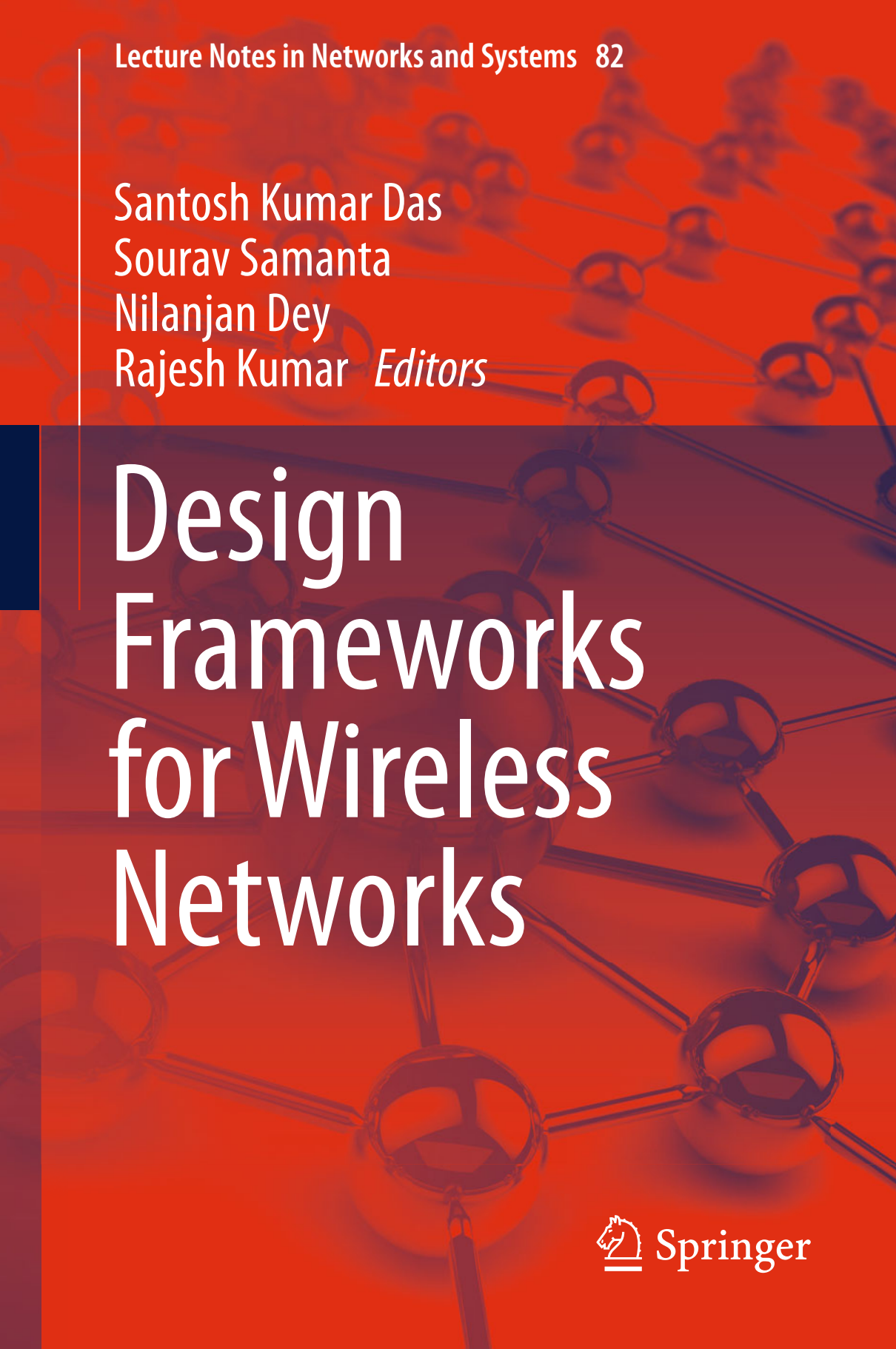
Lecture Notes in Networks and Systems 82

Santosh Kumar Das
Sourav Samanta
Nilanjan Dey
Rajesh Kumar *Editors*

Design Frameworks for Wireless Networks



Springer

Lecture Notes in Networks and Systems

Volume 82

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

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

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

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

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

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

Santosh Kumar Das · Sourav Samanta ·
Nilanjan Dey · Rajesh Kumar
Editors

Design Frameworks for Wireless Networks

Springer

Editors
Santosh Kumar Das
School of Computer Science
and Engineering
National Institute of Science
and Technology (Autonomous)
Brahmapur, Odisha, India

Sourav Samanta
Department of Computer Science
and Engineering, University Institute
of Technology
University of Burdwan
Bardhaman, West Bengal, India

Nilanjan Dey
Department of Information Technology
Techno India College of Technology
Kolkata, West Bengal, India

Rajesh Kumar
Department of Electrical Engineering
Malaviya National Institute of Technology
Jaipur, Rajasthan, India

ISSN 2367-3370 ISSN 2367-3389 (electronic)
Lecture Notes in Networks and Systems
ISBN 978-981-13-9573-4 ISBN 978-981-13-9574-1 (eBook)
https://doi.org/10.1007/978-981-13-9574-1

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

Foreword

I am delighted to write the foreword for the first edition of the book *Design Frameworks for Wireless Networks* on the eve of 5G network implementation around the world. The global economy is making groundings for 5G technology for society. Wireless network revolution is bringing essential alterations to data communication and networking for developing integrated heterogeneous networks (HetNet). Freeing the user from the cable network, it provides personal networks, wireless LAN, mobile cellular systems, distributed computing, and communications at anytime and anywhere. The framework of wireless network for Industry 4.0-based interoperability performs seamless connections of cyber-physical systems, crowd and smart device connectivity using IoT.

Focusing on the user aspects, wireless networks provide crowdsensing and crowdsourced network. Privacy-preserving incentive mechanism in mobile crowdsensing makes wireless network self-organized and sustainable. Blockchain-based decentralized wireless network is providing concessions and trust-based architecture. Software-defined wireless network architecture supports application-aware service provisioning in IoT. The application, infrastructure, and control layers enable software-defined networking (SDN). Device management facilitates the users to control their devices in the network. Software-defined wireless network helps in adapting real time to transactions in dynamic cyber-physical environment. The father of mobile communication, Martin Cooper, formulated the Law of Spectral Efficiency, known as Cooper's Law. "The law states that the maximum number of voice conversations or equivalent data transactions that can be conducted in all of the useful radio spectrum over a given area doubles every 30 months."

Satellite-based wireless network uses C band (6/4 GHz), Ku band (14/11 GHz), and Ka band (30/27 GHz) for television industries. Nowadays, IPTV and VoIP become essential for mobile network. Bandwidth designers use millimeter-wave frequencies for small antenna apertures and atmospheric low attenuation of rain.

Higher frequency wireless network in-between 100 GHz and 1 THz where, tiny wavelength makes these frequencies suitable for high-resolution positioning and imaging. The applications are short-range networking, vehicular networks, and drone-to-drone connectivity.

The major challenges are wireless network protocol design, low-latency communications, specification design and implementation, and performance evaluation of protocols. In wireless network context, hybrid transmission technologies are essential elements. Network themes' challenges are cross-layer design, planning and control, services, operations management, survivability, reliability, virtualization, network programmability, measurement and modeling, pricing economics, and implementation of efficient routing protocol.

Design of automation and troubleshooting techniques are essential for self-organized wireless network. IoT plays a major role in system integration and automation. IoT algorithms enable software and hardware connectivity and enormous scale interoperability to mitigate heterogeneity.

Optimization-based network lifetime enhancement techniques and algorithms are essential for wireless network design point of view. The aim is to exploit tolerance for uncertainty to achieve tractability and robustness at little cost. In wireless network application, convergence of the areas of fuzzy, rough, and nature-inspired techniques are used to address the real-world complexities of wireless network. The design of ambient intelligence system using pervasive, ubiquitous, and cognitive wireless network is a major challenge. Wireless multimedia systems' tools are developed using virtual reality and augmented reality.

Security, privacy, and trust are the major challenges of wireless domain. Service and semantic computing; dependable, reliable, and autonomic computing; smart agents; context awareness; multimodal intelligent wireless services; and secure wearable health sensors and actuators are the emerging areas.

The strategy of sensing and aggregation technique are the progresses of multi-sensor information fusion to provide the synergism. The major challenges of wireless information fusion are multilevel wireless fusion, multi-classifier, multi-source fusion system, real-time self-improving fusion system architectures, and distributed wireless sensor system deployment.

The book *Design Frameworks for Wireless Networks* edited by Santosh Kumar Das, Sourav Samanta, Nilanjan Dey, and Rajesh Kumar illustrates the complex wireless network issues in a user-friendly manner. This book has four major parts—Part "Design and Enhancement of Security and Privacy Technique"; Part "Design of Automation and Troubleshooting Technique"; Part "Design of Optimization Based Network Lifetime Enhancement Technique"; and Part "Design and Implementation of Efficient Routing Protocol". The implementation of traffic priority-aware medium access control protocol for wireless body area networks is discussed in detail. I strongly recommend this precious book written by renowned

researchers for the students, faculty members, and scientists working in the field of wireless network. It is my hope and expectation that this book will provide an effective learning experience and referenced resource for all networking people.

Dr. Debashis De
Director, School of Computational Sciences
Professor, Department of Computer Science and Engineering
Senior Member IEEE, Associate Editor, IEEE ACCESS
Maulana Abul Kalam Azad University of Technology
(Formerly, West Bengal University of Technology)
Kolkata, West Bengal, India

Preface

In the last few decades, the applications of wireless network increase rapidly due to several features over wired network such as frequent mobility, minimum cost, and dynamic and fast communication. These features avoid two constraints of wired network like installation and maintenance of numerous pieces of software and hardware. There are several variations of wireless network such as wireless sensor network (WSN), wireless body area network (WBAN), mobile ad hoc network (MANET), wireless ad hoc network (WANET), vehicular ad hoc network (VANET), software-defined network (SDN), and software-defined ad hoc network (SDANET). Each variation has some challenges in terms of certain factors such as cost, coverage, dependability, range, reliability, scalability, security, and speed. It causes several types of uncertainties and imprecise information. Hence, there is a need to design some novel or innovative ideas in the design frameworks of the above-mentioned wireless networks. Therefore, it has been assumed in larger awareness in academicians, researchers, computer professionals, industry people, and valued users.

Objective of the Book

This book contains the design frameworks of wireless network. It basically deals with the design, implementation, and enhancement of different variations of wireless network. The main aim of this book is to initiate huge modernization in the framework, designing algorithms of wireless network. It is edited for academicians, researchers, computer professionals, industry people, and valued users.

Organization of the Book

This book contains 18 chapters that are organized into four parts as follows. **Part "Design and Enhancement of Security and Privacy Technique"** contains five chapters that outline the design and enhancement of security and privacy techniques. **Part "Design of Automation and Troubleshooting Technique"** contains five chapters that highlight the design of automation and troubleshooting techniques. **Part "Design of Optimization Based Network Lifetime Enhancement Technique"** contains five chapters that illustrate the design of optimization-based network lifetime enhancement techniques. **Part "Design and Implementation of Efficient Routing Protocol"** contains three chapters that demonstrate the design and implementation of efficient routing protocols.

Part "Design and Enhancement of Security and Privacy Technique" (Chapters "An Analysis and Comparison of Security Protocols on Wireless Sensor Networks (WSN)"–"Deep Learning and Machine Learning Techniques for Intrusion Detection and Prevention in Wireless Sensor Networks: Comparative Study and Performance Analysis")
This part outlines the different security and privacy mechanisms of wireless network. These mechanisms are illustrated in terms of Internet of things (IoT), E-health care, supervisory control, data acquisition, and intrusion detection and prevention. The short descriptions of these chapters are given as follows.

Chapter "An Analysis and Comparison of Security Protocols on Wireless Sensor Networks (WSN)"
This chapter mainly concentrates on security issues and security requirements. Moreover, it also analyzes and discusses some key management protocols for the secure transmission of data and compares them on the basis of performance. This work has provided a detailed description of the WSN-related information to extremely understand the concept of the network.

Chapter "On the Security Weaknesses in Password-Based Anonymous Authentication Scheme for E-Health Care"
This chapter addresses some security implications of E-healthcare domain taking into account an existing protocol. The overview of the protocol is addressed, and a lot of security loopholes are illustrated. The security comparison of the similar protocols has been made so that the analysis of the feasibility of the same could be made.

Chapter "Integrated Probabilistic Relevancy Classification (PRC) Scheme for Intrusion Detection in SCADA Network"
This chapter outlines a novel method named as probabilistic relevance classification (PRC) to overcome the issues of intrusion detection using fusion of hidden Markov model (HMM) and relevance vector machine (RVM) techniques. The main

intention of this work is to reduce the set of features and amount of database and to increase the detection rate. Finally, it helps to classify the attack as known or unknown.

Chapter "Intrusion Detection System in Internet of Things"
This chapter highlights the different intrusion detection system (IDS) for IoT and their comparisons in terms of detection rate, false positive, and accuracy related to static and mobility of devices. It also highlights the type of intrusion and triggers an alarm in the intrusion scenario to take appropriate preventive measure.

Chapter "Deep Learning and Machine Learning Techniques for Intrusion Detection and Prevention in Wireless Sensor Networks: Comparative Study and Performance Analysis"
This chapter outlines a comparative study and performance analysis of different machine learning and deep learning techniques given for intrusion detection and prevention system. Moreover, in this chapter, performance evaluation of the techniques is also illustrated based on a Dataset for Intrusion Detection Systems in Wireless Sensor Networks (WSN-DS).

Part "Design of Automation and Troubleshooting Technique" (Chapters "Study and Design of Route Repairing Mechanism in MANET"–"Ambient Intelligence for Patient-Centric Healthcare Delivery: Technologies, Framework, and Applications")
This part highlights various automation and troubleshooting techniques in WSN as well as MANET. These techniques are illustrated in terms of route design, route repair, resource allocation, detection of attacks, fault diagnosis, and intelligent application of the healthcare system. The short descriptions of these chapters are given as follows.

Chapter "Study and Design of Route Repairing Mechanism in MANET"
This chapter outlines the study and design of route repairing mechanism in MANET. In this chapter, the proposed routing protocol is based on ad hoc on-demand distance vector (AODV) routing protocol. The basic idea of this work is to find an optimal path based on the minimum hop count in the multipath environment.

Chapter "A Comprehensive Parameterized Resource Allocation Approach for Wireless Sensor Networks"
This chapter indicates a parameterized resource allocation method in WSNs. Basically, it is a multi-parameters based resource allocation method that design for congestion-free, energy-efficient, link-quality, and application latency-aware resource allocation. It addresses all the challenges which are discussed in the comprehensive model present in the chapter.

Chapter "Effect of Wormhole Attacks on MANET"
This chapter illustrates the effect of wormhole attacks in MANET. The characteristic of MANET are high mobility and dynamic. So, it causes main vulnerable to wormhole attacks and resulting degrades the network lifetime and performance. In this chapter, several issues and reasons of the wormhole attack are discussed.

Chapter "Distributed Online Fault Diagnosis in Wireless Sensor Networks"
This chapter highlights an online distributed system for fault diagnosis in WSN. It helps to provide continuous service of the network despite the occurrence of failure of few nodes in the network. Moreover, in this chapter, some of the burning issues related to distributed fault diagnosis of the intermittent faulty sensor are also addressed.

Chapter "Ambient Intelligence for Patient-Centric Healthcare Delivery: Technologies, Framework, and Applications"
This chapter outlines the technologies, frameworks, and applications of an ambient intelligence system. This system is based on patient-centric healthcare delivery in WBAN. The architecture of this system is secure and cloud-oriented. The basic aim of this algorithm is to transmit data from WBAN to cloud storage.

Part "Design of Optimization Based Network Lifetime Enhancement Technique" (Chapters "Evolutionary Algorithms for Coverage and Connectivity Problems in Wireless Sensor Networks: A Study"–"Image Encryption in IoT Devices Using DNA and Hyperchaotic Neural Network")
This part illustrates several optimization techniques for enhancing the network lifetime of different wireless networks. The basic purpose of this optimization is to solve several coverage and connectivity issues, detection of uplink, conflicting strategy management, and image encryption in IoT devices. The short descriptions of these chapters are given as follows.

Chapter "Evolutionary Algorithms for Coverage and Connectivity Problems in Wireless Sensor Networks: A Study"
This chapter aims to study and analyze the various evolutionary approaches like genetic algorithm (GA), particle swarm optimization (PSO), and ant colony optimization (ACO) which are applied to solve the coverage and connectivity problems for WSN. Moreover, this chapter highlighted few research challenges related to coverage and connectivity of WSNs.

Chapter "Nature-Inspired Algorithms for *k*-Coverage and *m*-Connectivity Problems in Wireless Sensor Networks"
This chapter provides some nature-inspired algorithms such as PSO, GA, differential evolution (DE), and gravitational search algorithm (GSA) that are studied and designed to solve the problem. The chromosome, vector, particle, and agent are efficiently represented in the algorithms. Furthermore, an efficient derivation of fitness functions is provided with the conflicting objectives.

Chapter "Swarm Intelligent Based Detection in the Uplink of Large-Scale MIMO Wireless Communication Systems"
This chapter highlights some of the promising bio-inspired techniques such as ACO and social spider optimization (SSO) and introduces one of the key applications of these algorithms, that is, to solve the combinatorial optimization problem of symbol detection in large-scale multiple-input–multiple-output (MIMO) systems.

Chapter "A Nonlinear Strategy Management Approach in Software-Defined Ad hoc Network"
This chapter outlines the design of an efficient path for SDANET using fusion of some intelligent techniques such as nonlinear formulation, fuzzy logic, and game theory. The game theory method is used to establish relationships among dynamic nodes. The nonlinear programming is used to estimate uncertainty in the parameters, whereas fuzzy logic is used to fulfill the linguistic requirements of the nodes.

Chapter "Image Encryption in IoT Devices Using DNA and Hyperchaotic Neural Network"
This chapter describes an image encryption algorithm for IoT devices. In this algorithm, neural network is used to control the various operations of the encryption scheme. Every neuron of the neural network uses the equation of chaotic maps as its transfer function.

Part "Design and Implementation of Efficient Routing Protocol" (Chapters "Implementation of Traffic Priority Aware Medium Access Control Protocol for Wireless Body Area Networks"–"Fuzzy Petri Nets-Based Intelligent Routing Protocol for Ad Hoc Network")
This part highlights some implementation of efficient routing protocols. The basic features of these routing protocols are traffic and priority management, designing of shortest path, and design of intelligent path with the help of nodes and link attributes. The short descriptions of these chapters are given as follows.

Chapter "Implementation of Traffic Priority Aware Medium Access Control Protocol for Wireless Body Area Networks"
This chapter illustrates designing a new routing protocol for traffic management. In this work, patient's data is categorized into two forms as emergency and non-emergency data, depending on high and low threshold values. It helps to implement data traffic prioritization for giving priority to the patient data. It helps to reduce average delay and energy consumption and increases final throughput.

Chapter "Enhanced Shortest Path Routing Protocol Using Fuzzy C-Means Clustering for Compromised WSN to Control Risk"
This chapter outlines the regions which cover the dense set compromised nodes (CNs) named as compromised regions (CRs). For preventing the attacks of CRs, in this work, a security method is proposed using fuzzy C-means clustering. It helps to increase the network lifetime and to find optimal cluster head.

Chapter "Fuzzy Petri Nets-Based Intelligent Routing Protocol for Ad Hoc Network"
This chapter describes an intelligent routing protocol using fuzzy Petri nets (FPNs). It consists of two phases such as evaluation of fuzzy cost and route selection. The first phase is used to evaluate the fuzzy cost of node and link using fuzzy logic. The second phase is used to evaluate the optimal route with the help of FPN model.

Brahmapur, India — Santosh Kumar Das
Bardhaman, India — Sourav Samanta
Kolkata, India — Nilanjan Dey
Jaipur, India — Rajesh Kumar

List of Reviewers

Abdul Wahid, IIT (ISM), Dhanbad
Abhijit Panda, NIST Berhampur, Odisha
Abhishek Kumar, SITE, Swami Vivekanand Subharti University, Uttar Pradesh
Ajay Kumar Yadav, Banasthali Vidyapith, Rajasthan
Alokeparna Choudhury, St. Xavier's College, Burdwan, West Bengal
Arun Prasad Burnwal, GGSESTC, Bokaro, Jharkhand
Arvind Kumar, AIACTR, Geeta Colony, Delhi
Asish Samantra, NIST Berhampur, Odisha
Bhabani Gouda, NIST Berhampur, Odisha
Bhavya Bansal, SITE, Swami Vivekanand Subharti University, Uttar Pradesh
Debashis Das, Techno India University, West Bengal
Gaytri Kumari Gupta, Jamshedpur Women's College, Jharkhand
Gitanjali R. Shinde, Smt. Kashibai Navale College of Engineering, Savitribai Phule Pune University, Pune
Harendra Kumar, Government Polytechnic Bilaspur, GEC Campus, Koni Bilaspur
Indradip Banerjee, UIT, Burdwan, West Bengal
K. Hemant Kumar Reddy, NIST Berhampur, Odisha
Madhuri Malakar, NIST Berhampur, Odisha
Mahendra Prasad, IIT (ISM), Dhanbad
Manish Mandloi, SKVM's NMIMS, Shirpur, Maharashtra
Meenakshi Panda, NIT Goa
Nabajyoti Mazumdar, CIT, Kokrajhar, Assam
Preeti Chandrakar, NIT Raipur
Rifaqat Ali, MITS, Madanapalle
S. S. Kulkarni, Sinhgad College of Engineering, Pune
S. Shitharth, Vardhaman College of Engineering, Hyderabad
Samiran Bera, IIT (ISM), Dhanbad
Samiran Gupta, Asansol Engineering College, Asansol, West Bengal

Sanjay Kumar Panda, VSSUT, Burla, Odisha
Sourabh Debnath, NIST Berhampur, Odisha
Sunil Kumar Gautam, Institute of Advanced Research, Gandhinagar, Gujarat
Trilochan Panigrahi, NIT Goa

Contents

About the Editors

Santosh Kumar Das received his Ph.D. degree in Computer Science and Engineering from Indian Institute of Technology (ISM), Dhanbad, India, in 2018 and completed his M. Tech. degree in Computer Science and Engineering from Maulana Abul Kalam Azad University of Technology (erstwhile WBUT), West Bengal, India, in 2013. He is currently working as Assistant Professor at School of Computer Science and Engineering, National Institute of Science and Technology (Autonomous), Institute Park, Pallur Hills, Berhampur, Odisha, India-761008. He is having more than eight years teaching experience. He has contributed more than 25 research papers. His research interests mainly focus on Ad-hoc and Sensor Network, Artificial Intelligence, Soft Computing, and Mathematical modeling.

Google Scholar Profile: https://scholar.google.co.in/citations?hl=en&user=AkQx5KoAAAAJ

Webpage: http://www.nist.edu/faculty/forms/faculty.php#FACULTLIST

Sourav Samanta is currently working as Assistant Professor in the Department of Computer Science and Engineering at University Institute of Technology, The University of Burdwan, West Bengal, India. Before joining the University Institute of Technology, he worked as lecturer at the GobindpurSephali Memorial Polytechnic, Guskara, Burdwan, West Bengal. He has completed M. Tech in Computer Science and Engineering from JIS College of Engineering, Kalyani, West Bengal and completed B.E in Information Technology from University Institute of Technology, Burdwan, West Bengal respectively. He has more than six years, academic experience.

His research area includes Bio Inspired Computing, Quantum Machine Learning and Information Security, Networking. He has published 40 research papers in various reputed International Journals and Conference and co-authored a book. He is a regular reviewer of IEEE Access and IEEE Sensor Journals. He serves as Program Committee member for various International Conferences. He has an interest in interdisciplinary research. He is a member of Computer Society of India and International Association of Engineers.

Google Scholar: https://scholar.google.co.in/citations?user=nZQ9wmwAAAAJ&hl=en

Nilanjan Dey is an Assistant Professor (Senior Grade) in Department of Information Technology at Techno India College of Technology (under Techno India Group), Kolkata, India. He has completed his PhD. in 2015 from Jadavpur Univeristy, Kolkata, India. He is a Visiting Fellow of Wearables Computing Laboratory, Department of Biomedical Engineering Univeristy of Reading, UK. He is the Visiting Professor of College of Information and Engineering, Wenzhou Medical University, P.R. China and Duy Tan University, Vietnam. He has held honorary position of Visiting Scientist at Global Biomedical Technologies Inc., CA, USA (2012-2015). He is a Research Scientist at Laboratory of Applied Mathematical Modeling in Human Physiology, Territorial Organization of- Scientific and Engineering Unions, Bulgaria, Associate Researcher of Laboratoire RIADI, University of Manouba, Tunisia and Scientific Member of - Politécnica of Porto. Before he joined Techno India College of Technology, he has served as an Assistant Professor at JIS College of Engineering and Bengal College of Engineering and Technology.

With more than 10 years of teaching and research experience, he has authored/edited more than 40 books with Elsevier, Wiley, CRC Press and Springer, and published more than 350 research articles. His h-index is 30 with more than 4000 citations. He is the Editor-in-Chief of Int. J. of Ambient Computing and Intelligence (IJACI, IGI Global,UK, Scopus), Int. J. of Rough Sets and Data Analysis (IGI Global, US, DBLP,ACM dl). He is the Series Co-Editor of Springer Tracts in Nature-Inspired Computing (STNIC), Springer and Advances in Ubiquitous Sensing Applications for Healthcare (AUSAH), Elsevier, Series Editor of Computational Intelligence in Engineering Problem Solving and Intelligent Signal processing and data analysis, CRC Press (FOCUS/Brief Series), De Gruyter Series on the Internet of Things and Advances in Geospatial Technologies (AGT) Book Series, (IGI Global), US, serves as an editorial board member of several international journals, including International Journal of Image Mining (IJIM), Inderscience, Associated Editor of IEEE Access (SCI-Indexed), and International Journal of Information Technology, Springer.

In addition, he was awarded as one among the top 10 most published academics in the field of Computer Science in India during the period of consideration 2015-17 during 'Faculty Research Awards' organized by Careers 360 at New Delhi, India on March 20, 2018.

His main research interests include Medical Imaging, Machine learning, Computer Aided Diagnosis as well as Data Mining. He has been on program committees of over 50 international conferences, a workshop organizer of 5 workshops, and acted as a program co-chair and/or advisory chair of more than 10 international conferences.

He has given more than 50 invited lectures in 10 countries, including many invited plenary/keynote talks at the international conferences such as ITITS2017 (China), TIMEC2017 (Egypt) and BioCom2018 (UK) etc.

Amazon: https://www.amazon.com/Nilanjan-Dey/e/B01MSMZDF1/

GoogleScholar: https://scholar.google.co.in/citations?hl=en&user=uZmrRHAAAAAJ

Wesite: https://sites.google.com/view/drnilanjandey/home

Rajesh Kumar received a Bachelor of Technology Degree with Honours from National Institute of Technology, Kurukshetra, India, in 1994. He also earned a Masters of Engineering Degree with Honours from the Malaviya National Institute of Technology, Jaipur, India in 1997; he earned a PhD. Degree from the Malaviya National Institute of Technology, Jaipur and University of Rajasthan, Jaipur in 2005. He was awarded Post Doctorate Research Fellow in the Department of Electrical and Computer Engineering at the National University of Singapore (NUS), Singapore, from 2009 to 2011. He joined the Department of Electrical Engineering at the Malaviya National Institute of Technology, Jaipur, India as a Lecturer in 1995. He is currently serving as Professor and Head. He is also adjunct faculty to Centre of Energy and Environment at Malaviya National Institute of Technology, Jaipur, India.

Dr. Kumar has carried out extensive research in various areas of theory and practice of intelligent systems, bio and nature inspired algorithms, smart grid, power electronics, power management, applications of AI to image processing and robotics. He has published more than 450 papers in international refereed journals and conferences. He has received and published 12 patents. He has supervised 15 PhD and 35 Master thesis. He has delivered more than 100 expert talks in various conferences and workshops. Dr. Kumar has won the Career Award for Young Teachers, Government of India in 2000. He received 06 best thesis awards, 05 academic awards, 12 best paper awards, 04 professional awards and 30 student awards.

He is Vice Chairman, IEEE Rajasthan Sub Section and Executive Member, IEEE PES-IAS Delhi Chapter and Computer Society of India, Rajasthan Section. He is Associate Editor of IEEE ITeN (Industrial Electronics Technology News), Associate Editor, Swarm and Evolutionary Computation, Associate Editor, IET Renewable and Power Generation, Associate Editor, IET Power Electronics, Deputy Editor-in-Chief, CAAI Transactions on Intelligent Technology, Associate Editor, International Journal of Bio Inspired Computing. He is an Editorial Member of more than 15 Journals. Dr. Kumar is also Senior Member IEEE (USA), Fellow IET (UK), Fellow IE (INDIA), Fellow IETE, Life Member CSI, Senior Member IEANG and Life Member ISTE.

GoogleScholar: https://scholar.google.co.in/citations?user=ZBaMrjUAAAAJ&hl=en

Website: https://drrajeshkumar.wordpress.com/

Design and Enhancement of Security and Privacy Technique

An Analysis and Comparison of Security Protocols on Wireless Sensor Networks (WSN)

Ranjit Kumar, Sachin Tripathi and Rajeev Agrawal

Abstract With increasing several applications of WSN, the provision of securing sensitive information of the entire network should be made for which sensor networks and ad hoc networks are introduced for the routing protocol. Many protocols as an opponent can disrupt the network or exploit precious data from the network which is not with the purpose of security. Large number of nodes, limited battery power, and their data-centric nature in routing WSN make routing a challenging problem in WSN. Therefore, security solutions should be properly formed because they have had a strong collision on large presentation. In this work, we mainly concentrate on security issues, security requirements, and we have also analyzed and discussed some key management protocols for secure transmission of data and comparing them on the basis of performance. This work has provided a detailed description of the WSN-related information to extremely understand the concept of the network.

Keywords Wireless sensor network (WSN) · Security · Cryptography · Key management protocols

R. Kumar (✉) · S. Tripathi
Department of Computer Science and Engineering, Indian Institute of Technology (Indian School of Mines) Dhanbad, Dhanbad 826004, Jharkhand, India
e-mail: ranjit_kumaruitbu@yahoo.co.in

S. Tripathi
e-mail: var_1285@yahoo.com

R. Agrawal
Department of Computer Science and Engineering, GL BAJAJ Institute of Technology & Management, Greater Noida 201301, India
e-mail: rajkecd@gmail.com

S. K. Das et al. (eds.), *Design Frameworks for Wireless Networks*,
Lecture Notes in Networks and Systems 82,
https://doi.org/10.1007/978-981-13-9574-1_1

1 Introduction

WSN has hundreds or thousands of little gadgets with detecting, preparing, and correspondence abilities for certifiable ecological observing [1, 2]. Sooner rather than later, from significant military checking applications to forest flame observing and security checking, they have been appointed to play important roles in different areas. Sometimes, WSN works with infrastructure based or infrastructure less as like wireless ad hoc networks [3–8]. Because it is rapidly used in different real-life applications. In this network, the smart sensor nodes (SSN) are equipped with one or more sensors, one processor, memory, one power supply, one radio, and low-power equipment, an actuator. The sensor's execution is to screen the physical and natural conditions, for example, dampness, weight, sound, and temperature. After their surveillance, they send information to their main place. The sensor network comprises collection of sensor hubs which are deployed in the scenario (Fig. 1).

The WSN network which does not interfere with the use of current security approaches does not have a resource in the different architectural layers, such as the inter-node status of communication and application level, focusing on the level of a node. For example, there are many barriers to limited resources for limited assets, unpredictable statement, and non-permissible functioning. The main motivation of the work is to briefly explain the concept of WSN. There are various issues related to the security of the information used in the wireless network [9]. It provides a detailed description regarding the security protocols.

This work is sorted out when pursues: inside Sect. 2, requirements and security threat models are discussed. Areas 3 talk about different conventions for WSN. Segment 5 illustrates the analysis and comparison of the WSN protocols. At last, the paper has been finishing up in Sect. 6 with conclusion.

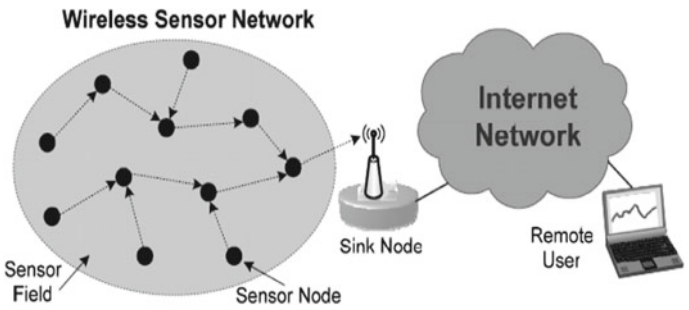


Fig. 1 Wireless sensor network

2 Literature Survey

Bletsas et al. [10] in this work have given different clustering approaches in WSN. First, we separate the protocol used in the WSN in the forms of protocol operation (PO), network structure (NS), and path estimate (PE). Second, we have provided a broad overview of the cluster-based routing protocol used in the block cluster, chain cluster, and grid cluster which forms the WSN, and we have discussed various issues in routing protocols and compared various clustering routing protocols based on various attributes

Priyadarshini et al. [11] discuss the conference which relies on session key foundation and open key cryptography for outside operator verification. An outside administrator passes on through an open key encryption framework with a BS, which talks with sensor center points through the sharing of a private key. The technique for this tradition is isolated into three phases: selection, affirmation, and session key establishment (SKE).

Biagioni et al. [12] proposed an effective cryptographic methodology for information security in WSNs utilizing the Modern Encryption Standard Version-II. The symmetric key encryption is introduced by MES V-II and the JSA and DJSA calculations are utilized and randomized technique by a calculation which is made by Nath et al. In this approach, a summed up and altered Vernam figure methodology is used with different square sizes and keys for each square. As an additional security reason for this count, info is furthermore added to this method. After the quick stage encryption is done, the entire record is divided into two exchanged parts and the balanced Vernam figure method with info and another key will be reiterated. Repeating this entire action, various events result in a system that is significantly secure.

Akyildiz et al. [13] in this essay proposed a multi-level security system which is introduced using a data-oriented random number generator to encrypt a tag of frames. The first level will be started using the interlacing method. Second, the suite-random number generator's value is the seed. Third, the bank will first distribute a numeral. Final status starts when the number is applied to the bank.

Wong et al. [14] proposed the method which introduces a flood dependency based on data sources in the river. The main idea behind this node is that each node can be considered as a data source, which sends the actual data after an event has been detected on a non-node; dummy data is available on all ion nodes in this node. This approach is difficult to distinguish between the opponent's original packet and dummy, which leads to dirt traffic and energy consumption. A new solution is suggested by using variable-sized dummy packets. Dummy patterns vary from actual packages, so energy conservation occured. However, an expert will still find it difficult to distinguish dummy real packages.

Collins et al. [15] proposed the capacity to investigate for security shortcomings, mishaps, and infringement appearing on a honeypot system for WSNs. This is a recommended way to deal with a model that needs more examinations to assess its adequacy as a total framework for recognizing system attacks and different attacks. The opposite side of this innovation has been connected to control utilization by

honeypot sensor hubs. This strategy does not have any significant bearing to other security issues and should, accordingly, be joined with different arrangements.

3 Security in Wireless Sensor Networks (WSN)

The sanctuary has been used largely as a word that features the characteristics of affirmation, decency, assurance, non-replay, and threatening to playback [16]. More dependence on the information given by the framework has been comprehensive, the further vital the threat of protected diffusion of information on the framework is extended. For the protected transmission of various sorts of information on the framework, various cryptographic, stenographic, and distinctive strategies are used which are remarkable. In this section, we talk about the structure security prerequisites and issues and how the frameworks are proposed for remote sensor frameworks.

3.1 Sanctuary Requirements in WSN

I. Data privacy: The safety methods have the assurance that no communication in the structure is comprehended by anyone aside from the expected receiver. In a WSN, issue of secrecy must address the accompanying prerequisites [17, 18]:

   (i) An SN is not allowed to read its readings to its neighbors, and if such recognition exists,
   (ii) The key distribution method (i.e., Diffie–Hellman) must be amazingly strong,
   (iii) Open data, for example, public keys and sensor characters of the nodes ought to likewise be scrambled in specific bodies of evidence to secure against traffic analysis attacks.

II. Data integrity: Make sure that an organization cannot send a message when it passes to the beneficiary from the sender.

III. Availability: These demands ensure that WSN's rulers are accessible both in and out of the way in the event of attacks, such as the service attack (DoS). Analysts tend to divide the methods of dividing this goal. If one of the systems uses the corresponding correspondence between the nodes, others utilize the use of a middle control framework to effectively distribute each message to its beneficiaries.

IV. Data Authentication (DA): Authentication guarantees the unwavering quality of the message by recognizing its starting point. In a WSN, the issue of validation ought to attend to the accompanying necessities:

(i) Communicating point is the one that it professes to be used among the two nodes for the transferring of the data.
(ii) The recipient ought to check that the acknowledged packets have verifiably originated since the real SN.

For confirmation to be accomplished, the two families could share a secret part to calculate message authentication code (MAC) of all imparted information. The collector will confirm the authentication of the got message by utilizing the MAC key.

V. Non-repudiation: It intends to assurance that the message exchanged has been sent and got by the parties professing to have sent and got the message.
VI. Availability: Availability means to ensure that the data resource is available for legitimate user [19]. It says data ought to be accessible dependably to the legitimate clients all through the system regardless of whether there are inner or outer failures, faults, errors, or attacks [20].
VII. Data Freshness: It guarantees that the intimation got amid trade is crude without any trace of reused data. In wireless sensor network, the data's may not be transmitted inside the given time interim, so we should ensure that it is new. To accomplish this, the time stamp is utilized. It comprises two sorts, for example, frail freshness gives a little request to the information's so delay cannot be determined, while solid freshness gives a general request and permits the count of delays [20].
VIII. Self-organization (SO): WSN is usually an ad-hoc network (AHN), where each SN should be autonomous and sufficiently adaptable to be SO and self-healing (SH) in any situations. There is no permanent framework accessible for the system supervision, so nodes should adjust themselves for the organization strategy [19].

3.2 Constraints in WSN

I. Resource constraints: Low computational power, small memory, low remote control data transmission, restrained as a range, no battery-operated string.
II. Small message size (SMS): The communication in SN has a little size contrasted and the existing networks generally for the most part. Therefore, there is normally no understanding of division in many applications in WSN.
III. Addressing proposals: Appropriate to a generally expansive number of sensor nodes, it is beyond the realm of imagination to expect to manufacture worldwide tending to plans for sending of countless SN as the visual projection of uniqueness preservation is elevated.
IV. Sensor location (SL) and idleness of data: Location responsiveness of SN is significant since information gathering is usually found on position. Likewise, there could be regular wonders together information, it is therefore very likely that this data has some recursion.

3.3 Security Threat Models

As indicated by Karlof et al. [21], terrorization in WSN may be ordered into the accompanying classes:

a. Insider attacks (IA) versus outsider: It happens when there are authentic points of a WSN Act in unexpected or unrecognized path. The invader may have incomplete key metric and other SN. IN are very difficult to recognize. Outdoor attacks can be considered as an attack on nodes with no WSN space. The outside invader does not have the most cryptographic materials on the SN.
b. Active versus passive attacks: Latent attacks are in listening stealthily on, or checking of parcels exchanged inside a WSN; the dynamic attacks incorporate a couple of changes of the information stream and the generation of a bogus stream in a WSN.
c. Laptop-class versus Mote-class attack: In laptop-class attacks, all competitors like a rival PC can be used, and it would be damaging a system more than a deadly sensor. In mote-class attacks, a WSN attacked by nodes with relatively powerful nodes, such as network nodes (NN).

Attacks against the WSN are categorized as critically or not. Navigation attacks, usually, side channel attacks include, for example, power-, timing-, or frequency-based attacks. For example, WSN's obvious distribution of clear side attacks, for instance, has many problems with other established frameworks, for example, MAC generation or encryption time can be used with time sensors using sensor nodes.

1. MAC generation: The cryptographic systems are designed to perform complicated encryption and the creation of message authentication becomes challenging in spite of various attacks from adversaries. Many protocols are designed based on the assumption that the host's posses a secret random string known as key and it is conveniently taken for granted that the entire key is kept secret from an adversary. There might be a possibility that an adversary may detect a part or entire key which is called as key exposure problem and it has significant practical interests.
2. Encryption time: This is generally the time required during the generation of keys, encrypted text, and decrypted text. The algorithm having less time for each of the processes is considered to be better algorithm.

Violent attacks are very common; most of them are portrayed in the following sections. Some attacks on sensor networks are as follows:

Attack on protocol layer (PL):

(1) Physical layer: This tile and associates adds:

I. JAMMING: Transmission of a signal to an attacker on base stations at the same frequency of the transmitter. This interrupts the radio conversations.

Defensive measures: It is the use of communicating with each other, i.e., the frequency hopping spread spectrum (FHSS) that makes the frequency hoop. This shows the swap of the bus data between different frequency channels [22].

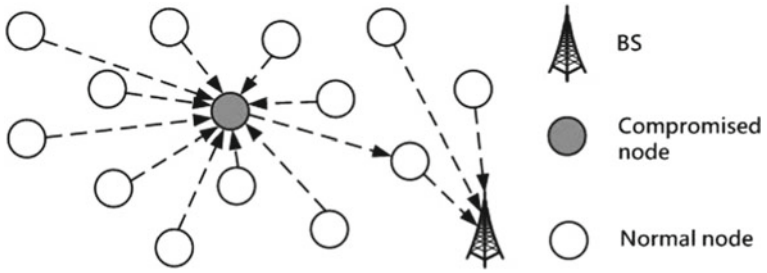


Fig. 2 Tampering attack

II. Tampering: The attacker is trying to go to a mechanical assembly such as chips. The treatment of bits also receives confidential data from the SN (Fig. 2).

Defensive measures: It also helps in containing secret data between the microcontroller and external memory chip. This process is known as eavesdropping.

(2) Data link layer (DLL): This tile and associates adds:

I. Collision/pileup: When an attacker finds the message that a message sends out, he removes his own signals to intervene. This causes conflicts when multiple nodes pass on the same frequency and data velocity. The packet can change the information to be considered worthless.

Defensive measures: Steps to deal with this attack can be prevented.

II. Exhaustion/collapse: Aggressor sends ease of data or demand in a channel that promotes deprivation. The origin of the attack is a PC or laptop.

DM: It may claim to reduce the MAC sending rate to avoid excess demand from the sensor network. As long as the sensor node enables us to transfer data over time, on these lines, the MAC channel for nodes has long been connected. [22]

(3) Network layer (NL): This layer contains attacks:

I. Selective forwarding (SF): SF is an approach to impact system interchange by trusting to the entire the taking contributing hubs in network are dependable to advance the information. In fixed-sent attacks, some malicious messages (MNs) provide some messages against sending a message (DCM). MN or attacking nodes may won't route definite messages and leave them. If that they leave every one of the packets during them, at that point it's known as a BHA. Be that as it may, on the off chance that they specifically forward packets, at that point it is termed as selective forwarding. The embarkation of this occurrence depends on two factors. First, the position of the malicious party, which is much higher than the BS, it will pull off more. The second is the quality of the dropdown messages. Special exchange of this is where a stronger point is to capture all of the nude nodes while most messages are excluded.

Defensive measures: Multipath routing could be used to counterattack. This lessens the likelihood of an attack by an enemy. To regulate the framework guard dog can be utilized.

II. Acknowledge spoofing (AS): An attacker can associate with environmental light air conditioner consent. Wrong error messages are created by the attacker. Making routing links. Thus, latency will be terminated and the organization will be assigned (Fig. 3).

Defensive measures: Each packet must be broken for a rival.

III. BHA (Black hole attack): In this attack, an MN sensor goes like a black hole [21] to drag for all traffic on the network. Especially in a flood-founded convention, he is listening to answers to the answers to the high-caliber or lowest goal–goal nodes for the BS. If you have a capable device capable of containing malicious nodes (for example, sink and SN), you can do it with packets that go between them. This attack can be influenced even by the nodes of significant means from basic stations. Figure 4 demonstrated the vision applied to a black hole/sinkhole attack.

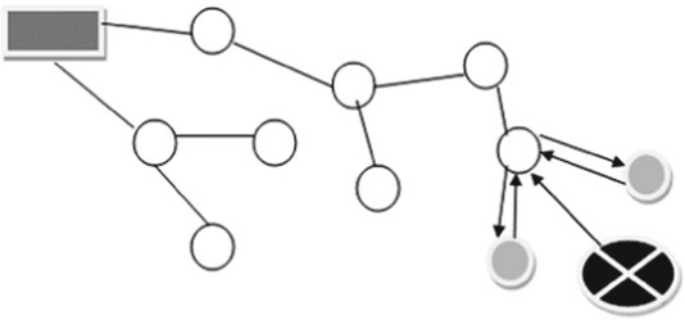


Fig. 3 Acknowledge spoofing

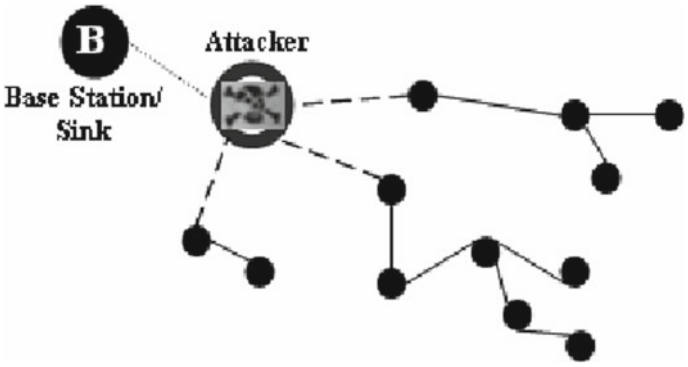


Fig. 4 Black hole attack

Defensive measures (DM): An arrangement ought to be executed, so one of the hubs on the system must be perceived by translate rate information disseminated through invalid hubs. Cryptographic procedures can be utilized.

IV. Wormhole attack (WHA): It sends offensive record bits to one place in the system at one place and sends them to the other places in the tunnel. Wormhole, WSN is a major threat to the child's tanning or rearrangement choices; there is no need to compromise a sensor in this network for such an attack, it can be done at the beginning of the stage when the sensor starts searching for the neighboring information (Fig. 5) [23].

DM: A four-way handshaking messaging system is used to counterattack. The private channel can likewise be utilized for security.

V. Sybil: According to [24], a self-trickery belonging is appended with a hub that keeps nearest node in various locations. Outsiders focus on these numerous areas and cause issues in dispersed capacity to get to multipath routing and bending in topology (Fig. 6).

Defensive measures: Validation procedure necessity is utilized to counterattack.

VI. Hello flood (HF): Attacker transmits hello packets starting with one node then onto the next. Attacker publicizes modest routes which lead to sending of communication to assailant [25].

Defensive measure (DM): Using the profile evaluation convention, you can oppose the HELLO FLOW.

According to nature, protocols named Proactive, Active, and Hybrid:

(a) Proactive Routing Protocol: These protocols are additionally called as table-driven routing protocols since they keep up the routing data even before expecting of this data. Every single hub keeps up directing data to each other hub in

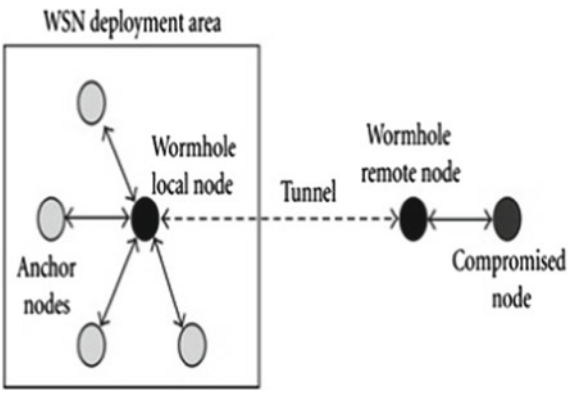


Fig. 5 Wormhole attack

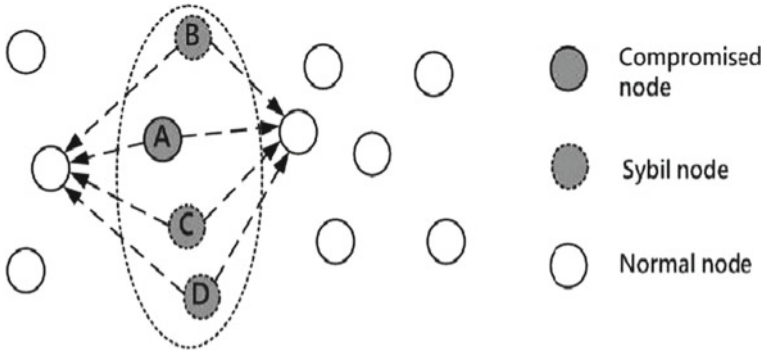


Fig. 6 Sybil attack

the system. Courses data is commonly kept in the steering tables and is intermittently refreshed as the system topology changes. The protocols under this classification keep up various numbers of tables. Moreover, they are not appropriate for extensive systems, as they have to keep up sections for every hub in the steering table.

(b) Reactive Routing Protocol: These protocols are likewise called as on-demand routing protocol as in these sort of routing protocols hub looks for course on-request, i.e., at whatever point a hub needs to send information it scans course for goal hub and builds up the association.

(c) Hybrid Routing Protocol: The combination of both above protocols is identified as hybrid routing protocols.

3.4 Security Solutions in WSN

WSN are exceptionally defenseless against attacks, it is imperative to embrace a few methods that can shield the system from a wide range of attacks it must be a guarantee that the framework is secured previously, amid and after any sort of attack [26]. Security guards and safety are the main tools for recovery. These locomotives have public key cryptography (PKC), semantic key encryption (SKE), and hash functions (HF) [27]. The SKE and HF are building blocks that make up the required infrastructure of the data stream. This is a confirmation of the classification and reliability of this channel. PKC guarantees assurance from the interest of outside substances and furthermore disposes of the issue of a malicious insider which attempts to utilize added one personality.

PKC guarantees by permitting confirmation of friends associated with the data trade. In light of the natives, it is conceivable to make superior system administrations. It is likewise similarly vital to have a key administration framework by building a safe key base.

Security is a widely used feature of authenticity, integrity, privacy, discontent, and anti-playbacks. The risk of secure transmission of information for the network, increasing the reliability of the information provided to the network. In this section, we discuss network security finances and technology for WSN.

(a) Encryption:

This system is opposed to inactivity, such as a candle. The sensor network is mostly wireless channels operating in public or wild areas. It is therefore uncommon to transfer emails from a device or add messages to the network. The traditional key of this problem is the three primary methods: the authentication codes, the similar key encryption schemes, and the public key cryptography.

(b) Symmetric encryption:

In this paper, the capacity to investigate security shortcomings, mishaps, and infringement has appeared on a honeypot system for WSNs. This is a recommended way to deal with a model that needs more examinations to assess its adequacy as a total framework for recognizing system attacks and different attacks. The opposite side of this innovation has been connected to control utilization by honeypot sensor hubs. This strategy does not have any significant bearing to other security issues and should, accordingly, be joined with different arrangements.

(c) Asymmetric encryption:

This is also known as public key cryptography. It uses two keys: The public key used by encryption, private key, and only the user of the key used to decryption it. Public–private keys are interconnected with any mathematical means. In other words, encrypted data with a public key can only be encrypted using its corresponding key.

(d) Cryptography:

Cryptography is of prime importance, the basic attitudes that make sure the essential elements, honesty, and confidentiality. Elliptic curve cryptography (ECC) is recognized as a practical approach for WSN. A good alternative is the ECC for RSA-based algorithms, as the size of the standard ECC keys, if it is too small for security [28].

4 Key Management Systems

In the wake of watching the imperatives and restrictions of sensor systems, obviously, these sorts of environment require trivial cryptography to accomplishing the abnormal state of security [29]. So as to give a protected security arrangement, all sensors need to concur between the costs, the death penalty, and security. Be that as it may, in the meantime, it is hard to accomplish three arrangement objectives. In such a circumstance, engineers are making gifts to the economy utilizing successful viable budgetary arrangements that are not authentic for key appropriation [29].

Accordingly, WSN requires various systems to enhance movement on the fundamental appropriation of the system, which is how they are utilized on verified settled systems.

4.1 Protocols and Methods Classification

Mainly techniques dependent on asymmetric or symmetric and hybrid frameworks tackle issue of the key foundation during a pre-distribution stage. The pre-distribution of encoding keys in a WSN is the reality of putting away these keys in the MN previous to exploitation. In literature, we discover a few characterizations of cryptographic key administration frameworks, for example, papers in [30–32]. A few classifications strategies depend on key participation, two nodes (pairwise) or more nodes (group restrictions) and more, abusing the possibility of joint testing. We made a classification and all major governments and distribution models were included in two larger families. The primary classification includes (i) symmetric projects (ii) and asymmetrical projects.

In connivance, the main model of writing will be examined by us as follows:

(i) Symmetric plans (SP): The plans of this segment utilize unbalanced to build up an open key between two hubs in a WSN. It's done in three stages which are given below:

I. Key Pre-circulation: Keys set in memory before conveying are a hub key hub. You can make a typical key between two hubs.
II. Shared-key discovery: Two general keys are easier to find after communicating with the protocol. On deployment, neighboring sensor nodes begin the discovery process to find out whether they share a common key, if they do, they establish a secure link. There could be many modes for the discovery phase, such as broadcasting the list of identifiers existing in their key ring in clear text or through a challenge-response mechanism.
III. Path key establishment (PKE): In the event that there is no open key between the two hubs you need to impart, you should locate a protected way between them. This way goes through a lot of hubs that as of now have secure connections. Two ways are utilized to verify correspondence when this way is set up. A key pre-distribution scheme called PIKE (peer intermediaries for key establishment) is used to achieve the path key establishment. PIKE can guarantee that any two nodes in a network always share a key with an intermediary node. This intermediary node is then used to establish a path key between the two nodes. But this approach makes a large fraction of neighboring sensor pairs that do not share preloaded keys, and thus they need to establish path keys.

Some security protocols are examined beneath:

3. SPINS: This is a suite of security and security hinders that are given by Prig and various different creators. It is advanced for asset restricted conditions and remote correspondences [33]. Twists have two secure squares: SNEP, μTESLA.

   I. SNEP utilizes a common counter between two interchanges gatherings and the counter is utilized to compute a message validation code (MAC) to give semantic security, information uprightness, decodialization, information classification, answer assurance, and refreshing frail messages. What's more, since protocol has lower communications systems, on the off chance that the quantity of controls is dependent on each counter, the convention will just offer up to 8 bytes for each message. For a solid new reason, the sender will make an irregular sound (anticipated 64-bit esteem) and will be incorporated into the beneficiary's demand message. Resister creates reaction messages and incorporates non-MAC processing.
   II. μTESLA produces authentic broadcasts broadcasting from symmetric premises but is presented with delayed key opening and single-function key chains. SPINS also accepts the certified routing application and security back key agreement with μTESLA and SNEP, along with minimum storage, calculation, and communications expenditure. Though few issues still report by SPINS, it will not be regarded as a possible source of DOS risk; SPINS depend on the station-based station because the pair's rear distribution key uses the security protocols; the communication key's update will not be considered. A practical key updating system is needed to prepare for security. Hidden channel leak, spins cannot solve a node problem.

4. LEAP: The LEAP (nearby encryption, validation convention) is a noteworthy administration convention for sensors that help in organize preparing utilizing the fundamental system to control the security impact of a hub that has been undermined for moment arrange neighborhoods. The possibility of the Leap+ was propelled by this intriguing perception that distinctive kinds of messages were exchanged between the sensor hubs. This perception has achieved the decision that an alternate enemy of bunch framework is insufficient for these diverse security prerequisites [34–36]. Backing for the foundation of four keys per node:

   I. Pairwise key: shared with different SN.
   II. Individual key: Shared amid a BS.
   III. Global key: All nodes shared on the network.
   IV. Cluster key: Shared through several neighboring points.

   Packages that have been exchanged for each node in the sensor network are categorized into several categories, for example, different criteria:

   I. Queries or commands sensor readings,
   II. Broadcast Packets versus Unix Packets,
   III. Manage packets, manage data packets, etc.

The security prerequisite for every parcel relies upon the particular classification. Most bundles need to confirm, at times, just the bundles are the codename. This shows that a solitary key framework isn't suitable for every safe correspondence important in sensor systems.

5. Tinysec: Karlof et al. [37] TinySec convention forward and complete activity of secure structure in WSN's information connect layer. This execution underpins two security alternatives: authenticity of messages without message verification and information encryption (TinySec-Auth) with data encryption (TinySec-EA). TinySec utilizes normal cryptographic calculations to guarantee protection and security value checking. The Skyjack calculation [38] for WSN is greatly improved than the two combination revelations found in RC5 (calculation utilized in spines). TinySec validation is determined utilizing RC5 Pre-key utilizing 104 bytes. Utilizing TinySec CBC encryption mode (cipher blockchain) utilizes CTR (utilizing SPINS). The CD will furnish a similar bundle encryption with similar arbitrary numbers. Basically, these numbers are used to generate the encryption, an important section defames it through recursion by the security modules of its repetition and then helps the opponents find the content of the messages. TinySec is actualizing a noteworthy conveyance venture, coming up to finish a noteworthy circulation framework for the all-encompassing system. Two centers have two fundamental symmetric keys shared to pass on. The first is used as scramble messages, and second to determine MAC messages.

6. Micro-PKI: Munivel et al. [39] a straightforward variant of conventional PKI, small-scale PKI propose a technique that is known as an open key foundation. The base station (BS) has an open key and another private. People in general key are utilized for verification of the BSand the private station (PS) is utilized to decode information sent from the hubs. Before conveying, the BS open key is put away in all hubs. Creators give two kinds of handhelds. First sort validation between the interface hub and base station the hub makes a symmetry session key and encodes it utilizing the general population key of the BS. To guarantee the respectability of messages, each message is proposed to coordinate with a MAC (code) utilizing a similar encryption key. For new hubs to join the system, people in general key of the BS is put away on these hubs previously sending.
7. TinyPK: Watro et al. [40] A strategy known as TinyPK dependent on the utilization of open keys and the guideline of Diffie–Hellman proposed establishing a mystery key between the two hubs in WSN. TinyPK utilizes reliable specialist to sign hubs and open keys. Prior to deployment, the CA key is distributed before all keys, so the key can be verified by deploying. Time and energy of the RSA algorithm selection nodes for encryption are of great use. This basic functionality can be about a dozen seconds long, which reduces the time within the network, reducing the effectiveness of reaction.
8. PKKE and CBKE: The two conventions as shown by Zigbee utilizing the recognizable proof of hubs in the key expansion. This is to utilize these personalities to create a solitary sharing key between each pair of hubs on a system. Be that as it may, a common key is created through shared associations between the two hubs.

Table 1 Comparison among security protocols

Protocols	Encryption	Freshness (CTR)	Overhead (Bytes)	MAC used	Key agreement
SPIN	Yes	Yes	8	Yes	Symmetric delayed
LEAP	Yes	No	Variable	Yes	Pre-deployed
TINY SEC	Yes	No	4	Yes	Any
MICRO-PKI	Yes	Yes	Variable	Yes	Open key foundation
TINY PK	Yes	No	16	No	Pre-deployed
PKKE and CBKE	Yes	No	8	No	Noninteractive key distribution scheme
C4W	Yes	Yes	4	No	Pre-deployed

This means that you need to send and receive more than one message before creating the key. To protect the power nodes you wish to share with a secret and such intermediate node, there are a number of ways to remove this mutual exchange. These methods are called field ID-NIKDS [41] (a noninteractive key distribution scheme based on identity) in cryptography.

9. C4 W: Jing et al. [42] proposed a methodology known as C4 W based on identifying nodes to estimate open keys. Nodes can calculate other nodes' public keys. What might supplant the jobs of a testament? Before sending, hubs and base stations will be stacked with their very individual keys (private/open key ECC) and general data on system hubs. C4 W technique setting up a solitary sharing key in two hubs utilizing the standard of Diffie–Hellman key exchange is to use without testaments. In Table 1, there is a comparison performed on the basis of different parameters.

5 Analysis and Discussion

5.1 Analysis Method

A few criteria are considered so as to look at changed techniques for key administration. We have exhibited in the standard models shown in Fig. 5. We begin with the hub's asset limits. The key management method necessitates that the hubs be conveyed to gather data. They need their memory space to keep their information and vitality inserted so as to guarantee their application job. The arrangement ought to likewise be adaptable and dynamic, and adaptability can go. Another basis to be regarded is the deficiency of viciousness. For example, when capturing nodes, an

opponent may use information that can be used to perform other attacks, network management, and storage. Key management should identify the noncompatible nodes (NCN) and authenticate network nodes (ANN) before allocating keys. Final criteria are the upgrade and cancelation of the keys. We can give importance to the consequence of significant distribution that must be dismissed by an obsolete key or an opponent. Keys must be renewed with secure links as well and the node's guarantee that the network's connectivity has more ways to throw its information. The technique of key network allotment should be proficient of ensuring excellent network connectivity. The departure or a node capture can limit the connectivity of other nodes on the set of connections. This mechanism should consider the distribution method by suggesting new safe steps.

5.2 Discussion

WSN studied various types of distribution and key organization. Merely the dimension of the keys hoarded in the memory storage nodes in table is evaluated and the coding algorithm is not the cryptographic primary scope. Stars in the list represent a quality. We placed three or two black stars in the "connectivity" range to indicate high degrees, medium or low connectivity, respectively. In the column "Resistance to attacks," we have created three, two, and one star. The pictures are really high and middle class and resistance to counteract attacks. On the other hand, the circle in the list must provide a default. There are three or two black circles in "resources at cost savings" that indicate that the dialogs use high-, middle-, and low-cost consumption, respectively.

Experts' keys utilizing SPINS and LEAPs additionally decrease the capacity of keys in the memory of the hubs. Be that as it may, the opposition of the attacks is low. The ace key can be undermined any longer and can be undermined with the keys after the arrangement. It is the most appropriate and fastest way they can be computed through a symmetry group method. The secret keys are used to transfer other secret keys, the references to the redesign, and revocation of the equations (obviously). The issue in the asymmetric diary is very simple as the public keys don't have to be confidential. Chan et al. show probability illustration low-power consumption doesn't require a large amount of computing capability. Anyway, the key size ring accumulated in memory nodes is one of the most expensive simmers on the size of this snail memory. Type physical nodes cannot resist captures. Better connectivity between network nodes is provided by PIKE scheme, except low presentation on scalability. In the form of the schema, Tiny is ideal for the PBC asymmetries. It is defensive for the most harasses in the RCSF. The fact that setting up a special key that is shared between the two nodes aided to decrease the larger storage ability in memory. In addition, this key generates energy between the nodes that protect the time when these interventions are calculated as a result. The diagrams used by the principles of certificates and PKI are mainly cost-effective in computation and energy consumption. The difference between symmetries and inequality may vary relying

on the required intensity of the network. Let's see if the equations can be resistant to their contemporary and inequitable diagrams.

6 Conclusions

This paper presented different security threat models and security requirement along with various protocol discussions. To face those attacks, we have presented a synthesis of cryptography systems and mechanisms that can secure the WSN. The lack of infrastructure such as PKI in the WSN has compelled the nodes to not have confidence in network and to create secure paths from the source of the data to the BS. Works like [42] have used the identities of the nodes and the principle of coupling in order to reduce, or even eliminate, the interactions between nodes to counter a maximum of attacks. However, to date there are no complete and dynamic solutions easily adaptable to WSN. Present routing protocols, such as SPINS and LEAP, are maturing in steering behavior. With the model of safe routing protocols, we can offer a good research method for the extension of original protocol if we can achieve security requirements through a minor change in SRD, INTRSN, etc. This provides the overall description of the protocols and their features and also explains various security-related concerns. In addition, for the future, these researches provide us a direction.

References

1. Akyildiz, F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. *IEEE Communications Magazine, 40*(80), 102–114.
2. Binh, H. T. T., & Dey, N. (Eds.). (2018). *Soft computing in wireless sensor networks*. Boca Raton: CRC Press.
3. Das, S. K., Yadav, A. K., & Tripathi, S. (2017). IE2M: Design of intellectual energy efficient multicast routing protocol for ad-hoc network. *Peer-to-Peer Networking and Applications, 10*(3), 670–687. https://doi.org/10.1007/s12083-016-0532-6.
4. Yadav, A. K., Das, S. K., & Tripathi, S. (2017). EFMMRP: Design of efficient fuzzy based multi-constraint multicast routing protocol for wireless ad-hoc network. *Computer Networks, 118,* 15–23.
5. Das, S. K., & Tripathi, S. (2018). Intelligent energy-aware efficient routing for MANET. *Wireless Networks, 24*(4), 1139–1159. https://doi.org/10.1007/s11276-016-1388-7. Springer.
6. Das, S. K., & Tripathi, S. (2019). Energy efficient routing formation algorithm for hybrid ad-hoc network: A geometric programming approach. *Peer-to-Peer Networking and Applications, 12*(1), 102–128. https://doi.org/10.1007/s12083-018-0643-3. Springer.
7. Das, S. K., & Tripathi, S. (2018). Adaptive and intelligent energy efficient rout-ing for transparent heterogeneous ad-hoc network by fusion of game theory and linear programming. *Applied Intelligence, 48*(7), 1825–1845. https://doi.org/10.1007/s10489-017-1061-6.
8. Das, S. K., & Tripathi, S. (2017). Energy efficient routing formation technique for hybrid ad hoc network using fusion of artificial intelligence techniques. *International Journal of Communication Systems, 30*(16). https://doi.org/10.1002/dac.3340.

9. Pradhan, C., Das, H., Naik, B., & Dey, N. (Eds.). (2018). *Handbook of research on information security in biomedical signal processing*. Hershey: IGI Global.
10. Bletsas, A., & Lippman, A. (2005). Spontaneous synchronization in multi-hop embedded sensor networks: Demonstration of a server-free approach. In *IEEE* (pp. 331–341).
11. Priyadarshini, V. M., Muthukumar, N., & Natarajan, M. (2011). Cellular architecture sensor for WSNs. *IJRRSE, 01*(02), 47–51.
12. Biagioni, E., & Chen, S. H. (2004). A reliability layer for ad-hoc wireless sensor network routing. In *Proceedings of the 37th Hawaii International Conference on System Sciences* (pp. 1–8). IEEE.
13. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2001). *Wireless sensor networks: A survey* (pp. 393–422). Electrical and Computer Engineering, Georgia Institute of Technology.
14. Wong, K. H., Zheng, Y., Cao, J., & Wang, S. (2006). A dynamic user authentication scheme for wireless sensor networks. In *Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous, Trustworthy Computing* (pp. 244–251). IEEE Computer Society.
15. Collins, M., Dobson, S., & Nixon, P. (2010). A lightweight secure architecture for wireless sensor networks. *Internet Technology and Secured Transactions, 2*(1/2), 12–136.
16. Aftab, M. U., Ashraf, O., Irfa, M., Majid, M., Nisar, A., & Habib, M. A. (2015). A review study of wireless sensor networks and its security. *Communications and Network*, 172–179.
17. Men, X., Shi, X., Wang, Z., Wu, S., & Li, C. (2016). *A grid-based reliable routing protocol for wireless sensor networks with randomly distributed clusters* (pp. 41–61). International School of Software, Wuhan University.
18. Undercoffer, J., Avancha, S., Joshi, A., & Pinkston, J. (2002). Security for sensor networks. In *CADIP Research Symposium*, 1–51. http://www.cs.sfu.ca/~angiez/personal/paper/sensor-ids.pdf.
19. Carman, D. W., Krus, P. S., & Matt. B. J. (2000). *Constraints and approaches for distributed sensor network security* (pp. 1–126). Technical Report 00-010, NAI Labs, Network Associates Inc., Glenwood, MD, USA.
20. Perrig, A., Szewczyk, R., Wen, V., Culler, D. E., & Tygar, J. D. (2002). SPINS: Security protocols for sensor networks. *Wireless Networks, 8*(5), 521–534.
21. Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols*, 113–127.
22. Saxena, A., Pal, O., & Saquib, Z. (2011). Public key cryptography based approach for securing SCADA communications. *Computer Networks & Information Technologies*, 56–62.
23. Fatema, N., & Brad, R. (2013). Attacks and counterattacks on wireless sensor networks. *International Journal of Ad Hoc and Ubiquitous Computing, 4*(6), 1–15.
24. Culpepper, B. J., & Tseng, H. C. (2004). Sinkhole intrusion indicators in DSR MANETs. In *Proceedings of the First International Conference on Broad band Networks* (pp. 681–688).
25. Hu, Y.-C., Perrig, A., & Johnson, D. B. (2003) Packet leashes: A defense against wormhole attacks in wireless networks. In *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies*. IEEE INFOCOM 2003, 30 March–3 April 2003, vol. 3, pp. 1976–1986.
26. Padmavathi, G., & Shanmugapriya, D. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. *International Journal of Computer Science and Information Security, 4*(1 & 2), 1–9.
27. Xiong, N. N., Cheng, H., Hussain, S., Qu, Y. (2013). Fault tolerant and ubiquotous computing in sensor networks. *International Journal of Distributed Sensor Networks*, 1–2. Article ID 524547.
28. Huang, A. (2005, October). *Security primitives for ultra-low power sensor nodes in wireless sensor networks*. Faculty of Engineering, the Built Environment and Information Technology, University of Pretoria.
29. Gaubatz, G., Kaps, J., & Sunar, B. *Public key cryptography in sensor networks—Revisited* (pp. 1–17). Department of Electrical & Computer Engineering Worcester Polytechnic Institute, 100 Institute Road, Worcester, MA 01609, USA.

30. Szczechowiak, Piotr. (2010). *Cryptographic key distribution in wireless sensor networks using bilinear pairings*. PhD dissertation, Dublin City University.
31. Hegland, M., Winjum, E., Mjolsnes, S. F., Rong, C., Kure, O., & Spilling, P. (2006). A survey of key management in ad hoc networks. *IEEE Communications Surveys & Tutorials., 8*(3), 48–66.
32. Camtepe, S. A., & Yener, B. (2005). *Key distribution mechanisms for wireless sensor networks: A survey* (pp. 1–27).
33. Ruj, S., Nayak, A., & Stojmenovic, I. (2011). Key predistribution in wireless sensor networks when sensors are within communication range. In S. Nikoletseas & J. D. P. Rolim (Eds.), *Theoretical aspects of distributed computing in sensor networks* (pp. 787–832). Berlin: Springer.
34. Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002, September). SPINS: Security protocols for sensor networks. *Wireless Networks, 8*(5), 521–534.
35. Zhu, S., Setia, S., & Jajodia, S. (2006). LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. *ACM Transactions on Sensor Networks, 2*(4), 500–528.
36. Celozzi, C., Gandino, F., & Rebaudengo, M. (2013). *Improving key negotiation in transitory master key schemes for wireless sensor networks*. Politecnico di Torino, lecture notes of the institute for computer sciences, social informatics and telecommunications engineering (vol. 122, pp. 1–16). Cham: Springer.
37. Karlof, C., Sastry, N., & Wagner, D. (2004). TinySec: A link layer security architecture for wireless sensor networks. In *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems* (pp. 162–175). New York, NY, USA: ACM.
38. Brickell, E. F. (1993). The SKIPJACK algorithm, July, vol. 28, pp. 1–7.
39. Munivel, E., & Ajit, G. M. (2010). Efficient public key infrastructure implementation in wireless sensor networks. In *International Conference on Wireless Communication and Sensor Computing* (pp. 1–6).
40. Sakai, R., Ohgishi, K., & Kasahara, M. (2000). Cryptosystems based on pairing. In *Symposium on Cryptography and Information Security (SCIS'00)* (pp. 26–28). Japan.
41. Jing, Q., Hu, J., & Chen, Z. (2006). C4W: An energy efficient public key cryptosystem for large-scale wireless sensor networks. In *2006 IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS)* (pp. 827–832).
42. Oliveira, L. B., Aranha, D. F., Gouvêa, C. P. L., Scott, M., Câmara, D. F., López, J., & Dahab, R. (2011). TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks. *Computer Communications, 34*(3), 485–493.
43. Devi, C., Dhivya, & Santhi, B. (2013). Study on security protocols in wireless sensor networks. *International Journal of Engineering and Technology, 5*(5), 200–207.

On the Security Weaknesses in Password-Based Anonymous Authentication Scheme for E-Health Care

Rifaqat Ali, Preeti Chandrakar and Aashish Kumar

Abstract With rapid change of Internet technology, E-health care services are available for the patients at anytime and from anywhere. The patients access these services using a public channel. Therefore, the security of privacy maintaining is the prominent issue in E-health service. In order to authorize the patients, the authentication protocol plays a fundamental role in E-health system. Nowadays, a number of protocols based on mutual authentication and session key agreement have been brought before in the domain of security. Recently, Mishra et al. brought an authentication scheme for the remote user in telecare medical information system (TMIS). The claims made suggested that their scheme defends user anonymity and provides an efficient login along with smooth password change phase where wrong input could be quickly identified and the user is also provided with the facility to change password without the intervention of server. However, the authors have shown that the protocol is inadequate for real-world application because of several problems (1) Designing imperfection in login phase; (2) Designing imperfection in authentication phase; (3) Designing imperfection in change of password phase; (4) Lack of biometric update or change phase; (5) Strong replay attack, and (6) Clock synchronization problem. Moreover, we present the performance comparison taking cost comprising with communication, computation, smart card storage, and also with relevant security features.

R. Ali (✉)
Department of Computer Applications, Madanapalle Institute of Technology & Science, Madanapalle 517325, Andhra Pradesh, India
e-mail: rifaqatali27@gmail.com

P. Chandrakar · A. Kumar
Department of Computer Science & Engineering, National Institute of Technology (NIT), Raipur 492010, Chhattisgarh, India
e-mail: pchandrakar.cs@nitrr.ac.in

A. Kumar
e-mail: aashish2096@gmail.com

S. K. Das et al. (eds.), *Design Frameworks for Wireless Networks*,
Lecture Notes in Networks and Systems 82,
https://doi.org/10.1007/978-981-13-9574-1_2

1 Introduction

The existence of life on this planet depends on a few factors among them are air, food, medication, etc. Medication or health care has its inception since the primitive ages and was one of the most critical elements, which have been taken care of. There implies plenty of improvements in the way medication is delivered since the time of its inception. The recent improvement and current age of modernization have revolutionized many fields ranging from defense, communication, services, etc. and each improvement setting its own benchmark. Every service which we avail has tried to make the life of human as easy as possible. Health care is also a stream, which has seen a drastic change in the way it was earlier and how it is now. Now, an attempt is made to provide each of these services available remotely and provide the same experience with many additional benefits. It comes bundled together in the name of TMIS (Telecare Medical Information System).

TMIS consists the services such as remote diagnosis, electronic medical records, etc. Remote diagnosis is the latest service, which is extremely useful for carrying out the diagnosis from a distant location. It becomes very useful in emergencies situation and providing instant medication and support. Another milestone is EMR (an electronic medical record), which supports the remote diagnosis. The only requirement for the services is the connection with the network and authorization to access the same. TMIS architecture described in Fig. 1. Generally, the user getting authorized via biometric check, if its success then it makes access the service otherwise it is denied. The subsequent medical data capture been made via the sensors embedded in the device and update with the device, which is then encrypted and propagated across the channel and finally to the central storage. The records as per request are availed at the hospital's end, and the details are accessed after decryption and then after that, the same is decrypted again and resent across the channel and the same is reflected in the central storage and the process goes on as a service.

Each of these services addressed comprises handling of sensitive data for each individual, which needs to be kept secure from that of adversary. There are numerous other reasons to keep the records secure. To address the security, there should be a proper message hiding and encryption technique, which should be used such as ECC (Elliptic Curve Cryptography), RSA (Ron Rivest, Adi Shamir, and Len Adleman), biometrics embedding, etc. to ensure that the system remains secure. Every technique have their own pros and cons, which makes it vulnerable to attacks various kinds. The new technique, which enables security for the services should be capable enough to deal with the shortcomings of various probable attacks and make the system robust enough to combat the consequences of attack if the adversary managed to intercept the channel. At the same time, the techniques should be efficient on the front of computation and communication standards to make it feasible enough to keeping other constraints into consideration (Fig. 1).

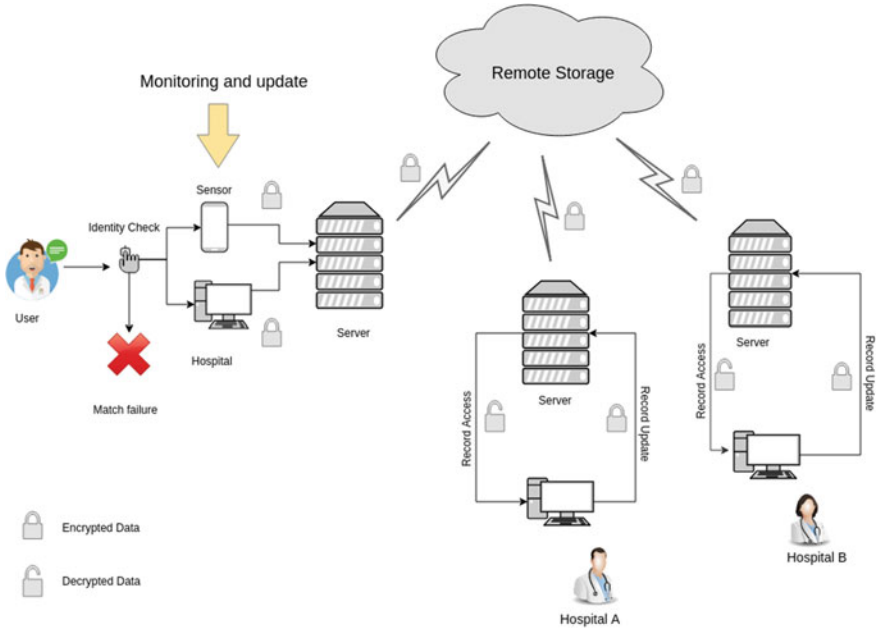


Fig. 1 TMIS workflow

1.1 Threat Model

For the sake of security, the scheme is proposed which would enable the secure transmission of information. However, the adversary always seeks an opportunity to make the attack and disrupt the smooth flow. There are few assumptions which are made before. There is no chance to seek or snoop information transmission in the reliable channel. Attempt to break one-way hash function always leads to failure. Adversary has the freedom to access monitor the data over the unreliable channel on which there would be an attempt to access transmission details. So, the protocol should be in a form that no adversary should be entertained and the transmission should be attack resistant.

1.2 Bio-hash Function

A hash function is a one-way transformation function. The hash function accepts an arbitrary length input and produces a fixed length string, which is called a hash value or a message digest.

Due to uniqueness characteristic and ability of biometric, various systems use biometric as an adopted method to solve authentication and verification problems.

However, a small change in biometric data may result in a massive change in the hash value. In other words, the result of the hash function will be changed due to the slight differences in the input and recognition errors will occur from slight biometric changes. To address this problem, a bio-function system is designed and studied [1, 2]. The bio-hash function has the following properties:

- Similar hash values are produced by the similar biometric information.
- Similar hash values are not produced by the different biometric information.
- Translation and rotation of the original biometric template should not have a substantial impact on hash values.
- Partial biometric information should be matched if sufficient detailed matters are present.

The hash function's certain class can be formulated to be everlasting to the order in which the input pattern is presented to the hash function, and such hash functions are referred to as the bio-hash function. So, the bio-hash function can solve the recognition error of general hash function and can authenticate a legitimate user even if the user's biometric information slightly change.

1.3 Contribution

In 2015, Mishra et al. [3] proposed an improved user authentication protocol for TMIS. They claimed that their scheme has the following merits: (i) efficient login phase and password change phase, (ii) Achieve user anonymity, (iii) Provide mutual authentication and Session key agreement, and (iv) Performance comparison with other similar schemes. We have pointed out several security weaknesses in Mishra et al.'s scheme such as Designing Imperfection in login phase, Designing Imperfection in authentication phase, Designing Imperfection in password change phase, Lack of biometric update or change phase, Strong replay attack, and Clock synchronization problem. The performance comparison of the other schemes is also made with which other protocols provide the overview about the respective protocol's feasibility. We even propose the future scope, which the field of security.

1.4 Organization of This Article

The chapter has been in the organized in the following manner. In Sect. 2, the details about the related literature work is discussed, which describes about the similar works and their respective contribution in the domain. The next Sect. 3 details about the Mishra et al.'s [3] scheme and summary of each phase involved in the scheme. Section 4 details about the cryptanalysis of the scheme and pointed out the flaws present in the scheme. Section 5 brings the performance comparison of scheme with the latest

protocols based on the parameter as storage cost, communication, and computation costs. We also address the future scope in Sect. 6 comprising of what the sector might hold. Finally, we arrive at the conclusion in Sect. 7.

2 Literature Review

The area of security is an active area of research and there has been numerous works in this area. After the first-ever authentication-based protocol was proposed in 1981 by Lamport [4] for which password was used for authentication. Many recent works have done in succession [3, 5–13] and few recent ones have been discussed here.

In 2015, Arshad et al. [5] brought an improvement to Bin Muhaya's [14] scheme, which was found to be prone to offline password guessing attack and which even fails in providing the perfect forward secrecy. Improvement provided led to an improvement in computation time by 2.73 times. In 2016, Wazid et al. [15] brought a complete analysis of the security requirements keeping the services into consideration. The analysis provides the mathematical review of methods used along with their future scope of improvement that should be addressed in the near future. Also, Aslam et al. [16] in 2016 proposed a complete summary of the related scheme proposed based on one, two, and three factors with their respective pros and cons. It also points the probable attacks and mathematical requirements to implement these security measures. The analysis enables complete comparison based on features and respective drawbacks wrt to each proposed scheme is made.

Again in 2016, Jiang et al. [17] brought an enhancement to Wu et al. [18] proposed a protocol, which relies on 3-factor remote authentication and which found a vulnerability in offline password guessing, and at the same time prone to user impersonation attack. Additionally, it failed to provide a recovery mechanism if the smart card is lost or stolen. Another proposal was by Wazid et al. [19] which was again an improvement to Amin and Biswas [20] scheme of 2015 who proposed a 3-factor authentication scheme and which was found to be vulnerable to many potholes as privileged-insider attack, replay attack, along with user and server impersonation attack and even stolen smart card attack. Improvement addressed drawbacks and ensured that the scheme is shielded to attack as stated.

In 2017, Jiang et al. [21] brought an improvement to Lu et al. [22] scheme, which relies on 3-factor authentication scheme and claims to be secure from attacks but fails in identity guessing, tracking attack, identity revelation, offline password guessing, and impersonation attack with both user and server. The scheme makes improvements in the drawbacks addressed earlier at the same time making it a balance between security and efficiency. In 2017, again, Wu et al. [23] brought before RFID-based scheme, which enables both forward and backward untraceability. Also, it enables keeping the details of tag and reader anonymous. The scheme meets all the required security milestones and at the same time is applicable for usage across the services.

In 2017, authentication scheme which was based on human biometrics was brought by Jung et al. [24], which was an improvement to Liu et al.'s [25] proposed

scheme in 2016, which used a biometric-based encryption scheme for health care but suffers numerous vulnerabilities as improper identification based on biometrics, spoofing attack and also fails to provide session key verification. The improvement provided by the protocol ensures that the system is secure with these loopholes mentioned in Liu et al. [25] scheme with security being enhanced. In 2017 again, Chatterjee et al. [26] provided an approach to carry out the authentication by setting the access control to the particular users as per requirement. It enables making group-based authentication scheme, which resists attacks and ensures data secrecy.

Another addition was by Mohit et al. [27] in 2017, which was an improvement to cloud-based Chiou et al.'s [28] scheme, which enables the patient and hospital to upload the data to the server which hereby could be used by the doctor for treatment and after further changes could be pushed to the server. It has its own flaw in the name of failing to preserve anonymity and safety against the stolen attack. The contribution of Mohit et al. [27] removes the drawback and improves communication and computation overheads.

In 2018, Kumar et al. [29] found that proposed Mohit et al.'s [27] protocol is a cloud-based system for mutual authentication in the domain of health care. It was found that the scheme has the drawbacks as stolen verifier attack, and many logged into the patient attack, impersonation attack, and failure for session key protection. These attacks are eradicated by Kumar et al. [29] and also improvement in computation and communication overheads. Again in 2018, Li et al. [30] brought before a cloud-based medical service where patients could securely use the service keeping privacy maintained. The scheme is even compared with protocols proposed earlier in a similar direction and proves that the scheme is shielded against the attack and provides a better computation, which makes the scheme practical for usage in cloud-based systems.

3 Overview of Mishra et al. [3] Protocol

We have summarized Mishra et al.'s [3] scheme. It has phases as registration, login, verification, password change, and smart card revocation phase, respectively. The used notations here are addressed in Table 1.

For initializing the system, first, the server S makes a choice for two prime numbers i and j of length 1024 bits, it then calculates n = ij. Then select a prime p and integer X in the form that $pX \equiv 1 \bmod (i-1)(j-1)$. Where i, j, and X are kept as secret while n and p published as public.

3.1 Registration Phase

Here, whenever a new user makes registration. He/she performs the below mentioned steps (Table 2).

Table 1 Meaning of symbols and notations of this manuscript

Notation	Description
U	User
RC	Registration center
S	Server
E	An adversary
ID	User identity
PW	U password
SC	Unique serial number of smart card
B	U's biometric key
X	S's secret(master) key
$h(.)$	Hash function
$H(.)$	Bio-hash function
N_c	U random nonce
N_s	S random nonce
$\|$	Concatenation operator
$\oplus$	*XOR* operator
SK	Session key

Step1: The new user U makes a choice for identity ID and password PW with full liberty. Then, submit the request for registration to the medical server with ID.

Step2: On receiving the request for registration by user U, S checks the uniqueness of ID. If it fails, then the session is aborted. Otherwise, allocates unique SC, it then calculates $J = h(X \parallel ID \parallel N \parallel SC)$, where SC is the unique serial number of smart card and take N = 0 if user is new, else set N to N + 1.

Step3: The S stores values as $\{J, n, e, h(.)\}$ in the smart card and sends smart card to user U. In addition, S keeps record of patient which is stored in the database and the new entry (ID, RID) is added in the database, where $RID = (N \parallel SC \parallel T_r)$ and T_r is the time of registration.

Step4: After the smart card is received, the user U gives biometrics B and calculates $L = J \oplus h(ID \parallel PW)$ & $V = h(ID \parallel H(B) \parallel PW)$, where H is a function which performs bio-hash. Then, swap the parameter L with J and then store the value V in the smart card. At the end, the smart card holds values as $\{V, L, n, e, h(.)\}$.

3.2 Login Phase

Here, whenever the user requires to avail the service, it logs into server, then insertion of smart card into a smart card reader and then the identity ID, password PW, and imprints biometric B as input.

Table 2 Comparison of related works with cryptographic method, their highlights, and year of work

Scheme	Cryptographic method	Highlights	Year
Arshad et al. [5]	ECC	Improvement of Bin Muhayas scheme Faster computation 2.73 times	2015
Wazid et al. [15]	–	Protocols analysis along with their scope of improvement	2016
Aslam et al. [16]	–	Protocol analysis based on one-, two-, or three-factor for authentication with their respective pros and cons Probable attacks and drawbacks known	2016
Jiang et al. [17]	ECC	Improvement to Wu et al. scheme Vulnerabilities due to attacks removed	2016
Wazid et al. [19]	ECC	Improvement to Amin-Biswas scheme Removal of vulnerabilities as replay, user and server impersonation and stolen smart card attack	2016
Jiang et al. [21]	ECC	Improvement to Lu et al. scheme Shield against vulnerabilities as identity guessing, tracking, identity revelation, online password guessing, user and server impersonation attacks	2017
Wu et al. [23]	–	RFID-based scheme which enables untraceability Enables keeping the details of tag and reader anonymous	2017
Jung et al. [24]	ECC	Improvement to Liu et al. scheme Biometric-based authentication Vulnerabilities removal as improper identification, spoofing attack and fails to provide session key verification	2017
Chatterjee et al. [26]	Key policy attribute-based encryption	Authentication by setting access control levels Group-based authentication scheme which resists attacks and enables secrecy	2017
Mohit et al. [27]	Digital signatures	Improvement to cloud-based Chiou et al. scheme Removes drawback and improvement in communication and computation overheads	2017
Kumar et al. [29]	Digital signatures	Improvement to Mohit et al. Vulnerabilities removal as stolen verifier, many patient logged in, user and server impersonation, and failure for session key protection attack	2018
Li et al. [30]	ElGamal signature scheme	Cloud-based medical service usage keeping privacy maintained Secure against probable attack and better computation	2018

Step1: Check for $V == h(ID \parallel H(B) \parallel PW)$. If this condition evaluates to false, the session is then aborted. Else, find $J = L \oplus h(ID \parallel PW)$.

Step2: Choose a random number r_u and find $A = J^{r_u} \bmod n$ & $C_u = h(ID \parallel A \parallel J \parallel T_u)$, then put forwards the login message AID to the S, here and T_u is latest timestamp.

3.3 Verification Phase

Here, both server and user checks the legitimacy of one another and a session key is created for safe transmission of information. Following are the steps involved in verification phase.

Step1: After receiving the message AID, the S calculates $AID^X \bmod n$ and gets $(ID \parallel T_u \parallel A \parallel C_u)$. It takes out the entry $RID = (N \parallel SC \parallel T_r)$ which is equivalent to ID in the recorded table. Next, S checks if $T_u > T_r$. The S then calculates $J = h(X \parallel ID \parallel N \parallel SC)$ and checks if $C_u =?h(ID \parallel A \parallel J \parallel T_u)$. If it fails, the session is terminated. Else, U is identified by S. Furthermore, replacement of RID with $RID^* = (N \parallel SC \parallel T_u)$ is made by S.

Step2: The S makes a choice for random number r_s and computes $D = J^{r_s} \bmod n$, $K_{us} = A^{r_s} \bmod n = J^{r_u r_s} \bmod n$. It then calculates the session key $sk_{us} = h(ID \parallel K_{us} \parallel J \parallel T_u)$ and $C_s = h(ID \parallel sk_{us} \parallel D \parallel T_u)$. At last, S assumes sk_{us} as session key and shares the message as $< D, C_s >$ with user U.

Step3: After the message is received, i.e., $< D, C_s >$, the smart card calculates $K_{su} = D \bmod n = J^{r_s r_u} \bmod n$ and also the session key $sk_{su} = h(ID \parallel K_{su} \parallel J \parallel T_u)$ and also calculate $C_s^{'} = h(ID \parallel sk_{su} \parallel D \parallel T_u)$. Now, check $C_s^{'} =?C_s$. If this condition fails, then terminate the session. Else, S identified by U. Both U and S agree on session keys sk_{us} and sk_{su}, i.e., $K_{us} = J^{r_s r_u} \bmod n = J^{r_u r_s} \bmod n$.

3.4 Password Change Phase

Here, the user is provided with facility to alter password without the aid of server.

Step1: The user U now adds smart card in the reader and then gives biometric B. Again, input for ID, PW, and new password PW_{new} is made.

Step2: The next smart card checks for $V == h(ID \parallel H(B) \parallel PW)$. If this check fails then the session is terminated. Else, calculate $J = L \oplus h(ID \parallel PW)$.

Step3: Then, smart card calculates $L_{new}=J \oplus h(ID \parallel PW_{new})$ and $V_{new}=h(ID \parallel H(B) \parallel PW_{new})$. Replacement of L with L_{new} and V with V_{new} is made.

3.5 Smart Card Revocation Phase

Here, the revocation of smart card is made if the same is lost or damaged by any such reason. Then, the smart is provided by the seever when the request is made.

Step1: The U makes a request to avail a new smart card to S along with an identity ID.

Step2: The S checks for the identity of U. If the U is not genuine or if ID is invalid, the session is then aborted. Else, we head toward the very next step.

Step3: The server S takes out $RID = (N \parallel SC)$ which is similar to ID in stored database.

Step4: S then frames the user specific smart card for U by storing the values $\{J_{new}, n, e, h(.)\}$ in it, where $J_{new} = h(X \parallel ID \parallel N + 1 \parallel SC_{new})$ and SC_{new} is new serial number of the smart card. Then, the smart card is sent to user U through a safe channel and replacement of RID with RID_{new}, where $RID_{new} = (N + 1 \parallel SC_{new})$ is made.

Step5: After gaining smart card, U performs **Step4** of registration phase.

4 Cryptanalysis of Mishra et al. [3] Scheme

4.1 Designing Imperfection in Login Phase

In the phase of login, the verification of $V == h(ID \parallel H(B) \parallel PW)$ will never be obtained because of the bio-hash function $H(.)$ is not present in smart card's memory. So, smart card reader cannot compute $H(B)$. Therefore, without the correct value of $H(B)$, the password verification, i.e., $V = h(ID \parallel H(B) \parallel PW)$ always turns out to be false. Further, computation of $J = L \oplus h(ID \parallel PW)$, $A = J^{r_u} \bmod n$ & $C_u = h(ID \parallel A \parallel J \parallel T_u)$ is done by smart card, which contains the value old identity and password. Therefore, the value of J, A, C_u is not correct without using proper value of identity and password. As a result, login message AID is incorrect. It is clear from the above explanation, Mishra et al.'s [3] scheme fails to verify identity, password, and biometric. This is a very severe drawback in Mishra et al. [3] scheme.

4.2 Designing Imperfection in Authentication Phase

In authentication, denial-of-service (DoS) attack can cause a permanent error on authentication by introducing unexpected data during the procedures of authentication. User U fails to login into the server using valid identity and password owing to the flaw in the authentication phase. This implies that inefficiency in the authentication phase would result in denial-of-service attack. An adversary may perform denial-of-service attack to cause the server to reject the login of a specific user. In Mishra et al.'s [3] protocol, the authentication phase has some design flaws, which is described as follows.

Step1: Let's suppose that user has lost smart card in some way. The user now wants to make the recovery of smart card then the user executes the smart card revocation phase.

Step2: After successful execution of smart card revocation phase, $RID = (N \parallel SC \parallel T_r)$ is replaces with $RID_{new} = (N + 1 \parallel SC_{new})$ and stores RID_{new} into the database.

Step3: In the next login session, the user shares the request for login via message $AID = (ID \parallel T_u \parallel A \parallel C_u)^e \bmod n$ to the server, where T_u is the current login time stamp.

Step4: After the message is received from user, the server in the beginning checks for the novelty of timestamp $T_u > T_r$. After execution of the phase of revocation, the timestamp T_r is not stored in the database. So, the server cannot retrieve the timestamp T_r. Therefore, the server fails to verify the uniqueness of the timestamp and the session is aborted.

4.3 Designing Imperfection in Password Change Phase

In Mishra et al.'s [3] protocol, the same signs of imperfection was found in password change phase as in that of login phase. In password change phase also, the verification is a failure because the bio-hash function is not present in the smart card. So, the reader always fails in verifying the password, identity, and biometrics as well. As a result, inefficient password change phase results in denial-of-service attack. Denial-of-service attack is a decisive attack, where the adversary can use some methods to work upon the server so that the legitimate user's access requests will be denied by the server. An attacker can modify the false verification information of a valid user for the next login phase. Afterward, the valid user will not access the server anymore. So, any illegal person could make changes in the user's password in the following manner.

Step 1: If attacker gains the smart card of user by some method and attempts to change the password of user.

Step 2: He/she then enters a random identity, password, and gives biometric B. After that, reader performs the verification but we know that this password verification always fails. So, a user U is re quested to give a new password PW_{new}.

Step 3: Attacker enters new password PW_{new} and smart card calculates $L_{new} = L \oplus h(ID \parallel PW) \oplus h(ID \parallel PW_{new})$ and $V_{new} = h(ID \parallel H(B) \parallel PW_{new})$. Then, replace its L with L_{new} and V with V_{new}.

Step 4: So, the attacker could change the legal user's password and after that legitimate user would not able to access his/her own account.

The above discussion shows that the Mishra et al.'s [3] scheme has an inefficient phase of password, which also leads to DoS attack.

