimal distortion", *IET Image Process*, Vol. 8, Iss. 11, pp. 647–654, 2014.
13. Anastasia Ioannidou, Spyros T. Halkidis, George Stephanides, "A novel technique for image steganography based on a high payload method and edge detection", *Expert Systems with Applications*, Vol. 39, pp. 11517–11524, 2012.
14. Hussain, M. and Hussain, "Embedding data in edge boundaries with high PSNR", *Proceedings of 7th International Conference on Emerging Technologies (ICET 2011)*, pp. 1–6, Sept 2011.
15. Mamta Juneja and Parvinder S. Sandhu, "A New Approach for Information Security using an Improved Steganography Technique," *J Inf Process Syst*, vol. 9, no. 4, 2013.
16. Deepali Singla and Mamta Juneja, "Hybrid Edge Detection-Based Image Steganography Technique for Color Images", *Intelligent Computing, Communication and Devices, Advances in Intelligent Systems and Computing*, Springer India, 2015.
17. Wu, D.C., and Tsai, W.H.: 'A steganographic method for images by pixel-value differencing', *Pattern Recognit. Lett.*, 2003, 24, (9–10), pp. 1613–1626.

Secure Geographical Routing Using an Efficient Location Verification Technique

S.L. Aruna Rao and K.V.N. Sunitha

Abstract MANET is a dynamic network which is formed by autonomous system of mobile nodes which are autonomous in nature and are connected through links which are wireless and does not support a fixed infrastructure and hence are called infrastructure less networks. Since MANET has a mobile topology and it purely depends on intermediate nodes to relay messages, position of nodes keeps changing from time to time. During data transmission several nodes enter and leave the network. As a result, MANETs are vulnerable to several attacks in which the attackers get access to the network through malicious nodes entering the network in disguise of valid nodes. Hence, in MANETs it is necessary to verify the nodes before using them to forward data packets/messages. In this paper we estimate the position of the nodes before using them as forwarding nodes, and once it is verified for authenticity we then use them for transmitting data packets hence ensuring secure routing while transmission.

Keywords MANET • SGRPVT • SLVP • Performance metrics

1 Secure Geographical Routing in MANET

Geographic routing is considered as the method of finding the routes to gather the location information about every node in order to take decisions related to traffic forwarding. Location information obtained from the strength of the collected signals transmitted by the source, surrounding node, destination nodes and intercepted by the GPS, location is updated by the satellite, instead of using infrastructure to specify certain paths. In order to use position-based routing protocol, details related to the location of every destination node, surrounding node should be present as the

S.L. Aruna Rao (✉) · K.V.N. Sunitha
BVRIT Hyderabad College of Engineering for Women, Bachupally, Hyderabad, India
e-mail: arunaraosl@gmail.com

K.V.N. Sunitha
e-mail: k.v.n.sunitha@gmail.com

message is forwarded to surrounding node within transmission range that lies nearer to the destination node.

1.1 Position Verification Technique for Secure Geographical Routing in MANET

A position verification technique is used to authenticate the accuracy of the given information related to the node position that is collected in the neighbor table and avoid every possible erroneous information related to the node position that may lead to incorrect forwarding decisions as a result of the malicious nodes. Hence the major concern is precision of the selected nodes as proper neighbors or not, so as to avoid the hackers from misleading the nodes into selecting the malicious non neighbors as neighbors. Ensuring that the node considered as a neighbor is actually a neighbor node is important in neighborhood discovery process and is called as verification. Based on reliable and dependable nodes, the neighbor verification techniques are performed, because these nodes are considered to be present for the validation of the other nodes as required by the controlling mechanism [1, 2].

2 Literature Review

Hsu and Lei [3] have presented A Geographic Scheme with Location Update for Ad Hoc Routing utilizing topology based routing and not on the basis of the flooding mechanism. Defrawy and Tsudik [4] have presented an Anonymous Location-Aided Routing in Suspicious MANETs. In this technique, Location Announcement Message is broadcasted by every node which consists of fields like location, time-stamp, temporary public key and a group signature. Lo et al. [5] have presented a Geographical Forwarding Scheme for Vehicular Ad Hoc Networks with Location Verification to find forwarding node so as to choose a proficient and steady vehicle such that it can be used as a forwarding vehicle in the network.

3 Proposed Position Verification Technique for Secure Geographical Routing

3.1 Overview

We propose a position verification technique in order to validate the claimed locations. Location of neighbour i.e. Target Node (TN) is computed based on distance measurements in the presence of measurement errors using (2) from [6] by

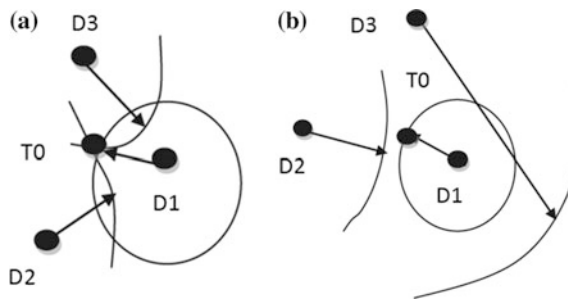
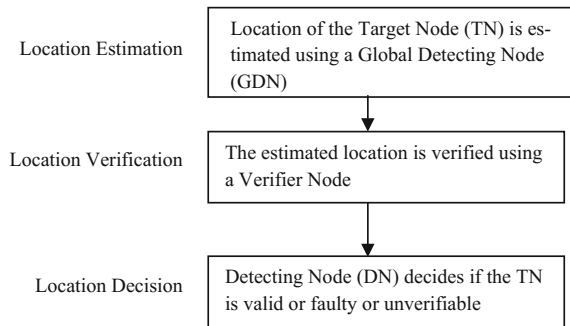
Fig. 1 Block diagram

Fig. 2 **a** In an ideal situation. **b** With measurement errors. *Dark circle* indicates the nodes (D1, D2, D3, T0). **a** is a situation which is ideal since propagation of signal circles cross at one point representing a unique location. **b** is a situation which is practical and has errors in the signal distances, hence the circles do not cross at one single point; in fact, they might not be able to cross at any point. Hence this scenario represents a situation where we may not be able to obtain a location with acceptable accuracy

computing the distance between every pair of nodes which are communicating among its neighbourhood in which MSE is used to evaluate and identify the location of target node whether TN is a malicious or benign. After estimating the location, process of location verification is started to verify the given location claim of target node by enabling the Detecting Nodes that performs verification test from [7] using the result (2) of computed distance. According to verification test target node is regarded as either Verified if be a benign node or faulty if have an incorrect position by Detecting Nodes otherwise the node deems as unverifiable and hence may not be proven to be either genuine or erroneous due to inadequate information (Fig. 1).

3.2 Computation of Node Location

In this section, the location of the Target Node (TN) is estimated considering that measurement errors can be present, for every pair of Detecting Nodes (DN) and Target Nodes (Fig. 2).

The location estimation process is described in Algorithm 1

Algorithm 1

1. D_1 initially sends a request to T_0 to remove error from the $dist_{sig0}$.
2. But since T_0 is a malicious node, it would not remove the error.
3. $dist_{eucl1}$ between D_1 and D_m is calculated. D_m can accurately localize D_1 and T_0 , hence $dist_{eucl1} \approx dist_{sig1}$ and $dist_{eucl0} \approx dist_{sig0}$.
4. $dist_{sig1}$ is measured.
5. $error_{meas1}$ is calculated based on $dist_{eucl1}$.
6. D_m is located at far away distance, D_1 and T_0 are situated close to each other. Hence the error at D_1 and T_0 can be considered to be similar i.e., $error_{meas1} \approx error_{meas0}$.
7. Remove the $error_{meas1}$ from $dist_{sig0}$ (as $error_{meas1} \approx error_{meas0}$).
8. Therefore, after the error removal, distance is given by $dist_{error_free} = dist_{sig0} - error_{meas0}$ when calculated at the GDN and $dist_{error_free} = error_{meas0}$ when calculated at the DN.
9. Location estimation of the node is given by

$$f_i(x_o^e, y_o^e) = dist_{error_free} - \sqrt{(x_o^e - x_i)^2 + (y_o^e - y_i)^2}.$$

3.3 Location Verification Mechanism

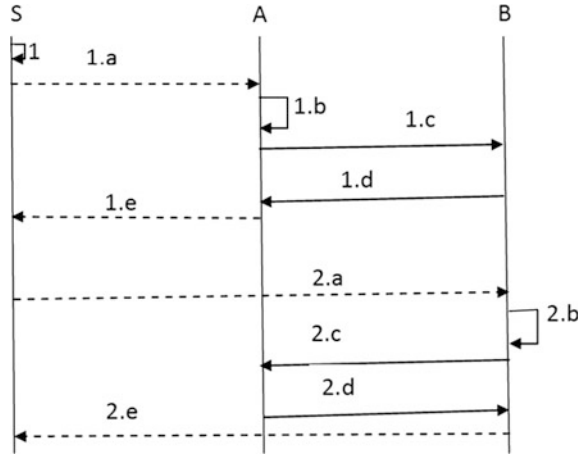
A unique mechanism for validation is used which allows source node in the network to verify whether the position of best candidate node corresponds to the position information stored at its neighbors table. In this validation mechanism, source node is generally assigned as a verifier that initiates the validation mechanism (Fig. 3).

The location verification process is described in Algorithm 2

Algorithm 2

1. S selects two candidates: target node T_0 and another node B with maximum score based on an algorithm in [7].
2. S sends PVR to T_0 and B as shown in step 1.a and 2.a.

Fig. 3 Location verification mechanism



3. After the reception of PVR request by S, the candidate T_0 and B confirm each other's location which is provided by S across their own neighbor table as specified in step 1.b and 2.b to check whether the position pointed by the verifier S matches to the position information stored in their neighbor table.
4. After initial verification, candidate T_0 and B send another PVR to each other requesting for their location indicated in step 1.c and 2.c.
5. Upon receiving the request, T_0 and B responds by generating a reply message as mentioned in step 1.d and 2.d contains its latest GPS coordinates which is provided to each other with its true positions.
6. T_0 , B sends its location information to S as shown in 1.e and 2.e.
7. Radio signals transmitted by satellite might be distorted at troposphere and the ionosphere.

A set of desirable GPS location $(x; y)$ is depicted as:

$$[S_a^x - B(T_0x)]^2 + [S_a^y - B(T_0y)]^2 \leq \Delta a^2$$

$$[S_b^x - T_0(Bx)]^2 + [S_b^y - T_0(By)]^2 \leq \Delta a^2$$

$$T_0(B) = (\max(PVR_b^x, T_{0b}^x), \max(PVR_b^y, T_{0b}^y))$$

$$B(T_0) = (\max(PVR_a^x, B_a^x), \max(PVR_a^y, B_a^y))$$

8. S merges both results obtained during verification and finds out whether the candidate node that has secured the highest score is at the correct position and as well fits itself to be the next node to be forwarded.

9. For this, cosine similarity measure is used to detect the resemblance between the position determined by verifier S and candidate node A and B. The resemblance is defined as follows:

$$\cos(\theta_{ini}) - \cos(\theta_{ver}) \leq \beta$$

where β is the resemblance coefficient of difference and closer to 0 means its better. The initial cosine angle is defined as follows:

$$\cos(\theta_{ini}) = \frac{\vec{SS}_{T_0} \cdot \vec{SB}_{T_0}}{|\vec{SS}_{T_0}| |\vec{SB}_{T_0}|} = \frac{(S_a^x - S_s^x) \cdot (B_a^x - S_s^x) + (S_a^y - S_s^y) \cdot (B_a^y - S_s^y)}{\sqrt{(S_a^x - S_s^x)^2 + (S_a^y - S_s^y)^2} \sqrt{(B_a^x - S_s^x)^2 + (B_a^y - S_s^y)^2}}$$

The cosine angle of the verify angle is defined as follows:

$$\cos(\theta_{ver}) = \frac{\vec{SS}_{T_0} \cdot \vec{SB}(T_0)}{|\vec{SS}_{T_0}| |\vec{SB}(T_0)|} = \frac{(S_a^x - S_s^x) \cdot (PVR_a^x - S_s^x) + (S_a^y - S_s^y) \cdot (PVR_a^y - S_s^y)}{\sqrt{(S_a^x - S_s^x)^2 + (S_a^y - S_s^y)^2} \sqrt{(PVR_a^x - S_s^x)^2 + (PVR_a^y - S_s^y)^2}}$$

where $\cos(\theta_{ini}) = \frac{\vec{SS}_{T_0} \cdot \vec{SB}_{T_0}}{|\vec{SS}_{T_0}| |\vec{SB}_{T_0}|}$ and $\cos(\theta_{ver}) = \frac{\vec{SS}_{T_0} \cdot \vec{SB}(T_0)}{|\vec{SS}_{T_0}| |\vec{SB}(T_0)|}$ are the mathematical formula of cosine similarity measure.

\vec{SS}_{T_0} is the vector from of S to S_{T_0} . \vec{SB}_{T_0} is the vector from S to B_{T_0} .

10. If the position is constant and has not differed much, then the candidate node which has the highest score will be chosen as the next forwarding node.
11. Otherwise, the above procedure shall remove the candidate node. This is done again until a proper next forwarder is picked.

By doing so, the proposed method is able to filter out the candidate nodes containing outdated position information and guarantees that the selected next forwarder has the capability to provide the most stable connection to maintain high degree of associativity with the sender node.

4 Results Obtained During Simulation

4.1 Setup Details

Position Verification Technique for Secure Geographical Routing (SGRPVT) is evaluated against Secure Location Verification Protocol (SLVP) [8] through

Fig. 4 No of nodes versus packets delivered

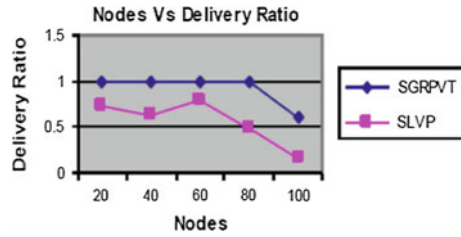
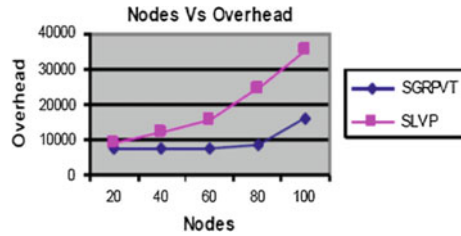


Fig. 5 Overhead versus no of nodes



Network Simulator-2. In an area of 1000×1000 m area random network is deployed. The speed of mobile nodes is varied from 5, 10, 15, 20 and 25. The distributed coordination function (DCF) acts as the MAC layer protocol for wireless LANs. The simulated traffic is CBR with UDP source and sink.

Figures 4 and 5 represents delivery ratio, and overhead where we infer that SGRPVT outperforms SLVP by 42% with respect to delivery ratio, and 45% overhead.

5 Conclusion

The paper, describes how to develop a position verification technique, in order to ensure that the selected position is accurate and reliable. In this work, initially a location estimation algorithm is developed to compute the precise position of the target node. The location is estimated with respect to the detecting node and with the help of a global detecting node. Next the location of the node is verified using a verifier node. For the verification purpose, we develop an algorithm in which the verifier node checks the accurateness of the target node position with respect to another candidate node with high reliability. According to verification test target node is regarded as either Verified if it is proved to be a benign node or faulty if it has an incorrect position otherwise the node is deemed as unverifiable and is not proved to be genuine or erroneous node because of inadequate information.

References

1. Papadimitratos, Panos, Marcin Poturalski, Patrick Schaller, Pascal Lafourcade, David Basin, Srdjan Capkun, and J-P. Hubaux, "Secure neighborhood discovery: a fundamental element for mobile ad hoc networking", *Communications Magazine, IEEE* 46, no. 2, pp. 132–139, 2008.
2. Shaik Arif Basha and G. Preethi Joshna, "Locating and Verifying of Neighbour Positions in MANETs", *International Journal of Computer and Electronics Research*, vol. 3, Issue 4, August 2014.
3. Hsu, Chia-Chang, and Chin-Laung Lei, "A geographic scheme with location update for ad hoc routing", *Fourth International Conference on Systems and Networks Communications (ICSNC)*, pp. 43–48. IEEE, 2009.
4. El Defrawy, Karim, and Gene Tsudik "ALARM: anonymous location-aided routing in suspicious MANETs." *Mobile Computing, IEEE Transactions on* 10, no. 9, pp. 1345–1358, 2011.
5. Lo, Chun-Chih, Shen-Chien Chen, and Yau-Hwang Kuo, "Geographical forwarding scheme with Location Verification for Vehicular ad hoc networks", *21st International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pp. 1–5. IEEE, 2013.
6. Dawei Liu, Moon-Chuen Lee, and Dan Wu, "A Node-to-Node Location Verification Method", *IEEE Transactions on Industrial Electronics*, vol. 57, no. 5, MAY 2010.
7. Marco Fiore, Claudio Ettore Casetti, Carla-Fabiana Chiasserini and Panagiotis Papadimitratos, "Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks", *IEEE Transactions on Mobile Computing*, vol. 12, no. 2, Feb 2013.
8. Song, Joo-Han, Vincent WS Wong, and Victor Leung. "A framework of secure location service for position-based ad hoc routing", In *Proceedings of the 1st ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks*, pp. 99–106. ACM, 2004.

Time-Efficient Discovery of Moving Object Groups from Trajectory Data

Anand Nautiyal and Rajendra Prasad Lal

Abstract The advent of numerous mobile devices and location acquiring technologies like GPS give rise to a massive amount of spatio-temporal data. These devices leave the traces of their positions in the form of a trajectory, which imparts valuable information regarding an object's mobility, as it moves with time. The identification of object groups has copious applications in various domains, like transport system, event prediction, scientific studies, etc. All the state-of-the-art algorithms for discovering object groups use DBSCAN Lo et al. (Kdd 96:226–231, 1996) [1] for clustering spatio-temporal data. However, the time cost for DBSCAN is $O(n^2)$ which can be futile for streaming data. Our work lies in improving the time complexity of the buddy-based traveling companion (a certain type of moving object group) discovery algorithm Tang et al. (ICDE, 2012) [2], Tang et al. (ACM Transactions on Intelligent Systems and Technology (TIST) 5(1):3, 2003) [3] by incorporating the grid based clustering algorithm Gunawan (PhD thesis, Masters thesis, Technische University Eindhoven, 2013) [4], which takes $O(n \log n)$ time. We also establish a novel concept of varying density with increasing snapshots.

Keywords DBSCAN · Clustering · Grid clustering · Trajectory · Buddy · Traveling companion

1 Introduction

GPS-equipped devices have proved to be a boon for the collecting and processing of locations of various objects and using them for countless applications like traffic analysis, social networking, event detection, anomaly detection, recommendation, etc. Objects move and publish their geographical positions as trajectories, which

A. Nautiyal (✉) · R.P. Lal
School of Computer and Information Sciences, University of Hyderabad,
Hyderabad 500046, India
e-mail: anandnautiyal@uohyd.ac.in

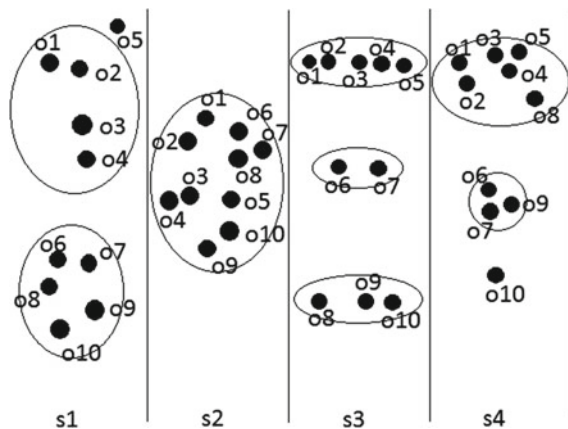
R.P. Lal
e-mail: rplcs@uohyd.ernet.in

depict the information about the spatial locations of moving objects. People move, and with them, they carry devices to connect with the world. These devices emit ginormous timestamped data as streams. There have been extensive applications of finding object groups moving together, or traveling companions [2, 3]. The cab routes can be studied for better taxi service and carpooling. Traffic analysis is another significant domain which benefits from the discovery of companions moving together.

The traveling companion problem deals with the discovery of object groups moving together. Clustering lies at the core of the traveling companion discovery. There are distinct clustering algorithms for spatio-temporal data with varying definitions, like Flock [5], Convoys [6] and Swarms [7] which can only work with static datasets. However, with streaming data an overwhelming amount of data can be collected in a few moments which can be quite difficult to handle. The traveling companion discovery uses DBSCAN [1], which finds a density-connected arbitrary group of objects, irrespective of their shapes. The DBSCAN has a high computational time of $O(n^2)$, a bottleneck for real-time applications. In this work, a grid-based clustering algorithm [4] is used having a time complexity of $O(n \log n)$. It proves to be an efficient method to cluster streaming data and discover traveling companions quickly. An example of traveling companion is demonstrated by Fig. 1 [2, 3]. In this example, the Clustering and Intersection Algorithm [2, 3] is used. The objects are clustered in a snapshot and then intersected with the clusters of the subsequent snapshots. At the end of snapshot s_4 , the objects o_1, o_2, o_3 and o_4 are found out as traveling companions.

In practice, objects can be dense, but it is not necessary for them to stay the same during the entire duration of the companion discovery. In realistic environments, a companion can become less dense with time. If there is a strict restriction on *minPts* [4], many potential candidates will be pruned. Such candidates should be produced as companions. To tackle this, we have used a range of *minPts* such that a companion can vary in density with time. Initially, the density is high but with subsequent

Fig. 1 Example of a traveling companion



snapshots it can fall within a specified range to be termed as a traveling companion [2, 3]. The remainder of this paper is organised as: Sect. 2 presents related work, Sect. 3 formally defines the problem, Sect. 4 explains the detailed grid-based companion discovery approach, Sect. 5 displays the results of the experiments graphically and finally we conclude this study in Sect. 6.

2 Related Work

There have been many similar studies to cluster moving together object groups. Some of them are flock [5], convoy [6], gathering [8], swarm [7], etc. Flock discovers a group of objects which are together for ‘k’ consecutive timestamps inside a disc of radius ‘r’. Convoy uses the density-connectedness [1] and has no restriction on shape and size. Swarm relaxes the constraint of clustering objects in consecutive timestamps. It can have non-consecutive timestamps. Gathering aims to find the coming together of certain objects for a particular time period.

3 Problem Definition

A sequence of snapshots s_1, \dots, s_n represent the trajectory data stream. Each snapshot has the spatial information of its constituent objects in the form of their latitudes and longitudes at a particular time. A snapshot can be represented as $s_i = (o_1, x_{1,i}, y_{1,i}), \dots, (o_n, x_{n,i}, y_{n,i})$, where $x_{j,i}, y_{j,i}$ are the spatial coordinates of object o_j at snapshot s_i . As soon as a snapshot arrives, the objective is to find a traveling companion.

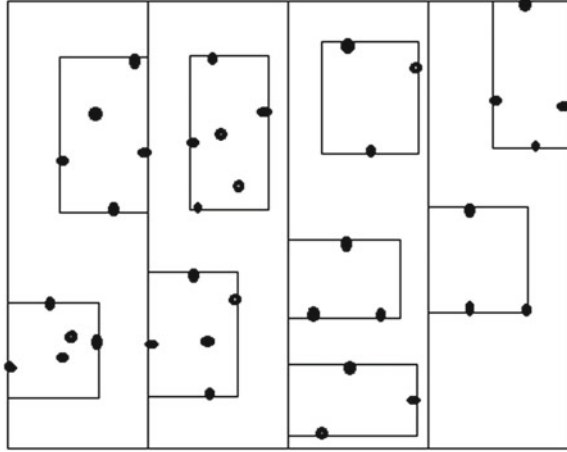
Definition 1 (*Traveling Companion*) Let δ_s represents the size threshold and δ_t represents the duration threshold, an object set q is a traveling companion if:

- (1) The constituents of q are density-connected [1] to each other for a period t where $t \geq \delta_t$;
- (2) $\text{size}(q) \geq \delta_s$.

4 Grid Based Companion Discovery

The Grid-based clustering is structured on several steps: Grid Construction, Buddy Assignment, Finding Core points and Cluster Formation. A grid is a collection of several rectangular boxes containing objects. A regular grid can have empty boxes, as the objects can be dense at a point and sparse or non-existent at the others. This leads to increase in unnecessary space. To overcome this, irregular grids come in

Fig. 2 An irregular grid



handy. Each box of an irregular grid has a diagonal and width of $Eps/\sqrt{2}$. On the arrival of a data stream, the objects are sorted with respect to their x coordinates, which forms a stripe of objects within Eps [4] of the first object. As and when a stripe is formed, it is processed to form several rectangular boxes. Inside a stripe, objects are sorted on the basis of y coordinates, and boxes are constructed similar to a stripe. An irregular grid can be visualised as represented by Fig. 2.

A buddy [2, 3] is a smaller group of objects inside a cluster. These mini group do not form a large cluster, but their information helps the intersection. A box within the grid can contain several buddies. They can be accessed by a Buddy Index [2, 3] which is a triplet $\{BID, ObjSet, CanIDs\}$, where BID represents the buddy's ID, ObjSet comprises the objects of the buddy and CanIDs stores the IDs of candidates containing the buddy. An example of buddy-based discovery is illustrated in Fig. 3 [2, 3] for 4 snapshots of 10 min each. In the figure, r_i is a companion candidate, o_i is an object, b_i is a buddy and s_i is a snapshot. The snapshot s_1 has 4 buddies, b_1 to b_4 . In snapshot s_3 , buddy b_3 becomes invalid, so it is removed from Buddy Index. At the end of snapshot s_4 , the traveling companion r_1 is found out containing buddies b_1 and b_2 .

The core points are the ones with at least $minPts$ in their Eps -neighbourhood [4]. If a box has at least $minPts$ in it, all of its points are marked as core points. This is justified by the fact that the diagonal of a box is of the length $Eps/\sqrt{2}$. And if the number of points in a box is lesser than $minPts$, single points p and q are taken from each of its neighbourhood boxes [4] respectively. If the Euclidean distance between these points is at most Eps and the number of points in the neighbourhood is at least $minPts$, we mark p as a core point.

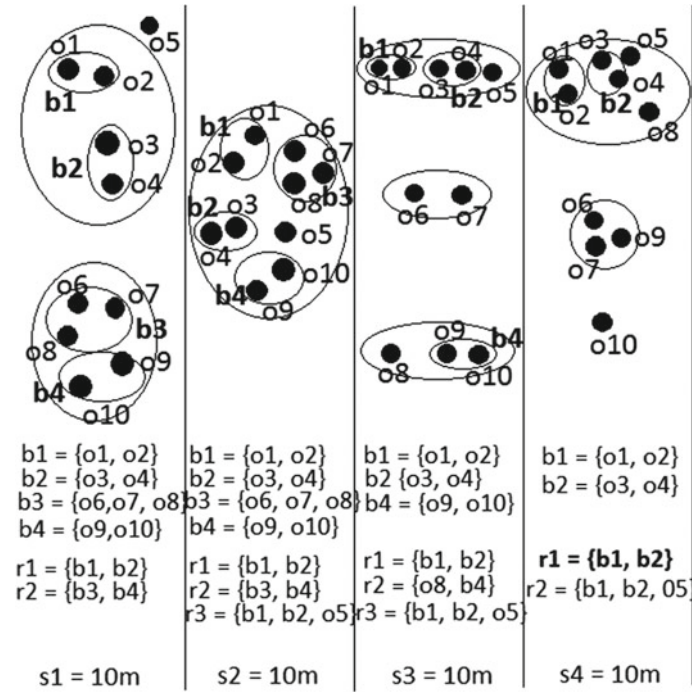


Fig. 3 Example of traveling companion

If the distance between two core points belonging to the neighbourhood boxes is at most Eps , they belong to a single cluster. To carry out the cluster formation, points are connected via edges of a graph. An edge is added between box b and its neighbour b' , if $dist(p \in b, q \in b') \leq Eps$. If the number of points in the neighbouring box b' is greater than $minPts$, then all those points can be added to the cluster. Algorithm 1 presents the grid-based clustering approach. The asymptotic time complexity of Algorithm 1 is $O(n \log n)$. The grid-based clustering, in sum, forms clusters containing buddies. These clusters take part in the companion discovery framework to produce the traveling companions. The clusters in a snapshot are intersected with the clusters of the subsequent snapshot, and their intersection is called a companion candidate [2, 3], i.e., a candidate with the potential of becoming a traveling companion. The Companion Discovery framework is given in Algorithm 2.

5 Experiments

The experiments are performed on the Microsoft T-drive Taxi [9] dataset for a different number of objects. Trajectories were generated up to 5000 taxis. Three datasets

Algorithm 1 Grid Based Clustering

Input: data stream S and Eps
Output: cluster set C

```

1: for all points  $p \in S$  do
2:   construct strips and add to ST
3: for all strips  $st \in ST$  do
4:   construct boxes and add to G
5: for all Box  $b \in G$  do
6:   Assign buddies w.r.t  $Eps$ 
7:   Mark core points w.r.t  $Eps$  and  $minPts$ 
8: Clustering step
9: for all unvisited Box  $b \in G$  do
10:  pick a point  $p$  from a buddy  $bud \in b$ 
11:  if  $p$  is a core point then
12:    for all unvisited Box  $b' \in$  neighbour boxes of  $b$  do
13:      pick a point  $q$  from a buddy  $bud' \in b'$ 
14:      if  $q$  is a core point then
15:        if  $dist(p, q) \leq Eps$  and  $noOfPoints > minPts$  then
16:          Add  $q$  to cluster  $c$ 
17:  Add  $c$  to  $C$ 

```

Algorithm 2 Companion Discovery Using Grid-Based Approach

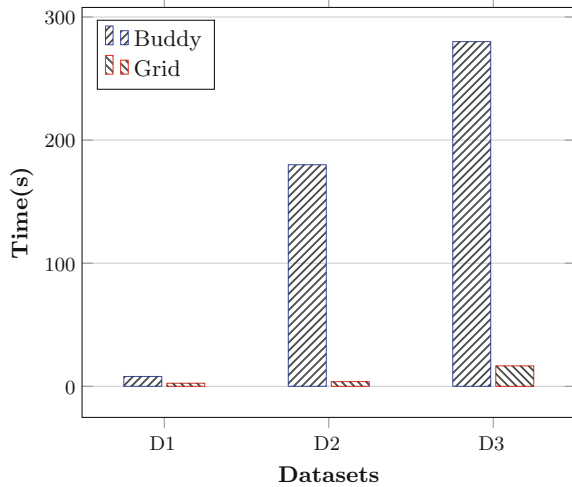
Input: size threshold δ_s , duration threshold δ_d , candidate set R , buddy index BI, data stream S
Output: a set of qualified companions Q

```

1: for all snapshot  $s$  of data stream  $S$  do
2:   initialize an arrayList of candidate set  $R'$ 
3:   Grid Based Clustering; //Algorithm 1
4:   Buddy Index Update
5:   for all candidate  $r_i$  in  $R$  do
6:     if  $size(r_i) < \delta_s$  then
7:       break;
8:     for all cluster  $c_j$  in  $S$  do
9:        $r'_i \leftarrow$  buddy-based intersection( $r_i, c_j$ )
10:      duration( $r'_i$ ) = duration( $r_i$ ) + duration( $s$ );
11:      remove intersected objects and buddies from  $r_i$ 
12:      if  $size(r'_i) \geq \delta_s$  then
13:        add  $r'_i$  to  $R'$ ;
14:        if duration( $r'_i$ )  $\geq \delta_d$  then
15:          display  $r'_i$  as a qualified companion  $q \in Q$ 
16:   for all cluster  $c_j$  do
17:     if  $c_j$  is closed then
18:       add  $c_j$  to  $R'$ 
19:    $R \leftarrow R'$ 

```

Fig. 4 Time comparison of buddy and grid



D1 (500 objects), D2 (1000 objects) and D3 (5000 objects) are used for performance evaluation. The grid-based approach outperforms the buddy based companion discovery and shows very promising results with an order of reduction in time. The resulting times have been demonstrated in Fig. 4.

6 Conclusion

This paper incorporates the grid-based clustering approach with the buddy-based companion discovery algorithm for finding traveling companions in streaming data. The $O(n^2)$ time complexity of clustering step in the traveling companion discovery is reduced to $O(n \log n)$ by using the grid-based approach. The efficiency of the grid-based approach is evident by the experimental results on different datasets of varying size. This reduction in time is highly significant to meet the requirements of real life applications.

References

1. M. Ester, H.-P. Kriegel, J. Sander, X. Xu, et al. A density-based algorithm for discovering clusters in large spatial databases with noise. In *Kdd*, volume 96, pages 226–231, 1996.
2. N. J. Y. J. H. A. L. C.-C. H. W.-C. P. Lu-An Tang, Yu Zheng. On discovery of traveling companions from streaming trajectories. *ICDE 2012*, April 2012.
3. L.-A. Tang, Y. Zheng, J. Yuan, J. Han, A. Leung, W.-C. Peng, and T. L. Porta. A framework of traveling companion discovery on trajectory data streams. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 5(1):3, 2013.

4. A. Gunawan. *A faster algorithm for DBSCAN*. PhD thesis, Masters thesis, Technische University Eindhoven, 2013.
5. M. Benkert, J. Gudmundsson, F. Hübner, and T. Wolle. Reporting flock patterns. *Computational Geometry*, 41(3):111–125, 2008.
6. H. Jeung, M. L. Yiu, X. Zhou, C. S. Jensen, and H. T. Shen. Discovery of convoys in trajectory databases. *Proceedings of the VLDB Endowment*, 1(1):1068–1080, 2008.
7. Z. Li, B. Ding, J. Han, and R. Kays. Swarm: Mining relaxed temporal moving object clusters. *Proceedings of the VLDB Endowment*, 3(1–2):723–734, 2010.
8. N. J. Y. S. S. Kai Zheng, Yu Zheng. On discovery of gathering patterns from trajectories. ICDE 2013, April 2013.
9. C. Z. W. X. X. G. S. Y. H. Jing Yuan, Yu Zheng. T-drive: Driving directions based on taxi trajectories. ACM SIGSPATIAL GIS 2010, November 2010.

Impact on Wave Propagation in Underground to Above Ground Communication Through Soil for UWB Buried Antenna at 3.5 GHz

Vandana Laxman Bade and Suvarna S. Chorage

Abstract A communication through soil using buried antenna is proposed. A transmitting and receiving antenna is used for communication through soil and measure the difference parameter of the ground surfaces such as depth of underground buried antenna in soil, attenuation, propagation of EM wave signals, ground conductivity. The research of WSN (wireless sensor network) UWB has enormously developed for communication through soil using antenna. It was found that the radiation of energy from aboveground to buried antenna that forms a spherical wave and wave propagation due to spherical surface wave is faster in ground surface than below the surface. This study include attenuation caused by different soil properties which is the main challenge because of their power. This paper studies that soil moisture, texture, depth, frequency impact on attenuation, wave propagation, signal to noise ratio, conductivity during communication through soil using buried antenna. This underground to above ground UWB communication is design at 3.5 GHz frequency using the simulation and measurement results with short distance and low soil moisture.

Keywords Wireless sensor network · Ultra wide band · Electromagnetic

1 Introduction

UWB buried antenna enormously developed in variety of application. In this paper transmitter to receiver communication through buried antenna through a soil that impact on wave propagation and this impact is depend on soil parameter like soil temperature, soil moisture, soil texture and that causes degraded the performance of

V.L. Bade (✉) · S.S. Chorage
Department of Electronics & Telecommunication,
BV's College of Engineering for Women, Pune 411043, India
e-mail: vandana1bade@gmail.com

S.S. Chorage
e-mail: Sschorage@gmail.com

wave propagation communication [1]. As the recently promising application of WSN increasing rapidly in research area like monitoring capabilities in the field of intelligent irrigation, sports field maintenance, border patrol, underground mines, agriculture security, navigation security, infrastructure monitoring, intruding detection and so on [1, 2] in this paper basically technology state that the communication of transmitter to receiver UWB microstrip path buried antenna through soil and parameter of soil like temperature, moisture, humidity and depth of soil between Tx and Rx antenna impact on the frequency and conductivity of wave propagation [1]. In this paper there are three communication link which is depend on the transmitter and receiver antenna location and these are following:

- Underground to aboveground communication, if the TX is buried and Rx antenna is above the ground.
- Underground to underground communication link, if the both TX and Rx are buried under the ground.
- Aboveground to underground communication link [1].

For Surface communication between two antennas, the parameter such as depth of the buried antenna and channel attenuation affect on the wave propagation and plays important role in channel path loss [3] recently the trueness of the agriculture, WUSNs are visualized to be a dire factor in enhancing water use efficiency by providing real time data information about soil properties [4] according to WUSN topology sensor network in which higher attenuation due to soil, air and water contain in it and permittivity of medium is change over time [4] UWB technology covers the large bandwidth over 500 MHz because of this benefits UWB technology covers the three main application.

- Signal intelligence and detection.
- Modern UWB operating in a 3.1–10.6 GHz frequency band.
- Ground penetrating radars (GPR) [5].

In this world nears about every 22 min somewhere and somehow the other is killed by landmines. A Steep amount of land goes to inactive due to a fear of landmines. Well informed technology used to detect the landmines as metal detector, nuclear magnetic resonance, electro optical sensors and thermal imaging. for landmine detection GPRs is one of the vulnerable challenging application for UWB radar technology [5]. In this paper the UWB microstrip antenna is design and communication of transmitter and receiver through soil is proposed also parameter of the buried antenna like depth of soil, channel attenuation between antenna, wave propagation properties, return losses, ground conductivity are measure [3]. The different transmission communication link through soil create different path loss in different angle but in particular underground channel is a particularly difficult environment or wireless communication due to greater path loss in soil medium [2].

2 Related Work

H. ZEMMOUR, ANTOINE DIET they studies the impact of the soil parameter on UWB buried antenna and include the e effect of frequency, burial depth, soil moisture and measure the parameter of UWB buried antenna using HFSS simulation software [1]. They state that how the quality of wave propagation is affected due to soil parameter and how the path loss increase with increasing depth of buried antenna. This research studied that soil is dancer than air and becomes high complex permittivity [1].

The recent research technologies is the accurate soil moisture reporting and regulation for the farm under all climate condition and monitor the water and mineral of soil [6] VINOD. P and HONG ZHOU experiments on magnetic induction and electromagnetic wave communication for WUSN. In this paper author study on monitoring, reporting and eventually regulating soil moisture condition for a typical pecan farm. HU.XIAOYA, GAO CHAO studied that wave propagation quality is depend on operating frequency as well as antenna gain also depend on the inter node distance and burial depth of sensors [2].

Keser and Weiss [3] in this paper author simulate the antenna and its EM field using FDTD technique and compare experimental path loss with obtained simulation. The goal of this study was when ground conductivity increased then channel attenuation increased and when ground conductivity was decreased then channel attenuation was decreased.

Dong and Vuran [7]. This paper concludes that sandy soil is less capable of holding water and this is primary factor of wave attenuation.

3 Proposed Wide Band Antenna Design

The design of proposed UWB buried micro strip patch antenna and geometry is shown in g.2. When design of antenna essential parameter is consider i.e. resonant frequency is selected for design is 3.5 GHz, dielectric constant of the substrate and height of dielectric substrate (Figs. 1 and 2).

Fig. 1 The proposed UWB buried antenna: a design with its geometric parameters

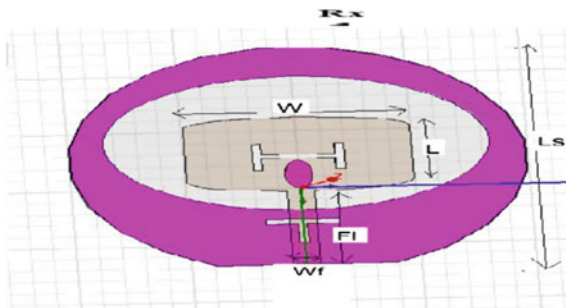
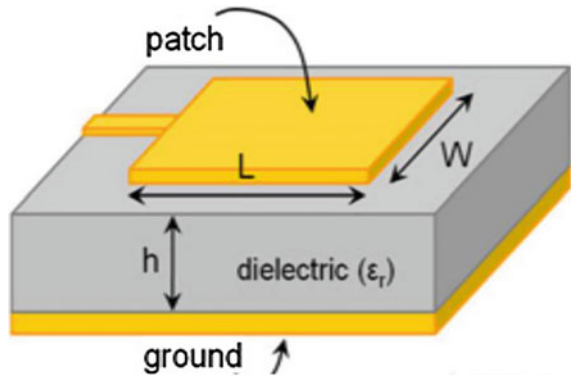


Fig. 2 The proposed UWB buried antenna: **b** Patch Antenna



The different slots and parasitic elements are added to improve the performance requirements. The proposed antenna is designed at operating frequency 3.2–3.7 GHz band for Wimax application and substrate Fr4 with low cost and 1.6 mm thickness is consider for design.

4 Design Methodology

The design of antenna is depend on calculation of the length, width and value of air gap. The value of resonant frequency (FR) is 3.5 GHz and dielectric substrate (h) is 1.6 mm the following parameter is important for calculation like length and width of UWB micro strip patch antenna is given below:

Step1: Calculation of Length of Patch (L)-The effective length due to fringing is given as

For $c = 3 \cdot 10^{11}$ mm/s, $\epsilon_r = 3.99$, $f_0 = 3.5$ GHz We get $L_e = 19.98$ mm. Due to fringing the dimension of the patch as increased by L on both the sides, given by

$$L_{eff} = \frac{c}{2f_0 \sqrt{\epsilon_{reff}}} \quad (1)$$

$$\Delta L = 0.412h \frac{(\epsilon_{reff} + 0.3) \left(\frac{W}{h} + 0.264\right)}{(\epsilon_{reff} - 0.258) \left(\frac{W}{h} + 0.8\right)} \quad (2)$$

For $W = 25.08$ mm, $h = 1.53$ mm, $\epsilon_r = 3.99$. We get $L = 0.70$ mm Hence the length the of the patch is: $L = L_e - 2\Delta L = 26.78$ mm.

Step2: Calculation of the width of Patch (W)

The width of the Microstrip patch antenna is given as For square patch we take $W = 1.5 L$. Therefore $W = 30.78$ mm.

Step3: Calculation of Substrate dimension

For this design this substrate dimension would be $L_s = L + 2 * 6 h = 40 \text{ mm}$,
 $W_s = W + 2 * 6 h = 46 \text{ mm}$.

Step4: Feed width

The first step is to compute the proper feed line width W_f to obtain a 50 ohm line. This is calculated by following formula

$$Z = \frac{377}{\sqrt{\epsilon_r} \left(\frac{W}{t-1.57} \right)} \tag{3}$$

where,

$Z = \text{Impedance} = 50 \text{ ohm}$, $r = \text{dielectric constant} = 4.4 \text{ (FR4)}$, $W = \text{width of patch}$, $t = \text{thickness of substrate} = 1.6 \text{ mm}$. From this we got: $W_f = 3 \text{ mm}$ with $Z = 50 \text{ ohms}$.

Step5: Feed length

$\lambda_m = c_0/f = 85 \text{ mm}$, $Fl = \lambda_m/4 * \text{sqrt}(4.4) = 11 \text{ mm}$, $Fl = 11 \text{ mm}$.

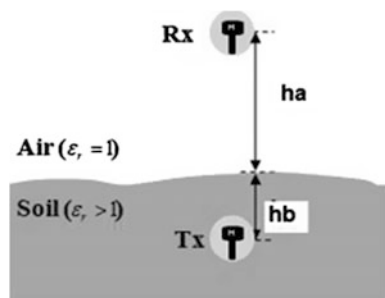
5 Impact of Soil on Ultra Wide Antenna

In this section using simulation result we can study the impact of soil on UWB buried antenna and different communication link ate presented. In the Fig. 3 transmitter antennas is buried with some height in soil and receiver antenna is keep above the ground from transmitter antenna with some height burial depth is denoted by h_b and height of separation between these two antenna is h_a .

The permittivity of soil is higher than air and wavelength of electromagnetic wave is insufficient to propagate through it, if we take soil permittivity is 2.5 in buried antenna case, soil sample is considered for five volumetric water content values (VWC) (Fig. 4).

The Return loss (s11) is that amount of power is lost to the lode and does not return as reflection return loss is similar to VSWR which indicates that how easily matching between transmitter and antenna has taken place. Ideal value of return loss

Fig. 3 Communication model



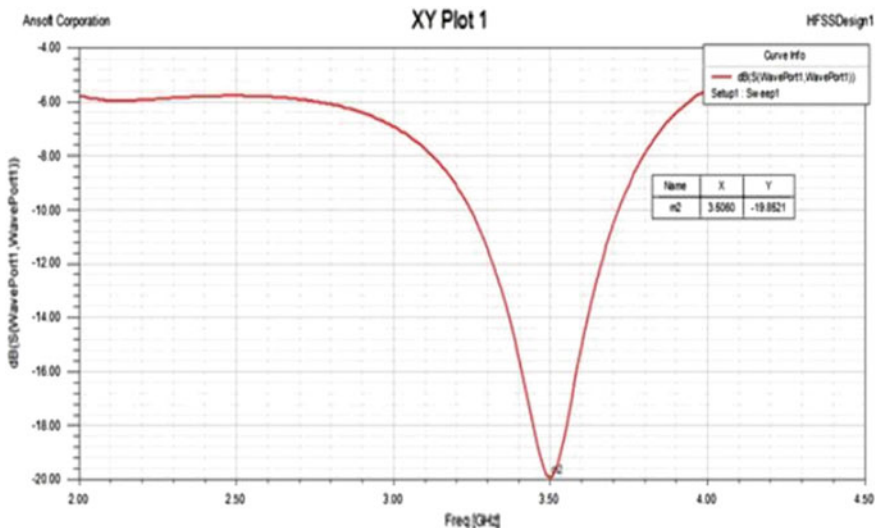


Fig. 4 Return loss of proposed antenna

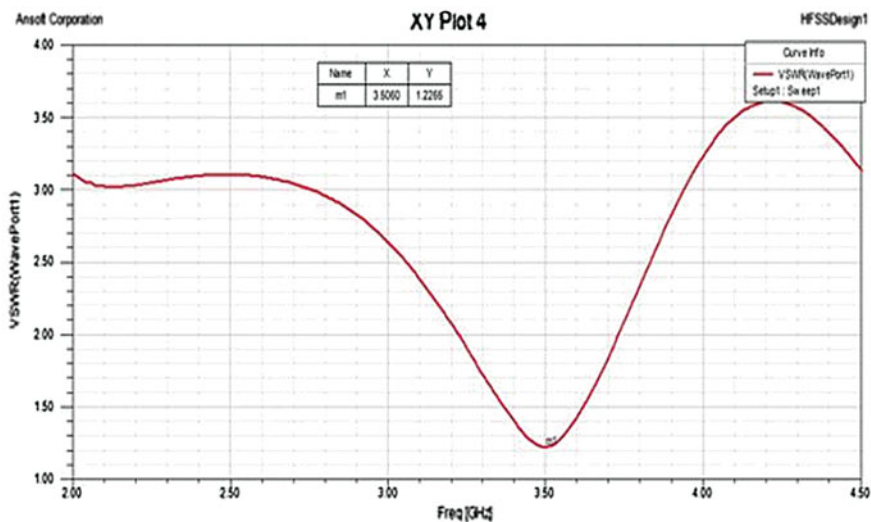


Fig. 5 VSWR

is around -10 db which is VSWR corresponds to ideal value of VSWR i.e. 2. The graph shows the SWR is measure of impedance matching of lode to the char impedance of transmission line and VSWR is nothing bur the maximum to minimum voltage along the transmission line. VSWR is calculated using level of reflected and forward wave. Increasing VSWR indicates an increase in mismatch

between the antenna and the transmission line. Figure 5 shows that value of VSWR is 1.23 with 520 MHz bandwidth.

Figure 6 shows that transmitter antenna is buried in underground and receiver antenna is place above the ground and this setup measure the return loss due to high permittivity of the soil. This TX and Rx are keeping far from some distance of each other. Due to high permittivity of soil the return loss (s11) and insertion loss (s21) changes when antenna is buried in soil. The soil moisture and depth of buried antenna impact on wave propagation when buried depth of antenna is kept fixed at some height (Fig. 7).