4.4 Lack of Biometric Update or Change Phase

The biometrics update requires because the biometrics has the problem of the aged deterioration. The most prominent properties in a authentication scheme using biometrics is that a legitimate user should be provided with the opportunity to change or update old password along with biometrics. Mishra et al.'s [3] scheme fails to provide biometric update or change phase.

4.5 Strong Replay Attack

In this attack, an attacker tries to be a legal user by retransmitting the previous executed messages to the desire entity. In Mishra et al.'s [3] protocol, in log-in phase, message $AID = (ID \parallel T_u \parallel A \parallel C_u)^e \bmod n$ is calculated on the patient's end and transmission of this message is made to the server across the public channel, where $A = J^{r_u} \bmod n$ and $C_u = h(ID \parallel A \parallel J \parallel T_u)$, where ID is patient's identity and T_u is current timestamp. It can be shown that Mishra et al. [3] protocol is susceptible to strong replay attack due to following reasons.

Step1: Suppose that the login message AID has intercepted by the attacker and retransmits after a short duration of time.

Step2: Upon obtaining the message from the attacker, the server first decrypts the message AID using the secret key d and retrieves $(ID \parallel T_u \parallel A \parallel C_u)$. Subsequently, server checks the novelty of time interval, i.e., $T_u > T_r$. But T_r does not exist in the database because in the previous user's authentication session, T_r is replaced with T_u. Therefore, the condition $T_u > T_r$ never obtained and server fails to check the originality of the timestamp.

Step3: Afterward, server calculates $J = h(X \parallel ID \parallel N \parallel SC)$ and checks if $C_u = h(ID \parallel A \parallel J \parallel T_u)$ and this condition always holds because AID is a valid message given by the genuine user. Therefore, the adversary is successful to login into the remote server using the previously intercepted message AID.

4.6 Clock Synchronization Problem

Any mutual authentication scheme is avoided from attacks as replay and man in middle with the help of timestamps. Unfortunately, clock synchronization problem [24, 26] arises using timestamp in huge networks like wide area networks, mobile communication, and satellite communication networks. The number of schemes depend on timestamp can resist replay attack by means of systems's timestamp provided the system clock must be synchronized; otherwise, the scheme will not work accurately. Through the network environments and transmission delay is not predictable, the possible replay attack is found in all the existing schemes those used timestamp.

According to the aforementioned explanation, Mishra et al. [3] scheme depends on timestamps. Definitely, it would face the clock synchronization problem.

5 Performance Comparison

To measure the feasibility of the protocol, it is mandatory to analyze the performance in the form of required storage requirement, communication cost, and computation cost. For comparison, a series of protocols in the related domain is taken as represented in Table 3 below.

In Table 4 below, the comparison of the protocol with their respective costs are made. For memory requirement analysis, standards assumed are IDs and timestamps taking 32 bits, random nonce of 64 bits, one-way hash function requiring 256 bits, bio-hash function requiring 160 bits, elliptic curve point consumes 320-bits, and for encryption or decryption, it requires 512 bits. In the comparison of the storage requirements, the cost comprises of storage in database and smart card if protocol makes use of it. Taking protocol P1, the storage requirement in database is of {ID_i, n_i = 96 bits} and for smart card storage, it requires {V_i, K_i, xP, l, h(.), H(.) = 832 bits}. Again, in the similar fashion, the storage requirement for the protocols P2, P3, P4, P5, P6, and P7 are {704 = (256 * 2 + 32 + 160), 672 = (160 * 3 + 32), 1248 = (256 * 3 + 160 * 3), 1216 = (512 + 256 * 2 + 64 * 3), 1280 = (512 * 2 + 256), and 1440 = (256 * 4 + 160 + 512)} bits, respectively.

Again, on the communication front, the requirement is because of the messages shared across the channel to achieve mutual authentication among the participants. Taking protocol P1 messages shared are M1{d_sP = 320 bits}, M2{AID_i, M_1, M_2} = 832 bits, and M3 {M_3 = 256 bits}. Collectively comprising of 1408 bits. Similarly, for P2, P3, P4, P5, P6, and P7 requirement is of {1344, 1442, 1696, 2464, 2240, 2496} bits, respectively.

For calculation of computation cost, the timing requirement for each operation is considered. The operations as hash function, symmetric key encryption, point multiplication, point addition, fuzzy extraction, modular exponentiation, inverse, and bio hashing represented by {T_H,T_S,T_{PM},T_{PA},T_{FE}, T_{ME}, T_{INV}, T_{BH}} whose operation

Table 3 Representation of protocols

Representation	Protocol
P1	Jiang et al. [21]
P2	Qiu et al. [31]
P3	Xu et al. [32]
P4	Arshad et al. [5]
P5	Ostad et al. [33]
P6	Chaudhry et al. [34]
P7	Wazid et al. [19]

Table 4 Comparison of various cost with other protocols

Parameter	P1	P2	P3	P4.	P5	P6	P7
Storage (bits)	928	704	672	1248	1216	1280	1440
Communication (bits)	1408	1344	1442	1696	2464	2240	2496
Computation time	$16T_H + 4T_{BH} + 6T_{PM} + 1T_{INV}$	$18T_H + 4T_{PM}$	$16T_H + 6T_{PM}$	$14T_H + 6T_{PM}$	$26T_H + 5T_{PM} + 2T_{PA} + 3T_S$	$19T_H + 7T_{PM} + 7T_S + 2T_{BH}$	$21T_H + 3T_{PM} + 3T_S + 2T_{FE}$
Time (s)	0.470175	0.2613	0.338645	0.38695	0.35499	0.5519	0.351975

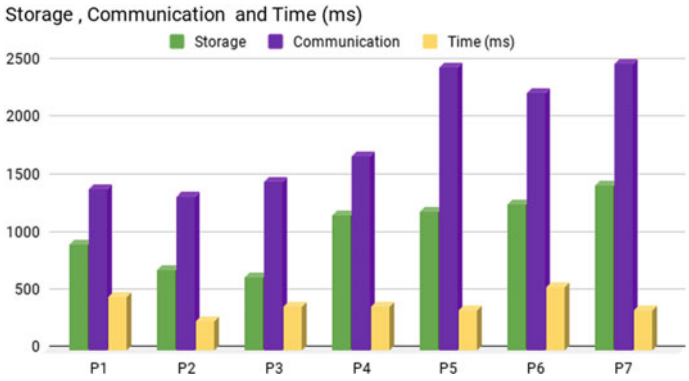


Fig. 2 Storage cost, communication cost, and time comparison chart

Table 5 Feature comparison of protocols

Feature	P1	P2	P3	P4	P5	P6	P7
User anonymity	✓	✓	✓	✓	✓	✓	✓
Impersonation attack	✓	✓	✓	✓	✓	✓	✓
Mutual authentication	✓	✓	✓	✓	✓	✓	✓
Known key security	✓	✓	✗	✓	✗	✗	✓
Perfect forward secrecy	✓	✓	✓	✓	✓	✓	✓
Replay attack	✓	✓	✓	✓	✓	✓	✓
Man-in-middle attack	✓	✓	✓	✓	✓	✓	✓
Offline password guessing attack	✓	✓	✓	✓	✓	✓	✓
Denial-of-service attack	✗	–	–	–	✓	✗	✗

time and corresponding values are (0.0005, 0.0087, 0.063075, 0.000262, 0.063075, 0.522, 0.003725, 0.02 s), respectively. Taking protocol P1, the operations being performed are $16T_H$,$4T_{BH}$, $6T_{PM}$, and 1 TT_{INV} which sums up the entire timing requirement to {16 * 0.0005 + 4 * 0.02 + 6 * 0.063075 + 0.003725 = 0.470175 s}. Similarly, for P2, P3, P4, P5, P6, and P7 requirement is of {0.2613, 0.338645, 0.38695, 0.35499, 0.5519, 0.351975} sec, respectively.

The graphical representation in Fig. 2 below shows the comparison of the protocol when their respective costs is made.

Now, in Table 5 below, the feature comparsion of the protocols is been made with the features which one protocol provides and the other fails to address. The properties such as Mutual authentication, Non-repudiation, User anonymity, Perfect forward secrecy, Biometrics protection, and attacks as Man in middle, Impersonation, Replay attack, Offline password guessing, and Denial of service are considered here.

6 Future Scope

There has been a series of modifications in the protocol itself after the first protocol by Lamport [4] was proposed. The changes have come in the name of factors used ranging from passwords, smart card, and biometrics. They have been successful in providing the security from the numerous attacks but in the upcoming scenario, there have to be some added ways to tackle the security issues. In the future scope, there could be an increase in the biometrics being used for authentication say multiple biometrics. The next scope could be in the name of usage wearable devices which could provide the authentication thus eradicating the use of passwords and ID for authentication. The improvement could be even in the name of usage of hashing function and its implementation which could reduce the computation time as well as the number bits involved. The dependency on any such equipment as the smart card and its reader should be reduced taking into account the capacity of the system to be fault tolerant with smart card and even the server as well.

7 Conclusion

In this work, E-health care domain is addressed with its security implications and taking into account the protocol given by Mishra et al. The overview of the protocol is addressed and a lot of security loopholes in the protocol for respective phases and also prone to some attacks. The security comparison of the similar protocols has been made so that the analysis of the feasibility of the same could be made. There has been a discussion on the scope in the domain of security and with that of added feature and characteristics, which could be utilized to come up with the feasible yet dealing with all the loopholes which could erupt in the time to come.

References

1. Chaki, J., Dey, N., Shi, F., & Sherratt, R. S. (2019, January 24). Pattern mining approaches used in sensor-based biometric recognition: A review. *IEEE Sensors Journal*.
2. Dey, N., Nandi, B., Dey, M., Biswas, D., Das, A., & Chaudhuri, S. S. (2013, February 22). BioHash code generation from electrocardiogram features. In *2013 3rd IEEE International Advance Computing Conference (IACC)* (pp. 732–735). IEEE.
3. Mishra, R., & Barnwal, A. K. (2015). A privacy preserving secure and efficient authentication scheme for telecare medical information systems. *Journal of Medical Systems*, *39*(5), 54.
4. Lamport, L. (1981). Password authentication with insecure communication. *Communications of the ACM*, *24*(11), 770–772.
5. Arshad, H., Teymoori, V., Nikooghadam, M., & Abbassi, H. (2015). On the security of a two-factor authentication and key agreement scheme for telecare medicine information systems. *Journal of Medical Systems*, *39*(8), 76.

6. Ali, R., & Pal, A. K. (2017). Three-factor-based confidentiality-preserving remote user authentication scheme in multi-server environment. *Arabian Journal for Science and Engineering*, *42*(8), 3655–3672.
7. Ali, R., Pal, A. K., Kumari, S., Karuppiah, M., & Conti, M. (2018). A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring. *Future Generation Computer Systems*, *84*, 200–215.
8. Ali, R., & Pal, A. K. (2018). An efficient three factorbased authentication scheme in multiserver environment using ECC. *International Journal of Communication Systems*, *31*(4), e3484.
9. Ali, R., & Pal, A. K. (2017). A secure and robust three-factor based authentication scheme using RSA cryptosystem. *International Journal of Business Data Communications and Networking (IJBDCN)*, *13*(1), 74–84.
10. Chandrakar, P., & Om, H. (2017). Cryptanalysis and extended three-factor remote user authentication scheme in multi-server environment. *Arabian Journal for Science and Engineering*, *42*(2), 765–786.
11. Chandrakar, P., & Om, H. (2017). A secure and robust anonymous three-factor remote user authentication scheme for multi-server environment using ECC. *Computer Communications*, *110*, 26–34.
12. Chandrakar, P., & Om, H. (2017). Cryptanalysis and improvement of a biometricbased remote user authentication protocol usable in a multiserver environment. *Transactions on Emerging Telecommunications Technologies*, *28*(12), e3200.
13. Chandrakar, P., & Om, H. (2018). An efficient two-factor remote user authentication and session key agreement scheme using Rabin cryptosystem. *Arabian Journal for Science and Engineering*, *43*(2), 661–673.
14. Bin Muhaya, F. T. (2015). Cryptanalysis and security enhancement of Zhu's authentication scheme for Telecare medicine information system. *Security and Communication Networks*, *8*(2), 149–158.
15. Wazid, M., Zeadally, S., Das, A. K., & Odelu, V. (2016). Analysis of security protocols for mobile healthcare. *Journal of Medical Systems*, *40*(11), 229.
16. Aslam, M. U., Derhab, A., Saleem, K., Abbas, H., Orgun, M., Iqbal, W., et al. (2017). A survey of authentication schemes in telecare medicine information systems. *Journal of Medical Systems*, *41*(1), 14.
17. Jiang, Q., Khan, M. K., Lu, X., Ma, J., & He, D. (2016). A privacy preserving three-factor authentication protocol for e-Health clouds. *The Journal of Supercomputing*, *72*(10), 3826–3849.
18. Wu, F., Xu, L., Kumari, S., & Li, X. (2015). A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client–server networks. *Computers & Electrical Engineering*. https://doi.org/10.1016/j.compeleceng.2015.02.015.
19. Wazid, M., Das, A. K., Kumari, S., Li, X., & Wu, F. (2016). Design of an efficient and provably secure anonymity preserving threefactor user authentication and key agreement scheme for TMIS. *Security and Communication Networks*, *9*(13), 1983–2001.
20. Amin, R., & Biswas, G. P. (2015). A secure three-factor user authentication and key agreement protocol for TMIS with user anonymity. *Journal of Medical Systems*, *39*(8), 1–19.
21. Jiang, Q., Chen, Z., Li, B., Shen, J., Yang, L., & Ma, J. (2018). Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems. *Journal of Ambient Intelligence and Humanized Computing*, *9*(4), 1061–1073.
22. Lu, Y., Li, L., Peng, H., & Yang, Y. (2015). An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem. *Journal of Medical Systems*, *39*, 32. https://doi.org/10.1007/s10916-015-0221-7.
23. Wu, F., Xu, L., Kumari, S., Li, X., Das, A. K., & Shen, J. (2018). A lightweight and anonymous RFID tag authentication protocol with cloud assistance for e-healthcare applications. *Journal of Ambient Intelligence and Humanized Computing*, *9*(4), 919–930.
24. Jung, J., Moon, J., & Won, D. (2017). Robust biometric-based anonymous user authenticated key agreement scheme for telecare medicine information systems. *KSII Transactions on Internet and Information Systems, 11*(7), 3720–3746. https://doi.org/10.3837/tiis.2017.07.023.

25. Liu, W., Xie, Q., Wang, S., & Hu, B. (2016). An improved authenticated key agreement protocol for telecare medicine information system. *SpringerPlus, 5*(1), 555. Article (CrossRef Link).
26. Chatterjee, S., Roy, S., Das, A. K., Chattopadhyay, S., Kumar, N., Reddy, A. G., et al. (2017). On the design of fine grained access control with user authentication scheme for telecare medicine information systems. *IEEE Access, 5*, 7012–7030.
27. Mohit, P., Amin, R., Karati, A., Biswas, G. P., & Khan, M. K. (2017). A standard mutual authentication protocol for cloud computing based health care system. *Journal of Medical Systems*, *41*(4), 50.
28. Chiou, S. Y., Ying, Z., & Liu, J. (2016). Improvement of a privacy authentication scheme based on cloud for medical environment. *Journal of Medical Systems*, *40*(4), 1–15.
29. Kumar, V., Jangirala, S., & Ahmad, M. (2018). An efficient mutual authentication framework for healthcare system in cloud computing. *Journal of Medical Systems*, *42*(8), 142.
30. Li, W., Zhang, S., Su, Q., Wen, Q., & Chen, Y. (2018). An anonymous authentication protocol based on cloud for telemedical systems. In *Wireless communications and mobile computing*.
31. Qiu, S., Xu, G., Ahmad, H., & Wang, L. (2018). A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems. *IEEE Access*, *6*, 7452–7463.
32. Xu, X., Zhu, P., Wen, Q., Jin, Z., Zhang, H., & He, L. (2013). A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems. *Journal of Medical Systems*, *38*, 1–7.
33. Ostad-Sharif, A., Abbasinezhad-Mood, D., & Nikooghadam, M. (2019). A robust and efficient ECC-based mutual authentication and session key generation scheme for healthcare applications. *Journal of Medical Systems*, *43*(1), 10.
34. Chaudhry, S. A., Khan, M. T., Khan, M. K., & Shon, T. (2016). A multiserver biometric authentication scheme for tmis using elliptic curve cryptography. *Journal of Medical Systems*, *40*(11), 230.

Integrated Probabilistic Relevancy Classification (PRC) Scheme for Intrusion Detection in SCADA Network

S. Shitharth, K. Sangeetha and B. Praveen Kumar

Abstract Detecting and identifying intrusions in a network is a challenging research area in the network security domain. Intrusion detection plays an essential role in computer network security since long. An Intrusion Detection System (IDS) is mainly used to detect an unauthorized access to a computer system or network. Moreover, it is capable to detect all types of malicious and harmful attacks in a network. The drawbacks of existing IDS are it can detect only the known attacks and it produces a large number of false alarms due to the unpredictable behavior of users and networks. It also requires extensive training sets in order to characterize the normal behavior of the nodes. In order to overcome these issues, an integration of Hidden Markov Model (HMM)–Relevance Vector Machine (RVM) algorithm namely, Probabilistic Relevance Classification (PRC) is proposed to detect intrusions in Supervisory Control and Data Acquisition (SCADA) network. Here, the power system attack dataset is used to detect the attacks in an SCADA network. In the preprocessing stage, the given data is preprocessed to segregate the relays as R1, R2, R3n and R4. Each relay contains the date, timestamp, control panel log report, relay log report, snort log report, marker, fault location, and load condition information. Then, the Boyer—Moore (BM) technique is employed to perform the string matching operation. After that, the PRC technique is implemented to classify the attack as known or unknown. The novelty of this paper is it manually trains the data and features for unknown attacks. The main intention of this work is to reduce the set of features, amount of database, and to increase the detection rate. The experimental results evaluate

S. Shitharth (✉)
Department of CSE, Vardhaman College of Engineering, Hyderabad, India
e-mail: shitharth.it@gmail.com

K. Sangeetha
Sri Satya Sai University of Technology & Medical Sciences, Madhya Pradesh, India
e-mail: sange0391@gmail.com

B. Praveen Kumar
Bharat Institute of Engineering and Technology, Hyderabad, India
e-mail: praveenbala038@gmail.com

S. K. Das et al. (eds.), *Design Frameworks for Wireless Networks*,
Lecture Notes in Networks and Systems 82,
https://doi.org/10.1007/978-981-13-9574-1_3

the performance in terms of False Acceptance Rate (FAR), False Rejection Rate (FRR), Genuine Acceptance Rate (GA), sensitivity, specificity, accuracy, error rate, and recall.

Keywords Boyer–Moore (BM) · Intrusion Detection System (IDS) · Hidden Markov Model—Relevance Vector Machine (HMM-RVM) · Power system attack dataset · Supervisory Control and Data Acquisition (SCADA) · Support Vector Machine (SVM) · Probabilistic Relevancy Classification (PRC)

1 Introduction

In today's era, Internet becomes a part of our business network and everyone in the highly competitive market wants to use the internet for their benefits. Corporate companies use Internet to develop their business by communication and an individual use the internet for social and personal objectives. Apart from that, attacks from Internet can abolish the great benefits of the internet. If the database is stolen, the web application is compromised or the server is disrupted, the underlying system suffers critically. So, the intrusion is harmful and one of the most wanted things in network security. Detecting and classifying intrusions and attacks in Supervisory Control and Data Acquisition (SCADA) network is one of the challenging tasks. It is a specialized computer network that provides an interconnection for field devices such as sensors and actuators, which are controlled by either a Personal Computer (PC) or Programmable Logic Controller (PLC). This network is usually connected with the outside corporate networks by using the specialized gateways. Moreover, the SCADA controls and monitors site over a long distance by having a specific firewall rules and password policies to attain a high level of security. An Intrusion Detection System (IDS) is mainly used to detect the harmful intrusions in a network. It acts like a sniffer that monitors the traffic in a network in promiscuous mode. Here, the network packets are collected and analyzed for rule violations with the help of pattern recognition. Generally, this process can be done in two ways such as

(1) Signature-based IDS
(2) Anomaly-based IDS.

In signature-based IDS, it generates a signature based on the characteristics of previously known attacks. But in anomaly-based IDS, it detects previously undocumented intrusions. Normally, the IDS consider the collection of objects, events, records, samples, and entities as input. Figure 1 shows the general architecture of IDS. It monitors the entire network, if there is any change in a network then the IDS will detect and block the intrusions.

The processing stages of IDS is shown Fig. 2, which includes

(1) Strategy,
(2) Response,
(3) Detection,
(4) Preparation.

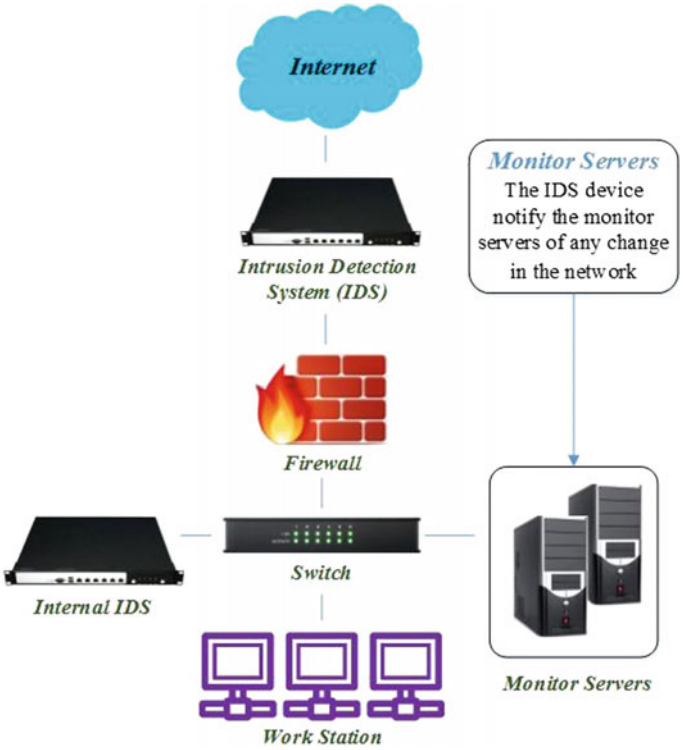


Fig. 1 Architecture of general IDS

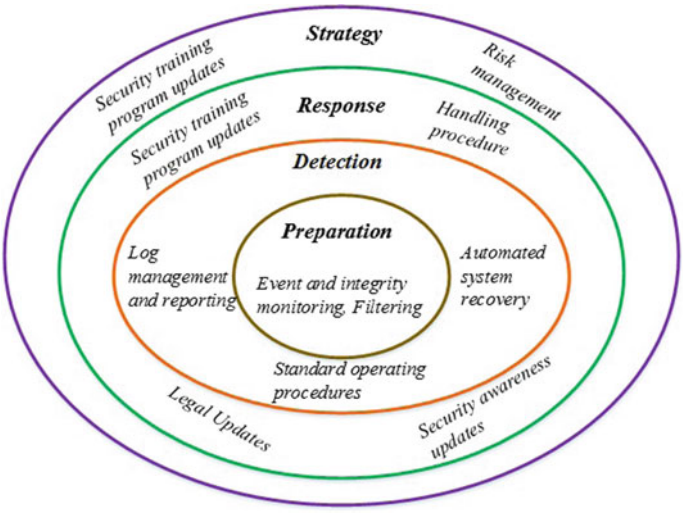


Fig. 2 Processes of IDS

In this work, a new IDS based on PRC technique is proposed to detect the known and unknown attacks in the SCADA network. Boyer–Moore (BM) is one of the exact string matching algorithms that are mainly used to match the text strings. Generally, the string matching algorithms are measured in terms of time and space complexities. The Hidden Markov Model (HMM) is a generative model that models the input data for clustering. Relevance Vector Machine (RVM) is a Bayesian classification method that is capable to deliver a complete probabilistic output.

The major contributions of this paper are as follows:

(1) Here, the power system attack dataset is used to detect the attacks in an SCADA network.
(2) In the preprocessing stage, the relays present in the given power control circuit are segregated into relay 1, relay 2, relay 3, and relay 4.
(3) Each relay contains different types of information such as date, timestamp, control panel log report, relay log report, snort log report, marker, fault locationn and load condition.
(4) After preprocessing the data, string matching is performed only for training set by using the Boyer–Moore (BM) algorithm.
(5) Then, the HMM-based clustering technique is employed to predict the kernels and to increase the efficiency of intrusion detection.
(6) Hence, the RVM-based classification technique is implemented to classify the attacks as known or unknown.
(7) If it is a known attack, the label of attack is predicted and the corresponding action is carried out to protect the SCADA network.
(8) If it is an unknown attack, the level of energy is estimated and the label of the attack is updated in both feature matrix and dataset.
(9) The novel concept of this paper is, it manually trains the data and features for unknown attacks.
(10) The advantage of this paper is it provides reduced set of features, reduced amount of database, and increased attack detection and classification rate.

This chapter is organized as follows: Sect. 2 presents some of the existing works related to Intrusion Detection System (IDS) algorithms and approaches. Section 3 gives the detailed description for the overall proposed PRC based IDS. Section 4 shows the performance and comparison results of the existing and proposed IDSs. Finally, this paper is concluded and the future work to be carried out is stated in Sect. 5.

2 Related Work

This section presents some of the existing works related to intrusion detection algorithms and frameworks in network security. Munshi et al. [1] designed a realistic and reliable Intrusion Detection System (IDS) architecture for an Advanced Meter-

ing Infrastructure (AMI) system and smart grid big data analytics. This architecture contains individual IDSs for three different levels of AMI components such as

(1) Smart meter,
(2) Data concentrator,
(3) AMI headend.

Moreover, this analysis identified various candidate algorithms for those AMI components. Aiping et al. [2] suggested a new data preprocessing method for Network Security Situational Awareness (NSSA). It was based on Conditional Random Fields (CRFs) that used different connection informations for attack detection and discovery of abnormal phenomenon. Davis and Clark [3] surveyed various data preprocessing techniques for network intrusion detection. It included the aggregation of packets into flows to allow the contextual analysis and statistical measures of packet headers. Parvat and Chandra [4] suggested a novel approach to improve the performance of deep packet inspection for detecting intrusions in a network. This approach was used to develop an application for multi-core, multi-threading inline intrusion prevention, and detection system. It improved the overall performance of the system by reducing the false attacks and reduced the load to dedicated security devices in the network.

Grilo et al. [5], integrated Wireless Sensor and Actual Networks (WSAN) and Supervisory Control and Data Acquisition (SCADA) system for monitoring Critical Infrastructures (CIs). The integration of SCADA and WSAN addressed some of the challenges in real-time, management, and security systems. Almalawi et al. [6] suggested an unsupervised anomaly detection approach for integrity attacks on SCADA systems. The major contributions of this paper are as follows:

(1) It automatically identified the consistent and inconsistent states of SCADA data.
(2) It automatically extracted the proximity detection rules from an identified state.

Here, an optimal inconsistency threshold was calculated to separate inconsistent and consistent observations. During this process, the fixed width clustering technique was extended to extract the proximity detection rules. Erez et al. [7] identified an irregular change in Modbus/TCP SCADA control register values by using a domain-aware anomaly detection system. Moreover, it automatically assigned registers into the three classes to learn the behavior of the network. Huang et al. [8] designed a new framework by using online and offline computing power and data distribution management system. Here, the transfers of measurement data were scheduled based on the communication bandwidth, computing power, and system operational requirements.

Karthick et al. [9] designed an adaptive network IDS by using a hybrid approach, which includes two stages: In the initial stage, the potential anomalies in the traffic were detected with the help of a probabilistic classifier and in the second stage, an HMM-based traffic model was employed to find the potential attack IP addresses. The main objective of this work was to implement more suitable models for effective functioning in real time. Koc et al. [10] suggested a Hidden Naïve Bayes (HNB) model to detect the intrusions as normal events or attack events. HNB provided

superior predictive performance than other Naïve Bayes models and it improved the accuracy of detecting Denial-of-Service attacks. Shamelisandi et al. [11] recommended an HMM technique to predict the real-time intrusions based on an optimized alert. The stages included in this framework are as follows:

(1) Data gathering,
(2) Detection,
(3) Alerts optimization,
(4) Prediction,
(5) Response.

In this chapter, the quality of alerts is improved by focusing on the severity of alert and this alert optimization has two parts such as correlation and optimization. Tobon Mejia et al. [12] suggested a failure prognostics method for estimating the Remaining Useful Life (RUL). This method was fully based on the utilization of Wavelet Packet Decomposition (WPD) technique and the Mixture of Gaussian Hidden Markov Models (MoG-HMM). Zhang et al. [13] suggested a Hidden Semi-Markov Model (HsMM) to predict the status of nodes under partial observation conditions. The HsMM technique modified the HMM model based on the presumption, which was more suitable to define the actual situation of the network system operation.

Qunhui [14] suggested a Relevance Vector Machine (RVM) based classification technique for analyzing the prediction probability of the classification results. An online network traffic classification algorithm was proposed in this paper to obtain the high classification accuracy. Hu et al. [15] developed a two-line AdaBoost-based IDS algorithm to handle the mixed attributes of network connection data. The major advantages of this model are as follows:

(1) The model was more suitable for information sharing.
(2) In this framework, the original data network was not shared so, that the data privacy was guaranteed.
(3) Moreover, the global detection model considerably increased the intrusion detection accuracy.

Jaiganesh et al. [16] surveyed various classification algorithms such as Support Vector Machine (SVM), Kernelized SVM, Extreme Learning Machine (ELM), and Kernelized ELM to classify the intrusions in a network. Moreover, two different intrusion detection approaches were also discussed in this paper, which includes

(1) Anomaly detection,
(2) Misuse detection.

An anomaly detection was an important tool that was mainly used for fraud detection, network-based intrusion detection, and unusual event detection. The main drawback of this method was it does not detect the well-known attacks. The misuse IDS analyzed the traffic and followed certain rules to detect an abnormal behavior. The major drawback of this method was it predicts only the known attacks. Horng et al. [17] integrated a hierarchical clustering with a feature selection procedure and

SVM techniques for detecting intrusions in a network. Here, the feature selection approach was applied to exclude unwanted features from the training set and the obtained SVM model classified the network traffic data in an accurate manner. In this paper, the most widely used dataset, namely, KDD cup 1999 was used to evaluate the performance of this system.

Xiang et al. [18] suggested a combination of Support Vector Machine (SVM)–Particle Swarm Optimization (PSO) techniques to improve the precision rate of network IDS. Here, the feature and parameters of SVM were coded to particle and the PSO was employed to select the optimal features and parameters among the particles. The major advantages of this method were listed as follows:

(1) It removed an unwanted and redundant features.
(2) It decreased the input vectors of SVM.
(3) Also, it provided high precision in the field of network security.

Ding et al. [19] developed an improved SVM classification technique to classify the network traffic and to improve the classification accuracy. The main objectives of this are as follows:

(1) The nature of the feature was represented with the help of probabilistic distributing area.
(2) The degree of the feature was identified by finding the area between two given traffic types.
(3) To cluster the input data and map it to a high-dimensional data space, the Gustafson–Kessel clustering technique was applied.

Panda et al. [20] proposed a hybrid intelligent approach based on the combination of classifiers for detecting intrusions in a network and to make the decision intelligently. Here, tenfold cross-validation method was applied to validate the final decision after applying the clustering technique. Furthermore, the meta learning strategy-based classifier was also used to improve the performance of this IDS.

3 Proposed Method

This section presents the detailed description of the proposed Intrusion Detection System (IDS) based on the Probabilistic Relevancy Classification (PRC) algorithm. The flow of the proposed PRC based IDS is shown in Fig. 3, which includes the following stages:

(1) Preprocessing,
(2) String Matching,
(3) Clustering and Classification,
(4) Attack Detection.

The main intention of this work is to detect and classify the network intrusions as known or unknown in SCADA network. The novel concept of this paper is it utilizes

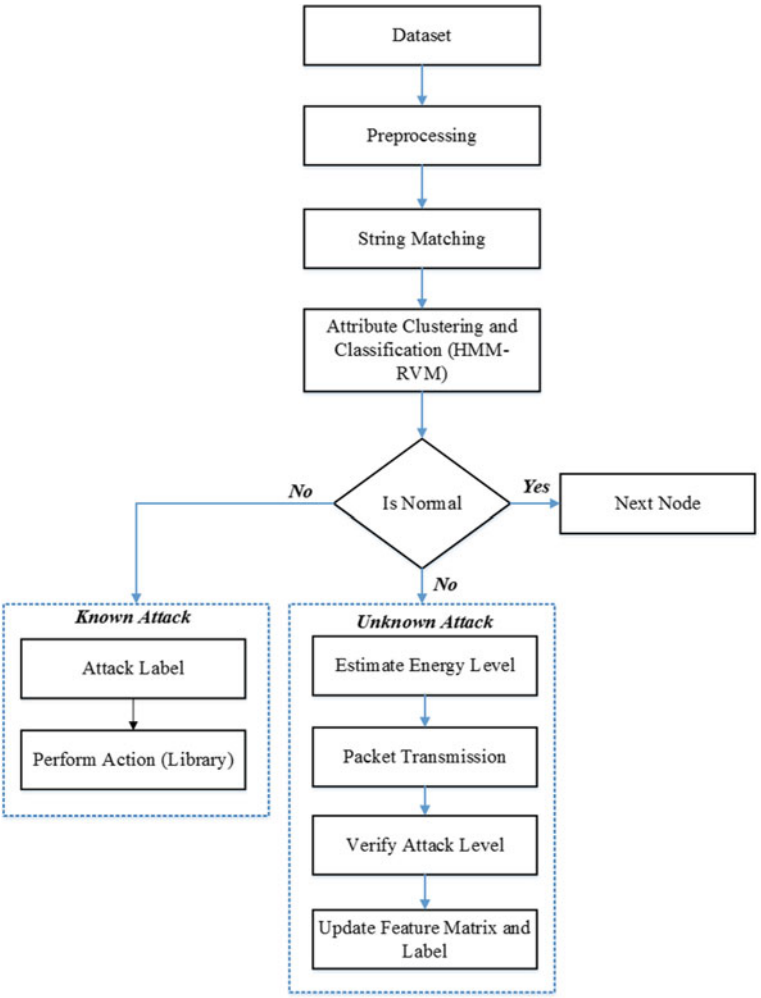


Fig. 3 Overall flow of the proposed PRC-based IDS

the combination of PRC technique for intrusion classification. Moreover, it gets the input data from the power control circuit dataset for evaluating the performance. The attacks detected by using the proposed system are listed in Table 1.

Initially, the data from the power system attacks dataset is given as the input and it will be preprocessed to segregate the relays used in the circuit. Then, the string matching is performed by using the Boyer–Moore (BM) algorithm. After that, the proposed PRC-based clustering and classification technique is applied to classify the attack as known or unknown. If it is an unknown attack, the energy is estimated and it will be updated in the feature matrix. If it is a known attack, the attack label is predicted and the corresponding action is carried out. The detailed step-by-step

Table 1 Types of attacks

Attack name	Abbreviation
Normal	Normal (0)
Naïve Malicious Response Injection	NMRI (1)
Complex Malicious Response Injection	CMRI (2)
Malicious State Command Injection	MSCI (3)
Malicious Parameter Command Injection	MPCI (4)
Malicious Function Code Injection	MFCI (5)
Denial of Service	DoS (6)
Reconnaissance	Recon (7)

description is provided in the following subsections. In this paper, the power system attacks dataset is used to detect the attacks present in the SCADA network. Figure 4 shows the framework configuration of power system used in this scenario. Various components used in this control circuit are listed as follows:

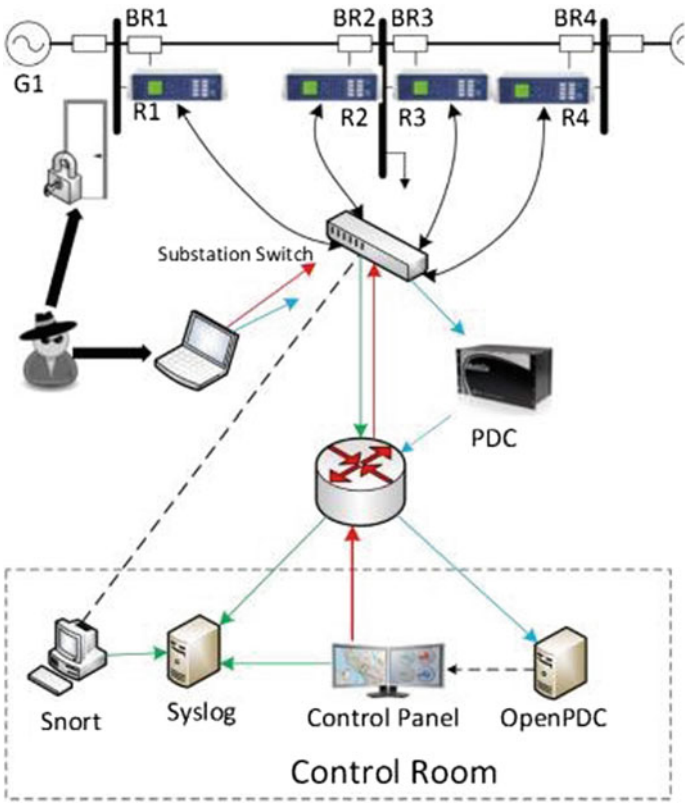


Fig. 4 Framework of power system

(1) G1 and G2—Power Generators.
(2) R1, R2, R3, and R4—Relays (i.e., Intelligent Electronic Devices (IEDs)).
(3) BR1, BR2, BR3, and BR4—Breakers.

3.1 Preprocessing

In this stage, the given set of values (i.e., text oriented) are preprocessed to segregate the relays used in Fig. 4. Here, the water and gas dataset values are preprocessed that separates the relays and its log report in Table 2. The list of parameters and attack vectors for the water and gas datasets is shown in below.

In this stage, it separates the relays into R1, R2, R3, and R4 and each relay contains the following information and is shown in Table 3.

Table 2 List of water and gas parameters

Gas parameters	Water parameters
Command address	Command address
Response address	Response address
Command memory	Command memory
Response memory	Response memory
Command_memory_out	Command_memory_out
Response_memory_out	Response_memory_out
Comm_read_function	Comm_read_function
Comm_write_function	Comm_write_function
Resp_read_fun	Resp_read_fun
Resp_write_fun	Resp_write_fun
Sub_function	Sub_function
Command_length	Command_length
Resp_length	Resp_length
Gain	HH
Resest	HH
Deadband	L
Cycletime	LL
Rate	Control_mode
Setpoint	Control_scheme
Control_mode	Pump
Control_scheme	Crc_rate
Pump	Measurement
Solenoid	Time
Crc_rate	Result
Time	
Result	

Table 3 Parameters of electric data

Network/Other	Relay 1	Relay 2	Relay 3	Relay 4
Date	R1-PA1:VH	R2-PA1:VH	R3-PA1:VH	R4-PA1:VH
Timestamp	R1-PM1:V	R2-PM1:V	R3-PM1:V	R4-PM1:V
Control_panel_log1	R1-PA2:VH	R2-PA2:VH	R3-PA2:V H	R4-PA2:VH
Control_panel_log2	R1-PA2:V	R2-PM2:V	R3-PM2:V	R4-PM2:V
Control_panel_log3	R1-PA3:VH	R2-PA3:VH	R3-Pa3:VH	R4-PA3:VH
Control_panel_log4	R1-PM3:V	R2-PM3:V	R3-PM3-V	R4-PM3:V
Relay 1_log	R1-PA4:IH	R2-PA4:IH	R3-PA4:IH	R4-PA4:IH
Relay2_log	R1-PM4:I	R2-PM4:I	R3-PM4:I	R4-PM4:I
Relay3_log	R1-PA5:IH	R4-PA5:IH	R3-PA5:IH	R4-PA5:IH
Relay4_log	R1-PM5:I	R2-PM5:I	R3-PM5:I	R4-PM5:I
Snort_log 1	R1-PA6:IH	R2-PA6:IH	R3-PA6:IH	R4-PA6:IH
Snort_log 2	R1-PM6:I	R2-PM6:I	R3-PM6:I	R4-PM6:I
Snort_log 3	R1PA7:VH	R2PA7:VH	R3PA7:VH	R4PA7:VH
Snort_log 4	R1-PM7:V	R2-PM7:V	R3-PM7:V	R4-PM7:V
Marker	R1-PA8:VH	R2-PA8:VH	R3-PA8:VH	R4-PM8:VH
Fault_location	R1-PM8:V	R2-PM8:V	R3-PM8:V	R4-PM8:V
Load_con	R1-PA9:VH	R2-PA9:VH	R3-PA9:VH	R4-PA9:VH
	R1-PM9:V	R2-PM9:V	R3-PM9:V	R4-PM9:V
	R1-PA10:IH	R2-PA10:IH	R3-PA10:IH	R4-PA10:IH
	R1-IM10:I	R2-PM10:I	R3-PM10:I	R4-PA10:I H
	R1-PA11:I H	R2-PA11:I	R3-PM11:I	R4-PM11:I
	R1-PM11:I	R2-PM11:I	R3-PM11:I	R4-PM11:I
	R1-PA12:I H	R2-PA12:I H	R3-PQ12:I H	R4-PA12:I H
	R1-PM12:I	R2-PM12:I	R3-PM12:I	R4-PM12:I
	R1:F	R2:F	R3:F	R4:F
	R1:DF	R2:DF	R3:DF	R4:DF
	R1-PA:Z	R2-PA:Z	R3-PA:Z	R4-PA:Z
	R1-PA:ZH	R2-PA:ZH	R3-PA:ZH	R4-PA:ZH
	R1:S	R2:S	R3:S	R4:S

The different types of network information segregated in this stage are as follows:

(1) Date,
(2) Timestamp,
(3) Control panel log report,
(4) Relay log,
(5) Snort log,
(6) Marker,
(7) Faulty location,
(8) Load condition.

3.2 String Matching

After preprocessing the data, the string matching is performed only for training data. In this paper, the Boyer–Moore (BM) algorithm is employed to perform the string matching operation. It is a generalized exact string matching algorithm that is used to approximate string matching. It is more suitable for natural languages and bio applications. It matches the string pattern from right to left over the pattern. The characters of the text below the pattern are examined at each alignment. Moreover, it starts the comparison at the rightmost character of the pattern with the character in the current text. Then, the pattern in the text is shifted from left to right between the alignments. The procedure of string matching is illustrated as follows:

Algorithm I – String Matching

Input: *Training data matrix Tr and Testing data matrix D;*
Output: *Matched string S and updated training set Tr2;*

```
Initialize k = 1;
Step 1: for i =1 to length (D)
Step 2:       for j =1 to length (Tr)
Step 3:             m = size of 'D';
Step 4:             if (D == Tr (j to m)) && (m ~= size (Tr (j))
Step 5:                   S = j;
Step 6:         Tr2 (k) = Tr (S); // Update training set at "S" matched
                index
Step 7:             else
Step 8:       Tr2 (k) = Tr (i); // Update training set at i^th index
Step 9:       end if
Step 10: end "j" loop
Step 11: end "i" loop
```

3.3 Clustering and Classification

After matching the string, the clustering and classification processes are performed to detect the known and unknown type of attacks. Clustering is defined as the process of classifying a large number of data points into groups, where all members in the group are similar in some manner. It is also defined as the grouping of data objects based on maximizing the intra-class similarities and minimizing the intercluster similarities. Clustering is a technique that finds the patterns in an unlabeled data with many dimensions. The main advantage of using HMM clustering is, it has the ability to detect the intrusions in an audit data. It is also used to extract the interactions between the attackers and networks.

Algorithm II – Attribute based clustering

Input: *Updated training set Tr2, Testing data matrix D and Label L;*

Output: *Clustered label CL;*

Step 1: *Initialization,*

Probability array, $\pi = P(q_1 = s_i)$

// Where, s defines the state of training set for I = 1, 2, … N, N is the size of training set Tr2 and q is the fixed state sequence for the length of D;

Step 2: ***for*** *(i = 1 to Row_size (D))*

Step 3: ***for*** *(j =1 to Column_size (D))*

Step 4: $s_i = Tr2\ (i, j)$ *// Extract the attributes from the training set;*

Step 5: $$d_i = \sqrt{(s_i - D_i)^2 + (s_j - D_j)^2}$$

Step 6: $q_{i,j} = L(d_i)$; *// Extract corresponding labels of training set;*

Step 7: $$\pi_i = \frac{\sum_{k=1}^{m} s_i\left(q_{i,j}(d)\right)}{m}$$

Step 8: $$\sigma_T = \sqrt{\frac{1}{m}\sum_{i=1}^{N}\left(S_i\left(q_{i,j}(d)\right) - \pi_i\right)^2}$$

$$\sigma_D = \sqrt{\frac{1}{n}\sum_{i=1}^{N}\left(D_i\left(q_{i,j}(d)\right) - \pi_i\right)^2}$$

Where, m is length of s_i *and n represents the length of* D_i*;*

Step 9: $$P(Tr2|\pi_i) = (2\prod \sigma_T^2)^{\frac{-N}{2}} * e^{\left\{\left(\frac{-1}{2\sigma_T^2}\right)\|Tr2-\pi_i\|^2\right\}}$$

//Estimates the probability for training feature, where N represents the size of training set Tr2;

Step 10: $$P(D) = (2\prod \sigma_D^2)^{\frac{-M}{2}} * e^{\left\{\left(\frac{-1}{2\sigma_D^2}\right)\|D_i-\pi_i\|^2\right\}}$$

// Estimates the probability of training feature, where M represents the size of training set D.

Step 11: ***If*** *(*$P(Tr2|\pi_i)$ *> P (D)) // Condition for attack feature verification;*

Step 12: $CL_i = L\left(P(D)\right)$ *// Selected attack node;*

Step 13: ***end*** *if;*

Step 14: ***end*** *'j' loop;*

Step 15: ***end*** *'i' loop;*

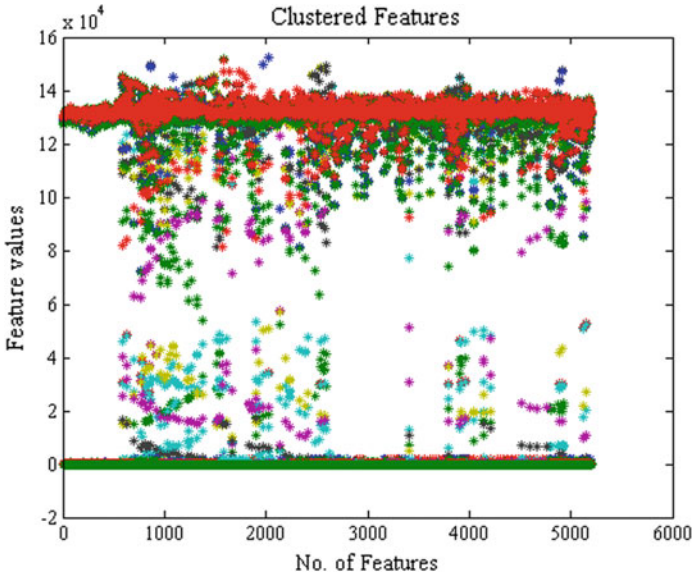


Fig. 5 Clustered output

The clustered output is shown in Fig. 5, where the attacking nodes are marked as red. In this paper, the RVM based classification technique is used to classify the attacks as known or unknown. The reason for using RVM is, it guarantees the reliability for designing IDS and it has a better generalization performance than SVM due to less support vectors.

Generally, the RVM is a new type of machine learning model that is based on a Bayesian formulation of a linear model. It provides appropriate results in a form of sparse data representation. It can generalize and provide interferences at a very low computational cost. Given a set of $\{D_i, Tr2_i\} = re_{i=1}^{n}$, where D_i represents the input vector and $TR2_i$ is their corresponding outputs. The output of RVM is illustrated as follows:

$$Tr2(D(CL)) = \sum_{i=1}^{n} w_i R(D(CL), D(CL)_i) + w_0 \tag{1}$$

where $w = [w_0, \ldots w_i]$ represents the weight vector, $R(D(CL), D(CL)_i)$ defines the kernel function. In RVM, the Gaussian kernel is used as an encountered kernel that is expressed as follows:

$$R(D(CL), D(CL)_i) = exp\left[-\frac{||D(CL) - D(CL)_i||^2}{2\sigma^2}\right] \tag{2}$$

where σ defines the width of Gaussian kernel. Then, the likelihood of the dataset is expressed as follows:

$$p\left(Tr2|w,\sigma^2\right) = \left(2\pi\sigma^2\right)^{-\frac{n}{2}} exp\left[-\frac{1}{2\sigma^2}||Tr2-\rho||^2\right] \tag{3}$$

$$\rho(D(CL)_i) = \left[1, R(D(CL)_i, D(CL)_1), R(D(CL)_i, D(CL)_2) \ldots, R(D(CL)_i, D(CL)_n)\right]' \tag{4}$$

Here, an explicit prior probability distribution is defined to improve the generalization ability of RVM, which is calculated as follows:

$$p(w|x) = \prod_{i=1}^{n} N\left(w_i|0, Tr2(CL)_i^{-1}\right) \tag{5}$$

where x represents a hyperparameter vector. The classifier function of RVM is defined as follows:

$$Tr2(D(CL)) = \rho'(D(CL))\left(\sum_{i=1}^{n} Tr2(CL)_i \rho(D(CL)_i)\right) \tag{6}$$

Moreover, it produces a function that is compromised by a set of kernel functions. This is known as the basis function and a set of weight functions, and this function represents a model based on the set of training data set for the learning purpose. In learning process, the kernels and weights are calculated and the model function is defined by fixing the weighted sum of kernels. From this set of training vectors, the RVM selects a sparse subset of input vectors. It is used to build a function and to estimate the output result. The relevant vector forms the basis function and compromises the model function. In this classification phase, the network data selected from the clustering phase is classified into normal or attack data. In this work, two main datasets, namely, gas and water are used for both training and testing. During the training phase, the PRC-based IDS can classify the data in the record into normal or attack (either known or unknown). The proposed IDS classifies the audit data as normal or abnormal based on a set of rules and patterns.

4 Performance Analysis

This section presents the evaluation results of the proposed PRC-based IDS. The experimental setup is done through MATLAB simulation. The framework set up has been done with the SCADA architecture that comprises of Power Generators of G1 and G2, IEDs (Intelligent Electronic Devices) of R1, R2, R3, and R4—Relays, BR1, BR2, BR3, and BR4—Breakers. Each relay contains different types of information such as date, timestamp, control panel log report, relay log report, snort log report, marker, fault location, and load condition.

Original data is collected from different Phasor Measurement Unit (PMU) sensors, then it is merged into a single database. Then, the total number of possible states in a database are minimized by quantizing the continuous states. In this work, IEEE C37.118 protocol is used to measure the power system transmission. The PMUs synchronous measurement data deliver at a rate of 120 samples/s. Hence, 56 different data sources are used. These contain 52 synchronous measurements, where 13 are selected from each relay location. A total of 15 features have been used in this work. Based on this setup, the implementation is carried further.

Here, the power system attack dataset is used to evaluate the performance. It is made from one initial dataset that contains 15 sets with 37 power system event scenarios. These scenarios are divided into natural events (8), attack events (28), and no events (1). It is randomly sampled into

(1) Binary,
(2) Three class,
(3) Multi-class datasets.

Here, the water and gas dataset [21] values are used to validate the results. The results are analyzed and evaluated in terms of False Acceptance Rate (FAR), False Rejection Rate (FRR), Genuine Acceptance Rate (GAR), sensitivity, specificity, accuracy, error rate, recall, and false detection rate.

4.1 Confusion Matrix

The confusion matrix for the proposed PRC-based classification system is shown in Fig. 6. Here, the attack predicted and actual classes are illustrated based on the number of data samples. In this matrix, it is evaluated that the PRC accurately predicts the attacking nodes in an SCADA network.

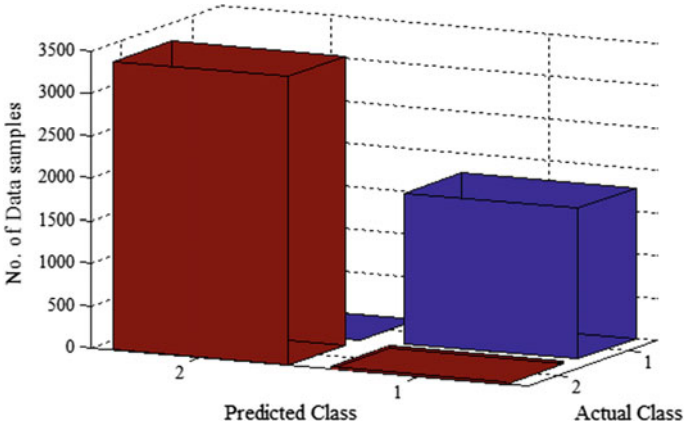


Fig. 6 Confusion matrix

4.2 Error Rate

The error rate is defined as the degree of errors occurred during the data transmission over a communication. If the error rate is higher, the data transfer will be less reliable. Here, the probability of the error rate is denoted as QE that defines how many times the base station takes an incorrect decision. In this paper, the performance of the algorithm is evaluated for attack classification. The error rate QE is calculated as follows:

$$Q_E = \frac{\#\ of\ incorrect\ decision}{T} \tag{7}$$

Figure 7 shows the error rate of the proposed system with respect to the number of attackers.

4.3 Recall

Recall is a true detection rate that is extensively used in many networking applications for evaluating the successful detection of class members. It is considered as more significant than the detection of other class members. The algorithms with higher

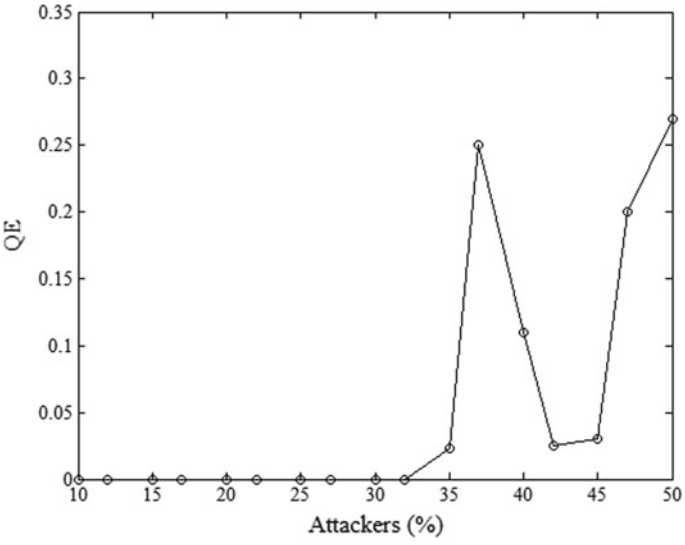


Fig. 7 Error rate

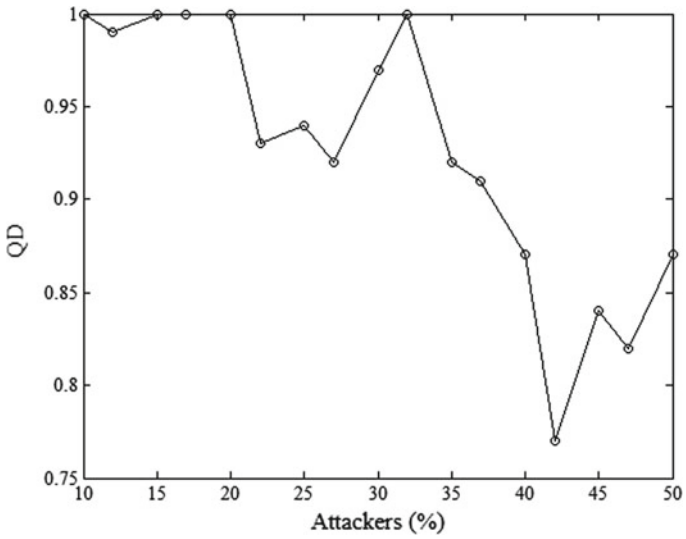


Fig. 8 Recall

value of recall are needed to improve the performance. In this work, identifying the network attackers is more important than identifying the honest users. The recall QD is calculated as follows:

$$Q_D = \frac{\#\ of\ attackers\ truely\ detected}{\#\ of\ actual\ attackers} \tag{8}$$

Figure 8 shows the recall value for the proposed system with respect to the number of attackers.

4.4 False Detection Rate

False Detection Rate (FDR) is a false positive rate that represents how many nodes are misidentified as attackers. If the algorithm has a lower false positive rate, it will give the better performance. The false positive rate QF is calculated as follows:

$$Q_F = \frac{\#\ of\ honest\ users\ misidentified}{\#\ of\ nodes\ identified\ as\ attackers} \tag{9}$$

Figure 9 shows the FDR of the proposed system with respect to the number of attackers.

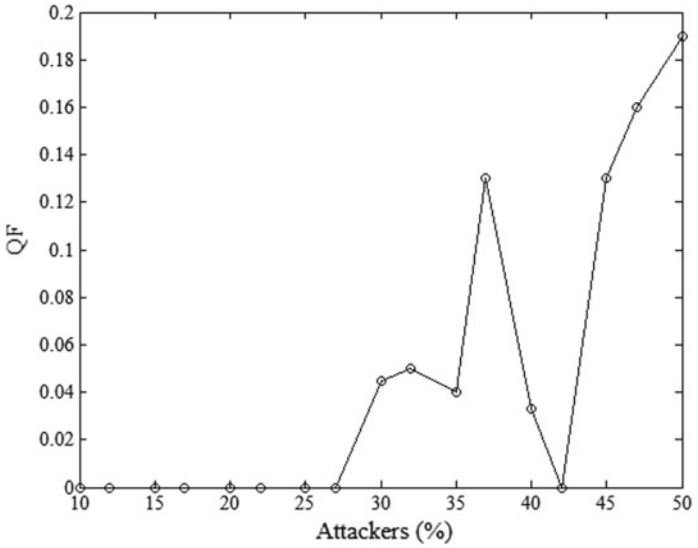


Fig. 9 False detection rate

4.5 Classification Result for Existing and Proposed Classifiers

The comparison between existing Neural Network (NN) [22] and proposed PRC classifiers is shown in Table 4. The results are evaluated in terms of False Positive Rate (FPR), False Negative Rate (FNR), and accuracy. When compared to the existing classifier, the proposed PRC provides the best results. Here, the parameters measured for negative alarm rate, HH alarm rate, H set point, L set point, and LL alarm.

The comparison between existing random forest, Jrip, AdaBoost+Jrip, mining path [23], and proposed PRC methods are evaluated in terms of accuracy, precision, recall, and F-Measure. The results are shown in Fig. 10.

4.6 Sensitivity, Specificity, and Accuracy

Sensitivity is defined as the proportion of true positives that are correctly classified by proposed PRC, which is expressed in terms of percentage. The sensitivity is the probability of getting a true positive test result in subjects. It is the number of true positives divided by the sum of the true positives plus false negatives. Similarly, the specificity is defined as the number of true negatives divided by the sum of true negatives plus false positives. The sensitivity and specificity values are calculated as follows:

Table 4 Classification results for existing NN and proposed PRC classifiers

Classification result		
Parameters	NN classifier	PRC classifier
Negative alarm rate		
FPR (%)	0	0
FNR (%)	0	0
Accuracy (%)	100	100
HH alarm		
FPR (%)	4.5	0.9
FNR (%)	0	0
Accuracy (%)	95.5	99.4
Above H setpoint		
FPR (%)	2.3	0.6
FNR (%)	3	0.8
Accuracy (%)	94.7	99.3
Above L setpoint		
FPR (%)	2.4	1.2
FNR (%)	3	0.9
Accuracy (%)	94.6	98.91
LL alarm		
FPR (%)	3.2	1.5
FNR (%)	0	0
Accuracy (%)	96.8	99.48

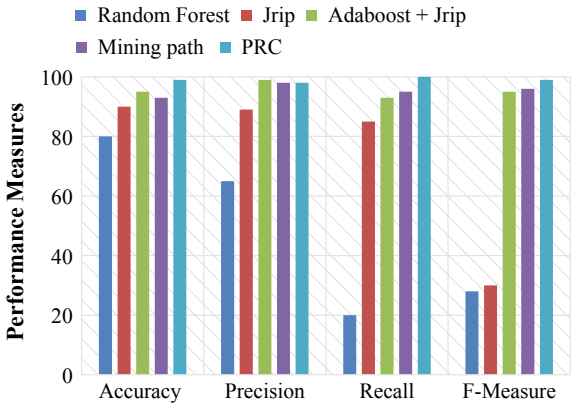


Fig. 10 Comparison between existing and proposed techniques based on accuracy, precision, recall, and F-Measure

$$Sensitivity = \frac{TP}{(TP + FN)} = \frac{Number\ of\ true\ positive\ assessments}{Number\ of\ all\ positive\ assessments} \tag{10}$$

$$Specificity = \frac{TN}{(TN + FP)} = \frac{Number\ of\ true\ negative\ assessment}{Number\ of\ all\ negative\ assessment} \tag{11}$$

The accuracy of the proposed PRC technique can be determined from both sensitivity and specificity with the presence of prevalence. The accuracy is calculated as follows:

$$Accuracy = \frac{(TN + TP)}{(TN + TP + FN + FP)} = \frac{Number\ of\ true\ correct\ assessment}{Number\ of\ all\ assessment} \tag{12}$$

where TP represents True Positive, TN represents True Negative, FP indicates False Positive, and FN indicates False Negative. The False Rejection Rate (FRR) is defined as the instance of a network security system failing, which incorrectly rejects the classification results in a network. It is calculated as follows:

$$FRR = \frac{\text{The number of false rejections}}{\text{The number of identification items}} \tag{13}$$

Similarly, the False Acceptance Rate (FAR) is defined as the ratio between the number of non-truly matching samples that is matched by the IDS system and the total number of tests. It is calculated as follows:

$$FAR = \frac{\text{The number of false acceptances}}{\text{The number of identification items}} \tag{14}$$

The Genuine Acceptance Rate (GAR) is defined as the ratio of truly matching samples that is matched by the system and the total number of tests. The performance measures for the proposed PRC is given in Table 5. It is calculated as follows:

$$GAR = 1 - \frac{\text{The number of false rejections}}{\text{The number of identification items}} \tag{15}$$

Table 5 Performance measures for proposed PRC

Measure	Value
True Positive (TP)	1769
True Negative (TN)	3402
False Positive (FP)	31
False Negative (FN)	0
Sensitivity	100
Specificity	99.0970
Accuracy	99.4041
GAR	99.7020
FAR	0.2980
FRR	0.2980

5 Conclusion

In this chapter, a new Intrusion Detection System (IDS) based on Hidden Markov Model (HMM)–Relevance Vector Machine (RVM), namely, Probabilistic Relevancy Classification (PRC) is proposed. Here, the power system attack dataset is used to evaluate the performance of the proposed system. In the initial stage, the given text-oriented data is preprocessed to segregate the relays into R1, R2, R3, and R4, where each relay contains different log informations. After that, the Boyer–Moore (BM) algorithm is used to perform the string matching operation. Then, the proposed PRC technique is employed to classify the attack as known or unknown. If the detected attack is known, the label of the attack is predicted and the corresponding action is carried out to protect the network. If it is an unknown attack, the level of energy is estimated and, it is updated in both feature matrix and dataset. The main intention of this paper is to accurately detect the intrusion in an SCADA network. The novelty of this concept is it manually training the data and features for unknown attacks. The advantages of the proposed technique are it provides a reduced set of features, reduced amount of database, and increased both the detection and attack classification rate. Moreover, the performance of the proposed PRC is compared with some existing techniques in terms of precision, recall, error rate, False Detection Rate (FDR), False Acceptance Rate (FAR), False Rejection Rate (FRR), Genuine Acceptance Rate (GAR), sensitivity, specificity, and accuracy.

In future, the proposed IDS will be enhanced to identify the data forwarding attacks such as sinkhole, wormhole in SCADA network.

References

1. Munshi, A. A., & Mohamed, Y. A.-R. I. (2018). Data Lake Lambda architecture for smart grids big data analytics. *Access IEEE*, *6*, 40463–40471.

2. Aiping, L., et al. (2010). A new method of data preprocessing for network security situational awareness. In *2nd International Workshop on Database Technology and Applications (DBTA)* (pp. 1–4).
3. Davis, J. J., & Clark, A. J. (2011). Data preprocessing for anomaly based network intrusion detection: A review. *Computers & Security, 30,* 353–375.
4. Shitharth, S., & Prince Winston, D. (2017). An enhanced optimization algorithm for intrusion detection in SCADA network. *Journal of Computers and Security*, *70*, 16–26. Elsevier.
5. Parvat, T. J., & Chandra, P. (2015). A novel approach to deep packet inspection for intrusion detection. *Procedia Computer Science, 45,* 506–513.
6. Grilo, M., et al. (2014). An integrated WSAN and SCADA system for monitoring a critical infrastructure. *IEEE Transactions on Industrial Informatics, 10,* 1755–1764.
7. Almalawi, et al. (2014). An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems. *Computers & Security*, *46*, 94–110.
8. Erez, N., & Wool, A. (2015). Control variable classification, modeling and anomaly detection in Modbus/TCP SCADA systems. *International Journal of Critical Infrastructure Protection, 10,* 59–70.
9. Huang, S.-C., et al. (2015). Evaluation of AMI and SCADA data synergy for distribution feeder modeling. *IEEE Transactions on Smart Grid, 6,* 1639–1647.
10. Karthick, R. R., et al. (2012). Adaptive network intrusion detection system using a hybrid approach. In *Fourth International Conference on Communication Systems and Networks (COMSNETS)* (pp. 1–7).
11. Koc, L., et al. (2012). A network intrusion detection system based on a Hidden Naïve Bayes multiclass classifier. *Expert Systems with Applications, 39,* 13492–13500.
12. Sendi, S., et al. (2012). Real time intrusion prediction based on optimized alerts with hidden markov model. *Journal of Networks, 7,* 311–321.
13. Tobon-Mejia, D. A., et al. (2012). A data-driven failure prognostics method based on mixture of gaussians hidden markov models. *IEEE Transactions on Reliability, 61,* 491–503.
14. Zhang, et al. (2012). Network security situation assessment based on hidden semi-markov model. In D.-S. Huang, et al. (Eds.), *Advanced intelligent computing* (Vol. 6838, pp. 509–516). Berlin, Heidelberg: Springer.
15. Qunhui, Z. (2013). Online network traffic classification algorithm based on RVM. *Journal of Networks, 8,* 1364–1369.
16. Hu, W., et al. (2014). Online adaboost-based parameterized methods for dynamic distributed network intrusion detection. *IEEE Transactions on Cybernetics, 44,* 66–82.
17. Shitharth, S., & Prince Winston, D. (2015). A comparative analysis between two countermeasure techniques to detect DDoS with sniffers in a SCADA network. *Procedia Technology*, *21*, 179–186.
18. Jaiganesh, V., et al. (2013). Intrusion detection systems: A survey and analysis of classification techniques. *International Journal of Advanced Research in Computer and Communication Engineering*, *2*.
19. Horng, S.-J., et al. (2011). A novel intrusion detection system based on hierarchical clustering and support vector machines. *Expert Systems with Applications, 38,* 306–313.
20. Xiang, et al. (2014). Network intrusion detection based on PSO-SVM. *TELKOMNIKA Indonesian Journal of Electrical Engineering*, *12*, 1502–1508.
21. Ding, L., et al. (2013). A classification algorithm for network traffic based on improved support vector machine. *Journal of Computers, 8,* 1090–1096.
22. Panda, M., et al. (2012). A hybrid intelligent approach for network intrusion detection. *Procedia Engineering, 30,* 1–9.
23. Pan, S., et al. (2015). Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data. *IEEE Transactions on Industrial Informatics, 11,* 650–662.

Intrusion Detection System in Internet of Things

Sunil Kumar Gautam, Hari Om and Kumar Dixit

Abstract The Internet of Things (IoT) is a fast-expanding network of smart heterogeneous objects. It refers to the physical devices that are capable of communicating with other physical devices. Unlike the wireless sensor networks (WSNs), IoT is connected to worldwide Internet that exposes it to global intrusion in addition to wireless attacks inside an IoT network. It is protected by cryptographic and network security techniques, but they are vulnerable to internal and external attacks. The IoT devices are resource constrained in terms of limited storage, battery, limited transmission range and processing. To protect these tiny devices from the inside and outside cyberattacks, we need a lightweight security system that can run efficiently and effectively on these IoT devices. We also need a system, which can identify the type of intrusion and trigger an alarm in intrusion scenario to take appropriate preventive measure. Hence, an Intrusion Detection System (IDS) plays an important role to prevent such cyberattacks in IoT. These devices can be static or mobile in an IoT environment; this must be considered while designing IDS for IoT system. This book chapter presents various IDSs for an IoT system and their comparisons in terms of detection rate, false positive and accuracy in both static and mobility of devices.

Keywords Intrusion detection system · Internet of Thing · Confusion matrix · Internet of Things protocol

S. K. Gautam (✉)
Department of Engineering & Computing, Institute of Advanced Research, Gandhinagar, India
e-mail: gautamsunil.cmri@gmail.com

H. Om · K. Dixit
Department of Computer Science and Engineering, Indian Institute of Technology (ISM), Dhanbad, India
e-mail: hariom4india@gmail.com

K. Dixit
e-mail: kumardixit88@gmail.com

S. K. Das et al. (eds.), *Design Frameworks for Wireless Networks*,
Lecture Notes in Networks and Systems 82,
https://doi.org/10.1007/978-981-13-9574-1_4

1 Introduction

Due to advancement in technologies and quest for betterment, hundreds of million devices are connected to the internet, which is further increasing exponentially. These devices, called Internet of Things (IoT), are very small and resource constrained that have limited capability in terms of processing power, power backup, size and storage. IoT devices are connected to each other, forming a network and also connected to conventional Internet. Strictly speaking, the Internet of Things is IP-connected resource-constrained devices connected to the Internet. Although there is conventional TCP\IP protocols suite that is capable to connect these devices to the global Internet, yet it is heavyweight and can degrade the efficiency of the constrained devices. The lightweight protocols such as 6LoWPAN, CoAP, RPL protocols and IEEE 802.15.4 are designed to IoT to enable the communication amongst the IoT devices. As these devices are connected to each other like MANETs and also to the internet, they are more prone to internal and external attacks. All potential cyberattacks on MANETs and VANETs are possible in an IoT network and also the external cyberattacks. Though the cryptographic techniques and Internet security techniques are applicable to IoT devices, yet they are very complex and cannot protect against various cyberattacks and also non-adaptive to new attacks. An Intrusion Detection System (IDS) can be a second line of defence to IoT system that can detect known and novel attacks in a particular node of IoT or in an IoT network, and triggers an alarm. An enhanced IDS system that can take preventive measure also at the same time of intrusion is called Intrusion Prevention System (IPS). The IoT devices being susceptible to intrusion and resource constrained need a lightweight security system. An IDS can be designed for resource-constrained IoT devices to protect the IoT system from internal as well as external intrusions.

2 Motivation

Confidentiality, Integrity and Availability are prime issues for the researcher. There is a dire need of an intrusion detection system that provide prime security and handle privacy in IoT network. It is not an easy task because IoT network constitutes heterogeneous devices where managing such kind of network is not an easy task. Therefore, the researcher proposed different security protocols and designed cryptographic techniques for managing security issues. In this chapter, we will discuss about existing efforts in the direction of ensuring privacy in using IDS in IoT networks.

3 Internet of Thing

Internet of Things (IoT) is an IP connected to the hybrid network of small sensor devices like WSNs and conventional internet. It is a heterogeneous system consisting of diverse types of sensor devices, which are resource constrained and connected to the internet. Unlike the WSNs, these devices have limited power options, low processing, low transmission range and connected to the outside world via Internet, and is identified by a specific IP address. The IoT devices can be a refrigerator, bulb, TV, PC, laptop or sever machine. Billions of potential devices can be connected through IoT [1].

3.1 IoT Architecture

The IoT system architecture as shown in Fig. 1 is decomposed into three layers such as Application layer, Network layer and Perception layer [1].

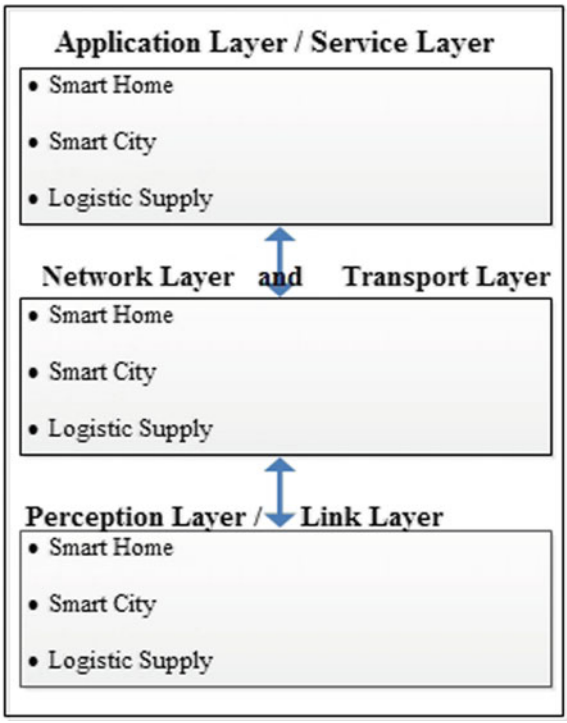


Fig. 1 IoT system architecture

i. **Perception Layer**
Primary layer of IoT is the perception layer, which is also known as the link layer. This layer gathers data/information from inside the IoT environment. It comprises sensor devices like temperature sensor, RFID sensor, sound sensor, GPS, Bluetooth, etc. The Perception layer can be divided into two parts:

- Perception node: used for data control.
- Perception network: to send the data to the controller.

ii. **Network Layer**
It is also known as the transport layer, which transfers the data from lower layer to upper layer, i.e. from the perception layer to application layer. It is capable to transmit the data over Internet and hence, it can communicate with various heterogeneous networks also. The devices dedicated to this layer are GSM, GPRS, 3G, ISDN, PSTN, Wi-Fi, etc.

iii. **Application Layer**
This layer, also called the service layer, provides services to an end user by converting the data into useful contents. An end user interacts with the help of a Graphical User Interface (GUI) to this layer. The smart home, smart city, Logistic supply, etc. are the high level services to which a user interacts with the help of application layer.

3.2 Life Cycle of IoT and Possible Attacks

IoT life cycle (Fig. 2) can be categorized into three major phases: manufacture, operational phases and bootstrap [2]. The IoT devices are prone to attacks especially in operation phase, but IoT is vulnerable to attacks from the starting of life cycle [3]. Security of IoT must be addressed in each phase of the IoT life cycle.

At the time of manufacturing, an entrusted can clone the software, firmware, physical characteristics and security configurations. Later, it can be used to launch other attacks such as a backdoor attack. During installation, a genuine thing may be substituted with a similar type of low-quality device, which can be vulnerable to intrusion. The man-in-middle attack, eavesdropping attacks, extraction of security parameters, etc. are possible in operational phase and in maintenance phase, the firmware replacement attack is possible. An intruder can change/add a malicious piece of code in firmware/software.

The IoT devices or framework also suffer some other challenges, which create intrusion in IoT network. Now, we address those challenges [4, 5]:

i. Profiling and Tracking: Most of IoT devices in a network associated with a specific address and having own identity. Therefore, the attacker easily led to profiling and tracking of IoT device. Thus, it is one major challenge that disallows such activities in IoT network.
ii. Localization and Tracking: The determining of positions of IoT device is creating another threat challenges for IoT network. Profiling information related to a

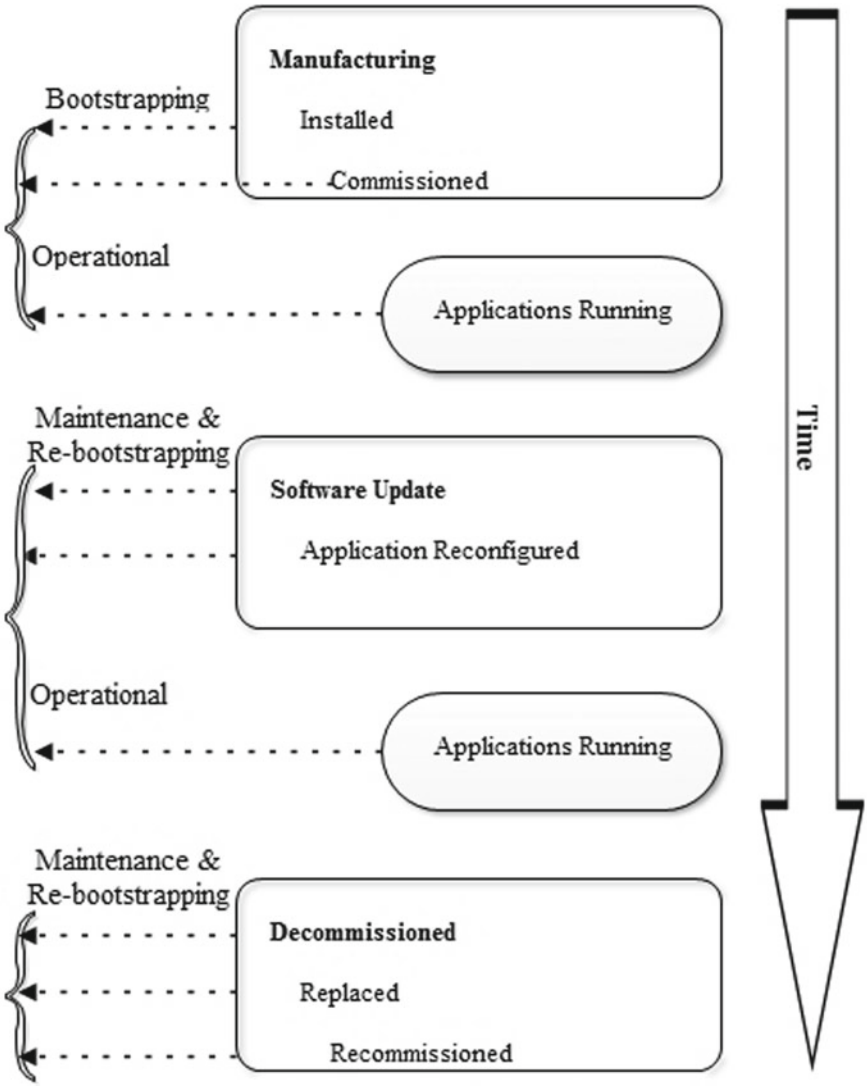


Fig. 2 IoT life cycle

certain individual to infer interests by the correlation between other profiles and data is very common in e-commerce applications. A huge challenge lies in balancing the interests of businesses for profiling and data analysis with user's privacy requirements.

iii. Protected Data Transmission: Data transmission is another challenging issue in IoT network because of data transmission in secure channel through a public medium without intercepting by anyone.

In Sect. 6, potential cyberattacks are discussed that are possible in the operational phase in the IoT environment.

4 Comparison of Internet of Things and Traditional IP Network

Internet of Things devices are resource constrained, e.g. they have a limited battery, limited processing power, low transmission range of sensors, etc. and also network links are lossy. The module of traditional IP Protocol is heavyweight and is not suitable for IoT system architecture. Researchers have developed a lightweight protocol corresponding to the traditional IP protocol for resource-constrained devices in IoT [6]. Figure 3 shows the layers in IoT protocol stack versus IP protocol stack.

4.1 IoT Protocol Stack

Following are the protocols in this stack:

i. **Constrained Application Protocol (CoAP)**
Internet Engineering Task Force has developed the Constrained Application Protocol, which is an application protocol for IoT devices to connect it to the internet. It is designed to replace the HTTP protocol for the application layer protocol of IoT.

ii. **User Datagram Protocol (UDP)**
The User Datagram Protocol is a lightweight connectionless protocol that is suitable for resource-constrained IoT devices. It provides checksum for data integrity and port number for communication to other nodes. IoT applications are time sensitive, hence prefer dropping of packets instead of waiting for delayed

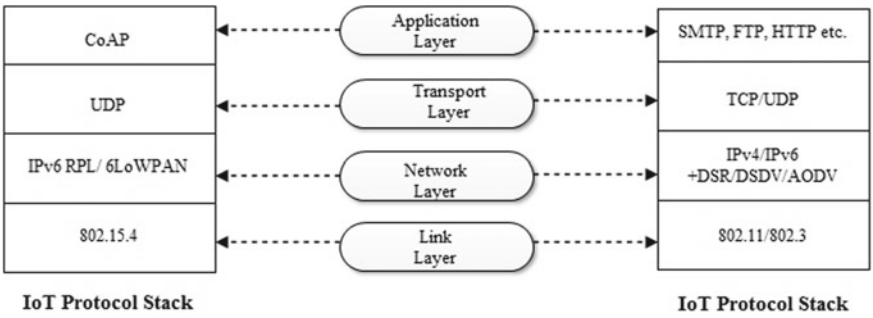


Fig. 3 IoT protocol stack versus IP protocol stack

packet. The UDP protocol satisfies this requirement and has been adopted for transport layer protocol.

iii. **Link Layer Protocol**
IoT implements IEEE 802.15.4 standardized protocol for sensor devices for medium access control layer. The frame formats of traditional network at link layer are not suitable for resource-constrained devices in IoT due to their overhead. IEEE 802.15.4 describes frame format, header and communication algorithm for IoT devices. To gain high reliability and meet the requirement IoT communications, it uses channel hopping and time synchronization. Slotted frame structures, synchronization, channel hopping, network formation, scheduling, etc. are the main features of IEEE 802.15.4 standard.

iv. **Network Layer Protocol**
IoT implements IPv6 Routing and Lossy network (RPL) and 6LoWPAN network at network layer for resource-constrained sensor nodes. Currently, billions of IoT devices are connected to the internet via IP, thus requiring a large address space. IPv6 is used to overcome the address space problem in IoT.

v. **Routing Protocol for low power and Lossy network (RPL)**
The RPL, which has been primarily designed to meet the specific requirement of IP IoT, is a novel standard routing protocol. It can enable one-to-one communication, one-to-many communication and many-to-one communication. RPL forms a DODGA (destination-oriented directed acyclic graph) with a root node and supports both unidirectional as well as bidirectional communication between the root and constrained nodes. The root, also called sink node, is directly connected to the internet using 6BR (IPv6 Boarder Router). It uses a three-way handshake process as follows.

- **DODAG Information Object (DIO) message**
  The root node broadcasts DIO message for the formation of topology.
- **DODAG Advertisement Object (DAO) message**
  Other nodes select the parent after receiving the DIO message and reply a DAO message to the parent asking the permission to join the parent.
- **DODAG Acknowledge message (DAO ACK)**
  Parent node gives permission by sending DAO ACK message based on rank value calculation of each node, which is done on basis of rank of parent and other parameters like energy of node and distance from node. If a new node wants to join a parent, it sends a DIS (DODAG Info Solicitation) message to find if any DODAG exists or not.

vi. **IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN)**
6LoWPAN integrates WSNs and IP-based infrastructure such as IEEE 802.15.4 networks. It uses the following mechanism for context-aware header compression:

(a) IP Header Compression (IPHC) to compress IPv6 header.
(b) Next Header Compression (NHC) to compress the User Datagram Protocol (UDP) header and IPv6 extension header.

The 6LoWPAN standard also redefines fragmentation and reassembly of packets because the payload size of link layer in 6LoWPAN network is very limited and the security protocol for large application data size makes IEEE 802.15.4 frame size larger than the maximum transmission unit (MTU) size (127 bytes). 6LoWPAN fragmentation scheme provides reassembly tag and an offset to every fragment and provides additional fragmentation if data size exceeds MTU size.

4.2 IPv6 Border Router (6BR)

The IoT networks are IP-connected 6LoWPAN networks. To connect an IoT system to the internet, a border device, called 6BR, is needed that connects 6LoWPAN network with the internet. Unlike WSNs, IoT networks are directly connected to the internet through 6BR making it accessible globally. This makes IoT systems vulnerable to external intrusions.

The remaining chapter is structured as follows. Section 3 describes the architecture and life cycle of IoT and Sect. 4 provides a comparison of the IoT protocol stack with the conventional wireless protocol stack. Section 5 introduces the basic concepts of IDS and its related terminology and Sect. 6 discusses various potential cyberattacks in the IoT environment. In Sect. 7, we discuss the existing network security techniques, which are also applicable to IoT devices and the need of IDS in IoT. Section 8 discusses important existing IDSs for IoT and provides comparative performance and accuracy of the proposed Intrusion Detection System. Finally, in Sect. 9, we conclude the chapter.

5 Intrusion Detection System

Intrusion Detection System is used to detect intrusive behaviour traffic in a network and the malicious node compromised by an adversary. It observes the network and nodes inside the network, detects the intrusion and notifies the user about intrusive behaviour. Intrusion can be vicious for constrained node in IoT and the IDS raises an alarm before the attacker begins to attack, by analysing traffic behaviour. It can detect both internal and external attacks inside an IoT environment. The internal attacks can be launched by the compromised nodes inside the IoT network, and the external attacks are launched by a global intruder from outside of the network. The IDS module can be deployed in a network (border router) or in an individual sensor node. It may be classified into two groups depending upon design and installation: network-based intrusion detection system (NIDS) and host-based intrusion detection system (HIDS). In IoT, the IDS can be installed in border router, or constrained node, or in both places to work in a collaborative manner [7]. The HIDSs is designed to collect information about the activities on a particular system and are host-based agent installed in a host that is susceptible to intrusion. The term host refers to

a computer or IP-connected sensor node in IoT; thus, a separate HIDS module is needed for each host. It works as an audit trail and keeps a log of every activity. The NIDS collects information from a network itself instead of each host inside the network. It inspects the header and content information of network packet moving across the network. The NIDS modules are installed in border routers of IoT and equipped with attack signatures or patterns and compare attack signature with the captured traffic.

IDS having several open issues in IoT system, namely, selection of detection method, attack detection range, management and security of alert traffic, alert correlation and improvement of validation strategies. In addition, the placement of IDS is another issue, Oh et al. and Lee et al. address this issue and proposed a distributed lightweight IDSs for IoT networks. To address this issue, Oh et al. and Lee et al. proposed a distributed lightweight IDSs. Krimmling and Peter also focused on detection method for attacks in IoT networks. Raza et al. also proposed a system that focused detection range of attacks the increased by developing specific modules for Suricata [8, 9].

5.1 Intrusion Detection Approaches

Intrusion detection approaches may be classified into three major categories: misuse detection-based IDSs, anomaly detection-based IDSs and hybrid IDSs [10].

i. **Misuse-based IDSs**
The misuse-based IDSs match the predefined attack signature or pattern with the existing profile; they are also known as rule-based or signature-based IDSs. Although this mechanism is very simple in use, yet it needs a lot of storage space with an increasing number of attacks. If an attack signature is not present in the database or the system is exposed to a new type of attack, this approach may fail. Due to incapability to detect unknown attacks and need of huge storage space to store signatures, this approach is not suitable for resource-constrained IoT devices [6].

ii. **Anomaly-based IDSs**
The anomaly-based IDSs use event-based detection approach by defining the normal behaviour profile of a network. Any activity differing from the normal profile is considered as an intrusion. This approach is more efficient than the misuse-based IDS and can identify the malicious contents in a reliable and precise way. It is however very costly operation for resource-constrained nodes [6].

iii. **Hybrid IDSs**
The hybrids IDSs combine the positive features of both IDSs to minimize the operation cost, storage cost and to achieve higher detection accuracy. An optimized hybrid IDS can be used for resource-constrained devices of IoT [6]. For

Table 1 Confusion matrix

Predicted class			
True class	Total instances	Condition positive	Condition negative
	Condition for positive	True positive	False negative
	Condition for negative	False positive	True negative

evaluating an IDS, we use a confusion matrix, which is defined as follows. The confusion matrix, also called the error matrix, is defined in Table 1.

In this confusion matrix, the following terms have been used that are defined below:

- **True Positive**: It refers to a condition of a legitimate attack that triggers an IDS to produce an alarm.
- **False Negative**: It refers to a condition of an event signalling an DS to produce an alarm when there is no attack.
- **False Negative**: It refers to a condition when no alarm is raised in spite of the fact that an attack has taken place.
- **True Negative**: It refers to an event when no attack has taken place and no detection is made.
- **True Positive Rate**: It is described as the ratio of true positive and the condition positive.
- **True Negative Rate**: It is described as the ratio of true positive and the condition negative.
- **False Negative Rate**: It is described as the ratio of false negative and the condition positive.
- **True Negative Rate**: It is defined as the ratio of true negative and the condition negative.
- **Accuracy of System**: It is defined as the ratio of correctly classified instances and total number of instances.

6 Cyberattacks in IoT Applications

The IoT devices are connected to each other using the networking protocols (IPv6 RPL, 6LoWPAN) and to the worldwide Internet through IP protocols. It makes IoT systems vulnerable to internal as well as external attacks. In an external attack, the intruder is not a part of the network that tries to get access to the system through the internet. In an internal attack, the intruder initiates an attack by the compromised nodes, which are part of the network itself. The possible cyberattacks on IoT are discussed below.

6.1 Wormhole Attack

The wormhole attack is possible in the RPL network. The network traffic and network topology can be very badly disrupted by the wormhole attack. Two intruders create a tunnel and pass all the traffic through it. There are two possible ways an attacker can perform the wormhole attack [1].

- **Packet replay wormhole attack**: A malicious node convinces two nodes, that is, genuine node and neighbour to each of the nodes by relaying the packets. In future, the victim nodes communicate via this malicious node. To perform this type of attack, only one node is sufficient.
- **Packet encapsulation wormhole attack**: To implement this type of attack, two or more malicious nodes are required. A malicious node encapsulates the packet in the payload and sends it to other malicious nodes. Later, one extracts the payload and transmits it.

6.2 Sinkhole Attack

In sinkhole attack, the intruder tries to attract the entire traffic of a particular area through a compromised malicious node inside the IoT network. This malicious node by showing an optimal path to its neighbours creates a metaphorical hole keeping the compromised node as a sink. Since routing information of a node is very difficult to verify, diagnosing the sinkhole is difficult. For example, strong power radio transmitter devices like laptop can provide high-quality routing path by transmitting enough power to cover a wide range of network area can be used to implement such attack [1]. Figure 4 shows the scenario of the sinkhole attack in IoT nodes.

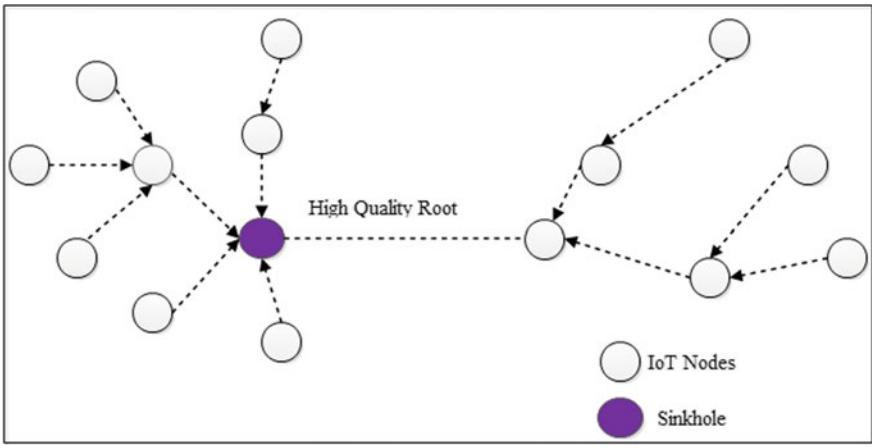


Fig. 4 Artificial high-quality root in sinkhole attack in IoT nodes

6.3 Selective Forwarding Attack

It compromised node may drop some packets and ensures further propagation. The attacker can drop or modify packets and can reliably forward them from a few compromised nodes to limit the suspicion of attack. Selective forwarding can take help from other attacks also, i.e. replay attack, DoS attack, blackhole attack, etc. [1].

6.4 Sybil Attack and Clone ID Attack

In this attack, the intruder keeps the same logical identity on several physical nodes and in sybil attack, the intruder keeps several logical identities on the same physical node. Both attacks aim to gain access to large part of a network [11].

6.5 Hello Flood Attack

In a routing protocol, a sensor node transmissions a hello message to tell its presence to its neighbours. A receiver node of this message may assume that the node is within the transmission range and adds it to its neighbours list. It is possible that the adversary has broadcast the hello message and become a part of the network [1].

6.6 Denial of Service (DOS) Attack

The sensor networks are generally vulnerable to intrusion related to snooping, spoofing, masquerading, Denial-of-Service (DoS) attacks. The DoS attacks impact the network communication partially or completely. As the sensor nodes of IoT are low powered and lossy, the impact of DoS attack is quite significant. For instance, Raymond et al. [12] have discussed the denial-of-sleep attacks on the Wireless Sensor Nodes (WSN) on Medium Access Layer. The intruders attack the power supply of a sensor node that directly affects the network life time. The DoS attack disrupts the communication between devices, making their unavailability. The DoS attack can be carried out externally or internally in IoT and is very hard to detect it unless the services have stopped working. There is also a distributed Denial-of-Service (DDoS) attack in IoT as discussed below.

i. **Flooding Attack**
   In this attack, the attacker overflows the network through sending packets to disrupt the service of legitimate users. Its examples include DNS flood, ICMP flood and UDP flood.

ii. **Reflection-based flooding attack**
The attacker creates several copies of an actual request packet of a legitimate user (victim) and sends it to server/router. The replies corresponding to these requests exhaust the victim sources. Its example includes a Smurf attack.
iii. **Protocol exploitation flooding attack**
The attacker exploits the vulnerabilities in protocol implementation and features of the victim that can consume resources of the victim. Its examples include TCP SYN-ACK flood, SYN flood, ACK PUSH flood, etc.
iv. **Amplification based flooding attack**
The attacker tries to create multiple messages through an application and diverts the traffic towards the victim, which is called amplification of traffic. The BOTNET application can be used for reflection and amplification in a network.

7 Security in IoT Applications

The IoT term, introduced in 1985, became popular in 1999. Many projects are being carried out to design new IoT systems in different fields such as health care, smart cities, smart home, supply chain management, etc. whose security is inevitable. Since the security is a major concern in the deployment of IoT in real-time scenarios, several groups are working on it. The IPv6 RPL and 6LoWPAN protocol enabled resource-constrained devices connected to the public Internet are also vulnerable to various types of attacks. Some cryptographic techniques (authentication and encryption) and network security techniques (IPSec protocols) have been implemented to IoT systems to provide end-to-end or link-to-link security in the communication of IoT devices [11].

7.1 IPSec Capabilities in IoT System

The IPSec provides the security and are as follows:

- In transport mode, the IPSec provides end-to-end security between two nodes in IoT.
- IPSec authentication header protocol ensures the integrity of IPv6 datagram. IPv6 datagram includes IPv6 header and application data.
- IPSec ESP protocol enables data confidentiality and also provides optional data integrity and authentication.

Using CoAP at application and Datagram Transport Layer Security (DLTS) provides end-to-end security. IEEE 802.15.14 may be used for hop-to-hop security in IoT [11].

7.2 Challenges and Design Criteria of IoT Security System

- A security system is not only resistant to attacks, but cab also be able to detect other attacks.
- It should use the capabilities of existing security protocols like IPSec and cryptographic techniques.
- IoT devices are resource constrained and cannot run heavyweight security protocols. So, there is a need to have lightweight protocol that can run efficiently and effectively on IoT devices, i.e. it should be compatible with RPL and 6LoWPAN protocols.
- IoT networks are connected to conventional Internet making them vulnerable to global intrusion along with internal intrusion. The security system designed for IoT must address both types of attacks.
- Apart from conventional cryptographic and network security methods, the IoT needs a security system to detect attacks in real time and raise an alert before intrusion takes place.
- IoT systems are exposed to known as well as unknown attacks. The security system must be capable to detect the misuse and anomaly-based attacks.
- It should have both intrusion detection and prevention capabilities.
- It should be scalable and deployable in most of the IoT systems all over the world.
- There are possibilities of new cyberattacks in future. The security system must be designed in such a way that more modules can be added to detect new attacks.
- It should protect the nodes as well network of IoT system that requires HIDS and NIDS.