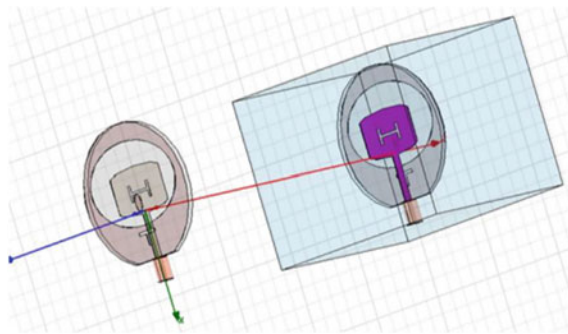


Fig. 6 Tx and Rx wideband proposed antenna

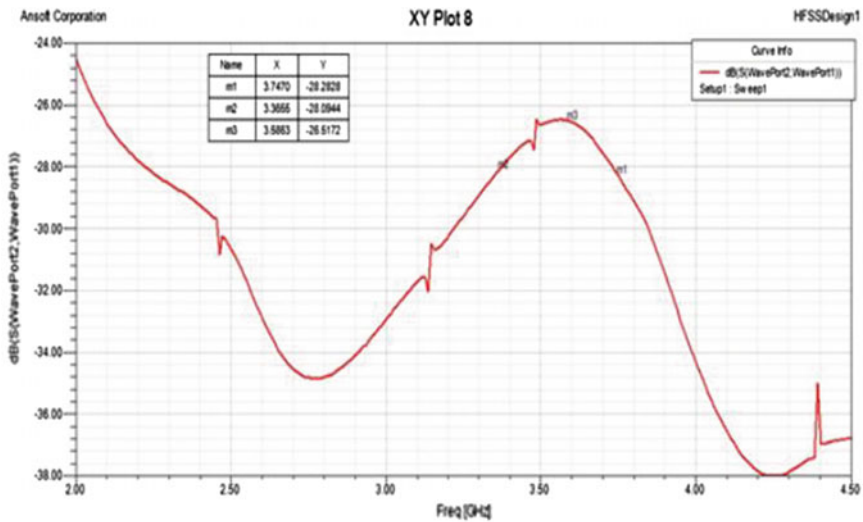


Fig. 7 S21 of wideband proposed antenna

The result of proposed antenna shows that when we increase the distance of buried antenna, attenuation is increase up to -28.38 db. The antenna plane pattern is dividing into two plane as E-Plane and H- plane. E- Plane consist of radiated electric field and H-plane consist of antennas radiated magnetic field potential and these planes are always orthogonal to directivity, side lobe level and front to back ratio. The gain of the simulated radiation pattern of micro strip patch buried antenna has been observed with 1.8 db in omnidirectional pattern.

6 Comparison Table

The work started with basic rectangle antenna with resonant frequency 3.5 GHz and bandwidth of 115 MHz. the same antenna was converted wide elliptical slot and an elliptical parasitic element which resulted into higher shift in frequency of operation at 3.58 GHz. This result shows an increase bandwidth of antenna. To improve more bandwidth a small T-slot is added in ground plane introduced. As seen from the Fig. 8, we got maximum bandwidth 520 MHz.

7 Experimental Set up and Result of System

The experiments were conducted in different links. The goal of these experiments is to measure antenna reflection coefficient returns loss s11, scattering parameter s21. In this measurement two port of network analyzer is connected to

Sr N o.	Shape of MSA	Freq (GHz)	Return Loss(dB)	VSWR	Bandwidth (MHz)	Directivity (dB)
1.	Simple patch with gnd slot	3.51	-15.63	1.39	115	2.45
1.	UWB antenna with ellipse slot in gnd	3.58	-26.00	1.12	450	1.65
2.	UWB antenna with T slot and ellipse slot in gnd	3.50	-19.85	1.22	525	1.70

Fig. 8 Comparison between above systems

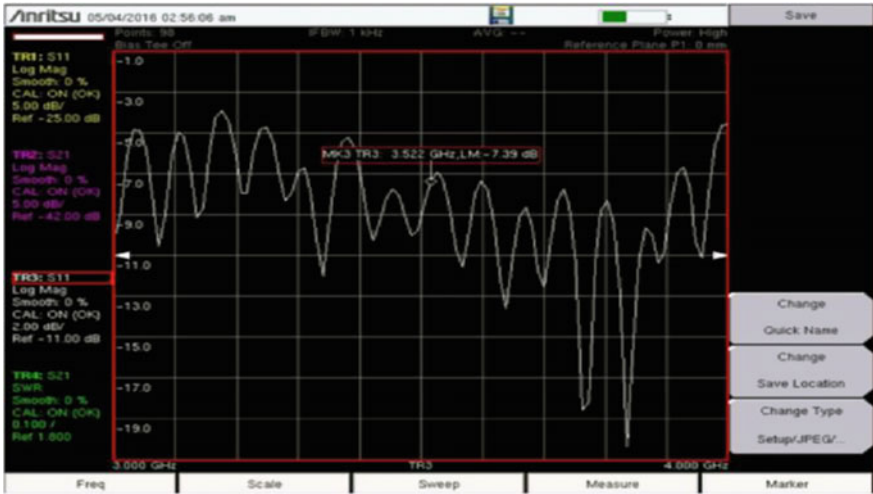


Fig. 9 An experimental result for the return loss (S11) in 3.5 GHz at 4 cm height between TX and RX

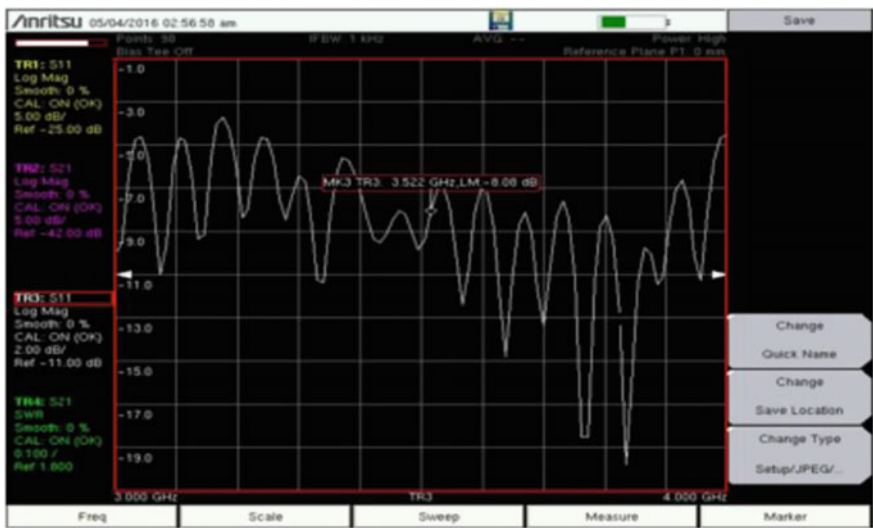


Fig. 10 An experimental result for the return loss (s11) in 3.5 GHz at 8 cm height between TX and RX

Tx and Rx antenna respectively. The transmitter antenna is buried in different material like soil, sand and urea etc. with some height from the receiver antenna and measure the s11 and s21. The experiments test is taken in different height i.e. 4, 8, 12 cm on words with different frequency (Figs. 9 and 10).

This experiments measure the s11 and s21 between the buried antenna and result is taken in above ground to under-ground and above the ground surface and all results compare with the simulation results.

Table 1 Comparison table of experimental result

Sr. no	Material (Used for communication between TX ANDrX)	Freq. in (GHz) distance	Between UG to AG in (cm)	S11 (dB)	S21 (dB)
1	Sand	3.4	4	-16.00	-15
	Sand	3.5	8	-9.34	-19.8
	Sand	3.6	12	-10.00	-12.68
2	Soil	3.4	4	-7.39	-24.26
	Soil	3.5	8	-8.08	-26.51
	Soil	3.6	12	-13.51	-29.2
3	Without material	3.4	4	-7.39	-26.01
	Without material	3.5	8	-9.34	-29.41
	Without material	3.6	12	-10.10	-34

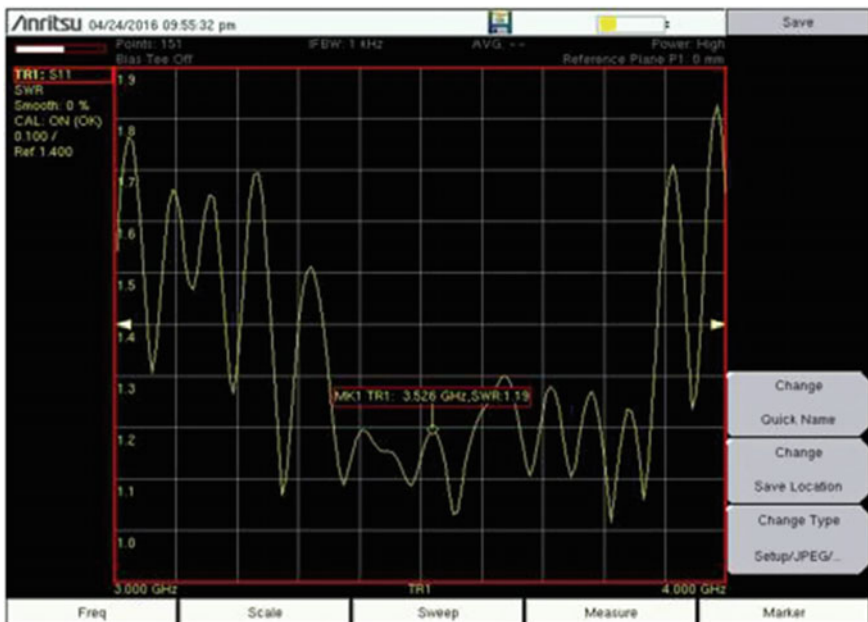


Fig. 11 Experimental result of VSWR

Transmitting antennas was buried in ground surface. The receiving antenna was placed at 4 cm, 8 cm, and 12 cm respectively above the ground surface from the transmitter buried antenna. The marrow of these experiments is that the path loss increases with increases burial depth of antenna and increases with frequency. Table 1. Shows that comparison between s11 and s21 in different frequency with different height by taking various materials between transmitter and receiver UWB micro strip patch buried antenna.

The VSWR is calculated using experimental result. This shows that as compare to simulation result of VSWR, experimental results of VSWR is 1.19 is decreased this indicates slightly decrease the mismatch between the antenna and the transmission line as shown in Fig. 11.

8 Conclusion

In this paper the material like soil, sand, urea impact on return loss as well as communication link between TX and Rx buried Antenna are analyzed for UWB wireless underground sensor networks. It is observed that the bandwidth of patch antenna is increased as compared to simple patch antenna. The simulation results show that attenuation is increased in dry soil with increasing distance. The experimental results conclude that the return loss increased with increasing the depth of buried antenna and with increasing frequency. The simulation and experimental results of UWB patch buried antenna gives better performance for wireless Wimax 3.4–3.6 GHz band application.

References

1. H. ZEMMOUR, Antoine DIET, "Impact of soil on UWB Buried Antenna and communication link in IR-UWB WUSN Application", "12th European Radar conference", vol. **43**, no. 6, pp. 334–337, Sept 2015.
2. H. Xiaoya, G. Chao, W. Bingwen and X. Wei, "Channel modeling for wireless underground sensor networks", "35th Annual Computer Software and Applications Conference Workshops", Munich, July 2011.
3. A. Kesar, E. Weiss, "Wave propagation between buried antennas", "IEEE Transactions on Antennas and Propagation", Vol. **61**, N.12, pp. 6152–6156, Dec 2013.
4. M. Dobson, F. Ulaby, M. Hallikainen, M. El-Rayes, "Microwave dielectric behaviour of wet soil Part 2 dielectric mixing models", "IEEE Transactions on Geoscience and Remote Sensing", Vol. **GE-23**, pp. 35–46, Jan 1985.
5. A UWB Monopole, Ping Cao¹, Yi Huang², "T-Antenna For GPR Application and Jingwei Zhang³ Chen, ZhiNing, and Michael Yan Wah Chia. Broadband planar antennas: design and applications", John Wiley Sons, 2006.
6. V. Parameswaran, H. Zhou, Z. Zhang, "Irrigation control using wireless underground sensor networks", 6th International Conference on Sensing Technology (ICST), pp. 653–659, 2012.
7. Xin Dong and Mehmet C. Vuran, "A Channel Model for Wireless Underground Sensor Networks Using Lateral Waves", 978-1-4244-9268 2011 IEEE.

8. M. Vuran, I. Akyildiz, "Channel model and analysis for wireless underground sensor networks in soil medium", Fourth Inter-national Conference on Intelligent Computation Technology and Automation, Physical Communication 3, Elsevier, pp. 245–254, 2010.
9. H. Zemmour, G. Baudoin, A. Diet, J. Fiorina, "Figures of merit of a small antenna in cluttered IR-UWB Wireless Sensor Networks applications", *IEEE International Conference on Ultra Wideband (ICUWB)*, pp. 141–146, Sept 2014.
10. I. Akyildiz and E. Stuntebeck, "Underground wireless sensor networks: research challenges". "Ad Hoc Networks 4 (Elsevier)", pp. 669–686, in press, June 2006.
11. Vandana Laxman Bade, Suvarna S.chorage, "Design of compact wide band transmit/receive patch Antenna pair for WUSN Application", "2nd IEEE international conference coimbatore, tamilnadu", *IEEE* march 2016.

A Comprehensive Architecture for Correlation Analysis to Improve the Performance of Security Operation Center

Dayanand Ambawade, Pravin Manohar Kedar and J.W. Bakal

Abstract With popularity of information system there is increased in various types of threads. Security Operations Center (SOC) is a central unit that monitor and control the organization traffic. The main function of the SOC is to provide an effective event detection by collecting log files information from different network devices (i.e. firewall, IDS, router etc.). The correlation analysis is known to be core and central part of SOC in which it correlate the different security events from more than one network security devices. In this paper, we propose a comprehensive architecture for correlation analysis that minimize the processing time of log les and gives effective way to implement mathematical model for correlation using a Venn diagram approach.

Keywords SEC • SOC • Event correlation

1 Introduction

With increasing in Internet connectivity and popularity, there are increase in different malicious attacks of various types in very less time. Hence, to protect our system from different kind of attacks we deployed various network security devices

D. Ambawade (✉)

Department of Electronics & Telecommunication,
Sardar Patel Institute of Technology, Mumbai 400058, India
e-mail: dd_ambawade@spit.ac.in

P.M. Kedar

Department of Computer Engineering, Sardar Patel Institute of Technology,
Mumbai 400058, India
e-mail: pmkedar@gmail.com

J.W. Bakal

Department of Computer Engineering,
Shivajirao S. Jondhale College of Engineering, Mumbai 421204, India
e-mail: J.W.Bakal@gmail.com

(such as IDS, firewall, router, reverse proxy server etc.). Each device having its own limitations and due to communication gap between all these network devices, the effectiveness of intrusion detection system degraded. Hence to overcome this problem the concept called Security Operation Center comes into picture. SOC is the centralized security infrastructure in which it collect log files and event information from different security devices and generate a common alarm detection system for some kind of malicious security event [1].

Correlation engine is the core part of the SOC in which is basically looking for some kind of correlation between all these security devices, but logically every device has its own log files and having its own rules for some kind of security attack and it will generate the alarm or report according to that rule [2]. Hence each network device will generate report and alarm for the same packet and it will increase the total number of reports and alarms. This will result a degraded the performance of overall correlation engine and SOC.

The paper begins with study of related work related to Security Operation Center and current mathematical model for correlation analysis [3]. In this paper, we proposed a comprehensive model for correlation analysis that collect log files, normalize log files and then with the help of SEC, it gives input information to implement Venn diagram approach of correlation analysis that will improve the performance of the correlation engine by reducing processing time for log analysis.

This paper is organized as: The Sect. 2 introduces related work regarding SOC and current mathematical approach. The Sect. 3 gives a detailed description about our comprehensive architecture for event correlation. In Sect. 4 we explain an experimental result that we got during implementation and, Finally we give conclusions and future scope in Sect. 5.

2 Related Work

2.1 Security Operation Center and Correlation

Pierre Jacobs et al. [4] propose a classification and rating scheme for SOC services, evaluating both the capabilities and the maturity of the services offered. They used Security Capability Assessment Model for SOC maturity and capability.

Afsaneh Madani et al. [5] explain a new comprehensive architecture for log management has been suggested. Finding an effective log management functional architecture for network events analysis is the main goal of this paper.

Deyang Zhang [1] analyzes the current algorithm of event correlation and proposes a security events correlation method. This method unifies the security events from different security equipment's and sorts them firstly, then combines the security events by the similarity.

Qishi Wu et al. [6] explains the visualization techniques that use for monitoring the situations using graphical representation of security events using Random Matrix Theory. In future scope they said evaluate the proposed system using real in-network and on-host sensor measurements in public network environments.

2.2 Correlation Using Venn Diagrams

Pravin kedar, D.D. Ambawade [3] proposed an mathematical model for correlation analysis. The basic idea of this paper is to represent each and every network security device with a Venn diagram as shown in Fig. 1. Venn Diagrams basically used to express relationship between two or more sets. They can then identify similarities and differences between this sets.

In general if there are N devices, there are N number of message and event generation in above system. It will reduces the performance of the correlation engine as there are more number of redundant messages for the same malicious packet.

As shown in Fig. 2 there are only one message alert for the one malicious packet. i.e. Common Alerts = ((Router Alert)\(Firewall Alert)\(IDS Alert)):

It will reduce the total number of redundant messages in the correlation engine.

By studying above literature review we can say that there is need to some combine architecture which can work based on searching criteria not based on number of lines in log data. Also accuracy of above describe system need to evaluate.

Fig. 1 Representation of security devices using Venn diagrams

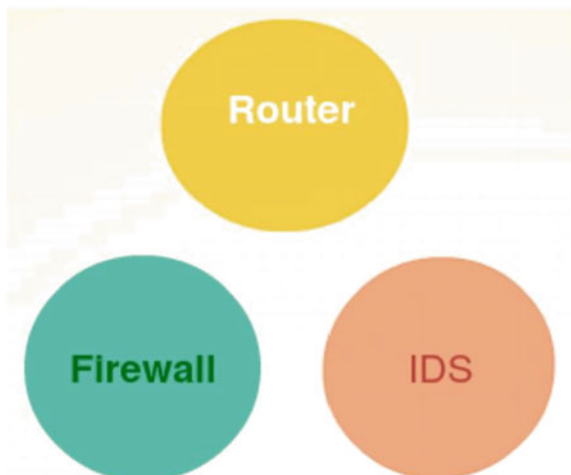
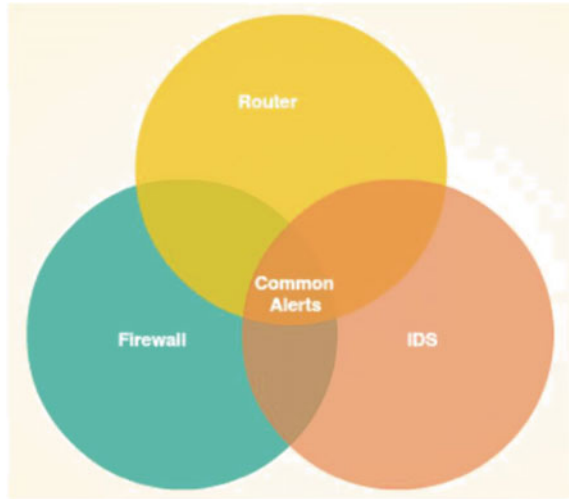


Fig. 2 Representing network devices using Venn diagram relationship



3 Pseudo Code for Proposed System

Algorithm 1 Correlation of log files

```

1: procedure correlation(A)
2:   for Each Network device  $i$  in A do
3:     Collect log files
4:     Normalize log files
5:     Correlate the input log files using SEC
6:     Express result in Venn diagrams
7:     Find the correlation using step 6
8:     result
9:   end for
10:  Return result
11: end procedure

```

4 Proposed Hybrid SEC+Venn Diagram Approach Overview

The proposed system is a combination of Simple Event Correlation (SEC) and Mathematical modal which is used to enhance the performance of correlation engine. As the effective system, there is requirement of accurate predictive results.

So instead of using any mining and filtering techniques, proposed system uses Sec for log files correlation.

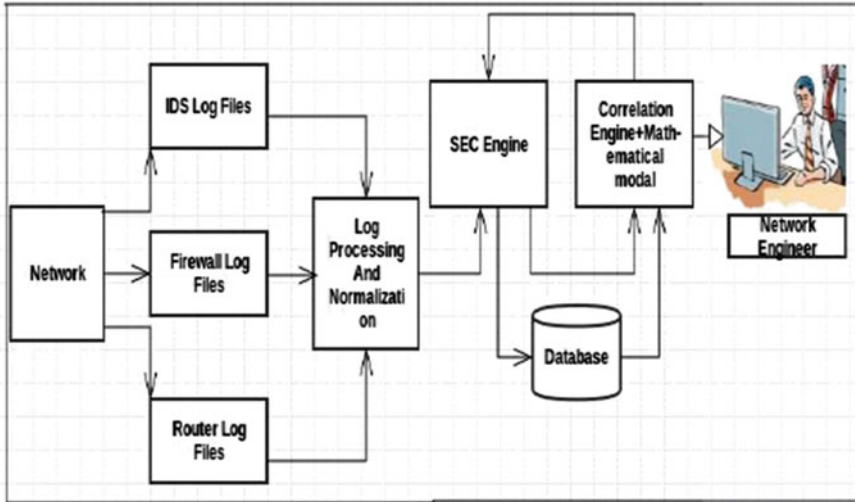


Fig. 3 System architecture

SEC receives input events in terms of log data and by executing rules specified in configuration files produces output events. As shown in Fig. 3, We collected log les from IDS, Firewall and Router. After collection we did normalization of all this log les as there is different log format for each network security devices. After the normalization, we given that data as input to the SEC and finally based on output of SEC we applied mathematical modal to identify the relationship between all this log les. The result of SEC gives alert classes which will be given as input for mathematical model.

5 Experimental Results

In this section, we are putting experimental result that we got while implementing our mathematical model.

SEC i.e. simple event correlator is a powerful event correlation engine that compare input files based on user defined end rules. SEC is a Perl script which reads an input stream from a file or pipe and applies pattern matching operations to the input looking for patterns specified by rules, found in configuration files.

Figure 5 is the main configuration rule file that contain rule for correlation, matching criteria and calendar rule that is responsible for the correlation between different input files. As seen in above conf file, we set Ip address 152.63.146.6 as matching and correlation criteria. Now we are giving collected and normalized log les input to above configuration rule. In our simulation we are giving Firewall and Router log les as shown in Figs. 4 and 6.

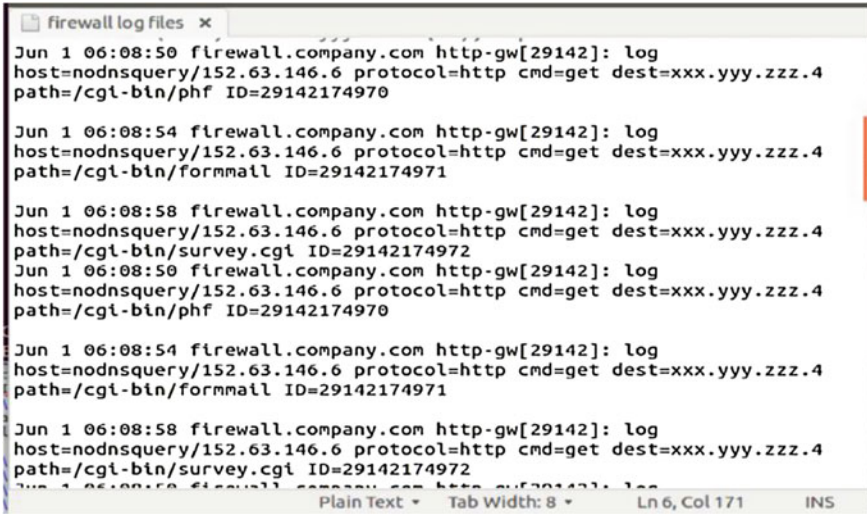


Fig. 4 Firewall log files

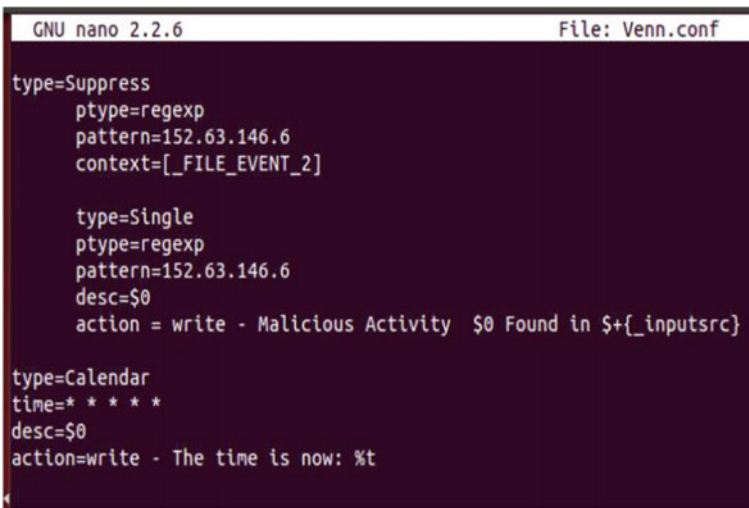
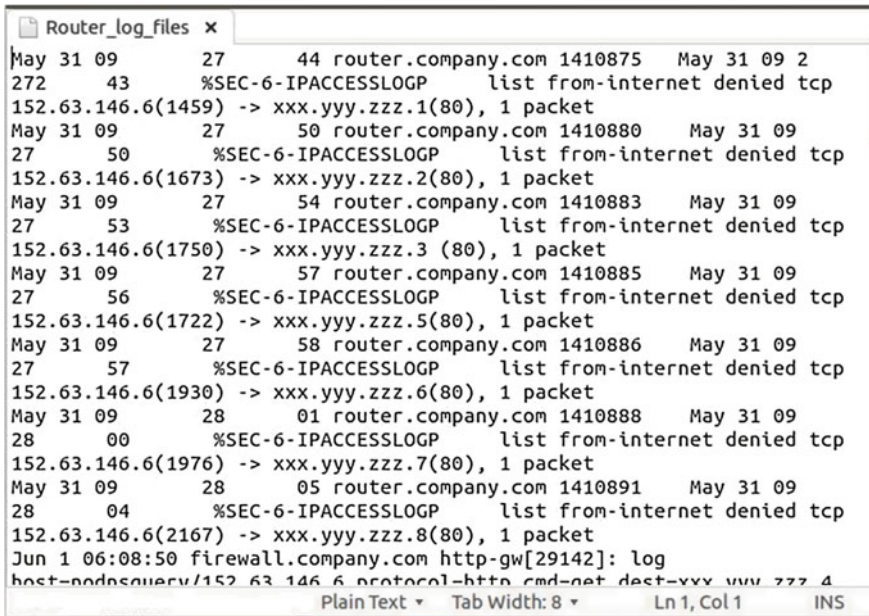


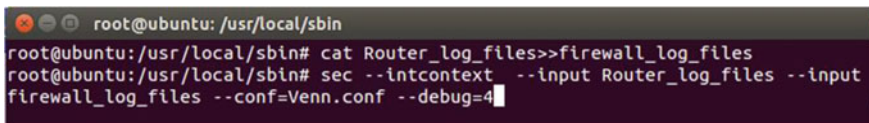
Fig. 5 Event matching rule file Venn.conf

As shown in log files of Router and Firewall, The Ip address 152.63.146.6 is initially found to doing some malicious scanning of network. Now we trying to find above Ip address in another network device log file. Now our next step is to give this log file to the configuration rule that we defined in Fig. 5. Logically it has to give matching Ip address message as Ip address 152.63.146.6 is present in both the log files (Fig. 6).



```
Router_log_files x
May 31 09 27 44 router.company.com 1410875 May 31 09 2
272 43 %SEC-6-IPACCESSLOGP list from-internet denied tcp
152.63.146.6(1459) -> xxx.yyy.zzz.1(80), 1 packet
May 31 09 27 50 router.company.com 1410880 May 31 09
27 50 %SEC-6-IPACCESSLOGP list from-internet denied tcp
152.63.146.6(1673) -> xxx.yyy.zzz.2(80), 1 packet
May 31 09 27 54 router.company.com 1410883 May 31 09
27 53 %SEC-6-IPACCESSLOGP list from-internet denied tcp
152.63.146.6(1750) -> xxx.yyy.zzz.3 (80), 1 packet
May 31 09 27 57 router.company.com 1410885 May 31 09
27 56 %SEC-6-IPACCESSLOGP list from-internet denied tcp
152.63.146.6(1722) -> xxx.yyy.zzz.5(80), 1 packet
May 31 09 27 58 router.company.com 1410886 May 31 09
27 57 %SEC-6-IPACCESSLOGP list from-internet denied tcp
152.63.146.6(1930) -> xxx.yyy.zzz.6(80), 1 packet
May 31 09 28 01 router.company.com 1410888 May 31 09
28 00 %SEC-6-IPACCESSLOGP list from-internet denied tcp
152.63.146.6(1976) -> xxx.yyy.zzz.7(80), 1 packet
May 31 09 28 05 router.company.com 1410891 May 31 09
28 04 %SEC-6-IPACCESSLOGP list from-internet denied tcp
152.63.146.6(2167) -> xxx.yyy.zzz.8(80), 1 packet
Jun 1 06:08:50 firewall.company.com http-gw[29142]: log
host-nodnsquery/152.63.146.6 protocol-http cmd-get dest-xxx.yyy.zzz.4
Plain Text Tab Width: 8 Ln 1, Col 1 INS
```

Fig. 6 Router log files



```
root@ubuntu: /usr/local/sbin
root@ubuntu:/usr/local/sbin# cat Router_log_files>>firewall_log_files
root@ubuntu:/usr/local/sbin# sec --intcontext --input Router_log_files --input
firewall_log_files --conf=Venn.conf --debug=4
```

Fig. 7 Command to run Venn.conf and read the input log files

Figure 7 gives basic command to read the input and run configuration i.e. As shown in Fig. 8, It giving output as “Malicious Activity Found in firewall log files”.

Like this we can give log files of network device as input and correlation can be done by using Venn.conf rule of SEC. The number of input files depends on number of network security device and each device represent one type of Venn. Hence we can easily find correlation between all network devices and that will reduce the number of malicious message and improve the accuracy of the correlation system in the Security Operation Center.

```

root@ubuntu:/usr/local/sbin# sec --intcontext --input Router_log_files --input
firewall_log_files --conf=Venn.conf --debug=4
SEC (Simple Event Correlator) 2.7.9
Reading configuration from Venn.conf
Opening input file Router_log_files
Opening input file firewall_log_files
Interactive process, SIGINT can't be used for changing the logging level
The time is now: Thu Apr 21 11:42:21 2016
Malicious Activity May 31 09 27 44 router.company.com 1410875 May 31 0
9 2 272 43 %SEC-6-IPACCESSLOGP list from-internet denied tcp 15
2.63.146.6(1459) -> xxx.yyy.zzz.1(80), 1 packet Found in firewall_log_files
Malicious Activity May 31 09 27 50 router.company.com 1410880 May 31
09 27 50 %SEC-6-IPACCESSLOGP list from-internet denied tcp 1
52.63.146.6(1673) -> xxx.yyy.zzz.2(80), 1 packet Found in firewall_log_files
Malicious Activity May 31 09 27 54 router.company.com 1410883 May 31
09 27 53 %SEC-6-IPACCESSLOGP list from-internet denied tcp 1
52.63.146.6(1750) -> xxx.yyy.zzz.3 (80), 1 packet Found in firewall_log_files
Malicious Activity May 31 09 27 57 router.company.com 1410885 May 31
09 27 56 %SEC-6-IPACCESSLOGP list from-internet denied tcp 1
52.63.146.6(1722) -> xxx.yyy.zzz.5(80), 1 packet Found in firewall_log_files
Malicious Activity May 31 09 27 58 router.company.com 1410886 May 31
09 27 57 %SEC-6-IPACCESSLOGP list from-internet denied tcp 1
52.63.146.6(1930) -> xxx.yyy.zzz.6(80), 1 packet Found in firewall_log_files
Malicious Activity May 31 09 28 01 router.company.com 1410888 May 31
09 28 00 %SEC-6-IPACCESSLOGP list from-internet denied tcp 1
52.63.146.6(1976) -> xxx.yyy.zzz.7(80), 1 packet Found in firewall_log_files
Malicious Activity May 31 09 28 05 router.company.com 1410891 May 31
09 28 04 %SEC-6-IPACCESSLOGP list from-internet denied tcp 1
52.63.146.6(2167) -> xxx.yyy.zzz.8(80), 1 packet Found in firewall_log_files

```

Fig. 8 Output of event matching

6 Performance Evaluation

In this section we explain performance parameters that obtain during above implementation. Figure 9 gives basic commands for dumping SEC state information.

By sending USR1 signal from command line to SEC engine, it records and display the internal performance parameter that obtain during execution of user defined rule. By default, SEC will dump this information to/tmp/sec.dump. We can use the -dump = filename parameter to change the default setting. The content of tmp/sec.dump is as shown in Fig. 10.

Using the scripts, and rules described in the simulation, several tests were performed. The following table lists results for data directly copied into the SEC input files.

As shown in Table 1, Run time, User time, and System time is mainly depends on number of matching events and not depends on size of log files. Hence it will improve the performance of event correlation as total time for log processing get minimize. We can see from Fig. 11 that even though number of lines in log file increased i.e. 802, we are getting less run time because correlation is based on matching criteria and number of matches in series 3 input is less. Hence we are getting less system and run time in this case.

```
root@ubuntu: /usr/local/sbin
root@ubuntu: /usr/local/sbin# ps -ax | grep sec
 1344 ?        S      0:00 /usr/sbin/dnsmasq --no-resolv --keep-in-foreground --
no-hosts --bind-interfaces --pid-file=/run/sendsigs.omit.d/network-manager.dnsm
sq.pid --listen-address=127.0.1.1 --conf-file=/var/run/NetworkManager/dnsmasq.co
nf --cache-size=0 --proxy-dnssec --enable-dbus=org.freedesktop.NetworkManager.dn
smasq --conf-dir=/etc/NetworkManager/dnsmasq.d
 2811 pts/0    S+    0:00 /usr/bin/perl -w /usr/local/sbin/sec --intcontext --i
nput Router_log_files --input firewall_log_files --conf=Venn.conf --debug=4
 2820 pts/13   S+    0:00 grep --color=auto sec
root@ubuntu: /usr/local/sbin# kill -USR1 2811
root@ubuntu: /usr/local/sbin# $SIGUSR1 received: dumping performance and debug data
```

Fig. 9 Basic commands and input to know state information

```
root@ubuntu: /
Performance statistics:
=====
Run time: 105 seconds
User time: 0.24 seconds
System time: 0.04 seconds
Child user time: 0 seconds
Child system time: 0 seconds
Processed input lines: 52

Rule usage statistics:
=====

Statistics for the rules from Venn.conf
(loaded at Thu Apr 21 13:06:45 2016)
-----
Rule 1 line 1 matched 0 events (Suppress rule with pattern: (?^:152.63.146.6))
Rule 2 line 6 matched 34 events ($0)
Rule 3 line 12 matched 3 events ($0)

Input sources:
=====
Router_log_files (status: Open, type: regular file, read offset: 5563, file size:
5563, device/inode: 1792/531710, received data: 0 lines, context: _FILE_EVENT_Rou
er_log_files)
```

Fig. 10 Performance of SEC of Venn.conf rule and input file

Also, By studding Figs. 5, 6 and 8 we can say that we are getting constant number of messages irrespective of number of network security devices as shown in Fig. 12. Security Alerts will remain constant in case of Venn diagram approach of

Table 1 Comparative performance of SEC+Mathematical model w.r.t input lines and matching events

No. of rules per file	No. of input lines	Run time (Sec)	User time (Sec)	Sys time (Sec)
3	52	105	0.24	0.04
3	72	142	0.26	0.08
3	802	57	0.18	0.03

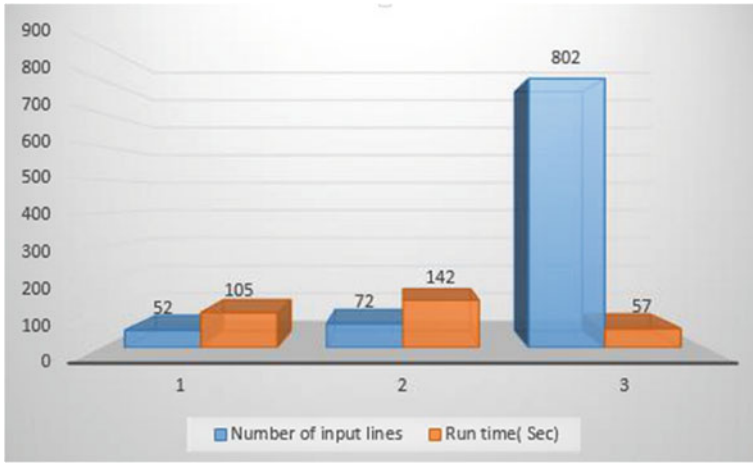


Fig. 11 Run-time comparison system

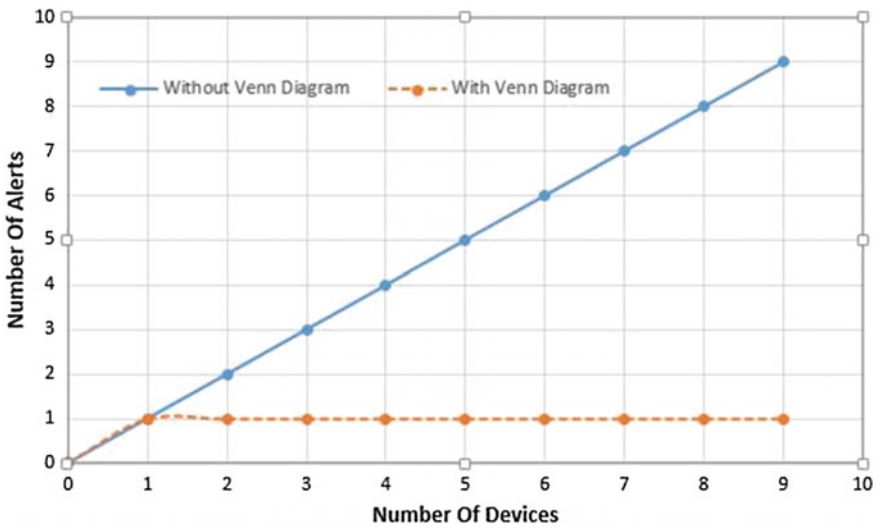


Fig. 12 Run-time comparison of two system

correlation analysis. With Existing system sometimes we get more than one Alert for the some ip address and number of system alerts may increase exponentially.

7 Conclusions

In this paper we proposed comprehensive system model for event handling and correlation analysis to generate the malicious alert in case of the malicious packet. Firstly, we studied impact of the size of log files on performance of the correlation engine and security operation center. Then we studied a current mathematical approach in correlation analysis. And then, we finally proposed new approach of correlation using SEC+Venn diagrams approach. We tested our system by taking real time log files from various security devices and then we generate the logical relationship using all log files. This will result the reduction of number of alert messages, reduction of processing time in case of big log files and helps reduce the false Alarm generation. In future we are interested to use our system for implementing real time security operation center.

Acknowledgements The authors thankful to the Sardar Patel Institute of Technology, India for providing the necessary facilities for carrying out this work.

References

1. Deyang Zhang, "The analysis of event correlation in security operations center", 2011 Fourth International Conference on Intelligent Computation Technology and Automation, *pages 1214–1216, 2011.*
2. Shuying Zhang, Yue Gao, Jianmei Ge, "The study of Network Event correlation Analysis based on Similar Degree of Attributes", 2013 Fourth International Conference on Digital Manufacturing Automation.
3. Pravin kedar, Dayanand Ambawade, J.W. Bakal, "Mathematical Model For Correlation Analysis Using Venn Diagrams Approach To Improve The Performance Of Security Operation Center", International Conference on Electronics and Communication Systems (ICECS), Coimbatore, India
4. Pierre Jacobs, Alapan Arnab, *Barry Irwin Department of Computer Science Rhodes University Grahamstown, South Africa*, "Classification of Security Operation Centers", IEEE Transactions on Dependable and Secure Computing, 2013.
5. Afsaneh Madani, Saed Rezayi and Hossein Gharaee, "Log Management comprehensive architecture in Security Operation Center (SOC).", *Network Security Group, ICT Security Faculty, Iran Telecommunication Research Center (ITRC), Tehran, Iran, pages 284, 189, 2011.*
6. Qishi Wu, Denise Ferebee, Yunyue Lin, Dipankar Dasgupta, "Visualization of Security Events Using an Efficient Correlation Technique", *pages 308–312, 2011.*
7. Jing Liu, Lize Gu, Guosheng Xu, Xinxin Niu, "A Correlation Analysis Method Of Network Security Events Based On Rough Set theory", Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China, *pages 517–519, 2012.*

8. Deyang Zhang, "The analysis of event correlation in security operations center", 2011 Fourth International Conference on Intelligent Computation Technology and Automation, *pages 1214–1216, 2011.*
9. Qishi Wu, Yi Gu, "A Graph Similarity-based Approach to Security Event Analysis Using Correlation Techniques", *IEEE 2013.*
10. Abe Chin-Ching Lin; Hsing-Kuo Wong; Tzong-Chen Wu, "Enhancing interoperability of security operation center to heterogeneous intrusion detection systems", *IEEE 2005.*
11. "Log Files." *Apache HTTP Server Version 2.0.* URL: <http://apache.org/docs-2.4/logs.html> (NOV 2015).

Systematic Approach to Intrusion Evaluation Using the Rough Set Based Classification

R. Ravinder Reddy, Y. Ramadevi and K.V.N. Sunitha

Abstract In the data driven world finding the appropriate user behavior is ambitious. Intrusion detection system is used to do such task, in most of the cases it is not accurate and time consuming process. In this approach, finding such behavior in effectively and accurately the rough set based approach and attribute scaling are used. Intrusion detection is the classification problem, it is used to differentiate between the normal and anomaly behavior accurately. In the process of evaluation all the attributes may not be involved in classification. Selecting the competent attributes from the dataset rough set based feature selection technique is adopted. The preferred attributes may not be scaled properly, scaling of the attributes improves the detection performance. In this approach, rough set based feature selection and attribute scaling are combined with classification to increasing the capability of intrusion detection and decreases the detection time.

Keywords Classification · Rough set theory · Intrusion detection · Attribute scaling

1 Introduction

The process of identifying the abnormal activity in the system is the main goal of the intrusion detection system (IDS), in the early days of detection is done by observing the log records of the system. Anderson has detected the first intrusion by

R. Ravinder Reddy (✉) · Y. Ramadevi
Department of Computer Science and Engineering, CBIT,
Hyderabad 500075, India
e-mail: ravindra_rkk@cbit.ac.in

Y. Ramadevi
e-mail: yrd@cbit.ac.in

K.V.N. Sunitha
BVRIT for Women, Bachupally, Hyderabad 500090, Telengana, India
e-mail: k.v.n.sunitha@gmail.com

auditing the log records [1]. This process of finding the intrusion is time consuming, later denning [2] has proposed first IDS model based on the user profiles by inspecting the audit data. Based on this approaches preparation of the model and test for intrusion takes huge amounts of time. Rather intrusion detection should be done in timely and accurately. In the late 90s data mining based approaches [3] has increased the detection rate and decreases the detection time. Later on this approach feature selection techniques [4] are adopted for dimensionality reduction. This approach has reduces the detection time considerably without affecting the detection accuracy. Rough set theory based approaches are proved significant performance gain by its feature selection techniques. In this work rough set based feature selection is used to reduce the dimensionality of the dataset. The obtained dataset contains the heterogeneous features, it severely affecting the accuracy of the model. Proper scaling of the data will enhance the performance of the model.

2 Related Work

2.1 Intrusion Detection

IDS have become essential in the security framework so that intrusions may be detected to prevent large scale damage before it is too late. Accelerated growth of the network usage activities has increased the rate of network attacks. Advancement in the network has increased the usage in all the aspects including financial transactions, which impact the major parts of the critical information like, confidentiality, integrity and availability (C I A triangle) [5]. Intrusion detection involves supervision of computers or networks to prevent unauthorized access, activity, or change of data. Based on the detection techniques, intrusions are classified into misuse, anomaly and hybrid. Misuse detection looks for known signatures. Anomaly-based network intrusion detection can detect the known as well as unknown intrusion [6]. Hybrid techniques combine both misuse and anomaly for evaluate the IDS effectively. Based on the detection source, it classified into Host based IDS (HIDS) and Network based IDS (NIDS).

2.2 Rough Set Theory

Intrusion detection is a classification problem. In the process of classification, all the features need not participate, and subsets of features (optimal) are used for evaluation of intrusion detection. Feature selection is necessary for reducing the dimensionality of the data [4]. The selection of features is a first step in the classification process for selecting the optimal features from the dataset. It requires a better feature selection technique. Feature selection is an essential task for intrusion

classification for timely detection of intrusion. In this work, reducing the feature vector dimensionality rough set based technique is applied for intrusion detection is presented.

Identifying the intruder behavior in the network as well as in the system is an arduous and time-consuming mechanism. Feature selection is used to determine a minimal feature subset from a problem domain. This must be done even while retaining high accuracy in representing the original features [6]. Rough set approach is mostly used for dimensionality reduction for removing the unnecessary features [7]. Zhang et al. [8] explained the capability of Rough Set Theory (RST) in determining the categories of attacks in IDS according to classification rules. Most of existing IDS use all the data features for detecting intrusions. In the literature of IDS very few researcher address the importance feature selection. The feature subset obtained exercises influence on the accuracy of the intrusion detection.

2.3 Test Bed

In the initial stages of IDS growth, the standard datasets are not available [9]. The KDD initiate the process and designed the standard intrusion dataset. Earlier TCPDUMP data has been used for evaluation of IDS. Before developing the KDDCUP99 dataset, Network capture packets are used in the evaluation of NIDS. System logs, command sequences and memory usage are used for HIDS. Evaluation of IDS needs standard dataset. In this work, to conduct the experimentation for Network-based IDS, the following standard benchmark datasets are used.

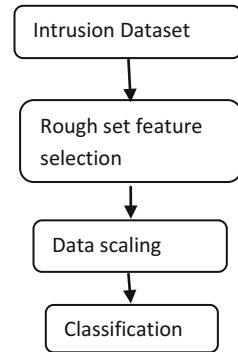
1. KDDCUP99
2. UNB ISCX
3. HTTP-CSIC

The KDDCUP99 [10] dataset is used in many of the intrusion applications it shows. Later ISCX and CSIC dataset are introduced for enhancing the IDS performance. ISCX dataset is prepared from the real time captured packets, the CSIC dataset is prepared for the web traffic applications.

3 Methodology

Intrusion detection dataset contains the both numerical and categorical attributes. The ranges of the attributes are affecting the classification performance in the system. The main power of scaling is avoidance of attributes in greater numeric ranges against those in smaller numeric ranges [11]. Another advantage is to avoidance of numerical difficulties during calculations. Rough set theory is derived

Fig. 1 Data flow in the system



to reduce the number of features, quick reduct algorithm is used to obtain the optimal number of features from the dataset.

Data scaling is applied for the obtained dataset for both the numerical and categorical features for enhancing the detection rate of the system. The scaled dataset is used to classify the intrusion model accurately. Process flow of the system as shown in the Fig. 1.

Algorithm: Data scaling based IDS model

Input: Intrusion Dataset

Output: Intrusion accuracy

Begin:

1. Intrusion dataset has given to the model
2. Rough set theory is used for feature selection
3. Data scaling is applied to the dataset
4. Perform the data mining based classification
5. Result analysis

End

4 Result Analysis

As measuring the performance of the classifier accuracy is not sufficient. Need a measure which represents the accuracy of the intrusion detection, to evaluate it F-measure and G-mean are used. The F-measure gives the harmonic mean of precision and recall, G-mean giving the geometric mean of normal and anomaly accuracies.

$$F - \text{measure} = \frac{2 \times \text{precision} \times \text{recall}}{\text{precision} + \text{recall}}$$

Table 1 Intrusion analysis to the original dataset

Dataset	Accuracy	Precision	Recall	F-measure	Kapaa	G-mean
KDDCUP99	97.37	0.974	0.974	0.974	0.94	0.974
ISCX	99.56	1	0.996	0.998	0.561	0.997
HTTP-CSIC	96.52	0.966	0.965	0.965	0.929	0.965

Table 2 Intrusion analysis with scaling

	Accuracy	Precision	Recall	F-measure	Kapaa	G-mean
KDDCUP99	99.95	0.999	0.998	0.998	0.998	0.998
ISCX	100	1	1	1	1	1
HTTP-CSIC	99.98	0.999	0.998	0.998	0.998	0.998

G-mean concerns the two accuracies of both classes at the same time [12]. G-mean is the geometric mean of specificity and sensitivity. It is used when performance of both classes is expected to be high simultaneously. It is a good indicator on overall performance. It is very useful for the imbalanced datasets.

$$G - mean = \sqrt{Sensitivity * Specificity}$$

The experimentation is conducted for the three intrusion datasets by using the data mining classification algorithm. The results shown in Table 1 are for the original dataset.

The dataset is refined using the rough set based feature selection and data scaling. The obtained results are shown in Table 2, the performance of the model has increased.