7.3 Need of IDSs in IoT

- Although the above security techniques provide security to IoT devices and network, yet these devices are exposed to intrusions inside 6LoWPAN and from the Internet. To protect from these attacks, the intrusion detection system (IDS) acts as the second line of defence to an IoT system.
  - The cryptographic and network security techniques are very complex that consume considerable bandwidth, CPU cycles and power. Hence, they are not appropriate for resource-constrained devices. IoT needs lightweight protocol that can run efficiently in tiny devices of IoT.
  - The cryptographic and network security techniques try to protect an IoT system from intrusion but they do not indicate about intrusive behaviour and may fail at any point of time.
  - The IoT systems are vulnerable to wireless intrusion in addition to external intrusion. There are newer attacks possible in IoT devices and network. So, the

hybrid detection approach of IDS can be helpful in detecting both known and unknown type of attacks.
- The IoT networks are exposed to both internal and external intrusions that must be addressed. The IDS can be deployed at both nodes and IoT network to ensure the security of IoT nodes as well as 6LoWPAN network.
- An IDS can be designed in such a way that more modules can be added in the future if needed.

8 Intrusion Detection System in IoT Applications

Designing of IDSs for IoT applications is an important task. Many authors have discussed IDSs for IoT system that is customized for conventional Internet or WSNs, but they do not meet the requirements of IPv6-connected IoT system. We discuss some existing IDSs, which are customized for IoT applications. Some IDSs have been designed to detect a particular type of cyber-attack as described in Sect. 6. Some are capable to identify all possible potential attacks, which is designed in such a way that more modules can be added if needed to identify new attacks in the future.

8.1 Intrusion Detection System for Dos Attack

IoT is very much susceptible to the DoS attack. Though there are cryptographic techniques, yet they are not able to overcome the DoS attack. The intrusion detection techniques work as the second line of defence to identify the DoS attack in Fig. 5 and other attacks. In [13], an intrusion detection system has been discussed to identify the DoS attack in 6LoWPAN networks before it impacts on the network in IoT; it also triggers an alarm to take preventive measures. The author has used ebbits platform and extended security framework to deploy IDS in ebbits networking framework. It has a physical world and IoT that are connected through the physical world adaptation layer as shown in Fig. 5. In IoT, it is done through network manager and DoS protection manager.

i. **Physical World**
Figure 6 shows an 6LoWPAN network that collects the data from the real-world devices. The smart devices like sensors, smartphone, RFID, etc. are connected to each other to form a physical world. The sensor hosts are connected to cluster nodes to form a network and all cluster nodes are connected to the border routers to deliver the data to network manager. The Physical World Adaption Layer (PWL) is a component of ebbits network to provide communication with the network manager.

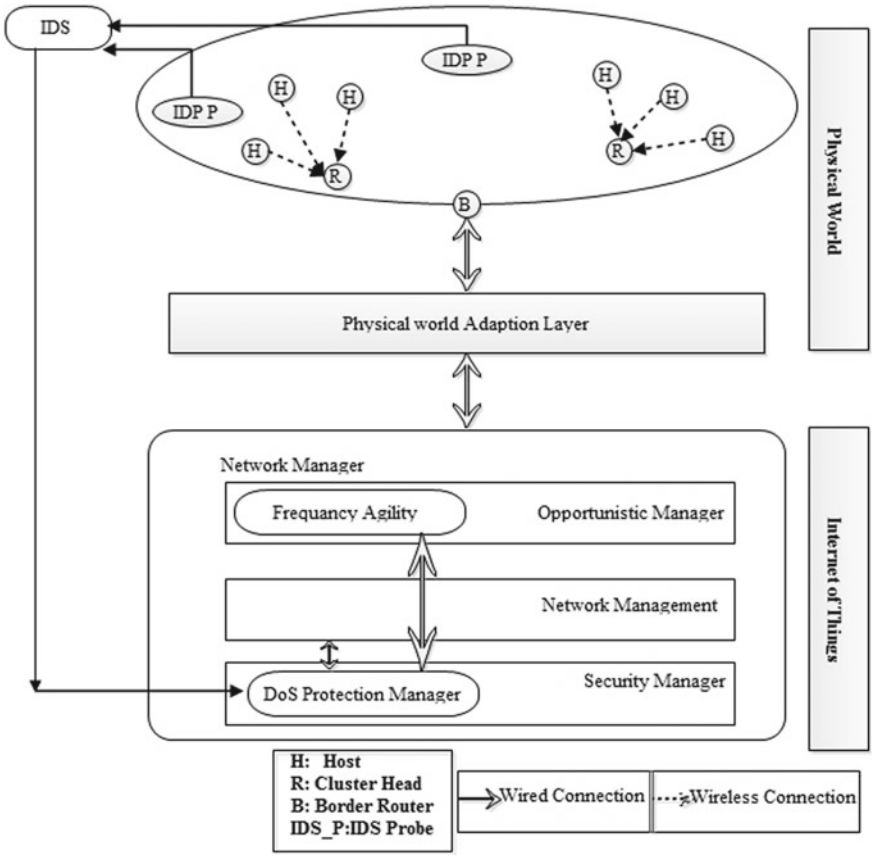


Fig. 5 DoS NIDS architecture

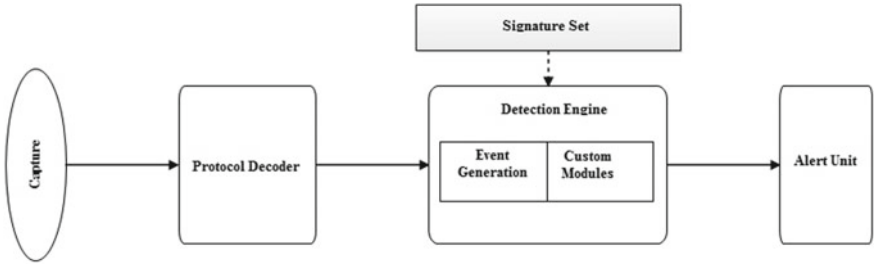


Fig. 6 Suricata IDS' architecture

ii. **Network Manager**
There are three major components of the ebbits network manager: network management, security manager and opportunistic manager. It consists of configuration services and monitoring tools. The opportunistic manager provides the available network communication. The security manager provides secure communication between the ebbits network manager and middleware by using a cryptographic technique [13].

iii. **DoS Protection Manager**
An Intrusion Setection System (IDS) sends an alert to the DoS protection manager in an intrusion scenario and the protection manager collects information from the opportunistic manager and network to get network information like packet dropping rate, average latency, interference rate, etc. in order to verify intrusion.

iv. **Intrusion Detection System**
The network intrusion-based IDS [13] monitors the network traffic with the help of IDS_P. The IDP_Ps are deployed inside 6LoWPAN to monitor the network packets in spite of the fact that it is not a part of the network and does not participate in any network communication. The 6LoWPAN is spread in a large area that requires multiple instances of IDS_P to cover the entire area. A wired connection is required with IDS as the wireless networks are not reliable. The network manager adopts open-source IDS, called Suricata, for its development [14].

v. **Ebbits Plateform**
The ebbits platform connects a public information system and the virtual enterprises by creating a communication infrastructure connect sensor and devices in a physical world dynamically and automatically, e.g. smart home, smart city. It consists of a server for event management, data management, communication, and application execution. It allows integration of new applications developed for ebbits platform.

- **IDS_Probe (IDS_P)**
The IDS probe is discussed in [15] that can sniff the packets in a promiscuous mode and operate with a firmware. It's connected with the IDS via an USB interface and can be realized as other interfaces in Linux system like Ethernet.
- **Suricata IDS**
This IDS supports complete IPv6 protocol and also automatic protocol detection capability. It is a multithreaded system and has an intrusion prevention ability. Since it works for only misuse detection, it requires a predefined set of attack signatures. It has three components as shown in Fig. 6: protocol decoder, detection engine, and alert response unit.
The protocol decoder of Suricata is divided into five layers: application, network, adaptation, data link and physical layers. It can decode a packet at the respective layer. The work [13] has enhanced its decoding capability. The detection obtains the message the IDS_P for a malicious packet. The IDS_P captures the packet and sends it to Suricata decoder that decodes and analyses

to identify any intrusive behaviour with respect to the protocol standard. The detection engine analyses the signature stored in the database and triggers an alarm whenever a signature match occurs.

8.2 *Intrusion Detection System for Wormhole Attack*

Pongle et al. [6] have discussed an intrusion detection system for wormhole attack that provides detection rate of 94, and 87% rate of both attack and attacker detection on the Contiki's network simulator. Figure 7 describes the intrusion detection model of paper [6]. An abnormal change occurs in a network whenever an intrusion, especially in case wormhole attack, happens, which is the basis of anomaly detection as given below.

- When an intrusion happens, more malicious nodes are added into the IoT topology.
- The neighbouring nodes become unreachable during intrusion.
- When a malicious node tries to enter a network, many control packets (DIO, DAO, DIS) exchange takes place through the ends of tunnel.

The intrusion detection system [6] not only detects the wormhole attack in an IoT system but also analyses the true positive rate. It has centralized and distributed modules as discussed below.

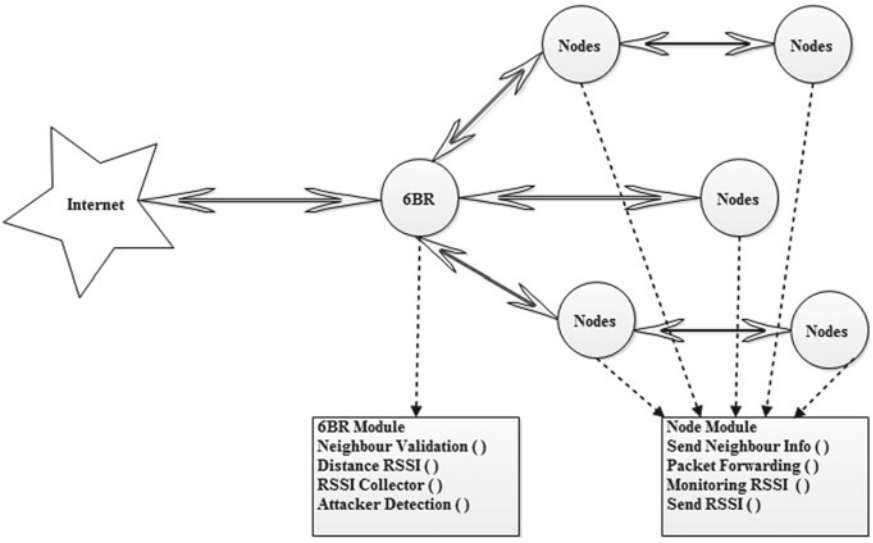


Fig. 7 Architecture of intrusion detection system

a. **Centralized Modules**

Following are the centralized modules in this IDS:

i. **Neighbours validation module**
This module collects the information about the neighbour nodes from all sensor nodes by using the distance between the node and its neighbours. If the distance found more than the transmission range of node, it takes following actions:

- Send the victim packet information to information sender node.
- Send this information to a node having distance more than the transmission range.

Table 2, shows the packet victim packet structure contains Vic_Dest_Field and Vic_coll_Field for destination node and other victim nodes, respectively.

ii. **Distance RSSI module**
The distance Received Signal Strength Indicator (RSSI) calculates the distance between two nodes and acts as converter from strength to distance and vice versa. It also provides the location and range information.

iii. **RSSI Collection module**
This module sends the victim packet to the victim node and waits for transmission to complete. It collects the RSSI value from all victim nodes and sends it to the 6BR; thus, providing the received RSSI values from all the nodes including the victim node in the range of attacker.

iv. **Attacker Detection module**
This module identifies the attacker using the received RSSI using the maximum distance RSSI from all received RSSI of nodes.

b. **Distributed Modules**

Following are the distributed modules in this IDS:

i. **Sender's neighbours information module**
This module stores the initial neighbour as an original neighbour in initialization before any intrusion, which is sent to 6BR through an existing route, if there is any change in neighbour number then the previous one occurs. Table 3, shows the packet structure for the neighbour information.

Table 2 Victim packet structure

2 byte	1 byte	1 byte
CODE(3)	Destination node ID	Other victim nodes
	(Vic_Dest_Field)	(Vic_Coll_Field)

Table 3 Nbr_Info packet structure

2 byte	1 byte	2 byte	1 byte	2 byte	2 byte	2 byte	
Code (2)	Sender node ID	Message instances	Forwarding node ID	Number of neighbours	Neighbour 1	Neighbour 2	…

ii. **Packet forwarding module**
The UDP at transport layer does not provide guaranteed packet delivery to destination; it is done with the help of other nodes to assure packet delivery to root. The urgent packets are sent through a default route and other packets are broadcast. When a non-urgent packet is received, it sent through the default root. A certain delay is introduced between packet transmission to avoid packet collision and buffer overflow. In case of victim, this module forwards the packet in a unicast manner to destination from the root node. Table 4 shows the forwarding packet structure.

iii. **Monitoring RSSI module**
If a node after getting a victim forwarding packet from the root node or broadcast finds its ID in destination node (in the second field) and other victim nodes (in the third field) of victim forwarding packet, it creates the victim broadcast packets by changing the values of the second field with the third field. These two nodes record each other RSSI values to form a victim broadcasted packet, and other nodes also record the RSSI value. To locate the attacker node, two victim nodes broadcast n victim packets.

iv. **Send RSSI module**
To detect intruder, each of n victim packets' recorded RSSI value must reach to the sink node. The packets are sent through broadcast, unicast and by default route to ensure delivery to sink due to unreliable UDP protocol. Each node waits until the victim packet is transmitted and after a certain delay, the RSSI packet is forwarded. Table 5 shows the packet structure of sending RSSI.

8.3 Intrusion Detection System for Sinkhole Attack

The IoT comprises unification and integration of all communication devices and all surrounding objects. The limited resources in IoT devices such limited processing power, storage capacity, link connection loss, low power, cause the routing attacks in IoT and the sinkhole is one such attack, which is very destructive. There have been discussed many methods to prevent sinkhole attack on MANETs, WANETs and WSNs. Most of them have an adverse effect such as high false positive rate, more

Table 4 Victim forwarding packet structure

2 byte	1 byte	1 byte
CODE(4)	Destination node ID	Other victim node ID

Table 5 Packet structure of sending RSSI

2 byte	1 byte	1 byte	1 byte	1 byte
Code (5)	Sender node ID	RSSI value 1	RSSI value 2	RSSI value 3

energy consumption, slow performance, etc. The intrusion detection systems such as watchdog strategies [16], reputation and trust mechanism [17] provide better security to the computer networks by reducing intrusion; but they have not been applied to IoT. The paper [18] has discussed an intrusion detection system to detect the sinkhole attacks in IoT routing services, called intrusion detection for sinkhole attack over 6LoWPAN for Internet of Things (INTI), which provides 70% detection rate with mobile devices and 90% detection rate with fixed devices in the presence of intruder node. It combines reputation and trust strategies, watchdog strategies for detection of intruder by analysing the nodes' behaviour. In reputation and trust strategy, a cluster of nodes based on reputation and trust is considered and the cluster leader analyses the data collected from its members using data redundancy to identify a malicious event. The watchdog strategy works in two phases. In the first phase, the motivating network nodes work in a cooperative manner to collect the evidences and in second phase, watchdogs detects the malicious node on the basis cooperative evidences. These techniques are effective in VANETs and MANETs, but not in IoT. It must be used with other approaches in order to provide security in IoT. This IDS has three components physical network model, communication model and attack model. The physical network model comprises the network devices, which are classified into free node, associated node, cluster node, leader node and base station node. The free nodes are not the part of any cluster that can move within the network. Leader node is associated with many member nodes. Associated node acts as a bridge between two clusters and passes information to other clusters. Leader node gets information from associated node and member nodes and passed this information to base station. The Communication model implements lightweight routing protocol RPL protocol (IPv6 protocol for low power and lossy network) as the IoT devices are resource constrained. In attacker model, an attacker may attack a member node, associated node or leader node in a given time as they are responsible for transmitting the packets. In the sinkhole attack, the attacker announces to other nodes that it has the shortest path to the destination and attracts the entire traffic towards it. It then discards the packets or performs a replay attack. The basic architecture of INTI is discussed below.

a. **INTI Architecture**
   The INIT has four modules that include configuration of cluster, monitoring of routing, detection of attacks and isolation of attacks, as shown in Fig. 8.

   i. **Configuration of cluster module**
      This module defines a leader based on the hierarchal system in order to increase the lifetime and enhance the scalability. A node has a dynamic role over time due to the mobility of devices or intrusion. All nodes are initially free that collect and transmit the control data using broadcasting. The control messages help the neighbouring nodes in deciding a leader. After leader selection, the leader waits for free nodes to join one of the clusters.
   ii. **Monitoring of routing module**
      It counts the number of input and output performed by a forwarding node. The observer node monitors the transmission performed by a node, called top

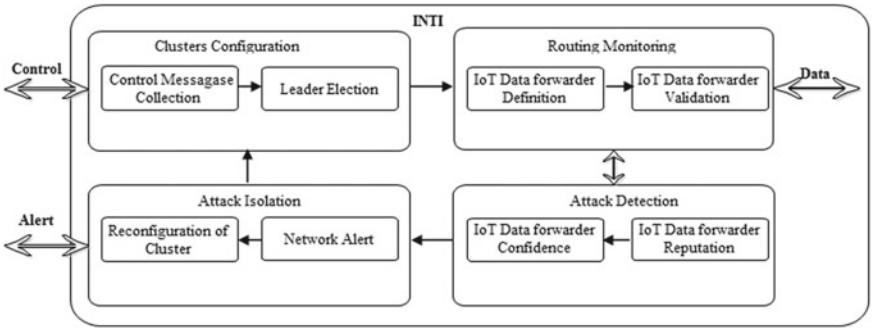


Fig. 8 INTI system architecture

node, which has a lower rank and is responsible for forwarding the packets to the observer node. If output stream count is equal to the incoming count, the node is a genuine node; otherwise, the node deviates from the normal profile.

iii. **Attacker detection module**
It finds the identity of the malicious node that performs the sinkhole attack by estimating the reputation and trust of the nodes to detect intrusion. It continuously maintains the integrity and security of the nodes and based on monitoring operation, the reputation is built inside the cluster or outside the cluster. The reputation is a perception to establish among the nodes by action, iteration, and exchange of information.

iv. **Attacker isolation module**
This module separates out the attacker node once intrusion has been detected. The node that has detected a sinkhole attack triggers an alarm and propagates it to other nodes. This node further sends a restoration message to its neighbours to isolate the attacker node. The restoration message consists of cluster rank to regroup the nodes same order. In case, the attacker node is a member node, cluster leader isolates this malicious node. In case it is the leader itself, either an associated node or a member node isolates this node and a new leader is elected. If it is an associated node, the leader with the largest rank isolates this node.

8.4 Intrusion Detection System for Internet of Things

In [11], an intrusion detection system, called it SVELTE, has been discussed that can detect several attacks like selective forwarding, sinkhole, spoofed routing information in IoT, besides other attacks like Sybil attack, clone ID attack, etc. [19–22].

- Signature-based detection techniques require more storage, whereas the anomaly-based detection techniques require more computation cost. The SVELTE is a hybrid intrusion detection system that maintains the balance between these two requirements.
- SVELTE can identify all types of attacks in IoT in a system as well as in a network.
- An IDS must mitigate the effect of intrusion and remove the malicious node after detecting it. As MAC or IP address can be spoofed easily, the SVELTE uses the white list to keep track of valid nodes.
- Any IoT protocol must be lightweight that can run on a constrained node in 6LoWPAN. The SVELTE is a very effective and lightweight protocol designed for IoT system.
- It should take advantage of existing security techniques such as DTLS and IPSec to provide end-to-end security.
- SVELTE is designed in such a way that it can be deployed at IoT nodes (i.e. HIDS) as well as boarder router (i.e. NIDS). Further, it acts as centralized as well as distributed module both.

The SVELTE has three modules, centralized at 6BR, that include 6LoWPAN Mapper, IDS and a mini firewall. There are two lightweight modules of the centralized module in each node. A module provides mapping information to 6BR to perform intrusion detection system and second module works with the centralized firewall. The third module at each resource constraint device handles end-to-end packet loss. Figure 9 shows the placement of IDS in 6BR.

i. **6LoWPAN Mapper**
The 6LoWPAN (6Mapper) is the main module of SVELTE placed in 6BR that reconstructs the RPL DODAG to provide information about each neighbour and its parent [23–25].

   a. **DODAG Construction**

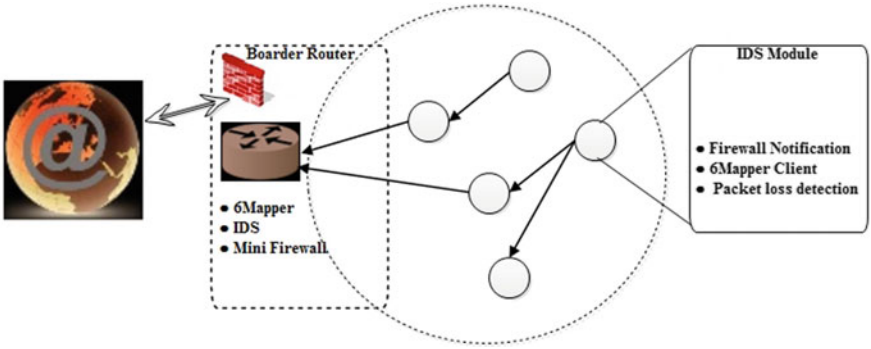


Fig. 9 IDS module placed in 6BR and in sensor nodes of IoT

- At regular interval, the 6Mapper sends mapping request packets to all nodes of the 6LoWPAN network that contain relevant information to identify RPL DODAG like DODAG version number, DODAG ID, RPL instance ID and timestamp of the mapping information
- Each node responds the request packet by appending its rank, its parent ID, all neighbours ID and their corresponding node rank. The Node ID is attached at the beginning of the reply packet by a node.

There are some challenges in Mapping as discussed below.

- Intruder can perform selective forwarding if the packet used to map is distinguishable to each other. It can forward packets only those which are necessary for mapping and may discard others. It, however, can be addressed by encrypting the packet content so that attacker cannot identify it. The message contents are already protected by upper layer security protocol such as DLTS or IPSec.
- To identify network mapping traffic, intruder can use the IP header and 6Mapper's host address. That is why IP header should not disclose any information that enables an attacker to identify that packet is used by 6Mapper. This issue can be addressed by assigning multiple IPv6 addresses to the 6Mapper, which is equal to the number of nodes in the network. When an attacker hacks a node, it will only know the mapping address of an individual node. Thus, the attacker cannot distinguish between the mapping packet and ordinary packet.
- In case the information sent by a node to mapper becomes oudated or an attacker changes the information intentionally, there may be inconsistency in mapping responses with each other. This may lead to a false alarm, if not controlled properly. This issue is addressed by an IDS system that can detect network inconsistencies.

ii. **IDS in SVELTE**
In [11], an IDS that uses 6Mapper has designed that describes three techniques: inconsistency detection in network graph, node availability checking and routing graph validity.

a. **Inconsistencies detection in network graph**
In IoT, an individual node can be hacked that can be used to perform other attacks. In 6LoWPAN RPL network, a hacked node can be used to send the altered rank information and rank of its neighbours. The IoT links are lossy that may cause inconsistencies in the information of network nodes. So, it is important to identify valid and invalid consistencies that must be rectified. Each node is verified to check consistency in the network and to detect incorrect information. The 6Mapper provides rank and node ID of the parent and neighbours of a node. Each edge is validated in the network about their rank to detect inconsistencies between two nodes. There is a possibility of false alarm because valid inconsistencies in mapping may occur due to the detected incorrect information. The valid and invalid consistencies can be detected using the number of faulty ranks report and the difference between reports of rank. A threshold value is used and if disagreement count is more than the threshold value, the node is classified as faulty. In case an

inconsistency is detected, the SVELTE either corrects it or removes the node. If the inconsistency occurs for the first time, it does not remove the node and corrects the faulty information as it may be due to valid consistencies. It keeps track of this information and if the same node is found faulty again, this node is removed from the whitelist maintained by 6Mapper.

b. **Node Availbilty Detection**
The detection of availability and its proper operability of a node or a set of nodes is important in IoT. A hacked node may launch other attacks in the network such as selective forwarding attack in which the malicious node drops the packet intelligently. For example, in RPL network, the CoAP protocol is used to send application data; an adversary can drop CoAP traffic and selectively forward the RPL traffic. Thus, network would behave as working properly but no useful traffic. The RPL DADOG routing table can be used as a basis of available node and the whitelist of valid nodes as the basis of detecting the nodes in the network. The nodes in whitelist are compared with RPL DODAG and the resultant difference is unauthorized nodes.

c. **Validity of routing graph**
An intruder can reshape the network topology to control the traffic in order to disrupt the network by broadcasting the false routing graph. For example, an attacker can advertise a good rank to its all neighbours in order to attract the traffic flow towards it, which is called the sinkhole attack. The SVELTE has been designed to detect the sinkhole attack by analysing network topology as inconsistency in routing graph indicates the intrusive behaviour in the network. In case a parent has higher rank that is child, it refers to a fault in the network as in RPL, the parent cannot have a higher rank than its child. The sinkhole attack can be detected by this method as an attacker will advertise the beneficial rank which is most likely to better rank than the parent. To remain sinkhole attack successful, the adversary must advertise a rank not better than the parent. This would increase adversary's node rank slightly over other nodes and thus, the impact of the attack would very little.

d. **Protection from clone ID and validity of Sybil attack**
In clone ID attack, an intruder keeps the same logical identity on several physical nodes, whereas in Sybil attack, an intruder keeps several logical identities on the same physical node. Both attacks try to gain access to a large part of the network. In SVELTE, the 6Mapper believes on the latest information received from each node and each node is identified by an IP address. The 6Mapper treats each node individually and if the identities of several devices are copied on to the same physical device, it hardly makes any impact. Thus, the Sybil attack has no impact on SVELTE. Since the 6Mapper considers the latest information from one of the nodes. It does not consider any difference if two clone nodes send the information to it. Thus, the Sybil attack may interrupt routing in a network, but it does not affect the 6Mapper directly.

e. **Protection from Hello flood attack**
In a routing protocol, a sensor node broadcasts a hello message to inform its presence to its neighbours. A node receiving this message may assume that node in its transmission range and adds it in the list of its neighbours. In SVELTE, the 6BR keeps the record of RSSI value received from each node. In [1], a method has been discussed that can be used in 6BR to detect the hello flood attack. It is assumed that communication is within a fixed transmission range which is very common in IoT. For each node if RSSI value is equal to fixed signal strength, then the node can be added to the network; otherwise, it is added into the blacklist and an alarm is generated. Two ray propagation models are used to calculate the fixed signal strength [26].

iii. **Mini firewall**
The SVELTE can detect and prevent an intrusion in 6LoWPAN network; however, the resource-constrained nodes are secured against global intrusion. For example, the denial-of-service attack from an outside network to 6LoWPAN network can easily be done. A firewall or the modules of 6BR cannot inspect the contents of a packet as end-to-end security is must in IoT. So, it is very difficult to differentiate between the legitimate and malicious traffic. Therefore, the mini firewall has been integrated with modules of 6BR to work in a cooperative manner with nodes of a 6LoWPAN network. This firewall can protect a 6LoWPAN network from an external host intrusion. It has a module in 6BR as well as in each resource constraint node in a distributed manner that provides both misuse and anomaly detection capabilities, making it suitable for real-time scenarios. The destination node can see the packet contents in 6LoWPAN network, analyse its behaviour to identify malicious activity, and sends a notification to 6BR. It helps to filter the traffic from the compromised host before it reaches to the nodes of the 6LoWPAN network.

There are a number of potential attacks and more attacks will be discovered against IoT. The SVELTE can be designed in such a way that it can be extended easily to detect other attacks. The 6Mapper can be extended easily conceptually as well as practically. The response packet can be extended if new intrusion detection requires more data to be added in the network graph. One can design a hybrid IDS using the data mining tools, machine learning, feature vectors or automata based approaches. It is possible to detect wormhole attack if the 6Mapper is extended with a signal strength of each neighbour node [26].

8.5 Comparative Analysis of SVELTE and INTI IDSs

Both the IDSs have been implemented in Coja simulator [27] and they have been compared in terms of efficiency and effectiveness to mitigate the sinkhole attacks.

They have been tested in terms of four parameters that include the detection rate, false positive rate, false negative and delivery rate [18].

- **Detection Rate**
  This parameter correctly classifies the incidences. The INTI and SVELTE provide 92% and 90% detection rate, respectively, for static scenario and in mobile case, it drops to 24% and 70%, respectively.
- **False Negative Rate**
  It is an amount of time attacks that were considered negative by the system. The INTI and SVELTE provide 28% and 38% false negative rate, respectively, for a scenario with mobile nodes.
- **False Positive Rate**
  It is amount of times sinkhole attack that were considered positive. The INTI and SEVLTE provide 3% and 4% false positive rate with fixed nodes and 30% and 39% with mobile nodes, respectively.
- **Delivery rate of packets**
  It is the number of packets delivered to the destination successfully, given by ratio of packet reached to the destination with respect to the number of packet originated from the source. In fixed scenario, the INTI has 95% delivery rate and the SVELTE has 99%. In mobile scenario, the INTI has more than 55% delivery rate and the SEVLTE does not support mobility.

9 Conclusion

In this chapter, we have discussed about the intrusion detection systems in IoT systems as most of IoT systems are prone to attacks at the operational phase. Initially, we discussed IoT architecture and its life cycle followed by a comparative study of the IoT protocol stack and conventional IoT protocol stack. The IoT protocol stack implements lightweight protocols for the resource-constrained devices like RPL, 6LoWPAN, CoAP, etc. The IoT systems are an IP connected network and hence vulnerable to the internal and external attacks. The IPSec and cryptographic techniques can be applied to an IoT system, but they have their limitation and complexities. The IDSs are very helpful in IPS design for IoT systems and they are collaboratively quite effective to prevent an attack in an IoT network. The IPv6 Internet protocol is used to connect millions of devices to the internet via IP. To design an IDS for an IPv6-connected network, which is compatible with RPL and 6LoWAPN network, is a challenging issue. Currently, there are no IDSs that can meet the requirement of an IPv6-connected network. Most of them are either customized for conventional Internet or the MANETs. We have discussed some of the recently developed IDSs for IoT and analysed them with respect to IoT systems. SEVLTE has been designed in such a way that it can detect all possible attacks and it can also be extended to detect new attacks in the future. We also provided a comparative performance in terms of false positive, true positive and accuracy in IoT systems in both fixed scenario and

in mobility. We have found that the accuracy of these IDSs fluctuates significantly for mobile nodes.

References

1. Sherasiya, T., Upadhyay, & H., Patel, H. B. (2016). A survey: Intrusion detection system for internet of thing. *International Journal of Computer Science and Engineering*, *5*(2), 91–98.
2. Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S. L., Kumar, S. S., & Wehrle, K. (2011). Security challenges in the ip-based Internet of Things. *Wireless Personal Communications, 61*(3), 527–542.
3. Garcia-Morchon, O., Kumar, S., Struik, R., Keoh, S., & Hummen, R. (2013). Security considerations in the ip-based Internet of Things (pp. 1–19).
4. Hameed, S., Khan, F. I., & Hameed, B. (2019). Understanding security requirements and challenges in Internet of Things (IoT): A review. *Journal of Computer Networks and Communications, 2019,* 1–14.
5. Neto, A. L. M., Souza, A. L. F., Cunha, I., Nogueira, M., Nunes, I. O., Cotta, L., et al. (2016). Aot: Authentication and access control for the entire iot device life-cycle. In *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM* (pp. 1–15). ACM.
6. Pongle, P., & Chavan, G. (2015). Real time intrusion and wormhole attack detection in Internet of Things. *International Journal of Computer Applications*, 1–9.
7. Fuchsberger, A. (2005). Intrusion Detection Systems and Intrusion Prevention Systems: Information Security Technical Report 10 (pp. 134–139).
8. Zarpelao, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications, 84,* 25–37.
9. Sherasiya, T., & Upadhyay, H. (2016). Intrusion detection system for Internet of Things. *International Journal of Advance Research* and *Innovative Ideas* in *Education (IJARIIE)*, *2*(3), 2244–2249.
10. Govindarajan, M., & Chandrasekaran, R. M. (2011). Intrusion detection using neural based hybrid classification methods. *Computer Networks*, 1662–1671.
11. Raza, S., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. *Ad Hoc Networks*, 2661–2674.
12. Naika, S., & Shekokarb, N. (2015). Conservation of energy in wireless sensor network by preventing denial of sleep attack. *Procedia Computer Science*, 370 – 379.
13. Kasinathan, P., Pastrone, C., Spirito, M. A., & Vinkovits, M. (2013). Denial-of-Service detection in 6LoWPAN based Internet of Things. In *9th International Conference on Wireless and Mobile Computing, Networking and Communications* (pp. 1–8). IEEE.
14. Suricata—The next generation intrusion detection system. http://www.openinfosecfoundation.org.
15. Tomasi, R., Bruno, L., Pastrone, C., & Spirito, M. (2011). Meta-exploitation of ipv6-based wireless sensor networks. In *3rd International workshop on Security and Communication Networks* (pp. 39–44).
16. Wahab, O. A., Otrok, H., & Mourad, A. (2014). A cooperative watchdog model based on dempster–shafer for detecting misbehaving vehicles. *Computer Communications*, 43–54.
17. Perez-Toro, C. R., Panta, R. K., & Bagchi, S. (2010). Rdas: Reputation-based resilient data aggregation in sensor network. In *7th IEEE Communications Society Conference on Sensor Mesh and Ad Hoc Communications and Networks* (pp. 1–9).
18. Cervantes, C., Poplade, D., Nogueira, M., & Santos, A. (2015). Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things. In *IEEE International Symposium on Integrated Network Management* (pp. 606–611).

19. Bhatt, C., Dey, N., & Ashour, A. S. (Eds.) (2017). *Internet of Things and Big Data technologies for next generation healthcare* (pp. 978–3).
20. Dey, N., Hassanien, A. E., Bhatt, C., Ashour, A., & Satapathy, S. C. (Eds.) (2018). *Internet of Things and big data analytics toward next-generation intelligence*. Berlin: Springer.
21. Hassanien, A. E., Dey, N., & Borra, S. (Eds.). (2018). Medical Big Data and internet of medical things: Advances, challenges and applications. CRC Press.
22. Binh, H. T. T., & Dey, N. (Eds.). (2018). *Soft computing in wireless sensor networks*. CRC Press.
23. Das, S. K., & Tripathi, S. (2018). Energy efficient routing formation algorithm for hybrid ad-hoc network: A geometric programming approach. *Peer-to-Peer Networking and Applications*, 1–27.
24. Das, S. K., Yadav, A. K., & Tripathi, S. (2017). IE2 M: Design of intellectual energy efficient multicast routing protocol for ad-hoc network. *Peer-to-Peer Networking and Applications, 10*(3), 670–687.
25. Yadav, A. K., Das, S. K., & Tripathi, S. (2017). EFMMRP: Design of efficient fuzzy based multi-constraint multicast routing protocol for wireless ad-hoc network. *Computer Networks*, *118*, 15–23.
26. Rappaport, T. S. (1996). *Wireless communications: Principles and practice* (Vol. 2). New Jersey: Prentice Hall PTR.
27. Österlind, F., Dunkels, A., Eriksson, J., Finne, N., & Voigt, T. (2006). Cross-level sensor network simulation with Cooja. In *Proceedings of 31st IEEE Conference on Local Computer Networks* (pp. 641–648).

Deep Learning and Machine Learning Techniques for Intrusion Detection and Prevention in Wireless Sensor Networks: Comparative Study and Performance Analysis

Pankaj R. Chandre, Parikshit N. Mahalle and Gitanjali R. Shinde

Abstract Nowadays, there is remarkable growth in technology and wireless sensor networks. These are primarily used for the purpose of communication. Communication between devices may be wired or wireless, hence, the chance of attacks through the networks is increasing daily. For secure communication, intrusion detection and prevention are primary concerns. Thus, analyses of intrusion detection and prevention techniques have become an important part of the engineering field. With the assistance of intrusion detection and prevention system, we are able to determine and then notify the normal and abnormal activities of the users. Thus, there's a requirement to design effective intrusion detection and prevention system by exploitation machine learning and deep learning for wireless sensor networks. In this work, a comparative study and performance analysis of different machine learning and deep learning techniques are given for intrusion detection and prevention system. The performance evaluation of these techniques is done by experiments conducted on WSN-DS dataset. The comparative analysis shows that deep learning classifiers shows better intrusion detection results than machine learning techniques. In this work, Convolutional Neural Network classifier is used.

Keywords Wireless sensor networks · Deep learning · Intrusion detection, and prevention system · WSN-DS

P. R. Chandre (✉) · P. N. Mahalle · G. R. Shinde
Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Savitribai Phule Pune University, Pune, India
e-mail: pankajchandre30@gmail.com

P. N. Mahalle
e-mail: aalborg.pnm@gmail.com

G. R. Shinde
e-mail: gr83gita@gmail.com

S. K. Das et al. (eds.), *Design Frameworks for Wireless Networks*,
Lecture Notes in Networks and Systems 82,
https://doi.org/10.1007/978-981-13-9574-1_5

1 Introduction

As we know that wireless sensor networks consists of a large number of nodes, which are distributed over a large space and one or more nodes can work as a Base Station. Basically, a sensor node deals with the information collection and then sends the collected information to the Base Station for the purpose of analysis. As we know, WSN has become an integral part of today's applications such as military, health care, industry, traffic control, home automation, environmental, and many more commercial applications [1]. Actually, a sensor node is different from a normal node like they are small in size and cost is low [2]. Again, a sensor node has limited energy, less memory capacity, and low bandwidth [3, 4]. Due to these features of a sensor node, security is a significant issue in WSN [5]. Because of the significant use of WSN, a sensor node becomes attractive to different types of attacks such as black hole, grayhole, flooding, Denial of Service, and TDMA. These attacks allow modifying collected data, and that may destroy the entire network also [6].

Deep learning techniques are mostly used to identify various types of attacks [7]. As we know that deep learning deals with data analysis which is used to build an analytical model. Nowadays, deep learning strategies are ending up ever fundamental because of different variables like expanding volumes and amounts of accessible information, the count procedure, which is less expensive and all the more incredible and moderate information stockpiling [8]. Deep learning techniques can construct snappy and naturally creating models which can investigate progressively noteworthy, increasingly complex information and convey quicker, progressively exact outcomes on an expansive scale. This examination procedure further encourages associations in distinguishing beneficial chances and keeping away from obscure dangers. A variety of attacks against WSNs are flooding, black hole, grayhole, TDMA, and many more.

The main aim of this paper is to provide a comparative study and performance analysis using different deep learning and machine learning techniques for intrusion detection and prevention for WSNs [9]. Machine learning techniques used are Random Forest (RF), K-Nearest Neighbors (KNN), Decision Tree (DT), Naïve Bayes (NB), and Support Vector Machine (SVM) [10]. For analysis purpose, an WSN-DS [11] is used as a dataset and Python is used as a programming language. An WSN-DS dataset consists of information about 4 types of attacks and consists of 19 columns as an attribute.

2 Literature Survey

Similar work in the field of discussion and gap analysis of the discussed methods adopted are presented in this section. A discussion on the existing literature related to the topic is presented below.

Myint and Meesad have proposed have proposed one classifier known as an Incremental Learning Algorithm, which is based on SVM [12]. In this, a prediction is done by using SVM and is going to reduce steps required for calculation and complexity of the algorithm, error set, and time is saved for repeatedly training the dataset. KDD Cup99 is used as a dataset to check the performance of the system. The proposed system can predict 41 features of the incoming dataset.

Nabila Farnaaz and M. A. Jabbar have proposed a model using RF classifier for intrusion detection [13]. The author considered RF as an ensemble classifier, and the model gives a better performance as compared to other traditional classifiers for the purpose of classification of attacks. For implementation purpose, NSL-KDD is used as a dataset, and the proposed model is efficient with a low false alarm rate and high detection rate [14].

Majjed et al. have proposed an effective deep learning approach STL-IDS supported the self-taught learning framework [15]. For feature learning as well as to reduce the dimension, the proposed system can be used. In this approach, to achieve a greater prediction accuracy of SVM the training as well as testing time is reduced. The proposed approach provides an improvement in network intrusion detection [16].

Sandhya Peddabachigari et al. have evaluated the decision tree for intrusion detection [17]. Intrusion detection with the decision was tested with 1998 DARPA dataset, and the system gives better performance as compared to traditional models in terms of accuracy. Again the results show that the training time and testing time is better as compared to Support Vector Machine.

Mrutyunjaya Panda and Manas Ranjan Patra have proposed a framework of NIDS based on Naïve Bayes [18]. For implementation KDD Cup 99 is used as a dataset and from the results, it is determined that the planned system offers higher performance in terms of false positive rate, procedure time and price.

Muna AL-Hawawreh et al. have proposed an irregularity location system for IICSs dependent on profound learning models that can learn and approve utilizing data gathered from TCP/IP parcels [19]. It incorporates a successive preparing process executed utilizing a profound autoencoder and profound feedforward neural system engineering, which is assessed utilizing two surely understood system datasets, to be specific, the NSL-KDD and UNSW-NB15. As the trial results exhibit that this method can accomplish a higher recognition rate and lower false positive rate than eight as of late created strategies, it could be actualized in genuine IICS conditions [20].

Hongtao Shi et al. have proposed another element streamlining approach dependent on profound learning and Feature Selection procedures to give the ideal and hearty highlights for traffic arrangement [21]. Right off the bat, symmetric vulnerability is abused to expel the insignificant highlights in system traffic informational collections, at that point, a component age show dependent on profound learning is connected to these applicable highlights for dimensionality decrease and highlight age, at last, Weighted Symmetric Uncertainty is misused to choose the ideal highlights by expelling the repetitive ones [22]. In light of genuine traffic follows, exploratory outcomes demonstrate that the proposed methodology cannot just effec-

Table 1 Comparative evaluation of machine learning classifiers

Paper no.	Classifier used	Precision	Recall	F1 Score
Shelke et al. [9]	Random Forest	99.67	95.30	98.67
Niyaz et al. [10]	Support Vector Machine	79.40	67.40	79.34
Almomani et al. [11]	Decision Tree	99.96	99.64	99.64
Myint and Meesad	Naïve Bayes	96.00	99.80	85.80
Al-Qatf et al. [14]	Support Vector Machine	95.80	96.80	70.00
Peddabachigari et al. [15]	K-Nearest Neighbor	85.20	83.00	82.40

tively decrease the element of highlight space, yet additionally beat the negative effects of multiclass lop-sidedness and idea float issues on ML techniques [23].

Wenchao Li et al. have proposed a new intrusion detection system based on K-nearest classification algorithm in WSN [24]. The proposed system is used to separate normal and abnormal node by monitoring the unusual behavior. In this, parameter selection and error rate of the intrusion detection system is analyzed. The proposed model gives better efficiency with a high detection rate and speed.

Table 1 shows the comparative evaluation for machine learning classifiers in terms of precision, recall, and F1 score. In Table 1, the authors have used KDD dataset for testing the application. The work presented in the literature survey shows that many more systems are available to detect intrusion in WSNs and intrusion detection already reached saturation. So, there is a need to design a system that will be able to prevent intrusion in WSNs.

3 Proposed Methodology

As we know that an intrusion detection system the only header is analyzed and on the basis of that some decisions are taken. But we are going to provide intrusion prevention system, in which headers, as well as payload both, are analyzed, and then some decisions are taken out. For the purpose of proactive intrusion prevention system, we are going to used supervised machine learning techniques. The proposed system will be able to detect and prevent intrusion with higher accuracy. The proposed architecture consists of multiple stages. The stages are as follows and depicted in Fig. 1:

Input—For the proposed system, we are going to provide a packet as an input. After providing packet as an input, we are going to consider header as well as payload for the purpose of analysis.
Preprocessing—After receiving a packet as an input, we need to perform preprocessing of the received packet. In preprocessing, we can consider feature extraction.
Learning—The next and important step in this is learning. Learning step deals with dividing given dataset into two parts, i.e., training dataset and testing dataset. So,

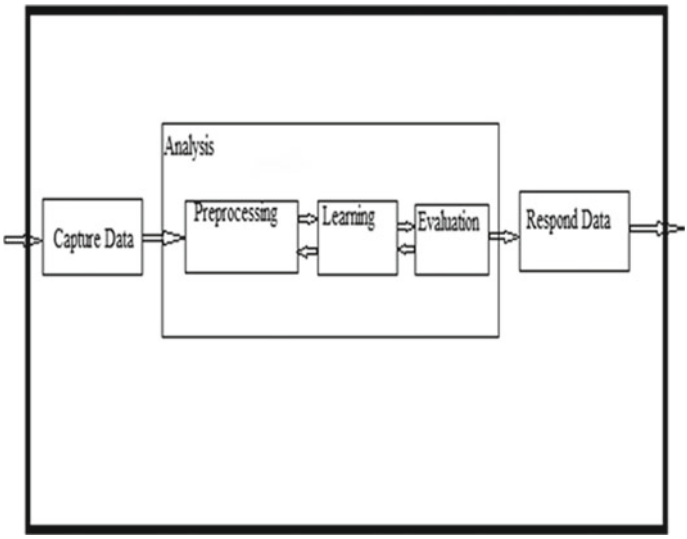


Fig. 1 System architecture for intrusion detection and prevention system

after dividing the dataset into two parts, we will apply machine learning model for the purpose of prediction.
Output—This step deals with the results generated by learning step. So simply, we can consider output as a filtered packet.

In the proposed system, the data received will be checked against dataset used or we can consider the real-time data for testing purpose. For learning purpose, two or more classifiers will be merging together to achieve better accuracy and the proposed system will prevent the attacks like grayhole, black hole, flooding, and TDMA.

4 Comparative Analysis and Discussions

As we know that machine learning consists of multiple statistical methods, which are used to handle regression and classification tasks with various dependent and independent variables [25].

In this paper, to measure the performance of the mentioned techniques, performance metrics are used. To calculate these performance metrics, value of attributes which resulted from training as well as testing dataset of WSN-DS are used. These values are often outlined as follows [26]:

True positive (TP): It can be outlined as, anomaly instances properly categorized as an anomaly.
False positive (FP): It can be outlined as, normal situations wrongly categorized as an anomaly.

True negative (TN): It can be outlined as, normal situations properly categorized as normal.
False negative (FN): It can be outlined as, anomaly instances wrongly categorized as normal.

Then, we can calculate the performance metrics using the following equations.

Accuracy (ACC): It is a metric which is used to indicate the proportion of correct classifications of the total records in the testing set.

$$ACC = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

Precision (P): It is a metric which measures the actual performance within the required answer space, i.e., among the positions.

$$P = \frac{TP}{TP + FP} \tag{2}$$

Recall (R): It is the metric by which we measure how much of the predicted answers are actually discarded or for every correct label, how many other true labels have we discarded.

$$R = \frac{TP}{TP + FN} \tag{3}$$

F1 Score (F): It is the harmonic mean of the two matrices P and R.

$$F = \frac{2 * P * R}{P + R} \tag{4}$$

In this, we have provided WSN-DS dataset as an input, and it is 90% of the entire dataset. Basically, an WSN-DS dataset is used for WSNs. An WSN-DS dataset is divided into two parts, i.e., train dataset and test dataset. Train dataset consists of 80% random samples and test dataset consists of 20% random samples of an entire dataset. A dataset consists of total 19 attributes, and 1 attribute is considered as a label for the purpose of prediction. An WSN-DS dataset is displayed by using Python script which is shown in Table 2. The formal working steps of all classifiers in Python are given below.

Step 1: Importing Libraries
In this, with the help of some script, we can import required libraries.

For example, import pandas as pd.

In our example, we have imported library pandas as a pd. Basically, pandas is an open-source library and provide high performance, it is easy to use, and data analysis tool for Python programming language.

Table 2 An WSN-DS dataset

Id	Time	Is_CH	Who CH	Dist_To_CH	ADV_S	ADV_R	JOIN_S	JOIN_R
0	101000	50	1	101000	0.00000	1	0	0
1	101001	50	0	101044	75.32345	0	4	1
2	101002	50	0	101010	46.95453	0	4	1
3	101003	50	0	101044	64.85231	0	4	1
4	101004	50	0	101010	4.83341	0	4	1

Step 2: Importing the Dataset

We can download datasets, which are available online [27]. For this research work, we have used datasets, which are stored on your system. We have a dataset as an CSV file with name WSN-DS, which is stored on E drive with folder name PNM on your system. Then we can use some script to read the dataset from this location.

For example,

df= pd.read_csv('E:\PNM\WSN-DS.csv')

Step 3: Data Preprocessing

Normally, data preprocessing consists of two steps. First, we have to divide data into attributes and labels and in the second, we have to divide data into train data and test data. To divide our data into attributes and label, just consider we have dataset with 19 fields. So simply, we can consider last filed as a label and first 18 fields as a attribute. For this, we can use Python script. For example,

Train_x= df_svc.iloc[:200000,2:-1]

Train_y= df_svc.iloc[:200000,-1]

Step 4: Train and Test

In research work, dataset is divided into two parts, i.e., train data and test data. Just consider we have a dataset with 300000 entries, so simply, we can divide entire dataset into train (80%) and test (20%) or train (70%) and test (30%). For splitting of dataset, we can use Python script. For example,

Train_x= df_svc.iloc[:200000,2:-1]

Train_y= df_svc.iloc[:200000,-1]

Test_x= df_svc.iloc[200000:,,2:-1]

Test_y= df_svc.iloc[200000:,-1]

In above example, we have considered first 200000 entries for train data and remaining 100000 entries for test data.

Step 5: Training the Algorithm

As we know that we have divided our dataset into train data and test data. Now, we have to train our algorithm by using some classifiers. To train our algorithm, we can use support vector machine, random forest, k-nearest neighbors, naïve Bayes, and decision tree as a classifier.

Step 6: Making Predictions
We have trained our algorithm, now, it's time to make predictions on the test data. So, for making predictions, we can use predict class.

For example, y_pred=models.predict(test_x).

Step 7: Evaluating the Algorithm
As usual, we can consider evaluation is nothing but the last step of our algorithm. For this, simply, we are interested to consider some metrics like precision, recall, and F1 score.

Step 8: Results
After evaluating our algorithm, we are going to display our results by printing a classification report. For this, we can use Python script.

For example,

print(classification_report(test_y, y_pred).

Table 2 shows the WSN-DS dataset. We can display the shape of the train and test data by using Python script.

For example, train_x.shape.

With the help of the above Python script, entries of the train data will be displayed like (200000, 16). It means train dataset consists of 200000 rows and 16 columns.

For example, test_x.shape.

With the help of Python script, entries of the test data will be displayed like (100000, 16). It means test dataset consists of 100000 rows and 16 columns.

These methods of machine learning are as follows:

4.1 Support Vector Machine

This section deals with the background, mathematics, principle, and advantages of Support Vector Machine classifier.

Background
Basically, SVM classifier is used for the classification and regression. In SVM, data is spat into data point by using hyperplane and it is used to determine the class of data point [28]. Nowadays, SVM is incredibly well-liked technique because of its accuracy and performance [29]. The distance from the boundary to the nearest data point is called as margin and the data point that lies closest to the classification boundary is called as support vector. When we deal with SVM, then we have to assume two things like

The margin should be as large as possible and
The support vectors are the most useful data points because they are the ones most likely to be incorrectly classified.

Mathematical Foundations

When we deal with SVM classifier, we need to deal with some concepts that we are going to use later. These concepts are as follows:

Length of a vector: The length of a vector v is known as its norm and it can be mentioned as ||v||. The Euclidean norm formula to compute the norm of a vector v = (v1, v2, v3, …, vn) is given as

$$||V|| = \sqrt{v_1^2 + v_2^2 + \cdots + v_n^2} \tag{5}$$

Direction of a vector: The direction of a vector v = (v1, v2, v3, …, vn) is mentioned as d and it can be defined as

$$d = \left(\frac{d_1}{||d_1||}, \frac{d_2}{||d_1||} \right) \tag{6}$$

Hyperplane: The two-dimensional linearly separable data can be separated by a line. The function of the line is $y = ax + b$. We can rename x with $x1$ and y with $x2$ and we will get

$$ax1 - x2 + b = 0 \tag{7}$$

If we define $\mathbf{x} = (x1, x2)$ and $\mathbf{w} = (a, -1)$, we will get

$$w \cdot x + b = 0 \tag{8}$$

This equation is derived from two-dimensional vectors. Normally, it also works for any number of dimensions. This is the equation of the hyperplane.

Principle

The working steps for Support Vector Machine are as follows:

Step 1:

We need to define optimal hyperplane: maximize margin.

Step 2:

Extend the definition mentioned in Step 1 for nonlinearly separable problems: have a penalty term for misclassifications.

Step 3:

Map data to high-dimensional space where it is easier to classify with linear decision surfaces: reformulate problem so that data is mapped implicitly to this space.

For an implementation of SVM, an WSN-DS is used as a dataset and Python is used as a programming language. The working steps of SVM classifier are applied to obtain the results. The results obtained after implementation are shown in Tables 3 and 4.

Table 3 shows the attacks predicted using SVM classifier. In Table 3, for ID number 16 and 147, actual attack type were flooding and normal but these attacks are predicted as normal and TDMA, respectively.

Table 3 Attacks predicted using SVM

	Actual_Attack_Type	Pred_Attack_Type
16	Flooding	Normal
19	Grayhole	Normal
40	Grayhole	Normal
44	Blackhole	Normal
46	Grayhole	Normal
91	TDMA	Normal
107	Grayhole	Normal
113	Grayhole	Normal
128	Grayhole	Normal
131	Flooding	Normal
132	Grayhole	Normal
138	Blackhole	Normal
144	Grayhole	Normal
147	Normal	TDMA
156	Flooding	Normal

Table 4 Classification report for support vector machine

	Precision	Recall	F1-Score
Blackhole	1.00	0.40	0.57
Flooding	0.00	0.00	0.00
Grayhole	0.00	0.00	0.00
Normal	0.93	1.00	0.96
TDMA	0.67	0.44	0.53
Avg/Total	0.88	0.92	0.90

Table 4 shows the classification report for SVM, in which black hole, flooding, grayhole, and TDMA attacks were detected. The accuracy of SVM is 89.00% and it is the average accuracy of all attacks.

Evaluation of Support Vector Machine classifier

The advantages of SVM classifier are as follows:

- The main advantages of SVM are that it works very well on the small and clean dataset.
- SVM is more efficient because it uses subsets of the training dataset.
- SVM is superb at computation speed and memory.
- SVM provides more accurate results.

The disadvantages of Support Vector Machine classifier are as follows:

- SVM not suitable for larger dataset because it requires more time to train data.
- SVM is less effective on noisier dataset.

SVM has many parameters that need to be set correctly to achieve better classification results for any given problem.

4.2 Naïve Bayes

This section deals with the background, mathematics, principle, and advantages of Naïve Bayes classifier.

Background

Basically, the Naïve Bayes method is used to perform classification. Naive Bayes methods are a set of supervised learning algorithms with the naïve assumption of independence between every pair of features [30]. Basically, a naïve Bayes classifier is an algorithm, which classifies the objects using Bayes theorem. Naive Bayes classifier assumes naïve or strong, independence between the attributes of data points [31]. Naïve Bayes classifier is used in spam filters, text analysis, and medical diagnosis and is widely used in machine learning because it is very simple to implement.

Mathematical Foundations

Naïve Bayes classifier is based on the Bayes theorem, which is used to provide a way of calculating posterior probability N(b|x) from N(b), N(x), and N(x|b). Now, consider the equation of Bayes theorem:

$$N(b/x) = \frac{N(x/b)N(b)}{N(x)} \tag{9}$$

where

N(b|x): is the posterior probability of class(b, target) given predictor(x, attributes). This represents the probability of b being true, provided x is true.
N(b): is the prior probability of class. This is the observed probability of class out of all the observations.
N(b|c): is the likelihood which is the probability of predictor-given class. This represents the probability of x being true, provided x is true.
N(x): is the prior probability of predictor. This is the observed probability of predictor out of all the observations.

Principle

The steps of Naïve Bayes algorithm are as follows:
Step 1:
First, we have read the training dataset DS.
Step 2:
Then we have to find out mean as well as standard deviation of the predictor variables in each class.

Step 3:
Repeat; calculate the probability of predictor variable F using the gauss density equation in each class; until the probability of all predictor variables has been determined.
Step 4:
Calculate the probability of each class.
Step 5:
Lastly, get the best probability.

For an implementation of Naïve Bayes, an WSN-DS is used as a dataset and Python is used as a programming language. The working steps of Naïve Bayes classifier are applied to obtain the results. The results obtained after implementation are shown in Tables 5 and 6.

Table 5 Attacks predicted using Naïve Bayes

	Actual_Attack_Type	Pred_Attack_Type
99820	Normal	Grayhole
99824	Normal	Grayhole
99837	Grayhole	Blackhole
99842	Normal	Grayhole
99851	Normal	Grayhole
99854	Blackhole	Grayhole
99860	Grayhole	Blackhole
99861	Normal	Grayhole
99868	Normal	Grayhole
99871	Normal	Grayhole
99872	Normal	Grayhole
99873	Normal	Grayhole
99880	Normal	Grayhole
99886	Flooding	Grayhole
99950	Normal	Grayhole

Table 6 Classification report for Naïve Bayes

	Precision	Recall	F1-Score
Blackhole	0.49	0.97	0.65
Flooding	0.29	0.49	0.37
Grayhole	0.16	0.57	0.25
Normal	1.00	0.87	0.93
TDMA	0.78	0.23	0.36
Avg/Total	0.94	0.85	0.88

Table 5 shows the attacks predicted using Naïve Bayes classifier. In Table 5, for ID number 99860 and 99950, actual attack type were grayhole and normal but these attacks are predicted as blackhole and grayhole, respectively.

Table 6 shows the classification report for Naïve Bayes, in which black hole, flooding, grayhole, TDMA attacks were detected. The accuracy of Naïve Bayes is 94.00% and it is the average accuracy of all attacks.

Evaluation of Naïve Bayes classifier

The advantages of Naïve Bayes classifier are as follows:

- It is computationally fast.
- It is very simple to implement.
- It works very well with high dimensions.
- It can be used for multiclass and binary classification problems.

The disadvantages of Naïve Bayes classifier are as follows:

- The main disadvantages of Naïve Bayes classifier is that it is not able to learn interactions between features.
- If the dataset is large then we can't use it because it gives poor performance.

For the implementation of Naïve Bayes, we have to calculate several conditional probabilities.

4.3 Random Forest

This section deals with the background, mathematics, principle, and advantages of Random Forest classifier.

Background

Basically, RF has mostly used algorithm because of its simplicity, and again, it is used for both classification and regression. RF produces, even without hyperparameter tuning, a great result most of the time [32]. Random Forest is a type of supervised learning algorithm. First, RF is used to create a forest to evaluate results. Then Random Forest builds multiple decision trees by picking "K" number of data points point from the dataset and then merges them together to get a more accurate and stable prediction [33]. For each "K" data points decision tree, we have many predictions and then we take the average of all the predictions. RF is an Ensemble learning Algorithm. Ensemble learning is the process by which multiple models combine together to predict one result.

Mathematical Foundations

As we know that the RF classifier belongs to a category of additive model that can be used to makes some predictions by combining decisions from a sequence of base model. Normally, we can mention this model in terms of equation like

$$f(x) = r_0(x) + r_1(x) + r_2(x) + \cdots \tag{10}$$

where

f is the final model which is nothing but the sum of simple base model ri
r is the base model.

Principle
The steps for Random Forest algorithm are as follows:
Step 1:
First, we have to select randomly "i" features from the entire "j" features with one condition i ≪ j.
Step 2:
Using the concept of best split point, we need to calculate node "n" from the "i" features.
Step 3:
Then again using the concept of best split, we need to split node "n" into daughter node.
Step 4:
Then repeat Step 1–Step 3 until "1" number of node has been reached.
Step 5:
We need to build forest by repeating Step 1–Step 4 for "k" number of times to create "k" number of trees.
Step 6:
To predict target, we need to take test features and we have to use the rules of each randomly created decision tree and store the predicted target.
Step 7:
Then simply find out votes for each predicted target.
Step 8:
Lastly, just consider the high voted prediction target as a final prediction.

For an implementation of RF, an WSN-DS is used as a dataset and Python is used as a programming language. The working steps of RF classifier are applied to obtain the results. The results obtained after implementation are shown in shown in Tables 7 and 8.

Table 7 shows the attacks predicted using Random Forest classifier. In Table 7, for ID number 144 and 173, actual attack type were grayhole and normal but these attacks are predicted as normal and flooding respectively.

Table 8 shows the classification report for Random Forest, in which black hole, flooding, grayhole, and TDMA attacks were detected. The accuracy of Random Forest is 94.00% and it is the average accuracy of all attacks.

Evaluation of Random Forest classifier
The advantages of the Random Forest algorithm are as follows:

- It can be used for both classification and regression.
- With Random Forest, it is very easy to view the relative importance it assigns to the input features.
- It is easy and handy algorithm.
- It is able to reduce overfitting.

Table 7 Attacks predicted using random forest

	Actual_Attack_Type	Pred_Attack_Type
0	Normal	Normal
1	Normal	Normal
2	Normal	Normal
3	Normal	Normal
4	Normal	Normal
5	Normal	Normal
6	Normal	Normal
7	Normal	Normal
8	Normal	Normal
35	Normal	Grayhole
144	Grayhole	Normal
161	Normal	Grayhole
164	TDMA	Blackhole
173	Normal	Flooding
188	TDMA	Blackhole

Table 8 Classification report for random forest

	Precision	Recall	F1-Score
Blackhole	0.49	0.97	0.65
Flooding	0.29	0.49	0.37
Grayhole	0.16	0.57	0.25
Normal	1.00	0.87	0.93
TDMA	0.78	0.23	0.36
Avg/Total	0.94	0.85	0.88

The disadvantages of the Random Forest algorithm are as follows:

- The main disadvantage of RF algorithm is that with large number of trees, algorithm will works slow and inefficient in real-time predictions.
- It is very hard to implement.
- When there is a nonlinear relationship between dependent and independent variables, then it may not work well.

4.4 Decision Tree

This section deals with the background, mathematics, principle, and advantages of Decision Tree classifier.

Background

Basically, Decision Trees belongs to a type of supervised machine learning, in which by considering particular parameter data is continuously splitted. The trees are often drawn by considering two things like decision nodes and leaves [34]. The decision nodes are considered where information is split and the leaves are considered as a final outcome or decision [35]. The decision tree algorithms are very popular algorithm and they are successfully applied to many more learning tasks.

Mathematical Foundations

In DT classifier, based on entropy, partition creation and stopping condition are predefined. Entropy can be defined as the representation of how much information is encoded by given data [36]. At each node of a decision tree, entropy is given by the following formula:

$$E = -\sum_{i=1}^{c}(p_i * \log(p_i)) \tag{11}$$

where

pi represents proportion of observations with class labels i, {i = 1 to c}

The information gain of the split can be measured by using the following formula:

$$IG = E(Parent) - weighted\ sum\ of\ E(childnodes) \tag{12}$$

Principle

The working steps of Decision Tree algorithm are given below.

Step 1:

First, we have to place the best attribute from the dataset at the root of the tree

Step 2:

Second, we have to divide train dataset into subsets. While dividing train data into subset, we should consider each subset should contain data with the same value for an attribute.

Step 3:

Lastly, just repeat Sep 1 and Step 2 on each subset until we find leaf nodes in all the branches of the tree.

For an implementation of Decision Tree, an WSN-DS is used as a dataset and Python is used as a programming language. The working steps of DT classifier are applied to obtain the results. The results obtained after implementation shown in Tables 9 and 10.

Table 9 shows the attacks predicted using DT classifier. In Table 9, for ID number 861 and 1147, actual attack type was normal and flooding but these attacks are predicted as flooding and normal respectively.

Table 10 shows the classification report for Decision Tree, in which black hole, flooding, grayhole, TDMA attacks were detected. The accuracy of Decision Tree classifier is 94.00% and it is the average accuracy of all attacks.

Table 9 Attacks predicted using decision tree

	Actual_Attack_Type	Pred_Attack_Type
175	Normal	Grayhole
214	Normal	TDMA
645	Normal	TDMA
861	Normal	Flooding
888	Normal	Flooding
1147	Flooding	Normal
1240	TDMA	Normal
1336	Normal	TDMA
1464	TDMA	Normal
1914	Flooding	Normal
2231	Normal	TDMA
2332	Blackhole	Grayhole
2370	Normal	TDMA
2513	Flooding	Normal
2687	Grayhole	Normal

Table 10 Classification report for decision tree

	Precision	Recall	F1-Score
Blackhole	0.00	0.00	0.00
Flooding	0.00	0.00	0.00
Grayhole	0.39	1.00	0.57
Normal	1.00	0.97	0.99
TDMA	1.00	0.86	0.93
Avg/Total	0.94	0.94	0.93

Evaluation of Decision Tree classifier

The advantages of Decision Tree classifier are as follows:

- It is very simple to understand, interpret and visualize.
- It can handle numerical as well as categorical data.
- It requires small efforts from users form the purpose of data preparation.

The advantages of Decision Tree classifier are as follows:

- It can be unstable because small variations in the data might result in a completely different tree being generated.
- Decision Tree users can create biased trees if some classes dominate.
- For responses with low sample size, decision tree gives poor prediction accuracy.

4.5 K-Nearest Neighbor

This section deals with the background, mathematics, principle, and advantages of K-Nearest Neighbor classifier.

Background

K-nearest neighbors is a simple algorithm that stores all available cases and classifies new cases based on a similarity measure [37]. In K-means algorithm, for each test data point, we would be looking at the K-nearest training data points and take the most frequently occurring classes and assign that class to the test data. Therefore, K represents the number of training data points lying in proximity to the test data point which we are going to use to find the class [38].

Mathematical Foundations

The Euclidean distance between two points is given as X1 = (x11, x12, …, x1n) and X2 = (x21, x22, …, x2n), which can be calculated by using the following equation:

$$dist(x_1, x_2) = \sum_{i=1}^{n} (x_{1i} - x_{2i})^2 \tag{13}$$

Principle

The steps of K-Nearest Neighbors algorithm are given below.

Step 1:

First, we have to find out value K and K is equal to the number of nearest neighbors.

Step 2:

Then, we have to calculate space between query instance and all the training samples.

Step 3:

Then, we have to sort the space and confirm nearest neighbors supported the Kth minimum distance.

Step 4:

Then we have to assemble the class Y of the closest neighbors.

Step 5:

Lastly, on the basis of majority of class of nearest neighbors consider the prediction value of the query instance.

For an implementation of KNN, an WSN-DS is used as a dataset and Python is used as a programming language. The working steps of KNN classifier are applied to obtain the results. The results obtained after implementation are shown in Tables 11 and 12.

Table 11 shows the attacks predicted using K-Nearest Neighbors classifier. In Table 11, for id number 99985 and 99987, actual attack type was normal and black-hole but these attacks are predicted as normal and blackhole respectively.

Table 12 shows the classification report for K-Nearest Neighbors, in which black hole, flooding, grayhole, TDMA attacks were detected. The accuracy of KNN classifier is 96.00% and it is the average accuracy of all attacks.

Table 11 Attacks predicted using K-Nearest Neighbor

	Actual_Attack_Type	Pred_Attack_Type
99971	Normal	Normal
99972	Normal	Normal
99973	Normal	Normal
99974	Normal	Normal
99975	Normal	Normal
99976	Normal	Normal
99977	Normal	Normal
99978	Normal	Normal
99979	Normal	Normal
99980	Normal	Normal
99981	Normal	Normal
99982	Normal	Normal
99985	Normal	Normal
99986	Normal	Normal
99987	Blackhole	Blackhole

Table 12 Classification report for K-Nearest Neighbor

	Precision	Recall	F1-Score
Blackhole	0.79	0.76	0.78
Flooding	0.73	0.58	0.65
Grayhole	0.76	0.67	0.71
Normal	0.98	0.99	0.99
TDMA	0.92	0.73	0.81
Avg/Total	0.96	0.97	0.96

Evaluation of K-Nearest Neighbor classifier

The advantages of KNN classifier are as follows:

- It is very simple to understand, easy to implement, it is very quick.
- It can be used for regression as well as classification problems.
- It is very effective if dataset is large.
- It is robust to noisy training data.

The disadvantages of KNN classifier are as follows:

- It is not capable to deal with missing value problems.
- It gives poor performance with imbalanced dataset.

We need to compute value of parameter k.

5 Deep Learning Approach

This section deals with the Deep Learning approach. To perform Deep Learning, we have used Convolutional Neural Network classifier.

Background

CNN is a specific type of artificial neural network which uses perceptron, a machine learning algorithm to analyses data [39]. We can apply CNN to image processing, natural language processing and any other types of tasks.

Principle

The working steps of CNN classifier are given below.

Basically, there are four steps in CNN. These steps are as follows:

Step:1

Convolution—This is the first layer of CNN, which receives an input signal and is called as convolution filters. Convolution is one type of process in which the network tries to label an input signal by referring to what it has learned in the past. If the input signal looks like previous flooding type attack it has seen before, the flooding attack reference signal will be mixed into or we can say convoluted with the input signal and then the output signal is then passed on to the next layer.

Step:2

Subsampling—This is the second layer of CNN, this layer receives the input from convolution layer and that input can be smoothened to reduce the sensitivity of the filters to noise and variations. The process of smoothing is called as subsampling.

Step:3

Activation—This is the third layer of CNN, which is used to control the signal flow from one layer to the next layer, emulating how neurons are fired in our brain. Again in this, output signals which are strongly associated with past references would activate more neurons, enabling signals to be propagated more efficiently for identification.

Step:4

Connectedness—This is the last layer of CNN which is fully connected. In this neuron, preceding layers are connected to every neuron in subsequent layers.

For an implementation of CNN, an WSN-DS is used as a dataset and Python is used as a programming language. The working steps of CNN classifier are applied to obtain the results. The results obtained after implementation are shown in Tables 13 and 14.

Table 13 shows the attacks predicted using CNN classifier. In Table 13, for ID number 74919 and 74920, actual attack type was normal and blackhole but these attacks are predicted as flooding and blackhole, respectively.

Table 14 shows the classification report for CNN, in which black hole, flooding, grayhole, TDMA attacks were detected. The accuracy of CNN is 98.00% and it is the average accuracy of all attacks.

Table 13 Attacks predicted using CNN

	Actual_Attack_Type	Pred_Attack_Type
74906	Flooding	Flooding
74907	Blackhole	Flooding
74908	Flooding	Flooding
74909	Flooding	Flooding
74910	Flooding	Flooding
74911	Flooding	Flooding
74912	Flooding	Flooding
74913	Flooding	Flooding
74914	Flooding	Flooding
74915	Flooding	Flooding
74916	Flooding	Flooding
74917	Flooding	Flooding
74918	Flooding	Flooding
74919	Normal	Blackhole
74920	Blackhole	Blackhole

Table 14 Classification report for CNN

	Precision	Recall	F1-Score
Blackhole	0.94	0.44	0.60
Flooding	0.87	0.92	0.89
Grayhole	0.64	0.90	0.75
Normal	0.99	0.99	0.99
TDMA	0.91	0.88	0.89
Avg/Total	0.98	0.97	0.97

Evaluation of CNN classifier

The advantages of CNN classifier are as follows:

- Weight sharing is possible.
- Requires less time for classification.
- CNN is able to learn relevant features.

The disadvantages of CNN classifier are as follows:

- High computational cost.
- Requires large amount of training data.
- Overfitting is the problem of CNN.

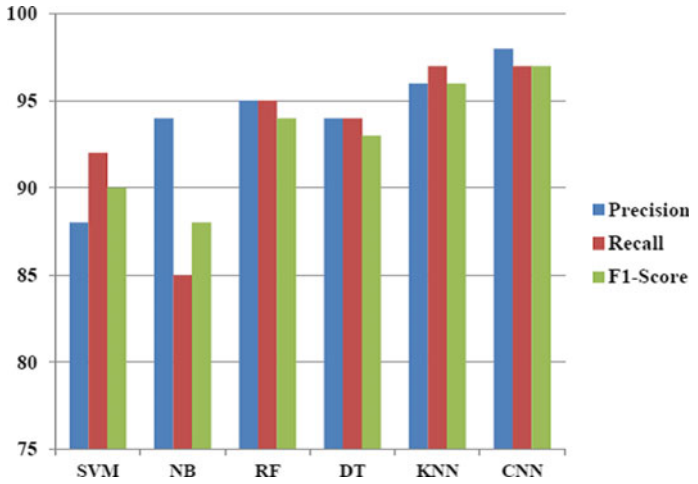


Fig. 2 Comparison of machine learning and deep learning classifiers (Precision, recall, and F1 score)

For the purpose of comparison, five algorithms of machine learning are considered, namely SVM, NB, RF, DT, and KNN. Again, for the purpose of comparison, we have considered Deep learning algorithm, namely CNN. For comparison purpose, precision, recall, and F1 score are considered, and their comparison results are shown in the following Fig. 2. From Fig. 2, we can say that the accuracy of SVM is lowest and accuracy of CNN is highest.

Table 15 shows the comparison of machine learning classifiers, i.e., SVM, RF, DT, NB, KNN, and CNN. On the basis of experimentation, we can say that the accuracy of SVM and CNN classifier are low and high, respectively. As we have mentioned, the accuracy of SVM is low. The mathematical reason behind the low accuracy is that SVM works better for small dataset and in our experimentation, we have used large dataset. Again, another reason behind low accuracy is that in this, we need to compute length of a vector and the distance of a vector. Again, we have mentioned that the accuracy of CNN classifier is high, and the mathematical reason behind that we have applied deep learning and it works better for large dataset and we have used large dataset for our experimentation.

6 Conclusion

From the discussions in the above sections, we understand the need to design a system that can prevent intrusions in an WSN. Due to anything, anytime, anywhere, and type of computing use of WSN has increased significantly. Looking at the various threats and several attacks in a wireless network, security is the prime concern. Intrusion is

Table 15 Comparison of machine learning classifiers

Classifier	Based on	Calculations	Advantages	Limitations	Accuracy
Support Vector Machine	Based on Object-Based Image Analysis	Computes length of a vector, distance of a vector	Fast classification of new objects	Slow training	Low
Random Forest	Based on group of decision trees	Computes number of decision trees, number of features to consider when computing the best node split	Easy to interpret	Low predictive accuracy	Medium
Decision Tree	Based on models for classification by using a series of decision rules	Evaluates binary trees by using ideal features and thresholds to create better trees	Better performance in nonlinear setting	Unstable	High
Naïve Bayes	Based on Bayesian statistics	It evaluates classifications using probability distributions	Decent classifier for several tasks	Assumes conditional independence of the data	Medium
K-Nearest Neighbor	Based on the class of the nearest neighbor on the feature space	Computes number of neighbors to use, weights of a neighbors	Very easy to add new training examples	Computationally expensive to determine nearest neighbors because it visits each training samples	Medium

one of the critical issues, and intrusion detection has already reached its saturation. Therefore, we need an efficient solution for effective intrusion prevention toward WSNs.

This paper presents a comparative study and performance analysis on intrusion detection and prevention system for WSN using machine learning as well as deep learning techniques. In this paper, the results of various machine learning as well as the deep learning techniques for attacks detection are presented. The results of deep learning techniques are better than the machine learning techniques. So, deep learning techniques are better to prevent intrusion. Through the literature survey, we understand that there is a need to develop a scalable and attack resistance system for intrusion prevention using deep packet inspection in an WSN. A system is proposed to detect and prevent intrusion from using deep learning for the WSN.

Hence, the proposed system can be used to detect and prevent attacks in all types of networks where security matters.

References

1. Abdullah, M. A., Alsolami, B. M., Alyahya, H. M., & Alotibi, M. H. (2018). Intrusion detection of DoS attacks in WSNs using classification techniques. *Journal of fundamental and Applied Sciences, 10*(4S), 298–303.
2. Babar, S., Mahalle, P., Stango, A., Prasad, N., & Prasad, R. (2010). Proposed security model and threat taxonomy for the Internet of Things (IoT). In *International Conference on Network Security and Applications*. Berlin, Heidelberg: Springer.
3. Binh, H. T. T., &Dey, N. (Eds.). (2018). *Soft computing in wireless sensor networks*. CRC Press.
4. Chowdhuri, S., Chaudhuri, S. S., Banerjee, P., Dey, N., Mandal, A., & Santhil, V. (2016). Secure minimum loss route selection of MIMO-based MANET in combined (indoor, outdoor, and forest) terrain (pp. 1–26). Working paper, International Journal Advanced Intelligence Paradigms.
5. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018, February). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence, 2*(1).
6. Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. (2013). Identity authentication and capability based access control (IACAC) for the internet of things. *Journal of Cyber Security and Mobility*, 309–348.
7. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks (Vol. 5). ISSN: 2169–3536. IEEE. Translations.
8. Dey, N., Wagh, S., Mahalle, P. N., & Pathan, M. S. (2019). *Applied machine learning for smart data analysis*. CRC Press.
9. Shelke, M. P., Malhotra, A., & Mahalle, P. (2017). A packet priority intimation-based data transmission for congestion free traffic management in WSNs. *Computers & Electrical Engineering*, 248–261 (Pergamon).
10. Niyaz, Q., Sun, W., Javaid, A. Y., & Alam, M. (2015, December 03–05). A deep learning approach for network intrusion detection system. In *BICT 2015*, New York City, United States.
11. Almomani, I., Al-Kasasbeh, B., & AL-Akhras, M. (2016). WSN-DS: A dataset for intrusion detection systems in WSNs. *Journal of Sensors, 2016* (Article ID 4731953) (Hindawi Publishing Corporation).
12. Myint, H. O., & Meesad, P. (2009). Incremental Learning Algorithm based on Support Vector Machine with Mahalanobis distance (ISVMM) for Intrusion Prevention. 978-1-4244-3388-9/09/$25.00 ©2009 IEEE.
13. Farnaaz, N., & Jabbar, M. A. (2016). Random forest modeling for network intrusion detection system. *Procedia Computer Science, 89*, 213–217 (Elsevier).
14. Al-Qatf, M., Lasheng, Y., Alhabib, M., & Al-Sabahi, K. (2018). Deep learning approach combining sparse autoencoder with SVM for network intrusion detection. IEEE Access. https://doi.org/10.1109/ACCESS.2018.2869577.
15. Peddabachigari, S., Abraham, A., & Thomas, J. (2016). Intrusion detection systems using decision trees and support vector machines. *International Journal* of *Advanced Networking and Applications, 07*(04), 2828–2834. ISSN: 0975-0290.
16. Chowdhuri, S., Das, S. K., Roy, P., Chakraborty, S., Maji, M., &Dey, N. (2014, November). Implementation of a new packet broadcasting algorithm for MIMO equipped Mobile ad-hoc network. In *International Conference on Circuits, Communication, Control and Computing* (pp. 372–376). IEEE.
17. Panda, M., & Patra, M. R. (2007, December). Network intrusion detection using Naïve Bayes. *IJCSNS International Journal of Computer Science and Network Security, 7*(12).

18. Muna, A L-Hawawreh, Moustafa, Nour, & Sitnikova, Elena. (2018). Identification of malicious activities in industrial internet of things based on deep learning models. *Journal of Information Security and Applications, 41,* 1–11.
19. Shi, Hongtao, Li, Hongping, Zhang, Dan, Cheng, Chaqiu, & Cao, Xuanxuan. (2018). An efficient feature generation approach based on deep learning and feature selection techniques for traffic classification. *Computer Networks, 132,* 81–98.
20. Kausar, N., &Taiar, R. (2016). A Disaster Management Specific Mobility Model for Flying Ad-hoc Network.
21. Li, W., Yi, P., Wu, Y., Pan, L., & Li, J. (2014). A new intrusion detection system based on KNN classification algorithm in WSN. *Journal of Electrical and Computer Engineering, 2014* (Hindawi Publishing Corporation).
22. Fong, S., Li, J., Song, W., Tian, Y., Wong, R. K., & Dey, N. (2018). Predicting unusual energy consumption events from smart home sensor network by data stream mining with misclassified recall. *Journal of Ambient Intelligence and Humanized Computing*, 1–25.
23. Mukherjee, A., Keshary, V., Pandya, K., Dey, N., & Satapathy, S. C. (2018). Flying ad hoc networks: A comprehensive survey. In *Information and Decision Sciences* (pp. 569–580). Singapore: Springer.
24. Van, N. T., Thinh, T. N., & Sach, L. T. (2017). An anomaly-based network intrusion detection system using deep learning. In *2017 International Conference on System Science and Engineering (ICSSE)*.
25. Agrawal, S. K., Singh, B. P., Kumar, R., & Dey, N. (2019). Machine learning for medical diagnosis: A neural network classifier optimized via the directed bee colony optimization algorithm (pp. 197–215). Academic Press.
26. Juma, S., Muda, Z., Mohamed, M. A., Yassin, W. (2015, February 28). Machine learning techniques for intrusion detection system: A review. *Journal of Theoretical and Applied Information Technology, 72*(3).
27. Chowdhuri, S., Chakraborty, S., Dey, N., Chaudhuri, S. S., & Banerjee, P. (2017). Propagation analysis of MIMO ad hoc network in hybrid propagation model and implement less propagation loss algorithm to find the minimum loss route. *International Journal of Information and Communication Technology, 10*(1), 66–80.
28. Zemmal, N., Azizi, N., Dey, N., & Sellami, M. (2016). Adaptative S3VM semi supervised learning with features cooperation for breast cancer classification. *Journal of Medical Imaging and Health Informatics,* 957–967 (American Scientific Publishers).
29. Xin, Y., Kong, L., Liu, Z. (Member, IEEE), Chen, Y., Li, Y., Zhu, H., et al. (2018). Machine learning and deep learning methods for cybersecurity. *IEEE Access, 6*.
30. Shah, S. A. R., & Issac, B. (2018). Performance comparison of intrusion detection systems and application of machine learning to Snort system. *Future Generation Computer Systems, 80*, 157–170.
31. Chowdhuri, S., Roy, P., Goswami, S., Azar, A. T., & Dey, N. (2014). Rough set based ad hoc network: A review. *International Journal of Service Science, Management, Engineering, and Technology (IJSSMET), 5*(4), 66–76.
32. El Mourabit, Y., Toumanari, A., Bouirden, A., & El Moussaid, N. (2015, June 5). A comparative evaluation of intrusion detection techniques in WSN. *Journal of Theoretical and Applied Information Technology, 76*(1).
33. Chatterjee, S., Ghosh, S., Dawn, S., Hore, S., & Dey, N. (2016). Forest type classification: A hybrid NN-GA model based approach. In Information systems design and intelligent applications (pp. 227–236). India: Springer.
34. Kamble, P. N., & Mahalle, P. N. (2013). Decision theory based auto-delegation (DTA-d) scheme for ubiquitous computing. *International Journal of Computer Applications* (Foundation of Computer Science).
35. Alsheikh, M. A., Lin, S., Niyato, D., & Tan, H.-P. (2015, March 19) Machine Learning in WSNs: Algorithms, Strategies, and Applications. arXiv:1405.4463v2 [cs.NI].
36. Chowdhuri, S., Dey, N., Chakraborty, S., & Baneerjee, P. K. (2015). Analysis of performance of MIMO ad hoc network in terms of information efficiency. In *Emerging ICT for Bridging*

the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI (Vol. 2, pp. 43–50). Cham: Springer.
37. Chowdhuri, S., Chakraborty, S., Dey, N., Azar, A. T., Salem, M. A. M. M., Chaudhury, S. S., et al. (2014). Recent research on multi input multi output (MIMO) based mobile ad hoc network: A review. *International Journal of Service Science, Management, Engineering, and Technology (IJSSMET), 5*(3), 54–65.
38. Li, Z., Dey, N., Ashour, A. S., Cao, L., Wang, Y., & Wang, D. (2017). Convolutional neural network based clustering and manifold learning method for diabetic plantar pressure imaging dataset. *Journal of Medical Imaging and Health Informatics* (American Scientific Publishers).
39. Bhattacherjee, A., Roy, S., Paul, S., Roy, P., Kausar, N., & Dey, N. (2016). Classification approach for breast cancer detection using back propagation neural network: A study (pp. 210–221). IGI Global.

Design of Automation and Troubleshooting Technique

Study and Design of Route Repairing Mechanism in MANET

Harendra Kumar, Madhuri Malakar, Sourabh Debnath and Mudassir Rafi

Abstract Mobile Ad hoc Network (MANET) is a frameless, wireless network with no central access point. The network consists of migrant nodes. Topology is highly dynamic, unpredictable, and its probability of link failure is high due to continuous mobility of the nodes. As a result, we find that the nodes are no longer reachable and it moves away from the mobile or active path. This maximizes the dropping estimate, end-to-end delay and also undergoes cut in packet delivery rate thereby leading to degradation of network efficiency. In order to conquer such consequences, our work proposes designing of a route repairing mechanism in MANET. The basic idea of our proposed routing protocol is to find an optimal path based on the minimum hop count in the multipath scenario. Based on the widespread simulation of the proposed mechanism, done by adopting NS2 and by relative study of the same with existing protocol AODV, it was found that the projected routing mechanism helps in enhancing the performance and brings about improvement in ratio of packet delivery, packet loss as well as end-to-end delay.

Keywords Mobile ad hoc network · Ad hoc on-demand distance vector · Route discovery · Route repairing · Optimal path

H. Kumar (✉)
Department of Computer Science & Engineering, Government Polytechnic Bilaspur, GEC Campus, Koni, Bilaspur 495009, India
e-mail: khandeharendra24@gmail.com

M. Malakar · S. Debnath · M. Rafi
School of Computer Science and Engineering, National Institute of Science and Technology (Autonomous), Institute Park, Pallur Hills, Berhampur 761008, Odisha, India
e-mail: malakar_m@nist.edu

S. Debnath
e-mail: dsourabh@nist.edu

M. Rafi
e-mail: mudassir.rafi23@gmail.com

S. K. Das et al. (eds.), *Design Frameworks for Wireless Networks*,
Lecture Notes in Networks and Systems 82,
https://doi.org/10.1007/978-981-13-9574-1_6

1 Introduction

Ad hoc network, a wireless network, lacks well-defined framework. In ad hoc network, each migrant node actions as router. This router discovers, controls routes for other nodes available in network. Within the network topology, these nodes may make a swift in such a way that it may lead to uncertain and frequent changes. There are a number of routing protocols defined for Mobile Ad hoc Networks (MANETs) [1–6]. The two defined categories of protocols, based on the route discovery principle, are proactive protocol and reactive protocol [1]. These two protocols serve different functionalities. In order to update route for every pair of nodes periodically, irrespective of requirements, proactive protocol is used whereas the reactive or on-demand routing protocol uses a broadcasting query-reply, i.e., Route Request–Route Reply (RREQ-RREP) procedure to determine the route, only when there is a need of data packet transmission. There are a number of applications of MANET in the field of civilian environment, law enforcement, military and disaster recovery [7]. To expedite these applications of abundant traffic among nodes, a stable and productive routing protocol is crucial. Figure 1 illustrates the organized communication in MANET. The challenge lies in the persistent change within the network topology, constrained battery capability of the nodes, and uncertain behavior of wireless channels in MANET. Within this network, critical task lies in selection of a long-lasting route [8–11]. Our protocol provides maximum priority route for MANET that may be viewed as a two-stage process, first for route discovery and the second for route recovery.

Characteristic of roving ad hoc network is modification in its topology where serious issue lies in mobile devices in terms of the power limitations [12]. As the network is mobile in nature, devices use battery as their power supply [13]. Therefore, the leading conservation of power technique becomes crucial for designing a system.

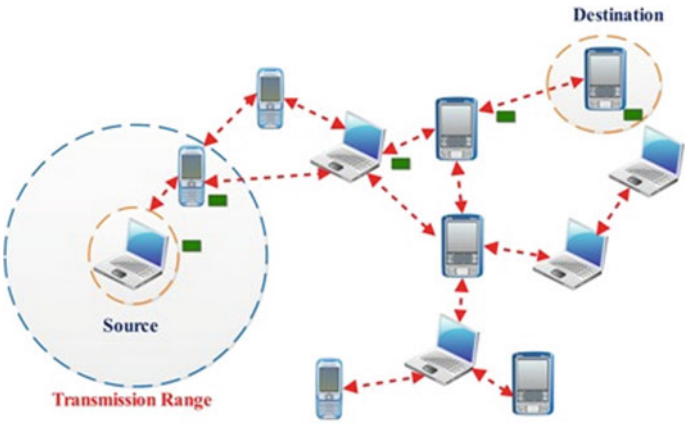


Fig. 1 Mobile ad hoc network

However, the security issue remains in terms of physical aspect. The possibility of attack on mobile network is easy compared to the fixed network.

Overcoming of the new security issues and troubles in wireless network is in high appeal [13]. Other than applications found in the field of military battlefield, commercial sector such as ad hoc mobile communication in between the ships, law imposition, taxi cabs, stadiums, boats, aircrafts, etc. There are a number of other applications found in personal area network such as laptop, cellular phone, Wireless LAN (WLAN), GPRS, and UMTS. Figure 2 illustrates classification of protocols used for routing.

Following are the list of challenges showing the inefficiencies and limitations in a MANET environment [14]:

- Limited wireless transmission range,
- Routing overhead,
- Battery constraints,
- Mobility-induced route changes,
- Potentially frequent network partitions,
- Immense power consumption,
- Depressed bandwidth, and
- Steep error rates.

The other part of our work is formulated as follows: Sect. 2 describes several works. Details of the suggested protocols have been described in third section. Fourth section illuminates results of simulation, comparison with extant protocol. Finally, Sect. 5 provides a conclusion to the paper.

2 Related Work

Route repairing is being extensively studied for the past two decades. Other than the works mentioned in [15], there are several other results which exist in the literature for routing via multiple paths in ad hoc networks. Some of the important works are as follows. The Destination-Sequenced Distance Vector (DSDV) routing protocol, proposed by Park et al. [16], illustrates the perception of classical Bellman–Ford routing algorithm with advancement in making it loop-free. Due to count to infinity and bouncing effect, the distance vector routing is subordinately strong compared to link state routing. Within the network, each of the device maintains a routing table. This routing table consists of entries for all the devices. Each of the devices keeps on broadcasting routing messages at regular interval times to keep the table updated. When the neighboring device packets transmitted routing information and identify ongoing cost of link to device, it tries to correlate the value and its equivalent value stored in its routing table. The value is updated if changes found and recomputation of route distance is done. Ng et al. [17] proposed a protocol named as cluster head gateway switch routing protocol. This is different because rather than using a flat topology, it uses hierarchical network topology. As proposed by Chiang,

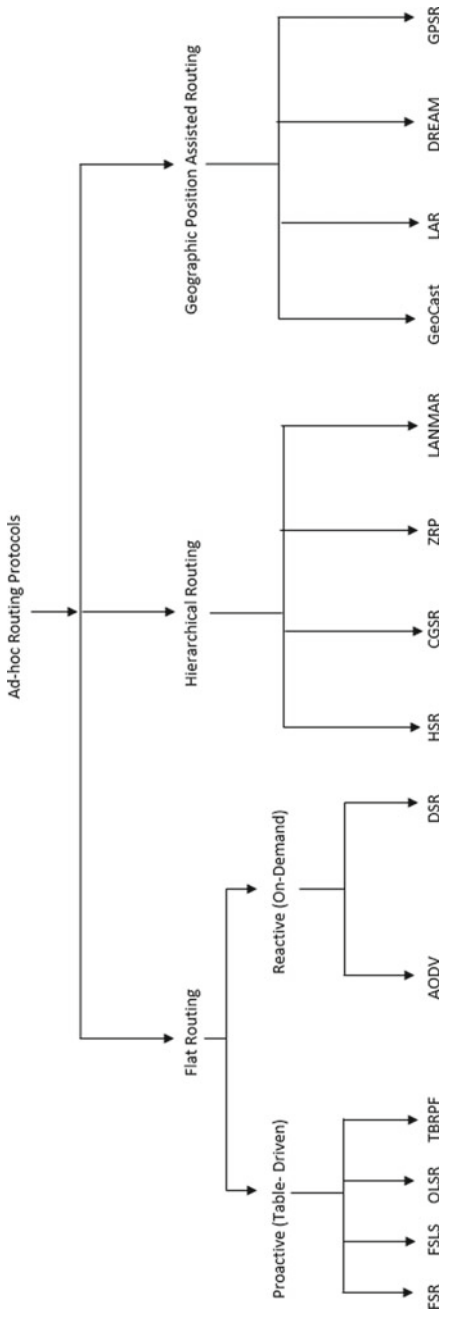


Fig. 2 Distribution of routing protocols in mobile ad hoc network

cluster head gateway switch routing protocol brings about an arrangement of cluster nodes by bringing about a coordination among each cluster member by allocating it to a special node termed as cluster head. In order to elect a node dynamically as a cluster head, an algorithm termed as Least Cluster Change (LCC) is applied. For each mobile node within a network, cluster member table is available to each of the nodes to store target cluster head. Each node broadcasts the cluster member table at regular intervals with the help of DSDV algorithm. CGSR, an expansion to DSDV, is used as underlying scheme for routing. The overhead is similar to DSDV. By using the method of cluster routing, DSDV is adjusted to route traffic from source to target. CGSR brings about an improvement into the routing conduct by routing packets through the cluster heads and gateways. Ad Hoc Backup Node Sets up Routing Protocol (ABRP), proposed by Chung et al. [18], is quite similar when compared to DSR. ABRP stores route substitute data in on-the-route node. Whenever there is failure of link, information is passed to the node acting as backup. In order to replace the ongoing current broken path, the backup node selects a path (if there exists one) by checking in its backup route cache. However, ABRP does not refurbish backup information of route to flash change in the topology. A dynamic route repairing protocol, enlightened by Yu et al. [13], reconstructs a collapsed path by adopting the content given by the nodes on hearing main route communication. Whenever these links steep, the brilliant protocol takes down declined links or nodes with substitute ones, adjoining the main route. A new local repair scheme proposed by Youn et al. [12] uses promiscuous mode. This scheme comprises two important modes: quick local repair scheme and adaptive promiscuous mode. Quick local repair scheme, with the help of related available information, helps in achieving faster local reroute discovery process for alive connection in the local area collected by promiscuous node. Adaptive promiscuous mode helps replay switching process between promiscuous and non-promiscuous mode. This helps conquer energy limits occurring because of promiscuous mode. Bird Flocking Behavior Routing (BFBR) protocol for an extreme mobile ad hoc network is proposed by Srinivasan et al. [19]. The protocol is divided into two parts: an encounter search and direction forward routing. An encounter search is useful in route discovery. Direction forward routing is useful in maintenance of route. Unlike the regular broadcast mechanisms, BFBR protocol preserves the bandwidth bypassing avoidable link traversals. During route discovery, link traversals are diminished by use of encounter search mechanism. Direction forward routing also aids in managing regional surrounding of each node to assure path accordance, thereby bringing about a reduction in overhead in routing. The mechanism is found complex in terms of maintenance of the route. Multi-Route Ad Hoc On-Demand Distance Vector Ant routing algorithm (MRAA) was proposed by Abdel-Moniem et al. [20]. The technique uses AODV to discover routes reactively. AODV discovers route on demand, whereas ACO generates path in between the nodes proactively, regardless of request. However, during data packet delivery, the technique reduces the end-to-end delay. As the technique uses alternate path for delivery of data packets, the forwarding is performed in limited time with minimum overhead. However, storage and maintenance of backup routes add to an overhead. Peer-to-Peer Bee Algorithm (P2PBA), proposed by Dhurandher et al. [21],

is designed to provide an effective peer-to-peer (P2P) file exploration in MANETs. The technique utilizes the concept of swarm-based intelligence, explaining foraging behavior of the honeybees. The files are fragmented into small packets. The packets are dispersed over judicious collection of spots. Certain criteria like safeguard of energy, retrieval troubles, and heterogeneous collection of nodes are not taken care of in this technique. Bird Flight-Inspired Routing Protocol (BFIRP) based on energy and position was proposed by Misra et al. [22]. The technique uses the methodology of forwarding the data packets to the destination, keeping into consideration the node's energy and distance from target. Protocol involves the degree of node's closeness to the great circular area, connecting the common as well as the target nodes. However, the protocol suffers from bandwidth problems. A local repair method, removing the pitfalls in ongoing local repair, was proposed by Jain et al. [23]. The improved local repair scheme focuses on end-to-end delay in transference and need of overhead. An ant algorithm is used by the repairing node to look for a new route for next to next node in the link during local repair. The size of F-ANT and B-ANT is reduced as well as it provides significant minimization in overhead. The idea of extant local repair trial method in AODV was proposed by Naidu and Chawla [24]. This was elaborated for broadcasting and minimization of flooding. For easy broadcasting, protocol establishes mobile nodes so that in case of link failure detection, local repair technique is applicable. The technique uses diameter perimeter model to maximize count of intermediate nodes. Our present work presents solution to bring about a reduction in route overheads of AODVLRT as well as investigates the intensified AODVLRT with extant local repair technique. This technique consists of two parts: perimeter routing, which is used for broadcasting; local repair method, which is used to decrease the flooding. However, this maximizes the count of intermediary nodes from origin to target. An on-demand delay and bandwidth-based quality of service (QoS) routing protocol (AODV-D), proposed by Subburam et al. [25], was elaborated for two main reasons: first and the foremost thing to be taken care of was to ensure that delay does not exceed the threshold value and second, to check the least possible bandwidth available for sending the packets. The projected routing protocol follows unicast-type two-hop local route repair protocol reclaiming the lost links accurately while maximizing network accuracy, expanding usage, depreciation in the count of control messages, and decreasing the repair delay. An algorithm to control traffic with the help of local route repair method was proposed by Rao et al. [26]. Whenever there is link failure at intermediary node, the number of hop of target is correlated with origin's hop count and if target is nearer to breakage link than origin, regional improvement is done. When regional repairing is in action, packet is saved in buffered echelon and as soon as an alternate route is found, the packet is passed on to the destination. QoS-aware Routing based on Ant Colony Optimization (QoRA) was proposed by Al-Ani et al. [27]. This technique uses QoRA to calculate QoS parameter locally and helps in avoiding blockage during information transfer with the aid of two architectural components. Each node has a running QORA entity. The QORA entity detects path according to stated QoS needs. The SNMP entity, the other component, consists of Simple Network Management Protocol (SNMP) agent and the Management Information Base (MIB). SNMP finds

applicable data for local node. Based on information or values, the QoS parameters are formulated thereby avoiding traffic during data packet transmission. However, this suffers from certain drawbacks such as high end-to-end delay and the technique pauses. AODV-Reliability (AODV-R), bundled by ant colony optimization, is enlightened by Singh et al. [28]. This is based on routing protocol for discovery of the abbreviated path by eliminating traffic. ACO algorithm is used by AODV-R to bring about an improvement in identification of precise path algorithm. Selection of most reliable path is done using AODV-R. It helps in reducing the possibility of link breakages at the time of change in network topology. However, it suffers from certain drawback by not fulfilling the requirements of QoS routing. An advanced method for path selection combined with AODV protocol uses Ant Colony Optimization (ACO) and the concept was enlightened by Sarkar et al. [29], to bring about an improvement in Quality of Service (QoS) in MANETs. The combination of ant colony with AODV helps in selecting best route for data transmission by utilization of path's pheromone value. Pheromone value of route is formulated based on end-to-end reliability, traffic, hop counts, and residual energy. The route with highest pheromone value is selected for data packet transmission. Das et al. [30] proposed a routing protocol for multicast ad-hoc network in order to create an energy effective path from origin to every multicast set built on two vague parameters such as distance and energy, whereas other parameters were not been considered by this proposed work which leads to its limitation. Hence, Yadav et al. [31] stretched the effort placed on multi-constraints method. They have considered three parameters that are delay, bandwidth, and energy. It supports to elect the best route with the help of fuzzy cost. Here too limitations occurred as it is a point-based membership function and fails to hold the fuzziness information. Henceforth, Das and Tripathi [32] proposed an energy-conscious-based routing protocol by considering five parameters such as distance, energy, delay, packets, and hop count. The objective of this routing is to search for an optimal route by considering multi-criteria decision-making and intuitionistic fuzzy soft set. It does not use any optimization method which leads to its limitation. So, by using above techniques several contradictory objectives may not be optimized. Das and Tripathi [33] brought up a routing technique based on nonlinear optimization technique. This nonlinear optimization technique is based on geometric programming which works with polynomial environment instead of polynomial environment. It helps to determine nonlinear parameters efficiently and enhance the network lifetime. A DUCR algorithm for wireless sensor networks was discussed by Mazumdar et al. [34]. This mechanism resolves the hot spot problem. To balance the receiving nodes, DUCR algorithm uses a well-organized approach to distribute the information to its parent nodes. It is scattered in nature and facilitates preferred performance of energy consumption, alive nodes, and lifetime of network. This algorithm is also stationary in nature, and it does not have the property of mobility which may increase the network performance. Mazumdar et al. [35] proposed a distributed fuzzy logic based energy-aware and coverage safeguarding uneven clustering algorithm (DECUC) for wireless sensor networks. While addressing the problems in wireless sensor networks, it intends to create a transition between coverage parameters and energy competence. It uses a fuzzy logic concept by taking parameters

such as distance from base station, enduring energy, and CS of a node for electing cluster heads and cluster radii. This algorithm is distributed in nature and facilitates better conduct in coverage preservation, network's lifetime, and energy efficiency. This algorithm is also stationary in nature; it does not have the property of mobility which may increase the network performance. Mazumdar et al. [36] discussed an energy-efficient fuzzy-based uneven clustering and routing algorithm (DFCR) for wireless sensor networks. This mechanism reduces the cluster size that is nearer to base stations which resolves the hot spot problem. This DFCR algorithm provides an efficient approach for cluster head selection and selection of next hop node for routing of information. It is scattered in nature and facilitates superior act in terms of energy consumption and lifetime of the network. Though it is stationary in nature, it does not have the property of mobility which is required for better performance. The directional sensor models, used in the coverage of ROI, was proposed by Chaya et al. [37]. The probability estimation method is used to calculate the threshold value. This was elaborated to directional sensor ratio with respect to omnidirectional sensors. The LP formulation for boosting the coverage area was provided. Fixed count in the number of sensors, different orientation ways were implied and future objective was to achieve the coordinated value of sensors in ROI. The key research work of CLDs was proposed by Sah et al. [38]. It played an important aspect in the past in context to WSNs [39]. Irrespective of layer's collaboration, focus was on minimizing the transference and collecting power, end-to-end delivery improvement, reduction of control packet overhead, and QoS. Apart from this, very small progress was observed in the area of security. Incentive-based replication strategy was proposed by Singh et al. [40] to provide incentive to the participating nodes, so that it does not act selfish. Community-based mechanism was provided for fair incentive to the nodes to carry packets from origin to target. The proposed strategies evaluated in terms of epidemic, prophet, spray and wait, and maxprop routing algorithms. This strategy works better than the existing strategies. Singh et al. [41] say IRS provided better result of delivery ratio when compared to epidemic and prophet routing algorithms. In IRS, incentive policy for selfish nodes was popularized in socially aware DTNs to sacrifice their selfishness and as per incentive value reputation relay nodes can cooperate in replication process and earn incentive value for transferring packets.

3 Proposed Work

Our work delivers a brand-new ad hoc routing protocol with rectifiable path which handles broken-link recovery in a competent way. The present work is an intuitive idea employed behind the proposed protocol. The proposed routing protocol begins by selecting all possible routes from origin S to target node D. This target node also known as terminal node of the network because this is final destination of the data transmission. Among all possible routes, we select maximum priority route on the basis of hop count for packet transmission. As the data packet is sent along the maximum priority route, if there occurs any link failure then node Ni sends route

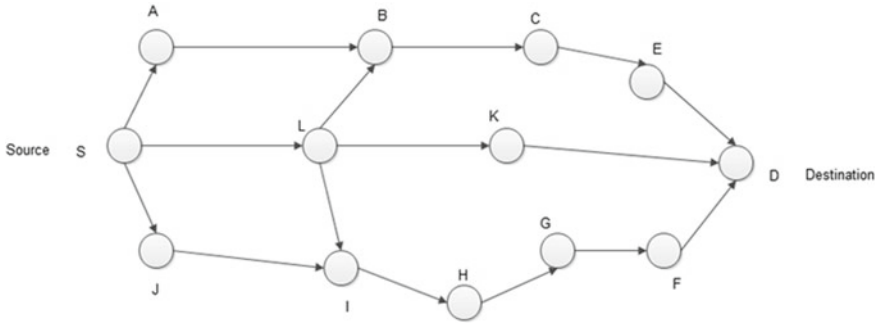


Fig. 3 An illustration showing the idea of proposed protocol

repair (RRP) message to the previous node N_{i-1} and then after node N_{i-1} broadcasts route request (RREQ) message to own neighbor node. After that if there is route from neighbor node to target then node N_{i-1} sends route repair ok (RROK) message to source. Now packet transmission again starts with repair route from source to target. Otherwise, if there is no route from neighbor node to target, in this case, the RREQ packet will be dropped and source node selects the already found route with next maximal priority for data packet transmission. No continual message flow and huge table preservation required. Figure 3 shows an illustration of the idea of our proposed protocol. The proposed work consists of two parts as (i) route discovery and (ii) route recovery.

3.1 Route Discovery

In this section, originating node introduces path detection by broadcasting a route request (RREQ), these route requests contain source node address, request id, source sequence number, destination sequence number, destination address, and hop count.

If destination node D is neighboring source node S, then the packet is sent directly to node D. Else, neighbor's node of S processing and forwarding RREQ packet throughout the network, so we will wait until all the paths between S to D are stored.

Now we calculate priority of each route, after that destination node D sends route replay (RREP) message to the source with maximum priority route, and thus route is established between source and destination. The flowchart for this mechanism is represented diagrammatically in Fig. 4 and algorithm is shown in Algorithm 1.

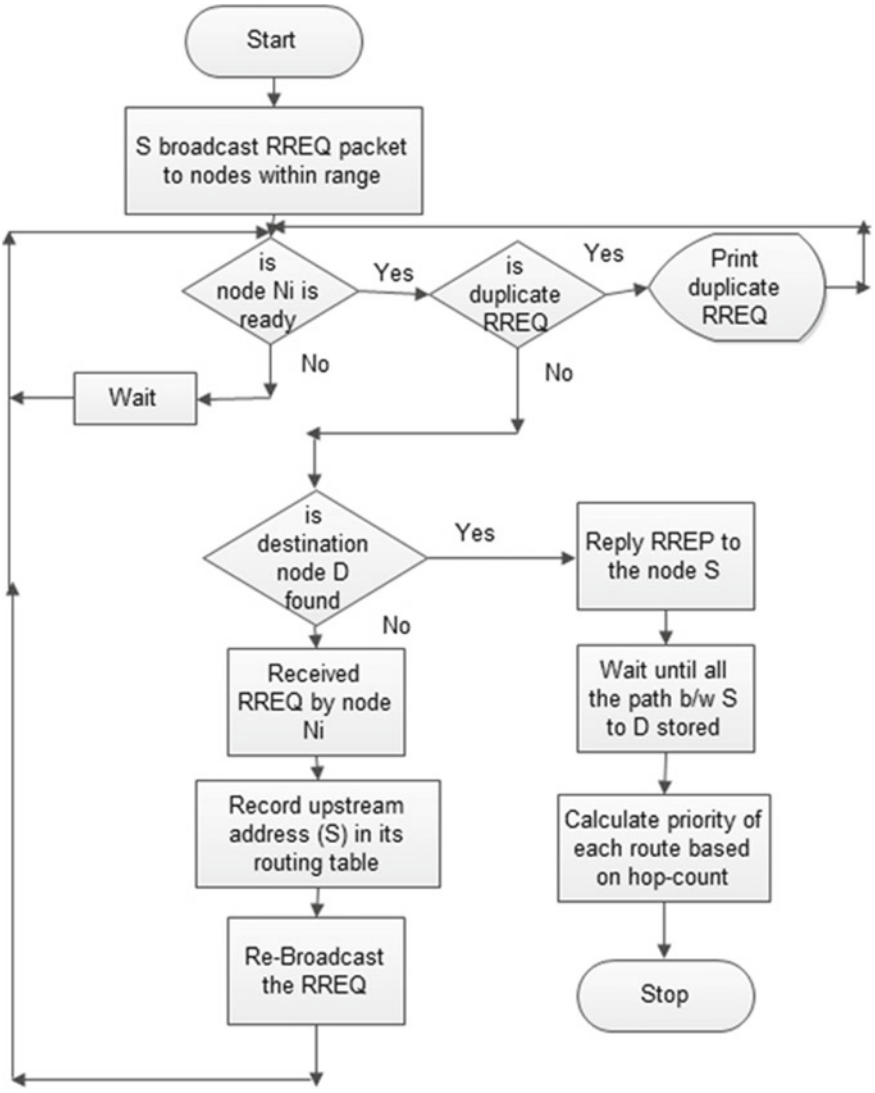


Fig. 4 Flowchart for route discovery

3.2 Route Recovery

In this section, during packet transmission, whenever node Ni finds a broken link in the main route, then node Ni sends route repair (RRP) message to the previous node N_{i-1}.

Then after node N_{i-1} broadcasts route request (RREQ) message to own neighbor node. After that if there is route from neighbor node to destination then node N_{i-1}

sends route repair ok (RROK) message to source, thus new repair route is established from source to destination. Now data packet transmission again starts with repair route from origin to target.

If no route from neighbor node to target, RREQ packet will be dropped and source node finds the route with next maximal priority for data packet transference. The flowchart for this mechanism is represented diagrammatically in Fig. 5 and algorithm is shown in Algorithm 2.

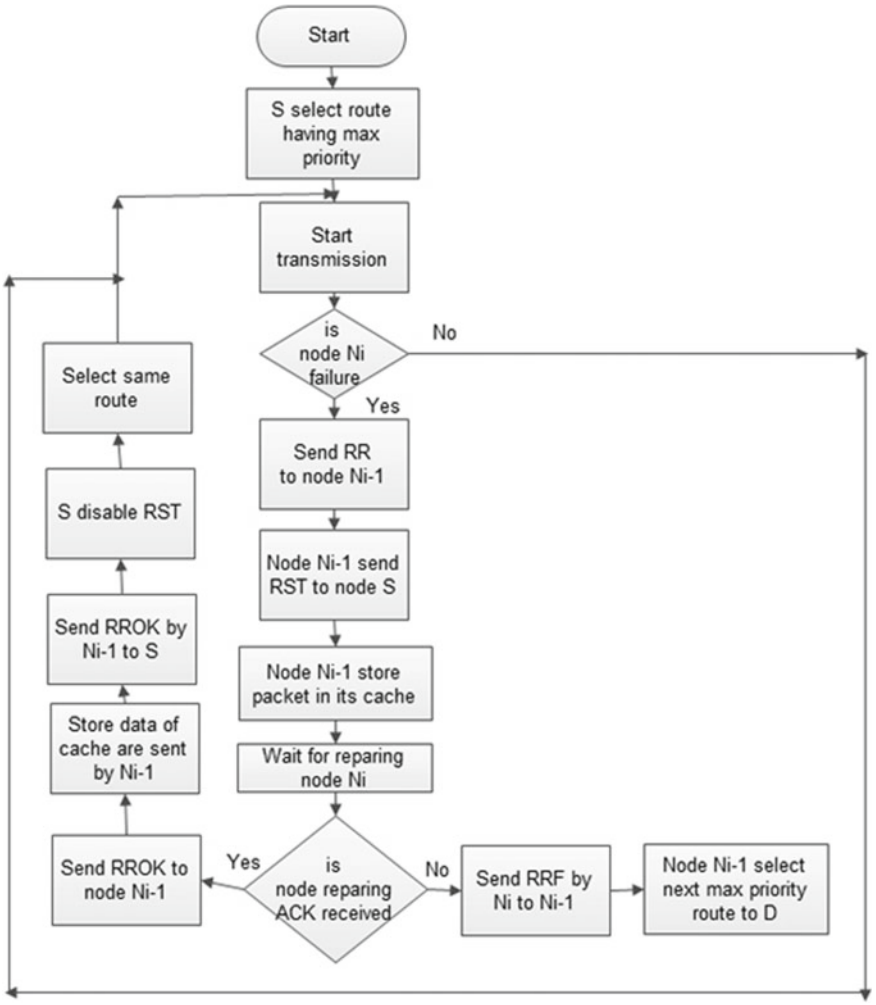


Fig. 5 Flowchart for route recovery

Algorithm 1: Route Discovery.

Input: Source node (S), Destination node (D)
Output: An optimal path

Initialization: i=0, f=0
while (true)
{
if (i==0)
{
S broadcast RREQ packets to its neighbors;
Neighbor node (n_i) accept non-duplicate RREQ packets;
}
if (n_i==D)
{
f=1
}
else
{
Update R_tableof n_i ; /* R_table is routing table */
Neighbor node n_i re-broadcast the RREQ packet to its neighbor;
i++;
}
if(f==1)
{
Destination node D send RREP packet based on shortest hop-count path;
break;
}
}

Algorithm 2: Route Repairing.

Input: Erroneous Link
Output: Recovery path

```
if (RERR==true)
{
while(true )
{
Node n_i generate and broadcast RREQ packet
to its neighbor  /* n_i is the preceding node of the failure link */
i++;
Neighbor node accept non-duplicate RREQ;
Update Routing table;
if (n_i==D)
{
f=1;
}
if(f==1)
{
Destination node D send RREP packet based on shortest hop-count path;
break;
}
}
}
```

Following is the step-wise representation of how a route is constructed and reconstructed whenever link failure occurs. Once a route is discovered, then information is propagated to destination from source.

Step-1:
An example showing route discovery's triggers route discovery by broadcasting an RREQ has been shown in Fig. 6.

Step-2:
Route discovery, intermediary nodes processing and transferring are shown in Fig. 7.

Step-3:
Shows discovery of route at destination D, and receiving three copies of RREQ in Fig. 8.

1. Through E.
2. Through K.
3. Through F.

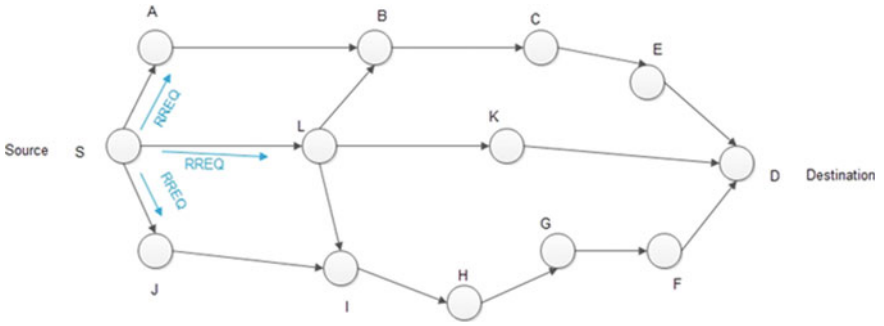


Fig. 6 Route discovery initiates by broadcasting RREQ

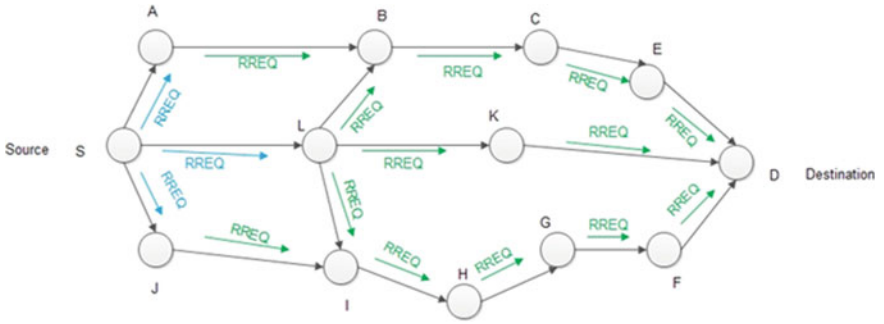


Fig. 7 An example showing route discovery, intermediate nodes are processing and forwarding

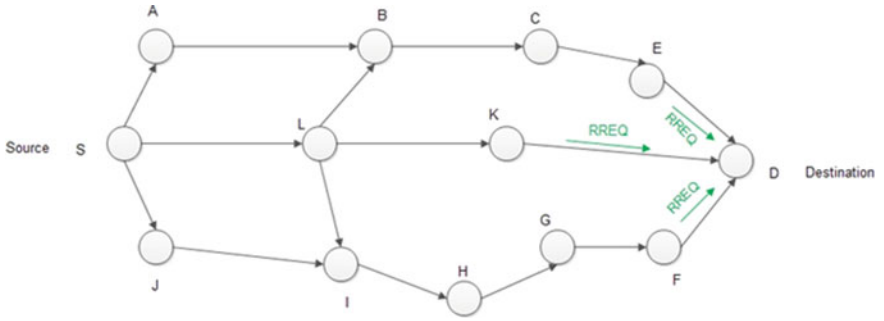


Fig. 8 During route discovery destination node D receiving RREQ

Step-4:
There are five feasible paths from source to destination and is shown diagrammatically in Fig. 9.

1. S->A->B->C->E->D with hop count value (HC1) = 5.
2. S->L->B->C->E->D with hop count value (HC2) = 5.
3. S->L->K->D with hop count value (HC3) = 3.
4. S->L->I->H->G->F->D with hop count value (HC4) = 6.
5. S->J->I->H->G->F->D with hop count value (HC5) = 6.

Step-5:
Destination (D) generates an RREP and forwards it through K which has highest priority route compared to other routes. Minimum hop count shows maximum priority route. Here HC3 < HC1 < HC2 < HC4 < HC5.

So select route with value (HC3) = 3, it is less than compared to other routes. Figure 10 shows route discover, destination D computing highest priority route and generating RREP.

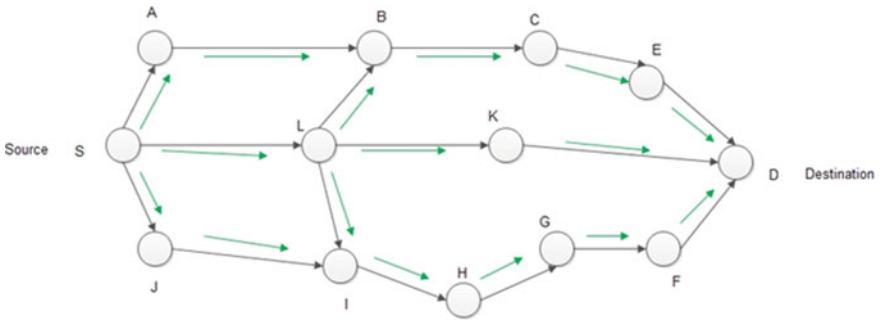


Fig. 9 An example showing route discovery, there are five feasible paths from source to destination

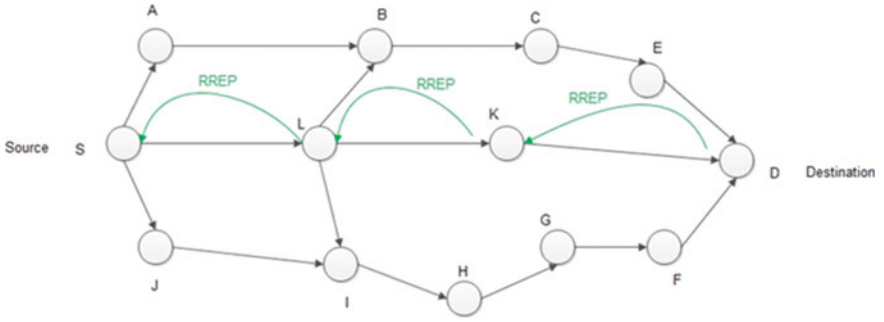


Fig. 10 During route discovery destination node D computing highest priority route and generating RREP

Step-6:
Figure 11 shows route discovery and establishment of maximum priority route between S and D.
Step-7:
How a packet transmission is done from source to destination is shown in Fig. 12.
Step-8:
In case if link fails or breaks during transmission, i.e., route error is shown in Fig. 13.
Step-9:
When a link breaks to continue the transmission process new route or route recovery is done and how it is done is shown in Fig. 14.
Step-10:
For route recovery, the node n_{i-1} broadcasts RREQ to its neighbor shown in Fig. 15.
Step-11:
Node n_{i-1} broadcasts RREQ, if there is a route from node n_{i-1} to destination then node n_{i-1} selects it, with maximum priority. If there are multiple maximum priority routes from node n_{i-1} to destination then node n_{i-1} selects any one route for sending packet. If there are no routes from node n_{i-1} to destination, then again it starts sending packet from source node with maximum priority route as shown in Fig. 16.

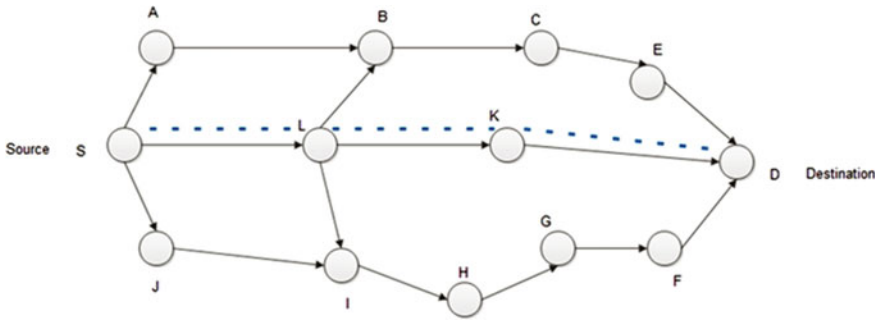


Fig. 11 Route discovery, a maximum priority route from S to D is established

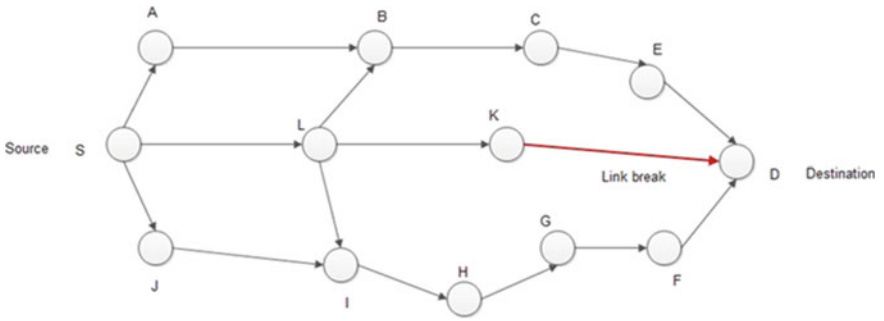


Fig. 12 An example shows transmission of packet from source to destination

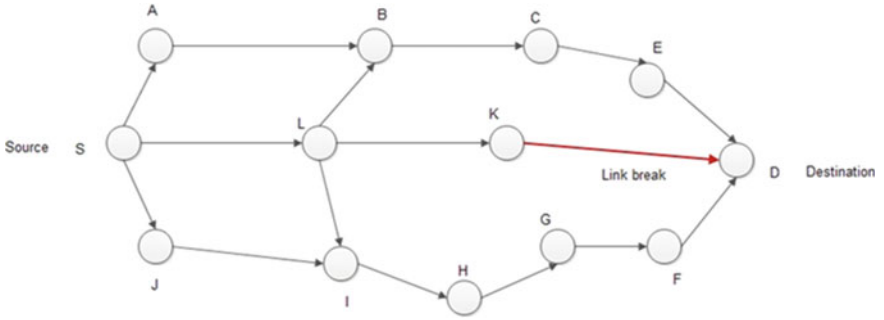


Fig. 13 An example showing route error, if any link is broken

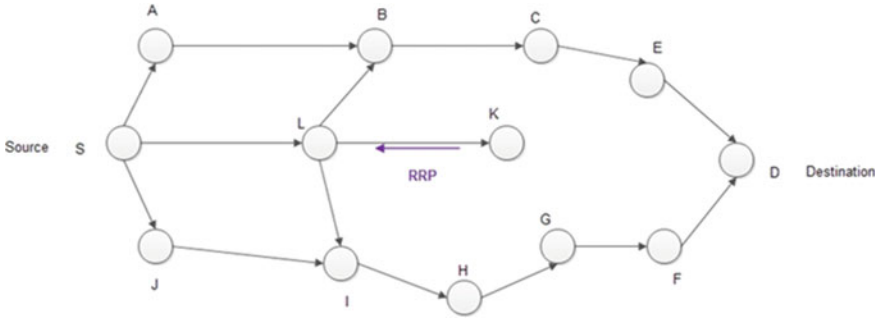


Fig. 14 An example showing route recovery, node n_i sends RRP (Route Repair) message to previous node n_{i-1}

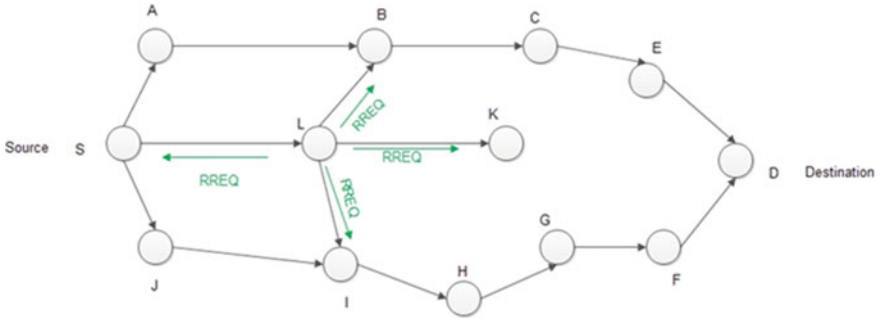


Fig. 15 An example showing route recovery, node n_{i-1} broadcasts RREQ to own neighbor

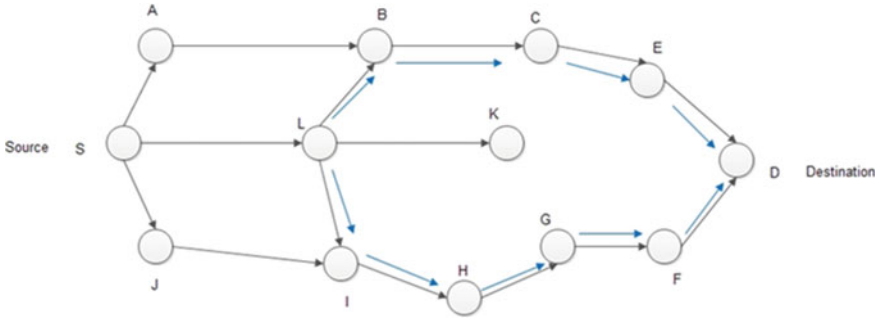


Fig. 16 An example showing route recovery, node N_{i-1} selects maximum priority route

In above example, it shows that there are two routes from node ni-1 to destination, first one is L->B->C->E->D with hop count value(HC6) = 4 and second one is L->I->H->G->F->D with hop count value(HC7) = 5.

Then node N_{i-1} selects maximum priority route for packet transmission to destination. The route is L->B->C->E->D which is more stable compared to L->I->H->G->F->D. Here HC6 < HC7.

Step-12:

In above Fig. 17, node N_{i-1} selects maximum priority route S->L->B->C->E->D with hop count value of 5 as compared to other route which is S->L->I->H->G->F->D with count value of 6 which is high compared to previous route, so node N_{i-1} selects maximum priority route, because lesser hop count shows maximum priority route.

Step-13:

In Fig. 18, repair node N_{i-1} starts sending packet with maximum priority route. Node N_{i-1} sends RROK message to source, then source disables the RST(Route Stop) message and starts to send the packets.

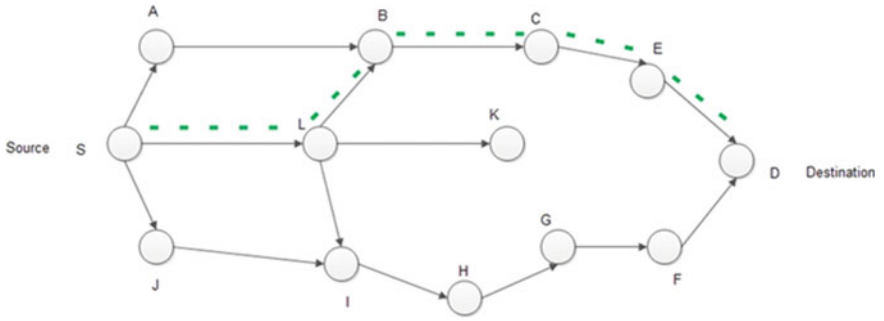


Fig. 17 An example showing packet transmission from repair route to destination

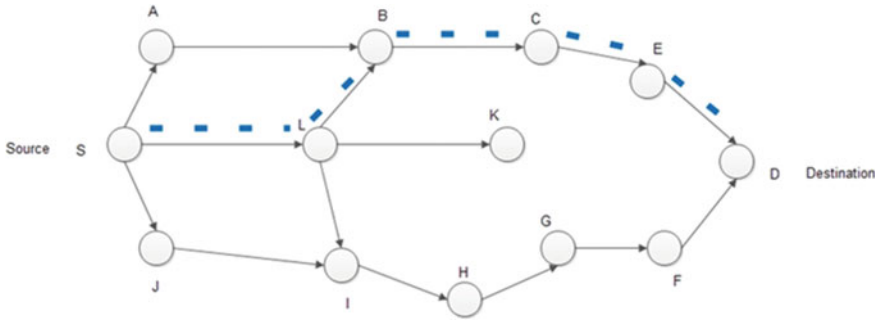


Fig. 18 An example showing packet transmission from repair route to destination

In worst case if node N_{i-1} is unable to repair the route, it delivers back RRF (route repair fail) message to the source. In such scenario, source node will select already found route with highest priority for sending packets to destination.

4 Simulation Results and Analysis

In Table 1, all the parameters that are required for our simulation are mentioned and we have used NS2 as our simulator for simulating our proposed work. The nodes were randomly deployed in a geographical position in the topology 700 × 700 and hence network is established among all the nodes. Number of nodes simulated in each iteration are 10, 20, 30, 40, 50, 60, 70, where transmission range is 550 m and traffic size is CBR. Total packet size is 100 bytes and packet rate is 10 packets per

Table 1 Simulation parameter

Parameter	Values
Topology	700 × 700
Simulation time	150 s
Pause time	10 ms
Number of nodes	10, 20, 30, 40, 50, 60, 70
Transmission range	550 m
Traffic size	CBR
Packet size	100 bytes
Packet rate	10 packet/s
Maximum speed	20 m/s
Routing protocol	AODV
X dimension of topography	500
Y dimension of topography	400

second in speed of 20 m/s. In the proposed technique, the base routing protocol is AODV. Figure 19 shows in which fashion nodes are deployed. In this figure, nodes indicated by MNi where i is the different integer indicating node ID. Node ID of source node is 0 and node ID of destination node is 11 and other nodes are working as hop nodes. Once route generated the packets then it forwarded to in this route, Fig. 20 shows how packets are being sent between nodes whereas Fig. 21 shows the mobility nature of nodes.

Figure 22 shows how packet drops whenever there is a breakage in route link between nodes.

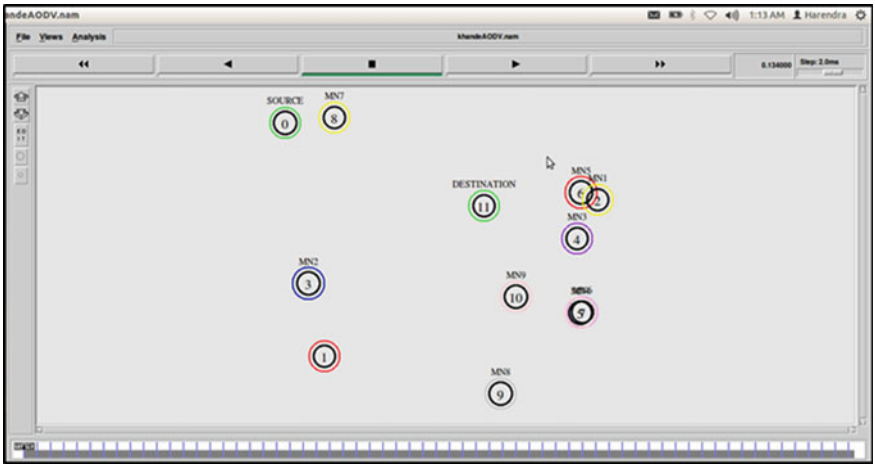


Fig. 19 Network topology

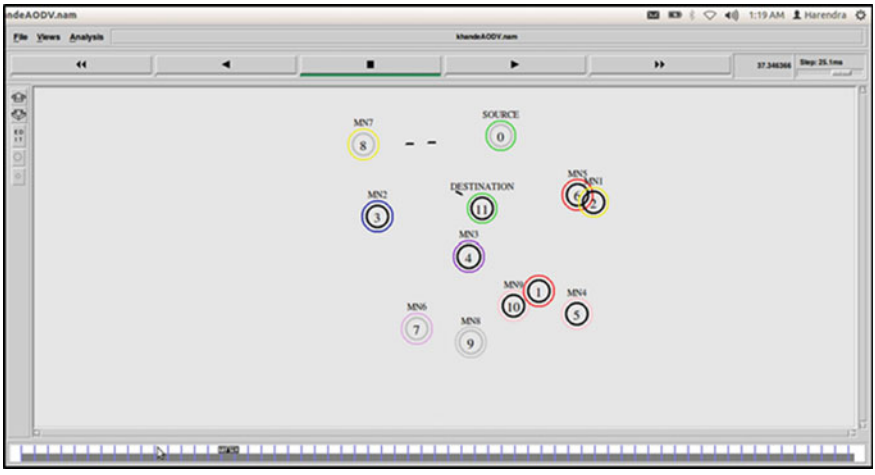


Fig. 20 Packet sent between routes

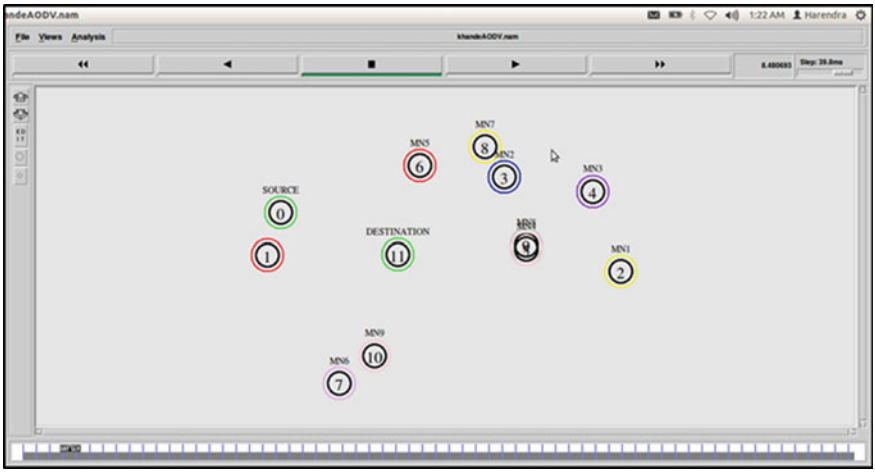


Fig. 21 Mobility of node

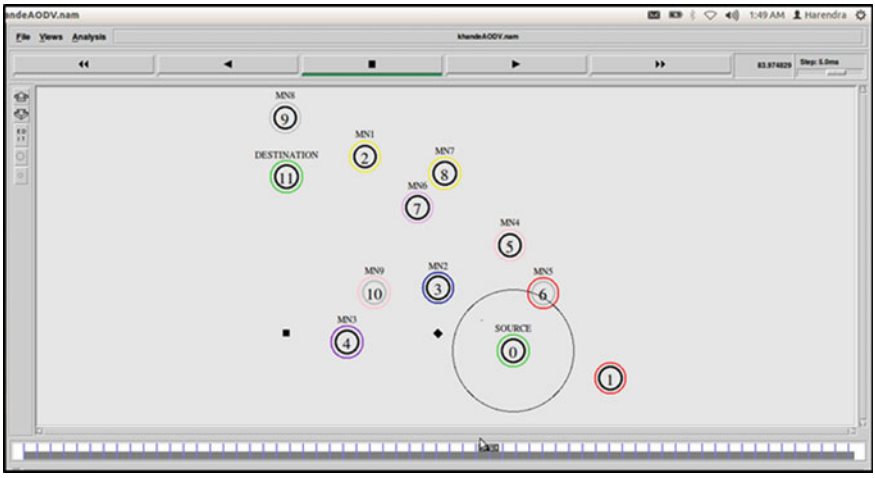


Fig. 22 Link breakage and packet dropping

Hence, they will find an alternate path to transmit their packets from origin to target as shown in Fig. 23, and trace file system is shown in Fig. 24. This figure contains different columns such as event, time, from node, to node, packet type, packet size, flags, fid, source address, destination address, sequence number, and packet id.

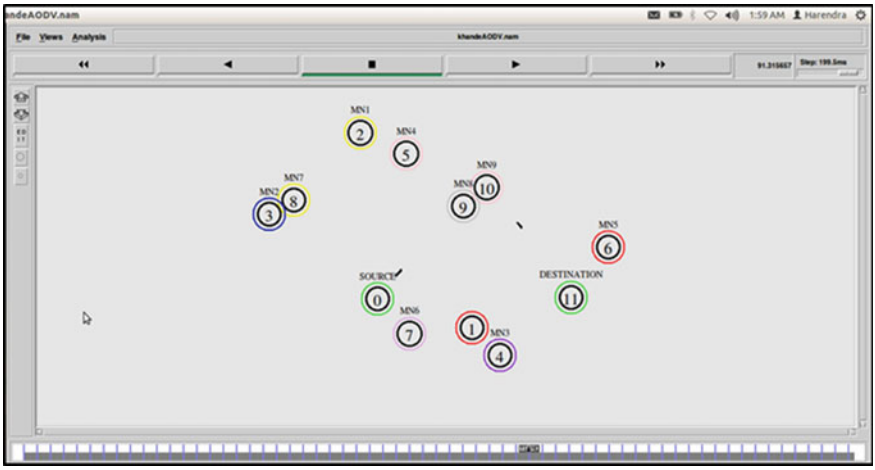


Fig. 23 Alternate path for sending packet

```
s 10.000000000 _0_ RTR  --- 0 AODV 48 [0 0 0 0] ------- [0:255 -1:255 30 0] [0x2 1 1 [11 0] [0 4]] (REQUEST)
r 10.000988114 _3_ RTR  --- 0 AODV 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [11 0] [0 4]] (REQUEST)
r 10.000988146 _9_ RTR  --- 0 AODV 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [11 0] [0 4]] (REQUEST)
r 10.000988726 _8_ RTR  --- 0 AODV 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [11 0] [0 4]] (REQUEST)
s 10.001869340 _3_ RTR  --- 0 AODV 48 [0 ffffffff 0 800] ------- [3:255 -1:255 29 0] [0x2 2 1 [11 0] [0 4]] (REQUEST)
r 10.002977445 _9_ RTR  --- 0 AODV 48 [0 ffffffff 3 800] ------- [3:255 -1:255 29 0] [0x2 2 1 [11 0] [0 4]] (REQUEST)
r 10.002977454 _0_ RTR  --- 0 AODV 48 [0 ffffffff 3 800] ------- [3:255 -1:255 29 0] [0x2 2 1 [11 0] [0 4]] (REQUEST)
r 10.002978108 _8_ RTR  --- 0 AODV 48 [0 ffffffff 3 800] ------- [3:255 -1:255 29 0] [0x2 2 1 [11 0] [0 4]] (REQUEST)
r 10.002978143 _4_ RTR  --- 0 AODV 48 [0 ffffffff 3 800] ------- [3:255 -1:255 29 0] [0x2 2 1 [11 0] [0 4]] (REQUEST)
s 10.005324160 _4_ RTR  --- 0 AODV 48 [0 ffffffff 3 800] ------- [4:255 -1:255 28 0] [0x2 3 1 [11 0] [0 4]] (REQUEST)
s 10.005399880 _9_ RTR  --- 0 AODV 48 [0 ffffffff 0 800] ------- [9:255 -1:255 29 0] [0x2 2 1 [11 0] [0 4]] (REQUEST)
r 10.006607985 _3_ RTR  --- 0 AODV 48 [0 ffffffff 9 800] ------- [9:255 -1:255 29 0] [0x2 2 1 [11 0] [0 4]] (REQUEST)
r 10.006608027 _0_ RTR  --- 0 AODV 48 [0 ffffffff 9 800] ------- [9:255 -1:255 29 0] [0x2 2 1 [11 0] [0 4]] (REQUEST)
r 10.007911077 _2_ RTR  --- 0 AODV 48 [0 ffffffff 4 800] ------- [4:255 -1:255 28 0] [0x2 3 1 [11 0] [0 4]] (REQUEST)
r 10.007911155 _5_ RTR  --- 0 AODV 48 [0 ffffffff 4 800] ------- [4:255 -1:255 28 0] [0x2 3 1 [11 0] [0 4]] (REQUEST)
r 10.007911159 _6_ RTR  --- 0 AODV 48 [0 ffffffff 4 800] ------- [4:255 -1:255 28 0] [0x2 3 1 [11 0] [0 4]] (REQUEST)
r 10.007911302 _10_ RTR  --- 0 AODV 48 [0 ffffffff 4 800] ------- [4:255 -1:255 28 0] [0x2 3 1 [11 0] [0 4]] (REQUEST)
r 10.007911433 _1_ RTR  --- 0 AODV 48 [0 ffffffff 4 800] ------- [4:255 -1:255 28 0] [0x2 3 1 [11 0] [0 4]] (REQUEST)
r 10.007911536 _3_ RTR  --- 0 AODV 48 [0 ffffffff 4 800] ------- [4:255 -1:255 28 0] [0x2 3 1 [11 0] [0 4]] (REQUEST)
s 10.008339023 _2_ RTR  --- 0 AODV 48 [0 ffffffff 4 800] ------- [2:255 -1:255 27 0] [0x2 4 1 [11 0] [0 4]] (REQUEST)
s 10.008980281 _8_ RTR  --- 0 AODV 48 [0 ffffffff 0 800] ------- [8:255 -1:255 29 0] [0x2 2 1 [11 0] [0 4]] (REQUEST)
s 10.009049241 _6_ RTR  --- 0 AODV 48 [0 ffffffff 4 800] ------- [6:255 -1:255 27 0] [0x2 4 1 [11 0] [0 4]] (REQUEST)
r 10.009767178 _6_ RTR  --- 0 AODV 48 [0 ffffffff 2 800] ------- [2:255 -1:255 27 0] [0x2 4 1 [11 0] [0 4]] (REQUEST)
r 10.009767366 _4_ RTR  --- 0 AODV 48 [0 ffffffff 2 800] ------- [2:255 -1:255 27 0] [0x2 4 1 [11 0] [0 4]] (REQUEST)
r 10.009767386 _1_ RTR  --- 0 AODV 48 [0 ffffffff 2 800] ------- [2:255 -1:255 27 0] [0x2 4 1 [11 0] [0 4]] (REQUEST)
r 10.009767670 _5_ RTR  --- 0 AODV 48 [0 ffffffff 2 800] ------- [2:255 -1:255 27 0] [0x2 4 1 [11 0] [0 4]] (REQUEST)
r 10.009767767 _7_ RTR  --- 0 AODV 48 [0 ffffffff 2 800] ------- [2:255 -1:255 27 0] [0x2 4 1 [11 0] [0 4]] (REQUEST)
r 10.009767782 _10_ RTR  --- 0 AODV 48 [0 ffffffff 2 800] ------- [2:255 -1:255 27 0] [0x2 4 1 [11 0] [0 4]] (REQUEST)
r 10.010985333 _2_ RTR  --- 0 AODV 48 [0 ffffffff 6 800] ------- [6:255 -1:255 27 0] [0x2 4 1 [11 0] [0 4]] (REQUEST)
r 10.010985471 _1_ RTR  --- 0 AODV 48 [0 ffffffff 6 800] ------- [6:255 -1:255 27 0] [0x2 4 1 [11 0] [0 4]] (REQUEST)
r 10.010985603 _4_ RTR  --- 0 AODV 48 [0 ffffffff 6 800] ------- [6:255 -1:255 27 0] [0x2 4 1 [11 0] [0 4]] (REQUEST)
r 10.010985770 _7_ RTR  --- 0 AODV 48 [0 ffffffff 6 800] ------- [6:255 -1:255 27 0] [0x2 4 1 [11 0] [0 4]] (REQUEST)
r 10.010985949 _11_ RTR  --- 0 AODV 48 [0 ffffffff 6 800] ------- [6:255 -1:255 27 0] [0x2 4 1 [11 0] [0 4]] (REQUEST)
s 10.010985949 _11_ RTR  --- 0 AODV 44 [0 0 0 0] ------- [11:255 0:255 30 6] [0x4 1 [11 4] 10.000000] (REPLY)
r 10.010985961 _5_ RTR  --- 0 AODV 48 [0 ffffffff 6 800] ------- [6:255 -1:255 27 0] [0x2 4 1 [11 0] [0 4]] (REQUEST)
s 10.012148000 _1_ RTR  --- 0 AODV 48 [0 ffffffff 4 800] ------- [1:255 -1:255 27 0] [0x2 4 1 [11 0] [0 4]] (REQUEST)
```

Fig. 24 Trace file

4.1 Packet Delivery Ratio

It is the ratio of number of packets received to the number of packets sent. It illustrates the level of delivered data to the destination. The greater value of packet delivery ratio signifies better performance of protocol.

From Fig. 25, we find that the packet delivery ratio increases with increase in the number of node counts. Hence, it can be said that, in terms of rate of data delivery, our protocol outstands AODV.

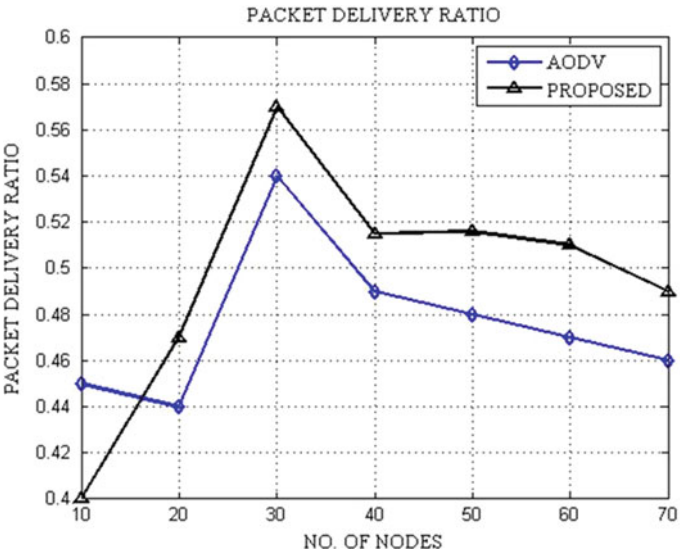


Fig. 25 Ratio of packet delivery versus nodes count

4.2 End-to-End Delay

End-to-end delay is transmission delay in data packets. Buffering during route discovery latency, queuing at interface queue, retransmission delays at the MAC, and transfer time may cause such delays. The minimized value of end-to-end delay represents improved conduct of protocol.

Hence, from Fig. 26, we can say that there is an approximate end-to-end delay with number of nodes. When the number of nodes is scarce, i.e., then the end-to-end delay is near about the same, but when the number of nodes is more than 40 then end-to-end delay maximizes. This shows that our protocol performs better than the AODV.

4.3 Packet Loss

It is defined as the difference between the number of packets transmitted by the origin and pocket by the target. The minimal value of the packet lost means better conduct of protocol.

From Fig. 27, we find that the packet loss rate of AODV and our protocol is approximately same for a less number of nodes. The loss in the rate of packets is increasing when the number of node is more than 10 nodes. So through this result we can conclude that for more number of nodes, the rate of packet loss of our protocol is lower than the AODV.

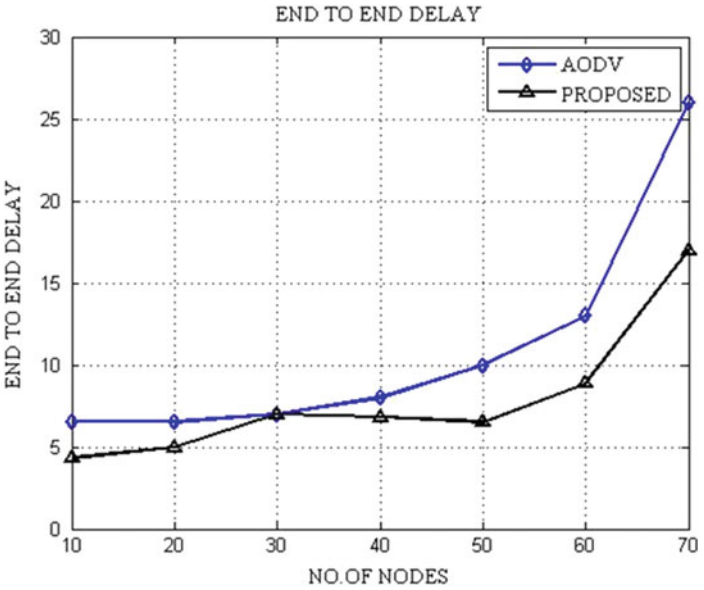


Fig. 26 End-to-end delay versus number of nodes

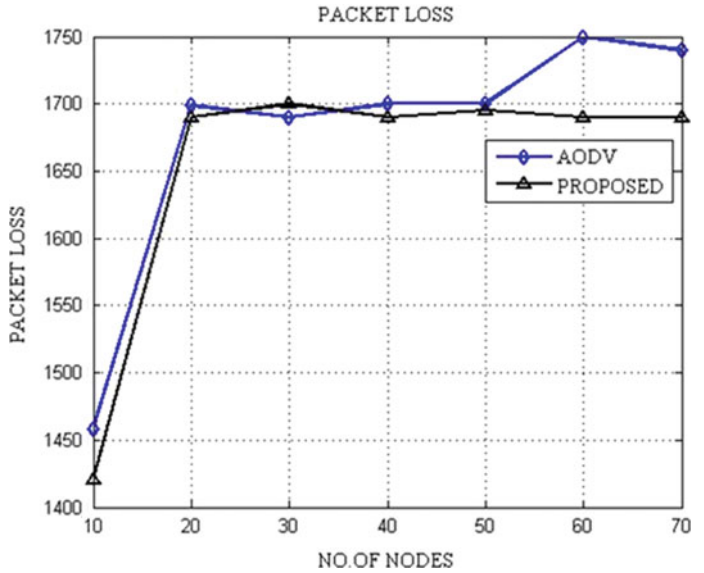


Fig. 27 Packet loss versus number of nodes

5 Conclusion

Changes in network topology limited the capacity of battery nodes. The unreliable behavior of wireless channel is a threat for descent routing in MANET. Selection of a long-lasting route is a demanding task in MANET. Our work explains a brand-new routing mechanism. When a route request message is added to the priority field, it refrains selection of unstable paths during establishment of a fresh path detection and adds the method of path repair to the route request message rather than beginning with a new routing discovery. NS-2 simulator is used to carry out the simulation. The simulation work shows improvement in the rate of packet loss, end-to-end latency, and throughput as well as network resources are utilized effectively.

Most of the enlightened routing protocols used for ad hoc networks are uni-path in nature. In uni-path routing, single route is used between origin and target node. In MANET, two protocols extensively used are DSR and AODV protocols. AODV and DSR are both on-demand protocols. In this paper, we used AODV protocol for route repairing mechanism. Future work includes identifying the route repairing mechanism using other existing protocol such as DSR, DSDV, OLSR, CGSR, TORA, etc.

References

1. Gautam, S. K., & Om, H. (2016). Computational neural network regression model for host based intrusion detection system. *Perspectives in Science, 8,* 93–95.
2. Das, S. K., & Tripathi, S. (2018). Adaptive and intelligent energy efficient routing for transparent heterogeneous ad-hoc network by fusion of game theory and linear programming. *Applied Intelligence, 48*(7), 1825–1845. https://doi.org/10.1007/s10489-017-1061-6.
3. Das, S. K., & Tripathi, S. (2017). Energy efficient routing formation technique for hybrid ad hoc network using fusion of artificial intelligence techniques. *International Journal of Communication Systems, 30*(16), e3340. https://doi.org/10.1002/dac.3340.
4. Das, S. K., & Tripathi, S. (2016). Energy efficient routing protocol for MANET using vague set. In *Proceedings of Fifth International Conference on Soft Computing for Problem Solving* (pp. 235–245). Singapore: Springer.
5. Das, S. K., & Tripathi, S. (2015). Energy efficient routing protocol for MANET based on vague set measurement technique. *Procedia Computer Science, 58,* 348–355.
6. Das, S. K., Tripathi, S., & Burnwal, A. P. (2015). Intelligent energy competency multipath routing in wanet. In *Information systems design and intelligent applications* (pp. 535–543). New Delhi: Springer.
7. Gautam, S. K., & Om, H. (2017). Comparative analysis of classification techniques in network based intrusion detection systems. In *Proceedings of the First International Conference on Intelligent Computing and Communication* (pp. 591–601). Singapore: Springer.
8. Yu, C. W., Wu, T. K., & Cheng, R. H. (2007). A low overhead dynamic route repairing mechanism for mobile ad hoc networks. *Computer Communications, 30,* 1152–1163.
9. Binh, H. T. T., & Dey, N. (Eds.). (2018). *Soft computing in wireless sensor networks*. CRC Press.

10. Chowdhuri, S., Das, S. K., Roy, P., Chakraborty, S., Maji, M., & Dey, N. (2014, November). Implementation of a new packet broadcasting algorithm for MIMO equipped mobile ad-hoc network. In *International Conference on Circuits, Communication, Control and Computing* (pp. 372–376). IEEE.
11. Chowdhuri, S., Chaudhuri, S. S., Banerjee, P., Dey, N., Mandal, A., & Santhil, V. (2016). Secure minimum loss route selection of MIMO-based MANET in combined (indoor, outdoor, and forest) terrain. Working paper. *International Journal Advanced Intelligence Paradigms*, 1–26.
12. Youn, J.-S. (2006). Quick local repair scheme using adaptive promiscuous mode in mobile ad hoc networks. *Journal of Networks, 1*(1), 1–11.
13. Jiang, M. H., & Jan, R. H. (2001). An efficient multiple paths routing protocol for ad-hoc networks. In *Proceedings of Fifteenth IEEE International Conference on Information Networking* (pp. 544–549).
14. Srinath, P., Abhilash, P., & Sridhar, I. (2002). Router handoff: A preemptive route repair strategy for AODV. In *IEEE International Conference on Personal Wireless Communications* (pp. 168–171).
15. Perkins, C. E. (1997, November). Ad hoc on demand distance vector (AODV) routing. In IETF Internet-Draft, draft-ietf-manet-aodv-00.txt.
16. Park, V. D., & Corson, M. S. (1997, April). A highly adaptive distributed routing algorithm for mobile wireless networks. In *Proceedings of the INFOCOM '97*.
17. Joa-Ng, M., & Lu, I. T. (1999). A peer-to-peer zone-based two-level link state routing for mobile ad hoc networks. *IEEE Journal on Selected Areas in Communications, 17*(8), 1415–1425.
18. Chung, C. M., Wang, Y. H., & Chuang, C. C. (2001). Ad hoc on-demand backup node setup routing protocol. In *Proceedings of Fifteenth IEEE International Conference on Information Networking* (pp. 933–937).
19. Srinivasan, T., Babu, T. N., Mahadevan, V., Nivedita, M., Sahitya, G., Meyyappan, A., et al. (2006). BFBR: A novel bird flocking behavior based routing for highly mobile ad hoc networks. In *Proceedings of International Conference on Computational Intelligence for Modelling, Control and Automation, and International Conference on Intelligent Agents, Web Technologies an Internet Commerce* (pp. 202–202).
20. Abdel-Moniem, A. M., Mohamed, M. H., & Hedar, A. R. (2010). An ant colony optimization algorithm for the mobile ad hoc network routing problem based on AODV protocol. In *Proceedings of 10th International Conference on Intelligent Systems Design and Applications (ISDA)* (pp. 1332–1337).
21. Dhurandher, S. K., Misra, S., Pruthi, P., Singhal, S., Aggarwal, S., & Woungang, I. (2011). Using bee algorithm for peer to peer file searching in mobile ad hoc networks. *Journal of Networks and Computer Applications, 34*(5), 1498–1508.
22. Misra, S., & Rajesh, G. (2011). Bird flight-inspired routing protocol for mobile ad hoc networks. *ACM Transactions on Autonomous and Adaptive Systems, 6*(4), Article No. 25.
23. Jain, J., & Gupta, R. (2011). On demand local link repair algorithm for AODV protocol. *International Journal of Computer Application, 35*(5), 20–25.
24. Naidu, P. P., & Chawla, M. (2012). Extended ad hoc on demand distance vector local repair trail for MANET. *International Journal of Wireless & Mobile Networks (IJWMN), 4*(2), 235–250.
25. Subburam, S., & Khader, P. S. A. (2012). Efficient two hop local route repair mechanism using Qos-aware routing for mobile ad hoc networks. *Indian Journal of Science and Technology, 5*(11), 3651–3659.
26. Rao, K. S., & Shrivastava, L. (2012). Efficient local route repair method in AODV to reduce congestion in MANET. *Corona Journal of Science and Technology, 1,* 35–38.
27. Al-Ani, A., & Seitz, J. (2016). QoS-aware routing in multi-rate ad hoc networks based on ant colony optimization. *Network Protocols and Algorithms, 7*(4), 1–25.
28. Singh, H., & Singh, P. (2017). Enhanced new clustering ant colony optimization based routing protocol AODV-R. *International Journal of Computer Applications*, *160*(9), 24–27.
29. Sarkar, D., Choudhury, S., & Majumder, A. (2018). Enhanced-Ant-AODV for optimal route selection in mobile ad-hoc network. *Journal of King Saud University—Computer and Information Sciences*. ISSN 1319–1578.

30. Das, S. K., Yadav, A. K., & Tripathi, S. (2017). IE2M: Design of intellectual energy efficient multicast routing protocol for ad-hoc network. *Peer-to-Peer Networking and Applications, 10*(3), 670–687. https://doi.org/10.1007/s12083-016-0532-6.
31. Yadav, A. K., Das, S. K., & Tripathi, S. (2017). EFMMRP: Design of efficient fuzzy based multi-constraint multicast routing protocol for wireless ad-hoc network. *Computer Networks, 118,* 15–23.
32. Das, S. K., & Tripathi, S. (2018, May 1–21). Intelligent energy-aware efficient routing for MANET. *Wireless Networks*, *24*(4), 1139–1159. https://doi.org/10.1007/s11276-016-1388-7.
33. Das, S. K., & Tripathi, S. (2018). Energy efficient routing formation algorithm for hybrid ad-hoc network: A geometric programming approach. *Peer-to-Peer Networking and Applications, 12*(1), 102–128. https://doi.org/10.1007/s12083-018-0643-3.
34. Mazumdar, N. & Om, H. (2017). DUCR: Distributed unequal cluster-based routing algorithm for heterogeneous wireless sensor networks. *International Journal of Communication Systems, 30*. https://doi.org/10.1002/dac.3374.
35. Mazumdar, N., & Om, H. (2017). Distributed fuzzy logic based energy-aware and coverage preserving unequal clustering algorithm for wireless sensor networks: Distributed energy-aware and coverage preserving unequal clusterING. *International Journal of Communication Systems, 30,* e3283. https://doi.org/10.1002/dac.3283.
36. Mazumdar, N., & Om, H. (2018). Distributed fuzzy approach to unequal clustering and routing algorithm for wireless sensor networks. *International Journal of Communication Systems, 31*(12), e3709. https://doi.org/10.1002/dac.3709.
37. Chaya, S., Jayasree, P. V. Y., Kumar, S., & Sah, D. K. (2018). Boolean directional sensor orientation solution for K-coverage in wireless sensor network. In *2018 4th International Conference on Recent Advances in Information Technology (RAIT)*, Dhanbad (pp. 1–6).
38. Sah, D. K., & Amgoth, T. (2018). Parametric survey on cross-layer designs for wireless sensor networks. *Computer Science Review, 27,* 112–134. https://doi.org/10.1016/j.cosrev.2017.12.002.
39. Sah, D. K., Shivalingagowda, C., & Praveen Kumar, D. (2018). Optimization problems in wireless sensors networks. In *Soft computing in wireless sensor networks* (pp. 41–62). Chapman and Hall/CRC.
40. Singh, A. K., Bera, T., & Pamula, R. (2018). PRCP: Packet replication control based prophet routing strategy for delay tolerant network. In *2018 4th International Conference on Recent Advances in Information Technology (RAIT)* (pp. 1–5). IEEE.
41. Singh, A. K., & Pamula, R. (2018). IRS: Incentive based routing strategy for socially aware delay tolerant networks. In *2018 5th International Conference on Signal Processing and Integrated Networks (SPIN)* (pp. 343–347). IEEE.

A Comprehensive Parameterized Resource Allocation Approach for Wireless Sensor Networks

Kumari Renuka and K. Hemant Kumar Reddy

Abstract Due to accelerated evolution in sensor dependency, WSN became popular. Since the past two decades, rational amounts of work have been recognized in different areas of WSN and its improvements. As a consequence of its dynamic properties and increase in its applications, it still draws researchers' attention to improve the quality of service. Constrained to its restricted computational capabilities and limited network capacities, it is indispensable to allocate the available resources to the critical and latency-sensitive applications in order to enhance the efficacy of these nodes. In WSNs, the role of routing is crucial and one of the most significant challenges in routing is energy consumption. The routing mechanism which drains the energy of the nodes will definitely result in poor performance. Battery life is a sensitive issue of these sensor nodes, power failure or low power can cause malfunctioning of certain nodes which in turn can create considerable topological changes and can affect the accuracy of these sensor nodes. Similarly, congestion control is another significant challenge in WSNs, which can lead to a major impact on the QoS parameters. Interference among the coexisting WSNs can cause significant variation in the link quality between the access point and a particular WSN. Consequently, affecting the performance of the WSNs. Hence, the link quality is also a considerable difficulty which must be taken into account in WSNs. By keeping the above challenges in mind, a multi-parameters-based resource allocation is contemplated in order to address all the challenges discussed above and design a comprehensive model for the resource provisioning. In order to accomplish the same, a multi-parameterized joint optimization model is proposed for WSNs which in turn leads to congestion free, energy efficient, link quality and application latency aware resource allocation network model. An algorithm is defined in order to deal with the computation complexity of the proposed model. Various simulation-based experiments are conducted in order to show the efficiency of the proposed model.

Kumari Renuka
Computer Science & Engineering, NIIT University, Neemrana, Rajasthan, India
e-mail: kumari.renuka@st.niituniversity.in

K. Hemant Kumar Reddy (✉)
Computer Science & Engineering, National Institute of Science & Technology, Brahmapur, India
e-mail: khemant.reddy@gmail.com

S. K. Das et al. (eds.), *Design Frameworks for Wireless Networks*,
Lecture Notes in Networks and Systems 82,
https://doi.org/10.1007/978-981-13-9574-1_7

Keywords Wireless sensor network · Resource allocation · Quality of service · Energy efficient routing · Multi-parameter-based allocation · Congestion control algorithm

1 Introduction

Any infrastructure which consists of communication, sensing and computing component which provides an administrator facility to react, instrument and observe the circumstances in a selective environment is regarded as a sensor network [1]. Typically, the administrator comprises of governmental, civil, industrial or commercial body. Possibly, the surrounding can be an IT structure, an organic system or the corporal world. Viewers see the networked sensor systems as a crucial technology which would process major usage in the coming years for a plethora of purposes like study of space, critical movement detection and vehicular movement.

Nowadays, networks of wireless sensors are generally built of huge number of economical devices, which are connected through wireless communications of low power. What differentiates a sensor network from a small group of sensors is basically the network's potential of enabling coordination, collaboration and cooperation amongst sensor assets. Whilst a number of sensors can directly be connected to processing stations and controllers (e.g. using LANs), a huge sum of sensors wirelessly transfers the collective information to a processing station which is centralized and it is required as a number of network applications is depended upon setup of hundreds or thousands of sensor nodes which are often set up to unreachable and remote areas only. Therefore, a wireless sensor is decked not only with a sensing material, but also an on-board storage, processing and communication capabilities. Beside these advancements, a sensor node is also responsible for data collection, for analyzing in network, fusion and correlation among data from other sensor nodes and its own sensor data. Many sensors collectively supervising massive physical environments, broadcast the information collected through sensors for remotely processing of visualization, storage systems and analysis. For an example, Fig. 1 depicts that the Internet is connected to two base stations and then to two of the sensor fields supervising two diverse geographical regions. Furthermore, the base stations are associated with different sensors from which it collects the data. The Internet includes the storage, analysis, mining and processing of data. Nowadays, sensors may also be illustrated as "smart" inexpensive devices which are bundled with more than one onboard sensing part. These, logically a part of central sink node, are low in cost and less power-consumable nodes solving multiple functionalities.

In brief, a WSN thus comprises of mainly three parts; sensors, observers and objects for sensing [2]. Wireless network provides a form of communication between observers and sensors. The most basic functionalities of the WSNs are data process-

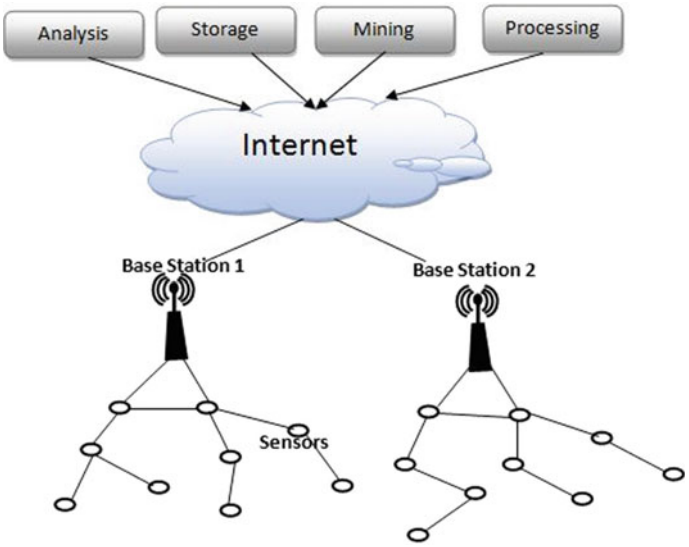


Fig. 1 Wireless sensor networks

ing, sensing, collecting data, distribution of gathered data, etc. Achieving some task of sensing among huge number of nodes and cooperation with just a handful of sensors along with only few functionalities and resources is one of the important characteristics of WSN. Moreover, in one WSN, movement of some nodes or even all of them is possible. Communication among nodes occur by ad hoc mode. Each and every node along with the ability to act as a role of router, they can also perform searching in dynamic fashion along with restoring and locating connections.

Sensors: It mainly comprises of sensing, transmission and units for power and storage. Its responsibility is to collect the data from an object in the physical world, storage of sensed information, making power efficient and easy calculation, and then transferring them to an observer.

Observers: They are the users who are actually using the wireless sensor network, who inspect, gather and exploit the data sensed passively or initiatively. These can comprise of men, computers or some other type of equipment. Before coming to any decision, they handle the sensed data by first mining them and then analysing briefly.

Sensing Objects: Sensing objects include temperature, humidity and so on, in which the observers are mainly interested in order to collect the information regarding it. Typically, the digital classifications of a few physical phenomena symbolize the sensing objects. Inside the network's distribution region, a WSN can sense a number of objects.

Typically, the architecture of WSN comprises of manager nodes, sink nodes, sensor nodes, etc. Primarily, a sensor field that observers are interested in are chosen and few sensor nodes then are deployed randomly in it. To exchange information, these nodes communicate among themselves through wireless channels. Second, a sink node is grouped around the field of sensors, to gather information received via sensor nodes. Finally, the gathered information is sent via the sink node to the node working as task manager via Internet. Because of number of reasons like the capacity of transceiver, the power supply, weight and equipment price, the distances of communication among sensor nodes are generally restricted as compared to the wired mode of sensor network. Through wireless channels, one node can only communicate among its neighbouring nodes. In case of out-of-scope communication among nodes, multi-hop router and multichannel routing mechanism should be used. Similar to other various communication networks, there are a large number of nodes included in WSN, which finally make the logic connections. Then, network topology is formed by overall connections between nodes [3]. For an example, there is a division of nodes into various levels in the hierarchical structure according to their abilities. There is more power in base stations compared to any other different nodes. In general, base station is regarded as the data centre and gateway to be able to connect with the other available networks. It is also sometimes regarded as the sink node. But the sink node acts as a receiver, they are data collector all sensor nodes send data to the sink node. A portion of typical sensor nodes is led by the cluster head. It handles collection of information from the subset and then some and commands are sent to them. There is another thing called topology control, which is concorded with WSN's topology. To handle WSN's logical connections, various special factors relevant to WSN like scarce amount of energy, unstable type of infrastructures, limited number of bandwidths, etc., should be considered as the methods and way for controlling topology. Routing technologies must also be considered simultaneously as some of the control methods. Moreover, along with the failures or movements of some nodes, the WSN will alter its logical topology.

1.1 Background of Wireless Sensor Network

Any such devices which gathers information regarding a process or physical entity, including the manifestation of actions such as state change, e.g., reduction in pressure or temperature using a sensing technique, is regarded as a sensor. Other examples consist of sensors which are natural, like the body of human is rigged full of sensors, which can receive and capture audio data like sounds (cars), smells (nose) and surroundings' optical information (eyes). These sensors which gather data of the object which is monitored without even touching them are considered as remote sensors. However, looking from a technical aspect, a sensor is regarded as any device that

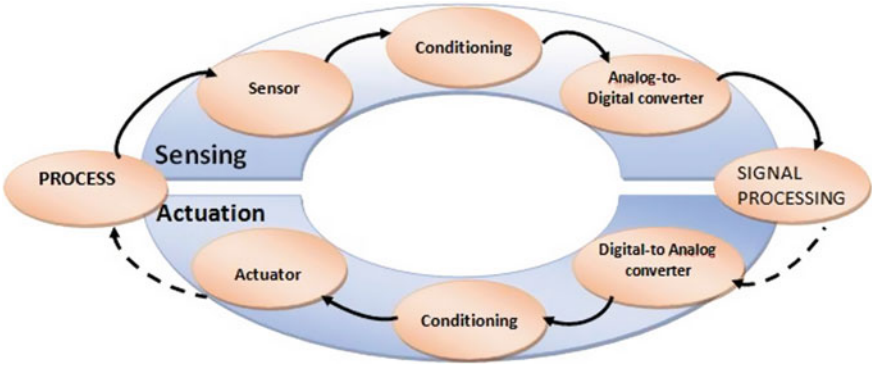


Fig. 2 Data acquisitions and actuators

transforms the existence of real-world's actions and their parameters into communicable signals which can get measured and investigated correctly. Additionally, other words often in use is a transducer, which makes the energy convert from one of the forms to the other. Thus, a sensor can also be regarded as a form of transducer, which translates real-world's energy into the electrical energy which may then get transferred to a controller or a system used for computing. One of the ways of how a task of sensing is performed is depicted stepwise in Fig. 2. Sensor device observes the aspect in the real planet (regarded often as system, plant or process). The electrical signals retrieved are transmitted via signal conditioning stage as most often they are not ready for immediate processing. To get the sensor signals ready for further use, here, a diversity of processes can be enforced to it. For example, to modify the magnitude of signal to match and improve the range of the consequential analog-to-digital conversion, attenuation (or amplification) of the signals may be required. Additionally, filters are frequently applied to the signal by signal conditioning to eradicate unwanted and redundant noise which is within the defined frequency ranges (like to expel 50 or 60 Hz noise gathered by nearby power lines, high-pass filters can be used). After applying conditioning, there is conversion of analog signal into digital signal for additional storing, analysis and processing, through the analog-to-digital converter (ADC). Nowadays, wireless sensor networks mostly include actuators, that entail them to control the real-world directly. Pump is an example of actuators which could be used to control the amount of fuel inserted into an engine, a motor that closes or opens a window or a valve or door controlling the hot water's flow. Wireless sensor and actuator network (WSAN) receives the command through controller (or processing device) which then converts them into actuator's input signals, which acts along with real process and thus making a closed and controlled loop, as depicted in Fig. 2.

1.2 Features of Wireless Sensor Networks

Usually, any network that has network system which is self-organizing and multi-hop and consists of varied nodes which use wireless communication to communicate with each other, is regarded as WSN. Generally, wireless LANs, networks of mobile cell, ad hoc, Bluetooth, etc., are included in wireless communication networks. WSN, as wireless communication network's special kind, comprises of various micro-sensor nodes which are low cost and deployed in the monitoring region. Such sensor nodes coordinate among themselves for sensing, gathering and doing processing of data from sensing of objects in network's coverage area, and then those being sent to the observers. Along with wireless communications network's commonness, WSNs in addition have their own following distinguishing features

Application Related: Through the sensing of physical quantities of objects, WSNs gathers data from the outside world. The requirements of network systems are different in different applications, which lead to great variations among hardware platforms, communication protocols and software systems. This leads to the variation in WSNs with the Internet whose protocols for communication are unified, and thus the platform accomplishes reliable and system goals efficiently. The remarkable trait of the WSNs, that comprises of the design work to be analogous to each special application that vitally varies with the traditional mode of networks. Users notify related incidents to the sensor network and thus not particularly to only an individual node when they require to inquire about some incident.

Large-Scale Distribution: In some huge stretch of areas, WSNs are usually deployed unanimously. When the area is expanding further, the density and quantity of nodes will increase greatly. Usually, it is very difficult to make maintenance as often the areas monitored are difficult to reach. Therefore, there should be presence of strong fault-tolerant along with highly robust hardware and software within the sensor network.

Dynamic Topology: WSN's topologies can be altered dynamically by many reasons. For example, in some cases, sometimes new nodes join or leave the networks; there may be mobile sensor nodes; for power saving, a few nodes are made to alter from sleep to work status without any restriction; due to few unpredictable reasons, some nodes can get broken any time. WSNs must have competency for reconstruction and self-adjustment along with the vigorous alteration among the networks' topological structures.

High Reliability: Often, WSNs are deployed in some unmanned areas or despicable environments over large scales, which make it very difficult or even impossible to maintain the network online. Thus, the sensor nodes are needed to be very stable, adaptable to various extreme environments and difficult to damage. Additionally, it is crucial to apply some security and privacy mechanisms for wireless sensor communication to avoid the stealing of monitoring data and to obtain counterfeit data by observers in few of the vital WSNs. Thus, all above needs high reliability in WSNs, to complement well robustness and fault tolerance.

Self-organization: Within network's real environments, there are various unpredictable factors. For an example, nodes' precise positions in advance cannot be conceived; due to reasons like exhaust of energy, some nodes also die; accurate forecasting of wireless communications quality constrained to environmental consequences cannot be done; there are some uncontrollable network environmental emergencies. There should be the capability of self-organizing in making of all above nodes. Without the interference of human or different pre-network facilities, self-configuration and self-management can be done by the nodes automatically and quickly.

1.3 Challenges and Constraints

Sensor networks suffer a diversity of unique constraints and challenges in spite of having a lot of commonalities with the other different distributed systems. These limitations reflex WSN's design, which leads to difference in algorithms and protocols from their correspondents in various other distributed systems. WSN's most vital design constraints are specified in this section.

1.4 Energy

Sensor nodes running with the restricted budgets of energy, is mostly the common limitation related with the design of sensor network. Generally, these nodes are steered by batteries, that should either be recharged or replaced (like when solar power is used) when used up. Although, they will be abandoned simply as and when their source of energy gets exhausted, that is at that moment neither option is available for those nodes. The strategy applied to energy consumption is significantly affected whether the battery can be recharged or not. There must be an operable sensor node, for non-rechargeable batteries, until either the battery can be replaced or its mission time finishes. Thus, type of application tells the length of the mission time, for example, sensors that can work for many years may be required by scientists supervising glacial movements while a sensor may be required only for few hours or days in case of a battlefield scenario. Consequently, energy efficiency is WSNs' first and foremost vital design challenge. All of the aspects of sensor node and network design get invaded by this requirement. For providing access to the wireless channel, the medium access control (MAC) layer provides with the required sensor nodes. For communication networks, there are some contention-based MAC strategies, viz, nodes might try if, at any time it can use the medium, and thus multiple nodes may collide as a consequence, which MAC layer has to look after to make sure that there will consequentially be successful transmissions. Disadvantages of such

approaches comprises of delays and overheads of energy provoked by collisions and mechanisms of recovery and to ensure that no transmissions will be missed, sensor nodes, at all the time, might have to listen to the medium continuously. Therefore, there are some contention-free sensor networks' MAC protocols, viz, medium's access is compulsorily governed, removing collisions and thus allowing shutting down of sensor nodes' radios when there no expected communications. The network layer's responsibility of searching for routes between sensor node and base station, and features of routes like length, available energy on relay nodes and required transmission power determines the overheads of energy of multi-hop communication. In addition to network protocols, operating system's design is impacted by the goal of energy efficiency (e.g. altering among tasks efficiently, small memory footprint), mechanisms for security of middleware and even applications themselves. For an example, to combine more than one reading from sensor or to eradicate redundant and frequent sensor data, in-network processing is often applied. This generates trade-off between communication (relaying the processed versus the original data) and computation (processing the sensor data), which can often be used to save energy.

1.5 Congestion

Along with support of varied applications' domains, WSNs are mainly classified into two types, viz, tracking and monitoring. These applications may generate upstream data which may either be query driven, event driven, hybrid or continuous. Relatively there is low traffic load in an event-driven application and it gets activated only when certain event occurs. Consequently, due to simultaneous generation of data by nearby nodes, congestion occurs in these applications. There is continuous sensing and transfer of information to the base station in continuous sensing applications. Since the network remains occupied in sensing in these applications all time, it leads to congestion. The network is handled centrally by base station in the applications which are query driven. In such applications, the base station broadcasts the query to the nodes, resulting into gathering of information. While on other hand, hybrid applications supports the bulk and continuous flow of information simultaneously. Congestion occurs in such applications because of inconsistent rates of data supervised by these flows. Hence, WSN's main challenge is congestion.

1.6 Node Deployment

For the development of protocols of WSN, another factor which is considered is the deployment of WSNs. The sensor nodes' positions are not required to be predetermined or engineered. This leads to randomly deploy in disaster relief operations or an inaccessible terrain. On the other hand, for the communication protocol stack, developing protocols that are self-organized is required by the random deployment.

Particularly, sensor nodes should be self-managing, such that these are able to collaborate and operate with different neighbour nodes, getting adapted to the failures, variation in environmental stimuli without human intervention and environmental changes in general. Moreover, after deployment of various sensor networks, they must work disregarded, viz, maintenance, repair and adaptation should be practiced in a self-governing fashion. Also, to make sure that there are no excessive energy overheads, there should be implementation and designing of all such self-management components.

1.7 Wireless Medium

There are various challenges posed to the designer of sensor network designer by the dependency on wireless networks and communications. For an example, fading in large and small-scale limits the radio signals' ranges, that is, there is attenuation of radio frequency (RF) signal when it travels through a wireless medium. Power that is received is inversely proportional to the square of the distance from the source of the signal. Consequentially, as distance increases between a base station and a sensor node, the required transmission power is also increased rapidly. Thus, splitting larger distances into several shorter distances is more energy efficient, but leads to the stimulation of supporting routing and multi-hop communications. It is required that in the multi-hop communication, the network's nodes should cooperate with each other to determine to serve as relays and to determine efficient routes.

1.8 Hardware Constraints

The ability of traditional computing systems has been increasing rapidly these days, still the main goal of WSNs is to produce a cheaper, smaller and further efficient and competent devices. As styled previously, the five node components styled previously must also fit an embedded system of matchbox sized. The execution of algorithm and designing of several protocols in WSNs are also affected by the hardware restrictions of the sensors. For an instance, each destination's entry in the routing table might be a lot massive to come into the memory of sensor. In sensor node's memory, only a small amount of data can be kept. Moreover, while in-network processing could be assigned to remove false data. More storage capacities and computational power may be required than the low-cost sensor nodes by few aggregation and fusion algorithms. Hence, many software architectures and solutions should be planned to function efficiently on hardware which are resource constrained.

1.9 Security

Various sensitive information is collected by the WSNs. When a sensor node is operated remotely and unattended, it leads to rise in their vulnerability to malicious attacks and interventions. Additionally, there is an insecure transmission in case of shared wireless medium. Depending on what is the type of sensor network application, there can be drastic repercussion of a viable intervention. If the readings of the sensors are not sent to the network's sink node with an apt possibility of success, it could hamper the proper accomplishment of decisions or control actions. Nonetheless, there can be substantial increase in energy consumption of the network, if the reliability is maximized. Although, to avoid any attack or it's related extent or damage, a number of solutions and techniques can be followed for distributed systems, tons of which may demand requirement for huge communication, storage and computation, which in most case unable to be fulfilled by the sensor nodes with resource constraint. Therefore, it is required by the designers of the network to take into consideration, the trade-off amongst amount of energy consumed and reliability, and thus put forward new solutions, which can be used for establishing key and distributing it, maintaining secrecy and authenticating node.

Currently, in Wireless Sensor Network, there have been numerous works devoted individually to the link quality, energy efficiency, routing, congestion control and QoS requirement, but no single model is there which addresses all the issues together. Hence, by considering all the challenges faced in Wireless Sensor Network, we are motivated to design a comprehensive model for the resource provisioning. Our main motive is to propose a multi-parameterized joint optimization model for WSNs which in turn will lead to congestion free, energy efficient, link quality and application latency aware resource allocation network model.

Based upon the several discussions above, these are the following contributions presented in this chapter

- An architecture is demonstrated to explain the importance of addressing all these challenges faced in wireless sensor networks.
- Keeping the main challenge an algorithm is defined for a multi-parameterized joint optimization in WSNs which in turn will lead to congestion free, energy efficient, link quality and application latency aware resource allocation network model.
- Several simulation-based evaluations are accompanied so that validation and evaluation of the effectiveness of the model which is put forward, can take place.

The remaining chapter is divided as follows. The chapter's related work is provided in the Sect. 2. Section 3 describes the architecture which explains the importance of addressing all these challenges faced in wireless sensor networks. The multi-parameterized joint optimization algorithm is proposed in Sect. 4 and Sect. 5 depicts the results based on simulation so that the efficacy of the model which is put forward gets proven. Finally, conclusion is described in Sect. 6.

2 Related Work

Wireless sensor networks (WSNs) comprises of minor devices incorporated with sensors to detect, investigate and closely observe the physical conditions. The phenomenon is essential for gathering and transmitting the data towards the base station. The gathering of data from the surrounding is the primary objective of the WSNs. In the twenty-first century, the Wireless Sensor Networks (WSNs) is extensively regarded as the utmost essential among the different technologies [1]. Empowered by latest approaches in wireless communication technologies and microelectronic mechanical systems (MEMS), small, smart sensors and less expensive positioned in a bodily region as well as connected across the links which is wireless, while the Internet offers unparalleled prospects for an innumerable choice of military and civilians' applications such as industry process control, battle field surveillance and environmental monitoring [2]. Prominent from traditional communication wireless networks, for example, mobile ad hoc networks (MANET) and cellular systems, WSNs have distinguished characteristics, for example, denser level of node deployment, higher fallibility of sensor nodes, and intensive energy, calculations, and storage restrictions [3], which creates many unexpected challenges in the development and exercising of WSNs. In the past decade, WSNs have been under limelight from both academia and industry all across the world. A huge amount of research pursuits has been carried out and still in progress to unleash and solve various design and application issues, and impacting advances have been made in the development and deployment of WSNs. It is anticipated that in the near future WSNs will be widely used across civilian and military fields, and transform the way we live, work and connect with the physical world [4].

Congestion control in WSNs—There are numerous types of sensors in wireless sensor networks (WSN) that gather environmental data. The data which is collected is then relayed by the utilization of multi-hop routing protocol from one sensor node to another to the preferred destination which is called sink. The analysis and data aggregation are accomplished at the sink node since there is restriction in sensor node's processing capabilities, memory and the power of battery. Hence, the main objective of many routing schemes is the finest resource utilization of WSN so to attain maximum throughput. Initially, the designing of the routing schemes which are trivial were focused much by the researchers to permit transfer of information in the WSN. Afterwards, it was comprehended by the researcher that there must be a mechanism which is efficient in order to tackle the problem which arises when the single link traffic or the overall traffic turns out to be larger than its individual, this is called congestion-control mechanism. Congestion control is crucially important as it precludes the traffic loss in bulk. In terms of time variant quantities, for instance, frequent change of the buffer and the network traffic, congestion control is an important research area. Sometimes congestion control can become further complex and

challenging when the resources are limited. Congestion is of two types—link and node congestion. The former typically results from overflow of the buffer and leads to severe high transmission delay and loss of cause the packet. The wireless channels collisions are usually led by the latter. When the channel is occupied by the sensor nodes concurrently then the collisions usually takes place. Various efforts have been put to discover the solution to congestion control and assure guaranteed transmission of data in WSNs. A scheme called decentralized predictive congestion control (DPCC) [5] recognizes the estimation of embedded channel to forecast congestion and the quality of channel exploiting the utilization of the queue. In DPCC, a desirable rate imposed through adaptive back-off interval selection scheme is chosen by the adaptive flow control algorithm. A rate control mechanism based on priority was implemented in [6] in order to tweak each and every traffic source's priorities so that it controls the congestion rate, modifies the traffic rates of source which is based on upstream nodes' congestion as of now and changes the contrast in service in wireless multimedia sensor networks according to requirement. The congestion might be successfully lessened by the traffic control but it leads to negative impact on the fidelity. Thus, a novel approach must be derived to remove congestion while satisfying the requirement of application fidelity. In [7], MintRoute algorithm is defined which service the hops from the radio links' quality and sink to discover next hop. There are often more than one path selected by MintRoute for routing of packets, in case of overloaded network. In that case, for recognizing the quality of link, various packets are used which are dropped at local node. Theory of potential in the classic physics is used in TADR [8] to model a potential field which is hybrid as well as virtual, using normalized queue length and its depth so that it forces the data packets there is no obstacle arising due to congestion and thus finally flow towards the sink. Yet, the algorithm described before, pays consideration only to the node or link congestion and is unable to distinguish accurately the degree of congestion of the node. Whenever the sensor node gets more packets, then it can forward then the extra packets are deposited in buffer. When the buffer size is full and more packets are arriving then congestion takes place and the excess packets get dropped. Congestion triggers several severe impacts. Whenever congestion takes place, the transmission delay as well as the network transmission performance like the expansion of packet loss rate can get extremely affected. The congestion control is an important challenge in WSNs, hence it must be considered properly.

Energy efficiency in WSNs—In WSNs, there is requirement for designing of protocols for transport layer which addresses the congestion efficiently while reducing network's lifetime, loss of packets and saving the amount of energy consumed. Hence, the responsibility lies on transport layer protocol for getting recovered from loss and congestion control. These factors lead to directly affect the application's QoS and whether the network has efficient energy under observation. Various software-based solutions are being derived by the several researchers so that the network's energy can be saved [5, 9, 10]. A comprehensive discussion on the different techniques

used to save the energy consumption is given in [4]. By minimizing the data rate of source, protocols for congestion control based on traffic diminishes the network's traffic load. Rather than searching for substitute routes, the same route is being used to delay the packets approaching the destination. This impact the energy consumption rate, in a single unit of time the devices consume large volume of energy, which in turn reduces the network's span of life. Opposing to congestion-control protocols based on traffic, the protocols based on resource take advantage of the resources which are idle in the network each time a node becomes the target. When congestion takes place, these protocols perform the routing again and reroute the extreme traffic towards the base station through alternative route, leading to which, there is balancing of traffic load between uncongested and the congested routes of the network while maximizing the network's span of life and the throughput. Moreover, the shortest route is chosen by the resource control protocols to delay their packets. Moreover, a control scheme for topology is always applied by these protocols [11] in order to maximize the number of alternative routes. Furthermore, these various ways can be utilized which in turn will stabilize the consumption of energy when the load on the network is dense. Since, the node exhausts their energy consistently maximum lifetime can be obtained. Hybrid congestion control protocols, they first attempt to control the congestion by inspecting the occupancy of the buffer of the nodes which are congested. Every time, when the buffer of the node which is congested reaches its maximum threshold value, an alternative route is chosen by using the resources of the network which are idle and do the routing again of the congested node's outgoing traffic to the base station instead of dropping the extra packets from the buffer or reducing the traffic rate. Evading congestion by using the hybrid congestion-control protocols appears to be a favorable option that leads to lessen packet loss, consistent utilization of energy and better throughput. On the other hand, in the sort of control messages, these protocols experience an increase in overhead.

Routing in WSNs—The design targets of routing protocols in WSNs differs between different applications and these protocols are application dependent as well. For an example, various applications need communication in real time, for an instance, there may be a dependency of fire fighter upon timely updates of temperature, so that there can be awareness of conditions of fire recently while the only requirement by soil monitoring system is that in hourly interval the measurements is being informed. Hence, the delay requirement must be met at least energy cost by the routing protocols. So, the features of sensor nodes must be considered by the designer of routing protocols accompanied by architectural and application requirement. Previously, many routing protocols have been modeled which guarantees energy efficiency but do not promise the QoS requirement. So, in the research of WSNs, the issue which has gained rise in importance is routing. Many efforts is being dedicated to the routing protocols as these vary based on architecture of the underlying network and user applications nature. An example of scheme for routing with two or more tier is the hierarchical routing, CHs behave like a backbone of routing and are the upper-tier

nodes, while the task of sensing is performed by the lower tier nodes. It was claimed by Kulkarni et al. [8] that networks which are multi-tier, possess extensible property and pose various benefits such as higher functionality, better coverage, better reliability and low cost over single-tier network. LEACH was among the first protocols based on clustering, as in [7]. To steadily allocate the energy load between network's nodes, there is exploitation of rotation of CH role in randomized fashion by the LEACH. Application where gathering of information takes place in a periodic fashion to a centralized locale and continuous supervising is required LEACH is highly preferred for such operations. Various assumptions have been made on LEACH in which the authors' outlook limit to the capability in various applications, like communication within the single hop. The concern of nodes' heterogeneity in energy's terms is tackled by Smaragdakis et al. [12]. By recognizing the influence from node's heterogeneity, the profit due to such applications would encourage their protocol's enhancement. For an example, wherever there is restriction of sensor's spatial density, the WSNs along with their applications are re-energized. Such protocol makes various kinds of assumption; it assumes that there is a direct path from all nodes to the sink. Knowledge of level of energy of other nodes in the network is essential to calculate the probability of CH election, which need extra communication overhead. In [13], a protocol called HEED was proposed by the author for sensors application which requires efficient aggregation of the data. HEED generates clusters which are stable with least message overhead by utilizing the information about the residual energy and the node degree. With respect to efficiency of energy, it performs better than the generic protocols for clustering. In spite of this, HEED undergoes a high network delay and is still heuristic in nature because of CH selection algorithm complexity. Contrasting the previous work aiming at the optimization of network lifetime and energy efficiency, minimum energy spanning tree for efficient routing (MESTER) was proposed by Yang et al. [14] for longer preservation of significant quality in gathering of information.

Link quality in WSNs—Management of the link quality is an important issue which must be kept into consideration as it makes an impact on the network performance as well. The fundamental idea is the temporal link-quality-based resource allocation management, which indicates the satisfaction of the several requirements such as network lifetime, fairness, energy efficiency and admissible link rates. Numerous years have been spent to examine the channel allocation and scheduling of link to achieve some of these demands by the researchers. Following are a few works which are already existing. A protocol of routing for energy-aware and link-stability was put forward by the Rango et al. [15] which assure the minimization of energy consumption and stability of quality of link in static wireless network. Various other works reveal the dependency between wireless links and the correlation between reception of packets on wireless links which are nearby. Hence even for calculation of most basic metrics, there may be vital problems of estimation due to the link independence assumption. So, there was a proposal of an opportunistic mode of

routing for correlated link by Wang et al. [16]. The model takes account of correlated links with a less value and leads to improvement in the performance. Alternatively, for downlink network which is wireless, Bodas et al. derived a scheduling algorithm for multiple channels [17]. An algorithm which is repetitive longest-queue-first, was put forward by the authors to reduce the network's delay to minimum. In the same way, the dynamic channel allocation algorithm was proposed by Chowdhury et al. to reduce message overhead and to maximize residual energy [18]. The use of multichannel allocation intensely varied the energy-constrained environment of WSNs. A routing protocol which has link awareness as well as uses energy efficiently was put forward by Ahmed [19] for WBANs so that with respect to energy efficiency and path loss, the behavior can be examined.