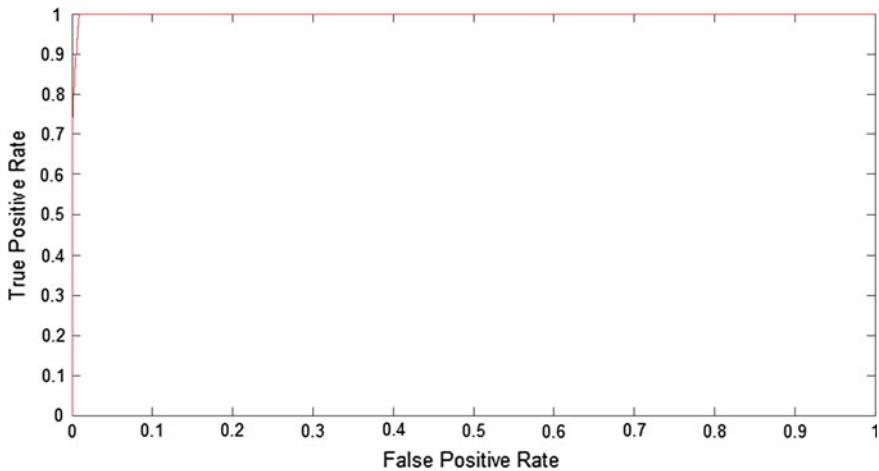


Fig. 2 ROC curve for ISCX dataset

The roc curve is plotted for ISCX dataset [13] has the maximum performance of the classifier as shown in Fig. 2.

5 Conclusion

In evaluation of IDS both the empirical risks and structural risks are important considerations. By adopting the rough set based feature selection reduction in dimensionality of the dataset has been achieved. This decreases the empirical risk of the model. Data scaling has improves the detection performance of the model. Experiments were conducted for the intrusion datasets and achieved performance gain.

References

1. J. P. Anderson, "Computer Security Threat Monitoring and Surveillance", Technical Report, April 1980.
2. Denning D, "An Intrusion-Detection Model", IEEE Transactions on Software Engineering, Vol. SE-13, No. 2, pp. 222–232, 1987.
3. Lee W and Stolfo S.J, "Data Mining techniques for intrusion detection", In: Proc. of the 7th USENIX security symposium, San Antonio, TX, 1998.
4. Dash M & Liu H., "Feature Selection for Classification. Intelligent Data Analysis", Vol. 1, No. 3, pp. 131–156, 1997.
5. Carlos A. Catania, Calos Garcia Garino, "Automatic network intrusion detection: Current techniques and open issues", Computers an Electrical Engineering 38, pp: 1062–1072, 2012.
6. Langley P, "Selection of relevant features in machine learning", In Proceedings of the AAAI Fall Symposium on Relevance, pp: 1–5, 1994.
7. Pawlak Z., "Rough sets", International Journal of Computer and Information Sciences, vol. 11, pp: 341–356, 1982.
8. L. Zhang, G. Zhang, L. Yu, J. Zhang, and Y. Bai, "Intrusion Detection Using Rough Set Classification", Journal of Zhejiang University Science. 5(9), pp. 1076–1083, 2004.
9. Shiravi A, Shiravi H, Tavallae M, Ghorbani AA, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection", Computer Security, Vol. 31, pp: 357–74, 2012.
10. Kwang-Kyu Seo. "A GA-Based Feature Subset Selection and Parameter Optimization of Support Vector Machine for Content – Based Image Retrieval", Lecture Notes in Computer Science, 2007.
11. Cao, Peng, Dazhe Zhao, and Osmar Zaiane. "Measure optimized wrapper framework for multi-class imbalanced data learning: An empirical study", The 2013 International Joint Conference on Neural Networks (IJCNN), 2013.
12. <http://iec.csic.es/dataset/>.
13. Sen S, Clark JA, "Evolutionary computation techniques for intrusion detection in mobile ad hoc networks", Computer Networks, 55, pp: 41–57, 2011.
14. <http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html>.
15. C.A Catania, C.G Garino, "Automatic network intrusion detection: Current techniques and open issues", Computers & Electrical Engineering 38 (5), pp: 1062–1072, 2012.

16. L. H. Zhang, G. H. Zhang, L. Yu, J. Zhang and Y.C. Bai, "Intrusion detection using rough set classification", *Journal of Zhejiang University Science*, 5(9), 1076–1086, 2004.
17. Lee W, Stolfo S. J., And Mok K. W, "A data mining framework for building intrusion detection models", In *Proceedings of the 1999 IEEE Symposium on Security and Privacy*, 1999.

Host-Based Intrusion Detection System Using File Signature Technique

G. Yedukondalu, J. Anand Chandulal and M. Srinivasa Rao

Abstract File signature technique enhances the efficiency of Intrusion Detection System. File Signatures are generated using Hashing Method and Superimposed Coding technique. In this paper, we focus on signature generation technique which is used to find out the malicious users. DARPA data set is used to apply this technique to find out the intruders through IDS. The Jaccard similarity measure is used to find out the distance between two binary strings since all the sequence of system calls in DARPA data set are converted into binary format. Clustering technique is applied to increase the efficiency of the Host-Based Intrusion Detection System.

Keywords File signatures • Intrusion detection • Hashing method • Superimposed coding technique • Similarity measure

1 Introduction

An Intrusion Detection System is a software application that continuously observes a network or system for abnormal activity. Any abnormal event noticed by IDS that can be reported immediately either to a system administrator or collected centrally using a security information and event management system. The intrusion detection system checks throughly the incoming and out going traffic of Host or a network.

G. Yedukondalu (✉)

Vignan Institute of Technology & Science, Vignan Hills, Deshmukhi, Hyderabad, India
e-mail: gyedukondalu@gmail.com

J. Anand Chandulal

K.L. University, Vijayawada, Andhara Pradesh, India
e-mail: dr.chandulal@yahoo.com

M. Srinivasa Rao

School of Information Technology, Jawaharlal Nehru Technological University Hyderabad, Hyderabad, India
e-mail: srmeda@jntuh.ac.in

Prior to the intrusion detection systems the firewalls were in use. They are partially replaced with IDSs because of faults in their design. IDS protects perfectly the computer network or a Host system from the malicious actions. There are numerous IDS, varying from antivirus software to hierarchical systems that monitor the traffic of an entire backbone network. In such networks, even if an intrusion is detected, the system cannot be shut down to check it fully since it may be serving users who are making deals or completing one transaction or the other [1]. The Intrusion Detection Systems are classified as network intrusion detection systems and host-based intrusion detection systems. It is also possible to categorize IDS by its detection approach: the most well-known variants are signature-based detection and anomaly-based detection. Section 2 gives a brief survey to understand different approaches to IDS. Section 3 clustering and Sect. 4 presents the proposed system. We conclude our work in Sect. 5 with experimental results.

Signature-Based Detection: The Signature-Based Intrusion Detection System monitors the packets in the network and matches with pre-computed attack patterns known as signatures. This approach is not efficient because any attacker comes with changing his signature then the system could not understand its altered behaviour.

Anomaly-Based Detection: Anomaly-Based Detection monitors network traffic and compare their state with the normal database defined by the systems administrator and look for intrusions.

Anomaly intrusion detection assumes that all intrusive activities are certainly anomalous. The anomaly-based detection is depends on how we are defining the networks behavior. The users of the network will be allowed into the server system based on the rules defined in the servers database. The behavior patterns of the incoming traffic is to be mapped with the database maintained in the server system while evaluating for intrusions.

2 Related Work

Wenke Lee et al. proposed a scheme that describe a data mining framework for adaptively building Intrusion Detection models. The main idea is to utilize audit records to extract features that describe each network connection or host session and apply data mining programs to learn rules that capture the behavior of abnormal and normal activities. These rules can be used for misuse detection and anomaly detection [2]. The rules dynamically generated or stored in information system are IP addresses of the client systems of a network. Dr. Sanjay Rawat et al. [3] proposed an approach for IDS that captures users behavior using “Singular Value Decomposition Technique”. This technique can help for fast intrusion detection. Dr. Sanjay Rawat et al. [4] proposed another approach for intrusion detection called Binary Weighted Cosine (BWC) metric for anomaly-based intrusion detection that rely on sequence of system calls. BWC technique enhances the capability of the KNN algorithm appreciably. Dr. Sanjay Rawat et al. proposed a speedy Host-Based Intrusion Detection scheme using rough set theory which helps to identify rules for

intrusion detection. Identifying rules dynamically to evaluate the incoming user is normal or adverse. Dr. Dash and Dr. G. Vijaya Kumari et al. proposed a framework “Masquerade Detection Using IA Network” using a novel technique of episode determination.

3 Clustering

Clustering is a concept that will be used to group similar objects together. Each group contains similar objects called a cluster. The properties of each object in a cluster is approximately similar. The features of objects of a cluster is dissimilar with the objects other cluster. We use k-means algorithm to cluster the DARPA data set. In a k-means algorithm, we can choose number of clusters that we are going create. The DARPA data set is made into three clusters in our experiment.

Here, the clustering technique played a vital role in reducing time to search for an intrusion. We calculated the centroid for each cluster. Now each cluster consists of sequence of system calls. Each sequence represents a kind of action done by a user on a host system. By using Jaccard similarity measure, the test sequence of system call is searched in a particular cluster for pattern matching.

4 Proposed Scheme: Signature Generation and Intrusion Detection

The Data Mining techniques are best suited for intrusion detection to trigger alarm when any intrusion takes place in a host system. The proposed IDS can thought of decision making using DARPA data set. Clustering and file signature techniques are applied on DARPA to identify the anomalous actions. The proposed scheme is shown in Fig. 1.

The DARPA Data set consists of test data, training data and attacks. This data set used in the detection process of intruders. Broadly the DARPA data set consists of test data of normal users, test data of anomalous users, training data of normal and anomalous users. Each data set is clustered using k-means algorithm. For each cluster the signature is calculated. Test data signature will be matched with signatures of the shortest distance cluster. Remaining clusters will be omitted for searching. Because of this approach the processing time will be effectively reduced. So the efficiency of ID system will be increased. The signature of test data of normal users will be compared with signatures of the training data of normal users. That user will be allowed to access the Host system. Likewise if the match found in the clusters of training data of anomalous users with the signature of test data of anomalous user. Then the ID system will give anomalous user as outcome.

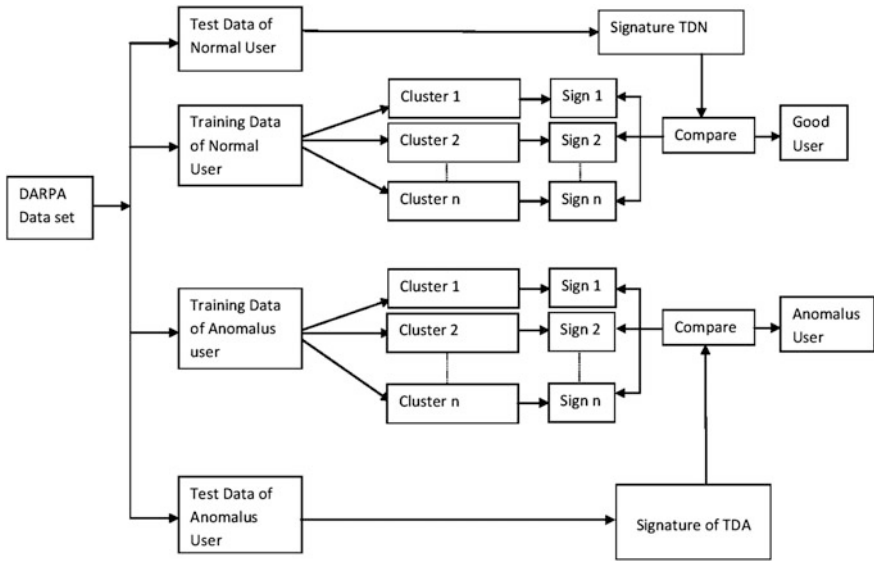


Fig. 1 Framework for host-based anomaly detection

4.1 File Signature

File signature method is an efficient technique for text retrieval. File signatures are computed using Hashing and superimposed coding technique.

Hashing Algorithm:

Input: n size of signature, r number of bits set to 1, Word[] word whose signature is to be computed.

Output: s signature of Word[], procedure Hash (n,r,word[]: in; s:out)

- Step1: $H(\text{word}) = 0$; $l = \text{length of the word}[]$; $p = nCr$;
- Step2: for $i = 1$ to l do
- Step3: $H(\text{word}) = H(\text{word}) * 2 + \text{ASCII}(\text{word}[i])$;
- Step4: End do
- Step5: $s = H(\text{word}) \bmod p$
- Step6: End

The following example illustrates the above algorithm. Let us suppose that $n = 4$ and $r = 2$. Then all the possible ($4 C_2$) combinations for the word DATA and its signatures are shown in Table 1.

The Hash value of word "DATA" is 1037 as per the above algorithm and the signature of word DATA is $1037 \bmod 6$. The resultant signature is integer 5 and its corresponding binary value is the signature of the word DATA. So the signature of

Table 1 Different signatures for the Word DATA

0	0011
1	0101
2	0110
3	1001
4	1010
5	1100

the word “DATA” = 1100. DARPA data set consists of total 606 text documents. Each document consists of sequence of system calls. Superimposed coding technique is used to compute the signature of the file. The computational steps involved are shown below:

Input: Doc document consists of k words w1, w2 ..., wk.
 Output: S signature of the document.
 Procedure superimposed-coding (.Doc : in; S : out)

1. for i = 1 to k do
2. si — Hash(n, r, wordi[]);
3. end do
4. S = s1 V s2 V ... V sk
5. End.

After file signature generation of DARPA data set over then it is divided into 3 groups using k-means algorithm. The distance between the test data sample to the random sample of cluster is computed using Jaccard Distance. The test data sample is matched with random samples from a particular cluster based on the distance.

Jaccard Similarity Measure:

The distance, dis between two binary strings are computed using Jaccard Similarity measure using the below equation

$$dis = \frac{a + b}{c + a + b + d}$$

where

- c no. of variables that equal 1 s for both signature and test strings
- a no. of variables that equal 1 s for signature and 0 s for test signature
- b no. of variables 0 for train signature and 1 for test signature
- d no. of variables that are equal 0 for both strings

For example:
 Original String = 11010
 Test String = 01110

Here

$$c = 2, a = 1, b = 1, d = 1$$

so, $dis = 1 + 1 / (2 + 1 + 1 + 1) 2 / 5 = 0.4$

The distance between above two strings is 0.4.

5 Experimental Results

DARPA dataset consists of total 606 text files. File Signatures are generated using java. For example some of the file signatures generated using Hash function and Superimposed Coding Technique is shown in below Table 2.

k-means algorithm applied on binary DARPA signatures dataset. The output shown in the Fig. 2.

The distances are measured using Jaccard distance technique to find out the distances between each cluster. Distance between test signature to corresponding clusters are calculated are shown below. The test signature of the file is very near to cluster 3 because its distance is short when compared with other clusters. So this technique will eliminate the first two clusters, obviously we search in cluster 3 to find out intruder. So the system is more efficient with respect to search time, the experimental results was shown in Fig. 3.

Table 2 File name with its file signature

The signature of file tr1-311.txt	1110011001010101
The signature of file tr10-320.txt	1111010111101110
The signature of file tr100-816.txt	0000101010001111
The signature of file tr101-818.txt	1110011000000101

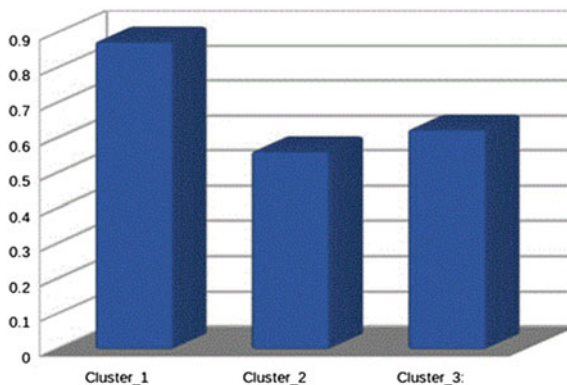


Fig. 2 K means output



Fig. 3 Distances between clusters with test sample

Table 3 Signature shows the behavior of User

File name	Signature	Result
Test signature of file tr1-305.txt	1111111011000110	Intruder detected

The test signature is verified in cluster 3 for pattern matching. This is matched with anomalous users database. So the test signal is an intruder which is shown in the below Table 3.

6 Conclusion

In this paper, the file signature is computed. It is a feasible framework and tries to explore a new approach to intrusion detection system. IDS data processing speed will be high because of the suitable clustering technique.

References

1. Conference on Fuzzy Systems, 2004, pp. 691–696. Sanjay Rawat, “On the use of Singular Value Decomposition for Fast Intrusion Detection System” In Proceedings- published in Electronic Note in Theoretical Computer Science URL:www.elsevier.nl/locate/entcs.
2. A Data Mining Framework for Building Intrusion Detection Models1 Wenke Lee Salvatore J. Stolfo Kui W. Mok Computer Science Department, Columbia University 500 West 120th Street, New York, NY 10027 fwenke,sal,mokg@cs.columbia.edu.
3. Subrat Kumar Dash, Sanjay Rawat, G. Vijaya Kumari and Arun K. Pujari, “Masquerade Detection Using IA Network”, First International Conference on Emerging Trends in Engineering and Technology, pp 504–507, IEEE, 2008.
4. Hind Tribak, Blanca L. Delgado-Marquez, P. Rojas, O. Valenzuela, H. Pomares and I. Rojas, “Statistical Analysis of Different Artificial Intelligent Techniques applied to Intrusion Detection System”, IEEE, 2012.

5. Sanjay Rawat, "Intrusion Detection System using text processing with Binary-Weighted Cosine Metric", In Proceedings: published in Electronic Notes in Theoretical Computer URL: www.elsevier.nl/locate/entcs.
6. S. Revathi and A. Malathi, "Data Preprocessing for Intrusion Detection System using Swarm Intelligence Techniques", International Journal of Computer Applications, Volume 75– No. 6, August 2013 [23] Iwan Syarif, Adam Pruge Bennett and Gary Wills, "Unsupervised clustering approach for network anomaly detection.
7. Faloutsos. C. "Access methods for text", *ACM Computing Surveys*. 1985.
8. Sreenivasa Rao, M., Pujari, A. K., Sreenivasan, B. "A new neural network architecture for efficient close proximity match of large databases". *IEEE Computer Society Press, Proceedings of the Eighth International Workshop on DEXA, France, Edited by R. R. Wanger*, 444–449, 1997.
9. S. B. Needleman and C.D. Wunch. "A general method applicable to the search for similarities in the amino acid sequences of two proteins. *Journal of Molecular Biology*", 1970.
10. Shang, H., Merrettal, T. H., "Tries for Approximate String Matching knowledge", *IEEE trans on ge and data Engineering*, 1996.
11. Bethina Schmitt and Sven berländer, "Evaluating and Enhancing Meta-Search Performance in Digital Libraries.

Intra and Inter Group Key Authentication for Secure Group Communication in MANET

G. Narayana, M. Akkalakshmi and A. Damodaram

Abstract Mobile Ad Hoc Network (MANET) is basically an infrastructure less network consisting of numerous member nodes connected to each other wirelessly. All the nodes in MANET work in cooperation with one another, by forwarding the data to its neighbor node which is within its transmission range, and the neighbor node, in turn forwards it, until the data reaches its respective destination. But, if there exists any malicious node in the network, then the data being transmitted gets damaged/compromised. This is possible since all nodes are linked wirelessly, which makes it easy for the attackers/malicious nodes to infiltrate the network. So to protect the network data, we propose an intra and inter group key authentication technique for secure group communication. In this technique, the network is divided into several groups. Each group has an intra group key to safeguard its privacy. When two nodes belonging to different groups want to communicate with each other, then they generate an inter group key and then securely carry out communication.

Keywords Secure group communication • Key authentication • Key encryption key • Security

G. Narayana (✉)

Department of CSE, JNTUH, Hyderabad, Telangana, India
e-mail: narayanag.1973@gmail.com

M. Akkalakshmi

Department of IT, GITAMS University, Hyderabad, Telangana, India
e-mail: lakshmi.muddana@gitam.edu

A. Damodaram

Sri Venkateswara University, Tirupati, Andhra Pradesh, India
e-mail: damodarama@rediffmail.com

1 Introduction

1.1 *Mobile Ad Hoc Network (MANET)*

The Mobile Ad Hoc Network (MANET) is made up of several nodes which are highly mobile and connected wirelessly through multi hop routes. MANET is an infrastructureless network and hence does not rely on centralized controlling points such as base station, access point, etc. Since wireless applications are increasing as in case of cable TV, video and audio conference, military communications, etc. wherein the wireless multicast is performed, it is important to ensure the safety of data being multicasted. The key management (KM) technique is employed to assure that just the authenticated members of the network get access to the respective authenticated group. Hence for secure multicast operations, it is necessary to employ a dynamic KM technique. But, there are issues in developing a secure MANET due to its salient features such as restricted battery life, conditioned processing, limited resources, etc. [1]. Some of the unique features of MANET are:

1. MANET is a self sustaining network and hence is independent of centralized controlling points. So most of the functionalities performed by the host, router, etc. are carried out by every member of the network. Thus, allowing the nodes which are not within each others communication range to communicate through intermediate nodes.
2. MANET is a not a centralized network. It is a distributed network.
3. Network resources are limited. For instance, battery power, bandwidth, memory, etc. [2].

1.2 *Secure Group Communication in MANET*

In MANET, group communication is an important function because of the cooperative performance of the member nodes in handling the network operations to achieve the successful data transmission after overcoming the irregular network behaviour in the absence of centralized network infrastructure. For instance, in military operations, the users update the surrounding status to be alert and conscious of the overall conditions and to respond accordingly. In MANET, the nodes are mostly dependent on the multicast for handling traffic conditions like route discovery or neighbor discovery to develop multihop paths, to maintain time synchronization, etc. This traffic needs to be delivered at the destination in a safe process. Some of the target aspects to be attained by this network are:

1. Message Confidentiality: to avoid the attackers or malicious nodes from getting access to data.
2. Message Integrity: to avoid destruction of the messages being transmitted.

3. Source Authentication: to overcome intentional attacks which may resend data or causing node impersonification [3]?

In MANET, safe group communication is attained by sharing a group key which allows the valid members to perform data encrypt and decrypt operations. All the group messages undergo encryption by the group key. In this way, all nodes in a group assist one another without worrying about malicious node attacks. Designing a group key agreement (GKA) protocol is an open issue since the origin of the Diffie–Hellman (DH) protocol. Large research is performed in order to make the DH key exchange process a general process, but not many research activities are successful because of the inability to use in the MANET. This inability is due to the fact that the researched and proposed techniques are not self sustaining and are also controlled by a centralized point. Also, the proposed techniques give importance only towards maintaining data security and not in preserving data [2].

2 Related Works

Xixiang Lv and Hui Li [2] have presented a Chinese Remainder Theorem-based secure group communication scheme. This scheme is capable of offering confidentiality and non-repudiating features. A shared encryption public key is generated by the group members based on the public key of each member, and hence it will also respond to various decryption needs. The confidentiality and non repudiation, which is necessary to safeguard the group communication is maintained by utilizing the shared public key and the corresponding secret key. Mohamed Younis et al. [3] have proposed a new Tiered Authentication scheme for Multicast traffic (TAM) for large scale dense ad hoc networks. In TAM, the features of time asymmetry and also the secret information asymmetry model are used together and clustering technique is used to minimize the data overhead and also to assure scalability. The one way hash function chain is used to validate source of the message in the multicast traffic in a cluster. Message authentication codes (MAC) which are developed on the basis of a specific key set are enclosed in the cross cluster multicast traffic. To validate the source, every cluster utilizes a specific key subset in order to determine its defined combination of authenticated MAC in the message.

Zhiguo Wan et al. [4] have presented an unobservable secure routing protocol referred as USOR in order to provide absolute unlinkability and also content unobservability for every packet category. USOR combines group signature as well as the ID based encryption technique for determining paths and hence works proficiently. Based on the analysis, it is observed that USOR safeguards confidentiality of the user from attackers which can attack internally or externally.

Hua-Yi Lin and Tzu-Chiang Chiang [5] have presented a dynamic multicast height balanced group key agreement (DMHBGKA) technique which permits a

user belonging to a multicast group to generate a group key in an effective manner and then safely deliver the traffic data from the transmitting node to the destination user residing within a different group in MANET. The proposed protocol divides the group members in the basis of location to form location based clusters. These clusters minimize the communication expense and also the key management expense that incurs during the entry and exit of the members into and out of the network. This protocol offers proficient key reconstructions, safeguards data multicasting technique, makes the network dynamic and also minimizes the overhead expenses related to security operations by employing the elliptic curve Diffie-Hellman (ECDH) cryptography key management.

Weichao Wang and Yu Wang [6] has proposed a technique for the formation and maintaining the multicast network. This technique allows robust change in the network topology and also allows balanced distribution of the network information. Communication within the group and also between different groups is facilitated in a safe manner by employing the proposed key distribution and update technique. The key shares are distributed using the adopted polynomials and then the LKH. (Logical Key Hierarchy) technique is used to attain effective key refreshment.

3 Intra and Inter Group Key Authentication for Secure Group Communication in MANET

3.1 Overview

In this paper, as an extension we propose an intra group and inter group authentication for multicast traffic in MANET. For secure authentication, the messages sent from group members to GM should be signed with a signature key. We assume that a member holds long-term private and public keys certified by a trusted certificate authority (CA). Each node uses the digital signature algorithm (DSA) for signing the messages [7]. Initially, the group members send an intra group key request (INTRA_REQ) to GM signed with their own private key. Members can obtain the key encryption key (KEK) securely from GM which is signed by the GM with its private key. The members after verifying the signature of the GM, obtain their KEK, the process flow is as shown in Fig. 1.

During intra-group key management [8], the GM generates a polynomial and broadcasts it to the members, from which the members can construct the intra-group key. Lock-secret denotes a secret value of a member. It locks the group key so that GM can securely transfer the polynomial to the members. Group members use their unlock-secret to extract the polynomial from GM's broadcast message of a locked group key [7]. Then the inter group key management is performed as described in [8]. The multicast from the source will be done to all relevant GM and then a within each of the target groups to forward the message to the receivers.

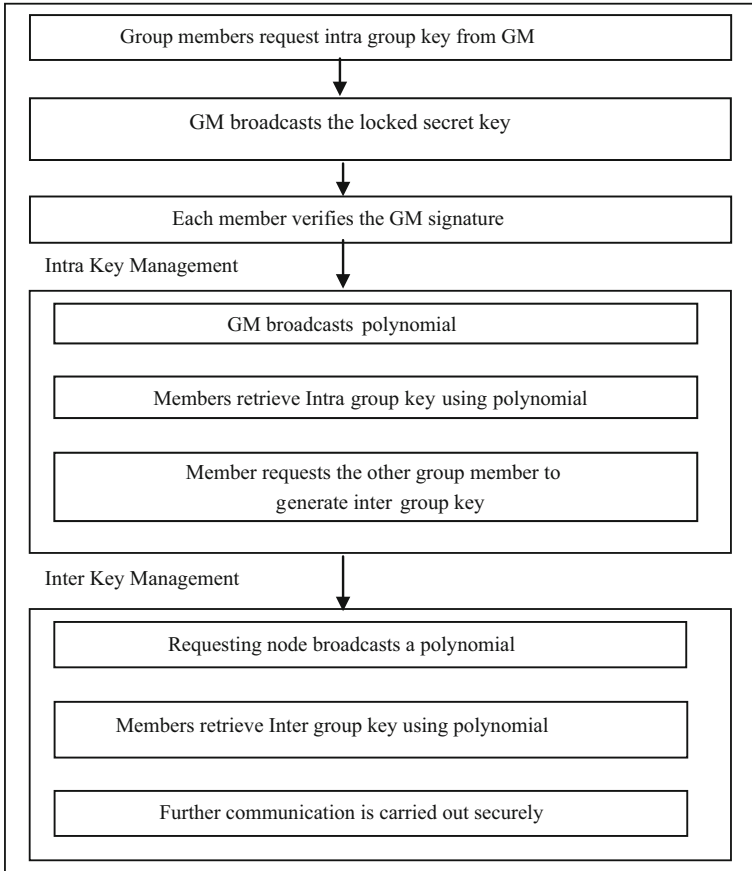


Fig. 1 Block diagram

3.2 Intra Group Key Management

Intra Group Key management is the key management technique employed within the group. Each group consists of many members and one group manager [7]. The group manager is responsible for issuing the key encryption key (KEK) and the intra-group key. This process is illustrated in Algorithm 1.

Algorithm 1

Notations:

- INTRA_REQ: intra key request message
- $G_{x(i)}$: private key of the group member
- GM: Group Manager
- K: random secret selected by GM

KEK _i :	Key Encryption Key of a Group member
i:	integer number
X _i :	locked encryption key
G _k mod p:	GM signed key
P:	predefined large prime number
G _k :	intra_group key
P:	Polynomial
X:	variable where the respective KEK has to be deployed
x(i):	lock secret key
y(i):	unlock secret key

Algorithm:

- Step 1 Each member of the group sends an INTRA_REQ message after signing it with its private key, $G_{x(i)}$ to the GM.
- Step 2 The GM selects a random secret, k and computes KEK_{*i*} and signs it with its private lock secret key and locks it.

$$(X_i)_k = (G_{x(i)})_k \quad (1)$$

- Step 3 Then the locked KEK_{*i*} is broadcasted by the GM to its group members.
- Step 4 On receiving the locked KEK_{*i*}, each member verifies the GM signature by unlocking it with its private unlock secret key.

$$KEK_i = ((X_i)_k)_{y(i)} \text{ mod } p = (G_{x(i).y(i)})_k \text{ mod } p = G_k \text{ mod } p \quad (2)$$

- Step 5 If the member determines the GM signature to be invalid then it ignores the received broadcast message.
- Step 6 If the GM signature is valid, then it accepts it.
- Step 7 Once all the group members have the KEK_{*i*}, the GM generates a polynomial P using all KEK_{*i*}.

$$P = (x - KEK_1) (x - KEK_2) \dots (x - KEK_n) + G_k \quad (3)$$

- Step 8 The P is locked by the lock secret so that the GM can ensure the security of P.
- Step 9 The P is broadcasted by the GM to its members.
- Step 10 On receiving the P, the members compute the intra group key by using its own KEK_{*i*}.

$$\text{Intra group key} = (x - KEK_1) (x - KEK_2) \dots (x - KEK_n) + G_k \text{ with } x = KEK_i \quad (4)$$

$$\text{Intra group key} = 0 + G_k$$

$$\text{Intra group key} = G_k$$

- Step 11 The members use its unlock secret to extract the P received from GM. In this way, the intra key is managed in the group by the group manager.

3.3 Inter Group Key Management [8]

In the inter group key management technique, the Pseudo Random Number Generator (PRNG) is used for key generation. In a network, there may exist several group, which need to communicate with one another [8]. For secure communication between the different group members, an inter group key is generated. This process is described in Algorithm 2.

Algorithm 2

Notations:

- Grp_i: group in the network
- N: total number of group in the network
- X_{recipient_grp, i}: polynomial sent to the recipient member from a member of another group

Algorithm

- Step 1 In a network there are n groups; Grp₁, Grp₂, ..., Grp_n.
- Step 2 The member of a group which wants to communicate with a member of another group, initially sends a INTER_REQ message with the id of the specific recipient member.
- Step 3 The message sent from other group is received by every member of the recipient group.
- Step 4 The intended member is able to decrypt the message using its secret lock key.
- Step 5 Then the requesting member sends a polynomial to the recipient group.
- Step 6 Each recipient member tries to decrypt the received message using the polynomial X_{recipient_grp,i} which is generated in a manner similar to Eq. (3) in Algorithm 1 in Sect. 3.2.
- Step 7 The polynomials are used to generate the inter group key as seen in Eq. (4) in case of intra group key in Algorithm 1.
- Step 8 Only the specified member node of the recipient group will be able unlock the locked polynomial.

Thus, even the inter key management is performed in a similar procedure as done for the intra key management to assure security in the network.

4 Results and Discussion

4.1 Simulation Parameters

The proposed Intra and Inter Group Key Authentication for Secure Group Communication (IIGKA) protocol is simulated in NS-2. Table 1 presents the simulation settings and parameters.

4.2 Performance Metrics

The proposed IIGKA protocol is compared with the polynomial based key management (PKM) [8] protocol and the following performance metrics are evaluated. Delay, packet delivery ratio, average residual energy, average packet drop and control overhead.

4.3 Results and Analysis

A. Varying the Attackers

The number of attackers is varied as 2, 4, 6, 8 and 10 with pause time 5 s.

The end-to-end delay occurred for IIGKA and PKM protocols are shown in Fig. 2. The figure shows that IIGKA has 12% lesser delay than PKM protocol, when the attackers are increased.

The packet drop and packet delivery ratio of IIGKA and PKM protocols are shown in Figs. 3 and 4, respectively. The figures show that the packet drop is 70% less and the delivery ratio is 49% higher for IIGKA, when compared to PKM.

The residual energy of IIGKA and PKM protocols is shown in Fig. 5. The figure shows that IIGKA has 4% higher residual energy than PKM protocol, when the

Table 1 Simulation parameters

Number of nodes	50
Area size	1000 × 1000 m
MAC protocol	IEEE 802.11
Simulation time	50 s
Traffic type	Constant Bit Rate (CBR)
Number of attackers	2–10
Propagation model	TwoRayGround
Antenna	OmnAntenna
Initial energy	10.1 J
Transmission power	0.3 W
Receiving power	0.8 W
Pause time	5, 10, 15, 20 and 25 s

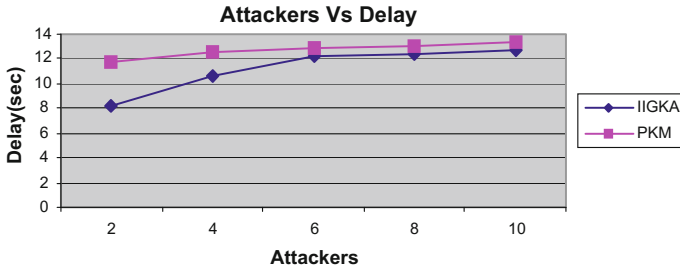


Fig. 2 Delay for varying attackers

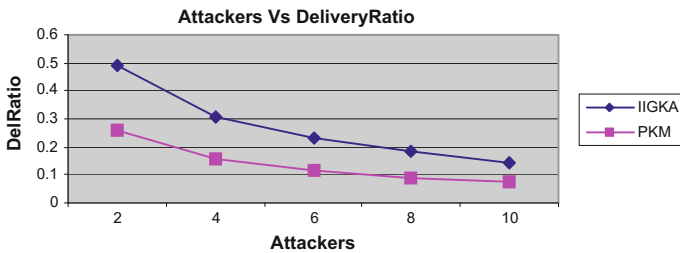


Fig. 3 Delivery ratio for varying attackers

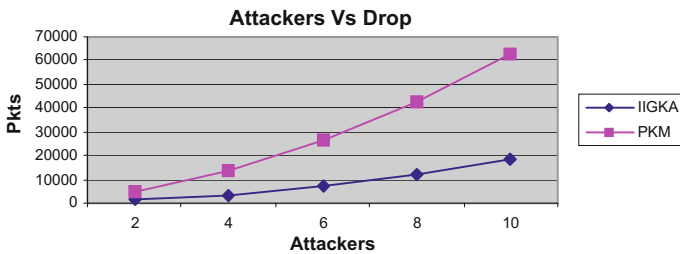


Fig. 4 Packet drop for varying attackers

attackers are increased. The control overhead occurred for IIGKA and PKM protocols is shown in Fig. 6. The figure shows that IIGKA has 62% lesser overhead than PKM protocol, when the attackers are increased.

B. Based on Pause Time

The pause time of the mobile nodes is varied as 5, 10, 15, 20 and 25 s for 4 attackers.

The end-to-end delay occurred for IIGKA and PKM protocols when the pause time is varied, are shown in Fig. 7. The figure shows that IIGKA has 3% lesser delay than PKM protocol.

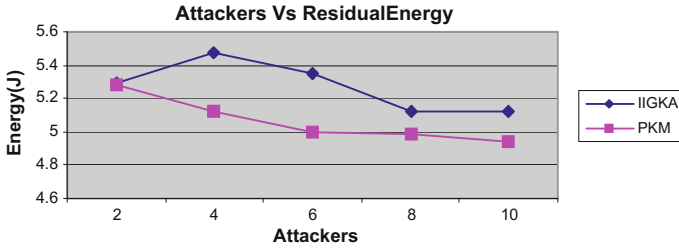


Fig. 5 Residual energy for varying attackers

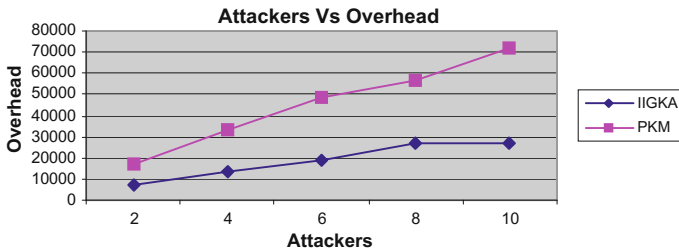


Fig. 6 Control overhead for varying attackers

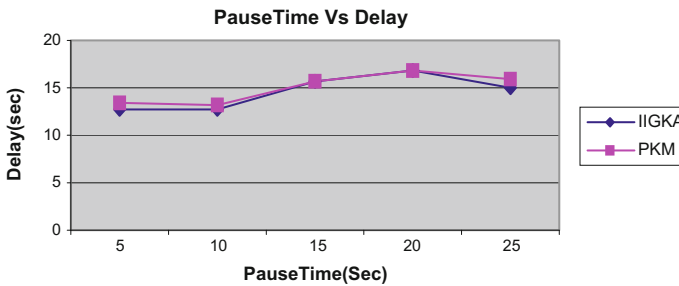


Fig. 7 Delay for varying pause time

The packet drop and packet delivery ratio of IIGKA and PKM protocols for varying the pause time are shown in Figs. 8 and 9, respectively. The figures show that the packet drop is 63% less and the delivery ratio is 52% higher for IIGKA, when compared to PKM.

The residual energy of IIGKA and PKM protocols for varying the pause time, are shown in Fig. 10. The figure shows that IIGKA has 4% higher residual energy than PKM protocol. The control overhead occurred for IIGKA and PKM protocols for varying the pause time are shown in Fig. 11. The figure shows that IIGKA has 52% lesser overhead than PKM protocol.

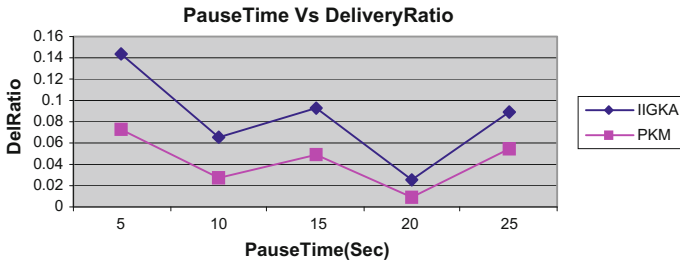


Fig. 8 Delivery ratio for varying pause time

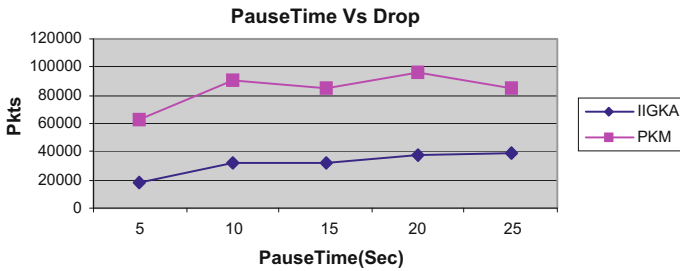


Fig. 9 Packet drop for varying pause time

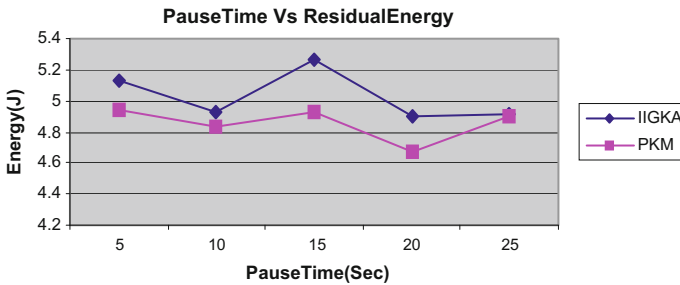


Fig. 10 Residual energy for varying pause time

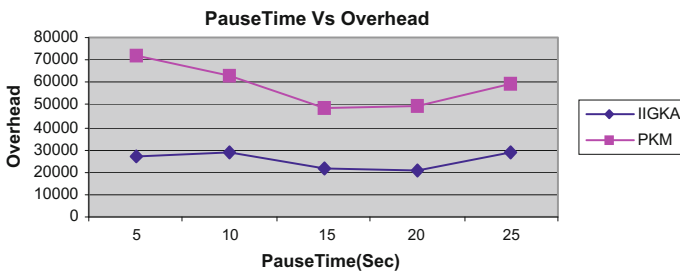


Fig. 11 Control overhead for varying pause time

5 Conclusion

An Intra and Inter Group Key Authentication protocol (IIGKA) for secure group communication has been proposed in this paper. Each member of the group requests its Group Manager for an intra group key. The group manager broadcasts a locked key and then broadcasts a polynomial to enable the retrieval of the locked key. In the inter group key authentication, a member requests another member of another group to aid in creating an inter group key. Then broadcasts the respective polynomial to enable the intended recipient to retrieve the inter group key. Once, the key is authenticated by the respective node, then the involved members can carry out secure communication in MANET.

References

1. Maria Striki, John S. Baras and Kyriakos Manousakis, "A Robust, Distributed TGDH-based Scheme for Secure Group Communications in MANET", IEEE, International Conference on Communication, PP: 2249–2255, 2006.
2. Xixiang Lv and Hui Li, "Secure group communication with both confidentiality and non-repudiation for mobile ad-hoc networks", IET Information Security, ISSN:1751-8709, 2010.
3. Mohamed Younis, Osama Farrag and Bryan Althouse, "TAM: A Tiered Authentication of Multicast Protocol for Ad-Hoc Networks", IEEE Transactions on Network and Service Management, Vol. 9, No. 1, MARCH 2012.
4. Zhiguo Wan, Kui Ren, and Ming Gu, "USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks", IEEE Transactions on Wireless Communications, 2012.
5. Hua-Yi Lin and Tzu-Chiang Chiang, "Efficient Key Agreements in Dynamic Multicast Height Balanced Tree for Secure Multicast Communications in Ad Hoc Networks", EURASIP Journal on Wireless Communications and Networking, PP: 1–15, 2011.
6. Weichao Wang and Yu Wang, "Secure Group-based Information Sharing in Mobile Ad Hoc Networks", IEEE International Conference on Communications, PP: 1695–1699, 2008.
7. Sukin Kang, Cheongmin Ji, and Manpyo Hong, "Secure Collaborative Key Management for Dynamic Groups in Mobile Networks", Journal of Applied Mathematics, Volume 2014, Article ID 601625, 10 pages.
8. Yanji Piao, Jong Uk Kima, Usman Tariqb, Manpyo Hong, "Polynomial-based key management for secure intra-group and inter-group communication," Journal of Computers & Mathematics with Applications, Vol. 65, 2013.

Performance of Efficient Image Transmission Using Zigbee/I2C/Beagle Board Through FPGA

D. Bindu Tushara and P.A. Harsha Vardhini

Abstract Image processing plays a major role in the efficient transmission of images. Representation of images mathematically and performing various operations in digital form makes the process more effective in today's communication systems. Performing this image processing and transfer through various wired and wireless technologies is the major concern. This paper deals with comparison of several such propagation modules for the transmission of images by performing image processing like image compression using discrete wavelet transform, edge detection and noise removal.

Keywords FPGA · I2C protocol · Beagle board · Image compression · ZIGBEE

1 Introduction

Images are the pictorial representation of information which also adds the advantage of its efficient transmission. This efficiency in transmission is increased by performing various image processing technologies and choosing the type of transmission media for its propagation. There are several technologies available for this propagation which includes both wired and wireless technologies. Availing of these depend on the factors including distance between transmitter, receiver and type, length of image to be transmitted. This paper mainly focuses on the three transformation techniques to be performed on image for its efficient transmission.

D. Bindu Tushara (✉) · P.A. Harsha Vardhini
Department of ECE, V.I.T.S, Hyderabad, India
e-mail: tushara.dewdrops@gmail.com

P.A. Harsha Vardhini
e-mail: pahv19@rediffmail.com

1.1 Image Compression

The process involves reduction of the pixel voltage values of an image resulting in its compression. The size of the image is reduced, which results in reducing the effect of redundancy and irrelevance of data in the image. This is done using discrete wavelet transform (DWT) by taking row and column matrix. The rate of compression depends on the size to which pixel voltage values are reduced. There are two forms of compression—lossy and lossless compression. Reconstruction of the original image is done without any loss of data in lossless compression whereas recovery of original image with some loss is lossy compression.

1.2 Edge Detection

The edges of an image are determined using edge detection which reduces the effect of noise in the image transmission. This is performed using kernel matrix masked over the image pixel matrix considered. The values are rounded off to the threshold value taken into consideration [1].

1.3 Noise Removal

There are several types of noise added to the image while its transmission. Due to occurrence of such noise, originality of the image changes with respect to change in the values of pixel intensity. The paper mainly focuses on the removal of one such noise called ‘salt and pepper’. Using sliding window protocol, sliding of the window consisting of the image pixel values is performed and filtering operation is done on it.

2 Transmission Modules

The transformation techniques performed on the image is done using programming FPGA and transmitting the resultant image using various wired and wireless technologies. This paper mainly focuses on the comparisons of such technologies in the efficient transmission of image from transmitter to the receiver section.

2.1 Zigbee Module

Zigbee module is one of the wireless techniques which interface the transmitter and receiver through FPGA. This module is used at the transmitter and receiver using

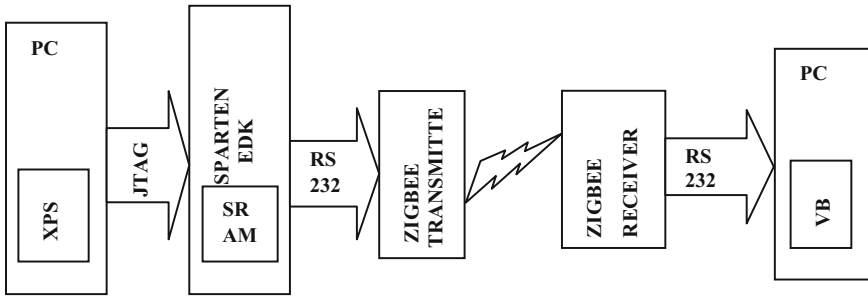


Fig. 1 Transmission using zigbee module

the corresponding modules at both the ends. Wireless transmission is with respect to the transmission done between the zigbee transmitter and receiver. This transmission is shown in Fig. 1.

2.2 I2C Protocol

This protocol is a form of wired transmission between the transmitter and display through FPGA using two control signals. SCL for applying of clock pulse at the start and stop of transmission and actual data transmitted through SDA [2, 3]. These

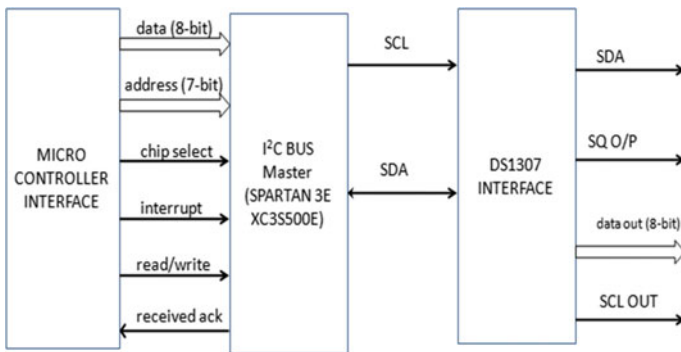


Fig. 2 I2C interface with FPGA

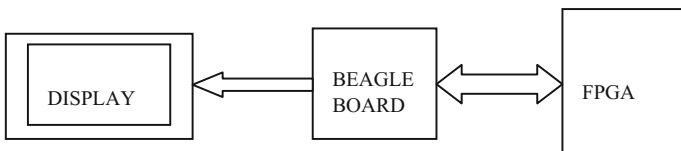


Fig. 3 Transmission with beagle board

Table 1 Comparison

Parameter	Zigbee	I2C	Beagle board
Complexity with hardware	Less	Same as that of zigbee	Comparatively less
Connectivity with FPGA	RS-232	SDA, SCL	I2C/data input, output Port
Transmission rate	Less	More	Higher
Speed of transmission	Moderate	Moderate	Higher
Processor involved	SRAM	DS13707	OMAP3530
Interfacing devices	Direct connectivity between FPGA and zigbee	Microcontroller interface	Direct connectivity through ports
Transmission medium	Wireless	Wired	Wired
Transmitter and receiver	Separate transmitter and receiver modules	No separate transmitter and receiver	No separate transmitter and receiver
Supporting FPGA module	Spartan 3E, EDK kit with SRAM	Spartan 3E	VIRTEX 5, VIRTEX 6
Programming language with FPGA	VHDL/C	VHDL/C	Linux
Software implementation	XPS	XILINX	XILINX
Transmission mode	16 Direct Sequence Channels	Depends on the speed of the bus	Full duplex transmission
Data rate	250 kbps	The data on the SDA line must be stable during the HIGH period of the clock	48 bps
Network topology	Point to point/multipoint	Master-slave	Multipoint connectivity with single board
Range of transmission	Up to 50 kms of distance	6 meters or 20 feet distance	Pixel Clock Frequency is 25–65 MHz
Operating voltage	3.3–3.6 V	Input reference levels are set as 30 and 70% of V_{DD} ; V_{IL} is $0.3V_{DD}$ and V_{IH} is $0.7V_{DD}$	3.3 V
Feasibility	Moderate	Moderate	Comparatively more as it is open source

are controlled by a micro controller and bus interface along with FPGA. The interface with I2C is shown in Fig. 2.