Various studies have been devoted in the field of wireless sensor networks. Shaikh et al. [20] have proposed an analysis on the design of high performance and efficient energy harvesting system in wireless sensors networks by presenting a comprehensive taxonomy of different energy harvesting techniques. Several drawbacks and limitation have been identified by them that need to be addressed in order to build efficient, reliable and cost-effective energy harvesting systems for Wireless Sensor Networks. Lin et al. [21] identified that in order to maintain a communication link which is reliable, the power control is an essential requirement and thus formulates a modest distributed protocol which permits the increase in power level with the purpose to assure the connectivity of network while maintaining energy efficiency. In their paper, they inspect the energy efficiency against connectivity of network and designed a protocol which can be instigated on the top of MAC protocols. Modern advances in wireless technologies have critically prompted the rise in Industrial Wireless Sensor Networks. Han [22] in his paper presents the comparison between four recent energy-efficient coverage strategies including: OTTC, CWGC, AR-SC and OCCH in terms of ratio of dead nodes, coverage time, network lifetime, average energy consumption, etc. Their findings intent to deliver IWSNs designers with valuable intuitions to select a suitable coverage strategy as well as gain performance indicators as expected in various applications of industries. Another important work has been present by Cheng [23]. In their work, they presented the occurrence of the latency energy trade-off in flooding. They model the issue as an undetermined-delay-constrained minimum spanning tree (UDC-MST) problem. In order to deal with the NP-hard problem they constructed an MDET algorithm to provide a flooding delay bounding energy optimal tree. A large volume of data is being produced by the various sensors which must be analyzed to extract useful information from it. From the analytics viewpoint, the main motive from analyzing such sensor data is to benefit insights from the energy consumption patterns. Fong [24] presented a modified version of VFDT which studies from results which are misclassified in order to filter the noisy data from maintaining and learning the accuracy of classification of prediction model which is induced. Mostafaei [25] focuses on QoS routing which is one of the important challenges in WSNs which must be addressed. They proposed a DLA algorithm with an intention to provide multi-constrained optimal path.

Hence, by considering all the challenges faced in Wireless Sensor Network we designed a comprehensive model for the resource provisioning in this chapter. Our main motive was to propose a multi-parameterized joint optimization model for WSNs, which in turn will lead to congestion free, energy efficient, link quality and application latency aware resource allocation network model.

3 System Model and Problem Statement

In this section we define a multi-parameterized joint optimization model for WSNs which in turn will lead to congestion free, energy efficient, link quality and application latency aware resource allocation network model. In a L × L square area the sensor nodes are arbitrarily distributed as indicated in Fig. 3. Periodically, the nodes representing the sensor collect information from the surroundings and then by multi-hop manner it forces the packets to the sink. Following are the descriptions.

i. In a square area, random distribution of one sink and N sensor nodes in number are established. After the deployment all the nodes will never make a movement.
ii. All the nodes which are ordinary have equivalent primary state and possess the isomorphic property.
iii. Sensor nodes supplies consistent energy supply.
iv. The transmission power can be differed by the nodes depending upon the receiver gap from its own position. Grounded upon the strength of the signal which is received, the distance between the receiver and transmitter can be computed.

Example of Congestion Situation

Figure 3 illustrates a situation where the congestion will appear. When the data is transmitted by sensor node B and C together by following the shortest path via node 1 then the congestion will take place at node 1 as shown in Fig. 3a, respectively. Situation will become enough worse than before if the node B selects the alternation path by passing the data packets to the node 2, there is a possibility congestion at node

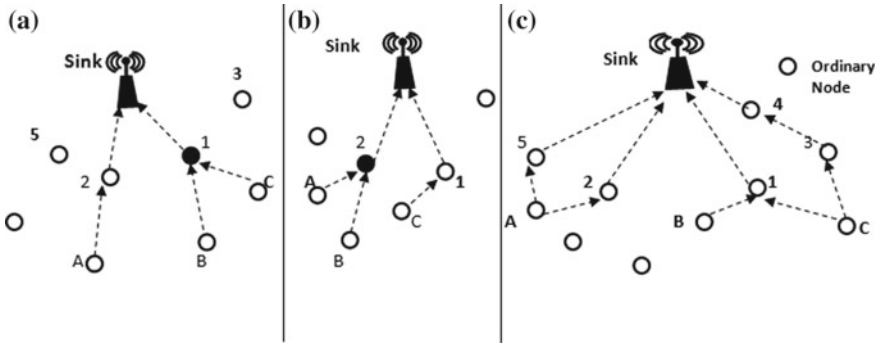


Fig. 3 An illustrative example

2 also as given Fig. 3b. However, this problem can be solved if the multipath routing is initiated by the sensor nodes which are forwarding the data packets. The ability of transmission with an intention to forward the packets containing data to the resources which are not used and the degree of congestion must be kept into consideration. Through this way, we can find more appropriate path to transfer the data packets. For an instance, the path C->3->4->sink and A->5->sink can be chosen to facilitate the transfer of data packet as shown in Fig. 3c. Multipath routing leads to better utilization of the resource as well as even distribution of the data packets amongst the network. Through this, the congestion can be minimized effectively while making the performance of the network better. But this has a various disadvantage associated with it, choosing the alternative path can lead to more consumption of energy as well as cause delay in transmission. However, if we consider the position of each node representing the sensor, deadline and the remaining time of the packets into account, then the disadvantages associated with it can be overcome. To achieve this goal, an optimized routing scheme grounded upon congestion control for WSNs is anticipated by us. Overall, the essence of our proposed algorithm is to enable multi-path routing via following the shortest path by keeping all the constraints in mind. The proposed routing algorithm will tend to increase enhancement in the congestion control and the accomplishment of the network in terms of better functioning.

4 Algorithm Design: CPRA

The multi-hop forwarding manner, centralized data acquisition and sudden event stream in wireless sensor networks are the major reasons for congestion, which leads to severe impact on accomplishment of the network in terms of transmission functionality and results in QoS degradation. An important idea behind our proposed model is to develop an algorithm which will discover a finest route among the sensor nodes which will be delayed controlled while minimizing the energy consumption. We will grab hold of congestion control and energy efficiency both together into consideration while conceiving the routing algorithms on behalf of WSNs. The model of the network can be depicted with a graph G (V, E), where V symbolizes the sensor nodes and E exemplifies the set of edges which stands for the links which is wireless among the sensor nodes. Table 1 describes the list of keywords which is used in the algorithm.

Algorithm 1 is used in order to obtain an energy-efficient route matrix by keeping the delay constraints in mind. In Algorithm 1, soon after we get the information of neighbouring nodes after the gossip stage, each individual source node s gathers information of every other individual source nodes Ns, and the expense of each individual edges W. In the route construction phase, every single node belonging to Ns can be incorporated into the route. Intermediate distance between two nodes is obtained from the route matrix, which is constructed using Euclidian distance between two nodes. Therefore, up to this point, we got W, which comprises of the cost of e edges covered by all the source nodes, either by sending the signal or receiving

Table 1 List of notations

Acronym	Definition
G (S, E)	Network topology (V = sensor node, E = edge between sensor nodes)
N	Source node
Sn	Set of neighbours of the source node
W	Sink node
T	Remaining time of the packets
Ds	Deadline set
Cp	Construction path
R	Routes
M	Minimum remaining time of the packets

it during the gossip. The stage involving construction of the route is grounded upon the original push forward insertion algorithm proposed by [26], modifying it to get equipped with the requirements of the WSNs. In this, for every single individual node, we find the least possible cost of the path to the node representing the sink according to the Bellman–Ford algorithm and then find those nodes with the maximum cost of the path to the sink. Thus, keeping in mind the lowest insertion cost, we incrementally select the candidate nodes. For each candidate node, overall delay requirement is also checked regularly. The least possible cost of the path to the node representing sink in our case is calculated by first permitting every single node representing the source to estimate the weight of the path that is minimal to every other nodes within the range of the gossip borders that make topographical evolution on the way to sink, as well as estimate the weight of the path from that particular node towards the sink with an intension that it can then select the one with the least possible total weight of the path. As each node, depending upon the node type, starts with the fixed amount of energy, the status of the nearby nodes can be accurately estimated. In that case, with the formerly held evidence, the minimum weight of the path from the intended source node to an adjacent node can be estimated. Imagine that there exists a path in the gossip stage, which acquires hops from given node to the node representing the sink, as well as the node is aware of the weight of the edge of the first hops as well, then by utilizing the average cost per link and number of hops whole cost of the path is evaluated. The source can then evaluate the cost of complete path from the sink to itself. The complete flow of the distributed algorithm is illustrated in Algorithm 1. Notice that, in order to choose the upcoming recipient node by either being chosen as the distant node to sink or obtaining a route construction packet, a node representing the source will be prompted. As soon as all the intended source nodes are incorporated into their personal route, the algorithm terminates. Also note that merely the status of the neighbourhood node is being taken into account in the route construction phase to estimate least possible cost of the path amongst the nearby source nodes.

ALGORITHM 1 : Delay Controlled Energy Efficient Route Matrix Detection (DCEERMD) (Topology Graph, Source node, Neighbours source nodes, A set of deadlines for each packet, Packets remaining time, Node representing sink)

Begin
Input: Source node n, the neighbour source node set Ns, Topology Graph G, the deadline set Ds, the sink node w and the remaining time of packets t.
Output: Routes Matrix constructed with least possible cost of the path such that there is no violation in Ds.
1: Collect status of neighbourhood nodes.
2: Using Bellman ford Algorithm, estimate least possible cost of the path of n and all si ϵ Ns belonging to sink node w.
3: Insert all nodes present in Ns in the list of potential candidates set C.
4: Get all the distances between all the source node and the sink as well as the distance between the neighbouring nodes of source and sink from the route matrix
5: **if** for all distanceBetween(n,w) > distanceBetween(si, w) then
6: goto line 14
7: **endif**
8: RoutesPacketConstruction=Check if the packet construction of the routes (Cp) is obtained of or not
if (RoutesPacketConstruction==true) **then**
9: Retrieve routes r that are partially constructed from Cp, and the least amount of time which is remaining for each packets m for r.
10: ExistingRoute= check if there is a previously allocated existing route to sink node
11: **if** ExistingRoute = true **then**
12: Inform the previous source node by sending a packet and then dismiss.
13: **endif**
14: eradicate k ϵ r from the Ns, then go to line 14.
15: **endif**
16: **for** the entire Nodes si ϵ C, **do**
17: Calculate total delay which is incremental as
incd = delayBetween (n, si) + delayBetween (si, w)
18: Calculate the expense of insertion as
costOfThePath (n, si) + costOfThePath (si, w)
19: If the expense of insertion is minimal, while the delay incd<m, then affix si to r.
20: Revise the residual time for individual packets i as ri = ri – delayBetween (n, si)
21: A construction packet is to be sent to si with payload r and dm = min ri
22: **endfor**
23: **if** (there is no candidate si) **then**
24: Send construction packet to w after choosing w as the next node.
25: Send the packets which are constructed along the routes that are vacant to individual si ϵ Ns.
26: **endif**
.**End**

The route matrix output of the Algorithm 1 is taken as an input of Algorithm 2. Algorithm 2 is the congestion-control routing algorithm, which is used in order to relocate the data packets from given potential source s to intended destination d by providing an optimized route. Initially for each source ‘s’ to destination ‘d’, we check

if there is any data to transfer. If the data demand exists then we acquire the evidence related to the transmission of the intermediate node. If the intermediate nodes are not involved in transmitting any information to other node representing sensor then we proceed to transfer the data, else we remove that particular sensor node and update the matrix.

ALGORITHM 2: Optimized Routing and Congestion Control Algorithm

Begin
Input: A catalog of R representing the routes from delay-controlled energy efficient algorithm.
Output: A catalog of routes R which are optimized after successful elimination of congestion

```
1: CostEfficientRouteMatrix = DCEERMD (G (V, E), n, Ns, Ds, t, w)
2  for each source s to destination d do
3:     if dataTransfer > 0 then.
4:         TransmissionOfIntermediateNode = Check whether the intermediate nodes are
           transmitting some data or not
5:                 if TransmissionOfIntermediateNode = true then
6:                     Wait until transmission is completed
7:                 end if
8:                 else
9:                     CongestedNode = Check at each intermediate node whether it con-
                       sist of packet equal to threshold or not
10:                        if CongestedNode = true then
11:                            Discard the intermediate node and update the CostEfficien-
                               tRouteMatrix
12:                        end if
13:                        else
12:                            Transfer the data successfully
13:                        end if
14:            end if
15: end for
.End
```

---

5 Performance Evaluation

With the intension to show the usefulness of the proposed model, we conducted various simulation-based experiments. We performed simulation for our proposed algorithm by using MATLAB, obtained the various results then compared it with TADR [8], MintRoute [7] and CCOR [27] which are propelled beneath the similar criteria. The sensor nodes are distributed in random manner over 300 × 300 ms field network in order to accomplish the multi-hop functionality. The highest communication radius is considered to be 40 m and the sink is positioned at (100 m, 100 m).

Table 2 Simulation parameters

Parameters	Value
Size of the network	300×300 m^2
Sink	(100, 100)
Number of nodes	50–400
Radius	40 m
Simulation time	200 s
Data packets	1024 bits
Size of the buffer	15 packets

Table 2 describes all the used network configurations for simulation. Roughly some of the simulation parameters are varied according to the requirement and are not constant all the time.

5.1 Parameters for Performance Evaluation

With an intention to estimate the performance of the network, three quantitative metrics are chosen by us. The three metrics are the following:

1. Loss Rate of Packet—The network transmission reliability is successfully reflected by the loss rate of the packets. PLR is the amount of packet which is obtained by the node representing sink to the packets in number transmitted by the source nodes.
2. Energy Consumption—Energy consumption reflects the efficient consumption of energy. Lower is the energy disbursed per packet, better is the energy efficiency. It is estimated by the overall amount of energy consumed divided by the overall packets in number obtained by the sink node.
3. Average of the routing hops—Since, the multi-path routing is used, hence the average of the routing hops plays a significant part in establishing the better response of the transmission.

With the purpose to inspect the performance and the ability of the proposed algorithm to eliminate congestion and save the consumption of energy, various situations are considered. The result of the packet loss by fluctuating the total number of nodes is described in Fig. 4. We have simulated our algorithm under various traffic loads and by fluctuating the nodes number in count from 50 to 400, effectively the amount of packet loss is estimated and is assessed with respect to the other algorithms. From Fig. 4, we can make an infer that our proposed algorithm outshines other algorithms such as MintRoute, TADR and CCOR. With the raise in the number of nodes in count, the percentage of packet loss increase but still less than the other three. One of the major reasons behind this is that TADR avoids the wireless channels collisions. It collects the packets then distributes the traffic of the data transfer within the net-

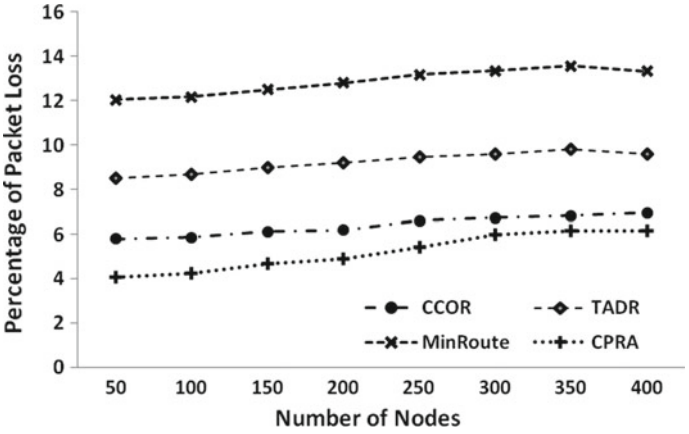


Fig. 4 Comparison of packet loss rate with varying number of nodes

work corresponding to the length of the queue field. MintRoute route the packets by making use of dropped packet at the local node, which results in droppage of various burst packets and hence increases the packet loss rate. CCOR performs better than TADR and MintRoute but still less than our proposed model as we determine the optimal route first then check the congestion in the network.

Our proposed algorithm makes use position of each node representing the sensor, deadline and the remaining time of the packets, hence lead to efficient utilization of the network resources by distributing the traffic over to the network. Figure 5 represents a graph of the total number of hops in average verses change in the count of nodes number. From Fig. 5, we can say that the number of hops in average of our proposed algorithm is almost similar to that of CCOR but lowest as assessed with respect to that of MintRoute and TADR.

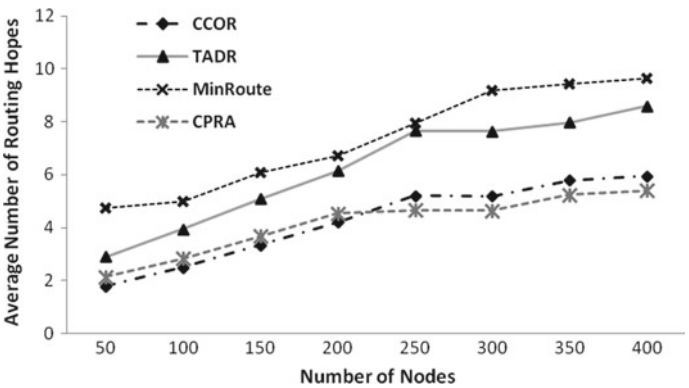


Fig. 5 Comparison of average number of routing hopes with varying number of nodes

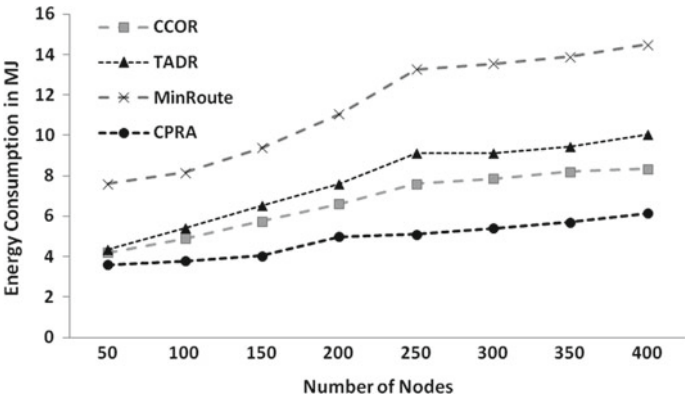


Fig. 6 Energy consumption with varying number of nodes

Consumption of energy percentage by differing the count of nodes in number is described in Fig. 6. The efficiency of energy of our proposed algorithm is a little better than that of CCOR, while much better than that of TADR and MintRoute. Since, MintRoute leads to more droppage of packets hence it cannot avoid congestion, so each sensor node consumes high volume of energy as compared to that of CCOR and TADR. Both CCOR and TADR dispense the traffic among the network. CCOR is subtler towards the congestion. Since it travels more hops hence consume more energy as compared to that of our proposed model. Since, our proposed algorithm chooses optimal route and more amount of data packets are productively being transported to the sink, hence it turns out to be valuable and conclusively accomplishes lower energy consumption by differing the number of nodes as compared to that of other three algorithms.

6 Conclusion

Due to rapid development in the sensor technology, WSN becomes popularized from the past two decades. Various rational amounts of works have been recognized in different areas of WSN and its improvements. As a consequence of its dynamic properties and increase in its applications, still, it draws researchers' attention to improve the quality of service. In this chapter, a multi-parameters-based resource allocation is contemplated in order to address all the challenges discussed above and design a comprehensive model for the resource provisioning. In order to accomplish the same, a multi-parameterized joint optimization model is proposed for WSNs, which in turn leads to congestion free, energy efficient, link quality and application latency aware resource allocation network model. An algorithm is defined in order to deal with the computation complexity of the proposed model. Various simulation-

based experiments are conducted in order to show the efficiency of the proposed model.

References

1. 21 ideas for the 21st century. *Business Week*, 30 August 1999 (pp. 78–167).
2. Chong, C.-Y., & Kumar, S. P. (2003, August). Sensor networks: Evolution, opportunities, and challenges. *Proceedings of the IEEE, 91*(8), 1247–1256.
3. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002, August). A survey on sensor networks. *IEEE Communications Magazine, 40*(8), 102–114.
4. Estrin, D., Culler, D., Pister, K., & Sukhatme, G. (2002, January). Connecting the physical world with pervasive networks. *IEEE Pervasive Computing*, 59–69.
5. Zawodniok, M., & Jagannathan, S. (2007). Predictive congestion control protocol for wireless sensor networks. *IEEE Transactions on Wireless Communications, 6*(11), 3955–3963.
6. Yaghmaee, M. H., & Adjeroh, D. A. (2009). Priority-based rate control for service differentiation and congestion control in wireless multimedia sensor networks. *Computer Networks, 53*(11), 1798–1811.
7. Heinzelman, W., Chandrakasan, A., & Balakrishna, H. (2000). Energy-efficient communication protocol for wireless microsensor networks. In *Proceedings of the 33rd International Conference on System Sciences*.
8. Kulkarni, P., Ganesan, D., & Shenoy, P. (2005). The case for multi-tier camera sensor networks. In *Proceedings of the 13th Annual ACM International Conference on Multimedia* (pp. 229–238).
9. Goldsmith, A. J., & Wicker, S. B. (2002, August). Design challenges for energy—Constrained ad hoc wireless networks. *IEEE Wireless Communications, 9*(4), 8–27.
10. Flora, J., & Kavitha, M. (2011). A survey on congestion control techniques in WSN. In *Proceedings of International Conference on Emerging Trends in Electrical and Computer Technology (ICETECT 2011)*.
11. Chen, D., & Varshney, P. K. (2004, June). QoS support in wireless sensor networks: A survey. In *Proceedings of the International Conference on Wireless Networks*, Las Vegas, USA.
12. Smaragdakis, G., Matta, I., Bestavros, A. (2004). SEP: A stable election protocol for clustered heterogeneous wireless sensor networks. In *Second International Workshop on Sensor and Actor Network Protocols and Applications (SANPA 2004)*.
13. Younis, O., & Fahmy, S. (2004). Heed: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. *IEEE Transactions on Mobile Computing, 3,* 366–379.
14. Yang, Y., Wu, H., & Zhuang, W. (2006). MESTER: Minimum energy spanning tree for efficient routing in wireless sensor networks. In *Proceedings of the 3rd International Conference on Quality*.
15. Wang, X., & Qian, H. (2011). Hierarchical and low-power IPv6 address configuration for wireless sensor networks. *International Journal of Communication Systems*. http://dx.doi.org/10.1002/dac.1318.
16. Wang, S., et al. (2015). Link-correlation-aware opportunistic routing in wireless networks. *IEEE Transactions on Wireless Communications, 14*(1), 47–56.
17. Bodas, S., Shakkottai, S., Ying, L., & Srikant, R. (2014, February). Scheduling in multichannel wireless networks: Rate function optimality in the small-buffer regime. *IEEE Transactions on Information Theory, 60*(2), 1101–1125.
18. Chowdhury, K. R., Nandiraju, N., Chanda, P., Agrawal, D. P., & Zeng, Q.-A. (2009, March). Channel allocation and medium access control for wireless sensor networks. *Ad Hoc Networks, 7*(2), 307–321.
19. Ahmed, S., Javaid, N., Yousaf, S., Ahmad, A., Sandhu, M. M., Imran, M., et al. (2015). Co-LAEEBA: Cooperative link aware and energy efficient protocol for wireless body area networks. *Computers in Human Behavior, 51*, 1205–1215.

20. Shaikh, F. K., & Zeadally, S. (2016). Energy harvesting in wireless sensor networks: A comprehensive review. *Renewable and Sustainable Energy Reviews, 55,* 1041–1054.
21. Lin, S., Miao, F., Zhang, J., Zhou, G., Gu, L., He, T., et al. (2016). ATPC: Adaptive transmission power control for wireless sensor net-works. *ACM Transactions on Sensor Networks (TOSN), 12*(1), 6.
22. Han, G., Liu, L., Jiang, J., Shu, L., & Hancke, G. (2017). Analysis of energy-efficient connected target coverage algorithms for industrial wireless sensor networks. *IEEE Transactions on Industrial Informatics, 13*(1), 135–143.
23. Cheng, L., Niu, J., Luo, C., Shu, L., Kong, L., Zhao, Z., et al. (2018). Towards minimum-delay and energy-efficient flooding in low-duty-cycle wireless sensor networks. *Computer Networks, 134,* 66–77.
24. Fong, S., Li, J., Song, W., Tian, Y., Wong, R. K., & Dey, N. (2018). Predicting unusual energy consumption events from smart home sensor network by data stream mining with misclassified recall. *Journal of Ambient Intelligence and Humanized Computing*, 1–25.
25. Mostafaei, H. (2019). Energy-efficient algorithm for reliable routing of wireless sensor networks. *IEEE Transactions on Industrial Electronics, 66*(7), 5567–5575.
26. Bouyssounouse, B., & Sifakis, J. (Eds.). (2005). *Embedded systems design: The ARTIST roadmap for research and development* (Vol. 3436). Lecture notes in computer science. Springer.
27. Ding, W., Tang, L., & Ji, S. (2016). Optimizing routing based on congestion control for wireless sensor networks. *Wireless Networks, 22*(3), 915–925.

Effect of Wormhole Attacks on MANET

Harsh Nath Jha, Samiran Gupta and Debabrata Maity

Abstract Mobile Ad hoc Network (MANET) is an infrastructure-less and self-organizing network of autonomous mobile nodes with wireless interfaces to construct a temporary wireless network using no dedicated routers, so the communication channels are freely accessible by the legitimate as well as the non-legitimate users. In MANET, each node operates as a router and transmits packets between source and destination while there is no assistance from the base station. Nodes within the transmission range of the source node accept the packet sent by the source and forward it along the route to the destination node. Due to the high mobility and dynamic nature, MANETs are more vulnerable to wormhole attacks, where the attacker may sniff the packets at one location and retransmit them to some other location inside or outside the network, resulting in the loss of throughput and bullying privacy. A wormhole attack is possible even if the communication channel provides authenticity and confidentiality, causing a serious security threat to wireless networks. Here, we are discussing the effects of wormhole attack on MANETs.

Keywords Mobile ad hoc network · Wormhole · AODV · Throughput · QoS · Attack · Smart node

H. N. Jha · D. Maity
Department of Information Technology, Asansol Engineering College, Asansol 713305, West Bengal, India
e-mail: ind.harshit@gmail.com

D. Maity
e-mail: debabrata2007@gmail.com

S. Gupta (✉)
Department of Computer Science and Engineering, Asansol Engineering College, Asansol 713305, West Bengal, India
e-mail: samiran.bappa@gmail.com

S. K. Das et al. (eds.), *Design Frameworks for Wireless Networks*,
Lecture Notes in Networks and Systems 82,
https://doi.org/10.1007/978-981-13-9574-1_8

1 Introduction

Mobile Ad hoc Network (MANET) [1–8] or ad hoc wireless network is a remotely hosted wireless network, where all the participating nodes are autonomous, i.e., self-hosting in nature, and do not need any dedicated router or server to host them. The individual devices connected in the network can communicate directly to each other as there is no role of any moderating hardware or a central access point, such as a gateway or a router. MANET nodes are mobile in nature; hence, there is no fixed topology in the network [9–11]. Each device plays the role of a router in the network as they themselves route the traffic to subsequent nodes in the network. This autonomous architecture of the network is highly helpful in designing remote communication channel in no time. However, this type of arrangement is fairly simple to configure, but at the same time, it is not a secure and reliable mode of communication.

From Fig. 1, we see that there are seven nodes participating in the channel and there is no intervention of any dedicated router, i.e., all the nodes are autonomously acting both as servers and nodes at subsequent steps. This small setup demonstrates the self-hosting nature of the nodes involved in communication to form a bigger communication channel. However, this highly dynamic topology in the channel is allied with the presence of one or more intermediate transceivers, between the individual nodes [12, 13].

Generally, this type of network arrangement is not popular with the end users who are much familiar with small- or medium-scale residential or business networks that are based on a conventional router-driven model.

Being peer-to-peer and rather hardware-less in nature, mobile ad hoc networks can prove extremely economical for small local area networks. As of now, MANETs

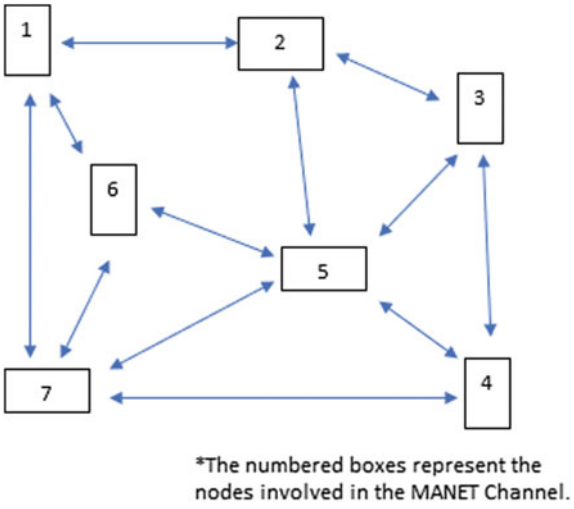


Fig. 1 Overview of MANET

cannot be implemented on a large scale, as a larger number of devices need a more concrete infrastructure.

This paper focuses on presenting a comprehensive and wholesome study of the mobile ad hoc networks with a perspective to have a thorough understanding about the characteristics of MANET (Sect. 3), its advantages and disadvantages (Sect. 3.1), and its working (Sect. 3.2).

MANETs face a big threat in the aspect of security, as it is extremely vulnerable to wormhole attacks. To mitigate this risk, we need a deep understanding of the subject. In this paper, we have presented the disadvantages of MANET in detail in Sect. 4. We have analyzed this major area of security issues in the context of different types and modes of attacks against MANET in this section.

Section 5 presents an overview of the working mechanism of wormhole attacks. Furthermore, types of modes and media of wormhole attacks have been discussed in Sects. 5.1 and 5.2. These kinds of attacks affect the channel performance in many ways, talked about in Sect. 5.3.

We have used NS-2 simulation environment to create a dummy MANET setup for demonstrating its vulnerabilities. The simulation environment configuration has been mentioned in Sect. 6. We have used the abovementioned setup to generate a wormhole attack on our dummy channel. The result obtained by this process is shown and described in Sect. 6.1.

Through our proposed work, we have tried to enlighten all the underlined risks involved in MANETs against wormhole attacks. This will facilitate us and other researchers to take an endeavor in this regard. Being able to fix these issues will help us to develop MANETs as a more reliable and secure communication environment.

2 Related Works

In this section, we are briefly visiting a few wormhole detection techniques as presented by different authors. Over the years, numerous researchers have analyzed wormhole attacks on MANETs and on the basis of their findings, proposed several defense mechanisms and Intrusion Detection System (IDS) to detect the attacks and thereby defend the network. Wormhole attack is a serious security threat to MANETs [14]. Yun et al. [15] proposed a GPS enabled detector node-based detection technique called WODEM. Genetic-based intrusion detection system for TCP/IP networks has been proposed by Yi et al. The research in [16] considered RREQ flooding attack. Kim et al. [17] designed a new artificial immune system for IDS which is based on a hierarchical approach inspired by the human immunity system. Hu et al. [18] introduced a wormhole detection technique with the help of temporal or geographical leash. Choi et al. [19] proposed an attack prevention algorithm called WAP (Wormhole Attack Prevention). Su [20] developed a technique called WARP (Wormhole Avoidance Routing Protocol) to avoid wormhole attack. Hayajneh et al. [21] proposed a newly developed protocol DeWorm that finds alternate routes to the destination so that if any node or group of nodes show malicious behavior then that particular route

is not used for any data transfer. Gupta et al. [22] developed a protocol named Wormhole Attack detection Protocol using Hound Packet (WHOP) by modifying AODV protocol for the purpose of wormhole detection. These are a few initiatives taken by different researchers in this field. However, we still do not have a full proof plan to tackle wormhole attacks with high precision. There is still a lot of scope for the implementation of methods to dodge these attacks against MANETs. Through our paper, we are magnifying the attack scenario, paving a foundation for further works in this regard for a much efficient shielding mechanism to be invented.

3 Characteristics of MANET

i. Dynamic topology: By default, the network topology is multi-hop in nature, but can randomly form unidirectional or bidirectional transmission spontaneously and randomly with time.
ii. Power supply constraint: All the nodes run mostly on batteries or similar source of energy, which is not a promising mode of power supply, hence the mobile nodes are characterized with lightweight features, less memory capacity, and power.
iii. Autonomity: The network is composed of individual devices which act as routers and host themselves.
iv. Low throughput: Due to intervention of factors like multiple access, interference condition, noise, etc., wireless networks are not as efficient as wired networks on the grounds of reliability, efficiency, and throughput.
v. High security threat: We already know that MANETs are infrastructure-less and involve no use of dedicated routers, hence a centralized firewall or host configuration is not available too, which leads to an increased risk of loss of throughput and Quality of Service (QoS) [23] and is surely a threat to any confidential data being circulated in the channel [24].
vi. Self-configuring: Ad hoc networks are self-organizing in nature and hence need minimum human intervention which again is an example of its dynamic and autonomous nature.

3.1 Ins and Outs of MANET

Mobile Ad hoc Networks have registered their popularity among its users at a large scale. It offers several benefits to its users, such as freedom from the requirement of a dedicated infrastructural setup and ease of configuration. It is more of a "plug and play" service. It has an equal number of drawbacks associated with it as well, which makes it risky to implement at a large scale. Here are some common advantages and disadvantages of MANETs.

Positive aspects:

i. No requirement of a central administration.
ii. Each node can act both as a router and a host, as required.
iii. Self-organizing nodes, independent of human intervention.

Negative aspects:

i. No centralized authorization scheme involved.
ii. Its infrastructure-less-ness causes serious security threats.
iii. Limited resources because of intercommunication interferences.

3.2 Working Principal of MANET

MANETs are based on numerous table-driven as well as table-less routing protocols. Ad hoc On-demand Distance Vector (AODV) protocol [25] is the most prominently used protocol for MANET setup. AODV algorithm allows mobile, dynamic, self-arranging, and multi-hop routing among participating nodes in the network channel which gives an upper hand in terms of route maintenance. The dynamic rerouting in AODV does not require the nodes to maintain routes with inactive nodes.

For instance, let us say there are 5 nodes in an MANET setup, named N1, N2, N3, N4, and N5, respectively. In a scenario where only nodes N1, N2, N3, and N4 are communicating and N5 is not exchanging any data, but still present in the network, N5 will still be allowed to be in the channel, but the working nodes will not be required to maintain a route with node "N5". Due to highly dynamic in nature, AODV implies real-time routing and reorientation of the routes in order to reduce the load on the channel.

The nodes are allowed to respond to the security breach and redesign the network topology periodically. As soon as an under-attack or affected node is reported, the system comes to know about the breach, and hence deauthorizes the malicious node(s) and stops them from all further transmissions.

AODV is mainly a table-driven protocol which strictly follows a REQUEST-REPLY setup to ensure end-to-end encryption. AODV uses Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) as message type definitions. For every transfer of packet between any two nodes, a route request is generated from the source toward the recipient node, for which in turn, the recipient replies with an acknowledgment of receiving the data. If the reply fails to reach the sender, then it assumes that the data has been lost or stolen and broadcasts an error message, thereby dropping any further transfers unless the issue is resolved.

AODV routing has two phases:

a. Route Discovery: Uses RREQ and RREP to discover new paths.
b. Route Maintenance: Uses RERR to convey any error, when found.

Every node has its own routing table in AODV protocol. This table contains route and hop-count information gathered through route discovery. Each participating node

has a specific table, containing information about the distance to a particular node. This distance is measured in hop-counts. The route table is composed of:

i. previous node,
ii. Hop-count,
iii. next Hop (i.e., next node),
iv. destination IP address, and
v. TTL (Time to Leave).

3.3 Commonly Used Terms in AODV Ecosystem

AODV utilizes standard meanings for CAPITALIZED words like MUST, SHOULD, etc., to note the priority level for different protocol features. Here, we have some other non-predefined terminology used in AODV:

a. Active route: A route having a valid routing table entry in the network. Only these nodes are authorized to forward data packets.
b. Broadcast: Transmitting data to 255.255.255.255 (the IP limited broadcast address) is called Broadcasting. It is useful to allow dissemination of data packets throughout the communication channel.
c. Destination: The target or recipient is known as the destination or the destination node. The destination node comes to know that it is the recipient when the IP header displays its address.
d. Forwarding node: It is an intermediate node that agrees to retransmit the data packets from a node to a subsequent hop location toward the unicast destination in the active route.
e. Invalid route: A route which has expired is termed as an invalid node. It is used for route repairs, storing previous valid route information and for future RREQ messages; however, it cannot be used to transmit data in the channel as it is an invalid state in the route table.
f. Originating node: Essentially the first node of the channel, i.e., the node from where the AODV route discovery (RREQ message) initiates and transmitted to other participants of the ad hoc network.
g. Reverse route: The route to return an acknowledgment (RREP message) to the originating node from the destination or forwarding node, confirming a successful transmission.
h. Sequence number: It is a strictly increasing counter variable which is maintained by each originating node. Other nodes use it to determine the freshness of the data packet(s) received in the channel.
i. Valid route: A route having a valid entry in the route table.

4 Problem Formulation

MANET, however, proves pretty handy if you want to set up a small-scale wireless LAN, but scaling up it faces some challenges in maintaining proper security as it is vulnerable to many types of attacks [26, 27], such as:

i. eavesdropping [28],
ii. Denial of Service (DoS) [29],
iii. jamming [30],
iv. black hole attack [31],
v. session hijacking [32], and
vi. wormhole attack [33], etc.

Against MANETs, wormhole attacks deal severe deterioration in the network's performance in terms of the following:

i. Quality of Service (QoS): It is the measure of the network's ability to attain maximum bandwidth and host other network performance elements like uptime, latency, and error rate [34]. In simple terms, higher the QoS, better the network performance.
ii. Throughput: The measure of units of information processed by a system per unit time is termed as throughput. It is also referred to as the measure of system productivity, as in the speed with which a specific workload can be successfully completed.
iii. Data rate: Data rate or data transfer rate denotes the transmission speed of data over a network, i.e., the number of bits of data transmitted per second. In data communication, data rate is generally expressed in bytes per second (B/s).
iv. Privacy: It is an aspect of communication that ensures that a particular data set is delivered to and accessed only by the intended recipients and not any unauthorized third-party body [35].

Here, in this paper, we are using AODV protocol to analyze, experiment, and explain the effects of wormhole attack on MANET by virtually simulating a dummy wormhole attack on a network with a number of nodes.

5 Wormhole Attack

Wormhole nodes create an illusion of having a shorter route within the network as compared to the original route [36]. This act confuses the routing mechanism by faking the shorter node which is not present in the route table. Due to the intervention of these malicious nodes in the network, the previous knowledge of node distances and hop-counts get overridden. As a result, the data packets get rerouted and start being transmitted through the new route as suggested by the attacking node, due to which the data packets have to pass through the attacking node, giving it an opportunity to gain access to them.

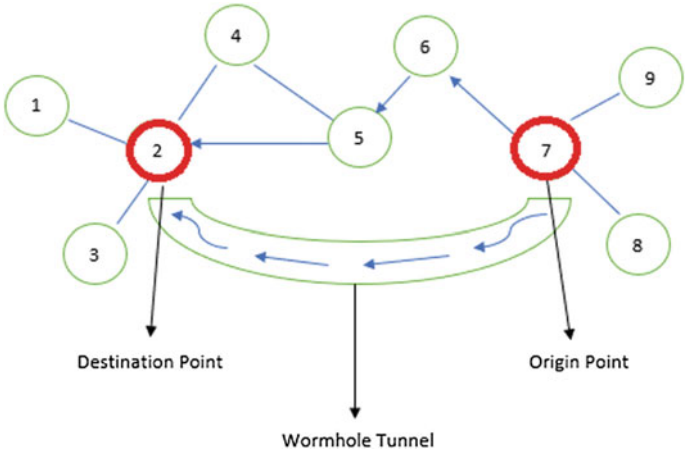


Fig. 2 Wormhole attack

The attacker may deploy multiple malicious nodes and also connect them through a tunnel. The attacking node starts recording the data packets passing through it and thereby getting a scope to drop the information toward another end of the wormhole.

MANETs are highly prone to this type of attack. The attack may be launched even without compromising any legitimate nodes or using any cryptography mechanisms because the attacker need not have a proper knowledge about the network to launch such attacks (Fig. 2).

A wormhole is created either by a two-ended wired link or a high-frequency link. The attacking node drains the data through this tunnel only, causing a serious threat to security and confidentiality of the data. As soon as an attack is detected, the network instantly suspends all communication until the service is ensured safe back online. This discontinuation of communication affects the throughput, data rate, and QoS of the communication channel.

5.1 Attack Medium

There are broadly two attack media in wormhole attacks on ad hoc networks, i.e., two basic topological arrangements as per which the malicious nodes work through an attack, namely:

i. In-band attack medium: This medium is characterized by the malicious nodes being connected through several other intermediate nodes in the channel. There exists a sub-channel from the attacker node to where it is tunneling the data. This sub-channel is necessarily a part of the fake route that the attacker node had manifested before (Fig. 3).

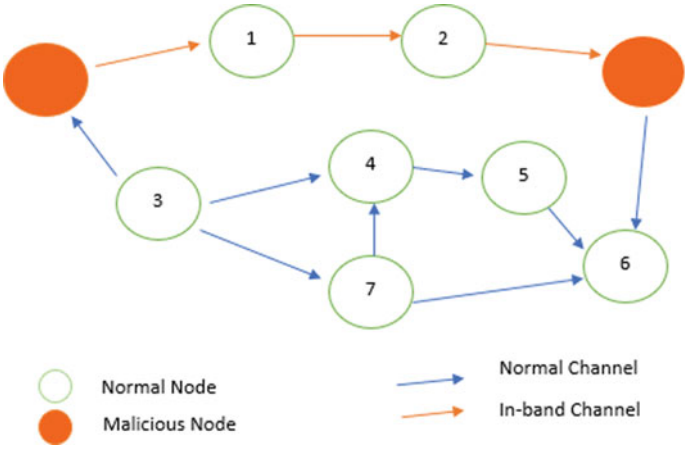


Fig. 3 Overview of in-band attack medium in wormhole attacks

ii. Out of the band medium: An out of the band medium attack is similar to in-band medium attack, except for the difference that the malicious nodes are not connected via any intermediate nodes, but directly to each other, hence the fake route contains no original nodes in the way (Fig. 4).

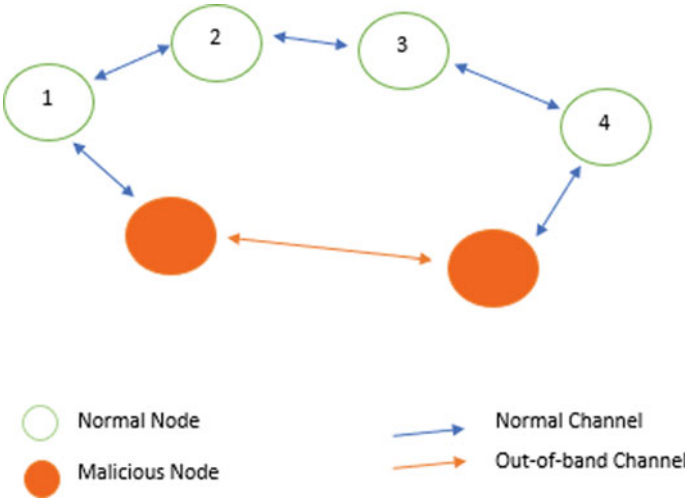


Fig. 4 Overview of out of the band attack medium in wormhole attacks

5.2 Attacking Modes

Wormhole attacks are performed in two modes, as follows:

1. Hidden Mode
    a. Packet Encapsulation: In this mode of attack, every data packet which is routed via the active route gets encapsulated on the wormhole end when received. This keeps the intermediate nodes from increasing hop-counts. The data packets are later brought to their actual state at the other end of the wormhole.
    b. Packet Relay: In this attack strategy, two malicious nodes relay the data packets between two distant but neighbor nodes to the malicious ones.
2. Participation Mode
    a. High Power transmission: In this mode of attack, it is essentially orchestrated by a single attacking node having a high transmission capability which can beat the route discovery mechanism and fake itself to be a shorter route and hence divert the traffic toward itself.
    b. Out-of-Band: This attacking mode involves a wormhole having two ends, also facilitated with a dedicated out-of-band nature channel with high bandwidth. This channel is located as a connection between the two ends of the wormhole.

5.3 Effects of the Attack

Wormhole attacks have a multi-faced damaging effect on MANET setups. These attacks, as discussed earlier, have a direct impact on the throughput, data rate, QoS, and privacy of the communication channel. Here are some effects of the attack on these networks, as follows:

i. selectively drops data package,
ii. disruption in routes,
iii. fear of leaking confidential data,
iv. manipulation of network traffic, and having attained the network data, the attacker may launch many other damaging attacks like protocol reverse engineering, cipher breaking, man-in-the-middle attack, etc.

We now present our findings on a virtually simulated wormhole attack, engaging a number of nodes under normal conditions, then under attack.

6 Simulation Environment

Over here, we are using Network Simulator (Ns-2) for presenting our proposed scenario, which is very popularly used by MANET community because it has a wide support for a number of routing protocols.

Ns-2 is an object-oriented simulator which runs in UNIX environment with the support of Object Tcl (OTcl) as frontend and C++ for backend. For our proposed simulation, the parameters are presented in Table 1.

We are presenting two test cases as follows.

In the first scenario, we simulate the network model under normal conditions (without any attack) and check the output as in terms of throughput.

In the next step, we launch a wormhole attack over the same network setup after a certain period of time. Here we observe that the throughput starts to fall immediately and after some interval, it reached zero.

Throughput: Throughput is the average quantity of data (in form of bits) received by the destination node in a unit of time within the network.

$$\textbf{Throughput} = \frac{\textbf{Number of bytes received} * \textbf{8}}{\textbf{Simulation time} * \textbf{1024}} \text{kbps} \tag{1}$$

Table 1 Simulation configuration details

Simulation parameter	Value/type
Simulation area	1000 m × 850 m
Channel type	Channel/Wireless channel
Interface type	Phy/WirelessPhy
Simulation time	1200 s
Mobility model	Random waypoint
Propagation model	Propagation/two-way ground
MAC type	Mac/802.11
Antenna model	Antenna/Omni antenna
Interface queue type	Queue/DropTail/PriQueue
Routing protocol	AODV
Link layer type	LL
Number of mobile nodes	15–30

6.1 Attack Simulation

- Case 1: Under normal circumstances

1. Initial random deployment of nodes (Fig. 5).

We deploy a number of nodes forming a self-arranging ad hoc network. In this network, the communication will take place which will be monitored to draw conclusions about the behavior and quality of the network under a normal scenario and then under attack too.

2. Data transfer between sender and receiver (Fig. 6).

We see a data transfer going on between nodes 0 (originating node) and 1 (destination node) via the intermediate node 2 (forwarding node) (Fig. 7).

Removing all the other nodes from the scene, we observe an expected behavior being shown by the channel. The data is being transmitted from node 0 to node 1 via node 2 without any loss.

3. Graphical representation of throughput under normal condition (Fig. 8).

From the scenario presented above, it is evident that we get maximum throughput under normal conditions (when the network is not under any wormhole attack) and

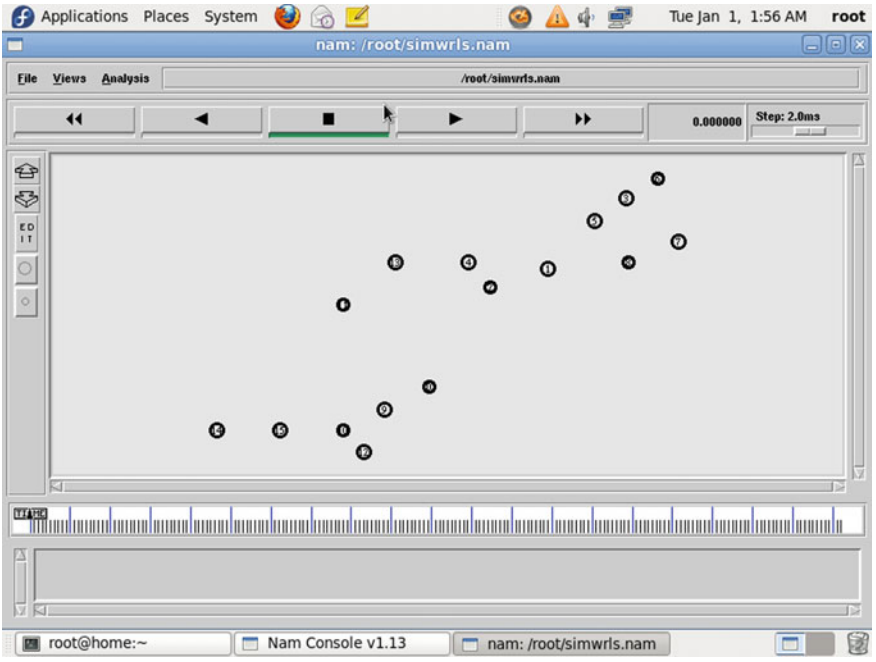


Fig. 5 Deploying nodes

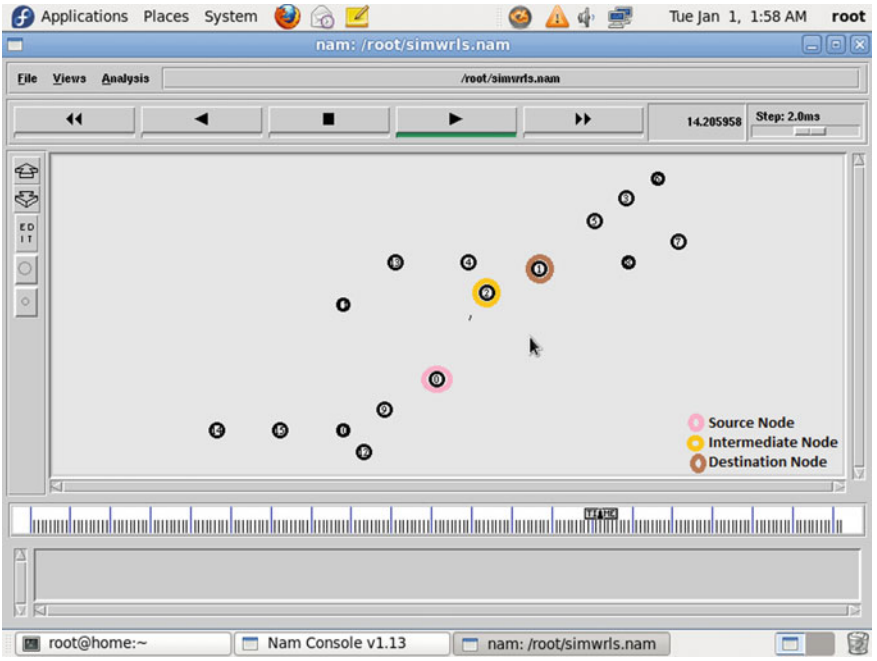


Fig. 6 Data transfer between nodes

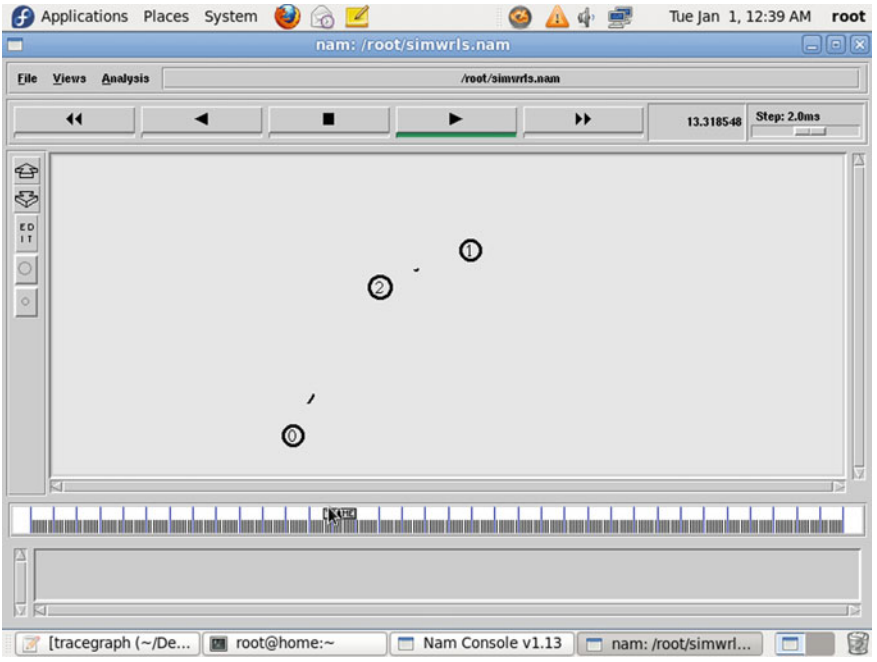


Fig. 7 Data transfer in action

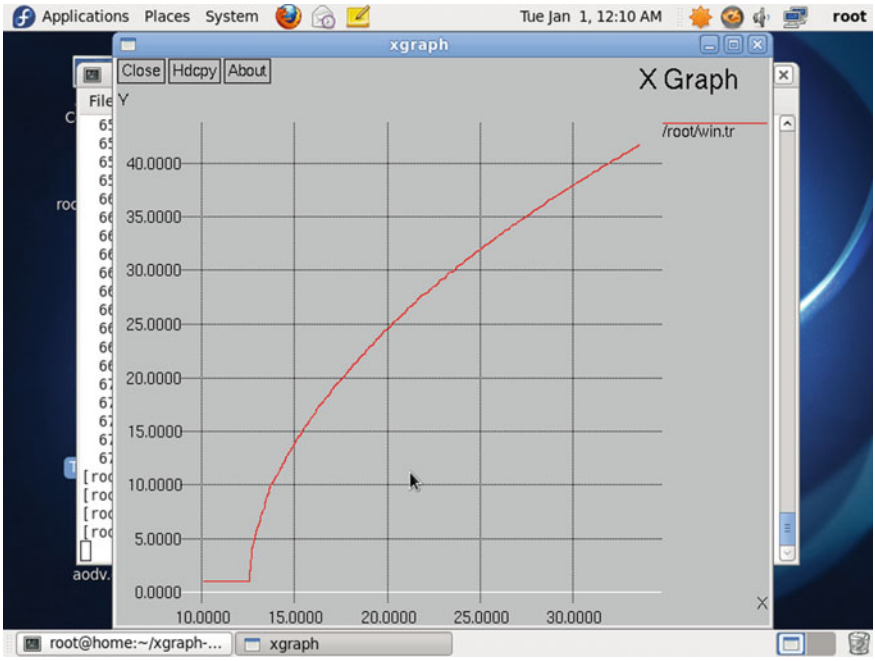


Fig. 8 Graphical representation of data transfer with respect to time

the graph shown above shows that we get a constant data flow from sender to receiver with respect to time (X-axis denotes time and Y-axis represents the flow of data). Hence, we conclude that an AODV-based MANET system gives a linearly increasing throughput with respect to time.

- Case 2: Under wormhole attack

1. Initial random deployment of nodes (Fig. 9).

Similar to our first case (when the system was not under any sort of attack), even in this case we deploy a number of nodes to take part in the communication channel. Even in this case, node 0 is the originating node, and node 1 is the intended recipient. This time, node 2 will act as a malicious node and attempt to drain the data that passes through it.

2. The attacker starts dropping data (Fig. 10).

We observe from that the attacking node has started dropping data off to some other location. Also to note that while node 2 is dropping data, due to its table-driven nature, the channel drops further data supply too. That is, as soon as node 2 starts draining data, node 0 stops sending data (Fig. 11).

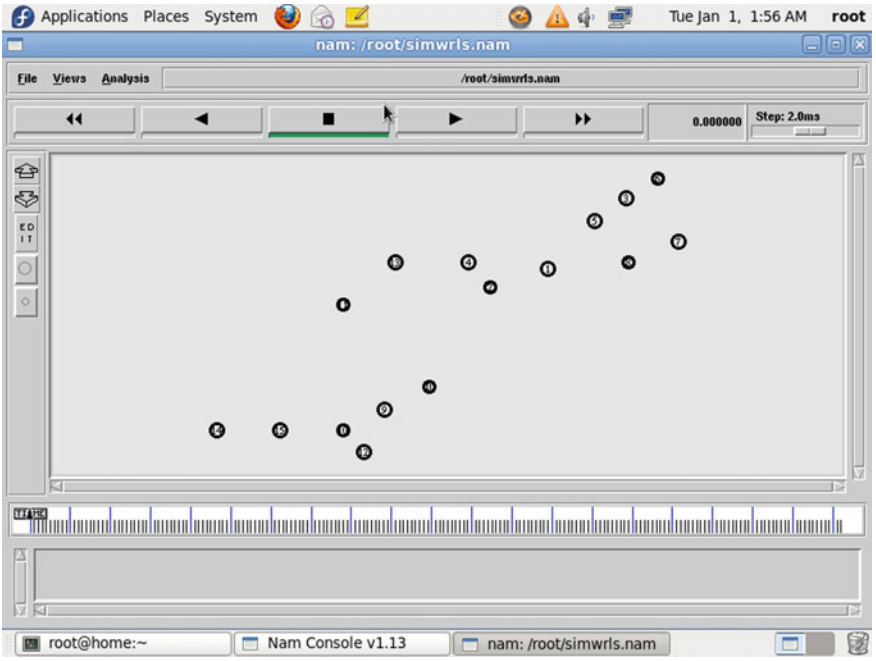


Fig. 9 Deployment of nodes

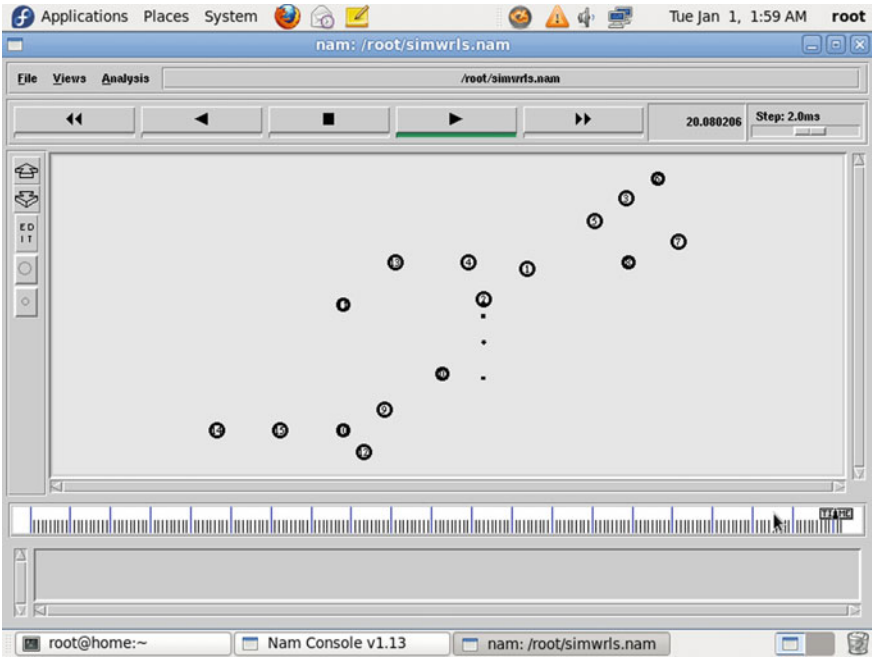


Fig. 10 Attack scenario

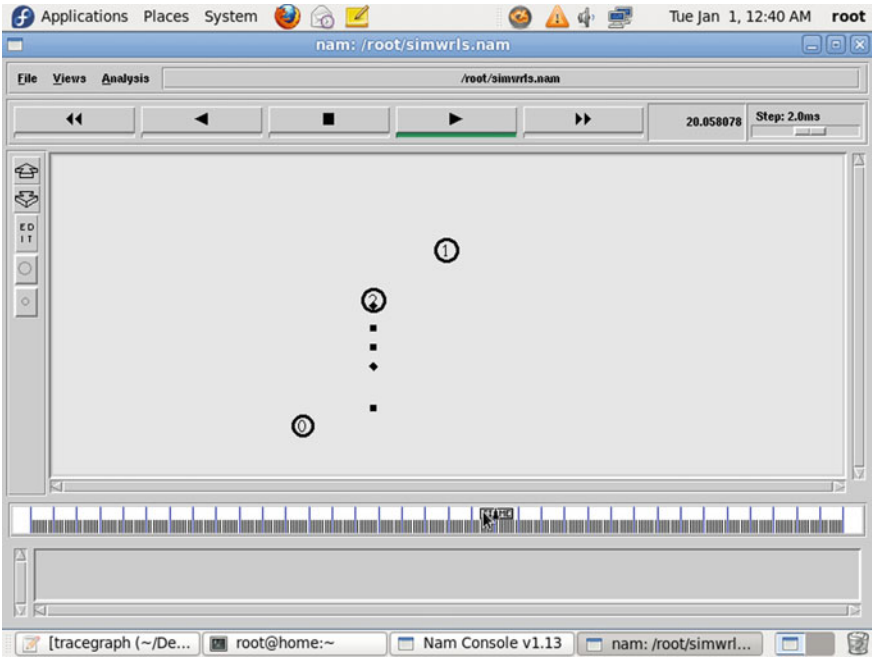


Fig. 11 Data draining in action

A continuous data drain by our malicious node can be seen from the above image. We also observe no data transfer from the sender, which means zero data rate and decreased throughput.

3. Graphical representation of throughput under attack (Fig. 12).

This graph shows the throughput of the channel with respect to time (X-axis denotes time and Y-axis represents flow of data). In the first half of the graph, a linear progression can be seen, which represents a steady-state communication before the network was attacked. As soon as we simulated a wormhole attack over the network channel, the throughput and data rate started to tend toward zero which clearly shows a loss in the overall throughput of the channel.

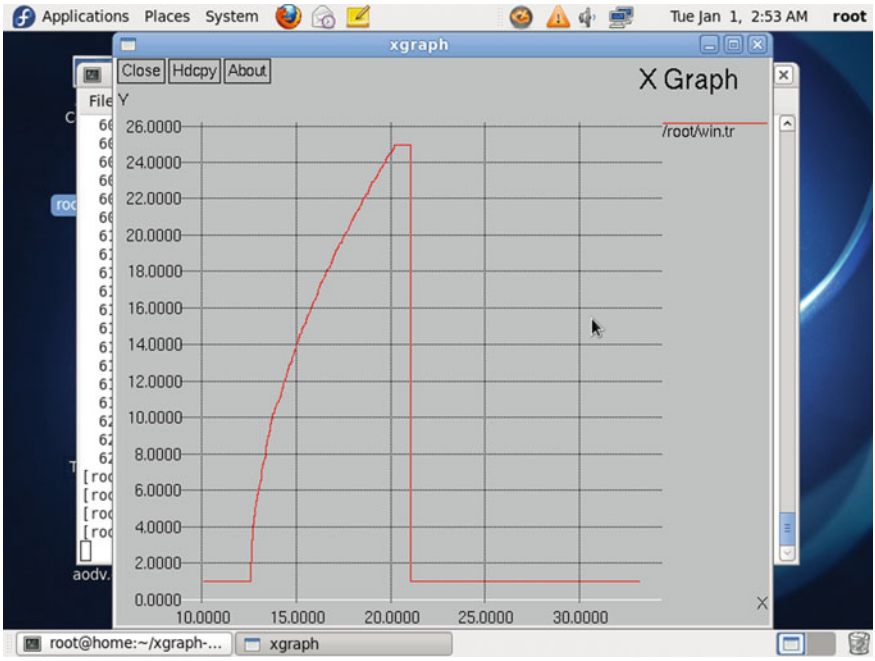


Fig. 12 Graphical representation of data transfer under attack

7 Conclusion

In this paper, we have presented a study on the effects of wormhole attacks on MANETs under AODV protocol using Ns-2 simulator. We observe that MANETs characteristically have a linear throughput trend under normal condition but the throughput is drastically degraded when under a wormhole attack.

Apart from throughput, wormhole attacks also affect other parameters of the network, like data rate and QoS. When we launched a wormhole attack against our network, we were able to see no data transfer; hence, we obtained a flat graph, dragging at zero mark, which indicates no data transfer whatsoever.

From this study, it is arguably clear that wormhole attack is a great threat to mobile ad hoc networks. This situation may prove even more damaging in real-life scenarios. Wormhole attacks not only compromise with the productivity of the network but also threaten privacy and integrity of data; hence, any confidential data is prone to this type of invasion. A wormhole attack is also difficult to detect, making it even more lethal. However, there are a number of techniques and mechanisms to beat wormhole attacks, but a more efficient approach toward implementing an MANET network immune to wormhole attacks is possible in future endeavors.

Acknowledgements The authors extend their gratitude and thanks to the Department of Information Technology and the Department of Computer Science and Engineering, Asansol Engineering

College, West Bengal, India for providing the necessary infrastructure for this study. We also thank everyone who motivated us to come up with this paper and those who helped us in proofreading and literature review.

References

1. Aarti, D. S. (2013). Tyagi, "Study of MANET: Characteristics, challenges, application and security attacks". *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(5), 252–257.
2. Das, S. K., Yadav, A. K., & Tripathi, S. (2017). IE2M: Design of intellectual energy efficient multicast routing protocol for ad-hoc network. *Peer-to-Peer Networking and Applications, 10*(3), 670–687. https://doi.org/10.1007/s12083-016-0532-6.
3. Gupta, S., & Das, B. (2013). An energy efficient and load aware routing scheme in multi sink wireless sensor networks. *International Journal of Engineering Research and Development, 6*(11), 31–35.
4. Gupta, S., & Das, B. (2013). Load based reliable routing in multi-sink sensor networks. *International Journal of Engineering and Science, 2*(12), 59–64.
5. Yadav, A. K., Das, S. K., & Tripathi, S. (2017). EFMMRP: Design of efficient fuzzy based multi-constraint multicast routing protocol for wireless ad-hoc network. *Computer Networks, 118,* 15–23.
6. Binh, H. T. T., & Dey, N. (Eds.). (2018). *Soft computing in wireless sensor networks*. CRC Press.
7. Chowdhuri, S., Chaudhuri, S. S., Banerjee, P., Dey, N., Mandal, A., & Santhil, V. (2016). Secure minimum loss route selection of MIMO-based MANET in combined (indoor, outdoor, and forest) terrain. Working paper. *International Journal Advanced Intelligence Paradigms*, 1–26.
8. Das, S. K., & Tripathi, S. (2019). Energy efficient routing formation algorithm for hybrid ad-hoc network: A geometric programming approach. *Peer-to-Peer Networking and Applications, Springer, 12*(1), 102–128. https://doi.org/10.1007/s12083-018-0643-3.
9. Ali, H., Shahzad, W., & Khan, F. A. (2012). Energy-efficient clustering in mobile ad-hoc networks using multi-objective particle swarm optimization. *Applied Soft Computing, 12*(7), 1913–1928.
10. Das, S. K., & Tripathi, S. (2018). Adaptive and intelligent energy efficient routing for transparent heterogeneous ad-hoc network by fusion of game theory and linear programming. *Applied Intelligence, 48*(7), 1825–1845. https://doi.org/10.1007/s10489-017-1061-6.
11. Das, S. K., & Tripathi, S. (2017). Energy efficient routing formation technique for hybrid ad hoc network using fusion of artificial intelligence techniques. *International Journal of Communication Systems, 30*(16). https://doi.org/10.1002/dac.3340.
12. Cho, J.-H., Chen, R., & Chan, K. S. (2016). Trust threshold based public key management in mobile ad hoc networks. *Ad Hoc Networks, 44,* 58–75.
13. Das, S. K., & Tripathi, S. (2018). Intelligent energy-aware efficient routing for MANET. *Wireless Networks* (Springer)*, 24*(4), 1139–1159. https://doi.org/10.1007/s11276-016-1388-7.
14. Nagrath, P., & Gupta, B. (2011, April). Wormhole attacks in wireless adhoc networks and their counter measurements: A survey. In *2011 3rd International Conference on Electronics Computer Technology* (Vol. 6, pp. 245–250). IEEE.
15. Yun, J., Kim, I., Lim, J., & Seo, S. (2007). WODEM: Wormhole attack defence mechanism in wireless sensor networks. In *ICUCT 2006*, LNCS (Vol. 4412, pp. 200–209).
16. Yi, P., Dai, Z., & Zhang, S. (2005). Resisting flooding attack in ad hoc networks. In *Proceeding of IEEE Conference on Information Technology: Coding and Computing* (Vol. 2, pp. 657–662).

17. Kim, J., & Bentley, P. (1999, September). The artificial immune model for network intrusion detection. In *7th European Congress on Intelligent Techniques and Soft Computing (EUFIT'99)* (Vol. 158, pp. 1–7).
18. Hu, L., & Evans, D. (2004, February). Using directional antennas to prevent wormhole attacks. In *NDSS* (Vol. 4, pp. 241–245).
19. Choi, S., Kim, D., Lee, D., & Jung, J. (2008, June). WAP: Wormhole attack prevention algorithm in mobile ad hoc networks. In *Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC 2008)* (pp. 343–348).
20. Su, M. Y. (2010). WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks. *Computers & Security, 29*(2), 208–224.
21. Hayajneh, T., Krishnamurthy, P., & Tipper, D. (2009, October). Deworm: A simple protocol to detect wormhole attacks in wireless ad hoc networks. In *2009 Third International Conference on Network and System Security* (pp. 73–80). IEEE.
22. Gupta, S., Kar, S., & Dharmaraja, S. (2011, April 25–27) WHOP: Wormhole attack detection protocol using hound packet. In *International Conference on Innovations in Information Technology (IIT)* (pp. 226–231).
23. Castellanos, W. E., Guerri, J. C., & Arce, P. (2016). A QoS-aware routing protocol with adaptive feedback scheme for video streaming for mobile networks. *Computer Communications, 77,* 10–25.
24. Yang, H., Luo, H., Ye, F., Lu, S. W., & Zhang, L. (2004). Security in mobile ad hoc networks: Challenges and solutions. *IEEE Wireless Communications, 11*(1), 38–47.
25. Perkins, C. E., & Royer, E. M. (1999). Ad-hoc on-demand distance vector routing. In *Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications* (pp. 90–100).
26. Sheikh, R., Chande, M. S., & Mishra, D. K. (2010, September). Security issues in MANET: A review. In *2010 Seventh International Conference on Wireless and Optical Communications Networks-(WOCN)* (pp. 1–4). IEEE.
27. Goyal, P., Parmar, V., & Rishi, R. (2011). MANET: Vulnerabilities, challenges, attacks, application. *IJCEM International Journal of Computational Engineering & Management, 11*(2011), 32–37.
28. Dai, H. N., Wang, Q., Li, D., & Wong, R. C. W. (2013). On eavesdropping attacks in wireless sensor networks with directional antennas. *International Journal of Distributed Sensor Networks, 9*(8), 760–834.
29. Jhaveri, R. H., Patel, S. J., & Jinwala, D. C. (2012). DoS attacks in mobile ad hoc networks: A survey. In *2nd International Conference on Advance Computing & Communication Technologies* (pp. 535–541).
30. Xu, W., Trappe, W., Zhang, Y., & Wood, T. (2005). The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing* (pp. 46–57).
31. John, N. P., & Thomas, A. (2012). Prevention and detection of black hole attack in AODV based mobile ad-hoc networks—A review. *International Journal of Scientific and Research Publications, 2*(9), 1–6.
32. Lupu, T.-G., Rudas, I., Demiralp, M., & Mastorakis, N. (2009). Main types of attacks in Wireless sensor networks. In *WSEAS International Conference. Proceedings. Recent Advances in Computer Engineering* (pp. 1–6).
33. Maheshwari, R., Gao, J., & Das, S. R. (2007). Detecting wormhole attacks in wireless networks using connectivity information. In *IEEE INFOCOM 2007—26th IEEE International Conference on Computer Communications* (pp. 107–115).
34. Basarkod, P. I., & Manvi, S. S. (2015). Mobility and QoS aware anycast routing in mobile ad hoc networks. *Computers & Electrical Engineering, 48,* 86–99.
35. Ning, P., & Sun, K. (2005). How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols. *Ad Hoc Networks, 3*(6), 795–819.
36. Sarkar, D., Choudhury, S., & Majumder, A. (2018). Enhanced-Ant-AODV for optimal route selection in mobile ad-hoc network. *Journal of King Saud University—Computer and Information Sciences*, 1–25. https://doi.org/10.1016/j.jksuci.2018.08.013.

Distributed Online Fault Diagnosis in Wireless Sensor Networks

Meenakshi Panda, Bhabani S. Gouda and Trilochan Panigrahi

Abstract In recent past, wireless sensor networks (WSNs) are used in various real-life applications where the nodes are randomly deployed in hostile environments. Different faults of sensors are inevitable due to adverse environmental conditions, low battery, and aging effect. Therefore, one major research focus in WSNs is to diagnose the sensor nodes regularly and to get the status of each of them. This helps to provide continuous service of the network despite the occurrence of failure of few nodes in the network. Some of the burning issues related to distributed fault diagnosis of intermittent faulty sensor in WSNs is addressed in this chapter. Further, how the performance of the fault diagnosis algorithm has been improved by employing robust statistical methods presented. The issue of intermittent fault diagnosis in WSNs is discussed using statistical methods which is the main focus of this chapter.

Keywords Wireless sensor networks (WSNs) · Hard and soft fault · Intermittent fault · Fault detection · Distributed self fault diagnosis

1 Introduction

Wireless sensor networks (WSNs) have gained worldwide scientific interest due to their ease of deployment and wide range of applications starting from terrestrial application to underground water application [1–3]. WSNs are equipped with tiny, inexpensive, intelligent sensor nodes. A sensor node includes one or more sensors, processors, memory, power supply, radio, and an actuator where each module per-

M. Panda · T. Panigrahi
National Institute of Technology Goa, Farmagudi, India
e-mail: meenakshi.nitrkl@gmail.com

T. Panigrahi
e-mail: tpanigrahi80@gmail.com

B. S. Gouda (✉)
National Institute of Science and Technology, Brahmapur, Odisha, India
e-mail: bhabani012@gmail.com

S. K. Das et al. (eds.), *Design Frameworks for Wireless Networks*,
Lecture Notes in Networks and Systems 82,
https://doi.org/10.1007/978-981-13-9574-1_9

forms different tasks [4]. WSN is a infrastructureless network and running with resource constraints such as limited battery power, short communication range, low bandwidth, and limited processing and storage in each sensor node. WSNs are worldwide famous network due to the services such as remote environmental monitoring, clock/time synchronization, sensor localization, routing, target tracking, event detection, security, clustering, event boundary detection, topology control, target localization, etc. supported by it.

A sensor node may equipped with various types of sensors such as mechanical, thermal, biological, chemical, optical, and magnetic sensors based on the application area on which sensor nodes are deployed [4, 5]. In fact, we are expecting sensor nodes should operate autonomously, robust and adaptive to the change in environment as sensor nodes are deployed in unattended and hostile environments. But the sensors are prone to have faults due to many reasons. The behavior of sensor network is suspicious because of the disorder in the mechanical or electrical problems in internal circuits inside the sensor node, battery depletion, hostile tampering, etc. Some times due to environmental degradation, the nodes are unable to perform as a normal node. Aging is another problem for arbitrary behavior of sensor node during operation [6].

Sometimes the sensor nodes are inactive in the network. It occurs when the transceiver module becomes faulty or the battery is completely drained, then such fault is known as hard fault [7, 8]. Whereas in some cases the behavior of the sensor is random. That kind of fault is termed as soft fault. But in real time, the faults manifest themselves as intermittent [9], i.e., the faulty sensor node generates faulty and fault-free reading at different time instants arbitrarily [10]. Intermittent fault may occur in the sensor node due to loose battery contacts, overheating of ICs, a noisy measurement from the sensors, and so forth. In fact, the intermittent fault is specified as a processor fault in literature, but it also occurs in sensor nodes in WSNs. Therefore, intermittent fault diagnosis in WSNs is required that too in distributed manner.

The fault diagnosis schemes used for WSNs are available in the literature do not address the dynamic faults, and therefore those methods cannot be used directly for the diagnosis of intermittent fault [7, 11–13]. But some authors have proposed how the existing diagnosis approaches can be extended to diagnose intermittent failures [14]. The ideas for intermittent fault diagnosis diagnose fault due to multiple causes, the diagnostic procedure is incremental and exploiting the iterative nature of diagnosis. These ideas are incorporated to diagnose the intermittent fault in WSNs.

In literature, authors have used statistical methods to find the soft or data faults in sensor network [15]. Intermittent faults of sensors have been diagnosed by different methods where the number of faults in a specified period calculated, but not distributed in nature [16, 17]. Whereas distributed approach in WSNs is always preferred over the centralized to make the network energy efficient as the former required less communication overhead. In fact, distributed algorithms are adaptive to the change in real time. Therefore, distributed intermittent fault diagnosis in sensor network is the main objective here. The performances such as diagnosis accuracy, false alarm rate, confidence interval, etc. of the fault diagnosis algorithms are evaluated and compared after implementing in NS3.

Finally, the chapter is organized as follows. The details about faults, error, and failure in WSNs are given in Sect. 2. The work done for the diagnosis of sensor nodes particularly for intermittent fault is given in Sect. 3. The system model is developed for the distributed fault diagnosis algorithm in Sect. 4. Data model with problem formulation is described in Sect. 5. Analysis of the robust distributed intermittent fault diagnosis algorithms is given in Sect. 7. Performance of all the algorithms for different parameters is compared after implementing in NS3 network simulator in Sect. 8. In Sect. 9, the chapter is concluded.

2 Faults, Errors, and Failures in Sensor Networks

The failure, fault, and error are the three related terms where error causes fault and fault causes failure. A failure means a discrepancy between the observed and expected sensor node states or behaviors. These unexpected behaviors of the sensor node are popularly known as sensor fault. The root cause of sensor fault is system disorder which occurs due to the mechanical or electrical problems in internal circuits available inside the sensor node, environmental degradation, battery depletion, hostile tampering, etc. When the sensor fault affects a sensor node it produces an erroneous result. The presence of a fault does not ensure that an error will occur. But the presence of erroneous data will ensure the sensor fault [18]. When the errors make a sensor node unable to perform its routine task, it results in a failure. So, sensor error is a subset of sensor fault and sensor fault is a subset of sensor failure. This relation is exemplified in Fig. 1.

The sensor fault can be modeled at different levels of abstraction. It can range from hardware or software level to system level or node level. Failures at hardware or software levels may result as errors at the system level and make the sensor node to behave abnormally. Generally, the hardware or software level of fault modeling is most generic, but the system level of fault modeling is easier to analyze as they consider the behavior of the faults [19]. Sensor faults are classified into various categories based on the failed components behavior, fault persistence, or the underlying

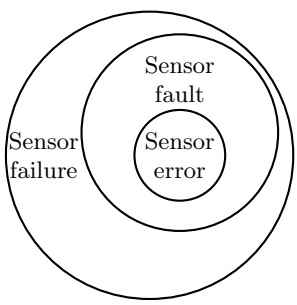


Fig. 1 A relationship between sensor error, fault, and failure

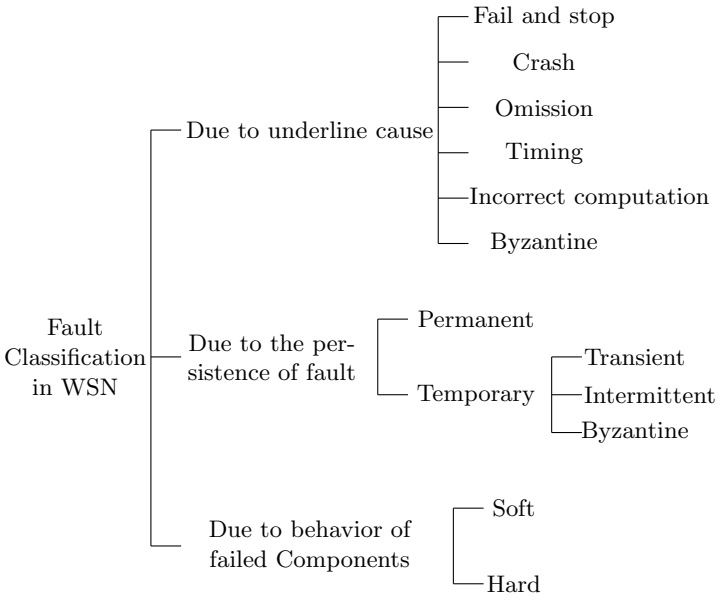


Fig. 2 Fault classification in WSN

cause [20, 21]. Based on the behavior of failed components, the faults can be hard and soft types.

A sensor suffering with hard faults is unable to communicate with neighbors whereas a soft faulty sensor can participate in normal operation of the network with altered behaviors. Based on persistence of fault, the sensor faults can be classified into three categories, namely, permanent, intermittent, and transient fault. Permanent or hard faults will remain silent throughout the life span of the network [22]. Temporary faults can participate in network operation and can be partitioned into external (transient) and internal (intermittent) faults. Faults are classified into many ways such as crash, omission, timing, incorrect computation, fail-stop fault, and Byzantine [22]. Crash faults may be considered as hard faults, whereas others are soft faults. The detailed description about the fault classification is summarized in Fig. 2.

3 Related Work

An overview of the work done in the area of fault diagnosis with special attention to intermittent fault is briefly introduced. The proposed methods, its advantage and disadvantages are discussed. If you look at the literature in early days, fault diagnosis of system and software is available. Detection of faults in digital circuits is given in [23] where the concept of a fault pattern for characterizing an intermittent fault is

presented. In [9], a notion of diagnosability for discrete event of a failed systems is explained. It follows a diagnosis procedure to be repeated in discrete event systems [14, 24]. However, these approaches are mainly used for the diagnosis of either a system or software. These methods may not be feasible to apply to diagnose the nodes in WSNs as sensors are suffering from battery constraint, low processing power, limited bandwidth, and low memory, whereas the algorithms developed for multiprocessor and wired computer networks need more energy.

Probabilistic-based fault diagnosis approach based on the remaining energy of the sensor node in WSNs is presented in [25]. Each sensor node exchanges message related to their remaining energy. For this, an extra message is exchanged over the network between the sensor nodes, which consumes energy.

Lee et al. in [16] have presented a comparison and time redundancy matrix based fault diagnosis approach. The method diagnoses both intermittent and transient fault by comparing its own sensed reading with its neighboring sensor nodes data for r consecutive rounds. Two threshold values are used: one threshold to find sensors partial fault status for each test interval and another is to find the minimum times the node should declare to be faulty, so that, its final decision to be faulty. This approach may not give good accuracy for a constant threshold. An optimal and adaptive threshold may be designed for better performance of the algorithm. Choi et al. [26] proposed an adaptive fault detection algorithm to identify the transient and intermittently faulty sensors over the static network which closely follows [16].

For the diagnosis of the intermittent faults in WSNs, time redundancy method is proposed in [27]. It is assumed that every node has minimum of three neighboring nodes. This may not be always guaranteed for strongly sparse sensor networks. For diagnosis the intermittently faulty sensor nodes, a binary tree over the entire network is constructed. This method is a semi-centralized approach and puts a communication overhead which reduces network lifetime.

Swarm algorithms are used to find the optimum parameters to diagnose the sensor network. Multi-objective particle swarm optimization (MOPSO) algorithm is used to select parameters for intermittent fault detection and then by using optimized parameters and comparison model detect the fault [17]. Evolutionary algorithms are not computationally efficient.

Sahoo et al. [28] proposed a hierarchical neighbor coordination based fault diagnosis algorithm which uses comparison, building, and dissemination phases. In comparison phase, sensor node collects the neighbor's data and residual energy and compare it with a predefined threshold (application dependent) to decide probable fault status (either 0 or 1) which is stored in neighboring table. As malicious nodes show abnormal energy consumption, this approach uses residual energy comparison as a parameter to strengthen the diagnosis process. The malicious nodes occur due to denial-of-service (DoS) attacks. The procedure is repeated and finally diffuse all the results and then compare it with a predefined threshold value in order to decide the fault status. In building phase, a spanning tree is constructed and sends the computed status through this tree to the central node in dissemination phase to visualize the global view of the network.

Clustering-based intermittent fault diagnosis approach is proposed by Swain et al. [29] in which analysis of variance method is used for identifying the status of the faulty sensor. This method is applied over the collected data at the cluster head and as a result it becomes suitable for both sparse and dense network.

Regressional learning based fault tolerance technique is a method where hard, soft, intermittent, and transient faults are identified [30]. To identify the hard fault, the neighbor coordination based time out concept is used. Neighbor majority voting method is applied to detect the permanent soft, intermittent, and transient faults. Then, regressional learning method is used to calculate how much time a faulty sensor persists in the network. This method is neither self-diagnosis nor distributed in nature.

The major disadvantages of present methods for intermittent fault diagnosis are the optimum threshold selection. The challenge in diagnosing the system accurately by using comparison model when both testing and tested sensors are faulty. To overcome this situation, in this chapter, a robust statistical based self-intermittent fault diagnosis protocol is established. This method is capable to generate an optimum threshold for testing the intermittently faulty sensor node which enhances the detection accuracy.

4 System Model

Detailed description about the network and fault model is given here. In network model, the topology of the sensor network algorithm with how the sensors are communicating with each other is described. Whereas, in fault model, the behavior of the sensors on the occurrence of different kinds of faults such as intermittent fault is presented.

4.1 Assumptions, Notations, and Their Meanings

The following assumptions are used for the development of distributed self fault diagnosis algorithm to diagnose faults of sensors in WSNs. These are as follows [15]:

1. Sensors are homogeneous in nature having uniform energy (i.e., uniform battery power) and transmission range.
2. In sensor network, sensors are able to send and receive the node Id and sensed data from their neighbors.
3. If a sensor fails to communicate with neighbors, referred as hard fault.
4. Network is static, i.e., the position of sensor nodes and the network topology remains same during the diagnosis period.
5. Links are symmetric in nature.
6. The links are fault free and the error is taken care by the MAC layer.

Table 1 Notations with description

Symbol	Description
S	Set of sensors in sensor network
C	Set of communication links
s_i	A sensor deployed at $P_i(xc_i, yc_i)$
N	Number of sensors deployed in the given terrine $R \times R$
NT_i	A table contains all information about its neighbors and itself known as Neighboring table of s_i
$Neg_i(n)$	A set of all the neighboring sensors of s_i at time instant n
$x_i(n)$	Modified sensed data of s_i at the time instant n
A	Actual sensed data of s_i
$v_i(n)$	Erroneous data sensed by s_i due to sensor circuit failure
$fs_i(n)$	Fault status of s_i at the time instant n
$FS_i(T)$	Fault status of s_i calculated by s_i after the time duration T
T_r	Transmission range of sensor nodes
$Nx_i(n)$	Set of neighbors data collected by s_i at the time instant n
S_G	A set of fault-free nodes
S_F	A set of faulty nodes
S_1	A set of hard faulty nodes
S_2	A set of intermittent faulty nodes
α	Probability that a sensor node s_i is suffering with intermittent fault
ζ	Minimum battery power at which a sensor node fails to work normally
T	Total observe time to diagnose the intermittent faulty sensor node
Δ_T	The time duration after which another test will be done to study the intermittent behavior of s_i
$MADi(n)$	Median absolute deviation over $Nx_i(n)$ at s_i
$MADN_i(n)$	Normalized median absolute deviation over $Nx_i(n)$ at s_i
N_a	Average degree of the network
N_i	Degree of s_i
p	A sensor's fault probability

7. All sensors periodically sense own data and accumulate data from the neighbors.
8. Sensors communicate by using UDP/IP communication protocol.

The notations used for developing and analyzing the distributed fault diagnosis algorithm are given in Table 1.

4.2 Network Model

Let N number of sensors are randomly deployed in a terrine of $R \times R$. Consider each sensor node s_i, $1 \leq i \leq N$ has known unique identifier (IP address) and position $P_i(xc_i, yc_i)$, where $0 \leq xc_i \leq R$, $0 \leq yc_i \leq R$ and has unique identifier (IP

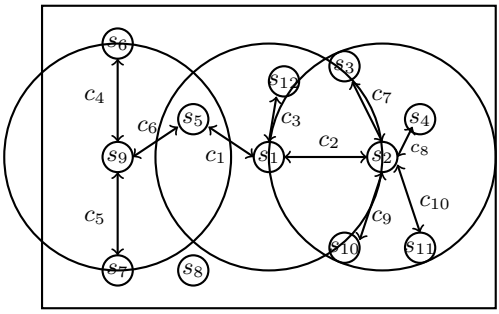


Fig. 3 Arbitrary network topology having $|S| = 12$ and $|C|=10$

address). In sensor network, s_i interacts with the neighbors and employs a one-to-many broadcast primitive in their basic transmission mode. Let T_r be the transmission range of s_i and which is assumed to be uniform for all the sensors. Sensor node lies within T_r of s_i at nth time instant is assumed to be connected. All the connected nodes of s_i belong to set of neighboring sensor nodes $Neg_i(n)$, $Neg_i(n) \subset S$. The number of nodes in $Neg_i(n)$ is known as degree of s_i. The average degree of sensors in a network depends on the T_r. The data sensed by s_i is locally stored and also sent to the neighbors.

All the sensor nodes are connected by a wireless interconnection network. Each sensor sends and receives message from the neighbors within a bounded time period in a synchronous WSNs. The MAC layer protocol used here for data communication of sensor nodes is IEEE 802.15.4.

A sensor network is generally considered as a graph $G(S, C)$ in which S represent a set of sensors and C is the set of communication link among the sensors. For example, in Fig. 3, an arbitrary network topology is depicted, where $S = \{s_1, s_2, s_3, \ldots s_{12}\}$ and $C = c_1, c_2, c_3, \ldots c_{10}$. The immediate neighbors of s_1 are (s_2, s_5, s_{12}) as they lie within T_r of the s_1. Multi-hop communication is feasible through the immediate neighbors. For example, a sensor node s_1 can communicate with s_9 through s_5.

4.3 Fault Model

The links are assumed to be fault free in WSNs. The faults in a link can be detected and corrected by using error detecting and correcting codes in the MAC layer of underlying networks. But the sensor nodes are subjected to faults due to many reasons. In fact, the data of fault-free sensors are always within an acceptable range. But when a sensor becomes faulty, it gives arbitrary value at a different time instant where the error is beyond the acceptable range. As an example, the fault model is depicted in Fig. 4 where 50 sensors are deployed, and out of them 18 sensors are introduced as faulty.

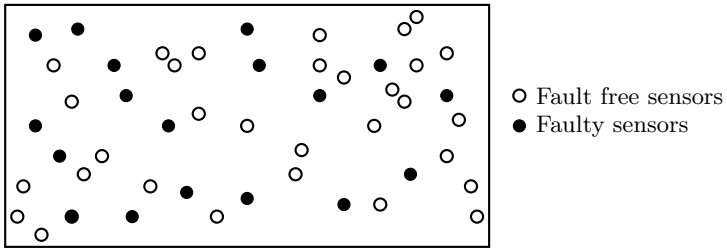


Fig. 4 A sensor network with fault-free and faulty sensors

Let p be the probability of a sensor being intermittently faulty. The set of randomly chosen sensor nodes ($\lceil pN \rceil$ numbers of faulty sensor node) which are subject to either hard or soft failures is denoted as S_F. The set S_F contains both hard and soft faulty sensors, which are further partitioned into two subsets S_1, and S_2, where S_1 and S_2 are the set of hard faulty and the intermittently faulty sensors, respectively. Therefore, the faulty components present in the network are $S_F = S_1 \cup S_2$. Then, the set of fault-free sensors present in the sensor network is defined as $S_G = S - S_F$, where $N = |S_G + S_F|$ and $|S_F| \ll |S_G|$, respectively. The $|S|$ denotes cardinality of a set S.

Here, it has been assumed that each s_i, $1 \leq i \leq N$ is acting as a smart sensor having the intelligence to diagnose itself as well as the capacity to take decisions when it participates with the normal operation of the network. Each s_i observes the outcomes over some time period. It is usually stated in terms of a sequence of outcomes of a sensor node that satisfy the following assumptions:

- The data of a sensor node in each time instant has two possible outcomes either fault free or faulty. In the language of reliability, this is called success and failure.
- The outcomes are temporarily and spatially independent, i.e., the outcome of at one time instant has no influence over the outcome of another time instant. Similarly, the outcomes of each sensor node are independent.
- At each time instant, the probability of failure to provide good data is α and the probability of sensor node able to provide good data is $1 - \alpha$ where $\alpha \in [0, 1]$ is the failure parameter of the process.

The data of each s_i, $1 \leq i \leq N$ at time instant n denoted as $x_i(n)$ is modeled by using the Bernoulli distribution of intermittent faults in successive measurement. The details are described in Sect. 5.

5 Data Modeling and Problem Formulation

Initially, it is assumed that the sensors in the network are fault free and supposed to diagnose their fault status. Each of the sensors in the network is subjected to an

intermittent fault during their course of action. Let p be the fault probability that a sensor is intermittently faulty which is same for every sensor.

5.1 Data Model

The data acquired by a sensor node at nth time instant is typically erroneous or noisy. The standard data model in a network is used here. The error usually occurs due to the problems in hardware and data communication [31]. This becomes severe in adverse environmental conditions and when battery is low. Here, the data transmission over ideal channels is assumed [32]. The error caused during transmission is corrected by error correcting codes used in the MAC layer protocol. In applications like parameter estimation [33, 34], event boundary detection [35, 36] and most of the fault detection algorithms [15, 32, 37] as well modeled the sensor observation as additive noise with the true value.

The outcome $x_i(n)$ of s_i at time instant n is the sum of true value A of the unknown parameter (e.g., the temperature, the humidity, *etc.*) but deterministic and random error [37]. Without losing the generality, the simplest data model of sensors observation is given as [38]

$$x_i(n) = A + \upsilon_i(n), \quad n = 1, 2, \ldots, K \quad K = \frac{T}{\Delta_T} \quad \text{and} \quad i = 1, 2, \ldots, N \tag{1}$$

where $\upsilon_i(1), \upsilon_i(2), \ldots, \upsilon_i(K)$ are erroneous data at respective sensor nodes. In the literature of WSNs [36, 39], it is assumed that the measurements from sensors have same mean, but the error in the erroneous data is different.

The sensor nodes are collecting data in regular interval ΔT for time duration T. The random erroneous data are temporally and spatially independent and have the same distribution function at each node F [15]. It follows that the observation $x_i(1), x_i(2), \ldots, x_i(K)$ are independent with common distribution function and can say that the $x_i(n)$'s are *i.i.d.*, i.e., independent and identically distributed. A conventional way to represent well-behaved data, i.e., data without fault, is assumed F is a normal distribution with mean A and variance σ_i^2 which implies $F = \mathcal{N}(A, \sigma_i^2)$ [15].

In fact, the measurement is erroneous whether the sensor is faulty or fault free. But the only difference is its variance of the measurement error for a fault-free sensor node is very less (nearly 1000 times) compared to that faulty sensor node [36]. However, the scenario is completely different when a sensor node suffered from intermittent fault. Whereas the intermittent fault sensor nodes provide an arbitrary data for some time duration and behaves as a good in another time.

5.2 Problem Formulation

Consider each sensor s_i is having K number of data which are measured at regular interval of time ΔT over a period of T. The data for sensors is generated by using (1) for both faulty and fault-free cases. Initially, each sensor is assumed fault free, and then introduce few sensors are suffering from an intermittent fault randomly. In a faulty sensor node, αK number of data are added with high error at random instant compared to the remaining data. Now, the objective is to detect the intermittent faulty sensors present in the sensor network by analyzing the data in a distributed manner. If every sensor node shares their K number of observations with their neighbors, then each node should keep $N_a K$ number of data, where N_a is the average degree of sensor nodes. But to avoid the memory problem, now each s_i, $1 \leq i \leq N$ share data $x_i(n)$ to its neighbors $Neg_i(n)$ in every cycle and predict the fault status at that time instant n. This process will continue for K times. Then, each sensor node decides by analyzing the K fault status.

6 Distributed Intermittent Self Fault Diagnosis Algorithm

The fault diagnosis algorithm can diagnose the fault status for each of the sensor nodes in the sensor network. The diagnosis may be done in two ways, such as centralized and distributed. In centralized approach, each sensor is supposed to send their data to a central processor through multi-hop communication. The central processor then broadcasts each sensor node's fault status after analyzing their received data using a fault finding method. The major disadvantage here is that it needs huge communication in the network which makes the algorithm energy inefficient as communication needs more energy.

Whereas, in distributed approach, every sensor share their observed data with immediate one-hop neighbors and then diagnose themselves after accumulating the data from the neighbors. Therefore, distributed approach reduces the communication overhead in the network and make the algorithm energy efficient. The diagnosis also takes less time here as the communication overhead decreases. No need to broadcast the fault status here, as all sensor nodes know their fault status along with the neighbors. Thus, it is also called self fault diagnosis algorithms. Now, the distributed intermittent fault diagnosis (DISFD) algorithm is discussed in detail.

It is common in WSNs that a particular type of fault repeats independently for multiple number of times. Therefore, the distributed algorithm is not only diagnosis fault which has occurred but also determines the number of times the fault has occurred. This kind of diagnosis is introduced in [40] as the notion of K-diagnosability.

The intermittently faulty sensors are identified by measuring the outlyingness of an observation from the neighbor's data after each observation. To make the algorithm robust, the modified three-sigma edit test operation $f_i(n)$ is followed here, which is specified in equation (8). In DISFD algorithm, each s_i measures the outly-

ingness present between its observed data x_i with the estimated sensed data which is calculated from the neighbor's data $\mathbf{Nx}_i$ and then compare the outlyingness $f_i(n)$ with a threshold θ. If the outlyingness exceeds θ, then s_i is identified as faulty and keep the fault status in $FS_i(n)$. This procedure repeats for K times. Finally, the intermittent fault status is computed by using Eq. (10) which is discussed in Sect. 7. The description of the distributed self fault diagnosis algorithm is given in Algorithm 1.

According to Algorithm 1, the fault status at each time instant for a sensor is computed for K times during the time interval T to identify whether s_i is fault free or faulty.

7 Analysis of the Distributed Fault Diagnosis Algorithm

The analytical analysis of the distributed fault diagnosis algorithm is discussed here. First, the data from an intermittent faulty sensor is analyzed. Later, the method used to diagnose the fault is discussed.

7.1 Data Analysis of an Intermittent Faulty Sensor

Let us consider an intermittent faulty sensor measures temperature in regular time interval for $K = 50$ times. The actual temperature is 25 °C. The measurement error is modeled as additive normal Gaussian variable with variance σ^2 when the sensor

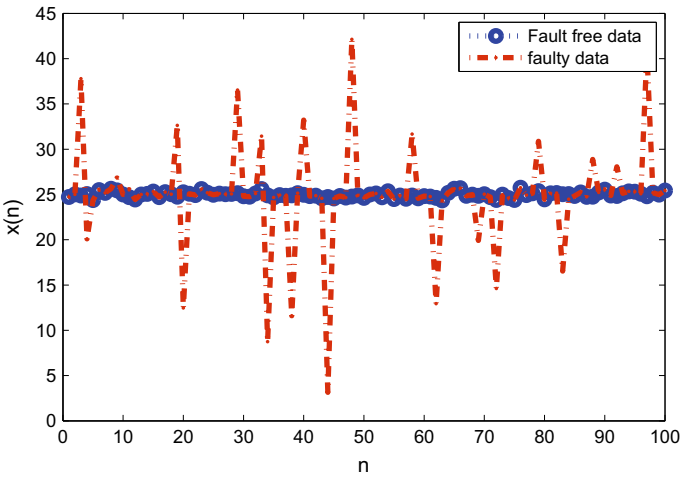


Fig. 5 Behavior of an intermittent faulty sensor node where 23 times the sensor node fails to provide correct data and remaining 77 times provides fault-free observation with limited error. The actual temperature is $A = 25$, the variances of the measurement error are $\sigma^2 = 0.1$ for good sensor, and $\sigma_f^2 = 100$ when the sensor faulty

ALGORITHM 1: Distributed Self Fault Diagnosis Algorithm

Data: Observed time period T, sensed data $x_i(n)$ at time n, intermittent fault probability (α), Battery power (ζ)
Result: Calculate S_1, S_2, and S_G at T
$S_1 = \phi$, $S_2 = \phi$, $S_G = \phi$, $ADM_i = \phi$, $mad_i = \phi$, $FSC_i = \phi$, $FS_i = \phi$
if $Re_i <= \zeta$ **then**
  $S_1 = S_1 \cup \{s_i\}$;
else
  for $n = 1 \cdots \frac{T}{\Delta_T}$ **do**
    s_i collects $\mathbf{Nx}_i(n)$ from $Neg_i(n)$.
    $\mathbf{Nx}_i(n) = \mathbf{Nx}_i(n) \cup \{x_i(n)\}$
    Sort($\mathbf{Nx}_i(n)$)
    /* Procedure for sorting all the elements of $\mathbf{Nx}_i(n)$ in ascending order */
    if $N_i\%2 = 0$ **then**
      $md_i = [\mathbf{Nx}_i(n, N_i/2) + \mathbf{Nx}_i(n, (N_i + 1)/2)]/2$
    else
      $md_i = \mathbf{Nx}_i(n, N_i/2)$
    end
    for $j = 1 \cdots N_i + 1$ **do**
      $ADM_i(n) = ADM_i(n) \cup \{(\mathbf{Nx}_i(n, j) - md_i)\}$
    end
    if $|ADM_i(n)|\%2 = 0$ **then**
      $mad_i(n) = [ADM_i(n, N_i/2) + ADM_i(n, (N_i + 1)/2)]/2$
    else
      $mad_i(n) = ADM_i(n, N_i/2)$
    end
    $MADN_i(n) = mad_i(n)/0.675$
    $FSC_i(n) = (x_i(n) - md_i)/MADN_i(n)$
    if $FSC_i(n) < 3$ **then**
      $FS_i(n) = 0$
    else
      $FS_i(n) = 1$
    end
  end
  if $T_i = \phi$ **then**
    $s = 0$
    for $k = 1 \cdots \frac{T}{\Delta_T}$ **do**
      $s = s + FS_i(n)$
    end
    if $s < \alpha(\frac{T}{\Delta_T})$ **then**
      $S_G = S_G \cup \{s_i\}$
    else
      $S_2 = S_2 \cup \{s_i\}$
    end
  end
end

Table 2 The 95% confidence interval of the mean temperature in degree centigrade

Fraction of suspicious data (α)	CI when different number of observation (K)	
	K = 50	K = 20
0 (fault free)	(24.90, 25.10)	(24.85, 25.13)
0.1	(24.08, 25.92)	(23.75, 26.26)
0.2	(23.43, 26.50)	(23.09, 26.97)
0.3	(23.02, 26.93)	(22.49, 27.39)
0.4	(22.91, 27.22)	(22.17, 27.85)
0.5	(22.70, 27.38)	(21.88, 28.24)

is fault free. The intermittent fault probability α of the sensor is assumed to be 0.2. This reflects that $K\alpha = 20$ times sensor node provides faulty observations randomly and remaining 80 times provides fault-free measurement. The variance of the data when sensor behaves faulty is $\sigma_f^2 = 100$. In Fig. 5, the outcomes of an intermittent faulty and a fault-free sensor for 100 iterations are plotted. It has been seen from the figure that the measurement error is limited when the sensor is fault free where the outcomes are around the true value 25 °C. In case of intermittent faulty sensor node, 23 times when sensor behaves faulty, then the outcomes are much deviated from the true value, whereas it behaves like a fault-free sensor node for remaining 77 times. The error may be large, but the average of the measured temperature is approximated to the true value. Therefore, by measuring the mean, one cannot detect the intermittent faulty sensor node. But the confidence interval (CI) of the mean of the distribution may increase. The 95% CI of the mean temperature in degree centigrade is given in Table 2 for different intermittent fault probabilities p.

From Table 2, it is observed that the CI is (24.90, 25.10) for a fault-free sensor node. The CI increases when the probability of suspicious data by a faulty sensor node increases. In fact, in distributed scenario, a node accumulates neighbor's data and predicts the fault status. To do this, the sensor nodes need to keep all the data from the neighbors which required large memory to store them [16]. In order to reduce the storage requirement, a few data from the neighbors are stored. However, from Table 2, it is evident that when the number of data points is less, the CI is more. Therefore, the method of comparing mean will not provide accurate solutions to diagnose the intermittent faults as in most of the conventional fault diagnosis algorithms the node compares its own data with the neighbor's data [17, 41] or mean of all the neighbor's data including its own [13]. In order to improve the reliability of the results, modified three-sigma edit test based diagnosis is adapted here to detect the intermittently faulty sensors.

Instead of storing all the data from neighbors, s_i only stores the absolute error (in Eq. 8) $f_i(n)$ in its memory. As sensor nodes are memory constrained, the storage required is reduced in the proposed algorithm.

7.2 Mathematical Analysis of the Distributed Fault Diagnosis Algorithm

Each node collects the neighbor's data $Neg_i(n)$ at time instant n and stored in $\mathbf{Nx}_i(n) = \{x_i(n)\}_{s_i \in Neg_i(n)}$. The outlyingness is being measured by estimating the mean $\hat{\mu}_i(n)$ and standard deviation (SD) of the neighbor's data. The standard deviation $\hat{\sigma}_i(n)$ at s_i is defined as [42]

$$\hat{\sigma}_i(n) = \sqrt{\frac{1}{N_i - 1} \sum_{s_j \in Neg_i(n)} (x_j(n) - \hat{\mu}_i(n))^2} \tag{2}$$

The outlyingness $t_i(n)$ of s_i is the ratio of the deviation of its data $x_i(n)$ from the estimated mean $\hat{\mu}_i(n)$ and SD $\hat{\sigma}_i(n)$. Now, $t_i(n)$ is given as

$$t_i(n) = \frac{x_i(n) - \hat{\mu}_i(n)}{\hat{\sigma}_i(n)} \tag{3}$$

Now apply the "three-sigma edit" rule, and consider s_i is faulty if $|t_i(n)| > \theta$. Otherwise, s_i may considered as fault free [12]. From the theory of statistics, the conventional three-sigma edit rule is ineffective when number of samples are less. According to the statistical feature if $N_i < 10$, then $|t_i(n)|$ is always less than 3 with the CI of 95%, where N_i is the degree of s_i. This shows that the rule may not work for the less connected sensor network. This measure is also unable to track if two sensor nodes are faulty where one faulty node's data is very large compared to other faulty nodes. In this situation, the less error valued faulty sensor node may be detected as fault free. This effect is called *masking*. The ineffectiveness of this measure is due to non-robust nature of mean and SD. There will be more deviation of estimated mean and SD when a faulty node is present in the neighborhood.

Masking is a problem in robust statistics where the small outliers are hidden by very large outlier. In order to overcome masking problem, median of data is used instead of non-robust mean which is sensitive to outlier [43]. The median of the data set $\mathbf{Nx}_i(n) = \{x_1(n), x_2(n), \ldots, x_{N_i}(n)\}$ is calculated as per the following equation. The data to be sorted in increasing order first.

$$x_1(n) \leq x_2(n) \cdots \leq x_{N_i}(n) \tag{4}$$

If $N_i = 2m - 1$, i.e., is odd for a integer of m, then the estimated median

$$Md_i(n) = Med(\mathbf{Nx}_i(n)) = x_m(n)$$

Similarly, for even value of N_i, i.e., $N_i = 2m$ for some integer m, then the median is determined as

$$Md_i(n) = Med(\mathbf{Nx}_i(n)) = \frac{x_m(n) + x_{m+1}(n)}{2} \tag{5}$$

Just like median is the robust alternative to mean, in statistics, median absolute deviation (MAD) is used as an alternative to the SD [43]. The MAD is defined as

$$MAD(x_1(n), \ldots, x_{N_i}(n)) = \text{Med}|x_i(n) - Md_i(n)| \tag{6}$$

Assuming normal distribution, it is observed that $MAD(x_1(n), \ldots, x_{N_i}(n)) = 0.675SD$. Therefore, the normalized median absolute deviation (about the median) MADN$\mathbf{Nx}_i(n)$ is defined as

$$\text{MADN}(\mathbf{Nx}_i(n)) = \frac{\text{Med}\{|x_i(n) - Md_i(n))|\}}{0.675} \tag{7}$$

Now MADN$(\mathbf{Nx}_i(n))$ can be used as SD. It is observed that the Med$(\mathbf{Nx}_i(n))$ and MADN$(\mathbf{Nx}_i(n))$ are robust over masking compared to that of $\hat{\mu}(n)$ and SD, when data is contaminated with outliers which is generated from the unknown mechanisms of the faulty sensor node. Now to make the measure of outlyingness in (3) robust, the mean is to be replaced by median and the SD is replaced by MADN. The new measure of outlyingness $f_i(n)$ to detect the fault status of a s_i is given by [15]

$$f_i(n) = \frac{x_i(n) - Md_i(n)}{\text{MADN}(\mathbf{Nx}_i(n))} \tag{8}$$

The accuracy of this method increases when degree of sensor nodes is high. But at the same time, the computation and memory requirement also increases with the degree of the sensor node.

A sensor node s_i has a K number of probable fault status for each of the neighbors. The modified three-sigma edit test operation $f_i(n)$ given in (8) is performed and the fault status of a sensor node is identified as

$$fs_i(f_i(n)) = \begin{cases} 1, & f_i(n) \geq \theta \\ 0, & f_i(n) < \theta \end{cases} \tag{9}$$

where θ is a threshold which is constant for all sensors. It is because, the standard data model used in sensor network, the deviation in the measured data known as error is having common statistics for all the homogenous sensor nodes deployed in a network. Therefore, the threshold is same for all the sensor node by keeping in mind that the statistics of the data are same at all the sensor nodes in the network.

This process is repeated for $K = \left\lceil \frac{T}{\Delta_T} \right\rceil$ times and the fault status for different instances are stored in $\mathbf{fs}_i$. At the end of K iterations, s_i establishes its own intermittent fault status by using (10).

$$FS_i(T) = \begin{cases} 1, & \sum_{k=1}^{K} fs(f_i(k)) \geq \lceil \alpha K \rceil \\ 0, & \sum_{k=1}^{K} fs(f_i(k)) < \lceil \alpha K \rceil \end{cases} \tag{10}$$

where $k = 1, 2, \ldots, K$ and $i = 1, 2, \ldots, N$.

8 Result and Discussion

The distributed fault diagnosis algorithms are implemented in NS3 (NS3 is an open-source network simulator which is used by considering a discrete event network simulation) [44]. In Table 3, the values of the network parameters used in the simulation of distributed algorithms are given. All the values are chosen here as an example. There are 1024 homogeneous sensors which are uniform randomly deployed in an area of $\{1000\,\text{m} \times 1000\,\text{m}\}$. The range propagation model is used here which models the propagation loss through a transmission medium. The model also calculates the received power (dbm) from transmitted power (dbm). A constant mobility model for the source and destination positions is considered. During the diagnosis period the nodes are assumed to be static. The performance of algorithms depends upon these modes and the parameters used in the sensor network. For example, the average degree (N_a) of the nodes completely relies on the transmission range of the sensors. The N_a will increase if the transmission range is increased. But the impact of change in any of the parameter will be the same for all the algorithms.

The performance of the discussed DISFD algorithm is compared with two similar kinds of algorithms such as DIFD1 [16] and DIFD2 [45]. Three parameters are used to compare the performance of different algorithms. These are defined as [15] follows:

– Detection accuracy (DA): It is defined as the ratio between number of faulty sensors detected as faulty and the total number of faulty sensors in the network.

Table 3 The simulation parameters

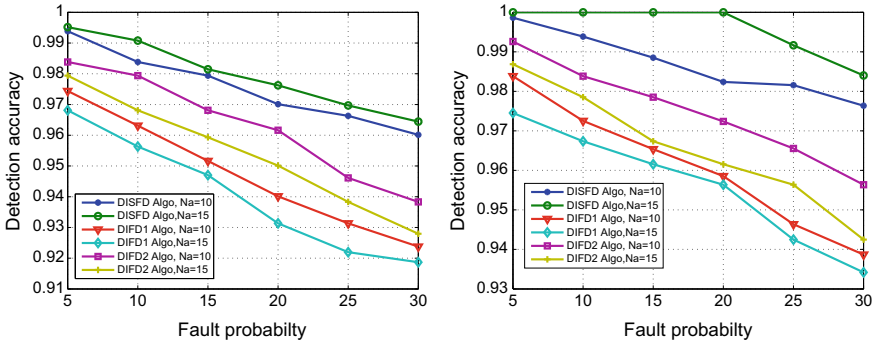
Simulation parameters	
Number of sensors (N)	1024
Simulation time	300 s
Propagation loss model	Range propagation loss model
Coverage area	$1000\,\text{m} \times 1000\,\text{m}$
Fault model	Normal random variable
Transmission range (T_r)	(56, 61) cm
Network type	Homogeneous
Node mobility	Constant speed mobility model
Environment condition	Variation in environment and noise is considered
Node distribution	Uniform random distribution
Node capacity	5 buffers for receiving packets
Sensed data of fault-free and faulty sensor node	Normal random variable with mean (μ) 30 and variance (σ) 1 and 1000 for fault free and faulty nodes respectively

– False alarm rate (FAR): The FAR is defined as the ratio between number of fault-free sensors detected as faulty and the total number of fault-free sensors in the network.
– False positive rate (FPR): The FPR is defined as the ratio of number of faulty sensors detected as faulty free to total number of fault-free sensors in the network.

8.1 Simulation Model

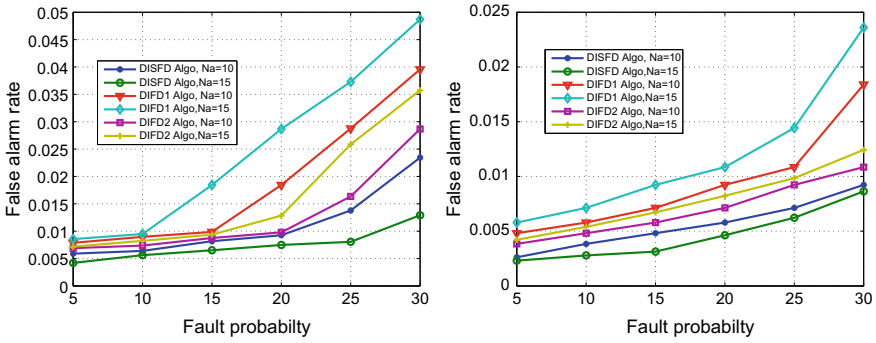
The simulation results for all the algorithms are provided for fault probabilities of 5% to 30% with step size of 5%. It is well known that the statistical method's performance improves with increase in data size. Therefore, the connectivity of sensor nodes in a network plays an important role. All the algorithms' performance are evaluated for average degree of sensor nodes Na of 10 and 15. In order to have the said N_a, T_r to be 56, 61 for average degree 10 and 15, respectively. Further, it is observed that, if a node suffers from intermittent fault for a long duration, identifying its fault status is reliable. Thus, all algorithms are tested for different intermittent fault probabilities (α). The value of α chosen 0.6–0.9 with the step size of 0.1. When an intermittent faulty sensor behaves faulty for more number of observations, identifying fault is reliable with high probability. However, difficulty arises when a node's sensed data is suspicious for less number of observations. The robustness of the algorithm is verified for different α and observed that the algorithm's performance degrades if the α is less than 0.6. The average over 100 experiments is plotted in each graph. The simulation results show that the DISFD algorithm performs well over the DIFD1 and DIFD2 algorithms.

The DA, FPR, and FAR performances of the distributed algorithms for different fault probabilities are given in Figs. 6, 8, and 7, respectively. Since the performance



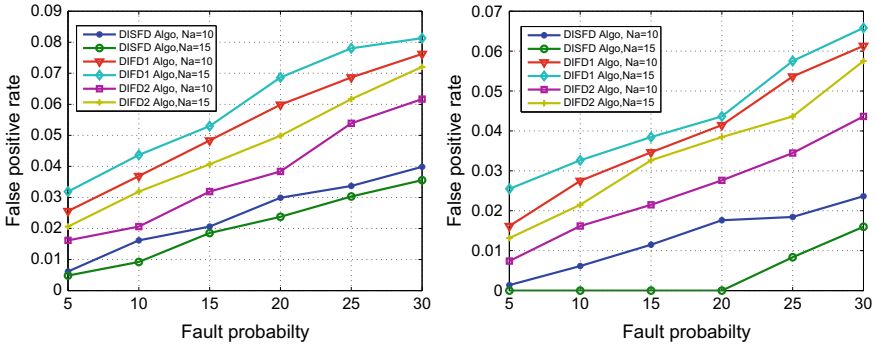
(a) For $\alpha = 0.7$, $N_a = 10$ and 15 (b) For $\alpha = 0.8$, $N_a = 10$ and 15

Fig. 6 DA versus fault probabilities plots of DISFD, DIFD1, and DIFD2 algorithms for different intermittent fault probabilities α and average degrees N_a



(a) For $\alpha = 0.7$, $N_a = 10$ and 15 (b) For $\alpha = 0.8$, $N_a = 10$ and 15

Fig. 7 FAR versus fault probabilities plots of DISFD, DIFD1, and DIFD2 algorithms for different intermittent fault probabilities α and average degrees N_a

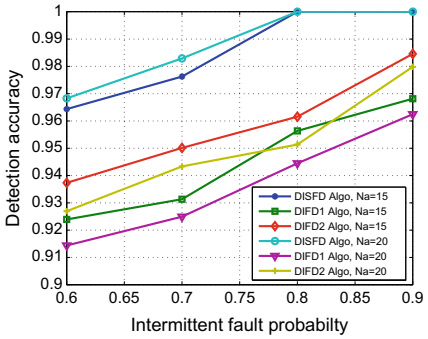


(a) For $\alpha = 0.7$, $N_a = 10$ and 15 (b) For $\alpha = 0.8$, $N_a = 10$ and 15

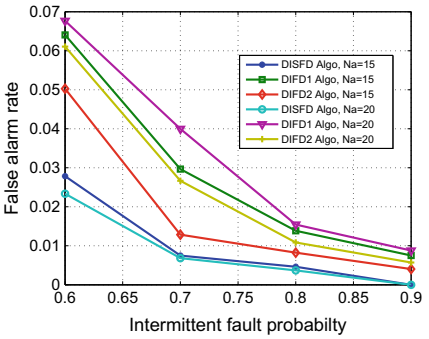
Fig. 8 FPR versus fault probabilities plots of DISFD, DIFD1, and DIFD2 algorithms for different intermittent fault probabilities α and average degrees N_a

of the algorithms depends on both N_a and α, the results are given for different α values 0.7 and 0.8 and N_a are 10 and 15. The performance of DA and FAR with respect to confidence interval for the α values range from 0.6 to 0.8 are given in Table 4 and Table 5, respectively. The performance of all the algorithms decreases with the increase in number of faulty node in the networks, i.e., fault probability p. Whereas the DISFD algorithm always performs well compared to that of other algorithms.

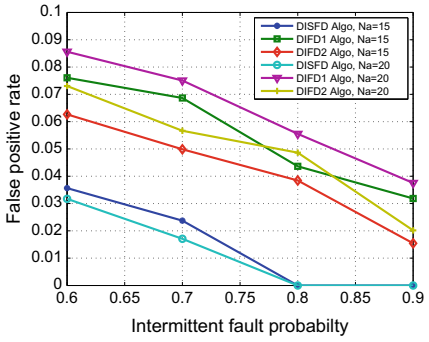
The proposed scheme gives nearly 96.5% DA, 2% FPR, and 3% FAR when intermittent fault probability α is 0.7, the average degree of the network (N_a) is 15, fault probability p is 0.3, and network size N is 1024. The DISFD algorithm achieves these performance improvements with 43%, 33% less message complexity as compared to Lee et al. and Yim et al. algorithms. Similar improvements over Yim et al. algorithm for same simulation environment and network settings. The



(a) DA versus intermittent fault probability



(b) FAR versus intermittent fault probability



(c) FPR versus intermittent fault probability

Fig. 9 Performance of the algorithms with respect to different intermittent fault probabilities when 20% sensor nodes are faulty in the network for average degrees 15 and 20. **a** DA versus intermittent fault probability (α) for fault probability $p = 20$. **b** FAR versus intermittent fault probability (α) for fault probability $p = 20$. **c** FPR versus intermittent fault probability (α) for fault probability $p = 20$

comparison results for $\alpha = 0.8$ and different values of N_a are shown in Figs. 6, 7, and 8. Similar improvement in performance of the proposed algorithm over existing algorithms is found. The improvement of the results in new algorithm is because of robust statistical method.

In the fault diagnosis algorithm, it is assumed that if a sensor node behaves faulty for more than 50% of the observations, then detected as faulty. Most of the existing algorithms are considered a node is intermittent faulty if 80% observations are suspicious. However, the analysis presented here for the performance of algorithms when 60–90% observations are faulty. In Fig. 9, the effect of α on the performance of all algorithms for average degrees 15 and 20 is given. The DA, FAR, and FPR versus α are plotted in Fig. 9a, b, and c, respectively. As per our expectation, the DA performance of all the algorithms increases with the increase in α which is shown in Fig. 9a.

Table 4 Confidence interval of detection accuracy for DISFD, Yim et al. (DIFD1) and Lee et al. (DIFD2) algorithms

IFP	FP	CI when Na = 10			CI when Na = 15		
		DISFD	DIFD1	DIFD2	DISFD	DIFD1	DIFD2
0.6	0.05	100.0, 100.0	92.99, 100.0	91.98, 100.0	100.0, 100.0	91.99, 100.0	88.99, 100.0
	0.10	96.27, 100.0	92.71, 100.0	91.67, 100.0	97.08, 100.0	91.02, 100.0	89.46, 100.0
	0.15	94.31, 99.69	92.90, 99.10	91.93, 99.45	94.33, 99.69	91.53, 98.44	89.02, 98.92
	0.2	94.66, 99.34	92.03, 97.94	91.07, 98.92	94.66, 99.34	90.75, 97.25	88.49, 97.59
	0.25	92.33, 97.66	89.87, 96.13	88.89, 97.11	92.33, 97.67	89.17, 96.68	87.63, 96.36
	0.3	92.57, 97.43	88.97, 95.03	88.02, 95.98	92.57, 97.43	88.97, 95.18	86.79, 95.26
0.7	0.05	100.0, 100.0	100.0, 100.0	92.99, 100.0	100.0, 100.0	93.09, 100.0	88.99, 100.0
	0.1	97.47, 100.0	94.94, 100.0	92.67, 100.0	100.0, 100.0	93.67, 100.0	89.46, 100.0
	0.15	95.79, 100.0	94.35, 99.69	90.47, 99.54	97.43, 100.0	92.93, 99.19	89.07, 98.92
	0.2	94.66, 99.34	93.93, 99.34	89.72, 98.27	95.98, 99.92	92.07, 97.98	88.45, 97.59
	0.25	94.95, 99.09	91.17, 96.82	88.89, 97.17	94.85, 99.09	89.87, 96.13	87.63, 96.36
	0.3	93.81, 98.19	90.51, 96.48	89.25, 96.74	95.09, 98.91	88.97, 95.08	86.79, 95.26
0.8	0.05	100.0, 100.0	100.0, 100.0	100.0, 100.0	100.0, 100.0	100.0, 100.0	92.99, 100.0
	0.1	100.0, 100.0	96.47, 100.0	94.44, 100.0	100.0, 100.0	95.44, 100.0	92.67, 100.0
	0.15	97.43, 100.0	95.59, 100.0	93.45, 100.0	100.0, 100.0	94.45, 99.69	93.45, 100.0
	0.20	97.20, 100.0	96.08, 99.91	92.47, 99.52	100.0, 100.0	93.63, 99.33	92.47, 99.52
	0.25	95.74, 99.71	94.88, 99.07	91.49, 98.58	97.89, 100.0	92.84, 98.48	91.49, 98.58
	0.3	96.44, 99.56	93.82, 98.17	90.51, 97.48	96.44, 99.56	91.52, 96.65	90.51, 97.48

8.2 Confidence Interval

The confidence interval is a range of values defined in such a way that there is a specified probability that the value of a parameter lies within the range. The range is

Table 5 Confidence interval of false alarm rate for DISFD, Yim et al. (DIFD1) and Lee et al. (DIFD2) algorithms

IFP	FP	CI when Na = 10			CI when Na = 15		
		DISFD	DIFD1	DIFD2	DISFD	DIFD1	DIFD2
0.6	0.05	0.39, 1.66	0.92, 2.57	0.95, 3.57	0.32, 1.53	1.83, 3.93	1.89, 4.23
	0.1	0.89, 2.58	1.84, 4.02	1.94, 4.42	0.73, 2.31	2.47, 4.91	2.77, 5.41
	0.15	1.76, 3.98	2.43, 4.93	2.73, 5.43	1.03, 2.87	3.50, 6.38	3.68, 6.98
	0.2	2.17, 4.66	3.10, 5.94	3.74, 6.67	1.68, 3.94	3.93, 7.06	4.63, 7.96
	0.25	3.08, 6.03	3.86, 7.08	4.86, 7.88	2.54, 5.28	4.42, 7.82	4.92, 6.82
	0.3	3.78, 7.11	4.51, 8.06	5.51, 8.96	3.19, 6.31	4.99, 8.69	5.99, 8.99
0.7	0.05	0.06, 0.96	0.19, 1.25	0.69, 2.25	0.01, 0.81	0.19, 1.25	0.69, 2.25
	0.1	0.13, 1.17	0.20, 1.32	1.23, 2.32	0.13, 1.17	0.27, 1.47	1.27, 2.47
	0.15	0.21, 1.40	0.29, 1.55	1.29, 2.55	0.14, 1.24	0.36, 1.71	1.36, 2.51
	0.2	0.22, 1.49	0.30, 1.65	1.32, 1.85	0.22, 1.49	1.01, 2.90	2.01, 3.95
	0.25	0.32, 1.76	0.59, 2.27	1.59, 3.47	0.24, 1.58	1.79, 4.20	2.79, 5.23
	0.3	0.54, 2.26	1.70, 4.17	2.73, 5.17	0.54, 2.26	2.38, 5.17	2.58, 5.77
0.8	0.05	0.00, 0.66	0.01, 0.81	0.71, 1.81	0.00, 0.66	0.06, 0.96	0.26, 1.86
	0.1	0.01, 0.86	0.07, 1.02	1.07, 2.02	0.00, 0.69	0.13, 1.17	1.13, 2.17
	0.15	0.07, 1.08	0.14, 1.24	1.14, 2.24	0.00, 0.73	0.21, 1.40	1.21, 2.44
	0.2	0.08, 1.14	0.15, 1.32	1.15, 2.52	0.01, 0.97	0.30, 1.65	1.35, 2.15
	0.25	0.16, 1.40	0.32, 1.76	1.32, 2.76	0.08, 1.22	0.41, 1.93	1.41, 2.13
	0.3	0.26, 1.70	0.35, 1.89	1.35, 2.49	0.26, 1.70	0.64, 2.44	1.64, 3.84

more for high probability. The 95% confidence interval (CI) is one of the commonly used parameters in literature. In this analysis, 95% CI for the parameters DA and FAR is provided for different values of p, α, and N_a in Table 4 and Table 5, respectively.

The CI performance of the algorithm better of the range is less compared to that of others. It is observed from the tables that the CI is less for DISFD algorithm compared to that of DIFD1 and DIFD2. As expected, there were some observations found for all the algorithms. The CI range increases with increase in p, decreases when α increases for constant p. It may be the reason that, when α increases, the faulty sensor provides inconsistent data more frequently which helps the fault detector algorithm to detect the intermittent fault behavior.

Similarly, the CI performance improves, i.e., the range decreases with the increase in N_a. This observation is for DISFD algorithm. Whereas, in DIFD1 and DIFD2 algorithms, the performance decreases, i.e., CI increases when connectivity increases (N_a increases). This is due to the neighbor coordination method for fault detection.

9 Conclusion

A self fault diagnosis algorithm to diagnose the intermittent faulty sensors using distributed approach in wireless sensor networks is presented in this chapter. The inconsistent behavior of the intermittent faulty sensor is diagnosed by using robust statistical approach. Each sensor accumulates data from the neighbors and then detects its own as well the neighbor's fault status for specific number of times. The final intermittent faults are decided after fusing all the decisions taken in the repeated teasing process. The performance of the present and two similar kinds of algorithm has been evaluated in NS3. The parameters such as detection accuracy (DA), false positive rate (FPR), and false alarm rate (FAR) are used for the performance comparison. The simulation results show that the DISFD algorithm is improved by 8, 5, 9% over Lee et al. and 2, 3, 7 over Yim et al. in DA, FAR, and FPR when fault probability is 30%, intermittent fault probability 7%, and average degree of the sensor is 20 of network size 1024. The robust method reduces the number of repetition required to diagnose the intermittent fault which makes the algorithm energy as well as storage efficient.

References

1. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. *Science Direct Transactions on Computer Networks*, *38*(4), 393–422.
2. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002, August). A survey on sensor networks. *IEEE Transactions on Communications Magazine, 40*, 102–114.
3. Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. *Computer Networks*, *52*(12), 2292–2330.
4. Binh, H. T. T., & Dey, N. (2018). *Soft computing in wireless sensor networks*. CRC Press.
5. Yuan, H., Zhao, X., & Yu, L. (2015). A distributed Bayesian algorithm for data fault detection in wireless sensor networks. In *2015 International Conference on Information Networking (ICOIN)* (pp. 63–68). IEEE.
6. Panigrahi, T., Panda, M., & Panda, G. (2016). Fault tolerant distributed estimation in wireless sensor networks. *Journal of Network and Computer Applications*, *69*, 27–39.
7. Nandi, M., Dewanji, A., Roy, B. K., & Sarkar, S. (2014). Model selection approach for distributed fault detection in wireless sensor networks. *International Journal of Distributed Sensor Networks*, *2014*(48234), 1–12.
8. Yu, M., Mokhtar, H., & Merabti, M. (2007). Fault management in wireless sensor networks. *IEEE Wireless Communications, 14*(6), 13–19.
9. Sampath, M., Sengupta, R., Lafortune, S., Sinnamohideen, K., & Teneketzis, D. (1995, September). Diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control, 40*(9), 1555–1575.
10. Ssu, K.-F., Chou, C.-H., Jiau, H. C., & Hu, W.-T. (2006, June). Detection and diagnosis of data inconsistency failures in wireless sensor networks. *Computer Networking, 50*, 1247–1260.
11. Banerjee, I., Chanak, P., Rahaman, H., & Samanta, T. (2014). Effective fault detection and routing scheme for wireless sensor networks. *Computers & Electrical Engineering*, *40*(2), 291–306.
12. Panda, M., & Khilar, P. M. (2012, December). Distributed soft fault detection algorithm in wireless sensor networks using statistical test. In *IEEE International Conference on Parallel, Distributed and Grid Computing (PDGC 2012)* (pp. 195–198).

13. Panda, M., & Khilar, P. M. (2012, December). Energy efficient soft fault detection algorithm in wireless sensor networks. In *IEEE International Conference on Parallel, Distributed and Grid Computing (PDGC 2012)* (pp. 801–805).
14. Jiang, S., & Kumar, R. (2006, January). Diagnosis of repeated failures for discrete event systems with linear-time temporal-logic specifications. *IEEE Transactions on Automation Science and Engineering, 3*(1), 47–59.
15. Panda, M., & Khilar, P. M. (2015). Distributed self fault diagnosis algorithm for large scale wireless sensor networks using modified three sigma edit test. *Ad Hoc Networks, 25, Part A*(0), 170–184.
16. Lee, M. H., & Choi, Y. H. (2008). Fault detection of wireless sensor networks. *Computer Communications*, *31*(14), 3469–3475.
17. Mahapatro, A., & Khilar, P. M. (2013). Detection and diagnosis of node failure in wireless sensor networks: A multi objective optimization approach. *Swarm and Evolutionary Computation*, *13*, 74–84.
18. Jalote, P. (1994, April). *Fault tolerance in distributed systems*. Prentice Hall.
19. Chessa, S. (1999). *Self-diagnosis of grid-interconnected systems, with application to self-test of VLSI wafers*. PhD thesis, Citeseer.
20. Elhadef, M., Boukerche, A., & Elkadiki, H. (2008). A distributed fault identification protocol for wireless and mobile ad hoc networks. *Science Direct Journal of Parallel and Distributed Computing*, *68*(3), 321–335.
21. Siewiorek, D. P., & Swmlz, R. S. (1992). *Reliable computer system design and evaluation*. Digital Press.
22. Barborak, M., Dahbura, A., & Malek, M. (1993). The consensus problem in fault-tolerant computing. *ACM Computing Survey*, *25*, 171–220.
23. Breuer, M. A. (1973). Testing for intermittent faults in digital circuits. *IEEE Transaction on Computers*, *22*(3), 241–246.
24. de Kleer, J., & Williams, B. C. (1987, April). Diagnosing multiple faults. *Artificial Intelligence, 32*(1), 97–130. ISSN 0004-3702.
25. Khilar, P. M., & Mahapatra, S. (2007, December). Intermittent fault diagnosis in wireless sensor networks. In *10th International Conference on Information Technology, (ICIT 2007)* (pp. 145–147).
26. Choi, J. Y., Yim, S. J., Huh, Y. J., & Choi, Y. H. (2009, February). A distributed adaptive scheme for detecting faults in wireless sensor networks. *WSEASE Transactions on Communication, 8*(2), 269–278.
27. Xu, X., Chen, W., Wan, J., & Yu, R. (2008). Distributed fault diagnosis of wireless sensor networks. In *11th IEEE International Conference on Communication Technology, 2008. ICCT 2008* (pp. 148–151).
28. Sahoo, Manmath Narayan, & Khilar, Pabitra Mohan. (2014). Diagnosis of wireless sensor networks in presence of permanent and intermittent faults. *Wireless Personal Communications*, *78*(2), 1571–1591.
29. Swain, R. R., Khilar, P. M., & Bhoi, S. (2018a). Heterogeneous fault diagnosis for wireless sensor networks. *Ad Hoc Networks, 69*, 15–37. ISSN 1570-8705. https://doi.org/10.1016/j.adhoc.2017.10.012. http://www.sciencedirect.com/science/article/pii/S1570870517301841.
30. Swain, R. R., Khilar, P. M., & Dash, T. (2018b). Fault diagnosis and its prediction in wireless sensor networks using regressional learning to achieve fault tolerance. *International Journal of Communication Systems, 31*(14), e3769. https://doi.org/10.1002/dac.3769. https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.3769.
31. Andreou, P. G., Zeinalipour-Yazti, D., Samaras, G. S., & Chrysanthis, P. K. (2014). A network-aware framework for energy-efficient data acquisition in wireless sensor networks. *Journal of Network and Computer Applications*, *46*, 227–240.
32. Wang, T.-Y., Chang, L.-Y., & Chen, P.-Y. (2009). A collaborative sensor-fault detection scheme for robust distributed estimation in sensor networks. *IEEE Transactions on Communications*, *57*(10), 3045–3058.

33. Krasnopeev, A., Xiao, J.-J., & Luo, Z.-Q. (2005). Minimum energy decentralized estimation in a wireless sensor network with correlated sensor noises. *EURASIP Journal of Wireless Communications and Networking*, *2005*(4), 473–482.
34. Xiao, L., Boyd, S., & Kim, S.-J. (2007). Distributed average consensus with least-mean-square deviation. *Journal of Parallel and Distributed Computing*, *67*(1), 33–46.
35. Wang, T.-Y., & Cheng, Q. (2008). Collaborative event-region and boundary-region detections in wireless sensor networks. *IEEE Transactions on Signal Processing*, *56*(6), 2547–2561.
36. Krishnamachari, B., & Iyenger, S. (2004, August). Distributed Bayesian algorithm for fault tolerant event region detection in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems, 24*(8), 1525–1534.
37. Luo, X., Dong, M., & Huang, Y. (2006). On distributed fault-tolerant detection in wireless sensor networks. *IEEE Transactions on Computers*, *55*(1), 58–70.
38. Nguyen, T., Nguyen, D., Liu, H., & Tran, D. A. (2007, July). Stochastic binary sensor networks for noisy environments. *International Journal of Sensor Network, 2*(5/6), 414–427.
39. Mahapatro, A., & Panda, A. K. (2014, September). Choice of detection parameters on fault detection in wireless sensor networks: A multiobjective optimization approach. *Wireless Personal Communication, 78*(1), 649–669. ISSN 0929-6212.
40. Jiang, S., Kumar, R., & Garcia, H. E. (2003). Diagnosis of repeated/intermittent failures in discrete event systems. *IEEE Transactions on Robotics and Automation*, *19*(2), 310–323.
41. Panda, M., & Khilar, P. M. (2014). Energy efficient distributed fault identification algorithm in wireless sensor networks. *Journal of Computer Networks and Communications, 2014*.
42. Ross, S. M. (2010). *Introduction to probability models* (10th ed.). Academic Press, Inc.
43. Rousseeuw, P. J., & Croux, C. (1993, December). The mean and median absolute deviations. *Journal of the American Statistical Association, 88*(424), 1273–1283 (Theory and Methods).
44. Network Simulator (ns3). (2013). http://nsnam.org.
45. Yim, S.-J., & Choi, Y.-H. (2010). An adaptive fault-tolerant event detection scheme for wireless sensor networks. *Sensors*, *10*(3), 2332–2347.

Ambient Intelligence for Patient-Centric Healthcare Delivery: Technologies, Framework, and Applications

G. S. Karthick and P. B. Pankajavalli

Abstract Current technological changes have implemented advanced solutions for enhancing the quality of human life. Ambient intelligence (AmI) is a powerful paradigm which is characterized by various computing technologies that enable the machines to interact with humans. Such developments made it possible to evolve different real-time solutions especially in the healthcare domain. This chapter describes how AmI infrastructures have emerged in the field of healthcare for providing effective solutions. Also, this chapter discusses the role of sensors and wearable devices in developing an ambient healthcare system. This chapter proposes a secured cloud-oriented architecture and algorithm for secure data transmission from wireless body area network (WBAN) to cloud storage. The proposed theoretical framework focuses on case-based and context-aware reasoning facility which satisfies the various use cases and requirements of ambient-based healthcare systems. Finally, an illustration case describes how the ambient care works in a hospital environment, and it also elaborates a few contexts, events, and rules using Unified Modeling Language (UML) class diagram.

Keywords Ambient intelligence · Human–computing interface · Wireless body area network · Artificial intelligence · Context-aware reasoning · Case-based reasoning · Markov chain model

1 Introduction

Ambient intelligence (AmI) is an innovative technology which is gradually empowering the lives of people through smart environment. AmI could be considered to be receptive, approachable, and responsive to human requirements, behaviors, postures, and emotional state. AmI is a universal dissemination of intelligence in everyday life

G. S. Karthick (✉) · P. B. Pankajavalli
Department of Computer Science, Bharathiar University, Coimbatore, India
e-mail: karthickgs@outlook.com

P. B. Pankajavalli
e-mail: pankajavalli@buc.edu.in

S. K. Das et al. (eds.), *Design Frameworks for Wireless Networks*,
Lecture Notes in Networks and Systems 82,
https://doi.org/10.1007/978-981-13-9574-1_10

by integrating several hardware and software with the support of wireless communication technologies and sensors. Assume that a portable device monitors the health status of a person continuously for diagnosing abnormal health conditions; this in turn encourages the person to change the habits and communicates to the doctor for offering optimum health solutions. Such portable device may be fabricated or embedded into the regular clothing, and it resembles the ambient intelligence science fiction.

The future of AmI is focused on incorporating the intelligent computing to the healthcare environments which would help with timely medical intervention for healthy living. Conventional computing model is comprised of user interfaces like keyboard, mouse, and display units which cannot be used in the same form in large ambient environments. For example, an ambient system encompasses various sensors for recognition of shapes, activities, odors, and sounds. Hence, the data accumulated from distinct sensors require different user interfaces and have to be simplified for achieving increased efficiency of the system. Therefore, conventional computing models are no longer needed in modern computing paradigm, but it integrates the sensors and microcontrollers into every object that work together coherently for supporting the users. AmI strongly depends on the artificial intelligence techniques, which allows successful understanding of the health- and wealth-related information acquired from sensors. Such information are accumulated together and adapted to the environment as per user transparent and anticipatory needs. The well-known characteristics of AmI systems [1] are elaborated below (Fig. 1):

- Intelligence: AmI systems are capable of analyzing the data intelligently for understanding the contemporary context and offer intelligent recommendations.

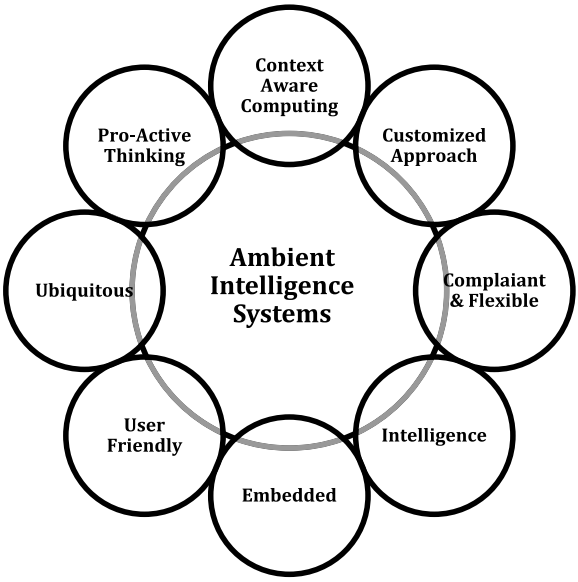


Fig. 1 Characteristics of ambient intelligence systems

- Embedded: AmI applications are mainly comprised of embedded systems, intelligent sensing technologies, and actuators which can be deployed and operated autonomously.
- User-Friendly: AmI systems could be made efficiently with high-end user-interface design in such a way that end users can easily communicate and interact with the system.
- Context-Aware Computing: It explores the better understanding of the substantial and situational information of ambient systems.
- Customized Approach: It provides personalized services for the satisfaction of individual user needs.
- Proactive Thinking: It can predict the desires of an individual without the knowledge of the individual.
- Compliant and Flexible: AmI systems could be viewed as highly compliant and flexible because it can easily adapt to the varying needs of individuals.
- Ubiquitous: The adherence of ubiquitous computing allows merging of numerous invisible sensors into real-time ambient environment. Miniaturization is an important characteristic of ubiquitous computing that minimizes the size of embedded components and thus making the system more mobile.

Moreover, the intelligence of AmI is an important aspect which is drawn from the improvements in the artificial intelligence (AI) domain. The adoption of AI techniques like logical reasoning, activity recognition, and decision-making into the AmI systems confidently strengthen the characteristics like proactive, compliant, flexible, and ubiquitous [2]. In addition, it also relies upon the wireless sensor network (WSN) that enables data collection, humanoids and robots to develop more natural compliant AmI systems. Different computing devices are used to attain the vision of enriched AmI system. The widespread use of computing devices like smartphones, sensing technologies, tracking systems, and object identification tags are pooled in together to spark the recognition of AmI systems in our environments.

The quality and cost of healthcare services are increasing aggressively and worsen the individual's quality of life due to an increased aging problem or a chronic disease this in turns pawns demand for different healthcare services. The substantial improvements in information and communication technology (ICT) can be used in implementation of autonomous and anticipatory healthcare services. In the past decades, web-oriented healthcare platforms and electronic health records (EHR) has been considered as an improved healthcare service. In this era, with the emergence of smart technologies, healthcare services are moving toward remote health monitoring systems [3].

Such remote health monitoring systems started improving rapidly with the advance researches in the area of sensor networks and embedded systems [4]. Specifically, AmI systems have the potential to provide uninterrupted healthcare delivery services, monitoring or anticipatory systems for elder people or individuals with illness and also capable of providing living assistance by capturing their desires. This improves the lifestyle of the individuals by providing revolutionary communication and monitoring for healthcare services. In the healthcare domain, AmI systems are

allied with decision support, EHR, knowledge reasoning, telemedicine, and medical informatics. AmI offers a facility for remote observation of patient's health records, radiological reports, and information. Nowadays, robots are widely used in various forms for several purposes, applications, and tasks. It is being used for surgery assistance and rehabilitation. In rehabilitation systems, robots are designed to operate in hospital as well as in home environment which is very convenient for aged people or patients with chronic diseases. Some of the other applications of robotics in the field of healthcare are as follows: (i) autonomous wheelchair, (ii) nurse assistant, and (iii) robot-based therapy for autism patients and marrow transplant children.

This chapter investigates the vital idea behind the AmI and its characteristics which supports the human-to-computer interaction systems. Section 2 reviews the major supporting technologies which work together to offer compliant services to end users of AmI systems. Section 3 examines how the AmI exploited the healthcare domain to provide an interactive real-time healthcare solution, and Sect. 4 presents the secured cloud-oriented WBAN architecture for healthcare systems. Section 5 provides a patient-centric healthcare framework, and Sect. 6 explores the four important AmI applications in healthcare. Finally, Sect. 7 illustrates how patients are monitored under ambient-based hospital environment.

2 Supporting Technologies for Ambient Intelligence Systems

AmI is an upcoming paradigm which benefited through various disciplines of computing technologies [5]. The main intention of AmI is to elevate an environment by interconnecting sensors and its associated devices via networks. This kind of system can be developed to anticipate the requirements of the users of a concerned environment and take decisions based on real-time data collected. AmI systems inherited the features of sensors, networks, human–computer interface (HCI), pervasive ubiquitous computing, software agent, Internet of things (IoT), and artificial intelligence playing a significant role in AmI systems but none of these technologies cover the full space of AmI. These technological resources work together to offer compliant and intelligent services to the end users in their environments as shown in Fig. 2.

2.1 Sensors

Sensors play a vital role in designing a real-time AmI system and adopting it into the physical environment. The theoretical algorithms will not have any practical use if it is not used as an intelligent agent upon the environment. Therefore, to transform theoretical algorithms into intelligent algorithms, it requires sensory data from the environments. The sensor observes the environments and derives valuable information

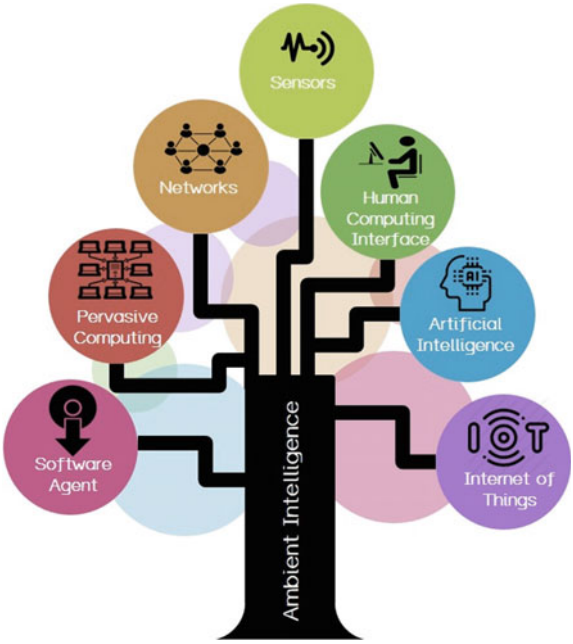


Fig. 2 Ambient intelligence and supporting technologies

using computational capacity. Such derived information is used to take appropriate action for changing the nature of environment. Making of sensor data as an intellectual property is a tedious task. The features of conventional data analysis techniques are inadequate for handling the sensor data due to the generation of a large amount of multidimensional data. The other key challenges in the processing of sensor data are as follows: (i) generation of noisy data due to the usage of imprecise sensors, (ii) missing values may rise upon the failure of sensors, and (iii) variation in spatial and temporal component of sensor data. AmI systems may deploy a centralized or distributed processing model for processing the sensor data. In centralized processing model, data are stored at a central server where the data fusion and data processing happen. In the distributed processing model, each sensor is equipped with processing capability to perform local data processing and communicated to the storage server. The choice of deploying the appropriate model is based on the type of sensor and computational structural design for developing the system. Generally, sensors measure the position [6] and observe temperature, humidity, pressure, noise, and physiological signs of human body [7, 8]. Sensors are characteristically small and can be included in any applications of AmI. Widely used ambient environments and body sensors for monitoring the physiological conditions of the patients are depicted in Table 1.

Table 1 Body and environment sensors used in ambient intelligence systems

Ambient application area	Sensors	Insights	Data rate	Data format
Ambient body sensor	Blood pressure sensor	Used for predicting the rate at which blood propelled in the arteries of the heart	Low	Numeric
	Body temperature sensor	Used for measuring the skin temperature, fever, and hyperthermia	Very low	Numeric
	Electrocardiogram (ECG) sensor	Used for analyzing the muscular function in the heart	High	Numeric
	Electroencephalogram (EEG) sensor	Used for screening and recording the brain activities, dizziness, and sleeping problems	High	Numeric
	Blood glucose sensor	Detects the glucose content in the blood via electrochemical strips on sensors	High	Numeric
	GSR (Galvanic Skin Response) sensor	It analyzes the skin conductance, through which mental stress can be detected	Very low	Numeric
	Pulse oximetry sensors	Used to find oxygen level in the blood	Low	Numeric
	Respiratory rate sensors	It predicts the respiratory diseases by evaluating the inhale and exhale rates of a human	High	Numeric
	Accelerometer	It is being used for assessing the motion of a human body, through which gait and fall can be detected	High	Numeric
Ambient environment sensors	Passive infrared sensor	Detects the motion or identifies the movements in the deployed environment.	High	Categorical
	RFID	Allows keeping track of objects and transmits object information	Low	Categorical

(continued)

Table 1 (continued)

Ambient application area	Sensors	Insights	Data rate	Data format
	Pressure sensor	Assess the pressure applied on tiles, mats, and other objects to detect various conditions of individuals	Low	Numeric
	Ultrasonic sensor	Detects the motion using ultrasonic waves	High	Numeric
	Camera/Microphone	Used for live video and audio streaming in ambient environment	High	Video/Audio

2.2 Networks

The network is the backbone technology for developing any AmI system through which context-based services are provided to the users. Especially, WSN provides a convenient, flexible, and dynamic infrastructure for transmitting data collected from the environment via sensors [9]. The data gathered and transmitted is a major concern for developing and managing the AmI services because the gathered information from the sensors decides the functions to be provided by the AmI systems. In a diversified environment, the WSN transmits the sensor data without any physical connectivity (wirelessly) from one node to other nodes for further processing of data. Meanwhile, the WSN is a combination of assorted of sensor nodes, and few design considerations have to be taken into the context which include power consumption, size of the node, cost, and network complexity. Moreover, while designing WSN, protocol and topology have to be considered in order to simplify the functionality of the nodes with minimum power consumption [9].

2.3 Human–Computing Interface

Human–computing interface is an imperative facet of AmI, because the system uses its intelligence to deduce the situations and users' necessities from the observations of the human assistant. A variety of users may require an interaction with the AmI systems; this can be achieved by integrating the HCI. Further, HCI can be described in two ways: context-aware and natural interface. The recent advancements in context-aware are acting as a vital factor for developing AmI and its related applications. These AmI systems are capable of inferring the current state or activity of the user (i.e., whether the user is sleeping or awake, whether the user is at office or home) and the concerned environment characteristics (i.e., room temperature and humidity).

Therefore, context-aware systems can intelligently maintain the information and its distribution [10]. The intelligence systems tend to reduce the human–computer interaction [11] but natural interface in AmI systems extends service or help immediately by inferring the situations and user's needs from the direct interaction with them. For example, an implanted blood glucose sensor on a human body continuously senses the glucose content in the blood and transmits the data to inference engine, where the system decides the required action or event to be fired. In case of low glucose content, it notifies the user or medical practitioners for further treatments. Moreover, HCI can be defined as an interface technology which develops a perceptive computing environment neither depends on user input nor active input. According to ISUI [12], HCI can be any of the following five classes:

- visual recognition (physical appearance),
- sound recognition (voice, music),
- smell recognition (aroma, odor),
- tactile recognition, and
- sensing technologies.

2.4 Pervasive Computing

Pervasive computing becomes a unified technology which is implemented on a distributed network and integrated intangibly into objects for supporting the user tasks. The systems have to support the dynamic nature of the users and various user contexts. Hence, the development of complex and error-prone systems needs support of pervasive computing that reduces the complexity by offering a bundle of supporting tasks. Some of the important functionalities of pervasive computing are as follows:

(a) Non-Constraint Remote Interaction: Pervasive computing is considered to be user-centric, because it helps real-time environment to achieve the specified task by using natural interaction patterns. For example, recognition of human activities, this avoids the physical intervention and makes use of real-time patterns for exploiting the task.
(b) Context Management: The basic objective of pervasive computing is to offer proactive and self-sustained environment which requires knowledge and decision-making capability. This vision can be accomplished by effective context manipulation.
(c) Application Transformation: Application building is another important functionality of pervasive computing. Only through application building complex computational logics come to reality. The high degree of heterogeneity and dynamic nature of AmI system transforms the application for accomplishing a difficult task.

For example, the pervasive systems in healthcare computing environment are articulated with sensors, microcontroller, actuators, and communication systems for

sensing, transmitting, and processing the health-related information. Thus, it transforms the existing objects in the environment as new or improves the existing objects using the ambient intelligence, which allows tasks to be carried out in non-obtrusive way.

2.5 Artificial Intelligence

Artificial intelligence can be considered as a well-recognized research domain which is being adopted for the improvement of ambient and smart environment applications. Artificial intelligence plays a predominant role in designing expert systems, through which it has gained significant learning outcomes [13]. AmI systems employ various artificial intelligence techniques for providing quality services and deploying AmI in the network interconnected smart environments. The implementation of artificial intelligence in AmI systems is highly beneficial when it is applied in the environment where the human involvement is not advisable. The AmI systems developed under AI concept must accurately forecast the scenario and act accordingly. Such kind of intelligent systems must have abilities like (a) learn, prioritize, and identify the desires of users; (b) accurate diagnosis of situations; (c) conscious on events applicability; and (d) offer an organized way to evaluate and react to situations in the environment.

2.6 Software Agent

A software agent is a self-governing program entity, which cooperates with environment and other external agents throughout its life cycle. AmI applications can be developed using agents by incorporating context awareness elements like places, devices, services, users, and activities. The important properties of software agents applicable to AmI applications are as follows:

- Autonomy: Software agent allows the AmI systems to work without direct human intervention and also have some control over their process.
- Persistence: The functionality of agent will run throughout the life cycle until the fulfillment of the user's desires.
- Reactive: It observes the concerned environment and reacts according to the dynamic nature of the environment.
- Communication Ability: These agents are able to cooperate with other external agents through another appropriate software agent.

2.7 Internet of Things

IoT can be visualized as aplenty of assorted objects communicating with humans and surroundings. Those objects are intended to sense the presence of users, activities, and behavior, and analyze the data using intelligent algorithms for effective decision-making [14]. IoT is one of the exhilarating research phenomena, which predominantly allows the human–computer interaction when it comes under real-time cases. It has been identified that there is an absence in understanding how IoT is supporting the ambient intelligence systems. The Internet of things (IoT) is a perpetrating technology which accelerated the growth of AmI with the emergence of simplified sensors that can be effortlessly incorporated in the environment. Each of which is assigned with the capacity of sensing the environmental factors and responding to particular conditions or events based on the typical situations. Hence, IoT has gained more importance with the facility of embedding the tiny sensors in everyday objects. This kind of tiny sensor is bounded with computational capabilities and also it can easily communicate to the Internet. Likewise, multiple domain features are extended to access the tiny sensors, actuators and generate data for controlling and performing under various contexts. As a result, AmI is identified as one of the major fields that integrate the IoT technology for bringing advancements in the lifestyle and society. Therefore, the success rate of any AmI systems depends on the effective combination of IoT technology in terms of sensor, devices integration, and data management techniques [15].

3 Emergence of Ambient Intelligence in Healthcare Delivery

Nowadays, well-developed countries are experiencing difficulties in providing quality healthcare services, and cost incurred in accessing the healthcare services is high. This will continue to worsen due to increased aging inhabitants, which exacerbate the various chronic diseases and made a remarkable demand for healthcare services. As a consequence, the cost of healthcare services is not feasible and so the developed countries tend to focus on identifying the suitable strategies for using the healthcare resources effectively. In specific, the improvements in ICT exploited the autonomous and beneficial healthcare services. The advancements in wireless sensors networks revolutionized the provision of feasible healthcare services through embedded monitoring systems [16, 17]. AmI systems have gained the potentiality to improve the healthcare services dramatically. In general, it can be utilized for remote monitoring of individuals or people with diseases, and it also can provide assistance in daily activities. Ultimately, AmI technology can support the rehabilitation with advanced monitoring tools and effective communication, which allows the people to lead a healthy lifestyle. A deeper insight about the universal environmental and healthcare

Table 2 Universal challenges and ambient-based solutions

Universal health challenge	Requirements	Existing systems	Ambient-based solutions
Posttreatment care, recovery and activity monitoring, and chronic disease management	Physiological vital signs measurements, activity, and sleep assessment	Manual observations, feedback, or survey measurements	Remote and continuous activity monitoring using pervasive sensing and intelligent mining
Aging population care and fall detection	Autonomous assessment of fall detection	Clinical interpretations with emergency push buttons	Automatic fall detection and balancing using the wearable sensors
Rehabilitation monitoring	Assisted living and performance monitoring	Clinical observations	Remote monitoring using sensing approach and performance measuring
Parental and baby care	Continuous monitoring	Discomfort sensor usage due to clunky issue	Issue resolved by miniaturization of sensors and embedded into clothing
Environment monitoring	Detecting environment changes via continued monitoring	Automatic satellite image analysis	Adoption of sensors in environment and event detection using intelligent computing

challenges and the role of sensors in providing ambient-based solutions is discussed in Table 2.

Various healthcare service providing entities and their AmI relationship are depicted as a mind map in Fig. 3, and also it is explained in a structured approach in terms of AmI in healthcare.

3.1 Medical Information Systems

A medical information system is a storage system which digitally stores the medical images, information and treatment history of patients as an electronic health record (EHR). Such records can be accessed by the authorized individuals like hospitals, practitioners, and insurance agents. Thus, it improves the healthcare record maintenance procedure and reduces the cost involved in it. Ambient intelligence systems made the EHR available anywhere anytime [18]. Data from any kind of sensor-enabled diagnostic devices will direct to the EHR through communication technologies. In the case of unavailability of network communication, the data gets stored provisionally in the same device until communications are available. Based

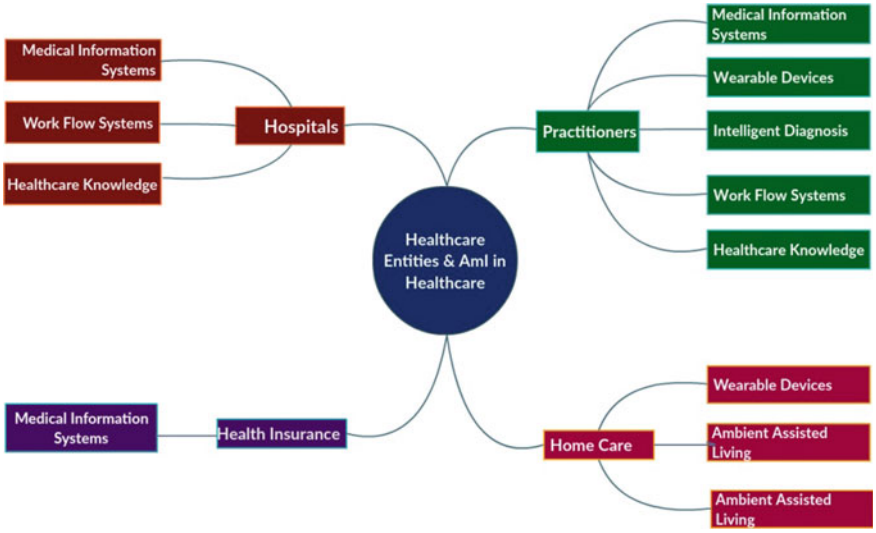


Fig. 3 Mind map of healthcare entities and AmI in healthcare

on the patterns and semantics, the records are categorized and stored, which enables the practitioners to take an effective decision.

3.2 Wearable Devices

Wearable devices with physiological sensors can be coherently be integrated into clothing or any kind of wearable (pendants, wristbands, and earrings) for collecting the health data. The textile sensors can finely integrate into clothing, and these sensors can record the physiological vital signs like pulse rate, ECG, oxygen saturation, and movements [19]. Enabling communication technology between the wearable devices and data centers, the transmission of data to the HER will occur. Thus, it forms the basis of ambient core system. In modest case, when the devices identify that the physiological parameters are beyond the predefined constraints, the system alerts the situation to the concerned individuals or groups. The main intention of adopting AmI into wearables is not only to sense and detect the abnormal physiological conditions of patients but for intelligently trigger the counteractions with the support of actuators. For example, an ambient-based glucose monitoring system was proposed in [20], which can offer a curative injection and relieve the patients from emotional stress. In designing ambient wearable devices, interoperability will be a major issue that will affect the consistent data transmission between wearables and software agents. To overcome this drawback, challenges like patient's identity, data accuracy, reproducibility, and device diversity have to be resolved [21].

Table 3 Comparison on existing AAL use cases

Existing AAL use cases	Retaining elders connected with caregiver	Self-monitoring of health parameters	Integrated with environment and controlled via actuators	Increased mobility	E-Pill box facility
Health at home [23]	Yes	Yes	No	No	No
Remote [24]	Yes	Yes	No	No	No
Clockwork [25]	Yes	No	Yes	No	No
WeCare [26]	No	No	No	Yes	Yes
Persona [27]	Yes	No	Yes	No	No
ReAAL [28]	Yes	Yes	Yes	No	No

3.3 Ambient Assisted Living (AAL)

Initially ambient assisted living has been developed to improve the life quality of elder inhabitants in the following aspects [22]: (i) enables elders with increased mobility and to live autonomously in a satisfied and secured environment, (ii) offers self-monitoring of their health parameters and (iii) keeps them connected with the caregivers via designated tools and networks. AAL allows people with chronic disease or aged people to live independently. AAL systems continuously monitor the health condition of the individuals at home. Likewise, medical practitioners ubiquitously access the health status of the individuals at anytime and anywhere. AAL is enhancing the quality of life with the following objective: (i) assisting the elderly people to live independently, (ii) helping people to remain socially interactive, (iii) identifying and managing the chronic conditions of individuals, (iv) helping elderly people be more mobile, (v) supporting daily activities, and (vi) helping the elderly lead dignified life. AAL has motivated the researchers to develop outstanding solutions for elderly needs and the various developed cases of AAL is compared in Table 3.

3.4 Health Knowledge

AmI systems cannot be fructified without proper knowledge representations and systems, which form the basis for reasoning, intelligent decision-making, and other ambient technologies. Certainly, conventional techniques such as knowledge representations, machine learning, and expert systems are predominantly explored in the development of healthcare applications. These applications are oriented on knowledge systems which can allow doctors, medical staff, surgeons, and pharmacists to

perform a specific task with the logical inference provided by the expert systems. By default, these systems contain the databases of various diseases, symptoms, treatments, drug delivery, and so on. Efficient expert systems cannot be designed with insufficient knowledge. Machine learning techniques can be used for analyzing the clinical data which provides the logical knowledge about a particular case and that will be updated in the knowledge database. In future, updated knowledge may be in high demand for the designing of expert medical system.

3.5 Intelligent Diagnosis

The gathering of health data through sensing technology is impractical to accelerate any kind of medical reactions. It needs an automatic intelligent system for detecting the signs of ailment and for disease diagnosis. In [29], the scientists presented an intelligent system that automatically diagnoses common child ailment conditions by intelligent processing of clinical records. The facility of intelligent disease diagnosis in ambient system will allow practitioners diagnosis of disease at the earliest.

3.6 Work Flow Process

Optimizing the tasks involved in clinical processes is another important area, which reduces the consumption of resources involved. A workflow is a representation of a particular process that can be processed by an intelligent system. The purpose of AmI is to provide a collection of services proactively based upon the current scenario. For example, the ambient system automatically updates the basic vital sign information of the patient into the EHR within the periodic interval of timings. This will successively reduce the time consumed for medical staff to do these types of repetitive tasks.

4 Role of Wireless Body Area Networks in Healthcare AmI Systems

In this section, the infrastructure and technologies of wireless body area network (WBAN) used in AmI healthcare systems are discussed. The appearance of wireless networks and the size reduction of sensing devices have resulted in the improvement of WBAN. The sensors are implanted under human skin or integrated on wearable objects. The innovation and practical enhancement of WBAN applications enables the continuous monitoring of health factors, which includes ECG, pulse rate, temperature, blood glucose, oxygen saturation, and so on [30]. In AmI healthcare systems,

WBANs offer the infrastructures for handling the streaming data and transmitting the data to practitioner's site for real-time diagnosis. WBAN in healthcare applications is certainly used for obtaining the physiological signals via sensors, which can be processed for acquiring reliable and precise healthcare estimations. At the same time, WBAN technologies have certain characteristics [31]: (i) energy consumption, miniaturization of sensor devices, standard protocols, patient-centric regulation, and simplified WBAN integration; (ii) encrypted sensitive healthcare data transmission; (iii) task migration from one node to another node during node failure; (iv) less error-prone data transmission and reception; (v) mobility, scalability, self-organization, and interoperability support; and (vi) reduced computational complexities for real-time processing.

In WSN, arrangements of sensor nodes are predefined by topological structures and the nodes are commonly organized using the star and mesh topological structure. Likewise, WBAN will also adopt the topological structures used in WSN. Every node in WBAN is self-battery powered that has to consume less amount of energy and to provide longer lifetime for each node. These two constraints are managed by using appropriate communication technologies like Bluetooth, Wi-Fi, and ZigBee. These are the low-cost short-range communication technologies used commonly in healthcare monitoring and controlling applications. The important aspect of AmI systems is context-aware decision-making capability which solely depends upon the data aggregated (physiological and body postures sensory data) from the WSNs or WBANs. The aggregated data decides how the intelligent systems can proactively interact with the environment. Table 4 depicts the various factors of WBAN-based healthcare applications.

Next, secured cloud-oriented ambient WBAN architecture is revealed in Fig. 4. It consists of three layers: (i) data generation layer, (ii) data aggregation and processing, and (iii) cloud-oriented data storage and access. Data generation layer constitutes the sensor integrated body area network and patient care environment, which consistently senses the vital signs from the patients and transmits the health data to next higher level layer where data aggregation and processing is done using local server or gateways. Finally, the collected health data are eventually stored in the cloud using EHR format. This cloud-oriented data storage enables the remote access of patient's health data and a novel algorithm has been proposed in Table 5 for encrypted transmission of data over WBAN. This layer is highly vulnerable to security attacks, and hence, the following factors must be considered for ensuring the security of data stored on cloud: (i) confidentiality, (ii) reliability, (iii) cleanness, and (iv) availability. To address the abovementioned factors, an algorithm has been proposed. This proposed algorithm can be deployed on cloud for secured data transmission between the medical practitioner and patients. The algorithm uses biometric multimodal modalities for authentication purpose, which offers tight security for the data stored in cloud, and this can be considered as a salient feature of this algorithm. The working procedure of the algorithm is as follows:

Table 4 Comparison of WBAN healthcare applications

WBAN-based healthcare projects	Deployed environment	Use case	Routing topology	Inter-WBAN communication	Intra-WBAN communication
Nonobstructive body area network [32]	Hospital and residential monitoring	Identifying the movements and postures and to raise alarms	Star topology	Wireless	Internet
Low-cost body inertial-sensing network [33]	Hospital	Gather three-degree posture orientation data from wearable inertial-sensing nodes	Mesh topology	Bluetooth	Wi-Fi
Medisn [34]	Hospital specific wireless sensor network	Medical emergency identification	Point–point and mesh topology	Wired	ZigBee
Lobin [35]	Hospital	Physiological parameters monitoring and patient's location tracking	Star topology	N/A	Wi-Fi
Life minder [36]	Home care	Analyze and identify the stress of an individual	Mesh topology	Bluetooth	Bluetooth
SMART [37]	Hospital waiting room	Monitors the patients in hospital waiting room	Star topology	Wired	IEEE 802.11 b
CareNET [38]	Remote health monitoring	Activity and fall detection	Multi-hop	N/A	ZigBee

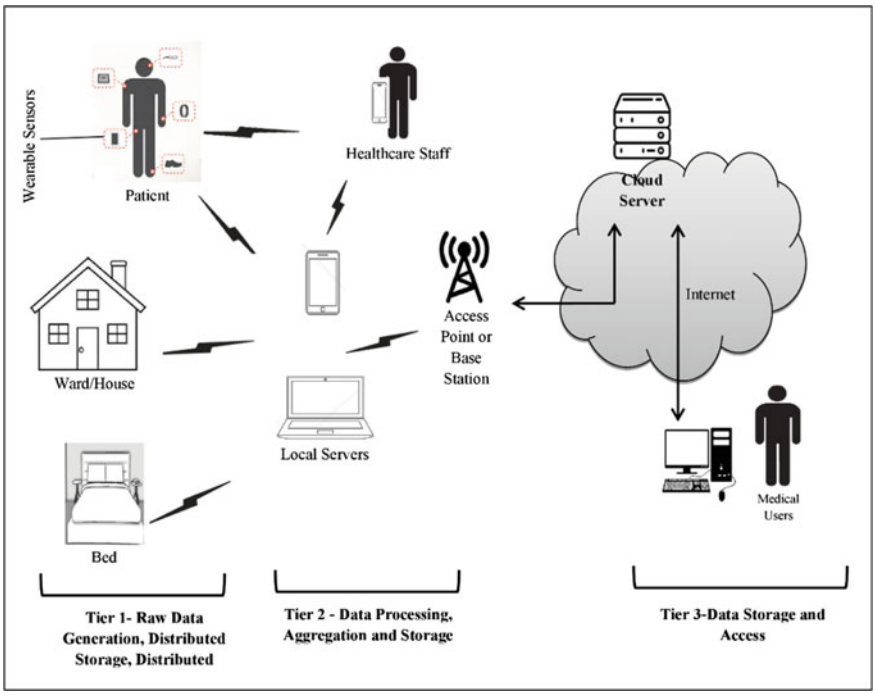


Fig. 4 Secured cloud-oriented ambient WBAN architecture

1. Initially practitioner validation is carried out (*practitioner_req = TRUE*).
2. Then, the practitioner gets authenticated using biometric multimodal modalities (*prac_biomultimodalties_pattern = prac_biomultimodalties_send)*. Where *prac_biomultimodalties_pattern* is the biometric multimodal modalities pattern of practitioner stored at cloud and *prac_biomultimodalties_send* is the biometric multimodal modalities of practitioner sent while issuing request. If the authentication is failed, the practitioners' request gets declined (*decline_prac_req*).
3. Next, the patients' physiological parameters are encrypted using Advanced Encryption Standard (AES) [39] with salt function to avoid data tampering during transmission, and this algorithm can work effectively in ambient-based healthcare systems. It stores the data in the cloud for future analysis (*Transmit the enc[i] &patient_biomultimodalties_send to cloud)*.
4. The stored data made available to the practitioners for analysis and data were decrypted using the secret key immediately upon the authentication using patient's biometric multimodal modalities (*patient_ biomultimodalties_send = patient_biomultimodalties_pattern)*. Here *prac_biomultimodalties_pattern* is the biometric multimodal modalities pattern of patient stored at cloud, and *patient_ biomultimodalties_send* is the biometric multimodal modalities of patient sent while issuing data access request.

Table 5 Secured cloud-oriented ambient WBAN algorithm

1.	**Initiate**
	Procedure: Physiological Parameters Encryption and Transmission
2.	**if** *practitioner_req=TRUE* **then**
3.	**if** *prac_biomultimodalties_pattern=prac_biomultimodalties_send* **then**
4.	**for** i=1 to n **do**
5.	*x[i]=patients physiological parameters measured*
6.	*encry[i]=encryption of x[i] using AES with SALT_Fun*
7.	**end for**
8.	*Transmit the enc[i] &patient_biomultimodalties_send to cloud*
9.	**else**
10.	*decline_prac_req*
11.	**end if**
12.	**else**
13.	*Transmit physiological parameters at regular time intervals*
14.	**end if**
15.	Procedure: Physiological Parameters Decryption
16.	**if** *patient_biomultimodalties_send=patient_biomultimodalties_pattern* **then**
17.	**for** i=1 to n**do**
18.	*decry[i]=encry[i] decryption using secret key*
19.	**end for**
20.	**else**
21.	*Data Mismatch*
22.	**end if**
23.	**Terminate**

5 Patient-Centric Ambient Healthcare Framework

The main purpose of ambient is to monitor the health and environment, which enhances elderly fall detection, activity recognition and monitoring, and connecting doctors and patients. Some of the identified major use cases of AmI systems are as follows: (i) home-based health monitoring (extracts the elderly physiological parameters and anomaly detection, (ii) notifications (reminds the user regarding the scheduled tasks or supervision of practitioners), (iii) information extraction using context and case-based reasoning, and (iv) behavior and activity pattern analysis (detect the anomaly and generate alerts). The communication between the end user and the framework should be realized to be dedicated and customizable. Table 6 depicts the difference between the traditional healthcare systems and the proposed system.

This section presents the proposed theoretical framework for AmI-based healthcare systems (shown in Fig. 5) with respect to the above specified use cases and end user requirements. Various components of this framework are illustrated below.

Table 6 Comparison of traditional healthcare systems and proposed patient-centric ambient healthcare framework

Traditional healthcare system	Proposed patient-centric ambient healthcare framework
Data are generated manually by direct consultation of medical practitioners	Data are machine generated without any human interaction, which enables continuous data collection
Practitioners offer the intervention during patient visit	Due to continuous monitoring of patient status, timely information is gathered and actions are triggered
Clinics and hospitals are centric points for providing healthcare	Considers patients as a centric point and offers healthcare services anywhere and anytime
Do not focus on aging population and patient with chronic diseases	Highly focuses on population and patient with chronic diseases
No guarantee for quality of service and safety	Increased quality of service and safety

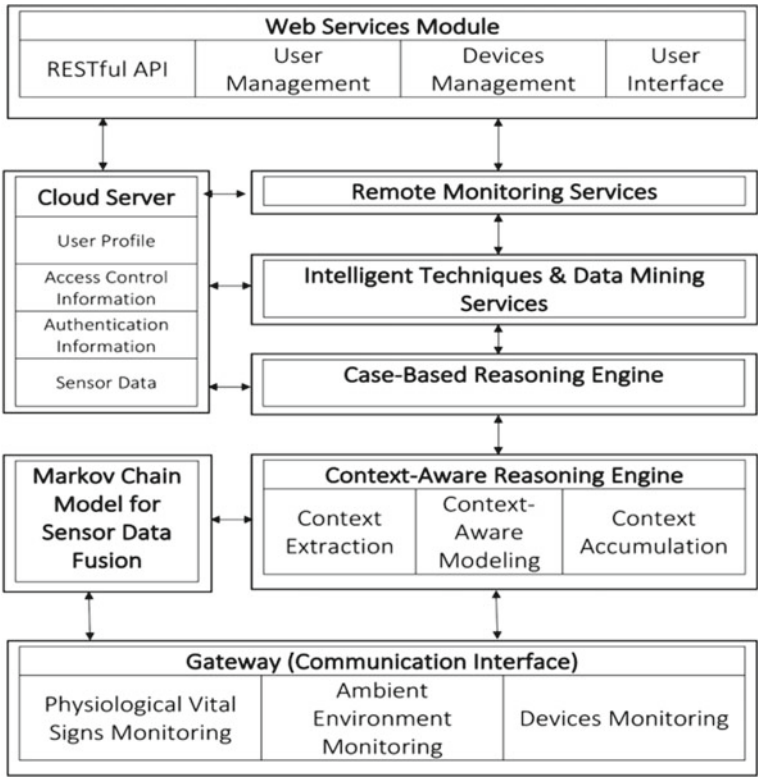


Fig. 5 Patient-centric ambient healthcare framework

5.1 Sensing and Communication

In the patient-centric sensing scenario, three different sensing modules have been included for achieving high degree of efficiency in AmI-based healthcare systems. The first module consists of body sensors whose function is to measure the vital signs and the second module incorporates ambient sensors which measures the environmental factors. The third module is object monitoring, which monitors and controls the functions of devices in that concerned environment. WSNs and WBANs principles as discussed in Sect. 4 can be used for sensor deployment, for gathering the information about the patients and their environments. The system gathers the data from the sensors, then the software agent lies in the gateway transmits the data to cloud storage through which it can be accessed remotely under distributed environment.

5.2 Context-Aware Reasoning Engine

Context can be any data/information which is used for describing the situation of entities in an environment. Context-Aware computing is a process using the contexts for providing the significant information and services to the end users targeted toward the particular user's needs. Context-Aware modeling offers the appropriate contexts for extending intelligent services. This methodology contains three major stages: (i) context information extraction, (ii) context-aware modeling and (iii) context accumulation as shown in Fig. 6. During the first stage, sensor data from $\{sd_1, sd_2, \ldots sd_m\}$ are gathered and the various contexts are extracted $\{ce_1, ce_2, \ldots ce_n\}$ using various preprocessing, data synchronization, and feature extraction techniques. The extracted context denotes the information about the user that is extracted from sensory data. For example, extracting the activities of the patient from the movement sensory data, in which each context information is denoted in the form of (n^c), where it can be numerical or categorical.

Next stage, context-aware modeling is considered as a core logical stage for context-aware reasoning. In this stage, context-aware modeling is accomplished using the context information extracted in the first stage, i.e., walking, standing, lying, and running. Based on the context values, the gathered sensory data are segregated and a context-aware reasoning model (rm^c) is built using the concerned context value (rn^c). For example, the model for activity "standing" will be built using the respective data values that contain "standing". Likewise, the same approach is followed for building each of the extracted contexts. In the final stage, the testing data for every context are accumulated and the decision is made.

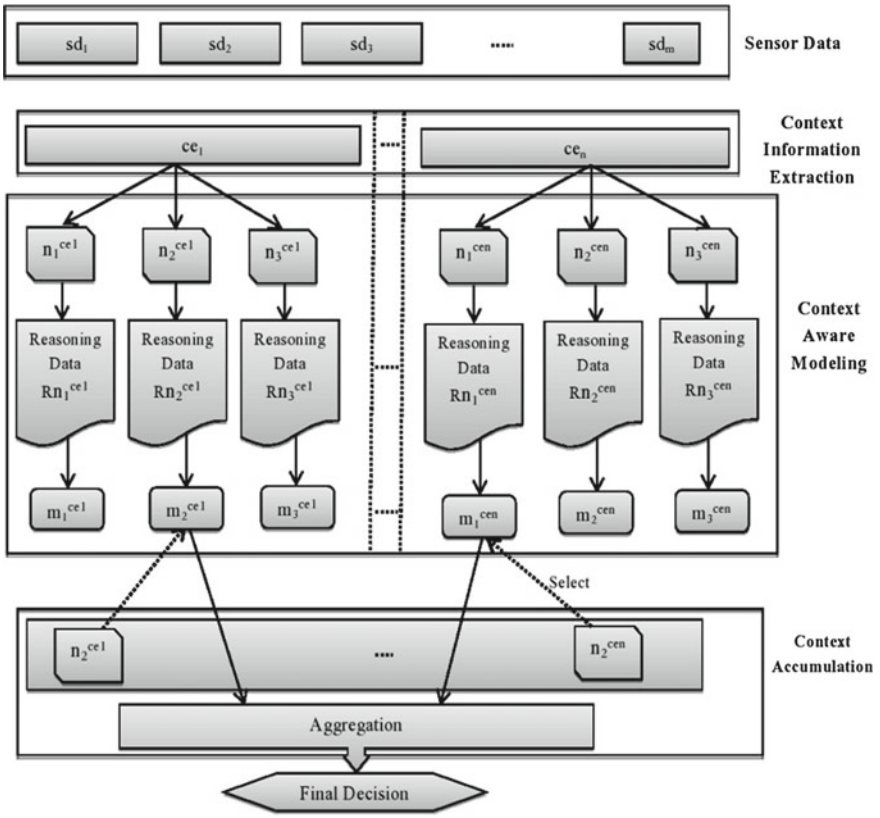


Fig. 6 Context-aware reasoning engine

5.3 Case-Based Reasoning Engine

Case-based reasoning will able to provide solution for new problems using the learning from past experiences or using the solutions of similar problems. This engine consists of three features: (i) problem statement, (ii) a solution set which can be applied to solve the problem, and (iii) a state reached when solution from a solution set was applied. Case-based reasoning manages the new incoming cases based on the experiences, which has four consecutive phases as shown in Fig. 7. The first phase initiated immediately upon the reception of new problem statement, and similar case descriptions are retrieved from the case storage using algorithms. Once the similar cases are gathered, the reuse phase identifies the optimal solution for the present problem. Then revise phase makes use of expert knowledge to modify the optimal solution proposed. In the final phase, the experiences learned during the other three phases are updated in the case storage.

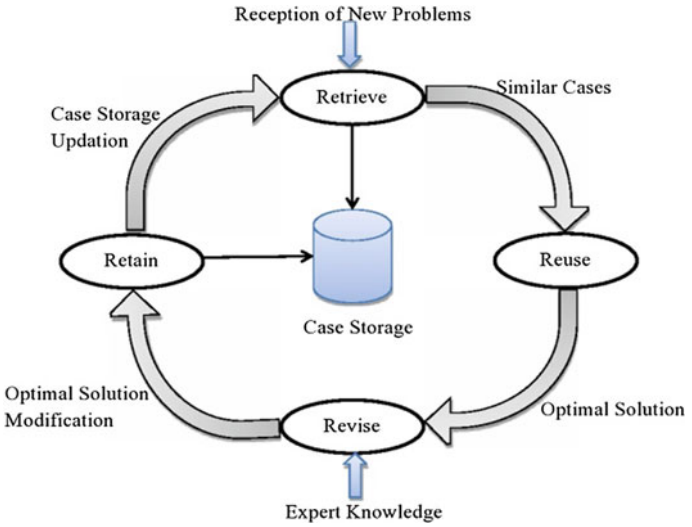


Fig. 7 Case-based reasoning cycle

5.4 Intelligent Techniques and Data Mining Services

During the sensor data analytics, AmI systems need a distributed or centralized model for extracting the high-level information [40]. From the ambient environment, the sensors transmit the data to a cloud server, where data fusion and inference operations take place. But in a few cases, each sensor node is facilitated with computational capacity which does the local computation partially. Considering both these cases, sensory data have to be analyzed for extracting the useful insights accurately. There are many artificial intelligence and data mining techniques utilized for analyzing the sensor data from ambient environment. Moreover, it is identified in the context-aware applications, classification, real-time predictions, and decision-making using various machine learning algorithms in remote and ambient-based healthcare systems [41, 42].

5.5 Cloud Server Storage and Data Management

The acquired raw sensor data, user profile, rules drawn from the context, and case-based modeling are stored in the cloud using the software agents. The real-time sensor data are published through the application running on the gateway; hence, the medical practitioners or caregivers can remotely communicate with the patients. On the server side, the sensory data are converted to generic XML format, which can be easily recognized by any web-based script or by reasoning engines for further

processing. User profile is a storage repository that takes control of maintaining the personal information, authentication information, and access control information.

5.6 Sensory Data Fusion Using Markov Chain Model

AmI is expected to provide the context-aware or case-based services, by manipulating the large amount of sensory data which are deployed in various environments [41]. At this juncture, AmI application must precisely infer the context of current situation, with the capability of handling the large amount of sensory data. Since these data are acquired from discrete sensors, it may be noisy and erroneous. To deal with this issue, the probabilistic techniques have to be adopted with this framework. In literature, to cope with uncertainty, Bayesian network was used as a probabilistic technique but it suffered from the drawback, which was well suited for deploying in static environment. Hence, it could not be used for AmI-based system due to its dynamic nature [42]. In this framework, Markov chain is used for inferring the useful knowledge for a given situational feature from the gathered set of sensory data. Each situational feature can be directly affected by the sensor data, and each of the sensor nodes is denoted by the notation sn^i, which can be considered as an acceptable sensor data manifestation of particular situation. The probable relationship between the current situation and its sensor data manifestation is given by $P(\boldsymbol{sn}_t^i|\boldsymbol{m}_t)$. Likewise, the current situation will directly continent on the historical situations as per the transition probability $P(\boldsymbol{m}_t|\boldsymbol{m}_{t-1})$. The value of a situational attribute will be a conditional probability which considers the historical situations and the set of sensory observation from starting time to the current time. Hence, the current situation is the determined from the historical situations and current situational observations and its simplified form can be written as (Eq. 1):

$$\begin{aligned}(\boldsymbol{m}_t) &= \boldsymbol{P}(\boldsymbol{m}_t|\boldsymbol{m}_0, \ldots, \boldsymbol{m}_{t-1}, \boldsymbol{sn}_0^0, \boldsymbol{sn}_0^1, \ldots, \boldsymbol{sn}_t^i) \\ &= \boldsymbol{P}(\boldsymbol{m}_t|\boldsymbol{m}_{t-1}, \boldsymbol{sn}_t^0, \boldsymbol{sn}_0^1, \ldots, \boldsymbol{sn}_t^i)\end{aligned} \tag{1}$$

By performing factorization on simplified (m_t), the following form is obtained (Eq. 2):

$$Fact(\boldsymbol{m}_t) = \eta\Big[\sum P(\boldsymbol{m}_t|\boldsymbol{m}_{t-1})(\boldsymbol{m}_{t-1})\Big]\big[\pi_i P(\boldsymbol{sn}_t^i|\boldsymbol{m}_t)\big] \tag{2}$$

This factorized function will be used at each situation, and it is mandatory to consider a noiseless reduced set of sensory data as shown in Fig. 8. The probable comparison of current situational feature with the historical features is expected to eliminate the noises. This procedure can be adapted to any AmI-based healthcare system during the designing phase which is targeted to achieve the effective performance of any system.

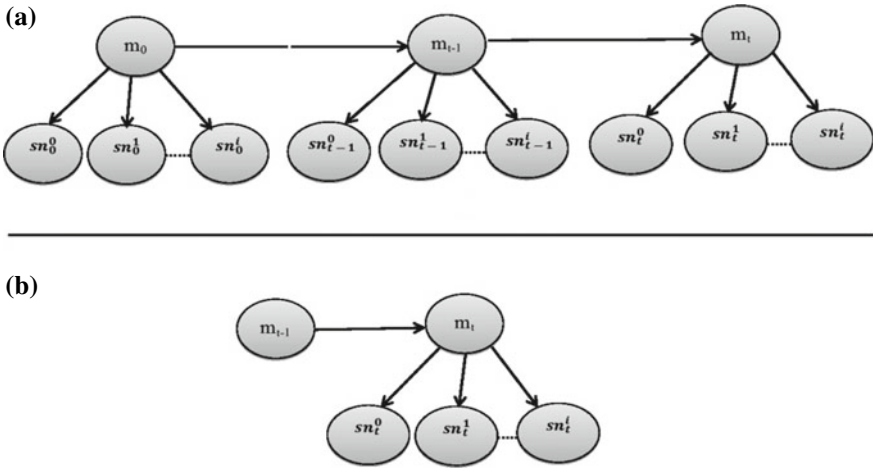


Fig. 8 Markov Chain model for situational feature extraction

5.7 Web Services Module

The various components of the framework are integrated using RESTful web services, which is a suitable platform for defining and implementing a shared Application Programming Interface (API). This can be considered as a software web agent that allows the flow of data from distributed ambient sensors to the framework. The gateway receives the sensory data and then converts into protocol defined format before letting into transmission. The communication protocols that are implemented within the gateway can autonomously decode the measurements or generate the measurement events using RESTful web services. The following use cases are supported by the web interface functionalities:

(i) User Management: The account management is performed by medical staff or caregivers. This web platform allows configuring the associates of one or more medical staff with an individual, through which their information can be viewed and maintained.
(ii) Device Management: The dedicated sensory devices used by individuals are integrated into the framework via a unique addressing scheme (physical or logical address) and the sensory data mapped with the corresponding individual profile.
(iii) Medical Profile: Provides user interface for accessing the treatment history of every individual via web services.

The identified key testing scopes for analyzing the architecture performance is depicted in Table 7 and after the successful implementation of these testing strategies, performing cost best analysis may become sensible [43].

Table 7 Testing scopes for IoT system components

IoT system components	Testing scopes
Sensors	Device hardware
	Embedded software
	Sensor response time and performance
Application	Application functionality
	Error handling mechanism
	User-friendliness
	User roles and access levels
Communication	Multiple request handling
	Network connectivity
	Interaction among devices
	Frequency of data transmission
	Data packet loss
	Data security—data encryption and decryption
Data storage	Data consistency and integrity validation
	Verification of data values

6 Major Applications of AmI in Healthcare

AmI systems aimed at delivering intelligent services and creating the environment as much dedicated to us. In this section, three major AmI-based healthcare applications are discussed.

6.1 Uninterrupted Health Status Monitoring

In the current decade, various noninvasive sensors are being developed for monitoring the physiological parameters likes ECG, EEG, glucose, heartbeat, and so on. These sensors are embedded in wearable devices like wristwatches, bands, and textiles. Regardless of monitoring healthy subjects, such sensors are used for monitoring the vital signs of patients with chronic diseases and also are highly useful in post-treatment monitoring. Typically, anomalous conditions of patients can be detected via continuous monitoring and enriching the human lifestyle.

6.2 Activity Recognition

It is viewed as an important application area of ambient systems, which are able to perceive the state of an individual that extracts valuable information and fed as input for other medical systems. Such systems deduce the activities of the individuals from embedded sensor units on wrists, chest, thighs, and ankles. The most common application of activity recognition is fall detection and gait monitoring, which becomes more effective while applying machine learning algorithms for sensory data analytics. Especially, elderly people residing individually at home can be benefitted by an automatic fall detection and alerting mechanism.

6.3 Human Stress and Energy Expenditure Assessment

This application continuously assesses the stress level and the amount of energy used by a person. Commonly, heartbeat rate, GSR, and pressure sensors embedded wearable devices are used for data acquisition and the machine learning algorithms analyze the gathered data. Few important ambient-based healthcare applications are presented in Table 8.

7 Illustration Case—Ambient Assisted Care (AAC) at Hospital

Let us assume a hospital room, where a patient must be monitored continuously in order to predict their recovery rate and also to diagnosis the severity of the disease. In Sect. 5.2, the various elements of context-aware reasoning have been described and this section elaborates the different example contexts with respect to patient and hospital environment. Additionally, this section classifies the various activities of patients after treatment using machine learning algorithms and deduces the best classification model for fitting into the scenario. Some of the example contexts (in which contexts are referred to as c_1, c_2, …c_n) are as follows:

c_1 Leaving the patients unattended during emergency.
c_2 Not able to press the emergency button.
c_3 Continuously physiological vital signs of patients signifying the abnormal condition.
c_4 Not taking the pills at expected time.
c_5 Not going to toilet within a periodic gap.
c_6 Frequently going to toilet and patient not returning from the toilet within a reasonable periodic timing.
c_7 Lack of sleep at nights.
c_8 Detecting the trips status and intimating the medicals staff.

Table 8 Ambient healthcare applications

Type of applications	Objective	Ambient sensors	Physiological sensors	Techniques
Continuous health monitoring	Measures the physiological parameters using sensor networks	Compulsory	Optional	Activity recognition
Emotional health monitoring	Analyze the psychological parameters and identify the emotional condition of individuals	Compulsory	Compulsory	
Behavioral monitoring	Monitors the human behaviors like cooking, eating, and sleeping using sensor networks	Compulsory	Compulsory	
Emergency detection	Detecting falls, health hazards using sensor networks	Optional	Compulsory	
Persuasive health systems	System assists the persons to lead a healthy life	Compulsory	Not required	Activity recognition and decision support systems
Rehabilitation and therapy	Provide remote services for the people who require therapy and treatment regularly	Optional	Compulsory	

c_9 Detectors identifies the person entering into the room.
c_{10} Gait monitoring during various daily activities after surgery

These varieties of contexts can directly impose the interaction rules at right situation with accurate reactions. Hence, contexts and interaction rules must be framed in such a way that can be understood and processed by computers. Generally, the rules for contexts may have characteristic format according to the active databases [44]:

ON event-occurs IF condition THEN execute-action.