Fig. 4 Noise free output image

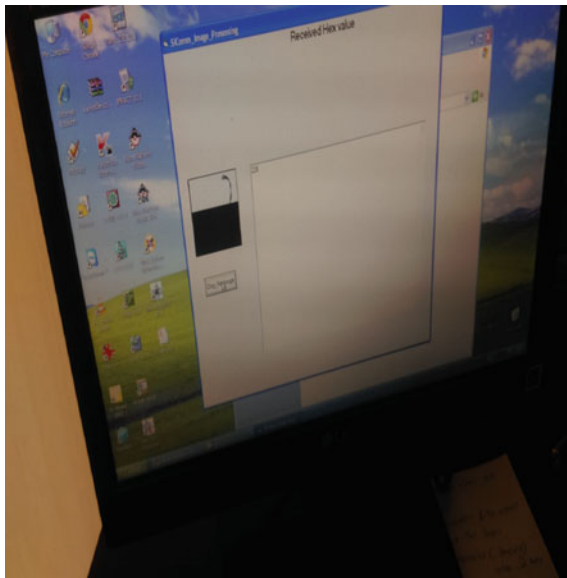
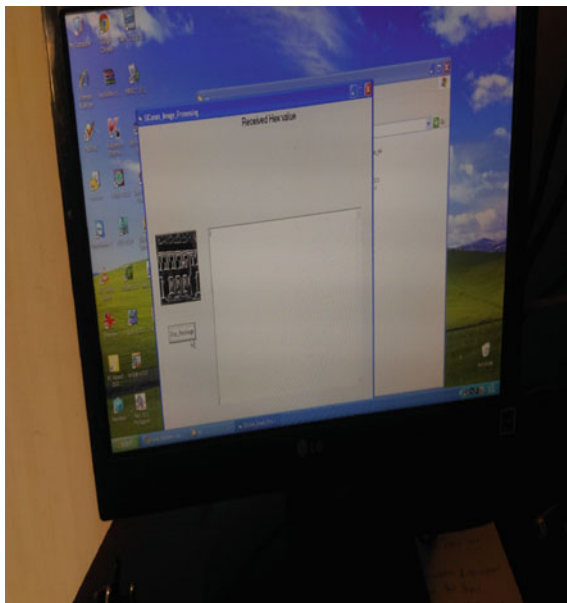


Fig. 5 Received image with edge detection



2.3 Beagle Board

This board is categorized as one of the wired communication transmissions between FPGA and display to transmit the image. The board serves the purpose of PC for getting the input image, performing required transformation on it and displaying it on the display screen [4]. This connectivity between the blocks is shown in Fig. 3. The input message is read from the board and the algorithm for image transformation is performed on FPGA. The resultant image is then given to the display by the board in the form of pixel transmission. The display can also be connected to FPGA kit by using PC. The bidirectional flow between FPGA and beagle board indicates the flow of pixel values of the original image and the transformed image [5]. The image can be read from a predefined one in the beagle board or can be taken from the camera connected to one of the ports of the beagle board.

3 Comparison Parameters

Comparison enhances the usage of available modules by increasing the efficiency of transmission and also makes the users familiar with the respective working techniques and parameters of the module. Proposed modules comparison [6] given in Table 1.

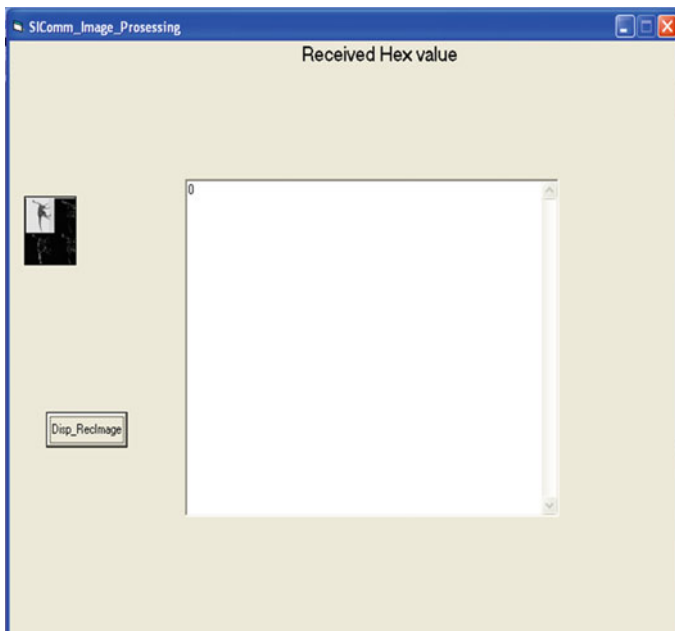


Fig. 6 Output compressed image

4 Results

The modified image is transferred using the modules and shown on the display. Figure 4 shows the noise free image using noise removal algorithm. Figure 5 shows received image with edges detected with edge detection algorithm.

Figure 6 shows the output image with compression rate of one fourth of the original image.

5 Conclusion

By making such comparisons, best outcomes can be achieved with great speed and ease. Beagle board is an open source system which makes it more feasible relative to other modules. This board replaces all other external interfacing hardware devices for its operation. More algorithms can be performed on this board to enhance the techniques in field of image processing.

References

1. Prof. (Dr.) P.K Dash “Implementation of Edge Detection Using FPGA & Model Based Approach” of IEEE 2014, Information Communication and Embedded Systems, pp: 1–6.
2. Prof. Jai Karan Singh, Prof. Mukesh Tiwari, Vishal Sharma “Design and Implementation of I2c master controller on FPGA using VHDL” International Journal of Engineering and Technology (IJET), Vol 4 No 4 Aug-Sep 2012, pp: 162–166.
3. R. Hanabusa, “Comparing JTAG, SPI and I2C,” Spansion’s application note, pp. 1–7, revision 01, April 2007.
4. Pradeep Kumar and Lokeshia “Real Time Implementation of Computer Vision Algorithms on Beagleboard” IOSR Journal of VLSI and Signal Processing, Volume 4, Issue 2, Ver. III (Mar-Apr. 2014), pp. 01–06.
5. Christopher R. Anderson, George Schaertl, and Philip Balister “A Low-Cost Embedded SDR Solution for Prototyping and Experimentation”.
6. Philips Semiconductors, “The IIC-Bus Specifications,” version 2.1, January 2000.

Modified Probabilistic Packet Marking Algorithm for IPv6 Traceback Using Chinese Remainder Theorem

Y. Bhavani, V. Janaki and R. Sridevi

Abstract Denial of Service (DoS) attack is creating a major problem to the internet security. Probabilistic Packet Marking (PPM) algorithm suggested a methodology to overcome the DoS attacks. This methodology selects a packet based on probability to store a part of the IP address of the router in the attack path. The victim combines the marked parts of the IP address, to form the IP address in the attack path. These combinations also contain IP address of routers which are not part of the attack path. They are therefore called false positives. To overcome this drawback we proposed Modified Probabilistic Packet Marking (MPPM) algorithm for IPv6. The packets are now marked with the unique value and this unique value is calculated using Chinese Remainder Theorem (CRT) for every IP address of the router in the attack path. This technique requires less number of marked packets to find the exact IP address, thus reducing the number of false positives. Though IPv6 header length is four times that of IPv4, we could successfully obtain the exact IP address of all the routers in the attack path.

Keywords IP traceback · Modified probabilistic packet marking algorithm · Chinese remainder theorem · Ipv6

Y. Bhavani (✉)

Department of Information Technology, Kakatiya Institute of Technology and Science,
Warangal, India
e-mail: yerram.bh@gmail.com

V. Janaki

Department of Computer Science and Engineering, Vaagdevi College of Engineering,
Warangal, India
e-mail: janakicse@yahoo.com

R. Sridevi

Department of Computer Science and Engineering, Jawaharlal Nehru Technological
University Hyderabad, Hyderabad, India
e-mail: sridevirangu@yahoo.com

1 Introduction

Denial of Service (DoS) attacks impact is usually on the legitimate users, and their services are being denied. Generally attackers are identified by their IP addresses, but the DoS attackers send their packets with spoofed IP addresses. To overcome this problem, the DoS attacks can be detected by constructing the attack path and finding the source router. IP Traceback method is one of the techniques to detect the DoS attacks, and to construct the attack path from the receiver to the sender. Many techniques have been proposed for IP Traceback in IPv4 [1–7] but at present IPv4 is being replaced by IPv6.

Packet marking is the most popular IP Traceback method. In packet marking procedure the routers mark the packets with their identity (IP address). At the victim, after receiving these packets, using the marked information traces the attack path from the victim to the source router.

Now a day's, the number of internet users has increased for more than 3.17 billion people up to December 2015 from that of 18000 sources using Internet, as per the statistics portal [8]. As the users increase, the required number of IP addresses also grows simultaneously. Hence the other alternative is IPv6 which must be used for all practical purposes.

Xuan-Hien Dang et al. [9] in their Probabilistic Packet Marking (PPM) method for IPv6 used the Flow label field of IPv6 datagram header to store the marking information needed to construct the attack path. The unavoidable disadvantage of this technique is that it requires more number of packets to construct the attack path.

Yulong Wang et al. [10] and Chi Chen et al. [11], proposed a hybrid IP traceback method for IPv6 networks. They combined the packet marking and packet logging techniques. The advantage is it records the path information both on the router and in the packets. The implicit disadvantage of this method is found to be storage overhead at the routers and collection of huge number of packets at the victim.

Syed Obaid Amin et al. [12] proposed IP traceback method for IPv6 networks. This method used the Hop by Hop extension header to store as a whole the marking information (128 bits of IP address), which in general could be used to store fragment information. Hence, this technique failed whenever the packet size exceeded the Path Maximum Transmission Unit (PMTU).

Long Cheng et al. [13] proposed an opportunistic piggyback marking for IP Traceback. This method assumed all the routers as traceback enabled routers and marking information is passed to the destination through external-flows also which reduced the delivery delay of messages to the victim. This method used the Flow label field to store the marking information.

In MPPM algorithm for IPv4 [14] using CRT, a unique value corresponding to the IP address is calculated and sent to the victim instead of the IP address itself.

This technique reduced the number of combinations and hence false positives. Ahmad Fadlallah [15] proposed a method to mark the far away routers from the victim without the packets re-marked by the nearer routers. So less number of marked packets are needed to construct the attack path.

In this paper, we have extended MPPM Traceback for IPv6 network. Our paper is articulated as follows: Sect. 2 outlines IPv6 header encoding. In Sect. 3 we describe the Modified Probabilistic Packet Marking algorithm for IPv6. Section 4 provides the results and Sect. 5 concludes the paper.

2 IPv6 Header Encoding

The main aim of the IP Traceback method is to find the source router of the attack path. The routers in the attack path store their IP address identity in the IPv6 header to find the source router. This section, explains the usage of Chinese Remainder Theorem for encoding the IPv6 header.

Chinese Remainder Theorem (CRT) states that

$$X \equiv a_i \pmod{m_i} \tag{1}$$

where $1 \leq i \leq k$ has a unique solution modulo M . Let $m_1, m_2, m_3, \dots, m_k$ be the pair wise relatively prime numbers.

According to our proposed methodology each router in the attack path, calculates a unique X value for its IP address using CRT. There are six kinds of extension headers in IPv6 [16] among which only Hop by Hop header can be used to send the X values. This header is examined and processed by every router along the packet path, but it creates fragmentation problem when the packet size exceeds the Path Maximum Transmission Unit (PMTU) [12]. The fragmentation is permitted only at the source of the path in the IPv6. The intermediate routers throw away the packets which need to be fragmented before they arrive to the actual victim. Xuan-Hien Dang et al. [9] avoided this problem using the Flow Label field to mark the packets. Xuan-Hien Dang et al. [9] suggested that as the Flow Label field of the IPv6 header is not used for other purposes, it could be used to send marking information. In our proposed system, the X value is sent to the victim by placing it in the Flow Label field of IPv6 header.

The IPv6 packet header format is shown in Fig. 1. In our proposed algorithm, we used 20 bit Flow Label to store the identity of the router. The IPv6 IP address length is 128 bits, and the corresponding X value so calculated is also 128 bits, this did not

Fig. 1 IPv6 header format

Version	Traffic class	Flow Label	
Payload length		Next header	Hop limit
Source address			
Destination address			

fit into the Flow Label of the IPv6. This draw back has inadvertently made us to fragment the IP address and the corresponding X value into 16 equal parts each of 8 bits.

For example the IP address 2001:0470:1F00:0296:0209:0000:FE06:67B4 is split by considering the two consecutive hexadecimal values as follows $IP_1 = 20$, $IP_2 = 01$, $IP_3 = 04$, $IP_4 = 70$, $IP_5 = 1F$, $IP_6 = 00$, $IP_7 = 02$, $IP_8 = 96$, $IP_9 = 02$, $IP_{10} = 09$, $IP_{11} = 00$, $IP_{12} = 00$, $IP_{13} = FE$, $IP_{14} = 06$, $IP_{15} = 67$ and $IP_{16} = B4$. If these IP address parts are directly sent to the victim as it is, it becomes difficult to combine the IP address parts correctly. Thus it could result in IP addresses that are not in the attack path (false positives). To overcome this, the above hexadecimal parts are converted to decimal and corresponding X value is calculated. This X value is fragmented and sent to the victim as an identity. The victim can combine the X value fragments wholly, as the X value is unique for each IP address, thus reducing the false positives. If the IP address is of the form 2001:db8:3c4d:1::1 then in our proposed algorithm it is considered as 2001:0db8:3c4d:0001:0000:0000:0000:0001, for dividing it into 16 equal parts.

The X value for the IP address 2001:0470:1F00:0296:0209:0000:FE06:67B4 is calculated by applying CRT Eq. (1). This X value is congruent modulo to IP_1 to IP_{16} as shown below.

$$X \equiv IP_i \pmod{m_i} \tag{2}$$

where $1 \leq i \leq 16$, and we assume $m_1 = 193$, $m_2 = 197$, $m_3 = 199$, $m_4 = 211$, $m_5 = 217$, $m_6 = 223$, $m_7 = 227$, $m_8 = 229$, $m_9 = 233$, $m_{10} = 239$, $m_{11} = 241$, $m_{12} = 247$, $m_{13} = 251$, $m_{14} = 253$, $m_{15} = 255$, $m_{16} = 256$. All these are pair wise relatively prime numbers.

So, the X value can be calculated as shown below

$$X \equiv \left(\sum_{i=1}^{16} IP_i b_i \right) \pmod{M} \tag{3}$$

where

$$M = \prod_{k=1}^{16} m_k \quad (3.1)$$

$$b_i = M_i \times M_i^{-1} \pmod{m_i}, \text{ here } M_i = M/m_i \quad (3.2)$$

The algorithm used to calculate X value at each router for its IP address is given below:

```

X=0
/* M, Mi, Minvi (Mi-1) are considered as BigInteger to store larger numbers. X data
type is also considered BigInteger to store 128 bit unique X value */
for( i=1 to 16 do)
{
    M=M.multiply(mi) //eqn 3.1
/* modInverse, multiply, divide add and mod are BigInteger functions to perform
mathematical calculations */
    Mi=M.divide(mi)
    Minvi= Mi.modInverse(mi)
    bi=Mi.multiply(Minvi)//above three steps solve eqn 3.2
    X= X.add(bi.multiply(BigInteger.valueOf(IPi)))
X=X mod(M) // eqn 3

```

The X value for the above given 16 IP address parts is 38010551344015449631255458692619104868 and its binary format is 111001001100010010000110111100001110001110100000010010011010110101011100101010000011010001101000101110100111001001100100. When the number of bits of X value is not equally partitioned into 16 parts, we have to place zeros to the left of binary format of X value so that it is partitioned into 16 parts. This X value is partitioned into 16 parts each consisting of 8 bits as $X_0 = 00011100$, $X_1 = 10011000$, $X_2 = 10010000$, $X_3 = 11011111$, $X_4 = 00001111$, $X_5 = 00011101$, $X_6 = 00000010$, $X_7 = 01001101$, $X_8 = 01101010$, $X_9 = 11100101$, $X_{10} = 01000000$, $X_{11} = 11101000$, $X_{12} = 11010001$, $X_{13} = 01110100$, $X_{14} = 11110010$, $X_{15} = 01100100$. Each two consecutive parts are concatenated into a fragment as X_0X_1 , X_1X_2 , X_2X_3 , X_3X_4 , X_4X_5 , X_5X_6 , X_6X_7 , X_7X_8 , X_8X_9 , X_9X_{10} , $X_{10}X_{11}$, $X_{11}X_{12}$, $X_{12}X_{13}$, $X_{13}X_{14}$, $X_{14}X_{15}$, $X_{15}X_0$ and are sent through the 20 bit Flow Label. The consecutive parts are combined in order to reconstruct the exact parts from X_0 to X_{16} at the victim.

Each fragment is placed in the Flow Label from 0th to 16th bit and fragment number from 17th to 20th bit to identify the fragment. The number of hops (distance d) from the victim to the source is stored in Hop limit field of IPv6 header format.

3 Modified Probabilistic Packet Marking (MPPM) Algorithm Using CRT in IPv6

3.1 Marking Procedure

In this MPPM algorithm for IPv6, at each router the unique X value for its IP address is calculated using CRT. This X value is divided into 16 parts. The marking procedure for IPv6 is explained as follows. At each router we passed a threshold probabilistic value (P_m). We also used a flag condition to avoid further marking of a marked packet by subsequent routers [17]. When a packet arrives at the router, a random number “rand” is generated, and it lies between 0 and 0.999. If rand is less than the assumed marking probability (P_m) and flag value is equal to zero then the fragment and the fragment number are stored in the Flow Label field. The maximum distance ($2 \times d$) is stored in the Hop limit field of IPv6 header. The flag is set to 1, indicating that it has been marked. When the subsequent router receives the marked packet and tries to mark, it is not allowed to be marked as the flag value is 1 already. The algorithm is as given below.

Marking Procedure at router R

```

Fragno  $\leftarrow$  0
For ( each packet  $pt$  received from router  $R$  )
{ Generate a random number  $r$  and between [0..1)
  If( $rand < P_m$  and  $flag=0$ ) then
     $pt$ .Flow Label[17-20]  $\leftarrow$   $fragno$ 
     $pt$ .Hop limit  $\leftarrow$   $2 \times d$ 
     $pt$ .Flow Label [1-16]  $\leftarrow$   $X[fragno] + X[(fragno + 1) \bmod 16]$ 
     $fragno \leftarrow (fragno+1) \bmod 16$ 
     $flag \leftarrow 1$ 
  if( $flag = 1$ )
     $pt$ .Hop limit =  $pt$ .Hop limit-1
}
```

3.2 Reconstruction Procedure

In this method, the victim after receiving the marked packet extracts the necessary information from IPv6 packet header to reconstruct the attack path. The fragment

(1–16 bits) information from the Flow Label field, fragment number (17–20 bits) of Flow Label field and the distance from the Hop limit field are extracted and placed in a table called as ‘Resulttable’. As the routers probabilistically mark the packets, at times we could have received same information from more than one packet, and hence the duplicates have to be removed. The remaining rows were ordered according to the fragment number and distance d , so that the successive fragments could be compared. This comparison permitted us to combine the correct part of the fragments in order to get the exact value of X . Let S_d denote the set of routers that are d distance away from the victim. This S_d is initialized as an empty set.

Now, for all ordered combinations of fragments, the successive fragments are compared to achieve the exact X value consequently the IP address of the router of the attack path is found. The above procedure is now explained with the help of an example. A fragment 0 which is a combination of X_0X_1 (a part of X value), is compared with the fragment 1 which is a combination of X_1X_2 of the same X value, at the same distance d . The least significant 8 bits (LS8 bits) of the fragment 0 i.e., X_1 is compared with the most significant 8 bits (MS 8 bits) of fragment 1. If this comparison is matched then we could get first 16 bits of X value i.e., X_0X_1 . Similarly X_2 (LS 8 bits) of fragment 1 is compared with X_2 (MS 8 bits) of the fragment 2. If this comparison was found to be true, then we concatenate X_2 to X_0X_1 to get 24 bits of X value. Similar process is continued for all the remaining fragments to achieve 128 bits of IPv6 address of a router altogether. Finally X_0 (LS 8 bits) of fragment 15 is compared with X_0 (MS 8 bits) of fragment 0 to check whether the right parts of X value are properly appended.

From the obtained X value we derived all the 16 parts of the IP address by applying modular inverse as follows.

$$IP_i \equiv X \pmod{m_i}$$

where $1 \leq i \leq 16$ and to obtain the IP address, IP_1 to IP_{16} are converted to hexadecimal values and concatenated as follows $IP_1IP_2: IP_3IP_4: IP_5IP_6: IP_7IP_8: IP_9IP_{10}: IP_{11}IP_{12}: IP_{13}IP_{14}: IP_{15}IP_{16}$.

Similar process was applied for all the fragments having different distances. From these X values by applying modular inverse and converting to Hexadecimal values we obtained the exact IP addresses in the attack path without any false positives.

Reconstruction procedure at victim v

Let Resulttable be a table of tuples containing fragno, fragment and distance for each packet pt from attacker

```

Resulttable.Insert(pt.fragno,pt.fragment, pt.distance)
  if pt.distance > maxd then
    maxd := pt.distance
  Remove duplicates from the Resulttable
  /* delete from Resulttable where ID not in (select min(ID) from Resulttable
  group by fragno, fragment, distance) */
  Let  $S_d$  be empty for  $0 \leq d \leq \text{maxd}$ 
  for  $d := 0$  to  $\text{maxd}$ 
    /* Select pt.fragno, pt.fragment from Resulttable pt, Resulttable pt1 where
    pt.substr(0,7) = pt1.substr(8,15) and pt.distance=d ordered by pt.fragno */
    for all ordered combinations & successive fragments
      if( $pt.\text{substring}(8,15) = pt1.\text{substring}(0,7)$ )
        /* where pt and pt1 are two successive fragments */
        if( $pt.\text{fragno} = 0$ )
           $S_d := pt.\text{fragment}$ 
        else
           $S_d := \text{Concatenate}(S_d, pt.\text{substring}(8,15))$ 
    for  $d=0$  to  $\text{maxd}$ 
       $\text{firstpart} := pt.\text{substring}(0,7)$ ;
       $\text{lastpart} := pt.\text{substring}(128,136)$ ;
      if( $\text{firstpart} = \text{lastpart}$ )
         $X_{bin} := S_d.\text{substring}(0, 128)$ 
        Convert  $X_{bin}$  from decimal to binary and store in  $X$ 
    /* Find  $IN_1 IN_2 IN_3 IN_4 \dots IN_{16}$  using CRT */
     $IN_1 := X \bmod 193$ 
     $IN_2 := X \bmod 197$ 
     $IN_3 := X \bmod 199$ 
     $IN_4 := X \bmod 211$ 
     $IN_5 := X \bmod 217$ 
     $IN_6 := X \bmod 223$ 
     $IN_7 := X \bmod 227$ 
     $IN_8 := X \bmod 229$ 
     $IN_9 := X \bmod 233$ 
     $IN_{10} := X \bmod 239$ 
     $IN_{11} := X \bmod 241$ 
     $IN_{12} := X \bmod 247$ 
     $IN_{13} := X \bmod 251$ 
     $IN_{14} := X \bmod 253$ 
     $IN_{15} := X \bmod 255$ 
     $IN_{16} := X \bmod 256$ 
    Convert  $IN_1$  to  $IN_{16}$  to hexadecimal, store in  $IP_1$  to  $IP_{16}$ 
    Combined IP address is:  $IP_1IP_2: IP_3IP_4: IP_5IP_6: IP_7IP_8: IP_9IP_{10}: IP_{11}IP_{12}: IP_{13}IP_{14}: IP_{15}IP_{16}$ 

```

Table 1 The IP addresses and the corresponding X values

IP address	X value (128 bits)
2001:0470:1F00:0296: 0209:0000:FE06:B7B4	00011100100110001001000011011111000011110001110 10000001001001101011010101110010101000000110100 01101000101110 1001111001001100100
2001:0470:1F00:0296: 0432:FF26:F236:F236	00011100011001011010001011111100010100001000001 10001001101001011001010100011010000000011111101 1000110110101011100010110000110110
2001:0470:1F00:0296: 0432:FF26:FF36:AB36	10010100011010001001111000000110001000011101100 11011000000101111101100101111001110011100100010 00 0001110000000011111110100110110

4 Results

We considered a linear network with three assumed IPv6 addresses R1, R2 and R3, where R1 is 2001:0470:1F00:0296:0209:0000:FE06:B7B4, R2 as 2001: 0470:1F00:0296:0432:FF26:F236:F236 and R3 as 2001:0470:1F00:0296:0432:F26:FF36:AB36. We implemented our proposed method as explained in Sect. 2 using Java language and its networking features. At each router its IP address is divided into 16 parts and each part is converted into its corresponding binary value. Then we calculated a unique X value by applying CRT on these 16 IP address parts as shown in Sect. 2 (Eqs. 3.1 and 3.2).

The unique X values for the above IP addresses are shown in the Table 1. For example let the X value corresponding to R1 be divided into 16 parts, as $X_0 = 00011100$, $X_1 = 10011000$, $X_2 = 10010000$, $X_3 = 11011111$, $X_4 = 00001111$, $X_5 = 00011101$, $X_6 = 00000010$, $X_7 = 01001101$, $X_8 = 01101010$, $X_9 = 11100101$, $X_{10} = 01000000$, $X_{11} = 11101000$, $X_{12} = 11010001$, $X_{13} = 01110100$, $X_{14} = 11110010$, $X_{15} = 01100100$. Then two successive parts are combined to form a fragment, some sample fragments are fragment 0 (X_0X_1) is 0001110010011000, fragment 1 (X_1X_2) is 1001100010010000, and so on to fragment 14 ($X_{14}X_{15}$) is 1111001001100100, fragment 15 ($X_{15}X_0$) is 0110010000011100. These fragments are stored in the IPv6 header of a packet along with its fragment number (fragno) and distance (d).

At the victim required marked packets information is extracted and the attack path is reconstructed as explained in Sect. 3.

5 Conclusions

To overcome the DoS attacks one of the best methods was to reconstruct the attack path and find the address of the source router. Accordingly, Savage et al. proposed PPM [1] which finds the IP addresses (IPv4) of various routers of the attack path,

but unfortunately with a very large number of false positives during the construction of the attack path.

This was now modified by us to MPPM which reduced drastically the number of false positives with the application of CRT. Even though the length of IPv6 is four times that of IPv4, we could successfully achieve the exact IP address of the router in the attack path as follows.

1. Considering the CRT rule, in our proposed method, the selected pair wise relatively prime numbers are 193, 197, 199, 211, ..., 253, 255, 256 as listed in the reconstruction procedure at victim v (Sect. 3.2).
2. The false positives occur only when the above listed relatively prime numbers lies between that number to 255 at each and every specified positions of the IP address. For example, even if false positive occurred it could occur when IP_1 address part lies between 193 and 255. Similarly, IP_2 lies between 197 and 255 and so on. This product term is very less when compared to 256^{16} .

Hence this high success rate helps the victim to construct the attack path exactly. The future scope of our idea can be extended to multiple attack paths environment.

References

1. Savage, S., Wetherall, D., Karlin, A., Anderson, T.: Practical Network Support for IP Traceback. In: ACM SIGCOMM conference, vol. 30. Issue 4, pp 295–306 (2000).
2. Song, D.X., Perrig, A.: Advanced and Authenticated Marking Schemes for IP Traceback. In: IEEE INFOCOM, pp. 878–886 (2001).
3. Dean, D., Franklin, M., Stubblefield, A.: An Algebraic Approach to IP Traceback. ACM Trans. Information and System Security, pp. 3–12 (2001).
4. Harsha K. Kalutarage., Siraj A. Shaikh., Indika P. Wickramasinghe., Qin Zhou., Anne E. James.: Detecting stealthy attacks: Efficient monitoring of suspicious activities on computer networks. Computers and Electrical Engineering, vol. 47. pp. 327–344, (2015).
5. Park, K., Lee H.: On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial-of-Service Attacks. In: IEEE INFOCOM (2001).
6. Marion Vasseur., Xiuzhen Chen., Rida Khatoun., Ahmed Serhrouchni.: Survey on Packet Marking Fields and Information for IP Traceback. In: International Conference on Cyber Security of Smart cities, Industrial Control System and Communications (SSIC) (2015).
7. Karanpreet Singh., Paramvir Singh., Krishan Kumar.: A systematic review of IP traceback schemes for denial of service attacks. Computers & Security, vol. 56. pp 111–139, (2016).
8. The Statistics Portal, <http://www.statista.com/topics/1145/internet-usage-worldwide>.
9. Xuan-Hien Dang, Emil Albright, Abdullah.: Performance analysis of probabilistic packet marking in IPv6. Computer Communications, vol. 30, pp 3193–3202 (2007).
10. Yulong Wang, Sui Tong, Yi Yang.: A practical hybrid IP traceback method for IPv6. Journal of Convergence Information Technology, vol. 7. pp. 173–182, (2012).
11. M. Hamed-Hamzehkoliae., Chi Chen., Xue Tian., Reza Sanei., Masoud Khalil Nezhad., “Bee-Based IP Traceback”, 11th International Conference on Fuzzy Systems and Knowledge Discovery, pp 968–972 (2014).
12. Syed Obaid Amin, Myung Soo Kang, and Choong Seon Hong.: A light weight IP Traceback mechanism on IPv6. In: EUC workshops, LNCS 4097, pp. 671–680, (2006).

13. Long Cheng., Dinil Mon Divakaran., Wee Yong Lim., and Vrizlynn L. L.: Opportunistic Piggyback Marking for IP Traceback. *IEEE Transactions on Information Forensics and Security*, vol. 11. pp 2, (2016).
14. Bhavani Y., Janaki V., Sridevi R.: IP traceback through modified probabilistic packet marking algorithm using Chinese remainder theorem. *Ain Shams Engineering Journal*, vol. 6, pp 715–722, (2015).
15. Ahmad Fadlallah., “Adaptive Probabilistic Packet Marking Scheme for IP Traceback”, *Computer Applications and Information Systems (WCCAIS)*, (2014).
16. Stephen, E., Deering, Robert, M., Hinden, Internet Protocol: Version 6 (IP v6) Specification, RFC 2460 (1998).
17. Bhavani, Y., Janaki, V., Sridevi, R.: IP traceback through Modified Probabilistic Packet Marking algorithm. In: *IEEE Region 10 Conference TENCON* (2013).

Taxonomy of Polymer Samples Using Machine Learning Algorithms

Kothapalli Swathi, Sambu Ravali, Thadisetty Shravani Sagar
and Katta Sugamya

Abstract The rapid growth in technology has led to the decrease in manual work and is creating most of the objects in various industries of machine-driven. One such automation need is found in the chemical industry where machine driven package needed for the classification of various kinds of plastics supported their absorbance values. One of the efficient algorithms used for cataloguing is through support a vector machine which provides a classification model that is trained and tested. A solution to automate the sorting of various kinds of plastic by using the Fisher iris data set (which is a result of Near Infrared Spectroscopy (NIRS)). Plastics are everyday used non-biodegradable materials once not disposed properly have adverse effects on the atmosphere. For recycling of plastics totally different sorts of plastics (polymers) need to be known and separate. For economic reasons plastics must known and sorted instantly. The Fisher Iris data set that can be employed by us is a result of NIRS. The NIRS techniques have been used for the instantaneous identification of plastics. Measurements made by NIRS are quite accurate and fast. The necessary algorithm needed to process the NIRS data and to obtain information on the polymer category is written on the general purpose, high-level programming language Python as well as on MATLAB. In order to extend the efficiency of this process we also implement KS algorithm.

Keywords Machine learning · SVM · KS algorithm

K. Swathi (✉) · S. Ravali · T. Shravani Sagar · K. Sugamya
Department of IT, Chaitanya Bharathi Institute of Technology, Hyderabad, India
e-mail: swathi.kothapally@gmail.com

S. Ravali
e-mail: ravali.sambu5@gmail.com

T. Shravani Sagar
e-mail: sagar.shravani10@gmail.com

K. Sugamya
e-mail: sugamya.cbit@gmail.com

1 Introduction

Plastics are omnipresent and defile the atmosphere. Throwing away of plastics has become a technological and social subject that has created and attracted a lot of attention from researchers, business people, politicians, environmental activists and the common people. One way to cut back the ecological pollution, due to plastic waste encompassing disposable and durable, is to salvage them. That is, to recover the used plastics from municipal or industrial wastes streams and convert them into new useful objects. Salvaging of plastic-wastes is steady gaining importance as result of the efforts on conservation of oil resources and the shortage of disposal sites. Moreover, it is uneconomical and the working conditions don't be solely unpleasant however even dangerous to health. Considering the above difficulties, an automatic plastic sorting approach, involving automatic identification of materials followed by a mechanical sorting, appears as correlate alluring different to manual sorting. NIR spectroscopy identifies individual plastic sorts and offers a capable approach to waste sorting.

Present systems of sorting are done either fully manually or mistreatment specialised machinery that is very expensive. It also needs lots of human resource for maintaining this method of sorting plastics. This manual process is not thus effective or efficient. It is highly prone to error. The cross verification of this manual process is once more extremely troublesome. So abundant of time is consumed in during this entire process. Hence associate machine-driven package which might kind the plastics supported the values obtained from NIRS is to be developed.

1.1 Objective

With this paper, we support in the development of a plastic sorting technology using NIR (Near Infrared) Spectroscopy. Different sorts of plastics viz, PPT, PVC etc. show different behaviour once subjected to Near Infrared rays. This difference in behaviour will be analysed to kind numerous kinds of plastics in pace and with negligible error. The technology has high value in the plastic exploitation business alongside several different similar industries. The main idea of this paper is to develop and to understand however on sorting of varied plastic sorts and then facilitate transfer this method for the exploitation of industry/business.

1.2 Problem Definition

The plastic waste typically includes six sorts of materials particularly, polyethylene (PE), poly-ethylene teraphthalate (PET), poly-propylene (PP), poly-vinyl-chloride (PVC), high density polyethylene (HDPE) and polystyrene (PS). The tentative lab

model classifies them and kinds PET alone. Through the existing set-up, PET materials can be typed close to 100% with up to 200 kg per hour outturn. The highest outturn is proscribed by the speed of the spectrograph utilized in the system. Higher throughputs up to 1 tonne/hr will be achieved by using high-speed spectrographs and quicker sorting routine.

The proposed methodology ought to be in a position to take the associates analysis of NIRS graphs as input and will provide an output that classifies the polymers supported their absorbance values and different characteristics [1].

2 Methodologies

The main plan of this paper was to develop a knowhow on sorting of various plastic varieties then facilitate transfer this methodology for the employment of trade. So the NIRS spectroscopy analysis is used to urge the dataset containing the polymer samples. Before, we have a tendency to discuss the method of classification we tend to would like to offer a speedy report on NIRS spectroscopic analysis.

Near-infrared spectroscopy (NIRS) might be a qualitative technique that uses the near-infrared region of the spectrum (from regarding 800 to 2500 nm). Typical applications embrace pharmaceutical, medical diagnostics (including blood glucose and pulse oximetry), food and agrochemical quality control. Plastic resins live composed of a spread of compound varieties. Similarities within the size and form of the resins build them difficult to differentiate by sight alone. During this application note, the utilization of NIR spectroscopy for representation of distinctive coloured plastic resins (Fig. 1).

2.1 SVM

In machine learning, support vector machines (SVMs, also support vector networks) square measure supervised learning models with associated learning algorithms that analyze information and acknowledge patterns, used for classification and regression analysis.

2.2 Discriminant Analysis Techniques

There are two types of these techniques; one of these techniques is LDA [2, 3]. Linear discriminate analysis (LDA) could be a technique used in statistics, pattern recognition and machine learning to seek out a linear combination of features/options that characterizes or separates two or lot classes of objects or events. Another technique under discriminant analysis is QDA. Quadratic

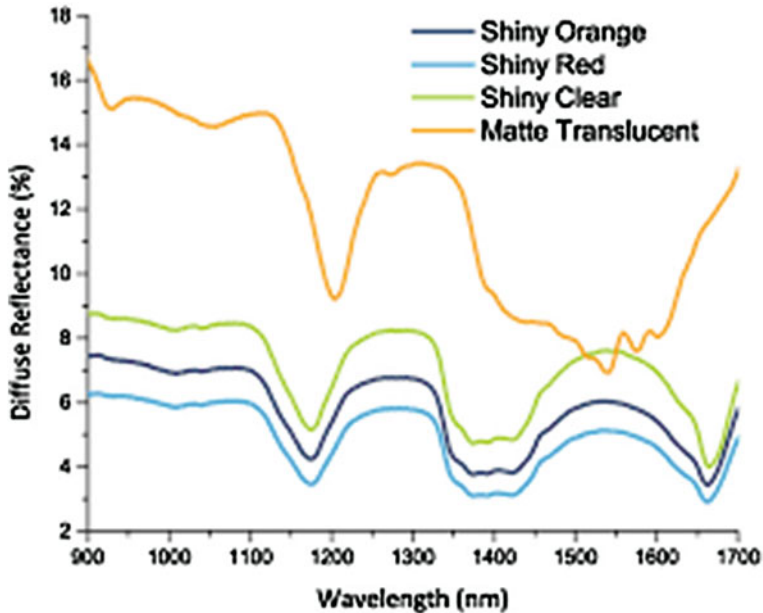


Fig. 1 NIRS Spectroscopy

discriminate analysis (QDA) is closely associated with linear discriminate analysis (LDA), wherever it's assumed that the measurements from every category square measure commonly distributed.

EXAMPLE OF FISHER IRIS

The Iris flower data set or Fisher's Iris data set is a variable data set introduced by Sir Ronald Fisher (1936) as an example of discriminant analysis. It's generally known as Anderson's Iris data set because Edgar Anderson collected the data to quantify the morphologic variation of Iris flowers of three related species. Two of the three species were collected within the Gaspé Peninsula "all from an equivalent pasture, and picked on the equivalent day and measured at the equivalent time by the equivalent person with the equivalent apparatus". The data set consists of fifty samples from each of three species of Iris (Iris setosa, Iris virginica and Iris versicolor). Four features were measured from every sample: the length and also the width of the sepals and petals, in centimetres. Supported the mix of those four features, Fisher developed a linear discriminant model to tell apart the species from one another (Figs. 2, 3 and 4).

Fig. 2 Fisher iris data set

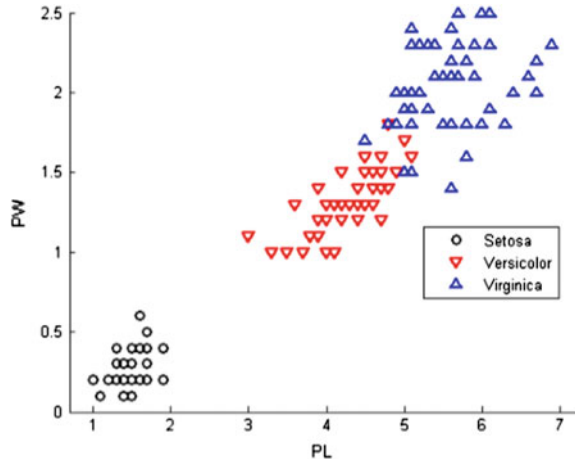
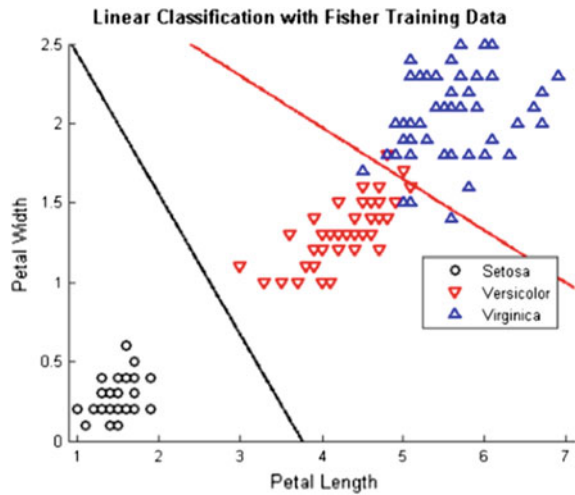


Fig. 3 Linear discrimination of fisher iris data set



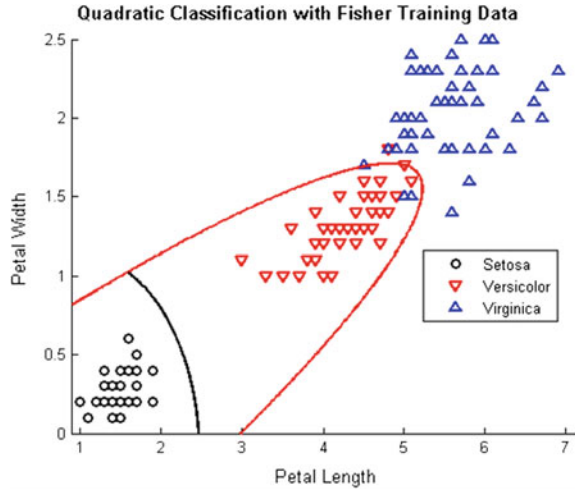
2.3 Types of Classifiers

Initially we implement the binary classifiers in python. The classifiers that we are using to compare the efficiencies are Linear, Polynomial, RBF and Linear SVC.

2.3.1 Linear Classifier

In the field of machine learning, the goal of applied math classification is to use an object's characteristics to identify which class (or group) it belongs to a linear

Fig. 4 Quadratic discrimination of fisher iris data set



classifier achieves this by creating a classification call supported the worth of a linear combination of the characteristics [4]. If the input feature vector to the classifier is a real vector, then the output score is [5]

$$y = f(\vec{w} \cdot \vec{x}) = f\left(\sum_j w_j x_j\right),$$

where \vec{w} could be a real vector of weights and f could be a function that converts the dot product of the two vectors into the specified output.

2.3.2 Polynomial Classifier

A quadratic classifier is employed in machine learning and applied math classification to separate measurements of two or more classes of objects or events by a quadric surface [4]. Statistical classification considers a collection of vectors of observations x of an object or event, every of that includes a familiar sort y . For a quadratic classifier, the proper solution is assumed to be quadratic within the measurements; therefore y set supported [6]

$$x^T A x + b^T x + c$$

2.3.3 RBF Classifier

In the field of mathematical modelling, a radial basis function network is an artificial neural network that uses radial basis functions as activation functions [4].

The output of the network is a linear combination of radial basis functions of the inputs and neuron parameters [7]. Radial basis function networks have many uses, including approximation, time, classification, and system control.

2.3.4 Kennard Stone Algorithm Significance

All the classifiers above defined are implemented in such a way that the training data and test data is split randomly and there is no particular way of splitting data by the user. So KS algorithm helps to split training and test data set separately by ranking the samples. KS algorithm ranks the data samples on the basis of their affinity to the support vectors and hence comes up with the best possible training set for the algorithm [8].

3 Results

3.1 Linear Classifier

The Fig. 5 shows that Linear classifier classifies Training data with an accuracy of 97% and testing data with an accuracy of 88.8% giving one sample to be wrongly classified as type 4 when it is type 3 and also wrongly classifying another sample as type 3 when it is type 4 which is represented by confusion matrix [9].

Fig. 5 Efficiency with linear classifier

```

None
Linear Classifier
[[2 0 0 0 0]
 [0 7 0 0 0]
 [0 0 3 1 0]
 [0 0 1 2 0]
 [0 0 0 0 2]]
TestData -accuracy score:
0.888888888889

[[18 0 0 0 0]
 [ 0 12 0 0 1]
 [ 0 0 16 0 0]
 [ 0 1 0 7 0]
 [ 0 0 0 0 13]]
TrainingData -accuracy score:
0.970588235294
    
```

Fig. 6 Efficiency with polynomial classifier

```

Polynomial Classifier
[[2 0 0 0 0]
 [7 0 0 0 0]
 [4 0 0 0 0]
 [3 0 0 0 0]
 [2 0 0 0 0]]
TestData -accuracy score:
0.111111111111

[[18 0 0 0 0]
 [13 0 0 0 0]
 [16 0 0 0 0]
 [ 8 0 0 0 0]
 [13 0 0 0 0]]
TrainingData -accuracy score:
0.264705882353

```

3.2 Polynomial Classifier

The Fig. 6 shows that Polynomial classifier classifies Training data with an accuracy of 26.4% by wrongly classifying all samples to be type 1 and testing data with an accuracy of 11.1% by wrongly classifying all samples to be type 1 which is represented by confusion matrix.

3.3 RBF Classifier

The Fig. 7 shows that Polynomial classifier classifies Training data with an accuracy of 95.5% by wrongly classifying one sample to be type 5 when it is type 4 and testing data with an accuracy of 77.7% by wrongly classifying three samples which is represented by confusion matrix.

3.4 Results for Implementation in MATLAB

3.4.1 Cross Validation

The Fig. 8 shows generation of testing data (66) and training data (20) using k-fold technique.

Fig. 7 Efficiency with RBF classifier

```

RBF Classifier
[[1 0 1 0 0]
 [0 6 0 1 0]
 [0 0 3 1 0]
 [0 1 0 2 0]
 [0 0 0 0 2]]
TestData -accuracy score:
0.777777777778

[[18 0 0 0 0]
 [ 0 12 0 0 1]
 [ 0 0 16 0 0]
 [ 0 1 0 6 1]
 [ 0 0 0 0 13]]
TrainingData -accuracy score:
0.955882352941
    
```

Fig. 8 Cross validation with K-fold technique

```

>> SVM_CrossVal

ans =

    0.7907

ans =

    66    18
     0     2
     0     0
    
```

3.4.2 Multi Class Classification

The Fig. 9 shows that Multiclass classifier classifies Training data with an accuracy of 79.49% by wrongly classifying 4 samples to be type 2 when it is type 3 and testing data with an accuracy of 75.0% by wrongly classifying two samples.

The Fig. 10 show ranking the samples in order to generate efficient set of training and testing data.

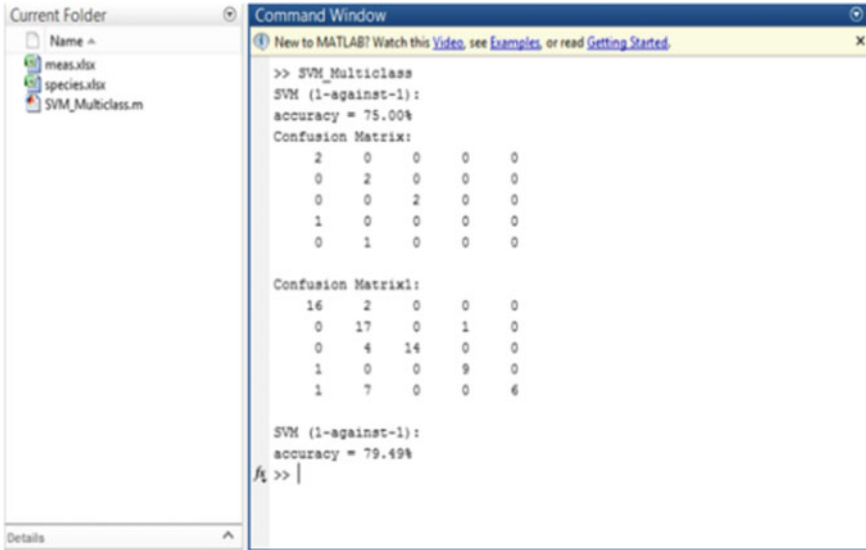


Fig. 9 Efficiency with multiclass classify

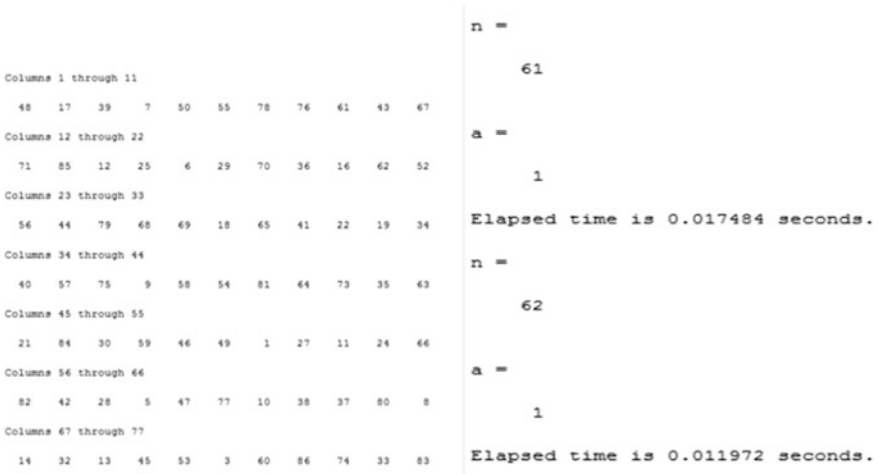


Fig. 10 Minimum number of training samples for which accuracy is 100%

4 Conclusion and Future Scope

In this paper, we implemented Support Vector Machine algorithm for separation of different classes of polymers [10]. The absorbance values of these polymers under NIR spectroscopy were collected to train and test the classifier in the algorithm.

First binary classification was applied; the data was then cross validated as well subjected to Kennard Stone algorithm. The accuracy achieved was 100% without cross validation and varied between 70 and 80% with cross validation and after the application of KS algorithm.

A multiclass classifying algorithm was found fairly efficient when implemented in MATLAB as well as Python. In MATLAB, the accuracy showed varied results from 75 to 90%. Whereas in Python, accuracy achieved with cross validation and with linear classifier was close to 95%. There is scope for further improvements such as implementation of KS algorithm to the Python code as well as application of various pre-processing routines to cancel out noise from the data.

References

1. Multiclass and Binary SVM Classification: Implications for Training and Classification Users, an IEEE paper published by A. Mathur and G. M. Foody.
2. Fast SVM Training Algorithm with Decomposition on Very Large Data Sets, an IEEE paper published by Jian-xiong Dong, Adam Krzyzak, and Ching Y. Suen.
3. Extreme Learning Machine for Regression and Multiclass Classification, an IEEE paper published by Guang-Bin Huang, Hongming Zhou, Xiaojian Ding, and Rui Zhang.
4. T. Van Gestel, J.A.K. Suykens, G. Lanckriet, A. Lambrechts, B. De Moor, and J. Vandewalle, "Multiclass LS-SVMs: Moderated outputs and coding-decoding schemes," *Neural Process. Lett.*, vol. 15, no. 1, pp. 48–58, Feb. 2002.
5. J.A.K. Suykens and J. Vandewalle, "Multiclass least squares support vector machines," in *Proc. IJCNN*, Jul. 10–16, 1999, pp. 900–903.
6. C.-W. Hsu and C.-J. Lin, "A comparison of methods for multiclass support vector machines," *IEEE Trans. Neural Netw.*, vol. 13, no. 2, pp. 415–425, Mar. 2002.
7. G.-B. Huang, K.Z. Mao, C.-K. Siew, and D.-S. Huang, "Fast modular network implementation for support vector machines," *IEEE Trans. Neural Netw.*, vol. 16, no. 6, pp. 1651–1663, Nov. 2005.
8. H. Drucker, C.J. Burges, L. Kaufman, A. Smola, and V. Vapnik, "Support vector regression machines," in *Neural Information Processing Systems 9*, 528 *IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART B: CYBERNETICS*, VOL. 42, NO. 2, APRIL 2012 M. Mozer, J. Jordan, and T. Petsche, Eds. Cambridge, MA: MIT Press, 1997, pp. 155–161.
9. Y. Tang and H.H. Zhang, "Multiclass proximal support vector machines," *J. Comput. Graph. Statist.*, vol. 15, no. 2, pp. 339–355, Jun. 2006.
10. G.-B. Huang, Q.-Y. Zhu, and C.-K. Siew, "Extreme learning machine: A new learning scheme of feedforward neural networks," in *Proc. IJCNN*, Budapest, Hungary, Jul. 25–29, 2004, vol. 2, pp. 985–990

A Comprehensive Analysis of Moving Object Detection Approaches in Moving Camera

Neeraj and Akashdeep

Abstract To detect moving objects is a difficult task for various image processing and computer vision applications viz., motion segmentation, object classification and identification, behavior understanding, event detection, object tracking and object locating. The process becomes even more difficult with moving camera as compared to static camera as both camera and object motions are combined in the detection process. Moreover, almost all real time video sequences incorporate pan/tilt/zoom camera which makes it essential to detect objects in moving cameras. This paper presents a survey of various moving object detection techniques in moving cameras and gives insight picture of the methods like background subtraction, optical flow, feature based object detection and blob analysis. It also mentions pros and cons of every technique used so far individually. The use of these approaches and progress made over years has been tracked and elaborated.

Keywords Object detection · Moving camera · Feature classification

1 Introduction

Object detection is defined as the process of detecting a change in the position of the object relative to its surroundings or a change in surroundings relative to the object. Areas that are highly explored in case of object detection incorporate face recognition and pedestrian detection. Object detection has applications in numerous territories of Computer vision, including image retrieval and video surveillance. Some of the applications of moving object detection can be listed as follows:

- Detection of pedestrians by moving vehicle having pan/tilt camera;
- Detection of obstacles in case of camera mounted on a moving robot;
- Detection of moving/flying objects in case camera is mounted on a drone;

Neeraj (✉) · Akashdeep
CSE Department, UIET, Panjab University, Chandigarh, India
e-mail: neer2890@gmail.com

- Detection of kids, people and toys in case of hand-held camera;
- Automated vehicle parking systems;
- Detection of objects in 360° videos;
- Detection of moving objects in satellite/space station videos.

Object detection in moving camera is intricate as contrasted to static camera in the sense that both foreground (the moving articles) and the background (rest part other than the items) stay in movement. Camera movement can likewise be characterized in two ways i.e., constrained (where way of moving camera is settled i.e., pan/tilt/zoom) and unconstrained (where the movement of camera is obscure). This study presents a summarization of recent approaches in the field of object detection in moving cameras.

There can be numerous methods available that can be applied to do so viz., BS (Background subtraction), optical flow, blob analysis etc. Traditionally, we use object detection in static cameras where background of the video is fixed and only the moving parts are random. So, it is easy to detect the objects in that case because the movement is only restricted to the objects. There may be some critical situations like illumination changes, blowing winds, and bad weather conditions in which some of the methods of static cameras lack behind. Tackling those conditions in static camera is a different issue but here, in case of moving camera, background and foreground, both move with respect to time and the problem of detection of moving objects become more complex.

2 Moving Object Detection Techniques

2.1 Background Subtraction

The goal is to leave only the foreground objects of interest by subtracting the background pixels in the scene. This technique can be generally categorized into two types i.e., background construction based background segmentation, in which video objects are detected using BS on the basis of construction of background information and foreground extraction based background segmentation, in which spatial, temporal or spatio-temporal information is used to obtain moving object and then motion change information detects it in successive frames.

Dongxiang Zhou et al. [1] proposed a technique for distinguishing moving objects from a moving camera taking into account SIFT features [2] (The Scale Invariant Feature Transform). At first, feature points are separated by SIFT calculation to process the relative change parameters of camera movement, guided by RANSAC [3]. The robustness of SIFT Features matching and selecting anomalies by a RANSAC calculation make the parameters of relative transform model to be figured precisely. Authors claimed that by using BS approach with dynamically-updated background model, foreground objects can be identified flawlessly.

However, as mentioned in Table 1, processing of the whole image takes longer time and it can be reduced by minimizing the search area to meet the requirements.

Zou, Xiaochun et al. [4] proposed a method of moving object segmentation in a complex moving camera motion. Some features are extracted using Harris corner detector algorithm [5], camera motion is estimated and panoramic image of the background is obtained. Finally, BS is used to segment the moving object regions. They used a self-made dataset to verify their results and claimed that their method works well in moving object segmentation but it the proposed method cannot adaptively update the background model used in the method.

Zamalieva, Daniya et al. [6] proposed a new method for exploiting temporal geometry for moving camera background subtraction. KLT feature tracker [7] is used to track the trajectories of a set of sparse feature points. As the trajectories are also sparse, the optical flow vectors of all the pixels are used to generate a set of trajectories. Epipolar geometry is then used to test whether a particular trajectory belongs to foreground/background. Authors claimed that the method can successfully detect the moving objects despite of appearance changes but they assumed the motion of camera is smooth in consecutive frames.

Wu-Chih Hu et al. [8] in their method extract feature points using Harris corner detector [5] followed by optical flow to get the motion vectors of moving pixels. Epipolar geometry is used to classify foreground/ background pixel. BS finds the motion regions of foreground. They used a self-made and public dataset to verify their results as shown in Table 1, claiming that their method outperforms the state-of-art methods but the method lacks in detecting the moving objects in case of heavy crowd of moving objects. Tables 1, 2, 3 and 4 provides the year wise specifications having contribution of the studies and their limitations with results that can be used as future works to every researcher.

2.2 *Optical Flow*

Optical flow is utilized for investigating the obvious movement of articles, surfaces and edges in a visual scene caused by the motion of observer, especially camera and the scene.

Guofeng Zhang et al. [9] used a method which emphasizes between two stages, i.e., the dense estimation and foreground labeling for a stable bi-layer division. They used structure from motion (SFM) method [10] to track feature points and picks the superior key frames. Output of SFM contains camera parameter set, and a sparse point set that map to the feature points in the video frames. Displacement vectors are used to compute the motion of every pixel in concurrent frames. Every pixel is then linked forward and backwards to the simultaneous frames based upon the pixel displacement forming motion tracks. If the root mean square error for a pixel is large then it belongs to the foreground and so on. They claimed that their method achieves a high quality foreground extraction without initially knowing the object motions. Whereas optical flow computation and motion parameters will

Table 1 Background Subtraction based studies

Reference	Specification	Contribution of study	Limitations	Evaluation
[1]	Background Subtraction + SIFT + RANSAC	Separated feature points through SIFT transform followed by RANSAC to identify foreground objects precisely	Image processing takes longer time	Precise and reliable objects
[4]	Background Subtraction + Harris corner detection	Camera motion is estimated based on robust features detected by Harris corner detector. Based on that panoramic image of the background is formed	The proposed method cannot adaptively update the background model	–
[6]	KLT feature tracker + feature point tracking + Epipolar geometry + Background subtraction	Optical flow is used to generate the set of trajectories using all pixels. The large subset belongs to background. Epipolar geometry between consecutive frames is used to test whether the trajectory belongs to foreground/background	The camera motion is assumed to be smooth in consecutive frames. HOPKINS dataset was used to verify the results	Average execution time is 48.2 s. Persons and cars can be detected with average scores as Precision: 83.4, 81.8 Recall: 74.7, 88.2 F-measure: 74.3, 87.6
[8]	Harris coner detector + pixel classification + background subtraction	Feature points are obtained using Harris corner detector followed by optical flow to get the motion vectors of moving pixels. Epipolar geometry is used to classify foreground/background pixel	Overlapping objects are overlooked. A self-made and a public dataset are used	Average overall Precision, recall and F-measures of the proposed method are Precision: 74.2% Recall: 73.6% F-measure: 73.4%

contain large errors if the background scene doesn't contain enough information and most of the regions are texture-less. Incorrect bi-layer separation may results when foreground object contains very thin boundaries.

Cheng-Ming Huang et al. [11] used KLT [7] feature tracker to track all important features (the corners or noisy texture) that can be reliably tracked from frame to frame. It specifies a patch around each feature point and searches for image patch in the neighboring region of every reference point to match. Two images having feature in the previous image were taken and we find the displacement of the feature point with its neighboring patch. Feature points having similar optical flows are grouped by which a window of objects is generated which is then compared with the color histogram of target predefined earlier. If they aren't similar then contour matching is performed to verify the target's outliers. Authors claimed that the method works well for the pan/tilt camera on a spherical camera platform

Table 2 Optical flow based studies

Reference	Specification	Contribution of study	Limitations	Evaluation
[9]	structure from motion (SFM) method + optical flow + feature point tracking + displacement vectors	Superior key frames are chosen using SFM method to track feature points in image. Displacement vectors are used to compute motion of every pixel in the concurrent frame and linked forward and backward in order to find foreground and background pixels	When most of the regions are texture-less, then optical flow produces large errors. Also, when foreground objects contain thin boundaries, incorrect bi-layer separation may result	Reliable results. Average computation time is 6 min per video
[11]	Kanade-Lucas-Tomasi (KLT) feature tracker + optical flow + neighboring patch + color histogram + contour matching	Classification of feature points according to similar optical flow vectors is used to compare with predefined target. Feature points with no class have to go through contour matching	Camera motion is bounded to pan/tilt	Reliable results
[12]	VSLAM + optical flow + dense feature tracks + graph based clustering + motion segmentation	VSLAM is used to find the location of moving camera and some perceived landmarks. Motion segmentation is done by using graph based clustering computed from optical flow based motion potentials	Average execution time is 7 min per frame	Average execution time is 7 min per video sequence producing efficient results

Table 3 Feature based object detection studies

Reference	Specification	Contribution of study	Limitations	Evaluation
[13]	Ego-motion + feature point detection	Measured ego-motion from feature points present in various numbers of regions except those in which moving objects exists and from that, a 3D structure of the scene is created to detect moving objects	The accuracy of region detection is not good enough and fails in detecting stationary objects	Although reliable results are obtained but some false detections may result
[14]	Multi-view geometric constraints + feature point extraction	Structure consistency constraint is used to detect the objects moving in the direction of camera movement	Automatic estimation of parameters such as temporal window size, intensity difference threshold etc., cannot be done	Average precision and recall values for experiments in two video sequences are given below: Precision: 37.7, 53.5 Recall: 86.7, 46.3
[15]	KLT feature tracker + RANSAC + background subtraction	A combination of feature points and homography is used to estimate background motion. RANSAC is applied for outlier detections. BS is applied finally to get foreground pixels	Only homography is not enough for moving object detection. An effective background modeling is required. Hopkins 155 dataset is used for evaluation	Evaluation is done based on precision, recall and f-measures. Computation time is also taken as a metric to evaluate performance

coordinate. A two level architecture i.e., top level for tracking the output of bottom level and estimates the target's position and bottom level for tracking the feature points, is used to improve the robustness of tracking.

Rahul Kumar Namdev et al. [12] proposed an incremental motion segmentation system to segment multiple moving objects and tracking environment by using visual Simultaneous Localization and Mapping (VSLAM). VSLAM is helpful in finding the location of moving camera while incrementally constructing a guide of an unknown environment and evaluating the locations of recently perceived landmarks. They computed optical flow and dense feature tracks from an image sequence while at the same time running a VLSAM framework in the background. VSLAM gives camera sense of self moving parameters which are utilized to compute multi-view geometric requirements which are then used to compute motion potentials. These alongside the optical flow based motion potentials are

Table 4 Blob analysis studies

Reference	Specification	Contribution of study	Limitations/dataset	Evaluation
[16]	Person tracking + 3-D depth estimation + camera calibration	Tracks persons by making use of distance to a target appearing in the images. It also uses pixel displacements and derivative of distance information to effectively segment color blobs	Cannot track blob efficiently in illumination changes and when the person being followed suddenly moves fast	Evaluation is done based on mean and standard deviations and the experimental measures states that the results are quiet effective
[17]	KLT feature tracker + Harris corner detector + blob detection	Feature points are obtained using Harris corner detector and tracked using KLT feature tracker. For moving object segmentation, authors used blobs and connected component labeling	VIVID dataset and two self made videos are used for evaluation	Average precision, recall and f-measures values in self-made and Vivid dataset are: Precision: 83.4, 89.7 Recall: 87.6, 92.3 F-measure: 85.1, 89.8

given to a graph based clustering to accomplish motion segmentation. Authors claimed that it's first such method to demonstrate dense motion segmentation with a solitary moving camera with multiple moving items. There are no restrictions on the movement to be affirmed either by the camera or the objects.

2.3 Feature Based Object Detection

In feature-based object detection, standardization of image features and alignment of reference points are of great significance. The images then are transformed into another space for handling changes in illumination, size and orientation. One or more features are extracted and on the basis of those features, objects of interest are modeled.

Koichiro Yamaguchi et al. [13] presented a method for finding the ego-motion of vehicles and for the detection of moving objects on roads by using a monocular camera mounted on a vehicle. The problems associated with ego-motion may vary in two categories i.e., when other vehicles are also present in the sight of camera and the roads, as fewer feature points are displayed by roads as compared to other backgrounds. They estimated ego-motion from the feature points associated with various numbers of regions other than those in which moving objects are there. After ego-motion estimation, they construct a 3-D structure of the scene and the

moving objects are detected. Authors claimed that their method accurately estimates the ego-motion of vehicles in severe situations in which camera moves nearly parallel to its optical axis. But their method fails at detecting the stationary objects and also, the accuracy of region detection of objects can be improved.

Chang Yuan et al. [14] presented a novel method which sequentially applies 2D planar homographies on each image pixel and classifies them into parallax, planar background or motion regions. Authors used structure consistency constraint and called it as a main contribution of their paper which is determined by the relative camera poses between 3 consecutive frames. Structure consistency constraint is important because it can also detect moving objects moving in the same direction in which camera is moving where Epipolar constraint fails to detect them. Authors claimed that the method robustly and effectively works when the scene contains enough texture areas for the extraction of feature points, when there is no parallax i.e., a planar scene or strong parallax i.e., large amount of parallax is needed to define reliable geometric constraints and when there exists a scene in which camera/objects cannot move abruptly. One thing that needs to be noticed is that the assumptions made by the authors are same as those made in previous approaches of motion and object detection. So, the method lacks in automatic estimation of some parameters such as intensity difference threshold and temporal window size etc.

Tsubasa Minematsu et al. [15] extracted feature points and tracked them by using KLT feature tracker [7]. A combination of feature points and homography is used to estimate the background motion. RANSAC is applied for outlier detections. Finally, BS is applied to get foreground pixels. The main limitation of the proposed method is that homography is not enough for moving object detection. An effective background modeling is required.

2.4 *Blob Analysis*

Blob detection routines are used to detect portions of image that contrast in properties, for example, brightness, shading or color, contrasted with surrounding areas. A blob is an area of a picture in which a few properties are consistent or nearly constant. Every point within a blob can be considered in some sense to be similar with one another.

Hyukseong Kwon et al. [16] proposed an efficient person tracking algorithm whose main goal is to find the distance to a target visible in the pictures taken by the moving cameras. So, the approach includes building one to one correspondence between the pixel displacement without using any intrinsic parameters and the control inputs to the pan/tilt units. Another goal of their method is to find the derivation of distance information by using the correspondence between the centers of masses of colored blobs segmented from both the camera images. Authors claimed that their method effectively tracks persons in a mobile robot environment

having two independently moving cameras. Their approach does not need any prior knowledge of the cameras like the size of CCD chips or the focal length of cameras. Their method is quite accurate for real-time person following in indoor environments. But changes in illumination can cause shifts in the centre of mass of blobs producing negative results in the method. Also, if the person being followed suddenly decides to move faster, then the effects become particularly pronounced.

Teutsch, Michael et al. [17] used blob detection method in evaluation of object segmentation to improve moving vehicle detection in Aerial Videos. They extracted feature points using Harris corner detector [5] and tracked them using KLT feature tracker [7]. For moving object segmentation, authors used blob detection. Objects are detected by connected component labeling. VIVID dataset [18] and two self made videos are used for evaluation of the results.

3 Conclusion

For analyzing digital images and segmenting relevant information from them, various researches on image enhancement, event and motion detection etc., have been studied. The techniques studied in the paper are used in almost every moving object detection algorithms. We had analyzed and concluded the limitations of every technique listed in Tables 1, 2, 3 and 4. And also, concluded that which conditions are suitable to apply a particular technique. As per the evaluations, videos with high resolution take longer processing time than lower resolution videos (ignoring the total lines of code). BS can be applied on videos that doesn't contain much occlusion, particularly when objects aren't overlapping and when camera is moving smoothly. It fails to detect objects in case of fog and illumination changes, casted shadows, very high lightening changes and when object moves slowly. Optical flow is prone to errors when camera rotates very fast or object moves fast, when object regions are texture-less and when object contains thin boundaries. Whereas feature based object detection gives best results in PTZ cameras and fails in detecting stationary objects and crowded regions. Also, it's a non-trivial task to locate required features accurately and reliably. Blob analysis can be useful to detect objects when object blobs are independently moving with one another and if overlapping of objects is clearly visible. It lacks in detecting objects in illumination changes. Blobs are sensitive to noise and tracking of blobs may fail while object being tracked moves suddenly. Heavy crowded areas make it difficult to detect objects using blobs. From above, it can be seen that every technique has some issues and some good characteristics. In particular, we cannot say which technique is best for moving object detection in moving camera. So, a combination of above techniques with some other algorithms can be applied on videos to detect objects effectively.

References

1. Dongxiang Zhou, Liangfen Wang, XuanpingCai, and Yunhui Liu.: Detection of Moving Targets with a Moving camera. In: the Proceedings of the IEEE International Conference on Robotics and Biometric, pp. 677–681, Guilin, China (2009).
2. Fischler, Martin A., and Robert C. Bolles.: Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography. In: Communications of the ACM, pp. 381–395 (1981).
3. J. Shi, C. Tomasi.: Good features to track. In: Proceedings of IEEE Conference on Computer Vision and Pattern Recognition, pp. 593–600 (1994).
4. Zou, Xiaochun, Xinbo Zhao, and Zheru Chi.: A robust background subtraction approach with a moving camera. In: 7th International Conference on Computing and Convergence Technology (ICCCCT), IEEE (2012).
5. Carlo Tomasi and Takeo Kanade.: Detection and tracking of point features. School of Computer Science, Carnegie Mellon Univ. Pittsburgh, CMU-CS-91–132 (1991).
6. Zamalieva, Daniya, Alper Yilmaz, and James W. Davis.: Exploiting temporal geometry for moving camera background subtraction. In: 22nd International Conference on Pattern Recognition (ICPR). IEEE (2014).
7. Sinha, Sudipta N., et al.: GPU-based video feature tracking and matching., Workshop on Edge Computing Using New Commodity Architectures. Vol. 27 (2006).
8. Hu, Wu-Chih, et al.: Moving object detection and tracking from video captured by moving camera. In: Journal of Visual Communication and Image Representation pp 164–180, vol 30 (2015).
9. Zhang, Guofeng, et al.: Moving object extraction with a hand-held camera. In: 11th International Conference on Computer Vision, (ICCV), IEEE (2007).
10. G. Zhang, X. Qin, W. Hua, T.-T. Wong, P.-A. Heng, and H. Bao.: Robust metric reconstruction from challenging video sequences. In: CVPR (2007).
11. Cheng-Ming huang, Yi-Ru Chen and Li-Chen Fu.: Real time object detection and tracking on a moving camera Platform. In: IEEE International Joint Conference (ICROS-SICE), pp. 717–722, Fukuoka (2009).
12. Rahul Kumar Namdev, AbhijitKundu, K Mahadev Krishna and C.V. Jawahar.: Motion segmentation of multiple objects from a freely moving monocular camera. In: IEEE International Conference on Robotics and Automation, pp. 4092–4099, River Centre, Saint Paul, Minnesota, USA (2012).
13. Yamaguchi, Koichiro, Takeo Kato, and Yoshiki Ninomiya.: Vehicle ego-motion estimation and moving object detection using a monocular camera. In: 18th International Conference on Pattern Recognition, (ICPR) Vol. 4. IEEE (2006).
14. Yuan, Chang, et al.: Detecting motion regions in the presence of a strong parallax from a moving camera by multiview geometric constraints. In: IEEE Transactions on Pattern Analysis and Machine Intelligence, pp. 1627–1641 (2007).
15. Minematsu, Tsubasa, et al.: Evaluation of foreground detection methodology for a moving camera. In: 21st Korea-Japan Joint Workshop on Frontiers of Computer Vision (FCV), IEEE (2015).
16. Hyukseong Kwon, Youngrock Yoon and Jae Byung Park.: Person Tracking with a Mobile Robot using Two Uncalibrated Independently Moving Cameras. In: IEEE Proceedings of International Conference on Robotics and Automation, pp. 2877–2883, Spain (2005).
17. Teutsch, Michael, Wolfgang Kruger, and Jurgen Beyerer.: Evaluation of object segmentation to improve moving vehicle detection in aerial videos. In: 11th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), IEEE (2014).
18. C. Stauffer.: Learning patterns of activity using real-time tracking. IEEE transactions on pattern analysis and machine intelligence, Vol 22 (2000).

Innovative Approach for Handling Blackouts in the Transmission Grid Through Utilization of ICT Technology

Gresha S. Bhatia and J.W. Bakal

Abstract The focus of development of the system is an attempt to make the transmission sector of the power grid smart in terms of utilizing modern information technologies to deliver power efficiently under varying conditions that may occur anywhere in the power grid. Power grids form the lifeline of modern society. Over the past few decades, it has been observed that there have been negligible innovations in the transmission grid operations. This has resulted in a number of blackouts and outages leading to multitude of system wide failures. Further, issues with respect to environment and stochastically aligned nature of the power grid, makes it difficult to automatically identify, diagnose and restore the system to normalcy, thereby making it a challenging task. This leads toward incorporating ICT technologies into the Energy Management System of the power grid. As the transmission grid forms a sub domain of the power grid that lies between the generation and distribution domains, managing this grid becomes crucial. Therefore, focussing on the transmission grid and considering the occurrence of blackouts and outages, this paper specifies the operations of the grid especially in the transmission sector. This is then followed by the issues faced and the role of ICT technologies in the transmission domain of the grid. The paper further elaborates the mechanisms to determine the failure and blackout situation, provide better decision making through the application of Information and Communication Technologies (ICT). This is then followed by the various ICT analysis performed based on the proposed mechanism.

Keywords Information and communication technologies (ICT) • Blackouts • Power failures • Transmission sector

G.S. Bhatia (✉)

Thadomal Shahani COE (TSEC), Bandra (W), Mumbai, India

e-mail: itsgresha@yahoo.co.in

J.W. Bakal

Shivajirao S. Jondhale COE, Dombivli (East), Thane, India

e-mail: bakaljw@gmail.com

© Springer Nature Singapore Pte Ltd. 2017

H.S. Saini et al. (eds.), *Innovations in Computer Science and Engineering*,

Lecture Notes in Networks and Systems 8, DOI 10.1007/978-981-10-3818-1_31

1 Introduction

Information and communication technologies (ICT) form the key components of economic growth. The effectiveness and growth of the ICT is determined by the ability of the component parts to talk to each other—to interoperate. Thus, ICT (Information and Communications Technology) is defined as a term that incorporates information that is captured, processed, stored, displayed or communicated through any of the electronic gadgets, communication device or application. These gadgets may include radio, television, cellular phones, computer and its associated networks along with the various application services that they provide such as communication etc. ICT is specifically defined in the domain in which they are applied. For example, if the context where in ICT is incorporated includes manufacturing, it is specified as ICT as applied in manufacturing. Similarly, when applied to education and healthcare, ICT is specified accordingly [1]. This paper elaborates on the mechanism to incorporate ICT into transmission domain of the power grid. The major focus is to enable the protection systems to reduce the amount of time delay of communication between the control center authorities of the grid and the utility companies. This in turn would save power thefts and prevent the losses incurred due to power failures and blackout conditions. Thus, the focus of this paper is to create awareness of the situation around through communicating the information across various sectors of the grid [2].

2 Operations in Power Grid

The control center within the transmission sector of the grid receives the subset of the power grid data obtained from the remote terminal unit (RTU) over communication channels. The major amount of data collected includes:

(1) **The switching information**

This indicates the changes that occur in the circuit due to the opening and closing of the switches connected through the circuit breakers to the respective nodes.

(2) **Operating parameters**

Analog variables comprising of the voltage, current and frequency components are considered as input over a time period, providing around 100 samples in one second. These samples are further synchronized and termed as synchronized phasor measurement.

3 Issues Faced by the Existing Systems

The systems operating at the transmission sector currently are facing a number of issues that include:

- (1) Huge amount of data is collected at the substations. However, the rate at which the information is collected and transmitted is different. Their failure/misbehavior puts additional burden on the working components causing them to misbehave that lead to a cascade of failures or large blackouts.
- (2) Based on the guidelines that are prepared off-line, the system operators, in case of an outage or a blackout condition perform the operations manually. These off-line guidelines, however, may not be accurate. This would further result in inappropriate actions towards handling a blackout scenario This leads to the entire operation being time—consuming and stressful for the system operators.
- (3) The vulnerability of the transmission sector of the power grid to information failures exposes the limitations of the insufficient operations of these systems that affect the operator’s situation awareness. This inefficiency leads to inappropriate communication of the critical information in an effective and timely manner. This further adds to the operators’ response to the failure.

Thus, innovative decision-support tools are required to increase and restore normalcy onto the network [3]. Therefore, the control center operators need an optimal and efficient way to broadcast the power flows to a number of consumers [2, 4, 5].

This paper thus focuses on utilizing ICT technology to modernize the transmission grid through the development of software. This simulated software will process the continuous streaming data, monitor the operations of the grid under varying conditions and further develop quicker response to prevent failure situations. This would in turn help systems for taking better and improved decisions.

4 Role of ICT in the Transmission Grid

Information and Communications Technology, known as ICT, comprises of integration of information processing, computing and communication technologies. Integrating this, especially, into the transmission grid aids in better management of resources [5].

Thus, for the systems to perform in an optimized manner, modern transmission grids need to be based on efficient design incorporating operation of ICT systems during normal as well as abnormal conditions. The application of the ICT technologies leads to

- (1) Significant improvements in the transmission grid operations, contributing to the smooth and effective communication of the situation at hand.

- (2) System operators cope more effectively as the real-time decision-making is supported by advanced monitoring and visualization mechanisms.
- (3) Moreover, these advanced automatic schemes contribute towards the prevention or mitigation of the impact of large power grid blackouts [6, 7].

5 Information Chain

The objective of the ICT infrastructure is to keep the operators constantly informed about the current operating state of the grid. Thus, the information flow throughout the transmission grid includes: [4, 8].

(a) **Capturing of the data:**

Voltage and current are a continuous set of data that is transferred from the generation unit, passing through various devices and reaching the control center through the Phasor Measurement Units (PMUs). These devices allow the power to be synchronized on a global basis using satellite technology and measure the line power flows, bus voltage and line current magnitudes which produce real-time data in the analog or digital form across the electrical network. This information is presented in an IEEE 1344 format and transmitted to a remote site over any available communication link [7–10].

(b) **Wide area measurement system (WAMS)**

The infrastructure incorporated into the grid comprises of utilizing the synchro phasor technology and high speed wideband communication. This infrastructure further monitors the phase angles of each phase, frequency, rate of change of frequency and angular separation at an interval of every few millisecond. Lack of computing power, coordinating and synchronizing the grid data makes the situational awareness a difficult task. [11]. To add to this further, though the basic configurations have remained unchanged over few decades, the signals used for monitoring and control have become digital, utilizing a standard communication protocol 61850 standard [12, 13].

6 Proposed Mechanism

The major concentration focused on in this paper is firstly on converting the real-time data into useful information. The phases involved in this include:

(i) **Measurement of information**

The data is collected through data concentrator at an appropriate site is further utilized for developing control schemes that help in power grid monitoring.

(ii) Data concentration and conversion

There is a need to convert the real-time data into useful information. This thus comprises of two sub-modules:

- (a) An module that receive the signals from sensors and power equipment
- (b) Processing/conversion module that process the signals digitally [14].

The primary data received and processed include processing towards limit value monitoring, alarm processing functions. These functions on the set of data received thereby relieve the operators from routine work and provide an actual value of the system state [15–17].

(iii) Communication system

The processed data is then transferred to the central monitoring unit through utilization of the ICT technologies.

(iv) Graphical user interface (GUI)

The GUI provides the state information on the operator’s console. This information would further help the operator to decide upon the most appropriate actions to implement, prioritize and present the data in a way that enables efficient monitoring and control of the system [18, 19].

7 Algorithm Incorporated

In order to apply the ICT technologies across the transmission sector of the grid, the algorithm is initiated through monitoring the current status of the grid. This grid monitoring is performed through the steps mentioned in the proposed mechanism as follows:

(a) Input to the system

- (1) The dependency graph of the network indicates the parent—child relationship between the various nodes of the network.
Let, Number of nodes = 4 (N_1, N_2, \dots, N_4), Number of edges = 3 ($E_1 \dots E_3$)
- (2) Determine the operating parameters of the system.
Let Voltage parameter = V_A, V_B, V_C , Current parameter = I_A, I_B, I_C
Frequency parameter = F
- (3) The area and region of operation of the control center
Let Region = R_1 , Area = $A_1 \dots A_4$.
- (4) The operating state of the system. The states are represented as the Normal state, alert state and failure state. The operating states are determined based on the parameters mentioned in Table 1 below [20, 21].

Table 1 Operating parameters

Value	Voltage (V)	Current (I)	Frequency (F)
Low (L)	178	4.5	49.7
Threshold low (TL)	198	5	49.5
Threshold high (TH)	245	16	50.2
High (H)	270	17.6	50.7

Table 2 Processing of the operating parameters

Date: 18th June 2015 At time—20:00:01.730		
Node	Phase	State
1	1	ALV
1	3	FHV
2	1	FLV
2	3	AHV

(b) Processing within the system**(1) Measurement of information**

Information of the various parameters namely 3 phase voltages, 3 phase Current and the frequency components at respective nodes are measured from the live system on a continuous basis.

(2) Based on the input parameters provided at the nodes, the processing module identifies the type of the fault and the location of the failure, when monitored for 50 ms with a step size of 20.

(c) Expected output form the system

Table 2 below indicates the type of failure that is measured based on the thresholds as indicated in Table 1.

Once the failure has been detected, it needs to be communicated quickly to the utility companies for quicker restoration [22, 23].

ICT is incorporated through the application of information technology through sending e-mails, SMS and Push notifications to the authorities.

8 Results and Evaluation

Communication to the utility authorities as well as the field engineers through utilization of the ICT mechanisms provides the application of information technology in the transmission sector domain of the power grid.

Use of ICT for communicating the message to the respective authorities comprises of sending the appropriate message through emails, SMS messages and Push messages respectively.

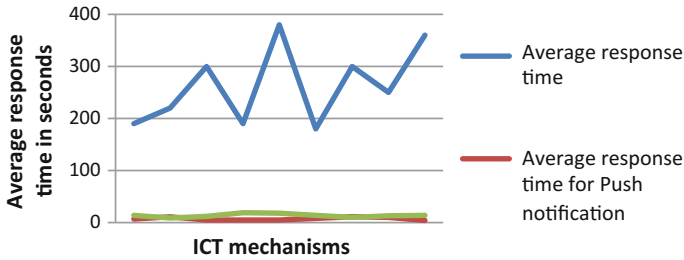


Fig. 1 Implementation of ICT mechanisms

As observed from the Fig. 1, e-mail takes approximate average of 260 s to communicate the information of power failure to the authorities. This is followed by the Push notifications that communicate the same information in around 30 s while the SMS service requires much lesser time i.e. around 20 s to send the information.

Therefore, it can be said that sending the information through SMS, followed by Push which is followed by the email to be sent should be the mode of ICT implementation for quicker communication and response.

It is further observed that the failure situation can lead to a blackout condition quickly as compared to the alert situation.

9 Conclusion

Transmission domain resides between the generation and distribution end of the power grid. However, technology application in this domain of the power grid is still at its nascent level. Therefore to provide for a better and faster mode of communication within the energy management sub system of the grid employment of WAMS and ICT technology forms a critical component. This paper thus focuses on the role played by ICT in the transmission domain followed by the proposed mechanism for handling failures and blackout scenario—identification, localization and restoration through quicker mode of ICT communication between the control center and the authorities. It is further observed that the amount of time taken by the ICT implementation through the e-mail facility is much more compared to the other ICT mechanism of PUSH notifications followed by the SMS service.

10 Future Scope

The future work for the implementation of ICT in the transmission domain comprises of employing the communication technologies for Outage management systems and increases situation awareness. Further, the impact of the unavailability of each ICT function or component varies depending on its criticality, purpose and time of occurrence. Therefore, there is a need to develop methods for evaluating and quantifying the amount of miscommunication caused by different failures or limitations under different system conditions. Therefore, development of comprehensive reliability databases, which can then be used to increase the accuracy of the reliability evaluation results and providing useful feedback to the authorities.

References

1. <http://searchcio.techtarget.com/definition/ICT-information-and-communications-technology-or-technologies>.
2. Nur Ashida Salim et al, "Critical system cascading collapse assessment for determining the sensitive transmission lines and severity of total loading conditions", *Mathematical problems in engineering*, volume 2013.
3. ShanShan Liu et al, "The Healing Touch", *IEEE power and energy magazine*, January 2014.
4. Massoud Amin, "Powering the 21st century", *IEEE power and energy magazine*, March/April 2005.
5. Kishor chavan et al, "Role Of ICT in Power System", *International Council On Large Electric Systems*, November, Maharashtra Electricity Regulatory Commission, November 13–15, 2013.
6. Vivek Pandey, "Electricity Grid management in India-An Overview", *Electric India-Vol 47*, Nov. 2007.
7. Xi Fang et al, "Smart Grid – The New and Improved Power Grid: A Survey", September 30, 2011.
8. Optimal Placement of Phasor Measurement Units for State Estimation, *Power System Engineering Research Centre, Texas A&M University*.
9. Thomas Degner, "Smart Grid Communications: Overview of Research Challenges," *Solutions, and Standardization by*.
10. Anjan Bose, "Smart Transmission grid applications and their supporting infrastructure", *IEEE Transactions on smart grids*, Vol 1, no 1, June 2010.
11. L. Balgand, V. Shah, B. Deck, and P. Rudolf, "Intelligent Electronic Device for Substation or Distribution Automation Systems", 2008.
12. SIEMENS, "Power Engineering Guide," 2008.
13. B A Carreras et al, "Blackout Mitigation Assessment in power transmission systems", *Hawaii International Conference on system Science*, IEEE, January 2003.
14. Theresa- Marie Rhyne' "Visualization Viewpoints Chasing the Negawatt: Visualization for sustainable living", *IEEE Computer Society* May/June 2010.
15. Vehbi C Gungor et al, "Smart Grid Technologies: Communication Technologies and Standards", *IEEE Transactions on Industrial Informatics*, Vol 7, No. 4, Nov 2011.
16. P Pentayya, "Model Technical Specifications for Phasor Measurement Unit", *POSOCO*.
17. Grace Q Tang,"Smart grid management and visualization", *IEEE* 2011.
18. P K Agarwal, "Indian power system SCADA project", Feb 2010.

19. Hou Y et al, "Constructing power system restoration strategies", 6th International Conference on Electrical and Electronics Engineering (ELECO 2009).
20. O. Alizadeh Mousavi, "Inter-area frequency control reserve assessment regarding dynamics of cascading outages and blackouts", Elsevier 2013.
21. Feng Shou et al, "Design and realization of regional power grid fault diagnosis and restoration systems", International Journal of Machine learning and Computing, Vol 3, Oct 2013.
22. Jayesh J. Joglekar, Dr. Y. P. Nerkar "Power Grid Restoration Optimization Considering Generating Plant Islanding Scheme".
23. M. M. Adibi et al, "Overcoming restoration challenges associated with major power system disturbances", IEEE power and energy magazine, Sept 2008.

A Comparative Analysis of Iris and Palm Print Based Unimodal and Multimodal Biometric Systems

Yakshita Jain and Mamta Juneja

Abstract Biometric systems are pattern recognition systems that are used to identify the authentic person based on his physical or behavioral characteristics. Due to some limitations faced by unimodal biometric systems, we use multimodal biometric systems. Outcomes of previous researches revealed these systems to be more reliable, dependable and secure. Iris and palm print are considered as powerful and unique biometrics, and if combined together, more accurate results can be obtained. This paper aims to review various feature extraction methods which has been applied on iris, palm print and combination of both. It also presents different fusion levels, such as feature extraction level, decision level etc. which has been used by numerous researchers to improve the precision of the system.

Keywords Multimodal · Biometrics · Review · Security · Iris and palm print

1 Introduction

Security has become a major concern everywhere these days. Many traditional methods of security like passwords, user identities, ID cards, badges and so on seem not to be sufficient for security as these all traditional methods can easily be forged. Passwords, if disclosed (knowingly or unknowingly) to some unauthenticated person, can create serious problems. Even the person can sometimes forget his/her password or user identity also. Security can be easily breached if the person's ID card or badge gets stolen. Compromise with the security of the system due to failure of such applications can lead to a big loss sometimes. In today's world, security is must for access to buildings, ATMs, laptops, mobile phones, online shopping

Y. Jain (✉) · M. Juneja
UIET/CSE Department, PU Chandigarh, Chandigarh, India
e-mail: yakshi.sliet@gmail.com

M. Juneja
e-mail: mamtajuneja@pu.ac.in

accounts, computer systems, offices etc. This problem leads to the increase in popularity of biometric systems.

1.1 Biometric System: Definition

Biometrics is the scientific study of determining a person's identity or authenticate a person utilizing his/her physical or behavioral characteristics. Biometric security systems are based on what we are, not just what we have (ID cards, access cards etc.) or what we know (passwords, user ids etc.). Biometric systems fall under the category of pattern recognition systems. In these systems, basically some features are extracted from the provided biometric and those features are stored as template in a database which is known as *an enrollment phase* of biometric system [1]. Next during *identification phase*, biometrics of the person are again captured and then extracted features are matched with the stored template.

1.2 Biometric Classification

Biometrics can be stratified into two broad categories named as physical and behavioral biometrics. *Physical biometrics*, which use some physical trait of a person to identify him like iris, figure print, hand geometry, height, face, retina etc. *Behavioral biometrics*, which uses behavioral traits of a person like handwriting, signature, voice, walk, hand or leg movement etc. Each trait has its own advantages and disadvantages over others. Suitable trait is chosen depending on the type of application, its environment and various factors like uniqueness, universality, performance, acceptability etc.

Biometric systems work in two modes [2, 3] namely verification mode and identification mode. *Verification mode* is when a person's claimed identity is verified by the system using some comparison techniques. The information captured in identification phase is compared against his/her own biometric data for this purpose. This is also called one to one comparing. *Identification mode* is when the captured biometric data are compared against all the templates already saved in the system to perceive the actual identity of the person.

1.3 Biometric System: Architecture

There are basically four components of any biometric system [1] i.e. (i) sensor/input module, (ii) feature/information extraction module, (iii) template matching module, (iv) decision making module as shown in Fig. 1:

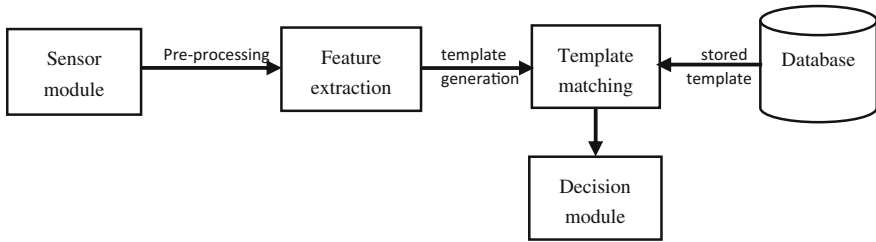


Fig. 1 Showing various modules of a biometric system

The sensor/input module is used to obtain the biometrics of the person. These are electronic devices like scanners, retina scanners, finger print sensor etc. which scans the biometric trait and produces an image of it for further use. This module depends completely on what type of biometric the system is using. It may be some simple camera or some very complex machine. *The feature extraction module* is the one where required features will be extracted from the acquired biometric. Required features/information are extracted and saved in the system's database in the form of feature vectors.

The matching module is the one where classification is done. Here the acquired feature vector is compared against the feature vector already saved in the system and accordingly, matching score values are generated. These matching score values further help in taking the decision. *The decision making module* is the final step in the system. Here final decision is taken based on the score values generated. Depending on that, the claimed identity will either be accepted or rejected (in verification mode) or the person is identified.

Biometric systems are further classified on the basis of a number of modalities used i.e. unimodal and multimodal systems. *Unimodal biometric* systems are the systems that use a single biometric trait for identifying or verifying the person. But these systems have various limitations like noisy or incorrect sensor data, dearth of individuality, high error rates, non-universality, spoofing attacks, lack of invariant representation etc. [4, 5] *Multimodal systems* are the systems which uses two or more modalities to identify or verify a person. These systems overcome most of these limitations, most importantly spoofing.

1.4 Fusion Levels

Multimodal systems utilize two or more biometric traits for the identification purpose. These modalities can be fused at different levels of the biometric system. Following are the three different levels where fusion is possible in multimodal systems [1, 5]:

Fusion at feature extraction level: At this level, captured data or the features extracted from them are fused together to get the results. Fusion at this level gives

the best results as direct image or its feature vector is richest in information. But this is the most difficult one to apply as feature vectors from various biometrics may not be compatible with each other.

Fusion at matching score level: Here score results of various matching classifiers are fused to generate the final result. This method of fusion is most widely used because of ease of access and better results.

Fusion at decision making level: Different results of acceptance/rejection are produced corresponding to each trait using feature vectors and classifiers and then finally, those decisions are combined through a voting scheme to take the final decision.

This paper reviews various feature extraction techniques applied for multimodal biometric systems. Also, different fusion levels and their corresponding methods are also discussed. For this review, two biometric traits are chosen, i.e. Iris and Palm print. Iris was chosen because of its uniqueness property for every individual [3, 6]. Even a person's left and right iris have different patterns. Also iris is easy to capture as compared to traits like retina. Similarly, palm print also has its uniqueness feature. Also, it supplies a larger area for feature/information extraction than other biometrics such as finger print etc. It also provides stability as only a few changes occur in features like principle lines, delta points, in longer duration of time.

2 Literature Review

2.1 Review of Iris

Iris gained its popularity as an effective biometric trait during the last decade. Iris has proven to be a most unique trait for identification as probability of two irises to be same is $1/1051$ according to Tiwari, Upasana et al. [7]. It was first used for personal identification in 1987 by Leonard Flom and AranSafir [8]. After that, many methods were formulated to extract iris from the whole image like circular Hough transform used by Ma, Li et al. [9]. They used exclusive OR technique for template matching. John Daugman [10] developed very successful algorithms for person's identification based on iris. But the major problem that arose was this algorithm got commercial and hence costly, moreover, it was very time consuming and complex algorithm. Then some other algorithms were also developed as an alternative to this, among which RED (Ridge energy detection) algorithm [11, 12] gained much popularity. This algorithm used local statistics (kurtosis) of the iris for segmentation and stored extracted features into horizontal and vertical polar coordinates, then used hamming distance for matching. This method is fast and gives good results even in the presence of illumination as it makes use of direction only. Meanwhile, many other methods were also developed like active contour method for iris localization by J. Daugman [13]. A major issue regarding iris recognition techniques stated above and many more that were proposed during that period of time,

was full cooperation from the user's side. Images taken in an unconstrained environment could create problems in recognition. Tan, Tieniu, et al. [14] proposed an algorithm to solve this problem in 2009. They used clustering based coarse iris localization and integrodifferential constellation was developed for pupil extraction. This technique was very much different from previous ones as they used clustering methods instead of filtering method. Santos et al. [15] proposed algorithm based on 1-D and 2-D wavelets for unconstrained environment. New algorithm using K-mean clustering, circular Hough transform for localization and canny edge detector was developed in 2013 [16]. N. Kaur and M. Juneja [17] developed an algorithm using Fuzzy c-mean clustering, circular Hough transform along with canny edge detection method for unconstrained environment. Amrata et al. [3] proposed method using Circular Hough transform, DCT (Discrete cosine transform) for extracting features and feed forward neural networks as a classifier. From these, FCM performed better than other methods. Some of the algorithms and their performance measures such as accuracy, FAR (false acceptance rate), ERR (equal error rate), FRR (false rejection rate) are depicted in Table 1. Information in the table indicates that J. Daugman's technique yields the best results till now.

2.2 Review on Palm Print

Palm print emerged as an effective modality for biometrics in the past decade because it can give wide room for feature selection and extraction as compared to traits like a fingerprint, it is quite invariant with time as compared to traits like face, image capturing in this case is easier and cheaper [18, 19]. There are five classes in which palm features can be classified i.e. geometric, line, point, texture and statistical. Major work on this biometric started in 2001 by A. Jain et al. [20], they worked on prominent principle lines and feature points of palm image. Palm print

Table 1 Comparison between various algorithms for iris recognition

Author	Evaluation parameter	Value
Leonard Flom and AranSafir [8]	Accuracy	98.00%
	ERR	4.73
Ma, Li, et al. [9]	Accuracy	99.9%
	FAR/FRR	0.01/0.09
Navjot and Juneja [17]	Accuracy	98.80%
Tisse et al. [33]	Accuracy	96.61%
	FAR/FRR	1.84/8.79
de Martin-Roche et al. [34]	Accuracy	97.89%
	ERR	3.38
Kaushik Roy et al. [35]	Accuracy	99.5%
	FAR/FRR	0.03/0.02

has also been successfully used in online systems for identification of persons using 2D Gabor filters for feature extraction [21].

Many other algorithms were developed using Sobel operator, HMM (hidden markov model) classifiers for identification giving up to 98% (approx.) identification rate [22–24]. Techniques stated above are line or point feature based methods, these methods provide a very high accuracy rate, but they require very high resolution images to work on. Techniques like PCA (principal component analysis) and ICA (independent component analysis) were also used for extracting statistical features of palm print [25]. The major problem with statistical feature based techniques is they cannot detect sensor noise. Similarly, many other algorithms were proposed based on methods like DCT [26], Contourlet transform [27], Fourier transform [28], Scale invariant feature transform for contactless images [29]. Among all these, DCT gives more accuracy for extraction of features like principle lines [19] and centric point of palm using Euclidian distance. S Chakraborty et al. used palm print for authentication using its texture features by 1D DTCWT (dual tree complex wavelet transform) and BPNN (back-propagation neural network) binary classifiers for matching purpose [18], this algorithm gave 98.35% of accuracy. Texture features based techniques like stated above, perform very well even in low resolution images and provide a high accuracy level, so they are considered to be better than others. Some of the major work done on this modality is shown in Table 2 along with comparisons made on the basis of the type of features extracted from palm, type of classifier used and various evaluation parameters like accuracy, FAR, FRR, GAR (genuine acceptance rate) etc.