Whenever an event-occurs is perceived with certain condition holds, then execute-action is implemented. AAC systems depend on smart hospital environment facilitated with various types of sensors to gather information about the patients and for

keeping them under medical surveillance. Some of the example rules r_i for anomaly detection in healthcare environment are depicted below:

r_1 If (activity is patient not able to press the emergency button) and (heartbeat rate is high) then context is abnormal.
r_2 If (activity is too much urinating) and (blood glucose is very high) then context is abnormal

In AAC system, the sensors are deployed in the smart hospital environment for collecting the events. The events are further analyzed by context-aware engine for extraction of context of the patients. Here ontologies and simple UML class diagram are used for representing the events, contexts, and its interactions for hospital scenarios. Ontological represents the smart hospital structures, events, and contexts for describing the functionalities in computational systems. Figure 9 illustrates the view of smart hospital ontology Smart_Hosp_Onto as a UML model, which includes rooms, hospital elements, and sensors.

Figure 10 depicts the smart hospital events and contexts using ontological representations Event_At_Hospital and Context_Derivation. Two concepts are presented, initially, events are represented which include the sensors, deployed location, associated element, and value generated on event establishment. There will be a specific event for every sensor deployed in Event_At_Hospital. The represented events are generated by the movement sensors and heartbeat rate sensors in Event_At_Hospital. The Fall_Eve and HeatRate_Eve events are obtained from the movement sensors and

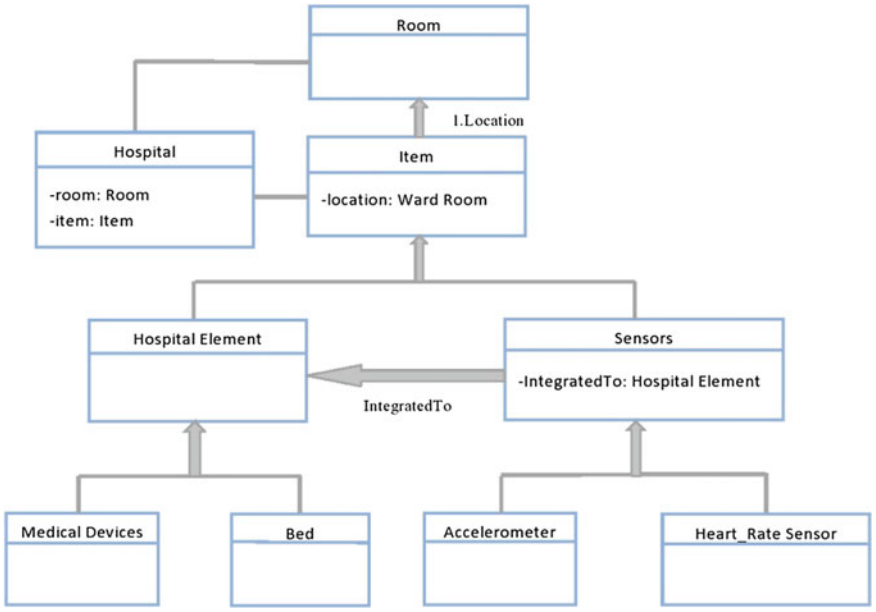


Fig. 9 Smart hospital ontology Smart_Hosp_Onto

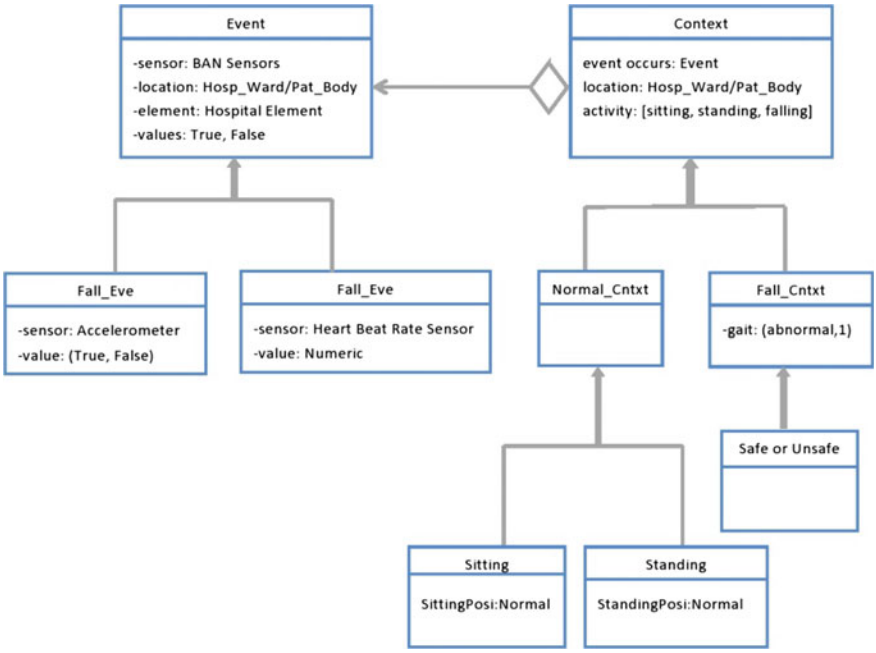


Fig. 10 Smart hospital events and contexts

heartbeat rate sensor. Each of the events has a unique event ID, through which particular context can be derived. The value for Fall_Eve is indicated as Boolean type either TRUE or FALSE, and the HeartRate_Eve is denoted by numerical type.

Then, Context_Derivation represents the current situational context of the patient. Every value of an event associated with a context and also it specifies the location and activity of patients. In this scenario, the context has two different types: Normal_Cntxt and Fall_Cntxt. From the various combinations of events, the system deduces the normal conditions of patients that include sitting, walking, and standing. On the other hand, Fall_Cntxt represents the situation of patient falling during gait analysis, and also, the context has been further classified into safe or unsafe state, which denotes whether the patient might have in emergency situation or not.

8 Conclusion and Future Scope

This chapter highlights many essential components of AmI and the role of AmI in healthcare. In order to develop an efficient AmI-based healthcare application cloud-oriented secured WBAN architecture, algorithm for secure data transmission and a patient-centric healthcare framework is presented. This chapter illustrates the various events, contexts, and rules related to hospital scenario with the help of UML class

diagram notations. However, attaining the estimated goal in AmI-based healthcare systems is still challenging and researchers have to work toward different issues associated with human-to-machine interactions, intelligent decision-making, implementing, automating, and security. Ambient technologies have not been applied into the healthcare applications and are in its infancy state.

In future, AmI-based healthcare systems require a more reliable software engineering and testing framework. A non-erroneous context extraction engine to predict the meaningful events and to match appropriate rules for corresponding event is needed. An ambient system to be designed for assisting and monitoring the handicapped people and also to anticipate their various needs is required. A self-controlled ambient system to detect the sensible situation and to provide high level of intervention for intensive care unit must be achieved. Several technical challenges like reliability, scalability, security, energy optimization, and dynamic networking have to be focused for strengthening the AmI systems. Device and sensor miniaturization to be developed further to reduce the sensor node power consumption at a reasonable cost. In future, seamless connectivity and data security will be considered as thrust areas and improved further.

References

1. Acampora, G., Cook, D. J., Rashidi, P., & Vasilakos, A. V. (2013). A survey on ambient intelligence in healthcare. *Proceedings of the IEEE, 101*(12), 2470–2494.
2. Cook, D., Augusto, J., & Jakkula, V. (2009). Ambient intelligence: Technologies, applications, and opportunities. *Pervasive Mobile Computing, 5*(4), 277–298.
3. Milosevic, M., Shrove, M. T., & Jovanov, E. (2011). Applications of smartphones for ubiquitous health monitoring and wellbeing management. *Journal of Information Technology and Aplication, 1*(1), 7–14.
4. Kameas, A., & Calemis, I. (2010). Pervasive systems in health care. In H. Nakashima, H. Aghajan, & J. C. Augusto (Eds.), *Handbook of ambient intelligence and smart environments* (p. 315). New York, NY, USA: Springer.
5. ST Advisory Group. The European Union report, scenarios for ambient intelligence in 2010.
6. Wolffenbuttel, R. F., Mahmoud, K. M., & Regtien, P. L. (1990). Compliant capacitive wrist sensor for use in industrial robots. *IEEE Transactions on Instrumentation and Measurements, 39,* 991–997.
7. Ermes, M., Parkka, J., Mantyjarvi, J., & Korhonen, I. (2008). Detection of daily activities and sports with wearable sensors in controlled and uncontrolled contitions. *IEEE Transactions on Information Technology in Biomedicine, 12,* 20–26.
8. Stanford, V. (2004). Biosignals offer potential for direct interfaces and health monitoring. *IEEE Pervasive Computing, 3,* 99–103.
9. Dey, N., & Ashour, A. S. (2017). Ambient Intelligence in healthcare: a state-of-the-art. Global Journal of Computer Science and Technology.
10. Orr, R. J., & Abowd, G. D. (2000). The smart floor: A mechanism for natural user identification and tracking. In CHI'00 extended abstracts on Human factors in computing systems (pp. 275–276). ACM.
11. Dix, A., Finlay, J., Abowd, G. D., Beale, R. (2003). Human computer interaction, 3rd ed., Prentice Hall.

12. Raisinghani, M., Benoit, A., Ding, J., Gomez, M., Gupta, K., Gusila, V., Power, D., & Schmedding, O. (2006). Ambient intelligence: Changing forms of human-computer interaction and their social implications. Journal of Digital Information, 5(4).
13. Augusto, J. C., Nugent, C. D. (2006). Smart homes can be smarter (pp. 1–15). Springer.
14. Elhayatmy, G., Dey, N., &Ashour, A. S. (2018). Internet of Things based wireless body area network in healthcare. In Internet of Things and Big Data Analytics Toward Next-Generation Intelligence (pp. 3–20). Springer, Cham.
15. Dey, N., Hassanien, A. E., Bhatt, C., Ashour, A., & Satapathy, S. C. (Eds.). (2018). *Internet of things and big data analytics toward next-generation intelligence*. Berlin: Springer.
16. Black, J. P., Segmuller, W., Cohen, N., Leiba, B., Misra, A., Ebling, M. R., Stern, E. (2004). Proceedings of the MobiSys 2004 Workshop on Context Awareness. Boston: 2004. Jun, Pervasive computing in health care: Smart spaces and enterprise information systems.
17. Bhatt, C., Dey, N., & Ashour, A. S. (Eds.) (2017). Internet of things and big data technologies for next generation healthcare.
18. Chiarugi, F., Zacharioudakis, G., Tsiknakis, M., & Thestrup, J. (2006). Ambient intelligence support for tomorrow's health care: the eu-domain platform. In The International Special Topic Conference on Information Technology in Biomedicine.
19. Kim, Y., & Wang, H. (2014). Textile-Based Body Sensor Networks and Biomedical Computing for Healthcare Applications. In X. Tao (Ed.), *Handbook of Smart Textiles*. Singapore: Springer.
20. Jung, C. A., & Lee, S. J. (2016). Design of automatic insulin injection system with Continuous Glucose Monitoring (CGM) signals. In 2016 IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI),Vegas, NV (pp. 102–105).
21. The role of wearable technology in healthcare interoperability. Journal of eHealth. Retrieved 10 February from https://thejournalofmhealth.com/the-role-of-wearable-technology-in-healthcare-interoperability/.
22. Active and assisted living programme. Retrieved January 2019 from http://www.aal-europe.eu/.
23. Culmone, R., Falcioni, M., Giuliodori, P., Merelli, E., Orru, A., Quadrini, M. (2014). AAL domain ontology for event-based human activity recognition. In 2014 IEEE/ASME 10th International Conference on Mechatronic and Embedded Systems and Applications (MESA), Senigallia (pp. 1–6).
24. Bekiaris, A., Mourouzis, A., & Maglaveras, N. (2011). The REMOTEAAL project: Remote health and social care for independent living of isolated elderly with chronic conditions. In International Conference on Universal Access in Human-Computer Interaction, Context Diversity, Lecture Notes in Computer Science (Vol. 6767, pp. 131–140). Springer, Berlin, Heidelberg.
25. Active and assisted living programme projects. Retrieved January 2019 from http://www.aal-europe.eu/our-projects/.
26. Alemdar, H. O., & Ersoy, C. (2010). WeCare: Wireless enhanced healthcare. In Mediterranean Conference on Medical and Biological Engineering and Computing (Vol. 29, pp. 855–858). Springer, Berlin, Heidelberg.
27. Tazari, M. R., Furfari, F., Ramos, J. P. L., Ferro, E. (2010). The PER-SONA service platform for AAL spaces, In Handbook of Ambient Intelligence and Smart Environments, Springer, pp 1171–1199. https://doi.org/10.1007/978-0-387-93808-0-43.
28. ReAAL. Retrieved January 2019 from http://www.cip-reaal.eu/home/.
29. Dey, N., Ashour, A. S., Shi, F., Fong, S. J., & Tavares, J. M. R. (2018). Medical cyber-physical systems: A survey. *Journal of Medical Systems, 42*(4), 74.
30. Dey, N., Ashour, A. S., Shi, F., Fong, S. J., & Sherratt, R. S. (2017). Developing residential wireless sensor networks for ECG healthcare monitoring. *IEEE Transactions on Consumer Electronics, 63*(4), 442–449.
31. Goswami, S., Roy, P., Dey, N., &Chakraborty, S. (2016). Wireless body area networks combined with mobile cloud computing in healthcare: A survey. In Classification and Clustering in Biomedical Signal Processing (pp. 388–402). IGI Global.
32. Felisberto, F., Costa, N., Fdez-Riverola, F., & Pereira, A. (2012). Unobstructive body area networks (BAN) for efficient movement monitoring. *Sensors, 12*(9), 12473–12488.

33. Guo, Y. W., Wu, D., Liu, G. Z., Zhao, G. R., Huang, B. Y., & Wang, L. (2012). A low-cost body inertial-sensing network for practical gait discrimination of hemiplegia patients. *Telemedicine and eHealth, 18*(10), 748–754.
34. Ko, J., Lim, J. H., Chen et al. (2010). MEDiSN: Medical emergency detection in sensor networks. ACM Transactions on Embedded Computing Systems, 10(1), article 11.
35. Custodio, V., Herrera, F. J., Lopez, G., & Moreno, J. I. (2012). A review on architectures and communications technologies for wearable health-monitoring systems. *Sensors, 12*(10), 13907–13946.
36. Khan, R. A., & Khan Pathan, A.-S. (2018). The state-of-the-art wireless body area sensor networks: A survey. International Journal of Distributed Sensor Networks.
37. Curtis, D., Shih, E., Waterman, J., Guttag, J., Bailey, J. et al. (2008). Physiological signal monitoring in the waiting areas of an emergency room. In Proceedings of BodyNets 2008. Tempe, Arizona, USA.
38. Jiang, S., Cao, Y., Iyengar, S., Kuryloski, P., Jafari, R., Xue, Y., Bajcsy, R., Wicker, S. (2008). CareNet: an integrated wireless sensor networking environment for remote healthcare. In Proceedings of International Conference on Body Area Networks. Tempe, Arizona.
39. Ruan, X. (2014). Building blocks of the security and management engine. In Platform embedded security technology revealed. Apress, Berkeley, CA.
40. Kleinberger, T., Becker, M., Ras, E., Holzinger, A., & Müller, P. (2007). *Ambient intelligence in assisted living: Enable elderly people to handle future interfaces* (pp. 103–112). Part II, HCII: InUniversal Access in HCI.
41. Cornacchia, M., Ozcan, K., Zheng, Y., & Velipasalar, S. (2017). A survey on activity detection and classification usingwearable sensors. *IEEE Sensors J., 17,* 386–403.
42. Yao, S., Swetha, P., & Zhu, Y. (2018). Nanomaterial-Enabled wearable sensors for healthcare. *Advanced Healthcare Material, 7,* 1700889.
43. Karthick, G. S.,, & Pankajavalli, P. B.,. (2019). Internet of things testing framework, automation, challenges, solutions and practices: A connected approach for IoT Applications. In D. Mala (Ed.), Integrating the Internet of things into software engineering practices (pp. 87–124). Hershey, PA: IGI Global. https://doi.org/10.4018/978-1-5225-7790-4.
44. Augusto, J. C., & Nugent, C. D. (2004, August). The use of temporal reasoning and management of complex events in smart homes. In Proceedings of the 16th European Conference on Artificial Intelligence, Amsterdam, The Netherlands (pp. 778–782). IOS Press.

Design of Optimization Based Network Lifetime Enhancement Technique

Evolutionary Algorithms for Coverage and Connectivity Problems in Wireless Sensor Networks: A Study

Subash Harizan and Pratyay Kuila

Abstract Coverage and connectivity play a vital role in the performance and proper functioning of wireless sensor networks (WSNs). Proper deployment of the sensor nodes has strong impact on proper functioning of the network. Moreover, it can further reduce energy consumption of the networks. It is noteworthy that the sensor nodes have limited sensing and communication range. Moreover, energy source of the sensor nodes is also limited. Therefore, it is very challenging to maintain desired coverage and connectivity in the network. Furthermore, the sensor nodes are prone to failure. Hence, the target/region must be covered by sufficient number of sensor nodes to avoid damages due to failure of one or more sensor nodes. This is also essential for connectivity too. Nowadays, evolutionary algorithms become the center of attraction among the researchers to solve the different optimization problems in the WSN. This chapter aims to study and analyze the various evolutionary approaches like genetic algorithm (GA), particle swarm optimization (PSO), ant colony optimization (ACO), etc. which are applied to solve the coverage and connectivity problems for WSN. The existing approaches are described with suitable illustration. Moreover, this chapter has highlighted few research challenges related to coverage and connectivity of WSNs.

Keywords Evolutionary algorithms · Coverage · Connectivity · Wireless sensor networks

1 Introduction

Nowadays, wireless sensor networks (WSNs) become more popular for the advancement in the microelectromechanical systems [1]. WSNs consist of large number of

S. Harizan · P. Kuila (✉)
Department of Computer Science & Engineering, National Institute of Technology Sikkim, South Sikkim 737139, India
e-mail: pratyay_kuila@yahoo.com

S. Harizan
e-mail: subashharizan@gmail.com

S. K. Das et al. (eds.), *Design Frameworks for Wireless Networks*,
Lecture Notes in Networks and Systems 82,
https://doi.org/10.1007/978-981-13-9574-1_11

tiny sensor nodes deployed randomly or deterministically to monitor the field of interest (FoI). Sensor node is a multifunctional device that consists of sensing unit, processing unit, storage unit, communication unit, power unit, mobilize, etc. Sensor nodes have ability to sense the target or phenomenon that occurs within its sensing range, process the sensory data, and transmits it to the base station directly or through multi-hop [2–4].

In WSNs, quality of service (QoS) is also measured by the coverage and connectivity. Coverage is defined as how well the point/area is covered or monitored by the sensor nodes in the place where it is deployed. Point/area is said to be covered or monitored if it is within the sensing range of the sensor nodes. Similarly, connectivity is also very crucial for the transmission of sensed data to the base station. Two sensor nodes are said to be connected if they are within the communication range of each other and there must exist a path from each sensor node to the base station. A simple WSN scenario for target coverage is given in Fig. 1. The sensor nodes have limited sensing and communication range and power source, and hence it is a very challenging issue to use this resource efficiently.

Optimal placement of sensor nodes with coverage and connectivity is an NP-hard problem [5, 6]. Therefore, it is very challenging issue to provide desired coverage and connectivity with minimum number of sensor nodes. Optimal deployment strategy of the sensor nodes has a great impact on the WSNs. There are mainly two types of deployment scheme in WSNs: preplanned and random. Preplanned deployment is preferable for the area which is accessible and this approach also provides the better network management with saving in cost and energy. On the other hand, random deployment scheme is used for the harsh environment where monitoring area is not accessible or human intervention is not possible.

Evolution of the species by Charles Darwin inspires the development of evolutionary algorithms (EAs) in order to solve the real-life applications. EAs are population-based approach where population consists of member of solutions which can explore the search space in each iteration to obtain the optimal solutions. Nowadays, evolutionary algorithms draw the attention of the researchers in order to optimize the

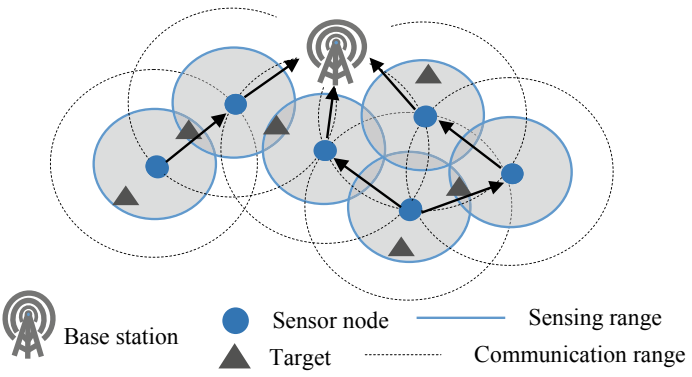


Fig. 1 A simple network scenario of target-based WSN with coverage and connectivity

different optimization problems of the WSNs [7]. Compared to other algorithms EAs are found to have better results. There are many EAs which are applied to WSN to optimize different issues related to coverage and connectivity and found to be effective. In this chapter, we have studied and provided a deep analysis of the existing EAs that are employed for the coverage and connectivity problems of WSNs. Finally, we have also provided research challenges and open issues in this domain.

2 Sensing and Communication Model

From literature, two facts about the sensing device can be observed. First one states that as the distance increases the sensing ability decreases. Second, sensing ability gets improved as the noise reduces. Mainly, two types of sensing models can be found in literature based on the detection probability, (i) binary disk-sensing model and (ii) probabilistic sensing model.

2.1 Binary Sensing Model

The sensing ability is constant in this model as the sensing range is assumed as circular disk of radius R_s known as sensing range. According to this model, an event/point/region is said to be sensed by a node if it lies within its sensing radius (R_s). Let us consider, (x_i, y_i) and (x_p, y_p) are the location of sensor node s_i and any point p in the area of interest and $d(p, s_i)$ be the Euclidean distance between p and s_i. The point p is said to be covered by s_i in binary disk-sensing model if the following equation (Eq. 1) holds:

$$C(p, s_i) = \begin{cases} 1, \text{ if}(p, s_i) \leq R_S \\ 0, \text{ Otherwise} \end{cases} \tag{1}$$

2.2 Probabilistic Sensing Model

The binary disk-sensing model is extended with more actual perception known as probabilistic sensing model. Probabilistic sensing model is given by following equation (Eq. 2):

$$C(p, s_i) = \begin{cases} 1, & \text{if } d(p, s_i) \leq R_S + R_e \\ -e^{\alpha\beta^{\lambda}} & \text{if } R_S - R_e < d(p, s_i) < R_S + R_e \\ 0, & \text{if } d(p, s_i) \geq R_S + R_e \end{cases} \tag{2}$$

where uncertainty detection of the sensor nodes is defined by R_e ($R_e < R_s$), α, β, and γ are the detection probability at distance less than or equal to R_S and $\beta = d(p, s_i) - (R_s - R_e)$. Equation 2 depicts that, a point is said to be covered if it lies within a distance $(R_s - R_e)$ from a sensor node, coverage diminishes exponentially as the distance between points and the sensor nodes increases if points are lying within an interval $(R_s - R_e, R_s + R_e)$. The points lying beyond distance $(R_s + R_e)$ are said to be uncovered. In a network, it may be possible that a point might be covered by multiple (k) sensor nodes then a point is known as k-covered.

2.3 Communication Model

The simplest communication model which is mostly found in the literature is binary disk model. Like the sensing range (R_S), communication range (R_C) is defined as the range up to which it can communicate with other nodes. Based on the transmission power level, different sensor nodes have different communication range. Two sensor nodes can communicate with each other if they are within the R_C.

3 Coverage and Connectivity

A reliable quality of service and management of resource are the two most important requirements that must be provided in WSNs. There are many factors that are needed to be considered while planning for coverage and connectivity in WSNs. Most of the WSNs are application specific. An efficient node deployment strategy would reduce the computation, cost, and communication overhead and simultaneously provide a high degree of coverage and maintain a global connectivity in a network which is nontrivial due to hostile environment conditions and severe resource constraint. In spite of failure of some nodes in a network, it is important to provide coverage along with connectivity so that network can be operational.

3.1 Coverage

An area/point is said to be covered or monitored by a sensor node if an area/point is within the sensing range of one or more active sensor nodes. Coverage can be classified depending on what exactly you are interested in monitoring. Coverage can be classified as follows.

3.1.1 Area Coverage

In area coverage, the main objective is to cover or monitor the region of interest where each point of region has to be covered. On the basis of application, area coverage is classified into partial coverage and full coverage.

In partial coverage, the area is partially covered which can ensure the desired degree of coverage sufficient and acceptable for the required applications. In partial coverage, nodes are deployed in such a manner that it will cover p percentage of total area known as p-coverage. Partial coverage saves the energy cost of the sensor nodes and simultaneously increase the network lifetime. It requires fewer numbers of sensor nodes than the full area coverage. For example, environment monitoring (like to calculate the temperature of particular region and forest fire detection during rainy season only 80% coverage of area is sufficient).

Full coverage of area is required when we need to cover or monitor entire area. In full coverage, every point of interest in a network area is covered by at least one (1) or more than one sensor nodes. To obtain a full coverage of an area is most expensive since it requires more number of sensor nodes. Degree of coverage is defined according to requirements of applications. In some application, simple coverage is required where each point of region is covered by at least one sensor node. Similarly, in multiple coverage each point of region is covered by at least k number of sensor nodes where ($k > 1$). In multiple coverage, network remains functional by ($k - 1$) nodes in spite of failure of a sensor node but in simple coverage it is not possible.

3.1.2 Point Coverage

In many applications, it is sufficient to cover or monitor the specific points of interest in the application area. Here, deployment cost is less since it requires less number of sensor nodes to monitor or cover the points of interest.

3.1.3 Barrier Coverage

In barrier coverage, nodes are deployed in such a manner that it will form a barrier in a specific path and transmit the information if they sense possible activities made by intruder to cross the barrier. Barrier coverage is applicable to make boundaries of the critical assets or infrastructure, such as country borders, coastal lines, boundaries of battlefields, and many more.

3.1.4 Sweep Coverage

In sweep coverage, it is sufficient to cover some points of interest periodically such that coverage or monitoring of points of interest is time variant. The point of interest

remains covered or monitor till the coverage period is guaranteed. Therefore, we can cover or monitor large number of point of interest with minimum number of mobile sensor nodes. It is not desirable to apply traditional work under static coverage to sweep coverage which results in poor performance and unnecessary extra overhead.

3.2 Connectivity

Connectivity is one of the vital issues for the transmission of sensed data to base station to take the necessary action. Network within a defined area is said to be connected if each deployed sensor node has at least one connected neighbor node. Data gathered or sensed by the sensor nodes need to be transmitted to the sink node or base station [8–10] by single hop or multi-hop. If a sensor node communicates directly with the base station for data transmission, then it is called a single-hop communication. In multi-hop communication, sensed data is transmitted to the base station via other intermediate sensor nodes [11–16]. Thus, WSN has great impact on connectivity because failure of any link among the sensor nodes may lead to the failure of communication in the network. If a WSN has single connectivity among the sensor nodes then it is called simple connectivity or 1-connectivity. Failure of any single node in such scenario may result in the communication failure in network. Whereas in k-connectivity, in spite of failure of a node, network remains connected by $(k - 1)$ number of sensor nodes.

4 Evolutionary Algorithms for Coverage and Connectivity

Evolutionary algorithms (EAs) are based on the evolutions of the species which is mainly inspired by the theory proposed by Charles Darwin. There are several methods by which mechanism of evolution can be implemented. EAs are generally designed for the optimization problem where main objective is to find out optimal solution from a large solution space. The steps of the EAs are as follows. Initially, a population is created with a number of individuals or solutions that are randomly generated. The individuals compete with each other for the survival. Survival of an individual is decided by its fitness. Individuals with higher degree of fitness have more chance to survive than the individuals with lower degree of fitness. Evolution processes are carried by the selection, reproduction, mutation, and recombination and survival of fittest. The EAs that have been employed for the coverage and connectivity problems for WSNs are studied below.

4.1 Genetic Algorithm

Genetic algorithm (GA) [17–21] is a population-based optimization algorithm inspired by Darwin's theory of evolution. Initially, a population of chromosomes or individuals is generated randomly. Each chromosome or solution is evaluated on the basis of the derived fitness function. The genetic operations, selection, crossover, and mutation are applied to evolve the better solutions from the population. In selection phase, different solutions or chromosomes are selected from population. Different selection methods are there like roulette wheel, tournament, rank, etc. Selection phase is followed by crossover operation, where selected parent chromosomes exchange their information to generate new child offspring chromosomes. There are various types of crossover operation, like one-point crossover, two-point crossover, uniform crossover, etc. Finally, diversity in the population is achieved by the mutation operation.

Gupta et al. [22] proposed a GA-based approach to deploy relay nodes in a WSN to provide the k-connectivity to the pre-deployed sensor nodes. Here, main objective is to select minimum number of potential positions to place the relay nodes such that they can ensure the k-connectivity to pre-deployed sensor nodes.

Chromosome length is considered the same as the number of sensor nodes and its corresponding gene value represents the relay nodes. Figure 2 shows a chromosome of length nine, where gene position five has value (6, 2) that represents that the sensor node s_5 is connected with the relay nodes 6 and 2, respectively, to form k-connectivity (here, $k = 2$). Similarly, sensor node s_1 is connected with relay node 1 and 3 and so on. To evaluate the chromosome, fitness function is defined as the minimum number of required relay nodes. Here, the fitness function ensures to provide the desired k-connectivity in the network. Connectivity between the deployed relay nodes is not considered.

Gupta et al. [23] presented a GA-based scheme to cover target points with minimum number of sensor nodes. Here, authors have considered the following conflicting objectives: (i) placement of minimum number of sensor nodes, (ii) k-coverage of the targets, and (iii) m-connectivity among the deployed sensor nodes. The target is said to be k-covered if it is covered by k number of sensor nodes and similarly a sensor node is said to be m-connected if it is connected to other m number of neighboring sensor nodes. The chromosomes are represented as a binary array of length the same as the number of potential positions in the network. The ith gene position with value one represents a sensor node is placed at ith potential position and zero value implies that position is without sensor node. A chromosome for the network scenario as given in Fig. 3a is represented in Fig. 3b. Here, gene value is one

(1,3)	(4,5)	(2,9)	(8,9)	(6,2)	(3,5)	(6,7)	(7,3)	(1,4)
s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9

Fig. 2 A chromosome representation [22]

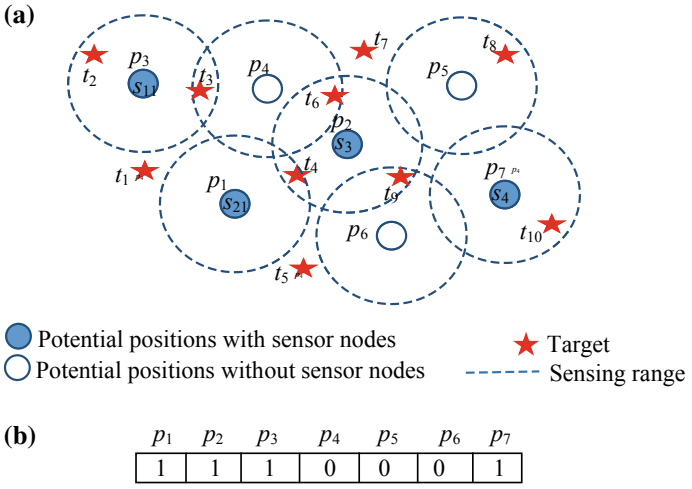


Fig. 3 **a** A simple network scenario and **b** corresponding chromosome as used in [23]

for positions 1, 2, 3, and 7, i.e., sensor nodes are placed at that potential positions, whereas positions 4, 5, and 6 are without sensor nodes as its gene value is 0.

Evaluation of the chromosomes fitness function is formulated considering all the objectives. Authors have used weight sum approach (WSA) to construct a fitness function for the multiple objectives, represented by following equation (Eq. 3):

$$F = w_1 \times (1 - f_1) + w_2 \times f_2 + w_3 \times f_3 \tag{3}$$

where w_1, w_2, and w_3 are the weight value such that $w_1 + w_2 + w_3 = 1$. Here, f_1 be the first objective function which implies the selection of minimum number of potential positions for the placement of sensor nodes. It is calculated as $f_1 = P_m/P_{t,}$ where P_m be the selected potential positions out of total number of potential positions P_t. k-coverage of all the targets is measured by the objective function $f_2 = \frac{1}{T_N \times k} \sum_{i=1}^{T_N} C_{\cos t}(t_i)$, where T_N is the total number of targets and coverage cost of target t_i is $C_{cost}(t_i)$. Third objective is represented by $f_3 = \frac{1}{P_m \times m} \sum_{i=1}^{P_m} CON_{\cos t}(s_i)$, where m is the predefined value for connectivity and $CON_{cost}(s_i)$ is the connectivity cost of the network. The multiple objectives are considered and they are conflicting with each other, and authors have not employed multi-objective EAs.

Rebai et al. [24] proposed a novel GA-based approach to deploy minimum number of sensor nodes to provide the full area coverage with guaranteed connectivity. The area of interest is assumed as an $M \times N$ grid. Each grid crossing point is considered for the placement of the sensor nodes. The length of the chromosomes is represented by the sum of $M + N$. Sensor nodes are placed by choosing the mth and nth gene values where m and n represent the rows and columns of the grid points. In this study, GA is integrated with an offspring correction phase which can repair the invalid chromosomes produced by the crossover operation. Required minimum

number of sensor nodes to provide the coverage of area and connectivity is taken as the fitness function. The mutation phase is also modified. First, in a chromosome, some connected sensor nodes are added and then each node is verified whether its removal affects or does not affect the connectivity. If it does not affect, then these nodes are muted.

Karatas [25] presented a GA-based deployment scheme of the heterogeneous sensor nodes for point and barrier coverage called hybrid coverage. Here, point coverage refers to the coverage of amenities inside the barriers, whereas in barrier coverage intruders are prevented from penetrating the barrier segment. For the coverage scheme, diffuse coverage model is applied. Chromosome represents the locations of the sensor nodes. The problem is expressed as a multi-objective optimization problem and formulated as integer nonlinear program (INLP) and integer linear program (ILP) to find the optimal solutions. Solution provided by the ILP is found to be better than the INLP which selects minimum number of sensor nodes to provide the desired coverage.

We have proposed an improved GA-based energy-efficient scheduling scheme for coverage- and connectivity-related issues in WSNs [21]. Among the densely deployed sensor nodes, a set of sensor nodes is activated by considering the residual energy of each active sensor node. Here, four objectives are considered as follows: activation of minimum number of sensor nodes, ensured full coverage of all the targets, maintain the connectivity among the activated sensor nodes along with base station, and residual energy level of the activated sensor nodes. Residual energy of the active sensor nodes is considered above the defined threshold value while activating the sensor nodes for coverage and connectivity. Chromosomes are represented in efficient way such that it will always produce a valid chromosome after genetic operations like crossover and mutation. Here, length of the chromosomes is taken as total number of sensor nodes deployed in the network. A novel mutation operation is also proposed where the redundant sensor nodes which do not have any role for coverage and connectivity in the network get deactivated.

Here, a novel mutation operation is defined as follows. Let us consider a network scenario with nine sensor nodes (s_1, s_2, …, s_9) and five target points (η_1, η_2, …, η_5) as shown in Fig. 4a. The corresponding chromosome for the scenario is represented in Fig. 4b. Here, for every activated sensor node, it is checked that whether or not the sensor node is participating for coverage and connectivity in the network. The redundant nodes that do not have any role in coverage and connectivity get deactivated. From Fig. 4a, it can be observed that sensor node s_7 does not have any contribution in target coverage and connectivity and thereby it does have effect in network formation. Therefore, in proposed mutation operation, the sensor nodes are deactivated which do not have any contribution in coverage and connectivity. The scenario of network after deactivation of node s_7 with corresponding chromosome is shown in Fig. 5a and b, respectively. Therefore, number of redundant active sensor nodes is reduced by the novel mutation operation.

Yoon and Kim [26] proposed an efficient GA technique for the maximum coverage with node deployment. Here, different types of sensor nodes with varying sensing radius are considered for the deployment. To achieve optimal locations for the sensor

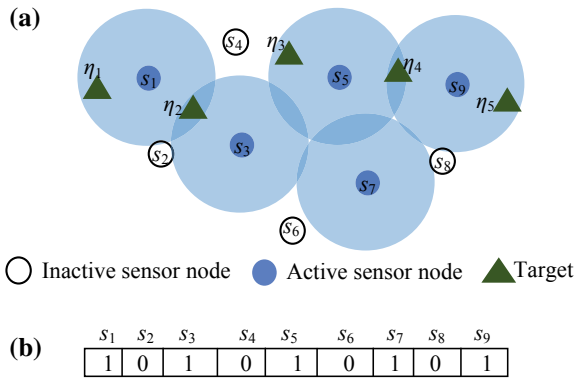


Fig. 4 **a** A network scenario before mutation and **b** corresponding chromosome [21]

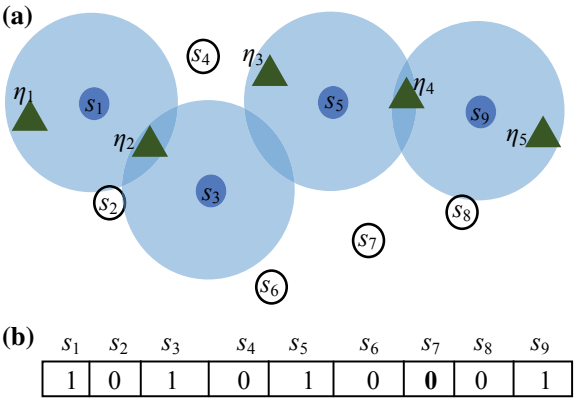


Fig. 5 **a** A network scenario after mutation and **b** corresponding chromosome [21]

nodes to provide the maximum coverage to the network is the main goal of this work. Chromosomes are encoded as a list of coordinate of the sensor nodes as shown in Fig. 6 with three types of sensor nodes. To avoid the redundant representation of the chromosomes, normalization technique is used in this study.

The chromosomes are evaluated using the Monte Carlo method based on the coverage ratio of the network. Three novel normalization methods are applied to increase the performance of the GA. First normalization method is called RAND where second parent is chosen for crossover without rearrangement of the genes value. Second and third normalization method called MINDIST and MAXDIST.

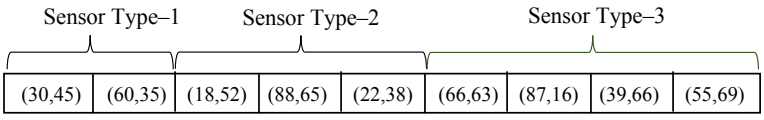


Fig. 6 Representation of a chromosome [26]

Simulation is conducted for all three normalization methods where MINDIST is found to be better in performance.

4.2 Harmony Search Algorithm

Harmony search algorithm (HSA) [27] draws inspiration from improvisation process of musicians to solve the various engineering problems. In this algorithm, we can control the search range and convergence speed. HSA is also a population-based algorithm which consists of following parameters as harmony memory (HM), harmony memory considering rate (HMCR), pitch adjusting rate (PAR), and termination criteria. Initially, population of harmony vectors are randomly generated in HM where each set of harmonies represents the complete solution to the problem. HM is updated by the operators as memory consideration, pitch adjustment, and random consideration. Harmonies are evaluated by the fitness function and HMs are updated by the harmonies with better fitness function. The process is repeated continuously till the termination criterion is achieved.

In [28], authors proposed an HS-based deployment algorithm to maximize the sensing coverage area of a WSN. Here, main objective is to place minimum number of sensor nodes on the optimal location to fulfill the coverage requirement of the network. Both binary and probabilistic sensing model are considered for coverage scheme. The probability of coverage $P_d(S)$ of demand point d lying on the overlap region of a set of sensor nodes S is represented by the given equation (Eq. 4):

$$P_d(S) = 1 - \prod_{s_i \in S} (1 - P_{\text{cov}}(s_i, d)) \tag{4}$$

where $P_{cov}(s_i, d)$ is probability of the demand point d covered by sensor node s_i. A demand point is said to be covered effectively if $P_d(S) > Th$, where Th ($Th = [0, 1]$) is the coverage threshold value. Based on the value of $P_d(S)$, probability of coverage of a demand point is divided into four classes (shown in Fig. 7) as follows:

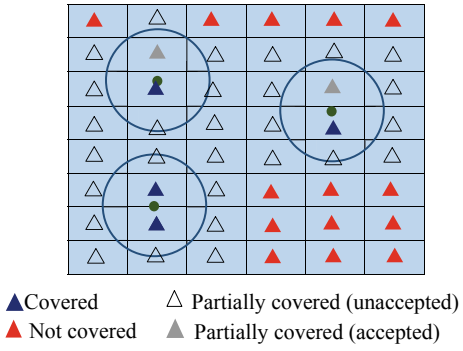


Fig. 7 Coverage representation for binary and probabilistic sensing scheme [29]

1. If $P_d(S) = 1$: demand point is fully covered.
2. If $Th < P_d(S) < 1$: demand point is partially covered (accepted).
3. If $0 < P_d(S) < Th$: demand point is partially covered (unaccepted).
4. If $P_d(S) = 0$: demand point is uncovered.

Variables of harmony memory (HM) are encoded as a location of a sensor node in terms of x and y coordinates with real number. In this study, upper bound and lower bound of the sensing field are considered to avoid the sensor node to waste their energy by residing on the boundary region. The lower bound and upper bound are represented by the following equations:

$$LXs_i = R_s - R_e \tag{5}$$

$$LYs_i = R_s - R_e \tag{6}$$

$$UXs_i = W - (R_s - R_e) \tag{7}$$

$$UYs_i = H - (R_s - R_e) \tag{8}$$

where LXs_i, LYs_i, UXs_i, and UYs_i are the lower and upper boundaries of the X and Y axes. The respective height and width of the network area are given by H and W. Sensing range and uncertainty range of the sensor node are represented as R_S and R_e. The main objective function is given by the following equation (Eq. 9):

$$F = \frac{1}{N} \times R_{\text{cov}} \times D_{\text{min}} \times C \tag{9}$$

Here, number of sensor nodes encrypted in the solution vector is represented by N. Coverage ratio of the network and minimum distance between sensor nodes distributed in the network are denoted by R_{cov} and D_{min} where $R_{cov} = EC_L/N_L$ (EC_L is number of effectively covered locations and N_L is total number of locations in monitor area). To avoid the objective function being zero, a constant value C is used. The solution vectors encoded in the HM are evaluated based on the given objective function itself given in Eq. (9). The proposed algorithm is simulated and compared with the existing algorithms. The obtained results depict that the algorithm selects minimum number of sensor nodes to provide a solution up to 100% of coverage ratio.

Nezhad et al. [30] proposed an improved HS algorithm for the energy-efficient deployment scheme. Main objective is to deploy optimal number of sensor nodes within a specified region such that all the deployed sensor nodes must be connected with each other and hotspot area should be k-covered. Mohamad et al. [31] presented HS-based k-coverage enhancement algorithm (KCEA) to enhance the initial coverage to provide the area of interest with degree of k-coverage. Here main objective is to find the location of the optimal position which can improve the degree as well as

computational cost. First, KCEA divides the area into number of nonuniform grids. Then, coverage status of each grid is determined.

Sharma and Gupta [32] presented an HS-based algorithm to improve the coverage and connectivity in WSN with minimum number of sensor nodes. Here, main objective is to cover the whole area of interest with sensing range and ensured that each sensor node must be within the communication range of at least one sensor node. Here, objective function $F_{objective}$ is defined as follows:

$$F_{objective} = \frac{R_{\text{cov}} \times R_{con} \times d_{\text{min}}}{R_{sen}} \tag{10}$$

where coverage ratio R_{cov} is the ratio between area covered by sensing range to total monitor area, connectivity ratio R_{con} is the ratio between number of connected nodes to the total number of nodes deployed, R_{sen} is defined as the number of sensor nodes deployed to number of sensor node required, and d_{min} is the ratio between the shortest and longest distance between the deployed sensor nodes.

Manjaarres et al. [33] presented an HS algorithm integrated with local search to find the best location of the additional sensor nodes based on the location of anchor nodes which are deployed prior to provide the efficient connectivity. In the network, pre-deployed sensor nodes are referred as anchor nodes and nodes need to be added to make efficient connectivity in the spare network are called non-anchor nodes. The positions of the non-anchor nodes are estimated by minimizing the sum of two objective functions, cost function (CF) and soft constraint violation (SCV). CF is defined as the squared error between the estimated and measured distance between the nodes that are within the range of one another. When there is violation in the neighborhood connectivity, SCV is taken into account. Newly generated vector solutions are evaluated by the function ($CF + SCV$).

4.3 Ant Colony Optimization

Ant colony optimization (ACO) [34] mimics intelligent behavior of ants to solve many real-life optimization problems. This algorithm is inspired by the foraging behavior of real ants which stands as the multi-agents or artificial agents in the algorithm. This behavior allows an ant to explore the search space to find the optimal solution to the problem. During searching for food, ants deposit pheromones on the way from nest to food source. The pheromones are followed by other ants of the colony. Ants can indirectly communicate with each other based on the pheromone trails. This behavior allows them to find the shortest path from nests to food source. Evaporation of phenomenon avoids the local convergence of optimal solutions.

Sun et al. [35] presented an improved ACO that is named as culture algorithm–ant colony algorithm (CA–ACA) to solve the problem of node deployment in grid-based WSNs. Here, the objective is to deploy optimal number of sensor nodes in such a manner that it covers all the required points in the network and maintain the

connectivity among them so that sensed data can be reached to the sink node. Here, culture algorithm is coupled with ACO. Li et al. [36] proposed an improved ACO for the efficient deployment of sensor nodes in WSNs. Here, main objective is to provide the guaranteed connected k-coverage of the point with minimum number of sensor nodes. Modification in conventional ACO is made based on the characteristics of the WSN for the next point selection process and updating process of pheromone. In next point selection process, an ant identifies all the points that are within its communication range and then it will apply stochastic local decision to select the next point. Pheromone is updated based on obtained quality of solution. For the proper operation of the algorithm, practical issues like obstacle detection and routing hop optimization are also considered. Detection of obstacle is designed to guide the ant to reach the desirable solution. The ant with optimal number of sensor nodes is accepted as a solution for the problem. The solution of the proposed algorithm is validated with simulation results.

In [37], an ACO-based approach is presented to solve the minimum cost reliability constraint sensor node deployment problem (MCRC–SDP). Authors define the reliability in terms of coverage and connectivity. Here, objective is to find the minimum nonoverlapping set of sensor nodes which can provide the coverage to all the targets and also maintain the connectivity with each other. A novel ACO is proposed by coupling the conventional ACO with local search heuristic approach.

Huang et al. [38] presented improved ACO sweep coverage (IACOSC) to achieve the coverage of the desired point of interest (POI) and data delivery in the WSN by the mobile sensor nodes. Here the main objective is to schedule minimum number of mobile sensor nodes to obtain dynamic coverage and to deliver the data to the base station (BS). To provide the coverage to all the point of interest, k numbers of mobile nodes are assigned for the P number of paths as shown in Fig. 8. Buffer size of mobile nodes is assumed to have limited size. Initially, artificial ants are used to create the coverage route (starts from the BS and ends to BS). Coverage efficiency is used as fitness function to evaluate the route. Finally, local search algorithm is used to delete the route created and sensor nodes are placed to optimize the route.

Liao et al. [39] proposed an ACO-based deployment algorithm for the full coverage of the monitoring area and prolonged network lifetime. Here, initial energy of

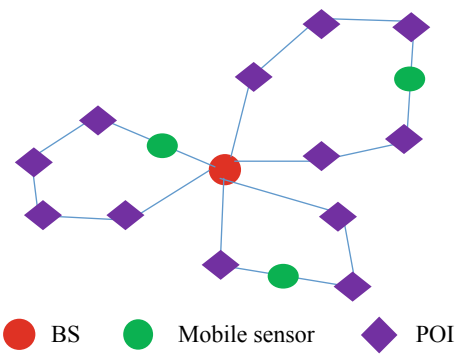


Fig. 8 Sweep coverage with variation in paths [38]

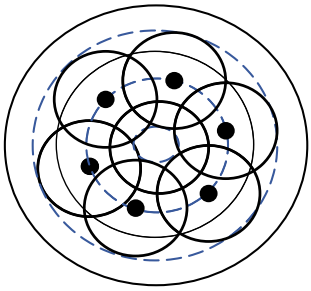


Fig. 9 Deployment scheme with coronas [39]

sensor nodes is considered to be different from each other. To solve this problem, authors virtually divided the network area into a number of coronas as shown in Fig. 9. Further, main corona of width d is subdivided into thinner coronas of width $d/2$ to maintain the coverage and connectivity in the network. Then, sensor nodes placed on any corona C_{i} have connectivity between the sensor nodes that are placed in corona C_{i+1} and C_{i-1}. Here, three methods are introduced to achieve the full coverage and prolonged lifetime by balancing the energy in the network. In the first method, authors computed the minimum average angle between the placed sensor nodes to achieve the full coverage with minimum sensor nodes. In the next two methods, sweep-based scheme and ACO algorithm are used. In sweep-based scheme, sensor nodes are moved as requested to balance the energy in the network, whereas in ACO scheme deployment problem is formulated for the multiple knapsack problem and applied for the deployment of the sensor nodes with prolonged network lifetime.

Liu and He [40] proposed a modified ACO to provide the grid-based coverage scheme with low-cost guaranteed connectivity (GCLC). Here, greedy migration mechanism is coupled with ACO for the movement of the ants to reduce the coverage cost. The algorithm adjusts the sensing and communication range to improve the energy hole problem and also prolong the network lifetime. Main objective is to select the minimum number of grid points to place the sensor nodes such that all the required points of interest should be fully covered. The simulation results of the proposed algorithm show that algorithm provides the low-cost coverage with guaranteed connectivity along with low consumption in energy with respect to other compared algorithms.

Liu [41] proposed a novel ACO with three classes of ant transitions (ACO–TCAT) to solve the problem of minimum cost grid coverage with guaranteed connectivity. In traditional ACO, only one class of ants is used for optimization. Here, three classes of ants are employed to progress the quality of solution space and also increase the searching speed. Three classes of ants increase the effectiveness of the algorithm. Each ant in class one chooses their next point based on the heuristically desirability and probability of the pheromone concentration. In second class, an ant chooses its next point called (point of solution) stochastically from the candidate points (set of points that are within its current position range) and transfer to it. Similar to the second class, the ants in third class select next point stochastically from the candidate

points and transfer it to point of solution. Candidate points of second and third class are different in nature.

Qasim et al. [42] proposed a modified ACO for the efficient deployment of sensor nodes which can reduce the sensing cost along with guaranteed connectivity. Proposed work is executed in two phases. In first phase, traditional ACO is applied for the grid-based coverage scheme with low-cost guaranteed connectivity (GCLC). Sensor nodes are placed in each point visited by the ants to cover PoI during its tour. In second phase, redundant sensor nodes are removed from the solutions of first phase. Only two ants make tour in the network. First ant traverses back from the last sensor nodes toward the sink nodes backward and removes the redundant nodes. While second ant restores the minimum sensor nodes that are necessary for connectivity removed by first ant as some of the redundant nodes are necessary for the connectivity.

4.4 Non-dominated Sorting Genetic Algorithm (NSGA–II)

Non-dominated sorting genetic algorithm–II (NSGA–II) [43] is one of the popular MOEA techniques. NSGA–II utilizes elitism, non-dominating sorting, crowding distance, and comparison operator. It is found to be very effective for solving the multi-objective optimization problem. As in GA, initially a parent population (P_P) is generated with population size, say N. Then offspring population (P_O) of same size as parent (N) is generated from the parent population using the GA operations (selection, crossover, and mutation). In each generation, both the populations are merged together to form a merged population (P_M) of size $2N$. Now, fast non-dominated sorting is applied on the P_M to form the fronts of different levels ($F_1, F_2, F_3, \ldots, F_k$). Thereafter, new population of size N is created for the next generation by adding the chromosomes from top (superior) fronts from the P_M. It may happen that the last front (say F_L) may contain more chromosomes than the required chromosomes to make the new population of size N. Required number of chromosomes are selected from the F_L based on the crowding distance. Here, chromosomes residing in the least crowded regions are preferred. Same process is continued till the termination criteria or acceptable solutions are achieved. The overall computational complexity of the algorithm is $O(mS^2)$, where m is the number of objectives and S is the size of the population.

Mahdi et al. [29] proposed an NSGA–II-based algorithm called TASCC (transmission range adjustment, scheduling, coverage, and connectivity control) to solve the multi-objective scheduling problems for cluster-based WSNs. Here, the considered objectives are maximizing the coverage rate, minimizing the number of active sensor nodes, and minimizing the unbalanced energy consumption with guarantee connectivity. Here, sensor nodes are assumed to be heterogeneous in nature with same sensing range and adjustable transmission range. Network area is assumed to be divided into grids where each grid constitutes the cluster with one cluster head (CH). Cluster formation is done in each round to prolong the network lifetime. CH

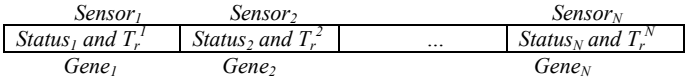


Fig. 10 Representation of a chromosome with status and varying transmission range used in [29]

is responsible for adjusting the communication range and determine the scheduling of sensor nodes by executing the TASCC algorithm. Chromosomes are represented as shown in Fig. 10, where each gene value represents status ($Status_i$) of the sensor nodes (i.e., active or inactive) and transmission range (T_r^i).

Jia et al. [44] proposed NSGA–II-based algorithm to provide the energy-efficient coverage by scheduling the set of sensor nodes. Connectivity is assumed to be ensured by considering the communication range as twice the sensing range. Here, main objective is to select minimum number of sensor nodes among the densely deployed sensor nodes to cover the area. In this work, energy consumption is reduced by keeping only optimal number of sensor nodes in active state while others remain in sleeping state to conserve their energy which results in extended network lifetime. Chromosomes are evaluated by the coverage rate of the network and the number of activated sensor nodes. Simulation results show that proposed algorithm is effective and simultaneously select optimal number of sensor nodes for coverage and connectivity.

Syarif et al. [45] proposed NSGA–II-based deployment strategy of the sensor nodes to full coverage of the targets and also maintain connectivity in the WSN. The fitness function consists of selection of minimum number of sensor nodes within the communication range of each other but not too close to each other. Deployment strategy is optimized by the efficient fitness function during each generation.

El-Sherif et al. [46] proposed NSGA–II-based approach to increase the number of set covers from the densely deployed sensor nodes and maximize the lifetime by minimizing the wastage energy. Covers are defined as the set of sensor nodes which can provide coverage to monitored area. Member sensor nodes of the covers are called the critical sensors whose lifetime is maximized by minimizing the difference factor (DF). In a cover, DF is defined as the difference between the remaining energy of the critical sensor and remaining energy of the minimum sensor energy after first unit time. In the chromosome, each gene mapped to the sensor in collecting order is shown in Fig. 11. Starting from the first gene algorithm examines whether cover is formed or not. If first gene forms a cover only by itself then it completes the cycle

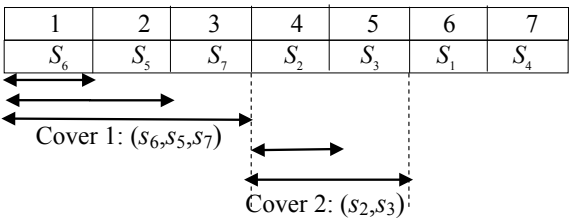


Fig. 11 Formation of cover sets [45]

and starts with next sensor to form another cover. If first gene does not form cover then it will add next gene and inspects if cover is formed or not if not again another gene is added and so on.

4.5 Some Other Evolutionary Algorithms

Wang et al. [47] presented a particle swarm optimization (PSO)-based coverage control algorithm for the energy-efficient coverage deployment. In this approach, first of all, sensor nodes are randomly deployed in the network area. Afterward, network area is divided into number of grids and then coverage rate and energy consumption of each grid are obtained by adjusting the sensing radius of the sensor nodes using PSO. The fitness function is derived in terms of minimization of the energy consumption as given in Eq. 11:

$$F = E_{ar} \tag{11}$$

where E_{ar} is the energy consumption per area which is defined as the ratio between energy consumed by all deployed sensor nodes by sensing area.

Panag and Dhillon [48] proposed a random-transition-based PSO (RTPSO) to maximize the lifetime of the WSN by solving the problem of disjoint coverage sets. Each disjoint coverage set provides the complete coverage to the targets and area. In this approach, PSO is integrated with random transition moves. To guide the particles toward the optimal solutions and to identify the redundant nodes, three random transition moves are introduced. Rout and Roy [49] proposed a dynamic deployment strategy based on the PSO algorithm where mobile sensor nodes are relocated to provide the efficient coverage with guaranteed connectivity. After initial deployment, mobile sensor nodes are relocated by minimum movement to satisfy the coverage and connectivity of the network with limited mobile sensors. Energy consumption is also considered by utilizing the minimum number of sensor nodes with minimum energy consumption.

Qin and Chen [50] proposed an area coverage algorithm based on differential evolution (DE) named as ACADE. Here, binary DE is revived to find the improved minimal cost subset of sensor nodes to meet the desired coverage. The framework of the proposed algorithm is based on the scaling factor where nonparametric variations are used. In order to avoid the unbalanced energy, a compensation strategy is applied by introducing positive and negative utility ratio. According to positive and negative compensation, an additional node is added to the subset which does not have sufficient coverage and redundant nodes are deactivated from the subset. During the formation of a subset, residual energy of the sensor nodes is also considered.

5 Research Challenges and Open Issues

Many works have been done for the proper and efficient coverage- and connectivity-related issues for the WSNs but still there remain some challenges and complications in this domain that has to be taken care. Here, we define some challenges and complications as follows.

5.1 Optimum Node Deployment

One of the very necessary challenging issues in the WSN is to deploy the optimal or minimum number of sensor nodes which provide the desired coverage and connectivity [25]. Lots of works have been done for the optimization of static network where topology is fixed. However, optimization for the dynamic or hybrid networks is not well researched.

5.2 Three-Dimensional Networks

Growing interest for underwater sensor networks, oceanographic data collection, pollution monitoring, etc. draws great attractions of the researchers toward the three-dimensional (3D) networks [51, 52]. The structure of the 3D network is much more complex than 2D network hence only assumption cannot satisfy all the constraints of the 3D as in real-life scenarios. Computational time and complexity for solving the coverage and connectivity problem in 3D network are much more than 2D network. Therefore, optimization in 3D WSN has also became the center of interest for the researchers.

5.3 Lifetime Maximization of Networks

Sensor nodes rely on the limited amount of energy source. Therefore, proper utilization of this energy is essential to prolong the network lifetime for many applications [53–56]. However, it is difficult to recharge the sensor nodes especially for the harsh environment. Many techniques like sleep scheduling, minimization of broadcast messages, transmission of data through coordinator, time scheduling for data gathering and transmission, etc. are proposed by the researchers to extend the network lifetime. Therefore, this topic is also one of the challenging issues among the researchers.

5.4 Fault Tolerance

Sensor nodes may get damaged due to hardware failure, human interference, environmental factors, etc. [3, 5, 22, 23]. that makes the network dysfunctional. Some applications require continuous monitoring where even failure of one node can create big problem. Therefore, to solve the issues related to faulty network, many researchers suggest to use extra sensor nodes called redundant nodes. Although these redundant nodes provide the backup to the faulty nodes, it is cost-effective. Some researchers suggest to maximize the degree of coverage (k-coverage) and connectivity (m-connectivity) such that network will remain functional even when some nodes may get damaged with extended network lifetime. Although these schemes solve the occurrence of fault in the network, it increases the cost of the WSNs.

5.5 Real-Time Protocols

Some applications in WSN required real-time data or information such that appropriate observations can be made or action can be taken. Due to failure of nodes or delay in data transmission, lost messages, noise, and congestion, WSN does not meet the real-time constraints within deadlines. Most of the works for the WSN have been solved for the routing focusing on the real-time issues. There are many other functions like data fusion, query processing, event or target detections, security, data transmissions, etc. which require great attention to fulfill the real-time constraints.

5.6 Nonuniformity in Sensing and Communication Range

Sensing and communication range of the sensor nodes are considered as binary disk model by most of the researchers. However, in reality, this assumption does not fit properly because sensing ranges are highly irregular and location dependent. Simultaneously, due to the presence of transitional regions communication range may fluctuate and irregular. Therefore, it is necessary to adopt some realistic model for the sensing and communication model rather than compromising with the binary disk model.

5.7 Coverage and Connectivity in Presence of Obstacles

To provide an efficient coverage and connectivity in presence of obstacles is a vital challenging issue. The obstacles present in the area of interest with an arbitrary shape and it needs to be modeled in order to solve the problem.

6 Conclusion

WSNs are designed for the specific application where coverage and connectivity are the two most fundamental issues that provide a great impact on the proper functioning of the network. Many works have been done in order to solve the problem related to coverage and connectivity. Nowadays, evolutionary algorithms are drawing the attractions among the researcher to solve the issues related to coverage and connectivity.

In this chapter, we have presented some existing works on coverage and connectivity in WSN based on the EAs. We have briefly described the coverage and connectivity with different types of coverage schemes and sensing models. Literature related to evolutionary algorithm based on coverage and connectivity is briefly described with example. In this literature, we have surveyed only limited evolutionary algorithms utilized for optimization in WSNs especially in coverage and connectivity. Finally, various open research challenges are also described.

Moreover, most of the problems on coverage and connectivity are multi-objectives in nature. Very few multi-objective EAs are employed to solve the problem. Few researchers have also developed some hybrid evolutionary algorithms for WSNs. Such hybrid approaches may be more efficient for some problems.

References

1. Kuila, P., & Jana, P. K. (2014). Energy efficient clustering and routing algorithms for wireless sensor networks: Particle swarm optimization approach. *Engineering Applications of Artificial Intelligence, 33,* 127–140.
2. Kuila, P., & Jana, P. K. (2017). *Clustering and routing algorithms for wireless sensor networks: energy efficient approaches* (1st ed.). CRC Press (Taylor & Francis Group). ISBN-13: 978-1498753821.
3. Azharuddin, Md., Kuila, P., & Jana, P. K. (2015). Energy efficient fault tolerant clustering and routing algorithms for wireless sensor networks. *Computers & Electrical Engineering, 41,* 177–190 (Elsevier).
4. Kuila, P., & Jana, P. K. (2014). A novel differential evolution based clustering algorithm for wireless sensor networks. *Applied Soft Computing, 25,* 414–425 (Elsevier).
5. Cardei, I., & Cardei, M. (2008). Energy-efficient connected-coverage in wireless sensor networks. *International Journal of Sensor Networks, 3*(3), 201–210.
6. Binh, H. T. T., & Dey, N. (2018). *Soft computing in wireless sensor networks*. CRC Press.
7. Kuila, P., & Jana, P. K. (2016). Evolutionary computing approaches for clustering and routing in wireless sensor networks. In *Handbook of research on natural computing for optimization problems* (pp. 246–266). IGI Global. ISBN 9781522500582.
8. Kuila, P., & Jana, P. K. (2014). Approximation schemes for load balanced clustering in wireless sensor networks. *Journal of Supercomputing, 68,* 87–105 (Springer).
9. Kuila, P., Gupta, S. K., & Jana, P. K. (2013). A novel evolutionary approach for load balanced clustering problem for wireless sensor networks. *Swarm and Evolutionary Computation, 12,* 48–56 (Elsevier).
10. Kuila, P., & Jana, P. K. (2014). Heap and Parameter Based Load Balanced Clustering Algorithms For Wireless Sensor Networks. *International Journal of Communication Networks and Distributed Systems, 14*(4), 413–432.

11. Kuila, P., & Jana P. K. (2012). Improved load balanced clustering algorithm for wireless sensor networks. *LNCS, 7135*, 399–404 (Springer).
12. Kuila, P., & Jana, P. K. (2012). Energy efficient load-balanced clustering algorithm for wireless sensor networks. *Procedia Technology, 6,* 771–777 (Elsevier).
13. Kuila, P., & Jana, P. K. (2012). An energy balanced distributed clustering and routing algorithm for wireless sensor networks. In *PDGC 2012* (pp. 220–225). IEEE Xplore.
14. Gupta, S. K., Kuila, P., & Jana, P. K. (2013). GAR: An energy efficient GA-based routing for wireless sensor networks. *LNCS, 7753,* 267–277 (Springer).
15. Gupta, S. K., Kuila, P., & Jana, P. K. (2013). Delay constraint energy efficient routing using multi-objective genetic algorithm in wireless sensor networks. In *ICECCS 2013* (pp. 50–59). Tata McGraw-Hill.
16. Azharuddin, Md., Kuila, P., & Jana, P. K. (2013). A distributed fault-tolerant clustering algorithm for wireless sensor networks. In *2nd ICACCI 2013* (pp. 997–1002). IEEE Xplore.
17. Golberg, D. E. (1989). *Genetic algorithms in search, optimization, and machine learning*. Addison Wesley.
18. Gupta, S. K., Kuila, P., & Jana, P. K. (2014). E^3BFT: energy efficient and energy balanced fault tolerance clustering in wireless sensor networks. In *IC3I 2014* (pp. 714–719). IEEE Xplore.
19. Gupta, S. K., Kuila, P., Jana, P. K. (2016). Energy efficient multipath routing for wireless sensor networks: a genetic algorithm approach. In *5th ICACCI 2016* (pp. 1735–1740). IEEE Xplore.
20. Bose, A., Biswas, T., & Kuila P. (2019). A novel genetic algorithm based scheduling for multicore systems. *AISC, 851*, 45–54 (Springer).
21. Harizan, S., & Kuila, P. (2019). Coverage and connectivity aware energy efficient scheduling in target based wireless sensor networks: An improved genetic algorithm based approach. *Wireless Networks 25*(4), 1995–2011.
22. Gupta, S. K., Kuila, P., & Jana, P. K. (2016) Genetic algorithm for k-connected relay node placement in wireless sensor networks. In *Proceedings of the Second International Conference on Computer and Communication Technologies* (Vol. 379, pp. 721–729). AISC. Springer.
23. Gupta, S. K., Kuila, P., & Jana, P. K. (2016). Genetic algorithm approach for k-coverage and m-connected node placement in target based wireless sensor networks. *Computers & Electrical Engineering, 56,* 544–556.
24. Rebai, M., Snoussi, H., Hnaien, F., & Khoukhi, L. (2015). Sensor deployment optimization methods to achieve both coverage and connectivity in wireless sensor networks. *Computers & Operations Research, 59,* 11–21.
25. Karatas, M. (2018). Optimal deployment of heterogeneous sensor networks for a hybrid point and barrier coverage application. *Computer Networks, 132,* 129–144.
26. Yoon, Y., & Kim, Y. H. (2013). An efficient genetic algorithm for maximum coverage deployment in wireless sensor networks. *IEEE Transactions on Cybernetics, 43*(5), 1473–1483.
27. Geem, Z. W., Kim, J. H., & Loganathan, G. V. (2001). A new heuristic optimization algorithm: Harmony search. *Simulation, 76*(2), 60–68.
28. Moh'd, A. O., & Al-Ajouri, A. (2017). Maximizing wireless sensor network coverage with minimum cost using harmony search algorithm. *IEEE Sensors Journal, 17*(3), 882–896.
29. Jameii, S. M., Faez, K., & Dehghan, M. (2015). Multiobjective optimization for topology and coverage control in wireless sensor networks. *International Journal of Distributed Sensor Networks, 11*(2), 363815.
30. Nezhad, S. E., Kamali, H. J., & Moghaddam, M. E. (2010). Solving K-coverage problem in wireless sensor networks using improved harmony search. In *2010 International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA)* (pp. 49–55). IEEE.
31. Mohamed, S. M., Hamza, H. S., & Saroit, I. A. (2015). Harmony search-based k-coverage enhancement in wireless sensor networks. *International Journal* of *Computer* and *Electrical Engineering, 9*(1), 19924.
32. Sharma, D., & Gupta, V. (2017). Improving coverage and connectivity using harmony search algorithm in wireless sensor network. In *International Conference on Emerging Trends in Computing and Communication Technologies (ICETCCT)* (pp. 1–7). IEEE.

33. Manjarres, D., Del, S. J., Gil-Lopez, S., Vecchio, M., Landa-Torres, I., & Lopez-Valcarce, R. (2013). A novel heuristic approach for distance- and connectivity-based multihop node localization in wireless sensor networks. *Soft Computing, 17*(1), 17–28.
34. Dorigo, M., & Di, C. G. (1999). Ant colony optimization: A new meta-heuristic. In *Proceedings of the 1999 Congress on Evolutionary Computation-CEC99 (Cat. No. 99TH8406)* (Vol. 2, pp. 1470–1477). IEEE.
35. Sun, X., Zhang, Y., Ren, X., & Chen, K. (2015). Optimization deployment of wireless sensor networks based on culture-ant colony algorithm. *Applied Mathematics and Computation, 250,* 58–70.
36. Li, D., Liu, W., & Cui, L. (2010). EasiDesign: An improved ant colony algorithm for sensor deployment in real sensor network system. In *2010 IEEE Global Telecommunications Conference (GLOBECOM 2010)* (pp. 1–5). IEEE.
37. Deif, D. S., & Gadallah, Y. (2017). An ant colony optimization approach for the deployment of reliable wireless sensor networks. *IEEE Access, 5,* 10744–10756.
38. Huang, P., Lin, F., XuL, J., Kang, Z. L., Zhou, J. L., & Yu, J. S. (2017). Improved ACO-based sweep coverage scheme considering data delivery. *International Journal of Simulation Modelling, 16*(2), 289–301.
39. Liao, W. H., Kuai, S. C., & Lin, M. S. (2015). An energy-efficient sensor deployment scheme for wireless sensor networks using ant colony optimization algorithm. *Wireless Personal Communications, 82*(4), 2135–2153.
40. Liu, X., & He, D. (2014). Ant colony optimization with greedy migration mechanism for node deployment in wireless sensor networks. *Journal of Network and Computer Applications, 39,* 310–318.
41. Liu, X. (2012). Sensor deployment of wireless sensor networks based on ant colony optimization with three classes of ant transitions. *IEEE Communications Letters, 16*(10), 1604–1607.
42. Qasim, T., Mujahid, A., Bhatti, N. A., Mushtaq, M., Saleem, K., Mahmood, H., et al. (2018). ACO-Discreet: An efficient node deployment approach in wireless sensor networks. In *Information Technology-New Generations* (pp. 43–48). Springer.
43. Deb, K., Pratap, A., Agarwal, S., & Meyarivan, T. (2002). A fast and elitist multiobjective genetic algorithm: NSGA-II. *IEEE Transactions on Evolutionary Computation, 6*(2), 182–197.
44. Jia, J., Chen, J., Chang, G., & Tan, Z. (2009). Energy efficient coverage control in wireless sensor networks based on multi-objective genetic algorithm. *Computers & Mathematics with Applications, 57*(11–12), 1756–1766.
45. Syarif, A., Benyahia, I., Abouaissa, A., Idoumghar, L., Sari, R. F., Lorenz, P. (2014). Evolutionary multi-objective based approach for wireless sensor network deployment. In *2014 IEEE International Conference on Communications (ICC)* (pp. 1831–1836). IEEE.
46. El-Sherif, M., Fahmy, Y., & Kamal, H. (2018). Lifetime maximization of disjoint wireless sensor networks using multiobjective genetic algorithm. *IET Wireless Sensor Systems, 8*(5), 200–207.
47. Wang, J., Ju, C., Gao, Y., Sangaiah, A. K., & Kim, G. J. (2018). A PSO based energy efficient coverage control algorithm for wireless sensor networks. *Computers, Materials and Continua, 56*(3), 433–446.
48. Panag, T. S., & Dhillon, J. S. (2018). A novel random transition based PSO algorithm to maximize the lifetime of wireless sensor networks. *Wireless Personal Communications, 98*(2), 2261–2290.
49. Rout, M., & Roy, R. (2017). Optimal wireless sensor network information coverage using particle swarm optimization method. *International Journal of Electronics Letters, 5*(4), 491–499.
50. Qin, N. N., & Chen, J. L. (2018). An area coverage algorithm for wireless sensor networks based on differential evolution. *International Journal of Distributed Sensor Networks, 14*(8), 1–11.
51. Cao, B., Zhao, J., Lv, Z., Liu, X., Kang, X., & Yang, S. (2018). Deployment optimization for 3D industrial wireless sensor networks based on particle swarm optimizers with distributed parallelism. *Journal of Network and Computer Applications, 103,* 225–238.

52. Mnasri, S., Nasri, N., van den Bossche, A., & Val, T. (2019). Improved many-objective optimization algorithms for the 3D indoor deployment problem. *Arabian Journal for Science and Engineering* 1–22.
53. Gupta, S. K., Kuila, P., & Jana, P. K. (2016). GA based energy efficient and balanced routing in k-connected wireless sensor networks. *AISC, 458*, 679–686 (Springer).
54. Gupta, S. K., Kuila, P., Jana, P. K. (2016). Energy efficient routing algorithm for wireless sensor networks: A distributed approach. In *Communication and Computing Systems: Proceedings of the International Conference on Communication and Computing Systems (ICCCS 2016)* (pp. 207–213). CRC Press, Taylor & Francis Group.
55. Singh, D., Kuila, P., & Jana, P. K. (2014). A distributed energy efficient and energy balanced routing algorithm for wireless sensor networks. In *3rd ICACCI 2014* (pp. 1657–1663). IEEE Xplore.
56. Binh, H. T. T., Hanh, N. T., & Dey, N. (2018). Improved cuckoo search and chaotic flower pollination optimization algorithm for maximizing area coverage in wireless sensor networks. *Neural Computing and Applications, 30*(7), 2305–2317.

Nature-Inspired Algorithms for *k*-Coverage and *m*-Connectivity Problems in Wireless Sensor Networks

Subash Harizan and Pratyay Kuila

Abstract Efficient deployment of the sensor nodes takes an important role in proper coverage and connectivity of the wireless sensor networks (WSNs). The key issues that need to be taken care during deployment are the number of deployed sensors, coverage of the target/region, and connectivity among the sensor nodes. As the sensor nodes are prone to various kinds of failure, it is essential for *k*-coverage of the targets and *m*-connectivity among the sensor nodes. Here, *k*-coverage of the targets indicates that all the targets are covered by at least k number of sensor nodes so that failure of $k-1$ sensor nodes can also ensure coverage of the targets. Similarly, *m*-connectivity of the sensor nodes indicates all the sensor nodes are connected with other $m-1$ sensor nodes. Note that the *k*-coverage and *m*-connectivity problem for WSNs is nondeterministic polynomial (NP)-hard in nature. In this chapter, nature-inspired algorithms are studied and designed to solve the problem. Particle swarm optimization (PSO), differential evolution (DE), genetic algorithms (GA), and gravitational search algorithm (GSA) are studied and designed for the problem. The chromosome, vector, particle, and agent are efficiently represented. An efficient derivation of fitness functions is provided with the conflicting objectives. An extensive simulation is also conducted.

Keywords Nature-inspired algorithms · *k*-coverage · *m*-connectivity · Wireless sensor networks

S. Harizan · P. Kuila (✉)
Department of Computer Science & Engineering, National Institute of Technology Sikkim, South Sikkim 737139, India
e-mail: pratyay_kuila@yahoo.com

S. Harizan
e-mail: subashharizan@gmail.com

S. K. Das et al. (eds.), *Design Frameworks for Wireless Networks*,
Lecture Notes in Networks and Systems 82,
https://doi.org/10.1007/978-981-13-9574-1_12

1 Introduction

Wireless sensor networks (WSNs) draw a great attention of the researchers for their various potential applications. A sensor node performs multiple functions as sensing, communication, and data processing. Sensor nodes can collaborate among them to monitor or sense the area of interest (AoI), collect the sensory data, process the data, and transmit to the base station (BS) directly or through multi-hop [1–4]. As the sensor nodes are equipped with limited energy source, it is very essential and challenging to conserve the limited energy [5–9]. Moreover, sensor nodes can sense and communicate within the limited sensing and communication range. A region/target is said to be covered if it falls within the sensing range. Similarly, two sensor nodes can communicate with each other if they are within the communication range of each other. Therefore, it is also very essential to provide an efficient coverage and connectivity [10–16] to monitor the region/target and to transmit the sensed data to the base station.

Deployment of sensor nodes has vital role for ensuring an efficient coverage and connectivity in the network. There are mainly two types of deployment scheme in WSN: preplanned [14] and ad hoc [14] deployment. In preplanned scheme, sensor nodes are deployed in planned manner in an accessible area and thereby the network has better management with saving in cost and energy. In ad hoc scheme, sensor nodes are deployed randomly in the harsh environment where human interference is not possible. Ad hoc deployment does not guarantee the coverage and connectivity. Thus, this scheme requires large number of sensor nodes for proposed function of the network.

Sensor nodes are prone to failure due to hardware failure, energy depletion, natural calamities, etc. As a result, network becomes functionless. Therefore, for better performance of the network k-coverage and m-connectivity are desirable. However, cost for the k-coverage and m-connectivity should also be optimized by deploying the minimum number of sensor nodes. Therefore, deployment of minimum number of sensor nodes for desire coverage and connectivity is an NP-hard [14, 16–18] problem. In limited time, it is not feasible or computationally very expensive to find the optimal solutions for the NP-hard problem.

In this chapter, we studied the target coverage with connectivity problem as in [14]. As an example, a network scenario with 7 target points (t_1, t_2, t_3, …, t_7) and 14 potential positions (ρ_1, ρ_2, ρ_3, …, ρ_{14}) is shown in Fig. 1. Here, among the 14 potential positions, 9 positions are selected to place the sensor nodes. We can also observe that all the target points are covered by at least three sensor nodes and each sensor node is connected with at least other two neighbor sensor nodes. Therefore, we can say that scenario of the network as shown in Fig. 1 in chapter "Ambient Intelligence for Patient-Centric Healthcare Delivery: Technologies, Framework and Applications" is three coverage of the target and two connectivity of the sensor nodes, i.e., 3-coverage and 2-connectivity.

Nowadays, nature-inspired algorithms (NIAs) are drawing a great attention of the researchers as these algorithms are found to be very efficient to find the optimal

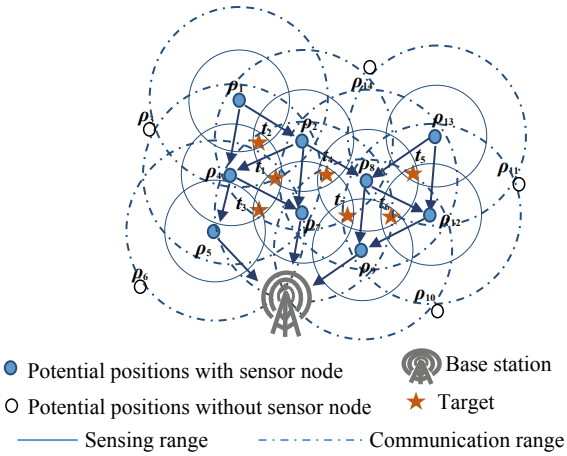


Fig. 1 A simple network scenario with 3-coverage and 2-connectivity [14]

solutions for the real-life complex problems. NIAs are classified into evolutionary algorithms (EAs) and swarm intelligence algorithms (SIAs). These algorithms are extensively used to solve many optimization problems of WSNs [19–29].

1.1 Author's Contribution

In this chapter, we have studied the *k*-covered and *m*-connectivity problem as in [14]. Various nature-inspired approaches like genetic algorithm (GA), particle swarm optimization (PSO), differential evolution (DE), and gravitational search algorithm (GSA) are also studied and employed for the above mentioned problem. Our contributions are summarized as follows:

- A linear programming (LP) is formulated for the aforesaid problem.
- Efficient representation of chromosome, particle, vector, and agent for GA, PSO, DE, and GSA, respectively. Moreover, they are generated such a way that validity of them cannot be disturbed after the operations of EAs (e.g., crossover, mutation, velocity and potion updation, etc.).
- Derivation of efficient fitness function is given. Here, three conflicting objectives are considered.
- An extensive simulation is conducted and comparisons are shown for the algorithms.

1.2 Organization of the Chapter

Rest of the chapter is organized as follows. Section 2 provides a brief overview of nature-inspired algorithms. Network model, problem formulation, terminologies, and derivation of fitness function are defined in Sect. 3. GA-, PSO-, DE-, and GSA-based approaches are discussed in Sects. 4–7, respectively. Experimental results are shown in Sect. 8 and the chapter is concluded in Sect. 9.

2 Nature-Inspired Algorithms

Nature-inspired algorithms (NIAs) are inspired by the processes, perceived from nature to solve the various optimization problems. These algorithms have drawn enormous attention of the researchers to solve various optimization problems in the field of engineering, biomedical, finance, etc. NIAs find the optimal solution for real-life problem which is classified as NP-hard. It is a population-based algorithm which is classified into evolutionary algorithms (EAs) and swarm-intelligence-based algorithms (SIAs). EAs are motivated by the theory of Charles Darwin called survival of the fittest. The individual in the population survives and reproduces offspring only if they can fit themselves in the given environment. Whereas SIAs are inspired by the collective behavior of swarms like bird flocking, fish schooling, ant colony, bee colony, etc. An overview of some popular nature-inspired approaches is as follows.

2.1 Genetic Algorithm

Genetic algorithm (GA) [30–34] is a population-based meta-heuristic optimization algorithm. A population of size N_p is created by randomly generating the chromosomes. Each chromosome represents the complete solution to the problem. Chromosomes in the population are updated by applying the genetic operations (selection, crossover, and mutation) to explore the search space to find the near-optimal solution. In the selection phase, a set of chromosomes are selected from the population. Selection operation is followed by the crossover operation. In crossover operation, two-parent chromosomes exchange their information to produce two child offspring chromosomes. Finally, a gene value is randomly selected and mutated. Mutation is also applied with some modification according to the application characteristic. This process repeats iteratively till the desired or satisfactory chromosome is obtained or maximum number of iterations.

2.2 Particle Swarm Optimization

Particle swarm optimization (PSO) [1, 35, 36] is a stochastic optimization method that is motivated by the social behavior of bird flocking or fish schooling. It can be observed that birds, fishes, etc. always travel in a group without colliding with each other. To avoid the collision, each member uses the group information and adjusts its position and velocity to follow the group. This approach reduces the efforts of each individual to find the food, shelter, etc. Initially, a swarm (say size N_p) of particles is created randomly where an individual particle represents a complete solution to a multidimensional optimization problem. All particles in the population have equal dimension (say D) and also initiated with random velocities in search space. In the dth dimension of the hyperspace, a particle P_i, $1 \leq i \leq N_p$ with position $\beta_{i,d}$, $1 \leq d \leq D$ can be represented as follows:

$$P_i = \left[\beta_{i,1}, \beta_{i,2}, \beta_{i,3,\ldots,}\beta_{i,d}\right] \tag{1}$$

The quality of the particles is evaluated by the derived fitness function. In order to search the near-optimal solution, the velocities and positions of the particles are updated in each iteration. The velocity of the particles is updated by two best particles, i.e., personal best ($Pbest_i$) and global best ($Gbest$). $Pbest_i$ be the best particle that has been observed so far for P_i. $Gbest$ be the best particle among the swarm. The velocity and position of the particles are updated as follows:

$$v_{i,d}(t) = w \times v_{i,d}(t-1) + c_1 \times r_1 \times \left(Pbest_{i,d} - \beta_{i,d}(t-1)\right) + c_2 \times r_2 \times \left(Gbest_{i,d} - \beta_{i,d}(t-1)\right) \tag{2}$$

$$\beta_{i,d}(t) = \beta_{i,d}(t-1) + v_{i,d}(t) \tag{3}$$

where w represents the inertial weight, c_1 and c_2 are positive constant values called acceleration coefficient, and r_1 and r_2 are two independently generated random number in the range [0, 1]. The update process will continue till the acceptable solution is achieved or the maximum number of iterations are reached.

2.3 Differential Evolution

Differential evolution (DE) [37–39] is one of the most powerful stochastic real parameter based evolutionary algorithms. DE is widely used to solve many optimization problems. Initially, a population (size say N_p) is created by randomly generating the set of vectors of dimension, say D. Each individual vector represents the complete solution to the problem. The quality of the vectors is evaluated by the derived fitness function. After the initialization of the population, the quality of the vectors is

enhanced by the mutation, crossover, and selection operation. In each iteration, the vectors are updated. The final solution is obtained by evaluating the solutions till the maximum iteration is reached.

DE with different variants can be represented in general form as $DE/\beta/\gamma/\delta$. DE denotes the differential evolution, β specifies the vector to be muted (which can be selected as randomly or best vector from population), γ specifies the number of vectors that are considered for mutation operation of β, and δ denotes crossover scheme (binomial or exponential). In the mutation operation, each candidate vector called target vector and other three vectors are randomly chosen. Thereafter, a new vector called donor vector is generated using mutation. Mutation operation is followed by crossover operation. In crossover operation, target vector and donor vector exchange their information to generate a child vector called trail vector. Finally, fitness function is used in selection operation to select the best vector among the trial vector and target vector for the next generation. Algorithm iterates continuously to generate the new vectors till the termination criteria are obtained or acceptable vector for the problem is achieved.

2.4 Gravitational Search Algorithm

Gravitational search algorithm (GSA) [40] is a population-based stochastic optimization technique. This algorithm is inspired from the law of gravitation and law of motion. In GSA, each solution is represented by agent that represents the complete solution for a multidimensional optimization problem. The agents are initialized with position, velocity, acceleration, and mass. According to the law of gravitation, objects in the universe attract each other by a gravitational force. During this movement, object having lower mass moves toward the object with higher mass. The objects with lower mass have higher acceleration whereas objects with higher mass have slower acceleration. The agents with lighter mass will get attracted toward the agent with heaviest mass. Performance of the agent is dignified by its mass. An agent with heavier mass is considered as the optimal solution to the problem. An ith agent from the population of size N_p is denoted as follows:

$$\lambda_i = \left\{\lambda_i^1, \lambda_i^2, \lambda_i^3, \ldots, \lambda_i^d\right\}, \ \forall i, \ 1 \leq i \leq N_p \tag{4}$$

where λ_{i}^d represents the position value of ith agent in the dth dimension. At iteration t, the gravitational force acting on agent λ_{i} from agent λ_{j} in the dth dimension is defined as follows:

$$F_{ij}^d = G(t) \times \frac{M_{pi}(t) \times M_{aj}(t)}{R_{ij}(t) + \varepsilon} \times \left\{\lambda_i^d(t) - \lambda_j^d(t)\right\} \tag{5}$$

where $G(t)$ is the gravitational constant at iteration t, ε is the small constant, passive gravitational mass of agent λ_{i} and active gravitational mass of agent λ_{j} are represented

by $M_{pi}(t)$ and $M_{\mathrm{aj}}(t)$, respectively, and $R_{ij}(t)$ denotes the Euclidean distance between two agents λ_{i} and λ_{j} at iteration t. The value of gravitational constant $G(t)$ with initial value G_0 is calculated as follows:

$$G(t) = G_0 \times (-\beta t)/e^{tmax} \tag{6}$$

where *tmax* denotes the maximum number of iteration and value of control parameter is represented by β. The total force applied by all agents on the agent λ_i in the dth is calculated by the following formula:

$$F_i^d = \sum_{j=1, j\neq i}^{Np} rand_j \times F_{ij}^d, \, where \, rand_j \in [0, 1] \tag{7}$$

The relation among mass (M), acceleration (a), and force is given by the law of motion. Therefore, the acceleration of λ_i in dth dimension is given as follows:

$$a_i^d = F_i^d(t)/M_{ii}(t) \tag{8}$$

where M_{ii} denotes the inertial mass of an agent λ_i. The velocity and position of λ_i are updated by using the following equations:

$$v_i^d(t+1) = rand_i \times v_i^d(t) + a_i^d(t) \tag{9}$$

$$\lambda_i^d(t+1) = \lambda_i^d(t) + v_i^d(t+1) \tag{10}$$

where $rand_i \in [0, 1]$. The gravitational and inertial masses of an agent are assumed to be equal in GSA, i.e., $M_{ai} = M_{pi} = M_{ii} = M_i$.

In a population, N_p agents are evaluated by the fitness function. In iteration t, among all agents, $best(t)$ and $worst(t)$ are the best and worst agents for the maximization problem denoted as

$$best(t) = max_{j\in[1,\ldots Np]} fit_j(t) \tag{11}$$

$$worst(t) = min_{j\in[1,\ldots Np]} fit_j(t) \tag{12}$$

The mass of every agent is calculated by the fitness value obtained from Eqs. (11) and (12). The mass M_{i} of an agent λ_{i} is determined as follows:

$$m_i = \frac{fit_i(t) - worst(t)}{best(t) - worst(t)} \tag{13}$$

$$M_i = \frac{m_i(t)}{\sum_{j=1}^{Np} m_i(t)} \tag{14}$$

The exploitation must fade in and exploration must fade out to avoid from trapping in local optimum as the laps of iterations continue. Therefore, only K agents with best fitness value, i.e., *Kbest* will apply force to others. *Kbest* value linearly decreases to one as it is a function of time. Thus, Eq. (7) could be revised as follows:

$$F_i^d = \sum_{j \in Kbest, j \neq i} rand_j \times F_{ij}^d, where\ rand_j \in [0, 1] \tag{15}$$

However, the subsequent changes in the position and velocity occur with the process of repeatedly updating the acceleration of the agent. This process of updating continues till the optimal solution is obtained or maximum iteration is reached.

3 Network Model and Problem Formulation

3.1 Network Model

Based on our problem, we have assumed a 2D WSN with few target points, a base station, and few predefined potential positions. Target points need to be monitored by placing the sensor nodes on the given potential positions. Assumed WSN is supposed to have the following properties [41–46]:

- All the target points and deployed sensor nodes are stationary.
- Target is said to be covered if it falls within the sensing range of sensor nodes.
- Two nodes are connected if they are within communication range of each other.
- A sensor node can sense more than one target point.
- All the sensor nodes have same sensing and communication range.

3.2 Terminologies

Before formulation of problem, first, we define some terminologies used in this chapter.

- $P = \{\rho_1, \rho_1, \rho_1, \ldots, \rho_N\}$ denotes the N number of predefined potential positions.
- $S = \{s_1, s_2, s_3, \ldots, s_Z\}$ denotes the set of Z number of deployed sensor nodes on selected potential positions.
- $T = \{t_1, t_2, t_3, \ldots, t_M\}$ denotes the M number of target points.
- R_{sen} and R_{com} denote the sensing and communication range of the sensor nodes, respectively.
- $D(s_i, t_j)$ represents the Euclidean distance between s_i and t_j.
- $SC_{cov}(t_i)$ denotes the set of sensor nodes that cover t_i, i.e.,

$$SC_{cov}(t_i) = \left\{ s_j | D\left(s_i, t_j\right) \leq R_{sen},\ \forall j,\ 1 \leq j \leq Z \right\} \tag{16}$$

- $TC_{\mathrm{cov}}(s_{\mathrm{i}})$ denotes the set of target points which are covered by s_{i}, i.e.,

$$TC_{cov}(s_i) = \left\{ t_j | D\left(s_i, t_j\right) \leq R_{sen},\ \forall j,\ 1 \leq j \leq M \right\} \tag{17}$$

- $C_{\mathrm{con}}(s_{\mathrm{i}})$ denotes the set of sensor nodes that are within the communication range of s_{i} toward BS, i.e.,

$$\begin{aligned} C_{con}(s_i) = \{ s_j | D\left(s_i, s_j\right) \leq R_{com}, \&D\left(s_i, s_j\right) \\ \geq D\left(s_j, BS\right), \forall j, 1 \leq j \leq Z \} \end{aligned} \tag{18}$$

- $COV_{\mathrm{cost}}(t_{\mathrm{i}})$ denotes the coverage cost of t_{i}.
- $CON_{\mathrm{cost}}(s_{\mathrm{i}})$ denotes the connection cost of s_{i}.
- k and m are the desired coverage and connectivity (k and m are some predefined value).
- *BS* denotes base station.

3.3 Problem Definition

Given a WSN with N predefined potential positions and M target points, we have to place the sensor nodes on selected potential positions, considering the following objectives:

- Selection of minimum number of potential positions for placement of sensor nodes.
- Placed sensor nodes must ensure the k-coverage of the targets.
- Placed sensor nodes must be m-connected among themselves.

Before formulation of linear programming (LP) of the given problem, we define the following Boolean variables:

$$\lambda_i = \begin{cases} 1, \ \textit{If a sensor node is placed at } \rho_i \\ 0, \ \textit{Otherwise} \end{cases} \tag{19}$$

$$\beta_{ij} = \begin{cases} 1, \ \textit{If } s_j \textit{ provides coverage to } t_i \\ 0, \ \textit{Otherwise} \end{cases} \tag{20}$$

$$\partial_{ij} = \begin{cases} 1, \ \textit{If } s_i \textit{ is within } R_{com} \textit{ of } s_j \\ 0, \ \textit{Otherwise} \end{cases} \tag{21}$$

$$\delta_i = \begin{cases} 1, \ \textit{If } \rho_i \textit{ is within } R_{com} \textit{ of BS} \\ 0, \ \textit{Otherwise} \end{cases} \tag{22}$$

Now, the LP of the given problem is defined as follows:

$$Minimize \sum_{i=1}^{N} \lambda_i \tag{23}$$

Subject to:

$$\sum_{j=1}^{Z} \beta_{ij} \times \lambda_j \geq k, \ where\, i = 1\, to\, M \tag{24}$$

$$\left(\sum_{j=1}^{Z} \partial_{ij} \times \lambda_j + \delta_i \right) \geq m, \ where\, i = 1\, to\, Z \tag{25}$$

$$\left(\lambda_j, \beta_{ij}, \partial_{ij}, \delta_i \right) \in \{0, 1\} \tag{26}$$

Constraint 24 ensures the k-coverage of each target point and m-connectivity among the deployed sensor nodes is ensured by the constraint 25. Restriction on the decision variables is given by constraint 26.

3.4 Derivation of Fitness Function

In this chapter, we have studied four nature-inspired algorithms. The algorithms are initialized with population which consists of member of solutions (i.e., chromosomes/vectors/particles/agents). The solutions are evaluated on the basis of fitness function. The following objectives are considered as in [14].

Objective 1 (*Deployment of minimum number of sensor nodes*): Let us assume that out of given N potential positions, Z numbers of potential positions are selected by particular solution to place the sensor nodes. The first objective is as follows:

$$Objective\ 1\text{: } Minimize\ O_1 = Z/N \tag{27}$$

Objective 2 (*Maximization of k-coverage*): The second objective is to maximize the k-coverage of all the target (M) points in the network which can be stated as follows:

$$Objective\ 2\text{: } Maximize\ O_2 = \frac{\sum_{i=1}^{M} COV_{cost}(t_i)}{(M \times k)} \tag{28}$$

where coverage cost ($COV_{cost}(t_i)$) of t_i, is defined as follows:

$$COV_{cost}(t_i) = \begin{cases} k, & If\ |SC_{cov}(t_i)| \geq k \\ SC_{cov}(t_i), & Otherwise \end{cases} \tag{29}$$

Objective 3 (*Maximization of m-connectivity*): Deployed sensor nodes on the selected potential positions must be m-connected and toward BS. The third objective can be stated as follows:

$$Objective\ 3: Maximize\ O_3 = \frac{\sum_{i=1}^{Z} CON_{cost}(s_i)}{(Z \times m)} \tag{30}$$

where connection cost ($CON_{cost}(s_i)$) of s_i is given as

$$CON_{cost}(t_i) = \begin{cases} m, & If\ |C_{con}(s_i)| \geq m \\ C_{con}(s_i), & Otherwise \end{cases} \tag{31}$$

The above objectives are conflicting in nature. Weight sum approach (WSA) [47] is found to be very efficient to form a single fitness function taking multiple multi-objective functions. Thus, WSA scheme is used as follows:

$$F = w_1 \times (1 - O_1) + w_2 \times O_2 + w_3 \times O_3 \tag{32}$$

$$\text{i.e., } F = w_1 \times (1 - (Z/N)) + w_2 \times \frac{\sum_{i=1}^{M} COV_{cost}(t_i)}{(M \times k)} + w_3 \times \frac{\sum_{i=1}^{Z} CON_{cost}(s_i)}{(Z \times m)} \tag{33}$$

where $w_2 + w_2 + w_3 = 1$ and $0 \leq w_i \leq 1$, $\forall i$, $i = 1$ to 3. The final objective is to maximize the fitness value, i.e.,

$$Objective = Maximize\ F \tag{34}$$

Based on this fitness value as defined in Eq. 33, the solutions are evaluated. Solution with higher fitness value is considered as the better solution.