Table 2 Comparison of some work done on palm print

Year	Feature extracted	Population size (persons)	Classifier used	Evaluation parameter	Values
2004 [23]	Line	320	HMM	Accuracy	97.80%
2008 [24]	Line	100	Hamming distance	Accuracy	94.84%
2003 [25]	Statistical	100	Euclidean distance, Cosine measure, PNN	Verification rate (TSR)	99%
2002 [28]	Texture	500		Identification rate	95.48%
2008 [27]	Texture	386	NED	GAR Decidability index EER	88.91% 2.7748 0.233%
2013 [18]	Texture	50	BPNN-GDX	Accuracy	98.35%
2015 [36]	Geometric	50 (JUET) 240 (IITD)		EER	0.31 0.52
2015 [37]	Geometric	168	SVM	FAR FRR	33.3% 73.3%

2.3 Review on Iris and Palm Print (Fusion)

As it has already been proven many times that multimodal systems give better results than unimodal systems. So the fusion of iris and palm print produces better identification results, then iris and palm print individually.

Both of these traits are quite complex to work upon, so less work has been done. But now this combination is gaining popularity due to its better performance results. The accuracy rates of these systems depend on multiple factors like type of fusion used, the technique of fusion used, types of features selected for extraction, types of images used as input, compatibility of the feature vectors of various modalities used etc. In 2012 R. Gayathri et al. used texture feature extraction to develop an algorithm for wavelet based feature level fusion with an accuracy of 99.2% and FAR of 1.6% [30]. Kihal et al. similarly worked on three different databases in their experiment, which proved that the superiority of the input image/data effects the precision rates [31]. They also performed all three types of fusions in their experiment to compare the results and worked on texture features of iris and palm print. Among all experiments they performed, best results were 100% GAR in decision fusion with a very small FAR. In 2015, SD Thepade et al. developed algorithm for the same trait in transform domain instead of spatial domain [32], they also worked on texture features, but used score level fusion and features were extracted using Haar, Walsh and Kekre transform. According to their results, Kekre performed better in all three with a GAR of 51.80 (approx.). Another algorithm developed was [6] based on techniques like RED algorithm, Harris

Table 3 Comparison between algorithms used

Year	Population size (persons)	Fusion level	Fusion method	Evaluation parameters	Values
2012 [30]	125	Feature level fusion	Wavelet based technique	Accuracy FRR	99.2% 1.6%
2014 [31]	200	Feature fusion, Score fusion, Decision fusion	Concatenation, Sum rule method, Error fusion	GAR FAR ^a FAR ^b	100% 2.10 ^{-3%} 4.10 ^{-4%}
2015 [32]	10	Score level fusion	Mean square error method	GAR	50.20 (Walsh) 51.80 (Kekre) 50.20 (Haar)
2015 [6]	7	Decision level fusion		RR	100% (iris) 100% (palm print)

^aFAR value for fusion of iris and CASIA palm print database [31]

^bFAR value for fusion of iris and PolyU palm print database [31]

feature extraction algorithm. They worked on geometric features of palm and choose decision level fusion for final results. Some of the work done on these two modalities is shown in Table 3 along with their fusion levels and respective methods used and different evaluation parameters.

3 Conclusion

This paper provides a comparative analysis of some of the work done on iris, palm print and their fusion. It can be easily seen that multimodal systems provide better identification results as compared to unimodal systems. Also, there are lots more options to work upon, to get better performance of the system like different types of features to be extracted, different fusion level methods etc. Iris and palm print both being difficult to get forged and complex for feature extraction, has come out as a very successful combination for multimodal biometric systems. Further work can be done on extracting the hand image from any kind of background using single algorithm. More features of palm print like geometrical, statistical can be used to check whether any improvement can be done with accuracy rate. Some other feature extracting techniques can be tried to make the authentication system faster. Different feature level, score level, decision level fusion methods can also be applied to test any improvement in performance.

References

1. Ross, Arun, and Anil Jain. "Information fusion in biometrics." *Pattern recognition letters* 24.13 (2003): 2115–2125.
2. Deshpande, S. D. "Review Paper on Introduction of Various Biometric Areas." *Advances in Computational Research* 7.1 (2015): 212.
3. Gupta, Amrata, and MrSachin Mahajan. "An Efficient Iris Recognition System using DCT Transform based on Feed Forward Neural Networks." (2015).
4. Arefin, MdMorshedul, and MdEkramul Hamid. "A Comparative Study on Unimodal and Multimodal Biometric Recognition.
5. Ross, Arun, and Anil K. Jain "Multimodal biometrics: An overview." *Signal Processing Conference, 2004 12th European*. IEEE, 2004.
6. Ms. Apurva D. Dhawale, Prof. Dr. K. V. Kale, "Fusion of Iris and Palm print Traits for Human Identification" *International Journal of Computer Techniques — Volume 2 Issue 1*, 2015.
7. Tiwari, Upasana, DeepaliKelkar, and Abhishek Tiwari. "Study of Different IRIS Recognition Methods." *International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 2* (2012).
8. Leonard Flom and AranSafir, "Iris recognition system," U. S. Patent 4641349, 1987.
9. Ma, Li, et al. "Efficient iris recognition by characterizing key local variations." *Image Processing, IEEE Transactions on* 13.6 (2004): 739–750.
10. Daugman, John. "How iris recognition works." *Circuits and Systems for Video Technology, IEEE Transactions on* 14.1 (2004): 21–30.

11. Ives, Robert W., et al. "Iris recognition using the ridge energy direction (RED) algorithm." *Signals, Systems and Computers*, 2008 42nd Asilomar Conference on. IEEE, 2008.
12. Memane, Mayuri M., and Sanjay R. Ganorkar. "RED Algorithm based Iris Recognition." *genetics* 1 (2012): 2.
13. Daugman, John. "New methods in iris recognition." *Systems, Man, and Cybernetics, Part B: Cybernetics*, IEEE Transactions on 37.5 (2007): 1167–1175.
14. Tan, Tieniu, Zhaofeng He, and Zhenan Sun. "Efficient and robust segmentation of noisy iris images for non-cooperative iris recognition." *Image and vision computing* 28.2 (2010): 223–230.
15. Santos, Gil, and Edmundo Hoyle. "A fusion approach to unconstrained iris recognition." *Pattern Recognition Letters* 33.8 (2012): 984–990.
16. Sahmoud, Shaaaban A., and Ibrahim S. Abuhaiba. "Efficient iris segmentation method in unconstrained environments." *Pattern Recognition* 46.12 (2013): 3174–3185.
17. Kaur, Navjot, and Mamta Juneja. "A Novel Approach for Iris Recognition in Unconstrained Environment." *Journal of Emerging Technologies in Web Intelligence* 6.2 (2014): 243–246.
18. Chakraborty, Soumyasree, Indrani Bhattacharya, and Amitava Chatterjee. "A palm print based biometric authentication system using dual tree complex wavelet transform." *Measurement* 46.10 (2013): 4179–4188.
19. Patel, Jugal Kishore, and Sanjay Kumar Dubey. "Deployment of Palm Recognition Approach using Image Processing Technique." *IJCSI International Journal of Computer Science Issues* 10.2 (2013).
20. Duta, Nicolae, Anil K. Jain, and Kanti V. Mardia. "Matching of palm prints." *Pattern Recognition Letters* 23.4 (2002): 477–485.
21. Zhang, David, et al. "Online palm print identification." *Pattern Analysis and Machine Intelligence*, IEEE Transactions on 25.9 (2003): 1041–1050.
22. Han, Chin-Chuan, et al. "Personal authentication using palm-print features." *Pattern recognition* 36.2 (2003): 371–381.
23. Wu, Xiangqian, Kuanquan Wang, and David Zhang. "HMMs based palm print identification." *Biometric Authentication*. Springer Berlin Heidelberg, 2004. 775–781.
24. Wong, KieYih Edward, et al. "Palm print identification using Sobel operator." *Control, Automation, Robotics and Vision*, 2008. ICARCV 2008. 10th International Conference on. IEEE, 2008.
25. Connie, Tee, et al. "Palm print Recognition with PCA and ICA." *Proc. Image and Vision Computing*, New Zealand. 2003.
26. Wong, K. Y. E., G. Sainarayanan, and Ali Chekima. "Palm print identification using discrete cosine transform." *World Engineering Congress*. 2007.
27. Butt, M., et al. "Palm print identification using contourlet transform." *Biometrics: Theory, Applications and Systems*, 2008. BTAS 2008. 2nd IEEE International Conference on. IEEE, 2008.
28. Li, Wenxin, David Zhang, and Zhuoqun Xu. "Palm print identification by Fourier transform." *International Journal of Pattern Recognition and Artificial Intelligence* 16.04 (2002): 417–432.
29. Morales, Aythami, Miguel Ferrer, and Ajay Kumar. "Improved palm print authentication using contactless imaging." *Biometrics: Theory Applications and Systems (BTAS)*, 2010 Fourth IEEE International Conference on. IEEE, 2010.
30. Gayathri, R., and P. Ramamoorthy. "Feature level fusion of palm print and iris." *IJCSI International Journal of Computer Science Issues* 9.4 (2012): 194–203.
31. Kihal, Nassima, Salim Chitroub, and Jean Meunier. "Fusion of iris and palm print for multimodal biometric authentication." *Image Processing Theory, Tools and Applications (IPTA)*, 2014 4th International Conference on. IEEE, 2014.
32. Thepade, Sudeep D., and Rupali K. Bhondave. "Bimodal biometric identification with Palm print and Iris traits using fractional coefficients of Walsh, Haar and Kekre transforms." *Communication, Information & Computing Technology (ICCICT)*, 2015 International Conference on. IEEE, 2015.

33. Tisse, Christel-loic, et al. "Person identification technique using human iris recognition." *Proc. Vision Interface*. 2002.
34. de Martin-Roche, D., Carmen Sanchez-Avila, and C. Sanchez-Reillo. "Iris recognition for biometric identification using dyadic wavelet transform zero-crossing." *Security Technology, 2001 IEEE 35th International Carnahan Conference on*. IEEE, 2001.
35. Roy, Kaushik, Prabir Bhattacharya, and Ramesh Chandra Debnath. "Multi-class SVM based iris recognition." *Computer and information technology, 2007. iccit 2007. 10th international conference on*. IEEE, 2007.
36. Sharma, Shefali, et al. "Identity verification using shape and geometry of human hands." *Expert Systems with Applications* 42.2 (2015): 821–832.
37. GafarZenAlabdeenSalh, Abdelmajid Hassan Mansour, and Malaz Fatah Elrahman Mohammed. "Hand Geometric Recognition System based on Support Vector Machines (SVM)." *Hand* 4.3 (2015).

Fairness Analysis of Fuzzy Adaptive Scheduling Architecture

Akashdeep

Abstract Fairness is key component for any scheduling algorithm. It is more crucial in IEEE 802.16 system where mix of real and non real time applications run concurrently. The study first proposes a three variable fuzzy based scheduling architecture for IEEE 802.16 networks. The proposed architecture solves uplink scheduling problem for IEEE 802.16 adaptively. The proposed system consists of three input and single output variable and makes allocations to real and non real time classes. The paper also lists results of experiment conducted to test fairness of proposed system. Fairness has been measured using Jain's Fairness index and comparisons have been done against contemporary techniques.

Keywords IEEE 802.16 • WiMAX • Fairness • Scheduler performance

1 WiMAX Scheduling

WiMAX stands for Worldwide Inter operability for Microwave Access which is a broadband wireless metropolitan area networks [1] and commercially popularized by WiMAX Forum [2]. No standard algorithm has been specified by standard for implementation of schedulers and this problem has been left as an open issue. Uplink and downlink scheduling is possible in WiMAX but uplink decision are difficult to implement as most recent information about queuing states of subscribers is not available. Many solutions have been proposed and few have been discussed in this section.

A number of queuing theories had been implemented for resource allocation in WiMAX like DRR by Shreedhar and Varghese [3], WRR, Opportunistic DRR by Rath et al. [4]. There have been few studies based on fuzzy logic in recent past. Few of these are listed in this section. Chen et al. [5] were the first to propose an effective fairness and quality of service guaranteed scheduling solution based on fuzzy logic

Akashdeep (✉)
UIET, Panjab University, Chandigarh, India
e-mail: akash.akashdeepsharma@gmail.com

for all service classes in WiMAX networks. The authors in [6] aimed to provide desired qos levels using neuro-fuzzy approach. Fuzzy logic based study was also proposed by Hedayati, Masoumzadeh, & Khorsandi using delay and channel conditions as inputs to fuzzy inference mechanism [7]. Use of fuzzy logic for implementing inter-class scheduler for 802.16 networks had been done by Sadri and Khanmohammadi [8]. Alsahag et al. [9] implemented a dynamic version of DRR algorithm using fuzzy logic concepts. The proposed work extracts recent information about queuing states of subscribers and utilizes that information to guide scheduling decisions. Parameters like latency and throughput are traced out from service flow specification together with amount of traffic in various queues of subscribers. These parameters are fed to fuzzy inference system which outputs a weight value employed as weight for real time classes.

2 A Fuzzy Logic Based Architecture

WFQ is one of the common algorithm used by vendors to configure their devices. The problem with WFQ is the static nature of weights which do not change according to requirements. The proposed architecture implements an adaptive weighted fair queuing algorithm implemented with help of fuzzy logic principles serving both real and non real time traffic classes. Real time classes consist of traffic from UGS, ertPS and rtPS having latency requirements while BE and nrtPS constitutes non-real time class. Scheduling framework for WiMAX with proposed fuzzy system is presented in Fig. 1. The framework aims to impart fairness to all traffic classes and avoid starving of main aim of proposed system is to offer fairness to all type of traffic and avoid starvation of non-real type traffic class. Traffic generated from variety of applications is classified into five different service classes and stored in respective queues by WiMAX classifier. A scheduler available at SS studies QoS requirements for these classes; predicts amount of bandwidth required for various service classes and communicates it to base station. Scheduler at BS performs two functions, first is to transmit data packets to destined SS and secondly to make bandwidth allocations to different SS as per their incoming requests. Separate queues are maintained for both these purposes. Base station calls fuzzy inference system for every bandwidth request received. Fuzzy system located at scheduler on BS is composed of three major steps: fuzzification, reasoning and de-fuzzification. Fuzzification is process of reading input variables into its linguistic form, normalizing them and fuzzifying their physical values. It comprises a process of transforming crisp values into grades of membership for linguistic terms of fuzzy sets. Various membership functions are used to associate a grade to each linguistic term. The next step of reasoning is used to derive inferences to manipulate values of input variables. This step uses stored rules in rule-base to draw inferences. The last step in fuzzy control system is de-fuzzification which is process of producing a quantifiable result in fuzzy logic given its fuzzy sets and membership degrees.

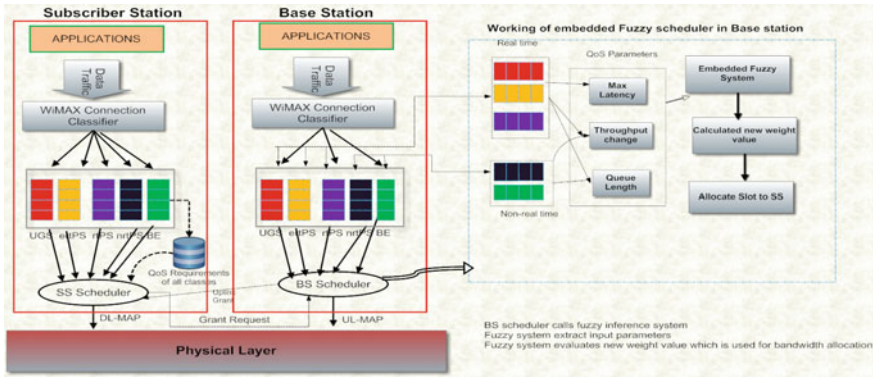


Fig. 1 WiMAX scheduling framework with fuzzy based inference

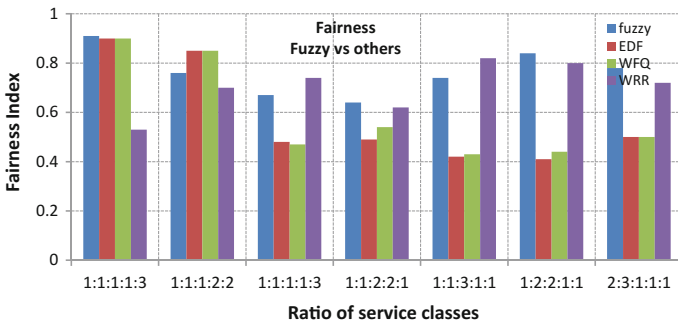


Fig. 2 Fairness comparison of fuzzy system with WFQ, EDF and WRR

It helps to calculate crisp numerical output weight value in our fuzzy control system to police bandwidth allocation of outgoing traffic.

3 Fairness Analysis of Proposed System

This experiment studies effects on fairness being offered to different applications by using variable combination or ratios of SSs. This experiment measures fairness for proposed method and draws comparison with WFQ, WRR and EDF algorithms. Fairness metric for three traffic classes namely rtPS, nrtPS and BE have been considered and Figs. 2 to 5 describe values observed for fairness by proposed and other algorithms. Fairness is measured using Jain’s fairness index. Figure 2 plots values of fairness obtained for proposed system as compared against various methods in different scenarios. It can be observed from the figure that performance of EDF is better for best effort class but there is decrease in performance levels with

increase in quantity of traffic from real time classes. This is because of the fact that these latency driven classes consume significant amount of bandwidth while nrtPS and BE compete for resources among themselves. This variable difference gets substantial and therefore leads to variability in observed fairness values. Values observed for both weighted algorithms sounded same as minimum reserved throughput was used for calculations. Both WRR and WFQ make use of minimum reserved throughput for weight assignment to different subscribers. Relatively stable values are observed by proposed method independent of increase or decrease in number of real or non-real time applications. It is a proof of the fact that proposed method is more fair as compared to other methods.

Experiments were also conducted to test fairness of different service classes for our proposed method and compared with WRR, WFQ and EDF algorithm. Figures 3, 4, 5 portraits fairness observed by rtPS, nrtPS and BE classes respectively. Fairness for only these classes has been observed as any scheduler never makes fixed allocations to these classes as is the case with UGS, ertPS where scheduler can make allocations to these classes.

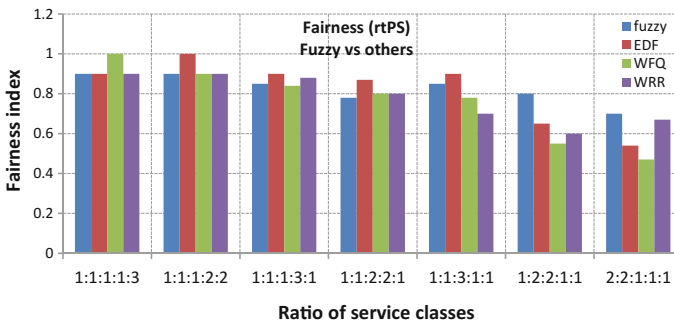


Fig. 3 rtPS fairness comparison of fuzzy system with WFQ, EDF and WRR

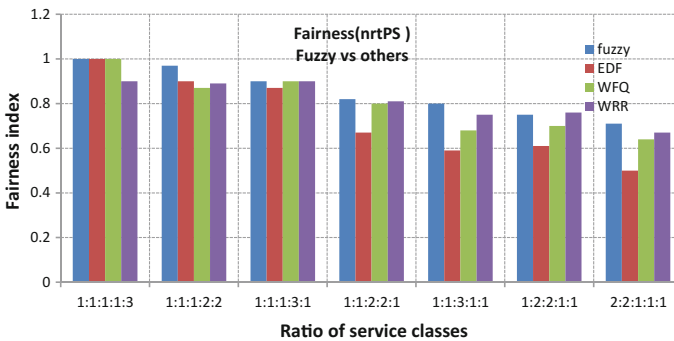


Fig. 4 nrtPS fairness comparison of fuzzy system with WFQ, EDF and WRR

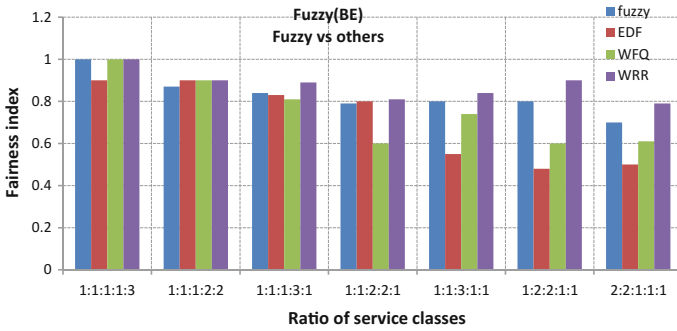


Fig. 5 BE fairness comparison of fuzzy system with WFQ, EDF and WRR

Figure 3 shows that EDF provides more fairness to rtPS when number of connections are limited but it decreases as more UGS and ertPS connections are added which shows that EDF is more inclined towards higher priority classes. WRR and WFQ are fairer but shows decline in fairness at relatively larger number of real time connections. Proposed method is more fair to non real time traffic classes nrtPS and BE as is evident in Figs. 4 and 5. This is because proposed method keeps track of relative increase in traffic of these classes and takes appropriate care by providing them suitable allocation opportunities. Increase in traffic of real time traffic eats up bandwidth allocation opportunities in other algorithms and tries to starve them but fuzzy system intelligently updates weight of its queues in order to prevent less priority classes from starving. EDF is least fair out of all algorithms as it gives more priority to UGS, ertPS and rtPS classes and therefore nrtPS and BE classes compete for slots with each other.

Fairness for BE traffic can be explained as follows, all algorithms are fair to BE class as number of connections are limited and resources are in abundance. Fairness for EDF and our proposed method decreases as UGS and ertPS traffic increases because both these algorithms consider latency requirements of real time traffic while making bandwidth allocations. WRR and WFQ are relatively fairer to BE even when numbers of real time connections are more this is because of implemented utility parameter used to measure fairness which considers fairness proportional to minimum reserved rate.

4 Conclusion

The paper has presented fuzzy based resource allocation mechanism for IEEE 802.16 networks. The proposed system makes the scheduler adaptive and helps to make allocations according to current traffic conditions. The study tests the performance of proposed method on account of fairness. Fairness has been tested by performing four different experiments and different ratio of traffic classes has been

taken. The results of the proposed system are promising as scheduler was able to offer enough fair number of allocations to even low prior non real time classes. Even in case of high ratio of real time classes considerable values for Jain's Fairness index were observed.

References

1. IEEE, 2010. Draft IEEE Standard for Local and metropolitan area networks Corrigendum to IEEE Standard for Local and Metropolitan Area Networks- Advanced Air Inter- face. IEEE P80216 m/D10, November 2010. 2010: 1–1132.
2. URL:- www.wimaxforum.org last accessed on April 2016.
3. Shreedhar M. and Varghese, G. 1998. *Efficient fair queueing using Deficit Round-Robin*. IEEE/ACM Transactions on Networking, 4(3), 375–385.
4. Rath, H. K., Bhorkar A. and Sharma, V. 2006. *An Opportunistic DRR (O-DRR) Uplink Scheduling Scheme for IEEE 802.16-based Broadband Wireless Networks* In Proc. of International Conference on Next Generation Networks (ICNGN), Mumbai.
5. Chenn-Jung Huang, Kai-Wen Hua, I-Fan Chena, You-Jia Chena, and Hong-Xin Chenb, “An intelligent resource management scheme for heterogeneous Wi-fi and WiMAX multi-hop relay networks”, Expert system with applications, Vol. 37, 2010, pp 1134–1142.
6. Kumar, D.D.N.P., Murugesan, K., Raghavan S. and Suganthi, M., *Neural network based Scheduling Algorithm for WiMAX with improved QoS constraints*. 2011. Proceedings of International Conference on Emerging Trends in Electrical and Computer Technology, 1076–1081.
7. Hedayti, F.K.; Masoumzadeh, S.S.; Khorsandi, S.: SAFS: A self adaptive fuzzy based scheduler for real time services in WIMAX system. Communications (COMM), 2012, 9th International Conference on, 247–250. (21–23 June 2013).
8. Sadri Y. and Mohamadi, S. K., 2013. *An intelligent scheduling system using fuzzy logic controller for management of services in WiMAX networks*. Journal of Super computers. 64, 849–861.
9. Alsahag, A.M., Ali, B.M., Noordin, N.K. and Mohamad, H. (2014), Fair uplink bandwidth allocation and latency guarantee for mobile WiMAX using fuzzy adaptive deficit round robin. Journal of Network and Computer Applications, 39, 17–25.

A Novel Approach for Emergency Backup Authentication Using Fourth Factor

K. Sharmila, V. Janaki and A. Nagaraju

Abstract In today's era of improved technology, ease of availability of Internet made every user to access the data at finger tips. Every day transactions are also accomplished online as it is very easy and take less time. Authentication and confidentiality plays a vital role in transmitting the data through the medium of Internet. Authentication is usually implemented through any or all of the authentication factors such as username, password, smart cards, biometrics etc. If the user is unable to provide any of the authentication factors to the system at that instance of time, the user becomes unauthenticated and cannot make any transaction even though, a legitimate user. In this paper we are proposing a new factor for authentication called the fourth factor. This is based on social relations where the legitimate but unauthenticated user can take the help of any trusted third party like a friend, spouse, blood relation who will support in the authentication process in case of failure of credentials. The user can be authenticated with the trusted party and can make a single emergency transaction.

Keywords Vouching • Trusted platform • Social authentication • Fourth factor

K. Sharmila (✉)

Department of CSE, Aurora's Research and Technological Institute, Warangal, India
e-mail: sharmilakreddy@gmail.com

V. Janaki

Department of CSE, Vaagdevi College of Engineering, Warangal, India
e-mail: janakicse@yahoo.com

A. Nagaraju

Department of CSE, Central University of Rajasthan, Ajmer, India
e-mail: nagaraju_aitha@rediffmail.com

1 Introduction

Authentication is considered as the key to security. Authentication in the field of information security is the process by which a system can confirm whether a given person or system is who they claim to be [1, 2]. Electronic authentication is a challenge for both the system and the user. If authentication is compromised, then the rest of the security measures are likely to be compromised as well. So we have to ensure that authentication process is implemented securely.

Authentication is a process in which the credentials provided by the users are to be compared to those that are stored in the database. If the credentials match, the process is completed and the user is granted access to the system. As many transactions are made online, the scope for vulnerabilities is also high [3]. Using one's credentials, any unauthenticated user becomes authenticated if the authentication system fails. In order to avoid impersonations during access control, the authentication techniques are made stronger. There are many authentication techniques available which are used individually as a single factor or with a combination of more than one authentication factors to exclusively identify a user [4].

The authentication factors are categorized as follows [1, 2].

1. Something you know. Ex: a secret password.
2. Something you have. Ex: a secure device with a secret key.
3. Something you are. Ex: a biometric.

In the next section, we will discuss in detail about the above authentication techniques.

2 Literature Survey

In the earlier days, authentication was done using only one factor called passwords. A password is a secret string that is used for authentication. It is termed as "Something the user knows" [1]. These are the most commonly used authentication factors in computer systems, because of their low cost and ease of use. But it is a challenge to the user's memory. As the technology is increasing day by day, security tokens such as one time passwords have come into existence. One time passwords are generated to increase the security and avoid risk on user's memory [2, 5]. Passwords are vulnerable to guessing attacks. So the user has to change the password frequently [6]. To overcome the flaws in one factor authentication, two factor authentication has come into usage [7]. In this, a combination of two factors is to be used in authenticating a user using smart card and PIN number. The methodology involved in manufacturing the smart cards should be tamper resistant and every user has to remember the PIN [8]. The difficulty in this type of authentication is that if any one of the factor fails, he cannot make a successful transaction [9].

Another advancement is the three factor authentication where Biometric authentication systems identify a user based on unique physical characteristics or attributes of a person to authenticate the person's identity [10]. It is a method of identifying an individual based on physical and/or behavioural characteristics [11]. Physical attributes in biometric authentication systems include fingerprint, Iris and voice patterns. They play a vital role as strong authentication factors. Behavioural attributes includes gestures and expressions, which is now limited to theoretical assumptions only and is under research [8].

The biometric authentication system extracts features from the users through a biometric sensor machine and stores it in the database which is used for future verification and authentication [11, 7, 8]. Biometric machinery implementation is cost effective and sometimes, the chance of rejecting an authenticated user is more as the characteristics of the user may not be identified by the machine, if there is even a minute change in the feature [12].

If the user fails to prove his identity with any of the three authentication factors, he would be unable to make any transaction and is treated as an inaccessible user. In such a situation, the user has to contact the Bank personally and get back his credentials which is time consuming. In this scenario, we are proposing a fourth factor, "someone you know" to prove the user's identity. The user is treated as a legitimate user and is permitted to do an emergency transaction [1, 2]. This is termed as Vouching [1].

2.1 Voucher System Properties

Vouching

The main objective of vouching is to provide emergency user authentication. The user can make at least one emergency transaction in case of any disaster or in case where he cannot authenticate himself [1]. Whenever the authorized user is unable to do a transaction due to mismatch of password or loss of debit/credit card or failure of biometrics, he has to make use of this Vouching.

Key Distribution

When we consider symmetric key cryptography, the sender and the receiver should own a secret key which can be exchanged before using any encryption techniques [11, 4]. Distribution of secret keys is complex since it involves either face-to-face meeting or usage of a trusted courier service. It may even include transmitting the key through an existing encryption channel [13].

In public key cryptography, the distribution of public keys is done through public key servers. When a user creates a public-private key-pair, he retains one key privately with him and the public-key is sent to the server where it is made public and can be used by anyone to send an encrypted message.

The main problem of authentication comes into existence while distributing a key. In the network security architecture, users are named by descriptive names and

not keys [14]. So, when we identify the name of a user, we should also find a method in securely finding the key that goes along with the named user.

When two parties A and B meet, A can give B a cryptographic key. This key is received without loss of integrity, since B knows that he has received it from A. A can also use a mutually trusted courier or a trusted third party to deliver a key to B in a secret and authenticated mode [15]. Shared-secret keys need to be distributed through a secure medium of transportation that is both confidential and authenticated [13]. Public keys do not need to be kept secret, but need to be distributed in an authenticated manner [6].

Cryptographic keys can also be delivered over a network. However, an active hacker might add, delete, or modify messages on the network. A good crypto system is needed to be ensured that the network communication is authenticated and confidential [11]. In the earlier days of cryptography, keys were never transmitted over the network since a compromised key may cause more damage than one compromised message [11, 16]. But, nowadays cryptographic systems are developed and implemented strongly so as to overcome that risk. Furthermore, with key-distribution protocol, it is possible to generate new keys periodically [8].

In the later section, we will discuss about social authentication which acts as fourth factor for authentication.

2.2 *Social Authentication*

In this section, we review on social authentication mechanisms. Social authentication is based on the principle that the user can identify a friend or a relative based on the attributes [1, 2]. But using this concept of identification and authentication is a big challenge in information transmission [11]. Social authentication is divided into two categories:

1. Trustee-based social authentication
2. Knowledge-based social authentication

Trustee Based Social Authentication System

Authentication is mainly based on three factors. “Something you know” like a password, “Something you have” like a RSA Secure Id, smart card [17], and “Something you are” like a fingerprint or an Iris. Brainerd et al. [1] have proposed the use of fourth factor, “Somebody you know”, a trust worthy person to authenticate the users. We call this fourth factor as trustee-based social authentication. Initially, Brainard et al. combined trustee-based social authentication with other authentication factor as a two-factor authentication mechanism. It was later adapted to be a backup authenticator. Schechter et al. have proposed a form of trustee-based social authentication system which was incorporated into Microsoft Windows Live ID system [2].

Knowledge Based Social Authentication System

Yardi et al. proposed a knowledge-based authentication system based on photos of the users. If a user belongs to the same group or not is tested as in the social networking sites. Facebook, in recent times has launched a similar photo-based social authentication system [18]. This system relies on the knowledge that the user identifies the person, who is shown in the photographs. However, recent work done by theoretical modelling and empirical evaluations has shown that, these photograph based social authentications are not resilient to various attacks.

3 Problem Statement

In this paper, we worked on the fourth factor authentication, which uses the concept of Vouching [1]. It can also be termed as emergency authentication. The main idea of our proposal is that if the user is unable to provide either his PIN number, smart card or bio-metrics [7], the inaccessible user should be able to authenticate himself for one transaction. Through this fourth factor, the identity of the user is proved, thus making the inaccessible user an authorized and authenticated user. The helper vouches his identity and grants him a temporary password to make one successful transaction.

To ensure the integrity and safety of the system, it is important to identify a person with whom the user is dealing is trustworthy. Authentication helps to establish trust between parties involved in transactions. It involves social relationships where a user trusts the other user when he cannot gain access to the system even though he is an authenticated user [1].

3.1 Prerequisites of Secure Fourth Factor Authentication

1. It is mandatory for every customer to submit the following details while registering himself at the organization like bank for opting Fourth Factor Authentication like
 - a. A mobile number preferably a 10 digit number.
 - b. A valid e-mail id.
 - c. A trust worthy person, preferably his/her Spouse, blood relation or a friend who is also a registered account holder of the same bank.
2. Every user is given a unique id as an account number and a secret key by the bank which is shared between the user and the bank.
3. Every user has to submit a secret question along with the answer which could be used by the bank as part of validation.

When a user provides all the three factors of authentication, his PIN, Card Number, Biometrics then the transaction is completed successfully. If he fails to provide any of the three factors, he cannot continue his transaction. In this case, even though he is an authorized user, he is unable to make his transactions and he has to identify himself to the bank [10]. At this juncture, the user opts for Secure Fourth Factor Authentication which we also term it as Emergency Authentication. In the rest of the paper, inaccessible user is called as Asker and the trustworthy person is termed as Helper.

Figure 1 shows the flow of transaction. There are three entities, the Asker, Helper and the Trusted Platform or the server.

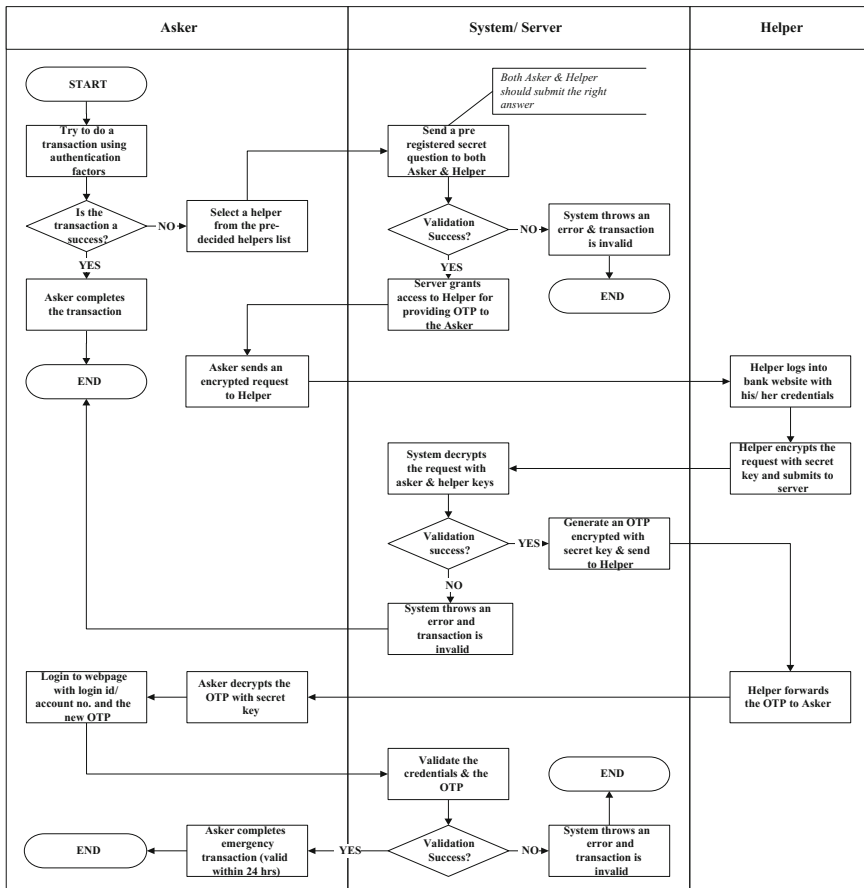


Fig. 1 Flow of transaction in secure fourth factor authentication

3.2 Algorithm

1. The first step the user has to perform, is to login to the respective bank web page.
2. If he tries to make any transaction, a message is displayed stating that “Your Card is blocked”.
3. An option is given to the user/Asker (As) whether he wants to make use of Emergency Authentication.
4. If he chooses “No”, then a message “Visit your Bank Personally” will be displayed.
5. If he chooses “YES”, then the pre-decided Helper’s (Hp) names are displayed on the screen.
6. After selecting the Helper (Hp), a secret question (Pre-registered with the bank) is sent to both Asker (As) and Helper (Hp).
7. If the answers to the above corresponding questions are correct, then the bank trusts both Asker and Helper as authorized and the bank accepts the request sent by the Helper.
8. The Asker sends his request in the form of an encrypted message to the helper. The request includes his Account number, security question and time stamp encrypted with the pre-defined secret key K_{AsB} . $As_req: E_{K_{SA}}\{AN_A, SQ_A, TS_{SYS}\}$
9. After receiving the above information, the helper (Hp) once again assures the Asker (As) through his own method of communication (personally, phone contact or any other possible means of communication).
10. The helper (Hp) has to login into the corresponding bank web page using his valid credentials. $Hp_resp: \{ID_{Hp}\}$
11. The helper then forwards the request received from the Asker, along with his own credentials (his Account Number/user id and password) to the bank. Here, the entire information is encrypted with pre-defined secret key K_{HB} (shared between Helper and Banker). $Hp_req_B: \{As_req, K_{HpB}\}$
12. The above information is validated by the server and if found correct, it sends an Emergency Password to the helper which is encrypted with the secret key K_{AsB} (Shared between Asker and Banker), to prevent any further modifications by the helper.
13. The Helper (Hp) forwards this information to the Asker (As).
14. The Asker (As) has to once again log on to the webpage using his existing credentials like login id or account number, whichever is available along with the received message in the provided text area.
15. The same pre-defined secret key is submitted by the Asker. As this is a valid message sent by the banker, OTP is generated.
16. The bank validates the Asker and then permits him to make his transaction using his same card number and this newly generated OTP. This facility is available to the users only once within 24 h.

4 Practical Implementation

We have implemented the Secure Fourth Factor Authentication protocol using Java, Tomcat server and MySQL Database. We have used AES Symmetric-key algorithm [19] that uses the identical cryptographic keys for both encryption of plaintext and decryption of cipher text. AES operates on a 4×4 column-major order matrix of bytes, called as the state. Most of the AES calculations are done in a special finite field. AES implements 10 cycles of repetition for 128-bit keys.

Each cycle/round consists of several processing steps. Each step contains four similar stages but different in execution, together with one that depends on the encryption key itself. A set of reverse rounds is applied in the algorithm to transform the cipher text back into the original plaintext using the same encryption key [19].

The Asker selects the Emergency Authentication Option in the Trusted Platform [3]. It displays the corresponding helpers list associated with the Asker. The Asker selects one helper from the list and a secret question is sent both to the Asker and the Helper. If both of them enter the correct answer, then the server treats both the users as legitimate users and grants permission to continue the transaction. The asker then sends his request to the helper. This request message is encrypted and sent to the helper. The helper receives the request from the Asker, logs into the trusted platform, proves his identity first and then forwards the request sent by the Asker to the Server [2, 3, 4]. The server validates the identity of both the users and forwards a onetime vouch code to the Helper [1]. The Helper then forwards the same to the Asker who enters this onetime vouch code at the server side [7]. If the entered vouch code is matched, then the server grants permission to the Asker to make one emergency transaction valid only for 24 h [6].

5 Experiments and Results

We have conducted experiments and our input is a combination of three parameters. They are account number of the Asker, secret answer of the Asker and the time stamp at which the request was generated. This input is converted into a fixed block size of 128 bits, as we have used AES algorithm. The input given to the algorithm is Account number + Secret key + Time stamp as shown in Fig. 2.

For example:

Account number of the Asker is 1057862349, Secret key is 1454661094765 and Time stamp is 102538.

The output for the corresponding input is as follows

Encryption key: 9d0811bad3e1cc77

Asker's OTP: 20646181

Helper's OTP: 66714972 (Figs. 3, 4 and 5)

Fig. 2 Scenario where the authenticated user fails to provide his credentials

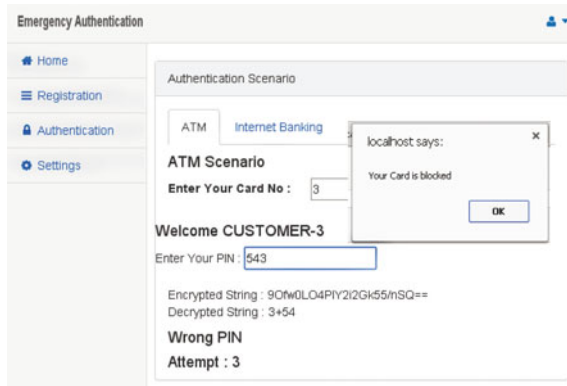


Fig. 3 Asker selecting his helper from the list of available helpers

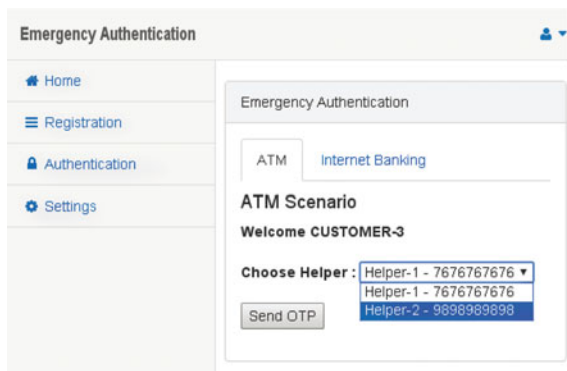


Fig. 4 User enters OTP generated by the server

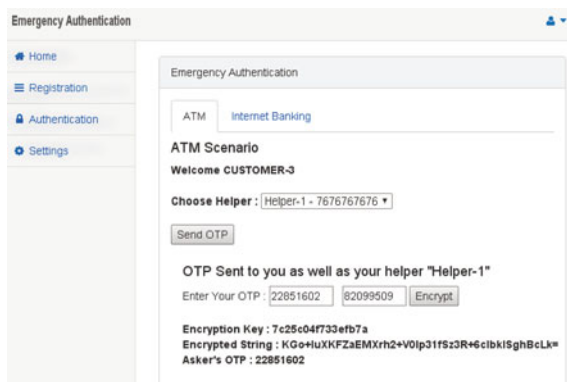
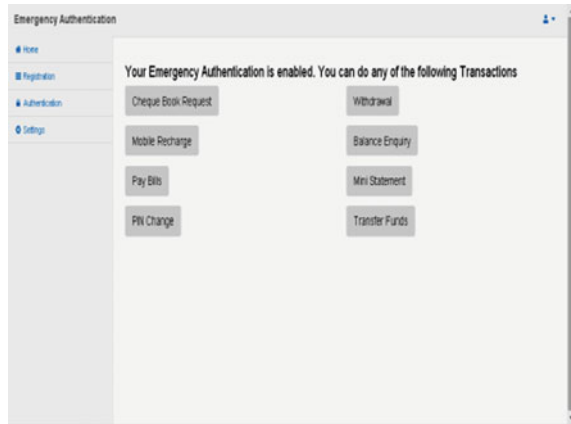


Fig. 5 System permitting the user to make an emergency authentication



6 Conclusion

In the traditional method of creating an account in any financial organization, an introducer is mandatory. A similar kind of concept has been introduced for our secure fourth factor authentication protocol. Our Proposal enables an inaccessible user to authenticate himself in emergency, where he cannot prove his identity due to the failure of any of his authentication factors. In our protocol, we have taken all the necessary steps to overcome the problem of misfeasors. Any trustworthy person cannot play the role of an Asker and he alone cannot make an emergency transaction without the secret key of the Asker. If a trust worthy person deceives the user, then our protocol may not reach the expectations. So selecting a trust worthy or a faithful person is more important in Secure Fourth Factor Authentication.

References

1. John Brainard., Ari juels., Ronald Rivest L., Michael Szydlo., Moti Yung.: Fourth Factor Authentication: Somebody You Know. ACM, (2010)
2. Schechter S., Egelman S., Reeder R.W.: It's not what you know, but who you know: A Social Approach to Last-Resort Authentication. ACM SIGCHI, Conference on Human Factors in Computing Systems, (2009)
3. McCune J.M., Perrig A., Reiter M.K., Seeing-is-believing: Using camera phones for human-verifiable authentication. in. IEEE Symposium on Security and Privacy, pp. 110–124, (2005)
4. Xinyi Huang., Yang Ashley Chonka., Jianying Zhou., Robert H. Deng.: A Generic Framework for Three-Factor Authentication Preserving Security and Privacy in Distributed Systems, in. IEEE Xplore, (2011)
5. Wen-Bin Hsieh., Jenq-ShiouLeu., “Design of a time and location based One-Time Password authentication scheme”, 7th International Wireless Communications and Mobile Computing Conference, 978-1-4244-9539-9, (2011)

6. EkoSediyono., Kartika Imam., Santoso., Suhartono., “Secure login by using One-time Password authentication based on MD5 Hash encrypted SMS”, 978-1-4799-2432-5, Aug. (2013)
7. Jiri Sobotka., RadekDolze.: Multifactor Authentication Systems, pp. 1–7, (2010)
8. Clancy C. T., Kiyavash N., Lin D. J.:. Secure Smartcard-Based Fingerprint Authentication, in. Workshop on Biometric Methods and Applications, (2003)
9. Stephen S. Hamilton., Martin C. Carlisle., John A. Hamilton.: A Global Look at Authentication, in. IEEE SMC Information Assurance Workshop, West Point NY, (2007)
10. Bhargav-Spantzel A., Squicciarini A., ElisaB.: Privacy Preserving Multi-Factor Authentication with Biometrics, pp 63–71, DIM Alexandria Virginia, (2006)
11. GarfinkelS. L., Email-Based Identification and Authentication: An Alternative to PKI, IEEE Computer Society, pp. 20–26, (2003)
12. Jain A., Hong. L., Pankanti. S.: Biometric Identification. In. Communications of the ACM, pp 91–98, (2010)
13. M. C. Chuang and M. C. Chen, “An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics,” Expert Systems with Applications, 41(1):1411–1418, (2014)
14. Chun-Ta Li., Cheng-Chi Lee., Hua-Hsuan Chen., Min-JieSyu., Chun-Cheng Wang., “Cryptanalysis of An Anonymous Multi-Server Authenticated Key Agreement Scheme Using Smart Cards and Biometrics”, 978–1-4799-8342-1/15, IEEE 498 ICCIN (2015)
15. FadiAloul., Syed Zahidi., Wassim El-Haj.:Two Factor Authentication Using Mobile Phones, in. IEEE International Conferenceon Computer Systems and Applications, AICCSA, pp. 641–644. (2009)
16. BijanSoleymani., MuthucumarMaheswaran.: Social Authentication Protocol for Mobile Phones in International Conference on Computational Science and Engineering, (2009)
17. RSA SecureID Authenticators: <http://www.rsa.com>
18. Yardi S., Feamster., Bruckman A.:. Photo-based authentication using social networks In WOSN, (2008)
19. RituPahal., Vikaskumar.:. Efficient Implementation of AES.:. International Journal of Advanced Research in Computer Science and Software Engineering, 3,7, (2013)
20. Xiao-Min Wang., Wen-Fang Zhang., Jia-Shu Zhang., Muhammad Khurram Khan.: Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards, (2007)

Automated Cooling/Heating Mechanism for Garments

Akash Iyengar, Dhruv Marwha and Sumit Singh

Abstract We present here an automated Temperature controlled clothing system. The innovative design uses conducting coils, which make use of the Peltier effect for controlling the comfortable temperature of clothing. It uses the micro-controller (Arduino) for sensing the temperature (Array of Sensors). Based on the temperature changes, the heating and cooling system can be activated or de-activated as required. The design facilitates a differential temperature control system for different parts of the body to maximize the comfort. The system can find numerous applications on real life.

Keywords Automated heating and cooling • Body temperature • Peltier effect • Heat transfer • Micro controller

1 Introduction

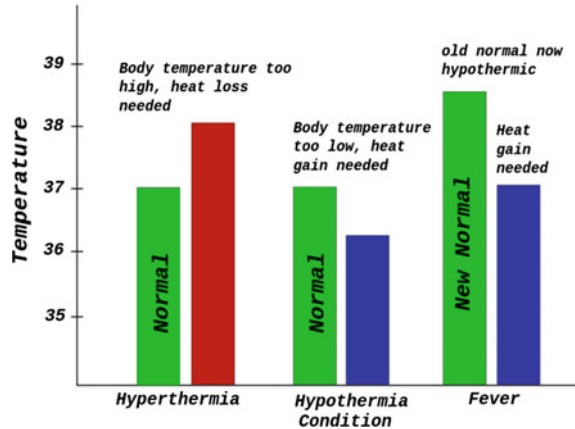
In today's fast paced and globally connected World, people's basic needs are very demanding and this is driving technology to create automated solutions for our daily problems. People in this decade have traveled to places where weather conditions contrast with where they live in. For Example: A person whose lived in India since his childhood now finds himself as a student in Wisconsin where he has to deal with extreme weather conditions (subzero temperatures and/or blistering hot weather in some parts of the world). In this case, technology can help a person to adapt and be comfortable. An automated temperature sensing process can be deployed to measure current body temperature with a variety of sensors to control it

A. Iyengar (✉) · D. Marwha · S. Singh
Department of Computer Science and Engineering, SRM University, Chennai, India
e-mail: akashiyengar72@gmail.com

D. Marwha
e-mail: marwha.dhruv@gmail.com

S. Singh
e-mail: sumitlucricket@gmail.com

Fig. 1 Temperature for various body conditions like hypothermia, hyperthermia and fever



according to the external temperature. Also, studies have shown that the very young and the very old people are very susceptible to cold which makes them susceptible to hypothermia and hyperthermia [1]. The graph shows the various temperature changes with respect to various conditions as shown in Fig. 1 [2].

2 Existing System

There are 2 different models which are in existence- Manual temperature control NASA Spacesuit technology and space blanket. In manual control, the temperature can be controlled with the help of a knob/dial which will regulate the power going to the coils and control the temperature. In NASA space-blanket technology, researchers have deposited vaporized aluminum onto plastic. The result was a very thin but durable sheet of material that is very good in reflecting the infrared waves that created heat. The material could either reflect and preserve body heat or ward off the intense radiation of the sun [3] the same material can also be used in sleeping bags which can reflect 90% of body heat. While in the spacesuit technology, it is layer of clothing which has a provision for rubber pipes through which liquid water is circulated which keeps the suit cool and helps the astronaut to maintain his/her body temperature.

3 Disadvantages of Existing System

- With regards to the spacesuit tech, it's not very practical for daily use.
- It is very expensive.
- The space blanket can only conserve heat. It cannot produce external heat based on the user's preference.
- A blanket can't we worn everywhere any time of the day. Its use is limited.

4 Proposed System

In our proposed system the system is split into three distinct components namely:

- Temperature Sensing Module
- Temperature Control Module
- Control Unit.

4.1 Temperature Sensing Module

Temperature is basically degree or intensity of heat present in a substance or object, especially as expressed according to a comparative scale and shown by a thermometer or perceived by touch [4]. In this model, an array of temperature sensors measures the temperature by sensing some changes in the physical characteristics. This is usually done with the help of temperature sensors which can be interfaced with a micro-controller. We will be using TSYS01 sensors for sensing the body temperature. This sensor measures the body temperature by measuring thermal radiation emitted from the body. It can measure temperature ranging from -40 to 125 °C at an accuracy of ± 0.1 °C. It provides a 24 bit temperature reading which indicate the actual body temperature [5]. The TSYS01 Sensor can be interfaced with any micro-controller by an I2C interface or an SPI Interface. Figure 2 describes the TSYS01 Architecture in detail [6].

4.2 Temperature Control Module

Now that we have proposed the temperature sensing module, the next step is to control the temperature of the cloth based on the input given by the temperature sensor. The heating and cooling is achieved with the help of “Peltier Effect”.

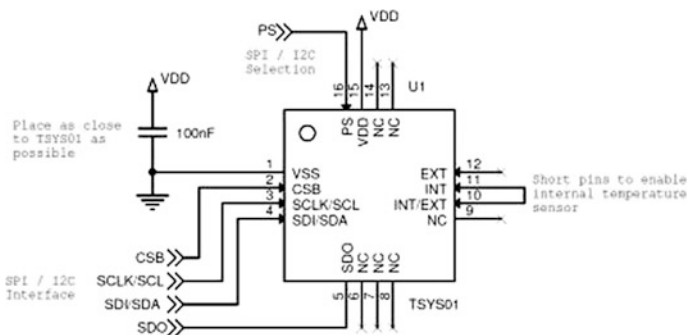


Fig. 2 TSYS01 architecture diagram

Fig. 3 TEC12706
semiconductor thermoelectric
peltier cooler/heater module



The **Peltier effect** is a temperature difference created by applying a voltage between two electrodes connected to a sample of semiconductor material [7]. This phenomenon can be useful when it is necessary to transfer heat from one medium to another on a small scale. This can be accomplished with the help of “TEC-12706” Semiconductor Thermoelectric Peltier Cooler/Heater Module. The module basically consists of electrodes that are typically made of metals with excellent conductivity. The semiconductor material between the electrodes creates junctions which in turn creates a pair of thermocouples. When voltage is supplied across these electrodes, thermal energy flows in the direction of charge carriers. When the flow of charge carriers is reversed, alternative heating and cooling can be achieved. For forward current flow, heating can be activated and for reverse current flow, cooling can be achieved [8]. Figure 3 describes the “TEC-12706”.

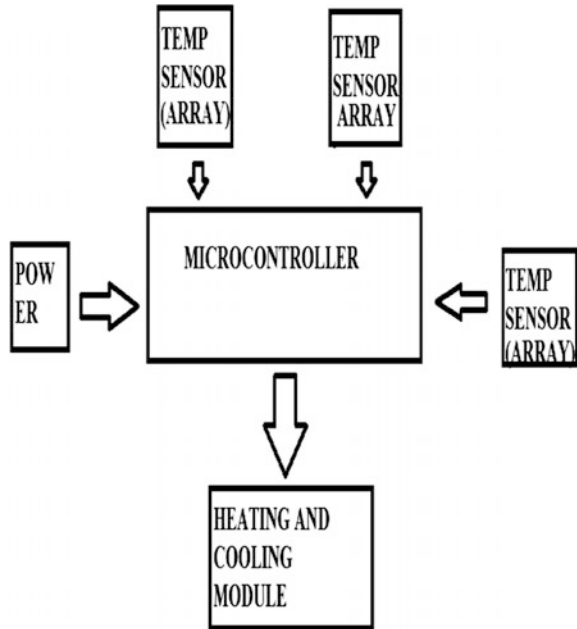
4.3 Control Unit

The controlling unit of the system is a micro-controller (Arduino UNO). It consists of pins (Analog/Digital) which can be used to attach various peripherals [9]. Here we are using the digital pin of the Arduino to connect the temperature sensor. The Arduino is programmed along with preset values for triggering the temperature controlling module of the system. The Arduino board also receives input in the form of temperature which can be used as a trigger mechanism (Fig. 4).

5 Working Principle

The module consists of the temperature sensor which records the body temperature. The temperature sensor basically is placed in contact with the skin and it constantly gets the body temperature as the input. This input is given to the micro controller

Fig. 4 Block diagram of the control unit



(Arduino) which primarily controls the temperature of the clothing. The micro controller basically consists of a program which compares the pre-defined temperature with the dynamic input of the sensor. If the temperature is below the pre-defined value, the heating system gets activated and when the temperature is above the pre-defined value, the cooling system gets activated. The temperature sensor and the micro controller together acts as a monitor for the body temperature.

Pseudo Code for Temperature Control

While (System is ON)

Gather temperature from various temperature sensors

Take an average of that value as the temperature using which the heating/cooling system will work.

If (body temperature < temperature)

Send +5v (HIGH) supply to the “TEC-12706” via micro controller for Heating

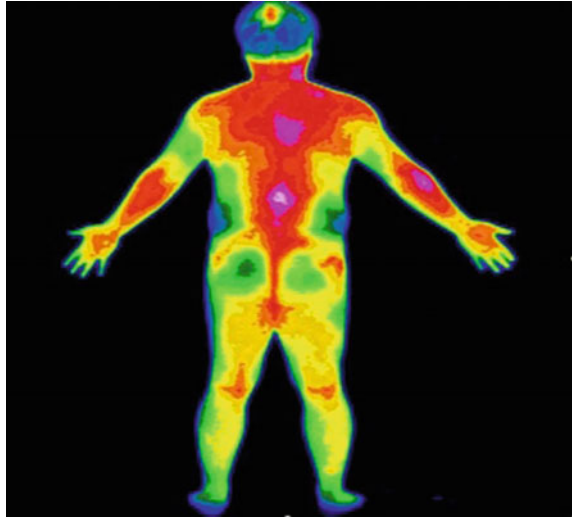
Else if (body temperature > temperature)

Send +5V (HIGH) to the “TEC-12706” via micro controller for cooling

Else

Send 0V (LOW) to the “TEC-12706” (No Change)

Fig. 5 Thermal Scan of an average human for heat/cold zones



6 Placement of Heating/Cooling Modules

The TEC 12706 module(s) should be placed in the areas where the body heat is released the most and these are the places where the heating and cooling will be most effective. Some research needs to be done in this area so as to identify the best places for placement of the module(s) which can be done with the use of thermal imaging. Reference [10], which is illustrated with the help of Fig. 5.

7 Safety

Since the clothing contains electronics which if not handled properly might give a shock to the user. To ensure that this does not happen, we can use a dual layer system wherein the electronics of the entire system is encased within a separate layer of material so as to create insulation around the electronic components so as to ensure that an accidental shock does not take place.

8 Heat Sink

For the efficient operation of the entire system, heat sinks need to be installed on top of the Peltier effect module so that the system works properly. For this, some Research needs to be done for designing a heat sink which will have the same

dimensions as the module and differential cooling can also be used meaning for different areas, different sized Peltier effect modules can be used with the corresponding heat sinks to provide the cooling and heating as required.

9 Battery Pack

An average module requires close to 24 V of power supply so based on the target application, the power requirements need to be altered. Also while implementing differential cooling, the wattage of the module needs to be taken care of and appropriate calculations need to be done to choose the correct one for the chosen system. Ideally, the battery pack could be made as a portable box type format which could be clipped to the hip to ensure portability and the casing needs to be made of a high heat dissipating material which would help the battery to perform at its best.

10 Hardware Implementation

The system uses the following components:

- Micro controller (Arduino UNO).
- Temperature Sensor (TSYS01).
- Peltier Semiconductor Heating/Cooling module (TEC-12706).
- Resistors.
- Breadboard.
- Wires or Conducting threads.
- Clothing on which system is to be made.
- Power Source (Battery).
- Software for programming the micro-controller (Arduino IDE).

11 Advantages of Proposed System

- The system is automated and it minimizes human effort.
- It can be used in varying climatic conditions.
- It is much more accurate as the input is received with the help of multiple temperature sensors.
- Plus it is suitable for daily use and it's practical in nature.

12 Disadvantages of Proposed System

- Initial R&D is expensive (Mapping of heat zones of the body, battery and heat sinks).
- The Heating/Cooling mechanism takes time to produce the required heating/cooling effect. (Not instantaneous in nature).

13 Conclusion

We conclude that the system is beneficial in both medical field as well as for daily use. The system can be improved and made more specific based on its use. It can be also implemented on any type of garment based on its size and some modifications may need to be made. Based on the same concept, further applications include:

- (1) Automatic Milk heating bottles for small kids
- (2) Specialized garments for small kids (2–3 yrs).
- (3) Automatic Temperature Management for Aquariums.

The possibility for the said topic as mentioned in the paper is endless.

Acknowledgements We would like to thank our friends and family for supporting us in this endeavor and we would also like to thank SRM University for supporting us.

References

1. <https://www.commons.wikimedia.org/File:Fever-conceptual.svg>.
2. www.webmd.com/a-to-z-guides/what-is-hypothermia.
3. <http://science.howstuffworks.com/innovation/nasa-inventions/nasa-technology-keep-warm.htm>.
4. <http://www.merriam-webster.com/dictionary/temperature>.
5. <http://news.thomasnet.com/fullstory/digital-temperature-sensor-provides-0-1-c-accuracy-612406>.
6. http://www.measspec.com/news/product/temperature/TSYS01AppNote.aspx?menu_id=598&tax_id=134.
7. <http://searchnetworking.techtargot.com/definition/Peltier-effect>.
8. <http://www.ioffer.com/i/tec1-12706-thermoelectric-cooler-peltier-12v-60w-548278650>.
9. <https://www.arduino.cc/en/Guide/Introduction>.
10. <http://outdoors.stackexchange.com/questions/681/what-are-areas-of-the-body-which-lose-heat-more-quickly-and-how-can-i-reduce-th>.

Anatomization of Software Quality Factors: Measures and Metrics

Aditi Kumar, Madhulika Bhatia, Anchal Garg and Madhurima

Abstract “If you cannot measure it, you cannot manage it”, this quote by Lord Kelvin is very much applicable to the world of Software Quality as well. Quality of software can be described as the extent to which it performs the task that the user has specified. It can be expressed in terms of multiple factors like reliability, readability, supportability et al. It can be best described as the amalgamation of these multiple factors. Not only the identification of factors but also of the metrics and measures were done by studying and analyzing various research papers and keeping them as the primary foundation. This paper focus on investigating the measures that is already available to determine the different quality factors. The results obtained are advantageous for software developers, researchers and academicians to recognize and distinguish the cadent used to dimension the different quality characteristics of the software. Moreover, the work focuses at giving some suggestions, using the potential deficiencies detected as a foundation.

Keywords Software measures · Analytics · Quality factors

1 Introduction

Quality is one of the primary issues on which most of the researchers work while developing a software. While selecting the software product the user ratify the software product’s quality, in terms of various quality factors. Software Quality Assessment should be in accordance with the Software Engineering process being used, and be relevant and applicable at the operation level. [1], therefore, it is not advised to upgrade the quality after the software is completed as it increases the cost remarkably and it makes the product defected. Hence to vanquish this problem the evaluation of software product quality is suggested at developer’s end during the formulation of software product [2]. The measurement of quality is mostly

A. Kumar (✉) · M. Bhatia · A. Garg · Madhurima
Amity University, Noida, Uttar Pradesh, India
e-mail: adi.5062134@gmail.com

conveyed in respect of metrics. Measurement of one or more quality criteria is done by software metric [3]. Many past studies have kept their focus on various factors and related sub factors that influence the software quality and some of the former studies talk about the measurements and metrics used to measure the level of specific quality factor. The key purpose of this paper is to give a general overview of the software metrics and all the measures and also to guide other readers and researchers to follow which metrics can be used to measure the different factors of quality.

2 Methodology

In this paper, methodical approach for reviewing the literature on the analysis of the measures and metrics of quality factors follow the same approach which were identified by Kitchenham and Charters [4].

2.1 Research Questions

The objective of this paper is to analyze certain measures and metrics for certain quality factors. The foundation of this analysis are the research questions (RQ) as described in Table 1.

3 Background and Related Work

Quality in use metrics identifies and recognizes the metrics used to measure the outcomes and the combined quality characteristics effects for the users. In more specific terms, these metrics care about the quality in customer's satisfaction. The metrics for performance, effectiveness, productivity and safety in real environment fall in this particular category [5]. At the end, external factors matter the most, but these external factors can be achieved only through the internal ones. In other words, if the implementers and designers want their users to enjoy the visible level of qualities, they must have applied some internal techniques that will ensure those hidden qualities [6].

Table 1 Research questions

Research questions	
RQ1	Which quality factor can be easily approached for measuring?
RQ2	Which measure is advised for usage of certain metric to determine different quality factors?

3.1 Object—Oriented Design Metrics and Measures

As specified by Srinivasan et al. [7] the underlying are the supreme measures to examine quality Object—Oriented design’s quality in the design phase. There are many design metrics based on object like coupling, cohesion, Inheritance, abstraction and encapsulation and package cohesion. There are many quality factors and measures for each like Understandability, effectiveness, extendibility and reusability.

3.2 Dynamic Metrics and Measures

Dynamic metrics helps in computing and measuring specific runtime attributes of components, programs, systems and subsystems. According to Tahir et al. [8], Sandhu et al. [9] and Choi et al. [10], underlying are some of the metric type which predict the qualities related to dynamic systems using the measures given in Table 3. A tool has been developed and deployed using the aspect—oriented programming (Aspectj) to perform dynamic analysis of applications written in java for collecting the data generated at the run time needed for the dynamic coupling tracer and dynamic cohesion metrics application has been developed in Aspectj for measuring the coupling [11] (Table 2).

Table 2 Dynamic metric and quality factors coverage

Metrics	Quality factors	Associated measures
Cohesion	Reusability	Calculate each instance of variable by the number of time it is being attained
		Message passing load (MPL)
Coupling	Understandability	MPL
	Reliability	Charts of real-time object oriented modeling (ROOM)
	To predict faults	Crosscutting degree of an aspect and base-aspect coupling
Complexity	Understandability	Decision points in the code
Polymorphism	Reusability	The polymorphic behavior index is $P/Total\ dispatches$ Where, $Total\ dispatches = (NP + P)$ $P = Unique\ polymorphic\ dispatches\ executed$ $NP = Unique\ and\ non-polymorphic\ dispatches\ executed$
		Efficiency

Table 3 Technical documentation quality metrics and quality factors coverage

Metrics	Quality factors	Tool used to calculate metrics
Clone detection	Maintainability	VizzAnalyzer
Test success and coverage	Usability	

3.3 Technical Documentation Quality Metrics

In Wingkvist et al. [12] it has been seen, that analogizing the text on XML structures and paragraph level, Clone detection computes the similarity between documents and size of two documents that are distinctive which are the indications of one of the quality of maintainability.

Test coverage measurement analyzes statically the complete structure of any technical documentation, dynamically logs those documents and the hyperlinks followed during testing, and then correlates the dynamic and static information [12], which indicates one of the quality of usability in technical documentation. DocFactory is one of the producers of technical documentation and VizzAnalyzer is a tool that assesses the document’s technical quality which supports metrics, such as, coverage analysis and clone detection. To conceptualize the metrics results, tools such as the yEd graph viewer and Microsoft Excel, can be used.

4 Results of the Study

A. Answering Research Questions

RQ1: Which quality factor can be easily approached for measuring?

After analyzing measures and metrics for different quality factors across the 20 studies in detail, it is found that understandability could be easily approached for measuring. Figure 1 shows the availability of many measures to estimate different quality factors. Results gives some evidence to suggest that many metrics and measures are there which can be used to determine the quality for Object-oriented systems.

RQ2: Which measure is advised for usage for certain metric to determine different quality factors

Many varied metrics and measures have been used in and finally included 20 studies. These mainly fall into source code metrics, dynamic metrics and metrics relating to documentation. Moreover, dynamic metrics across the 12 studies that

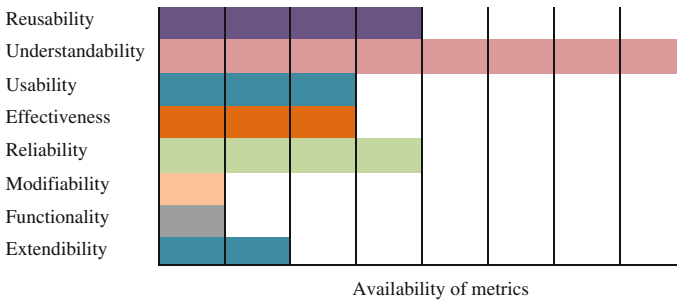


Fig. 1 Indicative levels of availability of measures to evaluate quality factors

were analyzed in detail puts forward measures relatively well. However after having a look at the findings from the individual studies, many authors report that quality is not only determined by process metrics but also in the form of product and also even by documentation metrics.

5 Conclusion

Metrics is a vital topic in the area of software engineering. Metrics can improve the quality of systems significantly. Therefore many measurement and metrics studies in the area of software engineering have been published. In this paper analysis and review of 30 studies shows that large number of metrics were used but it is extremely difficult for the researchers to discern and analyze the metrics and measures of quality factors for similar software systems. The set of metrics gives the vital measures to determine the software quality. It can be used and analyzed by future quality prediction researchers, software engineers and by journals and conference reviewers. Of the 30 studies that were viewed, only 20 satisfied the criteria and helped in determining what impacts on quality factors. The results advocate that many measures and metrics are available to discern the understandability of the system. It has been also found that many measures and metrics are available for object- oriented Systems. From this study, it has been also gain the knowledge that there is interdependence. between quality factors as measuring metrics computes more than one quality factors. There are many good measures are already available to determine quality in software systems that have been reported in software engineering.

Note: Authors are in process of developing a Mobile Application which calculate the software metrics for the programme or software and it will be a great help for project managers and software developers.

References

1. Grambow, G., Oberhauser, R., & Reichert, M. (2011). Contextual injection of quality measures into software engineering processes. *Int'l Journal on Advances in Software*, 4(1&2), 76–99.
2. Aman Kumar Sharma, Dr. Arvind Kalia, Dr. Hardeep, “An Analysis of Optimum Software Quality Factors”, *IOSR Journal of Engineering*, 2(4), 2012, 663–669.
3. Gillies, A. (2011). *Software quality: theory and management*. Lulu. com
4. Keele, S. (2007). Guidelines for performing systematic literature reviews in software engineering. In Technical report, Ver. 2.3 EBSE Technical Report. EBSE.
5. Pusatli, O. T., & Misra, S. (2011). A discussion on assuring software quality in small and medium software enterprises: An empirical investigation. *Tehnički vjesnik*, 18(3), 447–452 of scientific journals of croatia, 18(3), 2011, 447–452.

6. Mallikarjuna, C., Babu, K. S., & Babu, P. C. (2014). A Report on the Analysis of Software Maintenance and Impact on Quality Factors. *International Journal of Engineering Sciences Research-IJESR*, 5.
7. Srinivasan, K. P., & Devi, T. (2014). A Complete and Comprehensive Metrics Suite for Object-Oriented Design Quality Assessment. *International Journal of Software Engineering and Its Applications*, 8(2), 173–188.
8. Tahir, MacDonell, S.G., “A Systematic mapping study on dynamic software quality metrics”, Proc. 28th IEEE International Conference on Software Maintenance, Riva del Garda, Italy, 2012, 326–335.
9. Sandhu, P. S., & Singh, G. (2008). Dynamic metrics for polymorphism in object oriented systems. *World Academy of Science, Engineering and Technology*, 39.
10. Choi, K. H., & Temporo, E. (2007, January). Dynamic measurement of polymorphism. In *Proceedings of the thirtieth Australasian conference on Computer science-Volume 62* (pp. 211–220). Australian Computer Society, Inc.
11. Gupta, V. (2010). Object-Oriented Static and Dynamic Software Metrics for Design and Complexity (Doctoral dissertation, National Institute of Technology Kurukshetra-136119 India).
12. Wingkvist, A., Ericsson, M., Lincke, R., & Lowe, W. (2010, September). A metrics-based approach to technical documentation quality. In *Quality of Information and Communications Technology (QUATIC)*, 2010 Seventh International Conference on the (pp. 476–481). IEEE.

Dynamic Scheduling of Elevators with Reduced Waiting Time of Passengers in Elevator Group Control System: Fuzzy System Approach

Malan D. Sale and V. Chandra Prakash

Abstract From the commercial point of view, in tall buildings with multiple lifts or elevators, owners face problems like waste of space, more managing time and money. People travelling by lifts face problem of high waiting time. Elevator Group Control System (EGCS) manages several elevators in tall buildings for efficient carrying of passengers. Waiting time of people and car are major factors affecting the performance of EGCS. EGCS organizes elevators to reduce the performance evaluation measures. But, it is hard to achieve all measures. Hence, here we deal with the improvement of performance by reducing waiting time of the passengers. The proposed system introduces dynamic scheduling algorithm to schedule elevators dynamically. The proposed system uses fuzzy logic to schedule and dispatch the elevators. The main motive of the research work is to diminish the passenger's waiting time and car allocation time.

Keywords Elevator group control system EGCS • Fuzzy controller • Up-peak traffic • Down-peak traffic

1 Introduction

In tall commercial buildings with one lift passengers face many problems. Normally, during the peak periods in the morning and evening, people wait for lift; as everyone is in hurry and would like to reach home in time. During morning period people make up-landing calls but the lift waiting time is high as everyone want to reach office. There are more up-landing calls in the morning as compared to down-landing calls. This type of situation is called up-peak traffic. We may observe

M.D. Sale (✉) • V. Chandra Prakash
Computer Science and Engineering, K.L. University, Vaddeswaram,
Guntur District, Andhra Pradesh, India
e-mail: mdsale2006@gmail.com

V. Chandra Prakash
e-mail: vchandrap@kluniversity.in

opposite scenario in the evening. All people would like to reach home early, and hence they make down-landing calls; but they need to wait for lift. This type of traffic is called down-peak traffic. We may see the same scenario during lunch time when people go out for the lunch and come back after lunch. People waste their time in waiting for the lifts, resulting in frustration. The solution to this problem is to use EGCS to control the multiple lifts [1].

The proposed system is useful in all buildings where vertical transportation is provided with multiple elevators. Even or odd floor elevators can provide better performance with the dynamic allocation of a car. Nowadays when we use lift to go up and if any car call is made during the up-landing call then the car stops at the calling floor, if it is in between the calling floor and the destination floor. If a down landing call is made while the up call is in execution, the request will not be satisfied although it is a shortest distance call. In tall buildings with even and odd floor lifts, the even floor lift takes only the even floor calls and the odd floor lift takes only the odd floor calls.

Suppose some people want to reach their office located at even floor and return in the evening after office then they need to wait for an even lift, even though the odd lift is available. They waste time in waiting for lift. In addition, there is more power consumption by lifts. If the lifts are used dynamically in the peak traffic time to transport passengers from the ground/source floor to the destination floor, then people save their time. In the morning and evening time, passengers can use both even and odd lifts to go at an even/odd floor. In the remaining time lift works as either even or odd lift. To provide solution to this problem, EGCS can be used. An EGCS has four components viz. hall call buttons, car call buttons, elevators and a group controller to control all elevators in a group.

Proposed system uses fuzzy algorithm for implementation of EGCS. Fuzzy system is a rule based problem solving control system. The system has four main blocks: Fuzzifier to accept input values, fuzzy rules to apply on data, Inference engine to perform operation and DeFuzzifier to generate output. Figure 1 shows the Fuzzy System.

Fuzzy linguistic variables are the input and output variables with non-numerical values. Let traffic flow T is Fuzzy linguistic variable. Then, the values used to

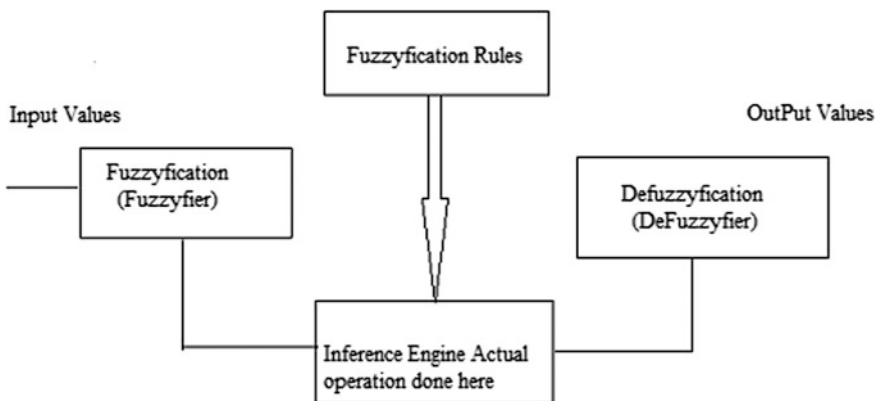


Fig. 1 A Fuzzy based system

describe this variable are either less or high or very less or very high. Traffic may be less traffic, more traffic, very high traffic or very less traffic. Fuzzy system uses membership functions in the Fuzzyfication and DeFuzzyfication steps to map the input values to the fuzzy linguistic variable or vice versa.

2 Literature Survey

Researchers have used different algorithms to schedule elevators. The algorithms are categorized as Fuzzy algorithm, Zoning based system, Artificial Intelligence, algorithms based on Neural Networks, and Genetic algorithms. The research of Jinsun, Qian-chuanzhao, and Peter B Luh uses the global process of optimization. A genetic algorithm is used by researchers for better solution [2]. Zoning based approach is referred in some studies but the approach failed to achieve dynamic based solution [3]. Neural network technique is used by Jianzhe Tai and Cheng shao, Suying yan. The system needs employee training to work efficiently. Due to lack of proper training, the system may fail to give expected output [4]. The study of M.M. Rashid focuses on floor information using fuzzy algorithms [5]. Electronic Microchips and DSP boards are used in various research works. Using microchip is cost effective and so not efficient to use. The time taken to respond a call is more due to the processing capabilities of electronic microchips.

The fuzzy approach used in existing system, does not allow dynamic dispatching of lifts. First solution for dynamic allocation of lifts is given by Cortes and Fernandez which concentrates on use of fuzzy based algorithm by assuming only one call button is available on each floor [6]. The analysis and simulation done in MATLAB using Monte-Carlo sampling helps in new research studies [1]. The study of Peter B. Luh, Bo xiong, and Shi-chungchang focuses on prediction of future traffic information and the destination entry method. Dynamic Programming is used as dispatching method in EGCS. The system works for normal operation but for heavy traffic the system needs more CPU time. Further improvement is required to improve CPU time [7]. Daniel nikovski and Matthew brand introduced a method to calculate elevators exact waiting time and to minimize the expected waiting time of passengers [3].

3 Proposed System

Figure 2 shows modular view of the system. The proposed system consists of two modules. First is Hall call module which passes calling floor Id to controller. Then controller passes control to the selected elevator. Second is Car call module which gives destination floor Id to controller and elevator moves to destination.

The Fuzzy controller applies fuzzy logic and selects elevator to serve the request. Control transfers to group of elevators, and then selected elevator goes to calling floor. Proposed Algorithm for dispatching of Elevators in EGCS works as

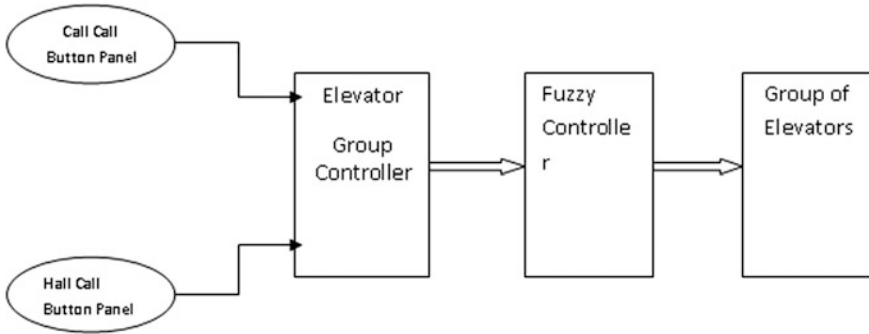


Fig. 2 Proposed system architecture

follows-First, get the system’s operational specifications, inputs and outputs. In Fuzzyfication phase: Convert input data to fuzzy set and then form inference rules with IF-THEN conditions. In DeFuzzyfication phase: Reconvert the fuzzy variables. Now choose the elevator on the basis of inference rules, pass the signal to selected elevator. Selected elevator moves towards the calling floor. Passenger enters in and presses car call button i.e. destination floor number. Send the signal to controller and finally the elevator moves towards destination floor.

Detailed Algorithm works in the following manner.

1. Let ‘S’ be the content of Elevator group control system as a final set.

$$S = \{I, O, P, F'\} \tag{1}$$

2. Identify the inputs as H and C.

$$S = \{H = \{H1, H2, H3 \dots \dots Hn \mid 'H' \text{ gives hall call signal.}\} \tag{2}$$

$$C = \{C1, C2, C3 \dots \dots Cn \mid 'C' \text{ gives car call signal.}\} \tag{3}$$

3. Identify the output as O.S = {O = {E, D}}

$$E = \{E1, E2, E3 \dots \dots En \mid 'E' \text{ gives elevator ID.}\} \tag{4}$$

$$D = \{D1, D2, D3 \dots \dots Dn \mid 'D' \text{ gives destination floor ID.}\} \tag{5}$$

4. Identify the processes as P.

$$S = \{P = \{P1, P2, P3\} \tag{6}$$

$$P1 = \{Hi, Ci \mid Hi \in H, Ci \in C \text{ where } C \cap H \neq \emptyset\} \tag{7}$$

where Hi is Hall Call, Ci is Car Call,

Success: if both calls found Failure: if either of the call not found

$$P2 = \{Hi \mid Hi \in H \text{ where } H \neq \emptyset\} \tag{8}$$

where Hi is Hall Call

Success: returns elevator ID number Failure: does not return elevator ID number

$$P3 = \{Ci \mid Ci \in C \text{ where } C \neq \emptyset\} \tag{9}$$

where Ci is Car Call

Success: set destination floor ID Failure: does not set destination floor ID

5. Identify failure cases as F'

$$S = \{\text{Failure occurs when } O = \{\Phi\} \tag{10}$$

$$I = \{p \mid p' \text{ is probability of power supply failure}\}$$

4 Results

The simulation environment consists of four parts: elevator group controller, central processing unit emulator which is used for convenience of programming and debugging, car emulator to generate hall calls and car calls and front-end of system. Eight floors and four elevators are considered in the simulation to find results. All floors are considered as a destination floor and ground floor is considered as a source floor and accordingly results are noted.

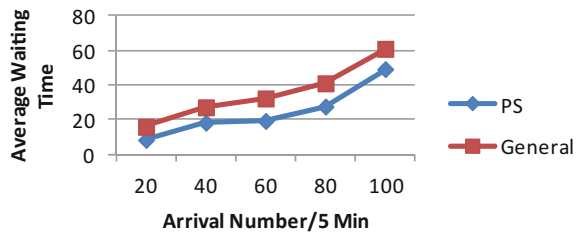
Table 1 shows the results generated by proposed system and basic EGCS for average arrival of passengers in every 5 min. Table 1 shows the Average waiting time of passengers and Average time of elevator to arrive at hall call, in seconds. Survey is conducted to identify the arrival of passengers in every 5 min and results are calculated.

From the results it has been observed that the proposed system gives optimal solution when compared with the basic system with respect to minimizing the average waiting time of passengers and elevator response time. Figure 3 gives comparison of proposed system and existing system.

Table 1 Proposed algorithm

Arrivals/5 min	Proposed algorithm		Basic EGCS Astern	
	Average waiting time (s)	Average lift time (s)	Average waiting time (s)	Average lift time (s)
20	8.53	24.20	16.12	36.22
40	18.46	26.22	27.34	47.89
60	19.47	31.22	32.46	55.28
80	27.75	36.16	41.17	63.56
100	49.32	43.17	61.04	76.34

Fig. 3 Comparison of general and proposed system



5 Conclusion

In the simulation environment, the algorithm is applied to simulate elevator group control system operation. The control strategy generation and hall call assignment part are the most important parts of the EGCS simulated by using Visual studio. Fuzzy algorithm achieves desired optimal solution for dynamic hall call assignment. Simulation results show that under the same simulation conditions, proposed control algorithm can achieve better control of the elevator group control optimization by reducing waiting time of passengers.

References

1. Lijunfu, Shenyang ligong, Tieganhao, “Analysis and simulation of passenger flow model of elevator group control system”, 9th International conference on fuzzy systems and knowledge discovery (fskd 2012), pages-2353 – 235629-(31 May 2012)
2. Jinsun, Qian-chuanzhao, Peter B Luh, “Optimization of group elevator scheduling with advance information”, IEEE transactions on automation science and engineering, vol. 7, no. 2, (April 2010)
3. Daniel nikovski and Matthew brand, “Exact calculation of expected waiting times for group elevator control”, IEEE transactions on automatic control, vol. 49, no. 10, October 2004.
4. Jianzhe tai and Cheng shao, Suying yang, “Dynamic partition of elevator group control system with destination floor guidance in up peak traffic”, China journal of computers, vol. 4, no. 1, (January 2009)

5. M.M. Rashid, Nahrul a. Rashid, md.Ataurrahman, aliasfarouq, "Design and implementation of fuzzy based controller for modern elevator group", IEEE symposium on industrial electronics and applications September 25–28, (2011)
6. J. Fernandez, P. Cortes, J. Munuzuri and J. Guadix, "Dynamic fuzzy logic elevator group control system with relative waiting time consideration", IEEE transactions on industrial electronics 2013 Volume: 61, issue 9,08 (November 2013)
7. Peter b. Luh, Bo xiong, and Shi-chungchang, "Group elevator scheduling with advance information for normal and emergency modes", IEEE transactions on automation science and engineering, vol. 5, no. 2, (April 2008)

Level Skip VLSI Architecture for 2D-Discrete Wavelet Transform

G. Kiran Maye and T. Srinivasulu

Abstract A low power and efficient 2-D Discrete Wavelet Transform architecture is proposed. Previous DWT architectures utilized flipping structures or modified lifting based schemes. In this over-lapped strip based scanning is utilized to reduce the number of clock cycles for reading the input pixels. In addition that, second level prediction and updating equations are derived directly. It is observed that the number of adders and multipliers are reduced. The hardware utilization and power consumption is decreased in order to improve the performance of the discrete wavelet transform. The execution results expose that the suggested architecture is enhanced in area competence of 1% slices, 1% of DSP 48 s, multipliers and adders are also decreased.

Keywords Discrete wavelet transform • Word length • Xilinx • FPGA • Area • Power consumption

1 Introduction

The DWT is a very computation-intensive process; the study of its hardware execution has gained much significance. For lossy and lossless compression correspondingly [1] the (9/7) and (5/3) wavelet filters are placed as the default filters. DWT is executed by employing convolution method which is based on filter bank

G. Kiran Maye (✉)

Department of ECE, Guru Nanak Institutions Technical Campus,
Ibrahimpattanam, Telangana, India
e-mail: kirangambala@gmail.com

T. Srinivasulu

Kakatiya College of Engineering, KU, Warangal, India
e-mail: drstadisetty@gmail.com

structures; however it needs large number of arithmetic computations and large storage area. The executions of one dimensional discrete wavelet transform (1-D DWT) by filter banks have been offered in [2–4]. The other method called lifting scheme that was brought in by Win Swelden in 1995 [5] to eradicate the need concerning to multiple addition along with multiplication processes that will be required with regard to convolving any filter with the image and as well it decreases the hardware difficulty. The discrete wavelet transform has turned out to be one of the most employed techniques for image coding and image compression algorithm [1, 5–9] such as the JPEG2000 standard [10, 11]. A high-level compilation tool is suggested in a new recent work [12], which produces VLSI architectures at the register transfer level [13].

The block diagram of 2-D DWT is displayed in Fig. 1. By employing one dimensional DWT on the rows and columns of the input image a 2D Discrete Wavelet Transform can be obtained. The input image is decomposed horizontally on the initial level of computation, by applying one-dimensional (DWT) with each row of getting two coefficients (L and H); consequently this is decomposed vertically by employing one-dimensional (DWT) with each column for obtaining four wavelet coefficients (LL, LH, HL and HH). For multi-level decomposition it executes the similar operation on the (LL) subband as the input.

In Fig. 2, the block diagram of lifting scheme is displayed. Lifting scheme has three steps they are split, predict and update. In split step the input is divided into odd and even samples. In predict step it calculates the high pass filter coefficient and in update step it calculates the low pass filter coefficient.

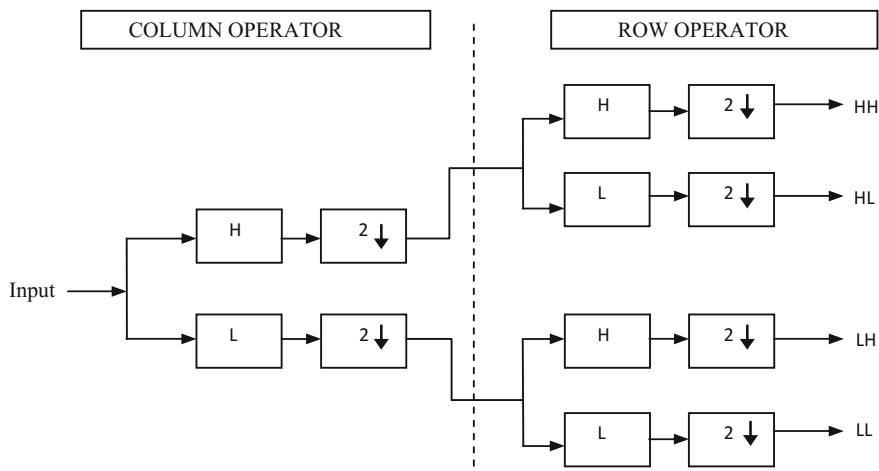


Fig. 1 Block diagram of 2-D DWT

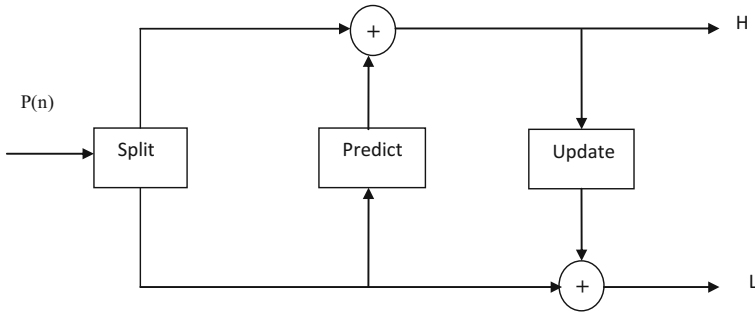
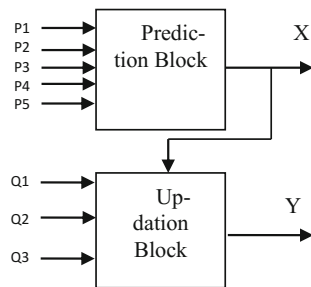


Fig. 2 Block diagram of lifting scheme for 1D-DWT

Fig. 3 Block diagram of proposed method



2 Proposed Method

In our proposed method for image compression a multilevel two dimensional discrete wavelet transform (2-D DWT) based on lifting scheme is designed for an area and memory efficient. The lifting scheme approach using the 9/7 wavelet filters reduce the hardware complexity and size of the on chip memory needed for implementation. It provides faster, easier, less demanding and more effective FPGA solutions.

The block diagram of the Level Skip 2D-DWT lifting based wavelet is specified in Fig. 3.

The architecture of the coherent 2D-DWT consists of two blocks namely prediction block and updating block. The input pixels are first fed to the prediction block to compute the high coefficients. The output from the prediction block is next fed to the up-dation block, and at the same time input pixel is also fed to the update block to calculate the lower coefficients.

The predict block needs five input pixels, namely P_1, P_2, P_3, P_4 and P_5 which is scanned through a overlapped-stripe based scanning method. While the update block needs three input pixels, namely q_1, q_2 and q_3 which is scanned through a stripe based scanning method [6]. The higher order coefficient and lower order coefficient is represented by X_i and Y_i respectively. The strip based scanning is utilized to read the three input pixel at each clock cycle and the last pixel is

overlapped for next clock cycle. The final second level prediction and updating equations are given as follows

$$X = A (P_1 + P_3) + BP_2 + CP_4 + DP_5$$
$$Y = \alpha P_1 + \beta P_2 + \gamma P_3 + dXi^2$$

The above algorithm is implemented in verilog using the following values of derived constants for a 32 bit data.

A = 9'b101111110, B = 9'b001111110,
C = 9'b101111110, D = 9'b0011111011;

Alpha = 14'b0011111101101, Beta = 14'b00111111010010,
gamma = 14'b1011111101010, del = 14'b00111111010101;

and the scaling factors

S_1 = 14'b0011111101110, S_2 = 9'b0011111110110;

3 Results and Discussions

The simulation and synthesis results for the implementation of 32-bit data are shown in Figs. 4 and 5.

The above algorithm is applied to an image, where with the help of single level lifting scheme a 2D-DWT is implemented which reduces the utilization of adders,

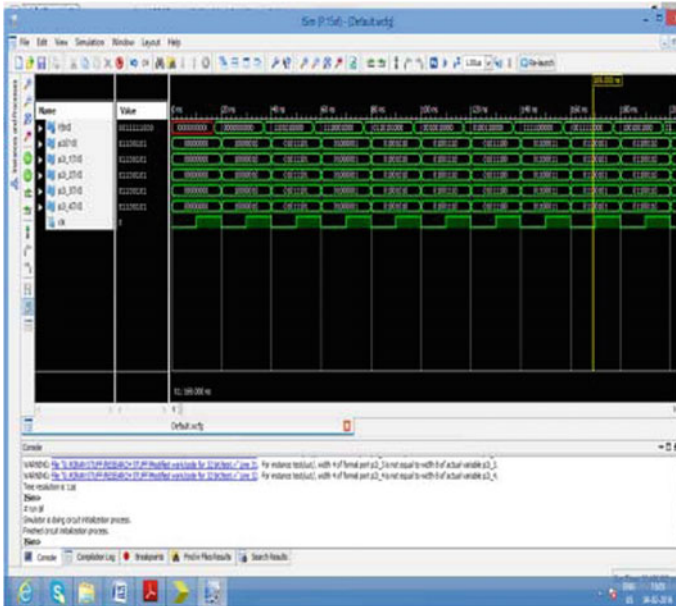


Fig. 4 Simulation results for 32-bit

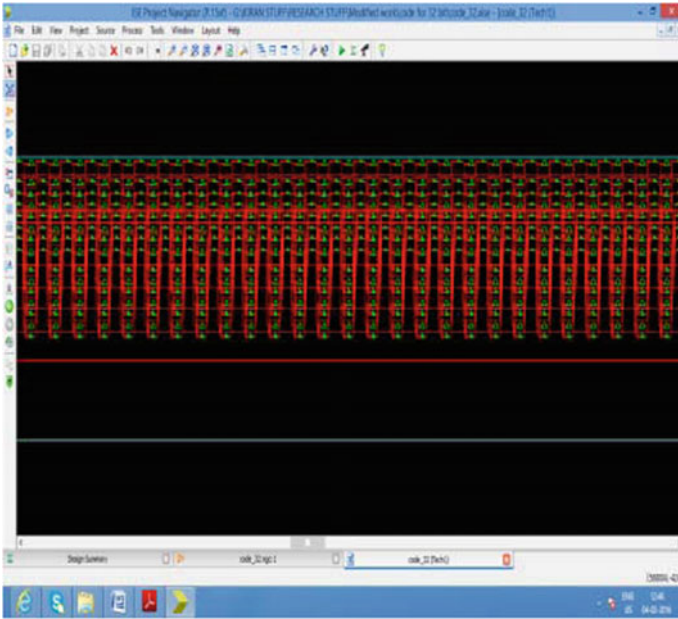
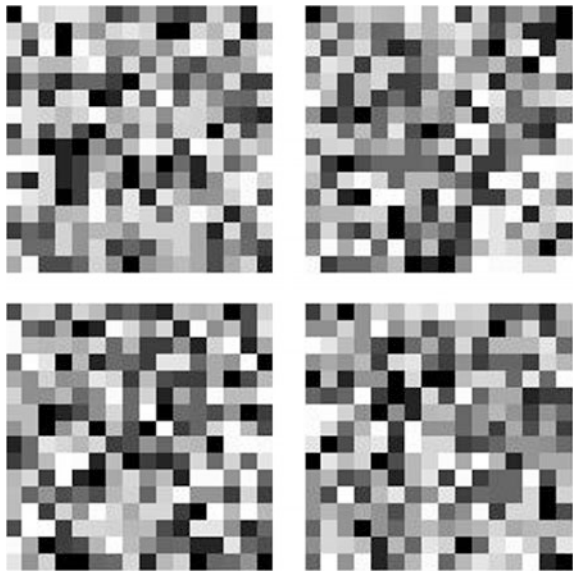


Fig. 5 Synthesis report for 32-bit

Fig. 6 2D-DWT applied to an image



multipliers and memory. The algorithm is implemented using XILINX VIRTEX 4 FPGA and targeted on an image and the result is shown in MATLAB using the following code and the result is shown in Fig. 6 (Fig. 7).

Device Utilization Summary (estimated values)			
Logic Utilization	Availed	Available	Utilization%
Number of Slices	2043	42176	4%
Number of 4 input LUTs	4080	84352	4%
Number of bonded IOBs	19	576	3%
Number of GCLKs	1	32	3%
Number of DSP48s	3	160	1%

Fig. 7 Device utilization results

Fig. 8 Xpower analyzer report For 32 × 32

On-Chip Power (W)	Used	Available	Utilization (%)
Clocks	0.006	1	---
Logic	0.000	4080	84352
Signals	0.000	5695	---
DSPs	0.000	3	160
DCMs	0.000	0	12
IOs	0.000	19	576
Leakage	0.840		
Total	0.847		

Thermal Properties	Effective TJA	Max Ambient	Junction Temp
	(C/W)	(C)	(C)
	6.0	79.9	55.1

Fig. 9 Xpower analyzer report For 32 × 32

Supply Summary		Total	Dynamic	Quiescent
Source	Voltage	Current (A)	Current (A)	Current (A)
Vccint	1.200	0.498	0.005	0.492
Vccaux	2.500	0.098	0.000	0.098
Vcco25	2.500	0.002	0.000	0.002

Supply Power (W)	Total	Dynamic	Quiescent
		0.847	0.006

The dynamic power consumption of the implemented architecture is calculated using a Xilinx Xpower analyzer. Xpower analyzer report is shown in Figs. 8 and 9 for 256 × 256 image. 0.006 W is the consumed dynamic power and the quiescent power is 0.840 W. Hence, the total power consumed in coherent DWT image fusion method is 0.847 W at 100 MHz frequency.

4 Conclusion

The Level skip lifting based 9/7 wavelet is proposed, the contribution of the method is the two level of 2D-DWT operation is made in a single level by simplification at each level. This reduced the area and power consumed to a large extent when

compared to other 2D-DWT architectures. By the use of overlapped strip based scanning for the predict and update blocks the temporary memory requirement is also reduced considerably. 0.006 W is the consumed dynamic power and the quiescent power is 0.840 W. Hence, the total power consumed in coherent DWT image fusion method is 0.847 W at 100 MHz frequency.

References

1. J.-R. Ohm, M. van der Schaar, and J. W. Woods, "Interframe wavelet coding: Motion picture representation for universal scalability", *Signal Processing: Image Communication*, Vol. 19, issue. 9, pp: 877–908, Oct. 2004.
2. A.S. Motra, P.K. Bora, and I. Chakrabarti, "An Efficient Hardware Implementation of DWT and IDWT", in *Proceedings of conference on convergent technologies for Asia-Pacific region (TENCON 2003)*, Vol. 1, pp: 95–99, Oct. 2003.
3. S. Masud, and J.V. McCanny, "Reusable Silicon IP Cores for Discrete Wavelet Transform Applications", *IEEE Transactions on Circuits and Systems-I*, Vol. 51, issue. 6, pp: 1114–1124, Jun. 2004.
4. Wei Zhang, Zhe Jiang, Zhiyu Gao and Yanyan Liu, "An Efficient VLSI Architecture for Lifting-Based Discrete Wavelet Transform", *IEEE Transactions on Circuits and Systems II*, Vol. 59, issue. 3, pp: 158–162, Feb. 2012.
5. G. Menegaz and J.-P. Thiran, "Lossy to lossless object-based coding of 3-D MRI data", *IEEE Transaction on Image Processing.*, Vol. 11, issue. 9, pp: 1053–1061, Sep. 2002.
6. J. E. Fowler and J. T. Rucker, "3-D wavelet-based compression of hyperspectral imagery", in *Hyperspectral Data Exploitation: Theory and Applications*, Chapter. 14, pp: 379–407, 2007.
7. L. R. C. Suzuki, J. R. Reid, T. J. Burns, G. B. Lamont, and S. K. Rogers, "Parallel computation of 3-D wavelets," in *Proceedings of Scalable High- Performance Computing Conference*, pp: 454–461, May 1994.
8. E. Moyano, P. Gonzalez, L. Orozco-Barbosa, F. J. Quiles, P. J. Garcia, and A. Garrido, "3-D wavelet compression by message passing on a Myrinet cluster," in *Proceedings of canadian conference on electrical and computer engineering*, Vol. 2, pp: 1005–1010, 2001.
9. Anirban Das, Anindya Hazra and Swapna Banerjee, "An Efficient Architecture for 3-D Discrete Wavelet Transform", *IEEE Transactions on circuits and systems for video technology*, Vol. 20, issue. 2, Sep. 2009.
10. David Salomon, *Data Compression: the Complete Reference*, Springer-Verlag, New York, 2nd edition, 2000.
11. Charilos. C, A. Skodras, T. Ebrahimi, "The JPEG 2000 still image coding system: an overview", *IEEE Transactions on consumer electronics*, Vol. 46, issue. 4, pp: 1103–1127, Nov.2000.
12. Bartholoma. R, Greiner. T, Kesel. F, Rosenstiel. W, "A systematic approach for synthesizing VLSI architectures of lifting-based filter banks and transforms", *IEEE Transactions on circuits and systems I*, Vol. 55, issue. 7, pp: 1939–1952, Feb. 2008.
13. Ahmed Al-Sulaifanie, Arash Ahmadi and Mark Zwolinski, "Very large scale integration architecture for integer wavelet transform", *IET Computers & Digital Techniques*, Vol. 4, issue. 6, pp: 471–483, Nov. 2010.

On the Construction and Performance of LDPC Codes

B.N. Sindhu Tejaswini, Rajendra Prasad Lal and V. Ch. Venkaiah

Abstract Low-Density-Parity-Check (LDPC) codes are excellent error correcting codes performing very close to the Shannon's limit, enabling efficient and reliable communication. Ever since their importance was known, a lot of research has gone into the construction/designing of efficient LDPC codes. Many different construction methods have been proposed so far. This paper explores some of these construction methods and includes their performance results on the Additive White Gaussian Noise (AWGN) channel. In particular, LDPC code construction using cage graphs and permutation matrices are investigated. Irregular LDPC codes have been constructed from regular LDPC codes using an expansion method, followed by their code rate comparison.

Keywords Channel coding • LDPC code • Parity-check matrix • Cage graph • Quasi-cyclic LDPC • Gray code • Code rate • SNR-BER plots

1 Introduction

Channel Coding, also called Error-Control Coding (ECC), is a mechanism of controlling errors in data transmission over unreliable communication channels [1]. The main aim of ECC is to help the receiver detect and correct errors introduced due to noise. The central idea here is that the message to be communicated is first 'encoded' by the sender, i.e. 'redundancy' is added to it to make it a codeword. This codeword is then sent through the channel and the received message is 'decoded' by the receiver into a message that resembles the original one. ECC has many

B.N. Sindhu Tejaswini (✉) · R.P. Lal · V.Ch.Venkaiah
SCIS, University of Hyderabad, Hyderabad, India
e-mail: sindhu.buddhavarapu@gmail.com

R.P. Lal
e-mail: rpls@uohyd.ernet.in

V.Ch.Venkaiah
e-mail: vvcs@uohyd.ernet.in

applications in many real-world communication systems such as in storage devices, bar codes, satellite communication, mobile networks etc. This paper is about a class of error correcting codes called LDPC codes, which are one of the best error-correcting codes today. They have gained huge importance for their practical advantages over other codes.

This paper is organised as follows. In Sect. 2, a brief explanation of LDPC codes is given. Section 3 describes the construction of LDPC codes using cubic cages, and Sect. 4 describes a method to construct regular quasi-cyclic (QC) LDPC codes. In Sect. 5, we explain the Gray code method of constructing regular LDPC codes and give a comparison of the above three methods. Section 6 has experimental results and finally, we conclude the paper in Sect. 7.

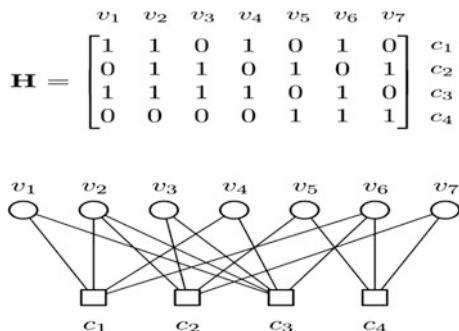
2 LDPC Codes—A Brief Overview

LDPC codes were first introduced by Gallager in 1962 [2]. They are a class of linear block codes which are defined by a sparse parity-check matrix, H . They are highly efficient and can provide performance very close to the channel capacity. They also have linear time encoding/decoding algorithms in terms of code length.

Tanner Graph. It is a graphical representation of the parity-check matrix [3]. The Tanner graph has two sets of nodes—check nodes and variable nodes, which represent the rows and columns of H respectively. See Fig. 1 as example.

The LDPC decoding algorithm is an iterative message-passing algorithm which is described on the Tanner graph. Performance of this algorithm is affected by the presence of cycles, especially short cycles, in the graph. Short cycles leave a bad effect on the decoder, as they affect the independence of the information exchanged in the decoding process, and prevent the decoder from converging to the optimum result. Hence, short cycles have to be avoided. The length of the shortest cycle in a graph is called *girth*. If the girth is large enough, then the decoder can run a good number of iterations and decode correctly before it is affected by the cycle. This is why high-girth codes should be constructed.

Fig. 1 LDPC code matrix and its tanner graph
(Source [4])



Construction. Construction of a code is the definition of the pattern of connections among the rows and columns of the H matrix [5]. The main objectives of code construction are good decoding and easier hardware implementation [5].

Performance Evaluation. In order to evaluate the reliability of a digital channel, a plot showing Signal-to-Noise-Ratio (SNR) versus Bit Error Rate (BER) values is used. The SNR-BER plot gives the BER values of the channel at different SNR values. A lower BER value indicates fewer errors and thereby, a better error correction mechanism.

We now discuss some approaches of LDPC code construction in the next few sections, which were implemented and analyzed by us.

3 Construction of Column-Weight Two Codes Based on Cubic Cages

This method [6, 7] produces regular column-weight two LDPC codes. A *regular* code has a fixed row-weight and a fixed column-weight. A (k, g) cage graph is a k -regular graph of girth g having the least possible number of vertices. A cage graph of degree 3 is called a cubic cage. Cage graphs can also be used to represent the parity-check matrix of an LDPC code. A procedure to construct cubic cages is as follows [7].

1. Take a cubic tree T (tree in which each node has a degree of 1 or 3) with t vertices in it. It has r end or leaf vertices, where $r = t/2 + 1$.
2. Make n copies of that tree $T_1, T_2, T_3, \dots, T_n$. The values t and n should be chosen carefully based on our girth requirement. Now label the vertices of the trees as $1, 2, \dots, t$ such that the first r labelling correspond to the r end vertices in each tree. Labelling should be different for odd-indexed and even-indexed trees.
3. Next, choose r random positive integers h_1, h_2, \dots, h_r where $h_i < n/2$ for $1 \leq i \leq r$. Each h -value corresponds to one end vertex of the trees i.e., h_1 corresponds to the vertices numbered as 1, h_2 corresponds to those numbered as 2 and so on.
4. Map/connect the end vertices of these n trees based to the following rule.
 - If the value of any h is x , then its corresponding vertex in the first tree is connected to that in the tree that is after $x - 1$ trees from it. Similarly, its vertex in the second tree is connected to that in the tree that is after $x - 1$ trees from it and so on.
 - Connection should be done in a cyclic manner, wherein vertices of the last trees are connected to those in the first trees based on the above same rule. The graph obtained after this procedure is the final $(3, g)$ cage graph.

As an example, see Fig. 2, wherein $t = 6$, $n = 4$, and the vertices are labelled as shown. This figure illustrates how connections are made, wherein the vertices corresponding to two h -values, h_1 and h_2 , are connected. Here, $h_1 = 1$ and $h_2 = 3$. Note that this figure is only for illustration purposes, and we do not claim that the graph shown in it is a cage graph. Also, the edges here are shown directed only for illustration.

Observation and Analysis. This method has been implemented by us and three cubic cages having girths 14, 15 and 16 respectively were constructed. To check for the possibility of obtaining higher girth cages, we tried out an experiment in which girth was calculated for all possible h -value sets. This however, did not give any higher girth. Other experiments can be carried out varying different parameters like —number of vertices in the cubic tree $T(t)$, number of copies of the tree (n) etc., which may perhaps yield higher girth cages.

4 Quasi-cyclic LDPC Codes Using Quadratic Congruences

This method [8] constructs a (j, k) regular QC-LDPC code, where j is the column-weight and k is the row-weight of the code. A quasi-cyclic code with index s is a code in which the circular shift of any codeword by s positions gives another codeword. One procedure to construct QC-LDPC is as follows.

1. Select a prime $p > 2$. Choose the desired j and k values. Now construct two sequences $\{a_0, a_1, \dots, a_{j-1}\}$ and $\{b_0, b_1, \dots, b_{k-1}\}$ whose elements are randomly selected from $GF(p)$. Note that every element in a sequence should be unique. Then form a preliminary $j \times k$ matrix Y as follows [8].

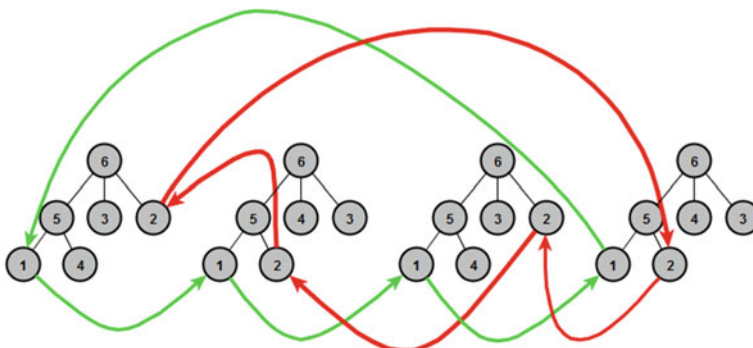


Fig. 2 Connection of trees based on two h -values ($h_1 = 1, h_2 = 3$)

$$Y = \begin{bmatrix} y_{0,0} & y_{0,1} & \dots & y_{0,k-1} \\ y_{1,0} & y_{1,1} & \dots & y_{1,k-1} \\ \vdots & \vdots & \ddots & \vdots \\ y_{j-1,0} & y_{j-1,1} & \dots & y_{j-1,k-1} \end{bmatrix}$$

where the (u, v) element of Y ($0 \leq u \leq j - 1$ and $0 \leq v \leq k - 1$) is calculated using the below equation for a fixed parameter d , $d \in \{1, 2, \dots, p - 1\}$.

$$y_{u,v} = [d(a_u + b_v)^2 + e_u + e_v] \pmod{p}$$

and $e_u, e_v \in \{0, 1, \dots, p - 1\}$.

2. Now, the parity-check matrix H can be written as [8]

$$H = \begin{bmatrix} I(y_{0,0}) & I(y_{0,1}) & \dots & I(y_{0,k-1}) \\ I(y_{1,0}) & I(y_{1,1}) & \dots & I(y_{1,k-1}) \\ \vdots & \vdots & \ddots & \vdots \\ I(y_{j-1,0}) & I(y_{j-1,1}) & \dots & I(y_{j-1,k-1}) \end{bmatrix}$$

where $I(x)$ is a $p \times p$ identity matrix whose rows are cyclically shifted to the right by x positions. The final obtained H matrix will be a $jp \times kp$ matrix. Girths of the codes constructed from this method vary depending on the choice of p, j, k, d, e_u and e_v values.

Observation and Analysis. This method has been implemented by us and regular QC-LDPC codes of various sizes were constructed. Their BER simulations were run on AWGN channel with BPSK modulation, and were compared to those of the same-sized random codes. In all cases, QC-LDPC codes had lower error rates than the random ones. See Sect. 6.1 for results.

5 Gray Code Construction of LDPC Codes

It is a simple method [9] to construct regular column-weight two LDPC codes.

1. Let H be the parity-check matrix of the code, and ρ be the required row-weight. Now let X be the decimal point set of H (a set consisting of decimal numbers, whose elements form the parity-check matrix H), having $\rho + 1$ elements in it ($X = \{X_0, X_1, \dots, X_\rho\}$), which satisfy one of the equations [9]

$$\begin{aligned} X_{i+1} &= 2X_i + 1 && \text{or} \\ X_{i+1} &= 2^i + X_i && \text{for } i = 0, 1, 2, \dots, \rho \end{aligned}$$

The first element is $X_0 = 0$ in both the cases.

2. H can now be constructed from X as follows. The elements of X form the first row of H . The subsequent rows are obtained by circularly shifting the previous row by one, until the first row repeats.
3. However, only codes with column-weight one are produced using this method. To obtain higher-weight codes, H is divided into sub-matrices as shown below. The number of sub-matrices is equal to the desired column-weight of the code.

$$\mathbf{H} = \begin{bmatrix} H_1 \\ H_2 \\ \vdots \\ H_Y \end{bmatrix}$$

H_1, H_2, \dots, H_Y are sub-matrices and Y is the desired column-weight.

4. Construction of H_1 is same as the construction of H as described above. For constructing H_2 , we fill the first row of H_1 in reverse order to form the first row of H_2 . The subsequent rows are formed by cyclically shifting the previous row by one, either to the left or right, until the first row repeats. The same construction method is used for all other sub-matrices, in which the first row of H_2 is taken in reverse order to form the first row of H_3 and so on. These sub-matrices are then appended together to form the final H (as shown above) [9].
5. Elements of H are now represented in their Gray code form to obtain the final binary H matrix of order $m \times n$. The number of bits to be used for Gray code representation is up to the designer, but must be sufficient enough to represent the largest element of H . This way, there is flexibility offered in terms of code length.

The Table 1 gives a quick comparison of the above three methods of construction.

Table 1 Comparison of LDPC construction methods discussed

Parameter	Cage graph LDPC	QC-LDPC	Gray code LDPC
Input	Cubic tree T , h -values	Prime p , required w_c and w_r , a and b sequences, e_u , e_v , d	Required w_c and w_r , and no. of bits for gray code representation
Output	Column-weight two LDPC code	Regular QC-LDPC code	Regular LDPC code
Suitability	For constructing high-girth codes, and also in cases where the channel is highly error-prone	When the encoding complexity has to be less. Also in long distance communications like NEC, and in high data rate applications	Generally suitable for simpler applications

6 Experimental Results

6.1 QC-LDPC Versus Randomly Constructed LDPC

SNR-BER simulations of two QC and random LDPC codes for 25 decoder iterations over AWGN channel are given below (Fig. 3). QC-LDPC outperformed random LDPC for all code lengths tested.

6.2 Comparing Code Rate with and Without Expansion

In many cases, irregular codes give better BER results than regular ones. But the construction of irregular codes is more complex. Instead, in order to construct an irregular code, we first construct a regular code and expand it to make it irregular. The expansion method for this is given in [10]. Here in our experiment, constructed regular codes were expanded by two levels to make them irregular. The results given in Table 2 show that expansion decreases the code rate. Lesser code rate indicates lesser message bits and higher parity bits in the codeword. This implies better protection. Hence, codes having lesser rates have better error correction ability. However, very low rate codes offer less channel throughput and are not desirable.

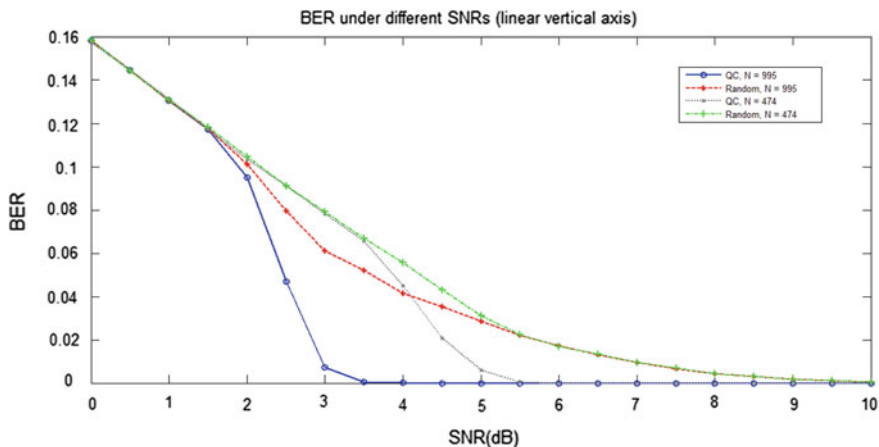


Fig. 3 237 × 474 QC versus random LDPC, and 597 × 995 QC versus random LDPC

Table 2 Comparison of code rates with and without expansion (Gray code construction method)

Row weight	Column weight	Code length (before)	Code length (after)	Code rate (before)	Code rate (after)
3	2	36	612	0.77	0.52
3	2	44	732	0.81	0.54
3	2	20	372	0.60	0.48
3	2	80	1272	0.90	0.56

7 Conclusion

This paper focused on some of the construction methods of LDPC codes and included their BER results. Comparison and suitability of these methods was briefly discussed. Any of these methods can be used to produce both regular and irregular codes (after expansion). It may be possible to obtain more efficient and higher girth codes with any of these methods on further experimentation.

References

1. Wikipedia: https://en.wikipedia.org/wiki/Error_detection_and_correction.
2. R.G. Gallager: *Low-Density Parity-Check Codes*. MIT Press, Cambridge, 1963.
3. Sarah Johnson: *Introducing Low-Density Parity-Check Codes*. v 1.1, ACoRN Spring School.
4. http://ita.ucsd.edu/wiki/index.php?title=File:Tanner_graph_example.png.
5. Gabofetswe Alafang Malema: *Low-Density Parity-Check Codes: Construction and Implementation*. The University of Adelaide, November 2007.
6. Gabofetswe Malema, Michael Liebelt: *High Girth Column-Weight-Two LDPC Codes Based on Distance Graphs*. EURASIP Journal on Wireless Communications and Networking, Volume 2007, Article ID 48158.
7. Geoffrey Exoo: *A Simple Method for Constructing Small Cubic Graphs of Girths 14, 15, and 16*. The Electronic Journal of Combinatorics 3 (1996), #R30.
8. Chun-Ming Huang, Jen-Fa Huang, Chao-Chin Yang: *Construction of Quasi-Cyclic LDPC Codes from Quadratic Congruences*. IEEE Communications Letters, Vol. 12, No. 4, April 2008.
9. Mrs. Vibha Kulkarni, Dr. K. Jaya Sankar: *Design of Structured Irregular LDPC Codes from Structured Regular LDPC Codes*. 978-1-4799-4445-3, 2015, IEEE.
10. Rakesh Sharma, Ashish Goswami: *A Robust Approach for Construction of Irregular LDPC Codes*. Proc. of the International Conference on Future Trends in Electronics and Electrical Engineering - FTEE 2013, ISBN: 978-981-07-7021-1, doi:10.3850/978-981-07-7021-1_69.

Performance Evaluation of Hysteresis Fed Sliding Mode Control of PMSBLDC Motor

M. Senthil Raja and B. Geethalakshmi

Abstract This paper presents a transient and steady state performance of PMSBLDC motor fed from current controlled voltage source inverter fed synchronous motor drive. The control algorithm is based on the estimation of firing angle from the measured currents and rotor position using Sliding mode control based Hysteresis method. Being a variable speed drive has been widely used in industries since it possess simple and better behaviour.. The BLDC motor control method containing sensors is considered. The system is simulated using MATLAB/simulink and behaviour of PMSBLDC motor is studied using Sliding mode control fed Hysteresis.

Keywords Brushless DC motor • Voltage source inverter • Hysteresis • Sliding mode control • Speed • Torque

1 Introduction

(BLDC) motors are synchronous motors in which magnetic field of stator and rotor rotate at same frequency without slip. It possess single, two and three phase. Hall effect sensors are used for finding the position of the rotor. Rotor pole of Hall effect sensor possess either North or South pole. The commutation sequence can be positive, negative or without both of them. Since the motor is without brushes, less maintenance is an advantage. Flat makes the speed and torque control better in BLDC and it also makes BLDC to operate at all speeds. Power is high due to reduced noise and thermal properties. Since the windings on the stator are connected to the case, it makes heat winding wastage better. Inertia is very less since the rotor possess permanent magnets and low noise. Speed and cost building are

M. Senthil Raja (✉) • B. Geethalakshmi
Pondicherry Engineering College, Pondicherry 605014, India
e-mail: senthilraja391@gmail.com

B. Geethalakshmi
e-mail: lakshmigeetha972@gmail.com

generally high. The control is presently little bit complicated. It is used for variable speed control. There is no slip between stator and rotor frequencies (Fig. 1).

2 Sliding Mode Control Based Hysteresis

The performance of sliding mode-Hysteresis control has been evaluated. PI controller controls speed error and then it was tested for load torque disturbance of 10–75% load conditions. The results prove load torque increasing with steady state error and speed increase with settling time. The load torque gets decreased then the system is unstable. It is concluded that performance of the SMC based is much better (Fig. 2).

3 Simulation

See Figs. 3 and 4.

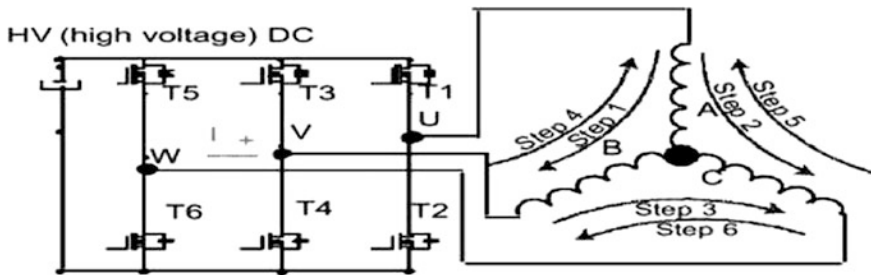


Fig. 1 BLDC motor

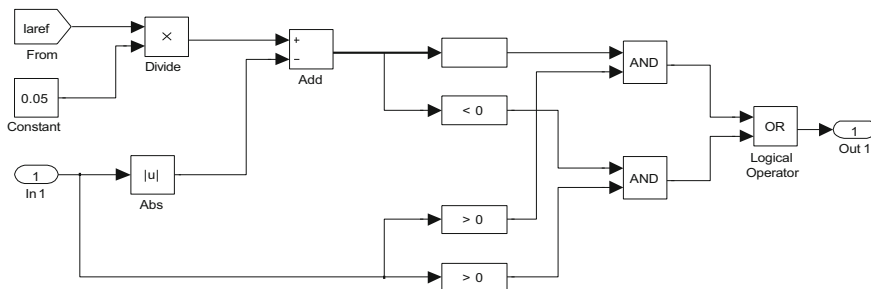


Fig. 2 Hysteresis control

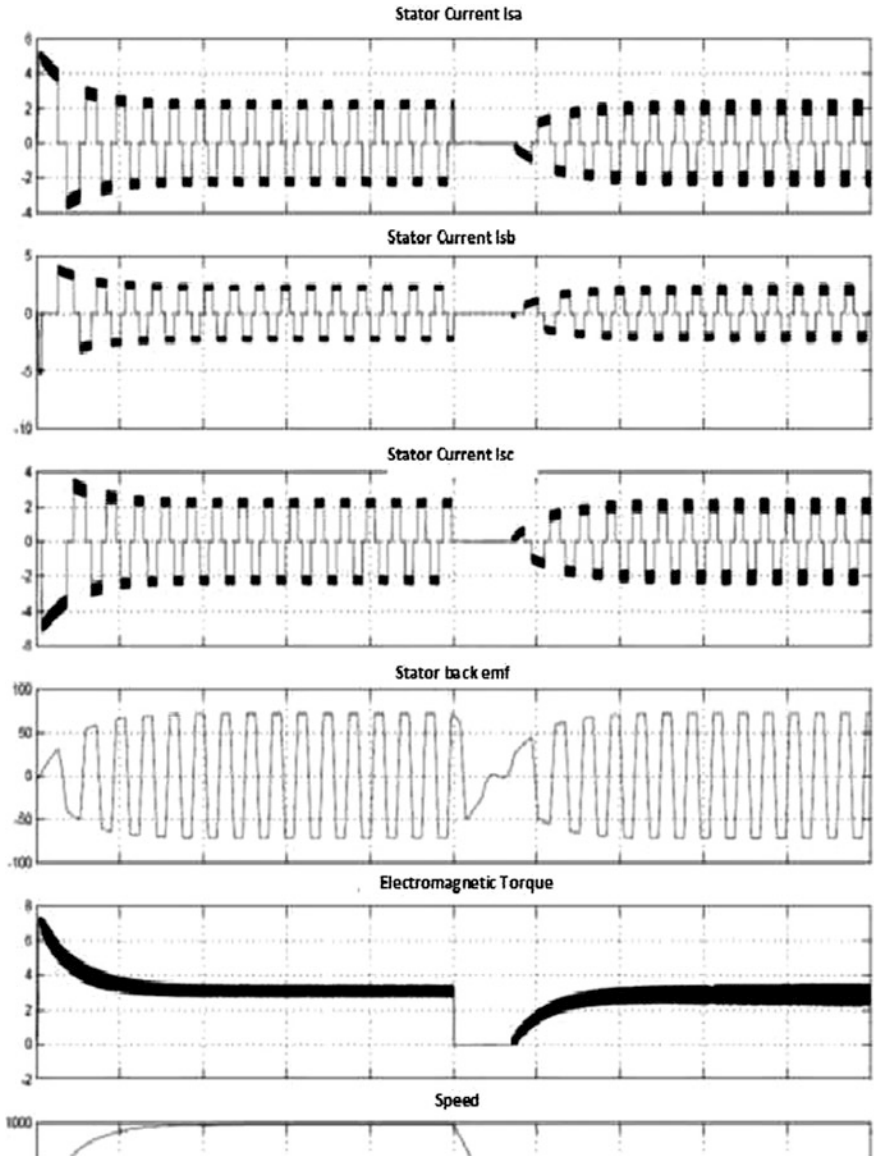


Fig. 3 Change in load

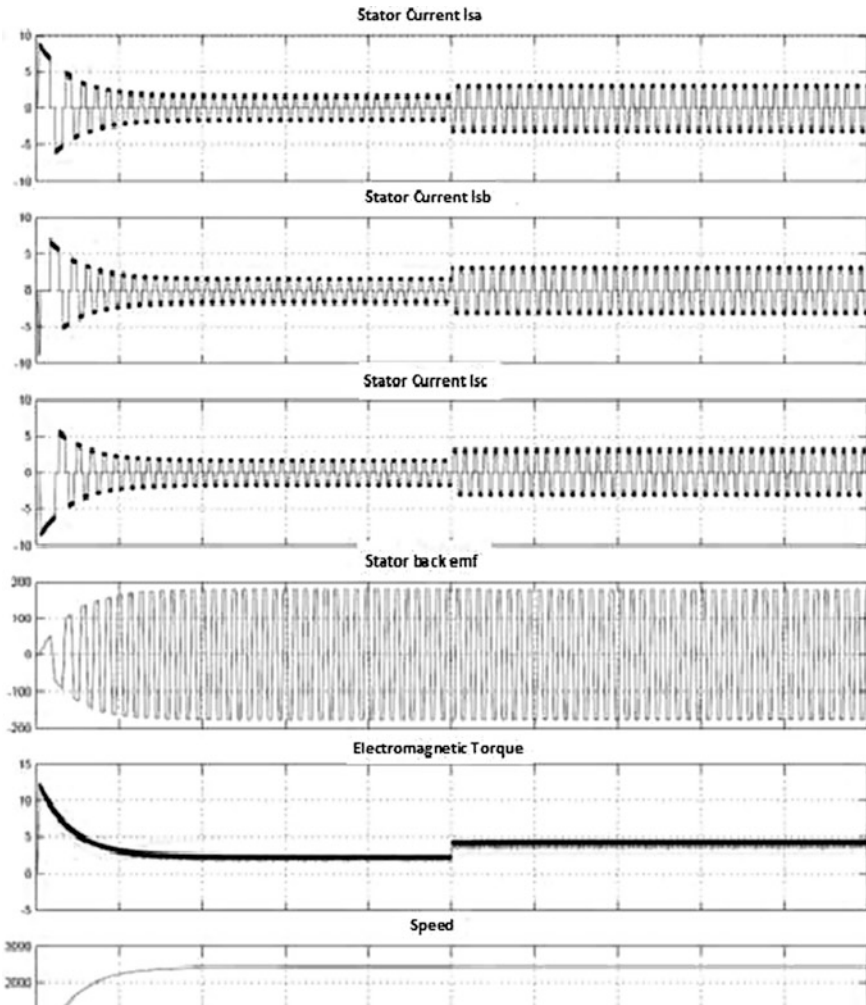


Fig. 4 During speed reversal

4 Conclusion

In this paper the behaviour of 3 phase PMBLDC current controlled VSC is studied using Hysteresis fed sliding mode control under different load condition. The system is simulated in Matlab/Simulink. The results are evaluated under load change and speed reversal condition thereby predicting the behaviour of PMBLDC.

References

1. Jessen Chen and Pei-Chong Tang, "A Sliding Mode Current Control Scheme for PWM Brushless DC motor Drives", *IEEE transactions on Power Electronics*, May 1999.
2. Utkin V.I, "Sliding mode control design principles and applications to electric drives", Industrial electronics, *IEEE transactions*, 1993.
3. E. A. Klingshirn, "High Phase Order Induction Motors, Part II – Experimental Results," *IEEE Trans., Power App. Syst.*, vol. PAS-102, pp. 54–59, Jan. 1983.
4. T. M. Jahns, "Improved Reliability in Solid-state AC Drives by Means of Multiple Independent Phase Driven Units," *IEEE Trans. Ind. Applicat.*, vol. IA-16, pp. 321–331, May/June 1980.
5. D. M. Erdman, H. B. Harms, J.L. Oldenkamp, "Electronically Commutated DC Motors for the Appliance Industry," *Conf. Rec. 1984 IEEE Ind. Applicat. Soc. Ann. Mtg.*, pp. 1339–1345.
6. M. Lajoie-Mazenc, C. Villanueva, J. Hector, "Study and Implementation of Hysteresis Controlled Inverter on a Permanent Magnet Synchronous Machine," *Conf. Rec. 1984 IEEE Ind. Applicat. Soc. Ann. Mtg.*, pp. 426–430.
7. Kusko, S. M. Peeran, "Brushless DC Motors Using Unsymmetrical Field Magnetization," *Conf. Rec. 1986 IEEE Ind. Applicat. Soc. Ann. Mtg.*, pp. 774–780.
8. V. Murty, "Fast Response Reversible Brushless DC Drive with Regenerative Breaking," *Conf. Rec. 1984 IEEE Ind. Applicat. Soc. Ann. Mtg.*, pp. 445–450.

A Selective Data on Performance Feature with Selective Algorithms

M. Bharat, Konda Raveendra, Y. Ravi Kumar and K. Santhi Sree

Abstract Now a days, there is rapid development in Computer Science and Engineering Technology as well as data has been increasing wildly and it is a major problem for users to quickly find the most relevant (or useful) information or data from large amount of data being stored in databases. To solve this problem so many researchers are found that the feature selection algorithms (or methods) are best methods to identify useful data (or information) from large amount of data present in databases. Feature Selection algorithm is useful in identifying (or selecting) most useful information from the entire large original set of features to improve accuracy. Feature Selection specifies a task that selects a subset of features and those are useful to solve domain problems. There are several important algorithms (or methods) available for selecting the relevant features from large set of features to improve accuracy of the results. This paper explains performance of various feature selection algorithms to find most relevant features from the entire set of features.

Keywords Feature selection · Performance of feature selection · Data mining · Relief

M. Bharat (✉) · K. Raveendra · Y. Ravi Kumar
Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad, India
e-mail: bharat870@gmail.com

K. Raveendra
e-mail: raveendrakk.csegnitc@gniindia.org

Y. Ravi Kumar
e-mail: Ravikumar.yeetha@gmail.com

K. Santhi Sree
Department of CSE, Jawaharlal Nehru Technological University Hyderabad,
Hyderabad, India
e-mail: kakara_2006@jntuh.ac.in

1 Introduction

The rapid development of Computer Science and Engineering Technology, the e-data (or information) is increasing rapidly. It is a major problem that, how quickly we can select most useful information (or data) from very large amount of data in databases. To solve this problem we used the technologies like data mining and information retrieval systems.

Feature Selection is the process of finding most useful information (or data or features) from the large amount of data that is stored in databases. The main goal of the feature selection is to improve the accuracy of the classification. The feature selection algorithms (or methods) become more popular in applications like datasets with thousands of features (or variables) are available. The datasets are includes text, bio microarray and image data. For high dimensional data feature selection algorithm improves both accuracy and classification of the very large data like thousands of features that consist of large number of irrelevant features and redundant features.

The main objective of feature selection algorithms is involves identifying and removing the most irrelevant features and redundant features. Because, irrelevant features do not contribute to the accuracy of the classification and redundant features, most of the information contains one feature which is already available in other features.

The feature selection algorithm is broadly categorized into four groups. They are filter, wrapper, embedded and hybrid methods. The first approach (or method) is filter method and it uses statistical properties of the features to filter the irrelevant features and the redundant features. This method is independent of learning methods (or algorithms) and computational complexity is very low and the accuracy of learning the algorithms is not guaranteed. The second method is wrapper methods, it provides the accuracy of learning methods (or algorithms) is high but computational complexity is very large. The third method is embedded methods; the examples of this method are artificial neural networks and decision tree. The fourth and final method is hybrid method it is a combination of both filter and wrapper methods. It achieves best performance with learning algorithms (or methods) as well as time complexity is very low.

The paper as mentioned, in Sect. 2 we briefly discussed about various feature subset selection algorithms, in Sect. 3 we compare and analyze of feature selection algorithms and in Sect. 4 conclusion has concluded as followed by references.

2 Feature Selection Algorithms

2.1 *Fast Clustering Based Feature Subset*

Selection Algorithm (FAST): The fast clustering is based on feature subset selection algorithm (FAST) is involves to identifying and removing the irrelevant

features and the redundant features from high dimensional data. The fast clustering based feature subset selection algorithm (FAST) works in two steps: (i) in first step, the features are divided into clusters by using prim's algorithms (that is graph-based clustering methods) and (ii) in second step, the most selective and representative features are selected from each clusters to form the most useful subset to improve the accuracy of classification. The fast clustering feature subset selection algorithm (FAST) performs very well on text, micro array and image data.

2.2 Relief Algorithm

Relief is proposed by Kenji Kira and Larry A. Rendell in 1992 [1]. Relief is a feature selection algorithm which finding (or selecting) relevant feature using a statistical method and it is not depending on the heuristic method. Relief algorithms also used in binary classification that is (classification by decomposition into a number of binary problems). The advantages of Relief algorithms are that it requires only linear time in training instances and the number of given features, Relief algorithm is noise-tolerant and robust to feature interactions.

2.3 Correlation Based Feature Selection

Algorithm (CFS): Correlation Based Feature Selection Algorithms (CFS) is finding features according to the degree of redundancy among the entire set of features. The Correlation Based Feature Selection Algorithms (CFS) aims to find the most useful subsets of features that are individually highly correlated with the target class but have low inter-correlation. Correlation Based Feature Selection Algorithms (CFS) calculates the measure feature-class and feature-feature correlations using symmetrical uncertainty and then finding most useful subset of features by using best first search. The advantages of Correlation Based Feature Selection Algorithms (CFS) are it not required to reserve any part of the training data (or features) for classification purpose and it works well on smaller datasets also. Correlation Based Feature Selection Algorithms (CFS) selects maximum most relevant features and removes redundant features. But the drawback of Correlation Based Feature Selection Algorithms (CFS) is it cannot handle datasets where the target class is numeric.

2.4 Fast Correlation Based Feature

Selection Algorithm (FCBF): The Fast Correlation Based Feature Selection (FCBF) algorithm consists of two steps: (i) in first step is a relevance analysis, the aim of this step is ordering the input variables (or features) depending on a

relevance value which is computed based on the symmetric uncertainty with respect to the target class. This step is also called removal of irrelevant features (or variables), which are those whose relevance value (or relevance score) is below a predefined threshold and (ii) in the second step is a redundancy analysis, the aim of this step is removing of redundancy features. The Fast Correlation Based Feature Selection (FCBF) algorithm uses also the symmetrical uncertainty measure, but the search algorithm (of features) is very different.

2.5 Reinforcement Learning Algorithm

The reinforcement learning algorithm used to identifying and selecting most useful relevant features related target class (or related problem) in reinforcement learning environment only. It is very difficult to using data mining techniques in reinforcement learning environments is due to the lack of datasets in a database. Feature and action selection is very important for reinforcement learning algorithms. The feature (or action) selection was not capable of improving the performance of the algorithm but it reduces the memory consumption.

2.6 The Stream Relief Algorithm

The Stream Relief Algorithm very useful in situations like where we need to distinguish stream sources by looking at the feature (or data). The Stream Relief Algorithm generates a training datasets at each time and it also apples feature mapping functions on streams for each time. The Stream Relief Algorithm takes the weight of each feature at each time and it also calculates the cost associated with each feature and it returns the ordered list of features. The Stream Relief Algorithm orders all the features with score that classification relevance and combines both cost estimation. The features having higher weights (or score) are more effective in classification. The Stream Relief Algorithm minimization the cost associated with classification and but it cannot give the accuracy of the classification within a time.

2.7 The Information Gain and Genetic

Algorithm: The Information Gain and Genetic Algorithm finding the features by using the idea of computation of evolutionary. The Information Gain and Genetic Algorithm use information gain based on the frequency of item to selecting the

most optimal (or most useful) features subset. The Information Gain and Genetic Algorithm improve the characteristics of weight vector and text similarity dimensions based on fitness of the function.

2.8 Las Vegas Filter Algorithm (LVF)

The Las Vegas Filter Algorithm (LVF) is used for feature selection. It considers the datasets with n features and repeatedly generates feature subsets randomly and computes evolution measure of random generates features. The Las Vegas Filter Algorithm (LVF) is implementation is very simple and getting the results is very fast. The drawback of The Las Vegas Filter Algorithm (LVF) is it is applicable only discrete features.

2.9 Hybrid Feature Selection Algorithm (HFS)

Hybrid Feature Selection Algorithm (HFS) uses both filter and wrapper methods for feature subset selection. Hybrid Feature Selection Algorithm (HFS) focuses on selecting most useful sub-feature set in which the selected features relevant in order to get good classification performance.

2.10 Sequential Floating Forward Search

Algorithm (SFFS): Sequential Floating Forward Search (SFFS) is a floating point (an exponential) cost algorithm that performs in a sequential manner. In each selection step the Sequential Floating Forward Search (SFFS) perform a forward step followed by backward step (a variable number (possibly null)). If a feature is added unconditionally then that features are removed as long as the generated subsets.

2.11 Threshold Based Feature Selection

Algorithm (TBFS): Threshold Based Feature Selection Algorithm (TBFS) working based on the Threshold formula with combination of other methods. Threshold Based Feature Selection Algorithm (TBFS) is very suitable for Gene micro array analysis. Threshold Based Feature Selection Algorithm (TBFS) have better performance for smaller subset of features (or attributes).

3 Analysis

Algorithm	Advantages	Limitations
FAST (Fast Clustering Based Feature Subset Selection)	<ul style="list-style-type: none"> • Uses symmetric uncertainty measure 	For Image data its does not perform to CFS
	<ul style="list-style-type: none"> • It Performs well on high dimensional dataset 	
CFS (Correlation Based Feature Selection)	<ul style="list-style-type: none"> • It works well on datasets with small size • It avoids the redundancy feature re-introduction 	<ul style="list-style-type: none"> • It cannot handle the datasets with target class is numeric
FCBF (Fast correlation Based Feature Selection)	<ul style="list-style-type: none"> • Uncertainty to measure the relevance between the feature-class and feature-feature 	Feature is very different
Relief	<ul style="list-style-type: none"> • Noise tolerant and robust to feature interactions • Is accurate even feature is interact 	Non optimal feature set size
Reinforcement Learning	<ul style="list-style-type: none"> • It reduces the consumption of memory. (i.e., Memory Consumption0) 	It is not improving performance of selection algorithm
The Stream Relief	<ul style="list-style-type: none"> • The computation cost is very low compare to other algorithms 	It cannot give the accuracy and the classification with in time
The Information Gain and Genetic Algorithm	<ul style="list-style-type: none"> • Improves the characteristics of weight vector and text similarity dimensions based on fitness of the function 	Improves the accuracy of classification only when the system has large extent
Las Vegas Filter	Implementation is very simple and very fast to find the results	It is applicable only for discrete datasets
Hybrid Feature Selection	It gets the better classification results	The computation cost is very high for high dimensional datasets
Sequential Floating Forward Search	It performs both forward and backward steps	It gives results for specified size only
Threshold Based Feature Selection	It is suitable for gene micro array analysis	It gives better performance with small size of datasets only

As per the analysis of various feature selection algorithms, The FAST algorithm performs very well on high dimensional datasets and accuracy is also very high with in less time.

4 Conclusion

In this paper, we briefly explained and analyzed various feature subset selection algorithms and explained the advantages and limitations of each and every algorithm.

References

1. Artificial Intelligence Foundations Theory and Algorithms, 2015.
2. Naidu, Kajal, Aparna Dhenge, and Kapil Wankhade. "Feature Selection Algorithm for Improving the Performance of Classification: A Survey", 2014 Fourth International Conference on Communication Systems and Network Technologies, 2014.
3. Zhang Yu; Yu Gang; Guan Yongsheng and Yang Donghui. "Feature Selection of Nonperforming Loans in Chinese Commercial Banks", International Journal of U- & EService, Science & Technology, 2015.
4. Chin, Ang, Andri Mirzal, Habibollah Haron, and Haza Hamed. "Supervised, Unsupervised and Semisupervised Feature selection: A Review on Gene Selection", IEEE/ACM Transactions on Computational Biology and Bioinformatics, 2015.
5. Sharma, Poonam, Abhisek Mathur, and Sushil Chaturvedi. "An improved fast clustering-based feature subset selection algorithm for multi featured dataset", 2014 International Conference on Advances in Engineering & Technology Research (ICAETR - 2014), 2014.
6. Nemade, Rachana T., and Richa Makhijani. "Unsupervised feature selection for linked data", International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), 2014.
7. Wang, Guangtao, Qinbao Song, Baowen Xu, and Yuming Zhou. "Selecting feature subset for high dimensional data via the propositional FOIL rules", Pattern Recognition, 2013.
8. Khalid, Samina, Tehmina Khalil, and Shamila Nasreen. "A survey of feature selection and feature extraction techniques in machine learning", 2014 Science and Information Conference, 2014.
9. Shang Lei. "A Feature Selection Method Based on Information Gain and Genetic Algorithm", 2012 International Conference on Computer Science and Electronics Engineering, 03/2012.
10. Zhao, Zhou, Xiaofei He, Lijun Zhang, Wilfred Ng, and Yueting Zhuang. "Graph Regularized Feature Selection with Data Reconstruction", IEEE Transactions on Knowledge and Data Engineering, 2015.
11. de L. Vieira, Davi C., Paulo J. L. Adeodato, and Paulo M. Goncalves. "Improving reinforcement learning algorithms by the use of data mining techniques for feature and action selection", 2010 IEEE International Conference on Systems Man and Cybernetics, 2010.
12. "A Lexicographic Multi-Objective Genetic Algorithm for Multi-Label Correlation Based Feature Selection", Proceedings of the Companion Publication of the 2015 on Genetic and Evolutionary Computation Conference GECCO Companion 15, 2015.

Author Index

A

Aggarwal, Akshima, 97
Akashdeep, 143, 151, 277, 307
Akkalakshmi, M., 233
Akriti, 39
Ambawade, Dayanand, 205
Anand Chandulal, J., 225
Aruna Rao, S.L., 177

B

Bade, Vandana Laxman, 193
Bakal, J.W., 205, 287
Balasundaram, Keerthi, 121
Bharat, M., 369
Bhardwaj, Avi, 29
Bhatia, Gresha S., 287
Bhatia, Madhulika, 39, 333
Bhavani, Y., 253
Bindu Tushara, D., 245

C

Chandra Prakash, V., 339
Chhabra, Amit, 97
Chorage, Suvama S., 193

D

Damodaram, A., 233
Dhir, Saru, 29

G

Ganesh, D., 159
Garg, Anchal, 333
Garg, Kanika, 89
Geethalakshmi, B., 363
Guda, Vanitha, 51

H

Harsha Vardhini, P.A., 245
Havisha, V., 113

Hooda, Madhurima, 39

I

Iyengar, Akash, 325

J

Jagli, Dhanamma, 73
Jain, Yakshita, 297
Janaki, V., 253, 313
Juneja, Mamta, 167, 297

K

Kaur, Kamaljit, 1, 81
Kaur, Mohanjeet, 167
Kaur, Parneet, 1
Kaur, Sumandeep, 81
Kedar, Pravin Manohar, 205
Kiran Maye, G., 347
Kumar, Aditi, 333
Kumar, Neeraj, 39

L

Lal, Rajendra Prasad, 185, 355
Leelavathy, N., 105

M

Madhurima, 333
Marwha, Dhruv, 325

N

Nagaraju, A., 313
Narayana, G., 233
Nautiyal, Anand, 185
Neeraj, 277

P

Pabboju, Suresh, 15
Padmavathi, P.V., 113
Paltani, Surbhi, 29

Pandey, Madhulika, 39
 Pullabhotla, Varsha, 9
 Purohit, Seema, 73

R

Rama Prasad, V.V., 159
 Ramadevi, Y., 217
 Ramanamurthy, S.V., 113
 Ravali, Sambu, 265
 Raveendra, Konda, 369
 Ravi Kumar, Y., 369
 Ravinder Reddy, R., 217
 Reddy, B. Raja Srinivasa, 131
 Revathy, P., 121
 Rishitha, D.S.M., 105

S

Sainath, N., 63
 Sale, Malan D., 339
 Sanampudi, Suresh Kumar, 51
 Santhi Sree, K., 369
 Senthil Raja, M., 363
 Sharmila, K., 313
 Shravani Sagar, Thadisetty, 265
 Sindhu Tejaswini, B.N., 355
 Singh, Bhaludra R. Nadh, 131

Singh, Jaiteg, 89
 Singh, Sumit, 325
 Sridevi, R., 253
 Srinivasan, Madhan Kumar, 121
 Srinivasa Rao, M., 225
 Srinivas Reddy, P., 63
 Srinivasulu, T., 347
 Subash Chandra, N., 73
 Sugamya, Katta, 15, 265
 Sunil Kumar, M., 159
 Sunitha, K.V.N., 177, 217
 Supreethi, K.P., 9
 Sushmitha, M., 105
 Swathi, Kothapalli, 265

U

Uma Mahesh, J., 63

V

Venkaiah, V. Ch., 355
 Vijay Kumar, G., 63
 Vinaya Babu, A., 15

Y

Yedukondalu, G., 225