4 GA-Based Approach

4.1 Chromosome Encoding

The chromosomes are encoded as in [14]. Here, the chromosome as a string of zeros and ones is taken. The number of potential positions in the network is taken as the length of the chromosomes. If the value of ith gene is 1 then it implies that the ρ_i is selected for the placement of sensor nodes. Otherwise, no sensor nodes are placed at ρ_i.

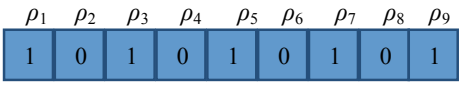


Fig. 2 Chromosome representation

Illustration: Let us consider a WSN with nine potential positions. Therefore, length of the chromosome is nine as in Fig. 2. It can be observed that gene value at position 5 is 1 which represents that the sensor node is placed at position ρ_5. Similarly, sensor nodes are also placed at ρ_1, ρ_3, ρ_7, and ρ_9. Whereas no sensor nodes are placed at ρ_2, ρ_4, ρ_6, and ρ_8 as the gene value at positions 2, 4, 6, and 8 is 0.

4.2 Initialization of Population

The initial population is randomly generated set of the chromosomes.

4.3 Fitness Function

Chromosomes are evaluated on the basis of the fitness function as defined in Sect. 2.4, Eq. 31.

4.4 Selection, Crossover, and Mutation Operation

In selection phase, two valid chromosomes called parents are selected from the population which can undergo crossover operation to produce new offspring. There are many selection methods like Roulette-wheel selection, rank selection, tournament selection, etc. Here, Roulette-wheel selection method is used.

Crossover operation is performed on two selected chromosomes. This operation is regulated by the crossover probability. Evolution of the search speed is reformed by varying this crossover probability. There are different types of crossover like one-point crossover, two-point crossover, uniform crossover, etc. Crossover points are chosen randomly in the chromosome beyond that the parent chromosomes exchange their information to produce new child chromosomes. Here, two-point crossover operation is used.

The crossover operation is followed by the mutation operation. In mutation operation, a randomly selected gene value within a chromosome is altered to produce a new species with arbitrary locus in the fitness landscape. Like crossover, performance of mutation operation is also regulated by the mutation probability. Mutation probability is usually lower than crossover probability. Mutation produces a chromosome which cannot converge in the local optimum.

5 PSO-Based Approach

5.1 Particle Representation

It is very essential to represent the particles in such a way that an individual particle must represent the complete solution to the problem. The dimensions of the particle are taken same as the number of potential positions (i.e., N) in the network. A swarm is a set of randomly generated N_P number of particles. The ith particle of the population may be represented by a vector P_{i} as follows:

$$P_i = \left[\beta_{i,1}, \beta_{i,2}, \beta_{i,3}, \ldots, \beta_{i,N}\right]$$

where each component is given as $\beta_{i,d}$, $0 \leq i \leq Np$, $1 \leq d \leq N$. Here, $\beta_{i,j}$ represents the jth component of the ith particle. Each component of the particles is initialized by randomly generated uniformly distributed number $rand(0, 1)$, $0 < rand(0, 1) \leq 1$. Here, if the component value (say jth component) of the particle is greater than the defined threshold value (Th) then the corresponding potential position (jth) is being placed with a sensor node. Otherwise, sensor node is not placed at the potential position.

Illustration: Let us consider a WSN with nine potential positions. Therefore, dimension of the particle is same as the number of potential positions, i.e., nine. Figure 3 shows the particle representation of the corresponding WSN. Now, random numbers are generated for each component of the particle. We can also define a threshold value Th (say 0.54) which is compared with each component value. If the generated ith component value is greater than the Th value then the corresponding ith position is selected to place the sensor node. From Fig. 3, it can be observed that the component value at positions 1, 2, 3, 5, 7, and 9 has value greater than the defined Th. Therefore, the potential positions ρ_1, ρ_2, ρ_3, ρ_5, ρ_7, and ρ_9 are chosen for placement of sensor nodes. However, no sensor nodes are placed at potential positions ρ_4, ρ_6, and ρ_8 as the component value at that 4, 6, and 8 is less than Th, i.e., 0.54.

5.2 Fitness Function

Here, same fitness function is used as discussed in Sect. 3.4, Eq. 31.

ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6	ρ_7	ρ_8	ρ_9
0.67	0.79	0.89	0.33	0.59	0.21	0.88	0.41	0.58

Fig. 3 Particle representation

5.3 Velocity and Position Update

In each iteration, the velocity and position of the particles are updated using Eqs. 2 and 3, respectively. Similarly, *Pbest* and *Gbest* are also updated accordingly.

6 DE-Based Approach

6.1 Vector Representation

The vectors are encoded same as the particles in PSO.

6.2 Fitness Function

The fitness function is used same as in GA and PSO.

6.3 Mutation

For the crossover and mutation operation, the *DE*/*best*/1/*bin* scheme is used. In differential mutation operation (say at *t*th generation for *i*th vector), a donor vector ($v_{i,t}^{donor}$) is created for each member vector (target vector) ($v_{i,t}^{tar}$) in the population. The best vector ($v_{\mathrm{i,t}}^{\mathrm{best}}$) and other two distinct vectors ($v_{x,t}$ and $v_{y,t}$) are randomly chosen from the population such that $i \neq x \neq y \neq best$. After that, difference of distinct vectors is multiplied with scaling factor F and added to best vector to generate a donor vector. The mutation operation can be defined as follows:

$$v_{i,t}^{donor} = v_{i,t}^{best} + F\left(v_{x,t} - v_{y,t}\right) \tag{35}$$

6.4 Crossover

Crossover operation is performed to generate a new vector called trail vector $v_{\mathrm{i,t}}^{\mathrm{trial}}$. Here, binomial crossover operation is performed in between donor vector and target vector. We choose a predefined crossover rate (say *CR*) and operation for crossover can be defined as follows:

$$v_{i,t}^{trial} = \begin{cases} v_{i,t}^{donor}, & if\,(rand[0,1] \leq CR) \\ v_{i,t}^{tar}, & Otherwise \end{cases} \tag{36}$$

Each component of the trail vector is generated as follows. For each component, we choose a random value between 0 and 1. Say for *i*th component of a trail vector a chosen random value is less than or equal to *CR* than *i*th component of trail vector is same as the *i*th component of the donor vector. Otherwise, *i*th component of trail vector is same as the *i*th component of target vector.

6.5 Selection

Survival among the trail vector and target vector which acts as a target vector $v_{i,t+1}^{\text{tar}}$ in the next generation $(t + 1)$ is decided by the selection operation. Derived fitness function as defined in Eq. 31 is used to evaluate both the vectors. If the fitness of the trail vector is found to be better than target vector then it will replace the target vector for the next generation. Otherwise, target vector will be part of next generation. The selection operation is defined as follows:

$$v_{i,t+1}^{tar} = \begin{cases} v_{i,t}^{trial}, & if\left(f\left(v_{i,t}^{trial}\right) \geq f\left(v_{i,t}^{tar}\right)\right) \\ v_{i,t}^{tar}, & Otherwise \end{cases} \tag{37}$$

where $f(v_{i,t}^{trial})$ and $f(v_{i,t}^{tar})$ represent the fitness of the trail vector and target vector for the generation *t*.

7 GSA-Based Approach

7.1 Agent Representation

Agents are represented in the same way as the particle.

7.2 Update Velocity, Mass, Position, and Force

The velocity, mass, position, and force of the agents are updated by Eqs. 9, 14, 10, and 15, respectively.

7.3 *Fitness Function*

Fitness function is used same as in GA, PSO, and DE.

8 Experimental Results

We have performed extensive simulation of the algorithms using MATLAB and C programming. We have considered the scenario for random deployment where potential positions are randomly taken in the network area of 300 × 300 m^2. BS is located at the position (300, 150) as shown in Fig. 4. The target points are denoted by the black triangle, potential positions are denoted by red circle, and selected potential points are denoted by blue circle. The used simulation parameters for PSO, DE, GA, and GSA are given in Table 1. It should be noted that it is very hard to

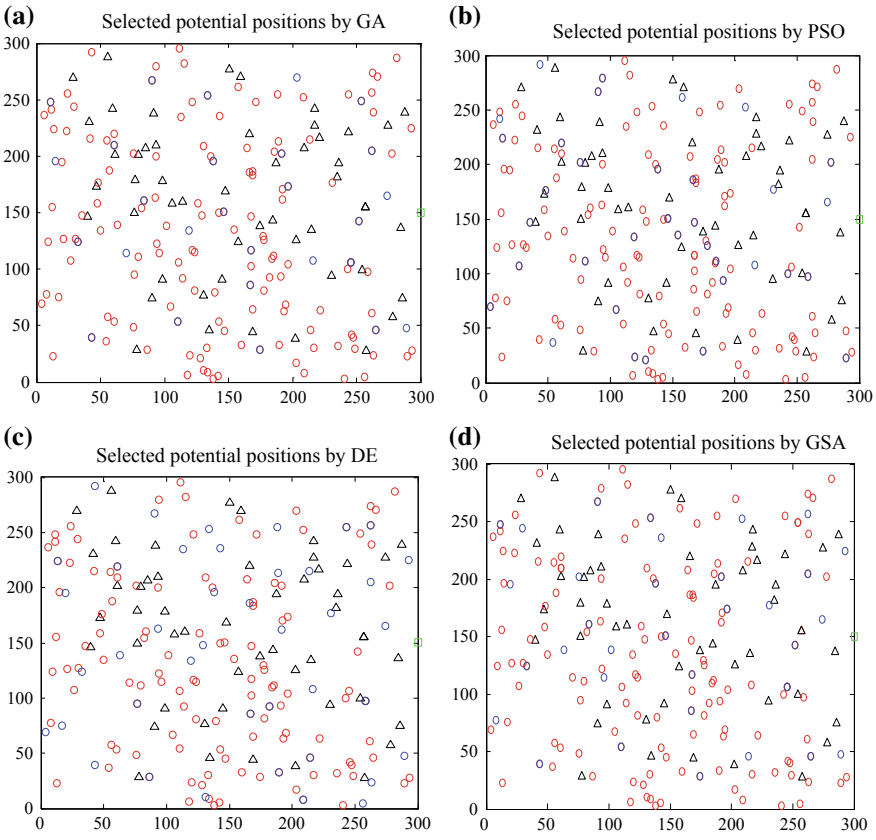


Fig. 4 Selection of potential positions by **a** GA, **b** PSO, **c** DE, and **d** GSA

Table 1 Simulation parameters

PSO		DE		GA	GSA	
c_1	1.4962	CR	0.7	Mutation rate 3%	G_0	3
c_2	1.4962	F	0.5		β	1
w	0.7968					
$v_{\max}$	0.5					
$v_{\min}$	−0.5					

precisely and accurately finalize the weight values. Therefore, we have tested for various combinations of the weight values and found a better result for $w_1 = 0.3$, $w_2 = 0.3$, and $w_3 = 0.4$. Therefore, we have taken the same.

We first execute the algorithms for $k = 1$ and $m = 1$ with randomly placed 50 target points and 150 potential positions. We have taken the sensing and communication range as 40 meters and 70 meters, respectively. The selected potential positions for the algorithms are shown in Fig. 4a–d. It can be seen that the PSO, DE, GA, and GSA select 36, 41, 27, and 33 potential positions, respectively. The objective 1 of the derived fitness function forces to select minimum number of sensor nodes. Other two fitness functions ensure coverage and connectivity.

We have also executed the simulation by varying the value of k from 1 to 3 and m from 1 to 3. The number of selected potential positions by the algorithms with varying the number of target points is shown in Fig. 5a–c. From Fig. 5a–c, it can also be observed that as the number of target points increases corresponding potential positions also increases for different values of k and m.

9 Conclusion

In this chapter, we have presented four nature-inspired algorithms, namely, GA-, PSO-, DE-, and GSA-based approach for the deployment of sensor nodes. The objectives for the deployment of sensor nodes are as selection of minimum number of potential positions for the placement of sensor nodes such that all the target points are k-covered along with m-connectivity among the placed sensor nodes. Linear programming is also formulated. Efficient representations of chromosome, particle, vector, and agents are illustrated for GA, PSO, DE, and GSA, respectively. To evaluate the solutions, derivation of an efficient fitness function is given by considering all the objectives. An extensive simulation is conducted for all the algorithms by varying the number of k and m, and target points. As all the algorithms are executed with the same derived fitness function, it is very hard to conclude and compare the performance among them. While, for a particular scenario, GA is proving better performance, for some other scenario, GSA may provide better.

In large industries, the scheme can be used to monitor some critical points like gas leakage, fire zone, etc. As the problem is multi-objective in nature, some suitable

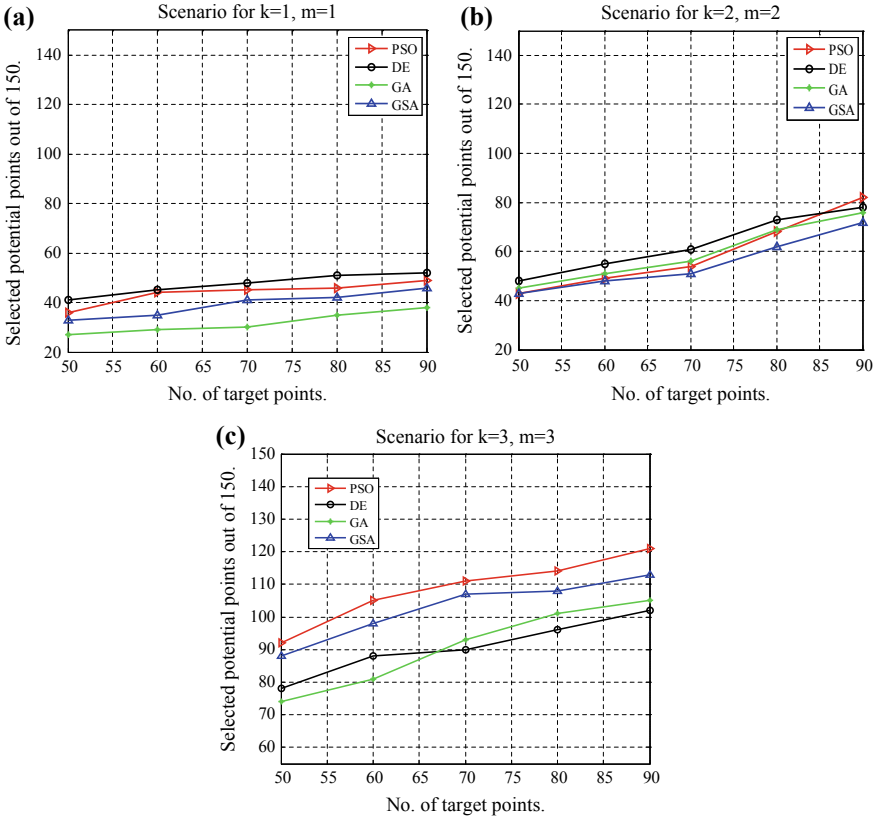


Fig. 5 Selection of potential positions by varying the number of target points for **a** $k = 1, m - 1$, **b** $k = 2, m - 2$, and **c** $k = 3, m - 3$

multi-objective evolutionary algorithm (MOEA) may be employed for the same. Mobility of the sensor nodes is not considered. The works may be extended by considering the mobility of the sensor nodes. Moreover, energy consumption of the sensor nodes is also not considered.

References

1. Kuila, P., & Jana, P. K. (2014). Energy efficient clustering and routing algorithms for wireless sensor networks: Particle swarm optimization approach. *Engineering Applications of Artificial Intelligence, 33,* 127–140.
2. El-Fouly, F. H., Ramadan, R. A., Mahmoud, M. I., & Dessouky, M. I. (2018). REBTAM: Reliable energy balance traffic aware data reporting algorithm for object tracking in multi-sink wireless sensor networks. *Wireless Networks, 24*(3), 735–753.

3. Kuila, P., & Jana, P. K. (2017). *Clustering and routing algorithms for wireless sensor networks: Energy efficient approaches* (1st ed.). CRC Press (Taylor & Francis Group). ISBN-13: 978-1498753821.
4. Gupta, S. K., Kuila, P., & Jana, P. K. (2014). E^3BFT: Energy efficient and energy balanced fault tolerance clustering in wireless sensor networks. In *IC3I 2014*, IEEE Xplore (pp. 714–719).
5. Rault, T., Bouabdallah, A., & Challal, Y. (2014). Energy efficiency in wireless sensor networks: A top-down survey. *Computer Networks, 67,* 104–122.
6. Muduli, L., Mishra, D. P., & Jana, P. K. (2018). Application of wireless sensor network for environmental monitoring in underground coal mines: A systematic review. *Journal of Network and Computer Applications, 106,* 48–67.
7. Azharuddin, Md., Kuila, P., & Jana, P. K. (2015). Energy efficient fault tolerant clustering and routing algorithms for wireless sensor networks. *Computers & Electrical Engineering*, *41*, 177–190. (Elsevier).
8. Kuila, P., & Jana, P. K. (2012) An energy balanced distributed clustering and routing algorithm for wireless sensor networks. In *PDGC 2012*, IEEE Xplore (pp. 220–225).
9. Azharuddin, Md., Kuila, P., & Jana, P. K. (2013). A distributed fault-tolerant clustering algorithm for wireless sensor networks. In *2nd ICACCI 2013*, IEEE Xplore (pp. 997–1002).
10. Rebai, M., Snoussi, H., Hnaien, F., & Khoukhi, L. (2015). Sensor deployment optimization methods to achieve both coverage and connectivity in wireless sensor networks. *Computers & Operations Research, 59,* 11–21.
11. Harizan, S., & Kuila, P. (2019). Coverage and connectivity aware energy efficient scheduling in target based wireless sensor networks: An improved genetic algorithm based approach. *Wireless Networks*, *25*(4), 1995–2011.
12. Karatas, M. (2018). Optimal deployment of heterogeneous sensor networks for a hybrid point and barrier coverage application. *Computer Networks, 132,* 129–144.
13. Gupta, S. K., Kuila, P., & Jana, P. K. (2016). Genetic algorithm for k-connected relay node placement in wireless sensor networks. In *Proceedings of the Second International Conference on Computer and Communication Technologies* (Vol. 379, pp. 721–729). In *AISC*. Springer.
14. Gupta, S. K., Kuila, P., & Jana, P. K. (2016). Genetic algorithm approach for k-coverage and m-connected node placement in target based wireless sensor networks. *Computers & Electrical Engineering, 56,* 544–556.
15. Dey, N., Ashour, A. S., Shi, F., Fong, S. J., & Sherratt, R. S. (2017). Developing residential wireless sensor networks for ECG healthcare monitoring. *IEEE Transactions on Consumer Electronics, 63*(4), 442–449.
16. Cardei, I., & Cardei, M. (2008). Energy-efficient connected-coverage in wireless sensor networks. *International Journal of Sensor Networks, 3*(3), 201–210.
17. Rout, M., & Roy, R. (2017). Optimal wireless sensor network information coverage using particle swarm optimisation method. *International Journal of Electronics Letters, 5*(4), 491–499.
18. Sharma, D., & Gupta, V. (2017). Improving coverage and connectivity using harmony search algorithm in wireless sensor network. In *International Conference on Emerging Trends in Computing and Communication Technologies (ICETCCT)* (pp. 1–7). IEEE.
19. Zungeru, A. M., Ang, L. M., & Seng, K. P. (2012). Classical and swarm intelligence based routing protocols for wireless sensor networks: A survey and comparison. *Journal of Network and Computer Applications, 35*(5), 1508–1536.
20. Kuila, P., & Jana, P. K. (2016). Evolutionary computing approaches for clustering and routing in wireless sensor networks. In *Handbook of research on natural computing for optimization problems* (pp 246–266). IGI Global. ISBN: 9781522500582.
21. Deif, D. S., & Gadallah, Y. (2017). An ant colony optimization approach for the deployment of reliable wireless sensor networks. *IEEE Access, 5,* 10744–10756.
22. Gupta, S. K., Kuila, P., & Jana, P. K. (2013). Delay constraint energy efficient routing using multi-objective genetic algorithm in wireless sensor networks. In *ICECCS 2013* (pp. 50–59). Tata McGraw-Hill.
23. Binh, H. T. T, & Dey, N. (2018). *Soft computing in wireless sensor networks*. CRC Press.

24. Binh, H. T. T., Hanh, N. T., & Dey, N. (2018). Improved cuckoo search and chaotic flower pollination optimization algorithm for maximizing area coverage in wireless sensor networks. *Neural Computing and Applications, 30*(7), 2305–2317.
25. Gupta, S. K., Kuila, P., & Jana, P. K. (2016). Energy efficient multipath routing for wireless sensor networks: A genetic algorithm approach. In *5th ICACCI 2016*, IEEE Xplore (pp. 1735–1740).
26. Qasim, T., Mujahid, A., Bhatti, N. A., Mushtaq, M., Saleem, K., Mahmood, H., et al. (2018). ACO-Discreet: An efficient node deployment approach in wireless sensor networks. In *Information technology-new generations* (pp. 43–48). Springer.
27. Xu, Y., Ding, O., Qu, R., & Li, K. (2018). Hybrid multi-objective evolutionary algorithms based on decomposition for wireless sensor network coverage optimization. *Applied Soft Computing*, *68*, 268–282.
28. El-Sherif, M., Fahmy, Y., & Kamal, H. (2018). Lifetime maximization of disjoint wireless sensor networks using multiobjective genetic algorithm. *IET Wireless Sensor Systems, 8*(5), 200–207.
29. Wang, J., Ju, C., Gao, Y., Sangaiah, A. K., & Kim, G. J. (2018). A PSO based energy efficient coverage control algorithm for wireless sensor networks. *Computers, Materials & Continua, 56*(3), 433–446.
30. Golberg, D. E. (1989). *Genetic algorithms in search, optimization, and machine learning* (Vol. 1989, No. 102, p. 36). Addison Wesley.
31. Kuila, P., Gupta, S. K., & Jana, P. K. (2013). A novel evolutionary approach for load balanced clustering problem for wireless sensor networks. *Swarm and Evolutionary Computation, 12,* 48–56. (Elsevier).
32. Gupta, S. K., Kuila, P., & Jana, P. K. (2013). GAR: An energy efficient GA-based routing for wireless sensor networks. In *LNCS* (Vol. 7753, pp. 267–277). Springer.
33. Gupta, S. K., Kuila, P., & Jana, P. K. (2016). GA based energy efficient and balanced routing in k-connected wireless sensor networks (Vol. 458, pp. 679–686). In *AISC.* Springer.
34. Bose, A., Biswas, T., & Kuila, P. (2019). A novel genetic algorithm based scheduling for multi-core systems (Vol. 851, pp. 45–54). In *AISC.* Springer.
35. Kennedy, J. (2010). Particle swarm optimization. *Encyclopedia of Machine Learning*, 760–766.
36. Panag, T. S., & Dhillon, J. S. (2018). A novel random transition based PSO algorithm to maximize the lifetime of wireless sensor networks. *Wireless Personal Communications, 98*(2), 2261–2290.
37. Storn, R. (1995). Differential evolution—A simple and efficient adaptive scheme for global optimization over continuous spaces. Technical report, International Computer Science Institute, 11.
38. Kuila, P., & Jana, P. K. (2014). A novel differential evolution based clustering algorithm for wireless sensor networks. *Applied Soft Computing, 25,* 414–425. (Elsevier).
39. Qin, N. N., & Chen, J. L. (2018). An area coverage algorithm for wireless sensor networks based on differential evolution. *International Journal of Distributed Sensor Networks, 14*(8), 1550147718796734.
40. Rashedi, E., Nezamabadi-Pour, H., & Saryazdi, S. (2009). GSA: A gravitational search algorithm. *Information Sciences, 179*(13), 2232–2248.
41. Gupta, S. K., Kuila, P., & Jana, P. K. (2016). Energy efficient routing algorithm for wireless sensor networks: A distributed approach. In *Communication and Computing Systems: Proceedings of the International Conference on Communication and Computing Systems (ICCCS 2016)* (pp. 207– 213) CRC Press, Taylor & Francis Group.
42. Singh, D., Kuila, P., & Jana, P. K. (2014). A distributed energy efficient and energy balanced routing algorithm for wireless sensor networks. In *3rd ICACCI 2014*, IEEE Xplore (pp. 1657–1663).
43. Kuila, P., & Jana, P. K. (2014). Approximation schemes for load balanced clustering in wireless sensor networks. *Journal of Supercomputing, 68,* 87–105. (Springer).
44. Kuila, P., & Jana, P. K. (2014). Heap and parameter based load balanced clustering algorithms for wireless sensor networks. *International Journal of Communication Networks and Distributed Systems*, *14*(4), 413–432.

45. Kuila, P., & Jana, P. K. (2012). Improved load balanced clustering algorithm for wireless sensor networks. In *LNCS* (Vol. 7135, pp. 399–404). Springer.
46. Kuila, P., & Jana, P. K. (2012). Energy efficient load-balanced clustering algorithm for wireless sensor networks. *Procedia Technology, 6,* 771–777. (Elsevier).
47. Konak, A., Coit, D. W., & Smith, A. E. (2006). Multi-objective optimization using genetic algorithms: A tutorial. *Reliability Engineering & System Safety, 91*(9), 992–1007.

Swarm Intelligent Based Detection in the Uplink of Large-Scale MIMO Wireless Communication Systems

Arijit Datta, Manish Mandloi and Vimal Bhatia

Abstract Large-scale multiple-input multiple-output (MIMO) system plays a vital role in realizing the ever-increasing demand for high-speed data in 5G and beyond wireless communication systems. MIMO systems employ multiple antennas at both the transmitter and receiver. These systems can achieve both the spatial diversity and the spatial multiplexing gain, which are required for enhancing the quality of service (QoS) and the capacity of wireless systems, respectively. Howbeit, reliable detection of the transmitted data streams is challenging due to the presence of inter-channel interference and inter-user interference. To address the above symbol detection issues, maximum likelihood (ML) (Van Trees, Detection, estimation, and modulation theory, part I: detection, estimation, and linear modulation theory, 2004, [34]) detection performs an exhaustive search over all the possible transmitted information symbols and achieves optimal bit error rate (BER) performance. However, being an NP-Hard problem, ML detection is practically unfeasible for large MIMO systems. Therefore, alternate low-complexity robust detection techniques are being devised for near-optimal detection in large MIMO systems. Nature-inspired algorithms have been an emerging choice to obtain a better solution for combinatorial optimization problems. Recently, nature-inspired algorithms has attracted the attention of researchers from wireless communication community, due to its simple implementation and low-complexity behaviour in solving research problems in communication. In this chapter, we have discussed some of the promising bio-inspired techniques such as ant colony optimization and social spider optimization, and introduced one of the key applications of these algorithms, that is, to solve the combinatorial optimization problem of symbol detection in large-scale MIMO systems. We have also

A. Datta (✉) · V. Bhatia
Discipline of Electrical Engineering, IIT Indore, Indore, Madhya Pradesh, India
e-mail: phd1601102003@iiti.ac.in

V. Bhatia
e-mail: vbhatia@iiti.ac.in

M. Mandloi
Department of Electronics and Telecommunications Engineering, SKVM's NMIMS (Deemed to be University), Shirpur Campus, Shirpur 425405, Maharashtra, India
e-mail: manishmandloi1@gmail.com

S. K. Das et al. (eds.), *Design Frameworks for Wireless Networks*,
Lecture Notes in Networks and Systems 82,
https://doi.org/10.1007/978-981-13-9574-1_13

compared the BER performance of different bio-inspired algorithms with the traditional low-complexity detection techniques such as zero forcing and minimum mean squared error detectors.

Keywords Large MIMO systems · Ant colony optimization · Social spider optimization · Maximum likelihood · Spectral efficiency

1 Introduction

Over the past decade, wired devices are being replaced by wireless devices due to the rapid growth of wireless technology. Hence, data traffic conveyed by these wireless devices is soaring. As indicated by CISCO's virtual networking index, global mobile data traffic will grow sevenfold from 2016 to 2021, reaching 48.3 Exabyte per month. The possible remedy to support this ever-growing data traffic is to yield high data speed along with high spectral efficiency. The channel capacity of the conventional single input single output (SISO) wireless communication system grows exponentially with the signal-to-noise (SNR) ratio [8]. Hence, to keep up with high data rates requirements in SISO, either transmit power or allocated bandwidth must be high. Since wireless system suffers from a paucity of bandwidth and is constrained to transmit power (to improve battery lifetime, to avoid inter-user interference, to prevent health hazards etc.), SISO systems are not the ultimate panacea to achieve high data rates for 5G and beyond wireless communication systems.

Multiple input multiple output (MIMO) wireless communication systems employ a multiple number of transmit and receive antennas and are capable to yield high-speed data along with high spectral efficiency. Hence, MIMO becomes a promising candidate for 5G and beyond wireless communication systems to meet the ever-increasing requirement for high data rates while maintaining both the constraints on transmit power and bandwidth [37]. Large MIMO systems with a large number of transmit antenna are capable to serve a large number of receive antennas over the same time and frequency band. As a consequence, large MIMO systems take advantage of spatial diversity and spatial multiplexing [30]. High diversity gain and spatial multiplexing, respectively, yield high link reliability and high multiplexing. Moreover, the achievable data rates from the MIMO system increases linearity with the number of antennas. Hence, large MIMO is a key technology for 5G and beyond wireless communication systems.

Though large MIMO systems provide high-speed data, the benefits of large MIMO systems for practical realization are blocked by high computational complexity for symbol detection in large MIMO systems [8, 30]. The optimal symbol detection for a large MIMO system is possible by maximum likelihood (ML) detection, considering the fact that the transmitted symbols are equiprobable. However, symbol detection with ML for a large MIMO system is a non-deterministic polynomial-time hard (NP-Hard) problem and requires exponential computational complexity with respect to the signal constellation [8]. Hence, ML detection is practically unacceptable for large

MIMO systems. To alleviate the computational load, linear detection techniques [8, 30] such as zero forcing (ZF) and minimum mean square error (MMSE) detection are proposed in the literature. Both ZF and MMSE require cubic computational complexity [5] for a large MIMO system. However, ZF and MMSE yield far inferior BER performance as compared to ML detection for large MIMO systems. To further improve the performance for large MIMO detection, nonlinear detection techniques [8] such as zero forcing successive interference cancellation (ZF-SIC), zero forcing ordered successive interference cancellation (ZF-OSIC), minimum mean square error successive interference cancellation (MMSE-SIC) and minimum mean square error ordered successive interference cancellation (MMSE-OSIC) are introduced in the literature. MMSE utilizes Tikhonov regularization and provides superior BER performance as compared to ZF. In ZF-SIC and MMSE-SIC, inter-user interference is successively cancelled during detection, consequently providing superior BER performance as compared to ZF and MMSE, respectively. ZF-OSIC and MMSE-OSIC successively detect the transmitted symbol based on a predefined order, and hence outperform ZF-SIC and MMSE-SIC, respectively. However, ZF, MMSE, ZF-SIC, MMSE-SIC, ZF-OSIC, MMSE-OSIC are capable to yield far inferior BER performance when compared to ML detection. Hence, the present research focus is to develop a low-complexity near-ML performance algorithm for symbol detection in large MIMO systems.

Several other well-known low-complexity symbol detection algorithms for large MIMO systems are multistage likelihood ascent search (MLAS) [29], random restart reactive Tabu search [13] (R3TS) and belief propagation (BP) [33]. MLAS performs multiple stages of likelihood ascent search (LAS) and outperforms MMSE-OSIC. However, multiple sequences of LAS increase its computational load and the performance depends on the initial solution. R3TS utilizes random initial points to perform parallel search stages of reactive Tabu search (RTS) [19], R3TS is a suitable detection technique for large MIMO systems with higher order modulation. However, the performance of R3TS degrades under imperfect channel state information (CSI) at the receiver. BP is a low-complexity graphical method, however, the BER performance of BP algorithm degrades for higher order modulation. Hence, other low-complexity alternatives need to be investigated for reliable symbol detection in large MIMO system under both perfect and imperfect CSI at the receiver.

Over the last several years, swarm and evolutionary techniques attract keen interest among communication researchers. Particle swarm optimization (PSO) [17], ant colony optimization (ACO) [15], genetic algorithm (GA) [28] and gravitational search algorithm (GSA) [31] are mostly explored algorithms to solve complex problems in communication and signal processing. There exist three variants of PSO for symbol detection in large MIMO systems, namely (a) binary particle swarm optimization (BPSO) [23], (b) standard particle swarm optimization (SPSO) [16] and (c) memetic particle swarm optimization (MPSO) [23]. However, PSO-based large MIMO detection algorithms suffer from early convergence to local minima. ACO and binary ant colony optimization (BACO) [24] are also proposed in the literature for symbol detection in the uplink of large MIMO systems. Though ACO-based detection techniques for large MIMO systems outperforms PSO-based detection, however,

BER performance of ACO-based detection algorithms degrades under imperfect CSI at the receiver. To improve the BER performance of ACO-based detection, congestion control ant colony optimization [26] (CCACO) is proposed in the literature. CCACO outperforms MPSO, BPSO, SPSO, ACO and BACO under CSI errors at the receiver. However, the computational complexity of CCACO increases with the number of antennas and population size. Moreover, CCACO shows inferior performance than the ML technique when the number of antennas scales up in the system. GA and GSA outperform conventional linear and nonlinear detection algorithm for small MIMO systems; however, the performance of both GSA and GA degrades for higher modulation schemes. As a consequence, alternative meta-heuristic technique which is capable to eliminate the drawbacks of existing techniques must be explored and developed for low complexity and reliable symbol detection in uplink large MIMO systems.

In this chapter, ACO and social spider optimizer (SSO) [22] based detection algorithms for symbol detection in a large MIMO system are discussed. ACO is found to be a superior alternative to avoid the early convergence issue of PSO. On the other hand, due to information propagation technique of SSO, SSO outperforms several existing swarm intelligence algorithms in the literature. All these motivate to explore ACO and SSO for low-complexity symbol detection in uplink large MIMO systems. Rest of this chapter is organized as follows. The system model for a large MIMO system is discussed in Sect. 2. Section 3 gives a brief overview of conventional large MIMO detection techniques. SSO and ACO based on large MIMO detection algorithms are discussed in Sect. 4 and Sect. 5 respectively. Simulation results are drawn in Sect. 6. Finally, Sect. 7 concludes the chapter.

2 System Model

Consider an uplink large MIMO system model with N_r base station (BS) antennas and N_t single antenna users. The received symbol vector, after demodulation and sampling, is expressed as [5]

$$\tilde{\mathbf{y}} = \tilde{\mathbf{H}}\tilde{\mathbf{x}} + \tilde{\mathbf{n}}$$

where $\tilde{\mathbf{y}}$ is $N_r \times 1$ complex received symbol vector, $\tilde{\mathbf{x}}$ is $N_t \times 1$ transmitted symbol vector, $\tilde{\mathbf{H}}$ is $N_r \times N_t$ complex Gaussian channel matrix with zero mean and unit variance. $\tilde{\mathbf{n}}$ is $N_r \times 1$ a complex additive white Gaussian noise with zero mean and variance σ^2. Without loss of generality, the above complex-valued system model is converted to a real-valued system model as

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n}$$

where $\mathbf{y}$ is $2N_r \times 1$ a real-valued received symbol, $\mathbf{x}$ is $2N_t \times 1$ transmitted symbol vector, $\mathbf{H}$ is $2N_r \times 2N_t$ real-valued channel matrix. $\mathbf{n}$ is $2N_r \times 1$ real-valued additive

white Gaussian noise vector. **H**, **y** and **n** are computed as

$$\mathbf{x} = \begin{bmatrix} \Re(\tilde{\mathbf{x}}) \\ \Re(\tilde{\mathbf{x}}) \end{bmatrix}_{2N_t \times 1} \quad \mathbf{y} = \begin{bmatrix} \Re(\tilde{\mathbf{y}}) \\ \Re(\tilde{\mathbf{y}}) \end{bmatrix}_{2N_r \times 1}$$

$$\mathbf{n} = \begin{bmatrix} \Re(\tilde{\mathbf{n}}) \\ \Re(\tilde{\mathbf{n}}) \end{bmatrix}_{2N_r \times 1} \quad \mathbf{H} = \begin{vmatrix} \Re\left(\tilde{\mathbf{H}}\right) & -\Im\left(\tilde{\mathbf{H}}\right) \\ \Im\left(\tilde{\mathbf{H}}\right) & \Re\left(\tilde{\mathbf{H}}\right) \end{vmatrix}_{2N_r \times 2N_t}$$

The information of perfect CSI at the BS is necessary for symbol detection in uplink large MIMO systems. CSI estimation [3] is performed generally through two methods (a) trained based approach [25] and (b) blind/semi-blind approach [27]. In training based approach, pilot symbols are transmitted that are known by the receiver. On the other hand, blind/semi-blind approach performs channel estimation without utilizing training symbols. Though blind/semi-blind approaches for channel estimation has higher bandwidth efficiency, training-based approaches dominate blind-based approach due to lower speed and poor performance of the blind-based approach. Howbeit, in practice, there exists imperfection in CSI estimation at the receiver [4], the large MIMO system model, under CSI estimation error at the receiver, is represented as

$$\mathbf{y} = \hat{\mathbf{H}}\mathbf{x} + \mathbf{n},$$

where $\hat{\mathbf{H}} = \mathbf{H} + \mathrm{e}\boldsymbol{\theta}$. H is the actual channel gain matrix. $\mathrm{e}\boldsymbol{\theta}$ is called the estimation error. For mathematical tractability, the elements of $\boldsymbol{\theta}$ are considered to be independent and identically distributed (i.i.d) complex Gaussian random variable with zero mean and unit variance. The parameter e denotes the accuracy of channel estimation. A pictorial view of the large MIMO system is shown in Fig. 1

3 Traditional Detection Techniques

In this section, traditional detection algorithms for low-complexity symbol detection in large MIMO systems are discussed.

3.1 Zero Forcing

Zero forcing (ZF) [8] is one of the linear detection techniques for symbol detection in large MIMO systems. Linear detection technique generates a soft estimate of the transmitted symbol using the linear transformation matrix **G**. In ZF detection, the large MIMO detection problem is formulated as

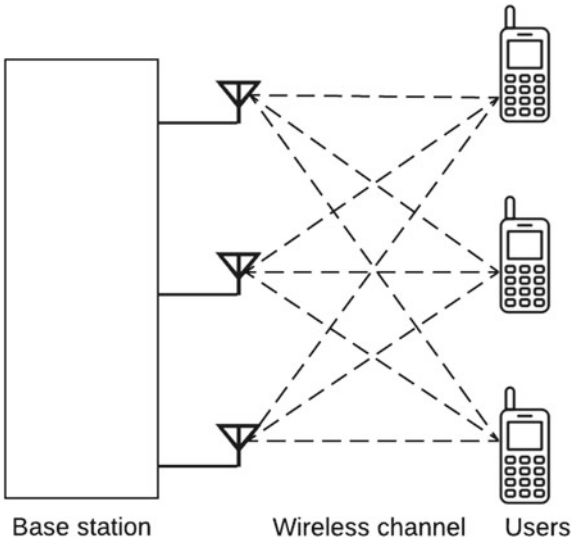


Fig. 1 Large MIMO system

$$\hat{\mathbf{x}} = \underset{\mathbf{x}\in A}{\arg min} ||\mathbf{y} - \mathbf{H}\mathbf{x}||_2^2$$

Hence, the objective of the MIMO detection problem is to minimize the objective function

$$f(\mathbf{x}) = ||\mathbf{y} - \mathbf{H}\mathbf{x}||_2^2$$

Taking the gradient of the objective function and equating the gradient to zero, we get

$$-2\mathbf{H}^T(\mathbf{y} - \mathbf{H}\mathbf{x}) = 0$$

Hence, the estimated symbol vector $\hat{\mathbf{x}}$ can be expressed in terms of the channel matrix $\mathbf{H}$ and received symbol y as

$$\begin{aligned}\hat{\mathbf{x}} &= \left(\mathbf{H}^T\mathbf{H}\right)^{-1}\mathbf{H}^T\mathbf{y} \\ &= \mathbf{G}\mathbf{y},\end{aligned}$$

where $\mathbf{G} = \left(\mathbf{H}^T\mathbf{H}\right)^{-1}\mathbf{H}^T$ is the linear transformation matrix that transforms the received symbol vector $\mathbf{y}$. $(.)^{\mathrm{T}}$ denotes matrix transpose. $\mathbf{G}$ is called the pseudoinverse of the channel matrix $\mathbf{H}$. ZF exhibits cubic computational complexity in terms of number of antennas and yields superior performance than the matched filter (MF) at high SNR region. However, at low SNR, the performance of ZF degrades due to

noise enhancement effect. Moreover, the performance of the ZF detector severely degrades with the number of antennas.

3.2 Minimum Mean Square Error

Minimum mean square error (MMSE) [8] is another linear detection technique, which is a special case of Tikhonov regularization. MMSE takes the noise variance as the regularization parameter and outperforms ZF detection. In MMSE, the large MIMO detection problem is formulated using L2-regularization as

$$\hat{\mathbf{x}} = \underset{\mathbf{x}\in A}{\arg min} ||\mathbf{y} - \mathbf{H}\mathbf{x}||_2^2 - N_0||\mathbf{x}||_2^2$$

Equating the gradient of the objective function to zero, we get

$$-2\mathbf{H}^{\mathbf{T}}(\mathbf{y} - \mathbf{H}\mathbf{x}) - 2\mathrm{N}_0\mathbf{x} = 0,$$
$$\hat{\mathbf{x}} = \mathbf{G}\mathbf{y}$$

where $\mathbf{A} = \left(\mathbf{H}^{\mathbf{T}}\mathbf{H} + \mathrm{N}_0\mathbf{I}_{2\mathbf{N_t}}\right)$ is called the MMSE filter matrix and $\mathbf{G} = \mathbf{A}^{-1}\mathbf{H}^{\mathbf{T}}$ is the linear transformation matrix for MMSE detection At high SNR, the regularization term becomes negligible and consequently, MMSE behaves like ZF at high SNR. However, MMSE outperforms ZF at low SNR. Though MMSE requires cubic computational complexity in terms of the number of antennas, the performance of MMSE also severely degrades with the number of antennas.

3.3 Maximum Likelihood Detection and Sphere Decoder

Maximum likelihood (ML) detection is a detection technique to yield optimal BER performance for large MIMO systems. ML minimizes the probability of erroneous decision of a symbol by considering all valid symbols in the constellation set. Consequently, the computational complexity of ML detection exponentially increases with the number of antennas. Hence, ML detection is practically infeasible for large MIMO systems with higher order constellations.

To reduce the computational load of ML detection, sphere decoder (SD) [1] is introduced in the literature, which utilizes the underlying lattice structure of the received signal. Hence, SD seems to be a promising solution for low-complexity symbol detection in the uplink of large MIMO systems. However, the computational complexity of SD depends on the channel condition and noise level, and consequently, SD has an exponential lower bound on complexity. Hence, SD is not realizable for practical systems where data processing at a constant rate is required.

In order to further improve the computational complexity of the SD, several improved SD techniques are proposed in the literature. These techniques can be classified into three broad categories [2, 7, 20, 21], (a) ordering techniques, (b) probabilistic techniques and (c) sequential M-algorithm-based techniques. However, all the above techniques yield variable computational complexity. Moreover, both preprocessing stage in ordering techniques and threshold computation stage in probabilistic stage require an additional number of computations. On the other hand, sequential M-algorithm based techniques require considerably higher computational complexity as compared to SD.

The issue of variable complexity of SD techniques is addressed in fixed sphere decoder (FSD) [36]. FSD solves the issue of variable complexity by restricting the search over a fixed number of transmitted symbols. However, FSD posses comparatively quite high computational complexity as compared to linear detectors and is practically realizable up to 32×32 MIMO systems. Instead of using depth-first tree search (DFTS) [9] as used in SD, a Dijkstra [14] inspired MIMO detection algorithm [10, 12] is also proposed in the literature for large MIMO detection.

4 SSO-Based Large MIMO Detection

In this section, social spider optimization (SSO) based symbol detection algorithm for uplink large MIMO system is discussed. SSO is a swarm intelligence based meta-heuristic technique which is based on the social foraging behaviour of spiders. The motivation behind exploring SSO for large MIMO detection is because of its superior exploration and exploitation capability as compared to PSO and wolf search algorithm (WSA) [35]. In SSO, the search space is considered as a spider wave and the position of a spider in the search space/spider web is the candidate solution. The quality of a solution is related to the objective function. SSO algorithm works on the following basic assumptions:

- A spider's position outside the web is assumed to be infeasible.
- The quality of the solution degrades with the value of the objective function at a position.
- The intensity of vibration inside the web is positive.
- The intensity of vibration from the global optimum position must not malfunction the scheme of vibration in the system.

A flowchart of the conventional SSO algorithm is shown in Fig. 2. However, conventional SSO is proposed for continuous domain problems and shows inferior performance for large MIMO systems. Moreover, conventional SSO is based on Markovian process [6] and consequently, each step is independent of the exploration history. As a result, conventional SSO results in rapid convergence to a locally optimal solution for uplink large MIMO systems.

The limitations of existing SSO are addressed in binary social spider optimizer (BSSO). BSSO utilizes both cognitive and social information of the spider swarm.

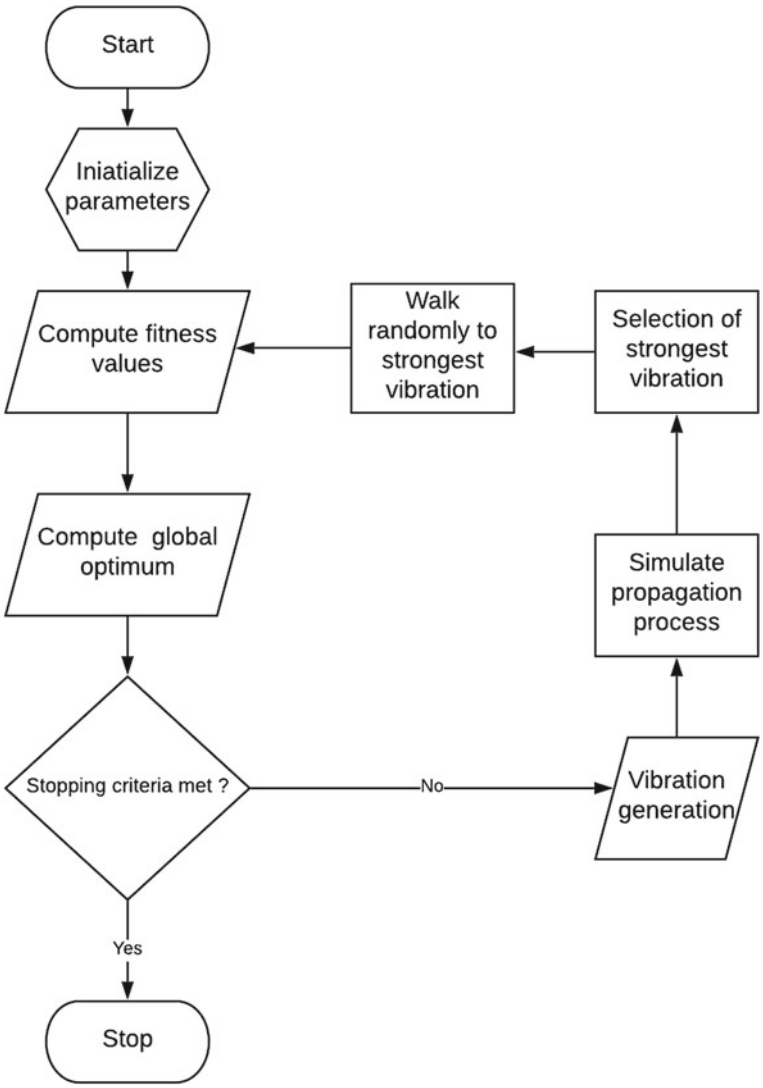


Fig. 2 Flowchart of the conventional SSO

In BSSO, the symbol is updated using the following rule for 4-QAM modulation

$$x_i^d(t) = \begin{cases} -1, & if\ \xi\left(x_i^d(t)\right) \geq \alpha \\ 1, & otherwise \end{cases}$$

where $\zeta(.)$ is the mapping function defined as

$$\xi(t) = \frac{v_i^d(t)e^{-g_i^d(t)}}{\sum_j v_j^d(t)e^{-g_j^d(t)}},$$

where, $\boldsymbol{g}_i^d(t+1) = c_1\omega_1\boldsymbol{g}_i^d(t) + c_2\beta_1\left(x_{lBest}^d - x_i^d(t)\right) + c_3\beta_2\left(x_{gbest}^d - x_i^d(t)\right) + esc()$.

The function $esc()$ is the escape function used by BSSO to improve the exploration capability of conventional SSO. x_{lBest} and x_{gBest} are, respectively, the local and global best solution achieved so far. ω_1, β_1 and β_2 are weight, cognitive and social best coefficients. c_1, c_2 and c_3 are uniformly generated random variables. BSSO uses information propagation technique which yields faster convergence in BSSO as compared to both PSO and ACO. In BSSO, the vibration intensity sensed at the ith position in dimension d from position s is denoted as

$$v_i^d(t) = v_0^d(x_0, x_i, t)e^{-d(x_s,x_i)},$$

where v_0^d is the intensity of vibration at the source. The distance $d(x_s, x_t)$ is computed as

$$d\left(x_i^d, x_s^d\right) = |\hat{y}_i - \sum_{j=1, j\neq i}^{2N_t} r_{ij}x_j - r_{ii}x_i|^2,$$

where $\mathbf{R}$ is the upper triangular matrix obtained from $\mathbf{H}$ and $\hat{y}_i \in \mathbf{Q^T y}$. $\mathbf{Q}$ is an unitary matrix. The pseudocode of BSSO is given in Algorithm 1 (Fig. 3).

Algorithm: BSSO for large MIMO detection

Input: $\mathbf{y}, \mathbf{H}, N_t, N_r$
Output: $\mathbf{x}_{gBest}$ (The global best solution)
for $k = 1 : Max\ number\ of\ generation$ **do**
  while $j \leq No\ of\ spiders$ **do**
    Calculate vibration $v_o^d(x_o, x_i, j)$ for each spider j at each direction i
    for $i \leq No\ of\ antennas$ **do**
      Update distance parameter, $d(x_s, x_i)$
      Compute vibration intensity, $v_i(t) = v_o(x_o, x_i, j)e^{-d(x_s,x_i)}$
      Compute function ζ
      Update symbol x_i based on function ζ
    end
    Update local best solution, $\mathbf{x}_{lBest}$
    $j = j + 1$
  end
  Update global best solution, $\mathbf{x}_{lBest}$
  Compute mapping function, $g(k)$
end

Fig. 3 Algorithm 1

5 ACO-Based Large MIMO Detection

In this section, ant colony optimization (ACO) [15] based symbol detection technique for large MIMO system is discussed. ACO is a nature-inspired optimization algorithm inspired by the foraging behaviour of ants. In ACO-based MIMO detection, the symbol detection problem is modelled as shortest path finding problem like travelling salesman problem (TSP). ACO-based large MIMO detection considers N_{ants} where each ant searches for the optimal path or the transmitted symbol set in each iteration based on a probability metric. In ACO-based MIMO detection technique, the number of cities is assumed to be equal to the transmit antennas N_t and the number of existing paths is equal to the modulation order M. For 4-QAM modulation and $2N_t = 8$, ACO based MIMO detection loosely solves TSP with 4 cities and 8 paths by minimizing the ML cost function.

In ACO-based MIMO detection [26], the ant colony tries to minimize the cost function in such a way that each city is visited just once. The cost function is formulated as

$$f(x) = \sum_{i=1}^{2N_t} d_{ik},$$

where d_{ik} is the distance of the kth path to reach the ith city. The distance is computed as

$$d_{ik} = \left| \hat{y}_i - \sum_{j=i+1}^{2N_t} r_{ij} x_j - r_{ii} x_i \right|$$

The above distance metric contributes to the amount of pheromone to be deposited on a specific path using the following two equations:

$$\eta_{ik} = \frac{1}{1 + d_{ik}}$$
$$\Delta\tau_{ik} = \eta_{ik} p_{ik}$$

Finally, a probability metric p_{ik} is used for selecting a specific path

$$p_{ik} = \frac{\tau_{ik}^{\alpha}}{\sum_{i=1}^{M} \tau_{ik}^{\alpha}},$$

where τ_{ik} is computed using the following equation

$$\tau_{ik} = \tau_{ik} - \rho\tau_{ik} + \omega\Delta\tau_{ik}$$

Algorithm: ACO based MIMO detection

Input: $\mathbf{y}, \mathbf{H}, \mathbf{R}, \alpha, \rho, \omega, \tau_{ik} = 1$
Output: $\hat{\mathbf{x}}$
while $j \leq$ *Number of ants* **do**
  for $i \leq$ *Number of antennas* **do**
    for $k \leq$ *Modulation order* **do**
      Compute distance parameter, $d_{ik} = \mid \hat{y}_i - \sum_{l=i+1}^{2N_t} r_{il}\tilde{s}_l - r_{ii}s_k \mid$
      Update mapping function, $\eta_{ik} = \frac{1}{1+d_{ik}}$
      Compute probability metric, $p_{ik} = \frac{\tau_{ik}^{\alpha}}{\sum_{i=1}^{M} \tau_{ik}^{\alpha}}$,
    end
    Update symbol $\hat{x}_i$ based on p_{ik}
    for $k \leq$ *Modulation order* **do**
      $\Delta\tau_{ik} = \eta_{ik} p_{ik}$
      Update pheromone level, $\tau_{ik} := \tau_{ik} - \rho\tau_{ik} + \omega\Delta\tau_{ik}$
    end
  end
  Compute new cost, $\hat{\mathbf{d}}_{new} = \| \hat{\mathbf{y}} - \hat{\mathbf{H}}\mathbf{x}^{(j)} \|^2$
  if $d_{new} \leq \hat{d}_{new}$ **then**
    Update global best solution, $\hat{\mathbf{x}} = \mathbf{x}^{(j)}$
    Update global best cost, $\mathbf{d_{best}} = \hat{\mathbf{d}}_{\mathbf{new}}$
  end
end

Fig. 4 Algorithm 2

The pseudocode of the congestion control based ant colony optimization (CCACO) algorithm is given in Algorithm 2 (Fig. 4).

6 Simulation Results and Discussion

In this section, the simulation results are drawn and discussed to compare the BER performances of various conventional and swarm intelligence based large MIMO detection techniques.

Figures 5 and 6 compares the BER performances of BSSO with ZF [8], MMSE [8], MMSE-SIC [8], MMSE-OSIC [8], DE [32], FA [18], SPSO [23] and MGSA [11] for uplink large MIMO wireless systems. As illustrated in Fig. 5, an SNR gain of approximately 5.3 dB is obtained by BSSO in comparison to MGSA for a targeted BER of 2×10^{-3} for 5×5 large MIMO system. Moreover, Fig. 6, shows that the BER performance of BSSO algorithms when the number of antennas is increased to 12. As shown in Fig. 6, conventional detection algorithms yield far inferior performance than BSSO. Moreover, an SNR gain of 3.8 dB is achieved in BSSO as compared to MGSA for a targeted BER of 10^{-2} for 12×12 large MIMO system.

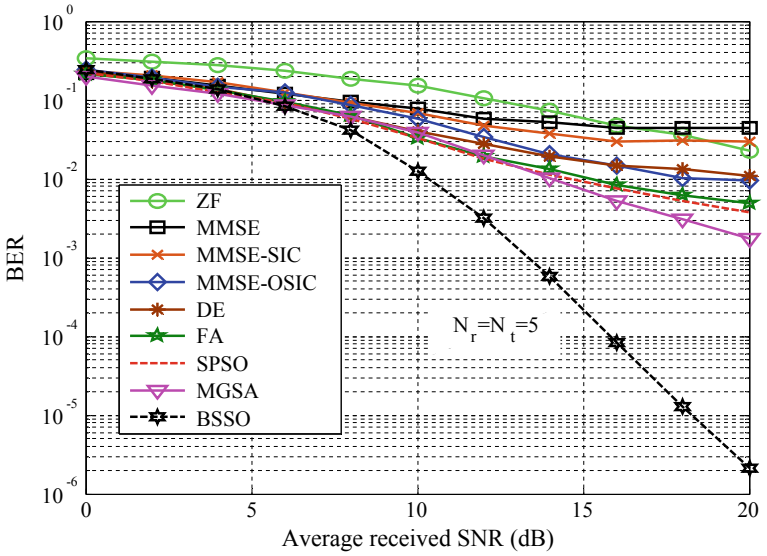


Fig. 5 BER performance of BSSO and conventional large MIMO detection algorithms for $N_r = N_t = 5$ and 4-QAM modulation

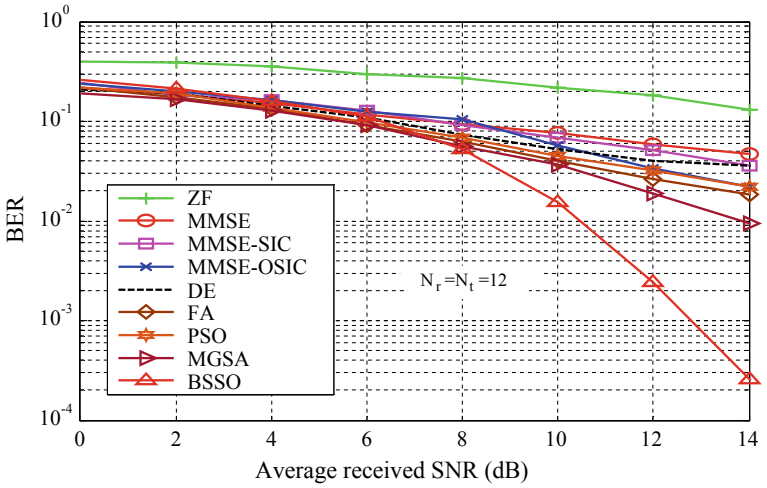


Fig. 6 BER performance of BSSO and conventional large MIMO detection algorithms for $N_r = N_t = 12$ and 4-QAM modulation

The BER performances of CCACO [26] are compared with several other existing large MIMO detection techniques in Figs. 7 and 8 for 5 × 5 and 12 × 12 MIMO systems, respectively. .It is shown in Fig. 7 that approximately 8 dB SNR gain is

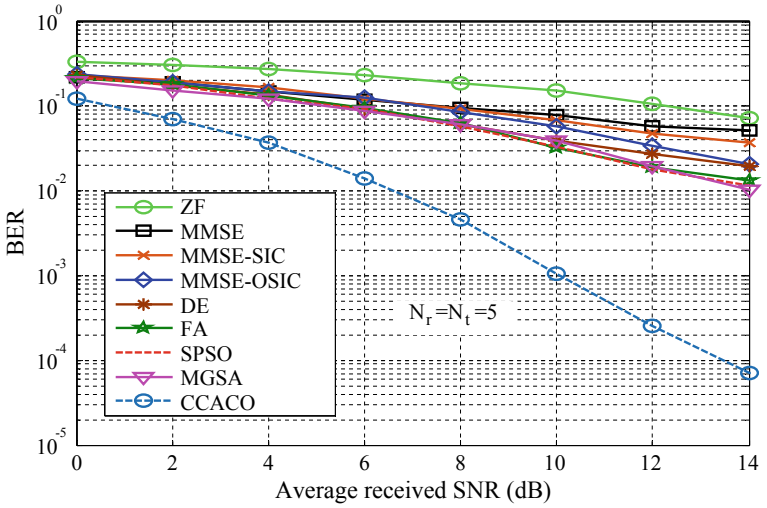


Fig. 7 BER performance of CCACO and conventional large MIMO detection algorithms for $N_r = N_t = 5$ and 4-QAM modulation

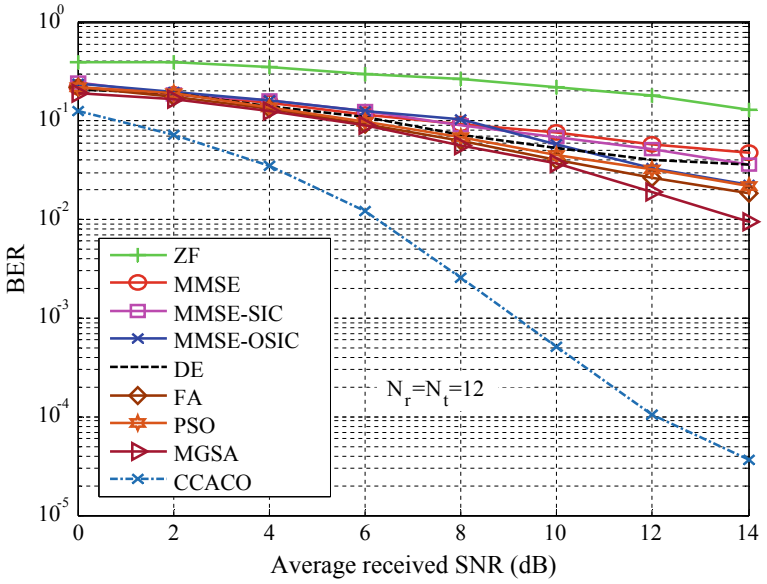


Fig. 8 BER performance of CCACO and conventional large MIMO detection algorithms for $N_r = N_t = 12$ and 4-QAM modulation

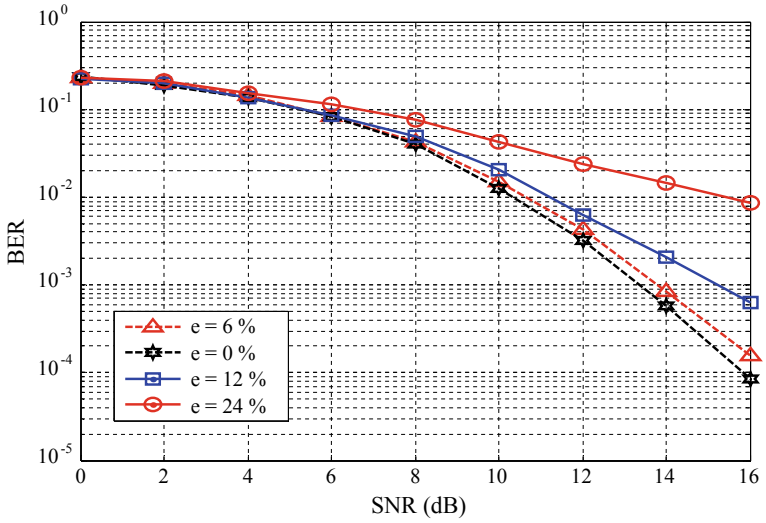


Fig. 9 BER performance of BSSO under different CSI estimation errors at the receiver for $N_r = N_t = 5$ and 4 QAM modulation

observed in CCACO in comparison to MGSA for a targeted BER of 10^{-2}. Furthermore, as depicted in Fig. 8, CCACO also outperforms MGSA when the number of antennas is increased to 12.

The robustness of BBSO and CCACO are validated in Figs. 9 and 10, respectively, for 5×5 large MIMO systems. It is observed that both the algorithms show very little degradation in BER performance even under 6% BER mismatch at the receiver. However, the performances of the algorithms are not satisfactory under severe CSI mismatch scenarios at the receiver. All these make BSSO and CCACO key enabling techniques for reliable and robust low-complexity symbol detection in the large MIMO system.

7 Conclusion

In this chapter, we discuss two swarm intelligence techniques namely ACO and SSO and their application in solving the combinatorial optimization problem of symbol detection in large-scale MIMO wireless communication systems. Simulations are carried out to validate the viability of swarm intelligence algorithms as compared to conventional detection algorithms for symbol detection in uplink large MIMO systems. Simulation results reveal that swarm intelligence algorithms, notably CCACO and BSSO are capable to outperform several existing swarm based as well as conventional detection algorithms for symbol detection in uplink large MIMO systems in terms of BER performance under both perfect and imperfect CSI errors at the

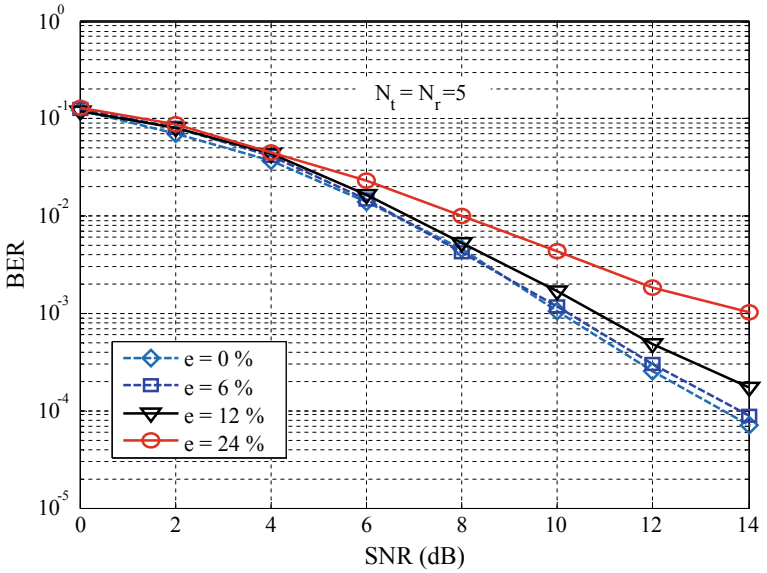


Fig. 10 BER performance of CCACO under different CSI estimation errors at the receiver for $N_r = N_t = 5$ and 4 QAM modulation

receiver. This proves the robustness of swarm intelligence algorithms than conventional algorithms for 5G and beyond wireless communication systems. Hence, swarm intelligence algorithms are promising candidates to meet high-speed data requirement in 5G and beyond wireless systems.

Acknowledgements This chapter is an outcome of Research and Development work undertaken project under Ministry of Electronics and Information Technology, being implemented as Digital India Corporation. The authors would also like to thank Indian Institute of Technology Indore for all the support.

References

1. Ahn, J., Lee, H.-N., & Kim, K. (2009). Schnorr-Euchner sphere decoder with statistical pruning for MIMO systems. In *6th International Symposium on Wireless Communication Systems, 2009. ISWCS 2009* (pp. 619–623). IEEE.
2. Barbero, L. G., & Thompson, J. S. (2007). Performance of the complex sphere decoder in spatially correlated MIMO channels. *IET Communications, 1*(1), 122–130.
3. Bazzi, S., Stefanatos, S., Le Magoarou, L., Hajri, S. E., Assaad, M., Paquelet, S., et al. (2019). Exploiting the massive MIMO channel structural properties for minimization of channel estimation error and training overhead. *IEEE Access, 7,* 32434–32452.
4. Bhatia, V., & Mulgrew, B. (2007). Non-parametric likelihood based channel estimator for Gaussian mixture noise. *Signal Processing, 87*(11), 2569–2586.

5. Bjornson, E., Larsson, E. G., & Marzetta, T. L. (2016). Massive MIMO: Ten myths and one critical question. *IEEE Communications Magazine, 54*(2), 114–123. https://doi.org/10.1109/MCOM.2016.7402270.
6. Buchholz, P. (1994). *On a Markovian process algebra*. Dekanat Informatik, Univ.
7. Chan, A. M., & Lee, I. (2002). A new reduced-complexity sphere decoder for multiple antenna systems. In *IEEE International Conference on Communications, 2002. ICC 2002* (Vol. 1, pp. 460–464). IEEE.
8. Chockalingam, A., & Rajan, B. S. (2014). *Large MIMO systems*. Cambridge University Press.
9. Cormen, T. H. (2009). *Introduction to algorithms*. MIT Press.
10. Datta, A., & Bhatia, V. (2017a). A near-ML performance hybrid dijkstra and firefly algorithm for large MIMO detection. In *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1–6). IEEE.
11. Datta, A., & Bhatia, V. (2017b). A robust MIMO detection algorithm using gravitationally coordinated swarm. In *2017 Conference on Information and Communication Technology (CICT)* (pp. 1–6). IEEE.
12. Datta, A., & Bhatia, V. (2019). A near maximum likelihood performance modified firefly algorithm for large MIMO detection. *Swarm and Evolutionary Computation, 44,* 828–839.
13. Datta, T., Srinidhi, N., Chockalingam, A., & Rajan, B. S. (2010). Random-restart reactive tabu search algorithm for detection in large-MIMO systems. *IEEE Communications Letters, 14*(12), 1107–1109.
14. Dijkstra, E. W. (1959). A note on two problems in connexion with graphs. *Numerische Mathematik, 1*(1), 269–271.
15. Dorigo, M., & Stützle, T. (2003). The ant colony optimization metaheuristic: Algorithms, applications, and advances. In *Handbook of metaheuristics* (pp. 250–285). Springer.
16. Eberhart, R. C., & Kennedy, J. (1995). Particle swarm optimization. In *Proceeding of IEEE International Conference on Neural Network*, Perth, Australia (pp. 1942–1948).
17. Eberhart, R., & Kennedy, J. (1995). A new optimizer using particle swarm theory. In *Proceedings of the Sixth International Symposium on Micro Machine and Human Science, 1995. MHS'95,* (pp. 39–43). IEEE.
18. Fister, I., Yang, X.-S., & Brest, J. (2013). A comprehensive review of firefly algorithms. *Swarm and Evolutionary Computation, 13,* 34–46.
19. Glover, F., & Laguna, M. (1998). Tabu search. In *Handbook of combinatorial optimization* (pp. 2093–2229). Springer.
20. Guo, Z., & Nilsson, P. (2006). Algorithm and implementation of the K-best sphere decoding for MIMO detection. *IEEE Journal on Selected Areas in Communications, 24*(3), 491–503.
21. Hassibi, B., & Vikalo, H. (2005). On the sphere-decoding algorithm I. Expected complexity. *IEEE Transactions on Signal Processing, 53*(8), 2806–2818.
22. James, J., & Li, V. O. (2015). A social spider algorithm for global optimization. *Applied Soft Computing, 30,* 614–627.
23. Khan, A. A., Bashir, S., Naeem, M., Shah, S. I., & Li, X. (2008). Symbol detection in spatial multiplexing system using particle swarm optimization meta-heuristics. *International Journal of Communication Systems, 21*(12), 1239–1257.
24. Khan, A., Bashir, S., Naeem, M., Shah, S. I., & Sheikh, A. (2007). Binary ant colony algorithm for symbol detection in a spatial multiplexing system. In *International Conference on Unconventional Computation* (pp. 115–126). Springer.
25. Khansefid, A., & Minn, H. (2015). On channel estimation for massive MIMO with pilot contamination. *IEEE Communications Letters, 19*(9), 1660–1663.
26. Mandloi, M., & Bhatia, V. (2015). Congestion control based ant colony optimization algorithm for large MIMO detection. *Expert Systems with Applications, 42*(7), 3662–3669.
27. Mawatwal, K., Sen, D., & Roy, R. (2017). A semi-blind channel estimation algorithm for massive MIMO systems. *IEEE Wireless Communications Letters, 6*(1), 70–73.
28. Mitchell, M. (1998). *An introduction to genetic algorithms*. MIT Press.
29. Mohammed, S. K., Chockalingam, A., & Rajan, B. S. (2008). A low-complexity near-ML performance achieving algorithm for large MIMO detection. In *IEEE International Symposium on Information Theory—Proceedings* (pp. 2012–2016).

30. Paulraj, A., Nabar, R., & Gore, D. (2003). *Introduction to space-time wireless communications*. Cambridge University Press.
31. Rashedi, E., Nezamabadi-pour, H., & Saryazdi, S. (2009). GSA: A gravitational search algorithm. *Information Sciences, 179*(13), 2232–2248. https://doi.org/10.1016/j.ins.2009.03.004.
32. Seyman, M. N., & Taşpinar, N. (2013). Symbol detection using the differential evolution algorithm in MIMO-OFDM systems. *Turkish Journal of Electrical Engineering & Computer Sciences, 21*(2), 373–380.
33. Som, P., Datta, T., Chockalingam, A., & Sundar Rajan, B. (2010). Improved large-MIMO detection based on damped belief propagation. In *IEEE Information Theory Workshop 2010, ITW 2010* (pp. 311–315).
34. Van Trees, H. L. (2004). *Detection, estimation, and modulation theory, part I: Detection, estimation, and linear modulation theory*. Wiley.
35. Wedde, H. F., & Farooq, M. (2006). A comprehensive review of nature inspired routing algorithms for fixed telecommunication networks. *Journal of Systems Architecture, 52*(8–9), 461–484.
36. Xu, T., Grammenos, R. C., Marvasti, F., & Darwazeh, I. (2013). An improved fixed sphere decoder employing soft decision for the detection of non-orthogonal signals. *IEEE Communications Letters, 17*(10), 1964–1967.
37. Zeng, J., Lin, J., & Wang, Z. (2018). Low complexity message passing detection algorithm for large-scale MIMO systems. *IEEE Wireless Communications Letters, 7*(5), 708–711.

A Nonlinear Strategy Management Approach in Software-Defined Ad hoc Network

Santosh Kumar Das and Sachin Tripathi

Abstract Software-Defined Networking (SDN) is a growing architecture of the modern era due to the programmable abstraction instead of consuming more hardware. It is frequently used in the ad hoc network due to its speciality of infrastructureless feature. Although, it is adaptable, manageable and cost-effective. However, it has several limitations like limited battery capacity of the nodes, variations of devices, unpredictable and linguistic requirements of the users. These limitations cause different types of uncertainties and imprecisions in the Software-Defined Ad hoc Network (SDANET) at the time of transaction. In response to this, the proposed work is designed for efficient path using some techniques such as nonlinear formulation, fuzzy logic, and game theory. The game theory method is used to establish relationships among dynamic nodes as players in cooperative as well as noncooperative manners. The nonlinear programming is used to estimate uncertainty in the parameters whereas fuzzy logic is used to fulfill the linguistic requirements of the players by making actual goal as imprecise goal. The combination of stated combined technique is known as nonlinear fuzzy game theory which is used to model the recognition of uncertainty and imprecise knowledge efficiently. The simulation and mathematical analysis of the proposed model are done in the LINGO optimization software. The simulation of the proposed work is validated with two existing methods and showed that outcomes of the proposed model are much better than the existing two methods in term of network metrics.

Keywords Software-defined ad hoc network · Nonlinear programming · Fuzzy logic · Game theory · Membership function

S. K. Das (✉) · S. Tripathi
Department of Computer Science and Engineering, Indian Institute of Technology (Indian School of Mines) Dhanbad, Dhanbad 826004, Jharkhand, India
e-mail: sunsantosh2007@rediffmail.com

S. Tripathi
e-mail: var_1285@yahoo.com

S. K. Das et al. (eds.), *Design Frameworks for Wireless Networks*,
Lecture Notes in Networks and Systems 82,
https://doi.org/10.1007/978-981-13-9574-1_14

1 Introduction

In the recent scenario, the applications used by the customers are basically more flexible and full of uncertainty which is covered by several types of networks as follows:

(a) **Wireless sensor network** [1–4]: It consists of several sensor nodes and base stations that help in recording and monitoring different conditions.
(b) **Wireless ad hoc network** [5–8]: It is an infrastructure-less, dynamic-topology-based network.
(c) **Cellular network** [9–12]: It is a method for splitting a large network into smaller groups called "cells". It consists of static and dynamic nodes.

Most of the functions of the abovementioned networks are based on hardware centric. But, in the last few years, growing demand of Software-Defined Data Centers (SDDCs) and adaptation of hardware into software cause the use of Software-Defined Networking (SDN) as emerging part of the above networks. In this paper, a routing protocol is designed for Software-Defined Ad hoc Network (SDANET). Before going to discuss main proposed problem, some of the basic concepts of SDANET are highlighted as given below.

1.1 Emergence Role in Softwarization

Softwarization is the main part of the SDN. It helps to increase the use of emerging software by decreasing the use of hardware. It makes the services and applications of the customers much easier with the help of quintuple virtualization (i.e., SOSAN) shown in Fig. 1 and short description is given as follows:

(a) **Server virtualization**: It is a process to split a single physical server into multiple servers in a virtual environment.
(b) **Operating system virtualization**: It is a method that allows the hardware to run multiple programs for multiple operating systems on a single machine by the help of software.
(c) **Storage virtualization**: It is a process to transmit data from physical storage device to a virtual storage system in the form of cloud storage.
(d) **Application virtualization**: It is Remote Method Invocation (RMI) system which is used to run software from a remote server and redirect it in the form of application in the client machine.
(e) **Network virtualization**: It is a combined method of network operations as well as network parameters with related software and hardware.

The abovementioned virtualization provides today's most precious services in the form of cloud computing [13], transparent computing [14], and fog computing [15].

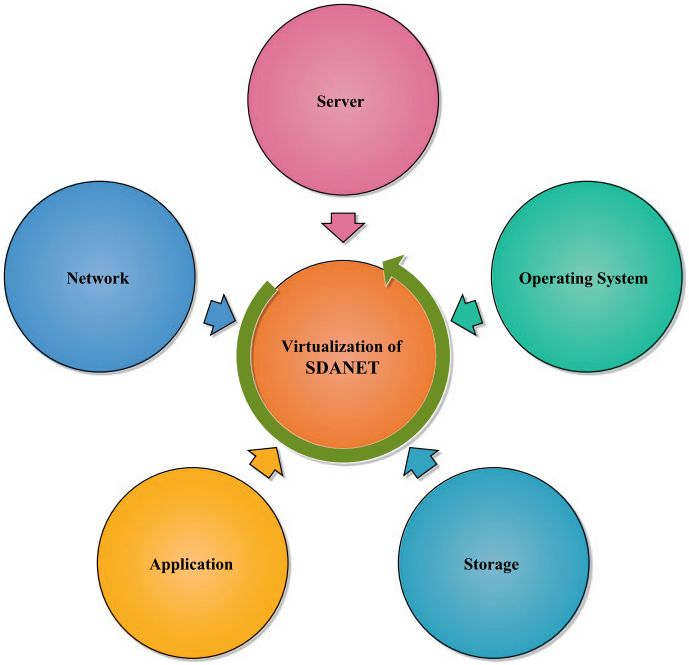


Fig. 1 The virtualization of SDANET

1.2 Frameworks and Architectures

The Open Networking Foundation (ONF) [16] is a group which develops different standardization of SDN. According to ONF, SDN is based on emerging architecture which is adaptable, dynamic, cost-effective, and manageable [17, 18]. It is based on some phases shown in Fig. 2. First layer consists of some programs that help to communicate between controller layer and several application programming interfaces. Control layer is a logical unit of the SDN which is used to receive instruction from top layer and transmit it in different hardware. Infrastructure layer helps to process and forward data and information into the path. Hardware used in the infrastructure layer is known as box and software used in the boxes is known as resident software. Basically, it is designed for flexible requirement of the customers. It provides intelligence by different distributed algorithms for deciding proper route in virtual environment and maintained the whole network efficiently.

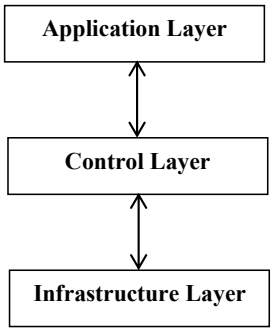


Fig. 2 Layer architecture of SDANET

1.3 Applications of SDANET in Social Networking

Social network is used for establishing personal relationship as well as social interaction among people via website. It helps to communicate one to another by posting messages, comments, and images. In modern era, maximum person spent most of their time in social network. It indicates way of connection that helps in mapping and measuring the relationship within organization, group, and people. SDANET plays a vital role in social networking. It facilitates the advantages of both SDN and ad hoc network. Due to features of infrastructure-less and dynamic topology, user can move freely in the transmission range [19–21]. Each user can send or transmit data independently [22–25]. The architecture of the social network is given in Fig. 3, where Fig. 3a indicates SDN system in social networking where SDN controller is situated between server machine and infrastructure layer. Infrastructure layer contains some boxes with resident software that provide the interaction between server and client machines where modem provides the Internet connection and firewall provides the protection from the viruses. Figure 3b shows a social group where multiple users are connected together to achieve one or multiple goals. Figure 3c shows same scenario for multiple groups. Figure 3d shows people are working on several social networks under an organization.

1.4 Implementation Issues and Prospective Solutions

SDANET has a combination of features of SDN and ad hoc network [26, 27]. It has a network intelligence controller that consists of emerging software programs for global view of the network. Due to adaptable and manageable natures of the SDANET, it has following limitations:

1. The fusion of different intelligent algorithms makes the whole softwarization more complex which is difficult to understand for a new administrator.

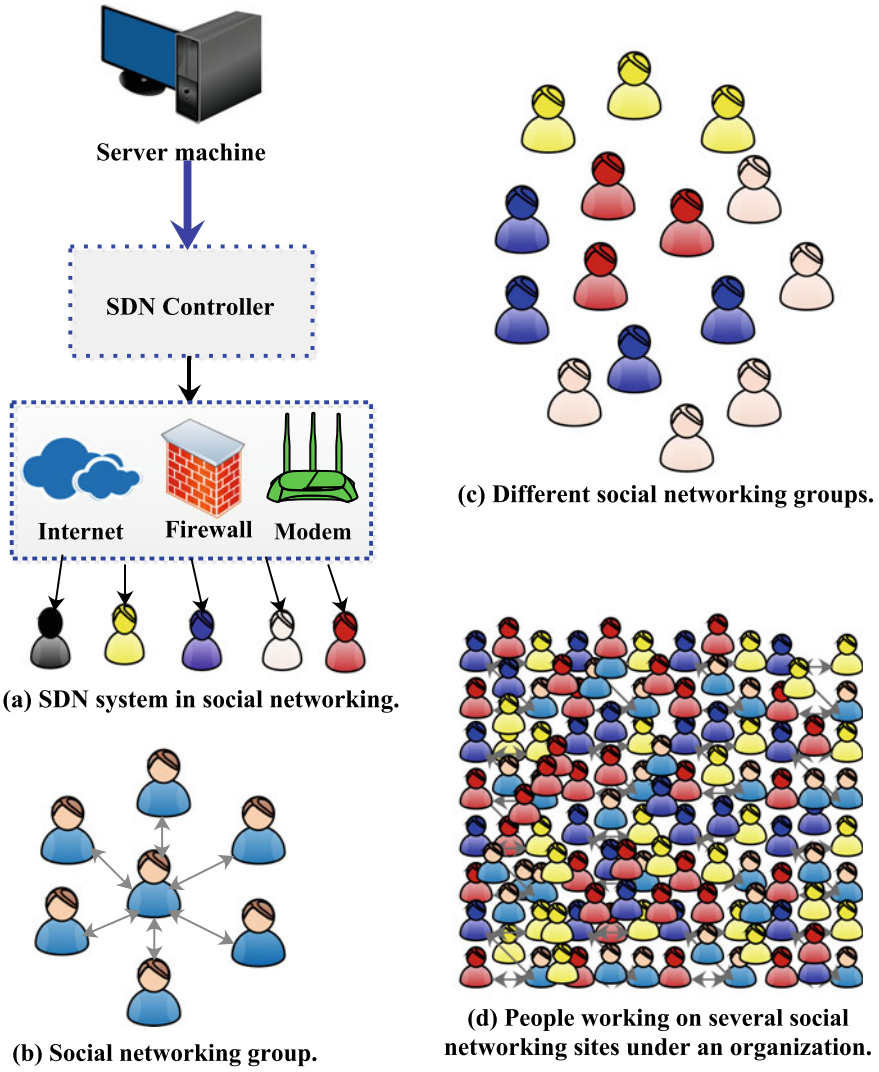


Fig. 3 SDANET in social networking

2. The coordination of different boxes make complicated to change any part of the program in the virtual environment. Because each box is linked with another box to achieve the main purpose of the SDN.
3. The full prospective of the network is not recognized at the time large cloud deployment due to limited capacity battery of the nodes and other inadequate network parameters.

4. Due to several uncertainties and imprecision, network administrator devotes a lot of time to configure and plan the network boxes with proper intelligent resident, but maximum time he/she handles lots of error and unsuccessful trials.
5. The two situations: "What will happen in response to a configuration change?" and "Whether the configuration is correct or not?" always make confusion.

Due to abovementioned limitations, SDANET has several issues such as (i) parental control, (ii) traffic prioritization, (iii) cap management, (iv) application control with simple interface and program, (v) frequently performance monitoring, (vi) custom packet processing through resident software, etc. To reduce the above issues, current paper proposes a routing protocol using game theory, nonlinear programming, and fuzzy logic which is a part of soft computing [28].

1.5 Motivations

The main issue of this network is energy efficiency. There are several routing methods that have been proposed in the last few years. However, most of the reviewed methods manage this problem with either game theory or linear programming. No one has discussed the different strategies of the nodes. To handle this gap, in this paper, a routing protocol is designed with the features of game theory, nonlinear programming, and fuzzy logic in cooperative and noncooperative manners. Finally, it is examined using some methods as stated in the literature and its performance with some metrics.

1.6 Our Contributions

The main contributions of this work are as follows:

(a) Highlighted pros and cons of social networking in context of SDN,
(b) Modeled the several mixed strategies of the nodes in both cooperative and noncooperative manners,
(c) Analyzed the utility of the nodes as players by modeling the proposed game with nonlinear programming and estimates uncertainty in the parameters, and
(d) Studied the feasible and optimal solutions with the effects of uncertainty to transform the actual objectives and constraints into the imprecise objectives and constraints.

1.7 Structure of the Paper

The remaining of the manuscript is structured as follows. Descriptions of existing works are defined in Sect. 2. In Sect. 3, the proposed model is illustrated. Section 4 demonstrates the performance evaluation including performance metrics and simulation setup. Finally, Sect. 5 provides the conclusion of the paper along with future scope.

2 Literature Review

In past some years, numerous routing protocols are proposed [29, 30]. Some of them are defined as Wang et al. [31] designed a novel routing method for the SDN based on multi-hop technique. In this protocol, SDN centralized controller provides the shortest path and disjoint multipath. The network lifetime of this protocol is more longer than existing approaches. Tahaei et al. [32] proposed a traffic measurement technique for SDN. It consists of two schemes such as elastic and fixed. The combination of both schemes enables accurate real-time traffic matrix that helps to maintain traffic of the network. It optimizes multiple objectives like controller communication and computational cost. So, it helps fine-grained monitoring task with high accuracy. Awad et al. [33] designed a routing method for SDN with discrete link rates. This is an integral flow routing technique which used two methods, namely, mixed integer linear programming and benders decomposition technique for improving the performance of the network and deriving the optimal path. Zhang et al. [34] designed a routing system for SDN. The main aim of this routing protocol to overcome two basic limitations such as problem of large number of forwarding rules and limited ternary content addressable memory. The authors designed this protocol in terms of both versions such as static and dynamic and analyze several network metrics and their complexities. Lin et al. [35] designed an energy-efficient method for SDN where network is organized as a mesh. The purpose of this method is to reduce energy consumption, apply security in route discovery and maintenance, and privacy preserving. Hence, it helps to reduce several internal attacks. Finally, it outperforms the existing protocols in term of some network metrics. Manisekaran and Venkatesan [36] analyze a method for SDN in wireless sensor network. It provides a software-based multi-flow in the network. It used two separate channels for control and data plane. These channels help to generate a software module in each node that manages topology of the network and helps to reduce battery power of the nodes. So, it enhances the performance of the network. Lee and Sheu [37] provides a segment routing technique for SDN. Segment routing defines a path of information in the network with an ordered list of multi-protocol label switching. This proposed technique helps to reduce cost of the packet and traffic of the network. This enhancement helps to balance the network operation and increases the bandwidth of the network. It outperforms some existing methods in term of network metrics. Medjkoune and

Sadou [38] designed a routing system named as EMDH using linear formulation. It formulates the issue with the fusion of binary formulation and linear programming based on basic motives: extend the network lifetime and accurate delivery of sensed information. But it has one drawback that it fails to manage conflicting strategies of the nodes. Alishahi et al. [39] designed a method for SDN that consists of nodes and central controller. The purpose of this protocol is to reduce the control interaction and complexity of the network by assigning some weight parameters in traffic class. Kashwan and Ravi [40] designed a system named as EASRP that used few novel techniques for optimizing network metrics and enhancing network performance using circuit switching techniques. Zhu and Gu [41] designed an efficient routing mechanism that concurrently meets two things in the route designed stage like minimum hops and RECI value. At last, it generates a system to manage the initiator and target nodes and enhances the performance. Yazdani and Zarifzadeh [42] designed a system named as NSG to handle residual energy using noncooperating system. The nodes of model try to connect own neighbor based on global and local connectivity system. Sridhar et al. [43] proposed a system named as EN-AODV for managing the process of receiving and sending nodes with the help of AODV mechanism. The basic aim of this protocol is to manage energy level and estimate control packet of the node.

Although the abovementioned literature used several techniques for enhancing network lifetime or sending–receiving data packets efficiently. But none of them manages the different strategies of the network in term of conflicting objectives. The proposed work covered this gap.

3 Proposed Model

This is main section of this proposed work. It divided into some phases, described in given outline.

3.1 Outline

The proposed model is illustrated in several phases given as follows:

(a) **Network model**: It described the information related to the proposed network.
(b) **Parameter structure**: It described the several network parameters that are used to model proposed objectives and constraints.
(c) **Strategy mapping for route selection**: It illustrates several strategies among players in both cooperative and noncooperative manners.
(d) **Nonlinear formulation for route selection**: It analyzes the actual objectives and constraints of the players for evaluating optimal solution.

3.2 Network Model

Let G is the network model given in Eq. 1, where W, L, N, S, U, and F are set of weights, links, nodes, strategies, utilities, and objective functions. The mathematical model of each element is shown in Eqs. 2–7. Weight indicates total number of data packet sent and received by a node n_i. Table 1 summarizes the main notation and symbols used in this paper. The proposed graph G works as cooperative or noncooperative game model based on the situation. The set of nodes works as player of the game. Link between two players works as communication media. The weight of the link defines the level of the SDN resources that handle by control layer. Strategy of the players may be pure or mixed depending on the behavior of the resident software. Utility function is used to assign a number to each player that represents possible outcomes of two strategies. The objective function is used to enhance the network metrics based on specific constraints. In this work, three objective functions are considered as network lifetime, throughput, and overhead which shown in Eqs. 8–10.

$$\mathrm{G(N, L, W, S, U, F).} \tag{1}$$

$$N = \{n_1, n_2, \ldots, n_a, n_{a+1}, \ldots, n_b, n_{b+1}, \ldots, n_{\xi_1}\}. \tag{2}$$

$$L = \{l_1, l_2, \ldots, l_a, l_{a+1}, \ldots, l_b, l_{b+1}, \ldots, l_{\xi_2}\}, \tag{3}$$

$$W = \{w_1, w_2, \ldots, w_a, w_{a+1}, \ldots, w_b, w_{b+1}, \ldots, w_{\xi_3}\}, \tag{4}$$

$$S = \{s_1, s_2, \ldots, s_a, s_{a+1}, \ldots, s_b, s_{b+1}, \ldots, s_{\xi_4}\}, \tag{5}$$

$$U = \{u_1, u_2, \ldots, u_a, u_{a+1}, \ldots, u_b, u_{b+1}, \ldots, u_{\xi_5}\}, \tag{6}$$

$$F = \{f_1, f_2, \ldots, f_a, f_{a+1}, \ldots, f_b, f_{b+1}, \ldots, f_{\xi_6}\}, \tag{7}$$

where $\xi_1, \xi_2, \xi_3, \xi_4, \xi_5$, and ξ_6 are indicated number of nodes, links, weights, strategies, utilities, and objective functions.

$$\begin{aligned} &\text{Objective 1:} \quad \tilde{\text{maximize}} \quad f_1(x) \\ &\text{subject to} \quad g_i(x) \leq b_i, \quad i = 1, \ldots, m \end{aligned} \tag{8}$$

$$\begin{aligned} &\text{Objective 2:} \quad \tilde{\text{maximize}} \quad f_2(x) \\ &\text{subject to} \quad g_i(x) \leq b_i, \quad i = 1, \ldots, m \end{aligned} \tag{9}$$

$$\begin{aligned} &\text{Objective 3:} \quad \tilde{\text{minimize}} \quad f_3(x) \\ &\text{subject to} \quad g_i(x) \leq b_i, \quad i = 1, \ldots, m \end{aligned} \tag{10}$$

Table 1 Notation description

Symbol	Description	Symbol	Description
N	Set of nodes	&&	And logical operator
L	Set of links	γ_3	Strategy 1
W	Set of weights	γ_4	Strategy 2
F	Set of objective functions	E_{rate}	Equilibrium rate
U	Set of utility functions	$Pay_{\Phi_{11}}$	Payoff at point 11
S	Set of strategies	$Pay_{\Phi_{12}}$	Payoff at point 12
n_i	Any node	$Pay_{\Phi_{21}}$	Payoff at point 21
l_i	Any link	$Pay_{\Phi_{22}}$	Payoff at point 22
w_i	Any weight	p	Probability of γ_3 of Player A
s_i	Any strategy	(1−p)	Probability of γ_4 of Player A
u_i	Any utility function	q	Probability of γ_3 of Player B
f_i	Any objective function	(1−q)	Probability of γ_4 of Player B
ξ_1	Number of nodes	V	Value of the game
ξ_2	Number of links	α_j	Probability of selecting strategy of Player A
ξ_3	Number of weights	A_j	Any strategy of Player A
ξ_4	Number of strategies	β_i	Probability of selecting strategy of Player B
ξ_5	Number of utility functions	B_i	Any strategy of Player B
ξ_6	Number of objective functions	C_{ji}	Constant of Player A
B	Bandwidth	C_{ij}	Constant of Player B
D	Delay	x_i	Decision variable of Player A
E	Energy	y_i	Decision variable of Player B
M	Mobility	$\mu z_i(x)$	Membership function of objective
P_1	Parameter set for bandwidth	$\mu g_j(x)$	Membership function of constraint
P_2	Parameter set for delay	λ_i	Aspiration level for lower bound for objective
P_3	Parameter set for energy	γ_i	Aspiration level for upper bound for objective
P_4	Parameter set for mobility	τ_i	Tolerance limit 1 for imprecise objective
n_{i+1}	Succeeding node	φ_i	Tolerance limit 2 for imprecise objective
l_1	Number of links	$\lambda_{j\prime}$	Aspiration level for lower bound for constraint
R_i	Any route	$\gamma_{j\prime}$	Aspiration level for upper bound for constraint
γ_1	Cooperation strategy	$\tau_{j\prime}$	Tolerance limit 1 for imprecise constraint
γ_2	Noncooperation strategy	$\varphi_{j\prime}$	Tolerance limit 2 for imprecise constraint
Ψ	Isolation function	$\sim$	Fuzzy operator

where f_i: $R^n \rightarrow R$: are different conflicting objecting functions; x = (x_1, x_2, …, x_{n-1}, x_n) are the design variables which are known as unknowns of the proposed problem, they must be linearly independent; $g_j : R^n \rightarrow R$: (i = 1, 2, …, m): inequality constraints.

3.3 Parameter Structure

In this phase, different elements of the network are discussed that help to achieve the goal of the proposed model. Eqs. 11–16 represent different network parameters (i.e., P_1 to P_5) which are used to define weight of the links.

$$P_1 = \sum_{i=1}^{l_1} B\ (n_i, n_{i+1})\ \forall\ nodes\ n_i \in R_i, \tag{11}$$

$$P_2 = \sum_{i=1}^{l_1} D\ (n_i, n_{i+1})\ \forall\ nodes\ n_i \in R_i, \tag{12}$$

$$P_3 = \sum_{i=1}^{l_1} E\ (n_i, n_{i+1})\ \forall\ nodes\ n_i \in R_i. \tag{13}$$

E is the residual energy defined as Eq. 14.

$$E_{res} = E_{init} - E_{con}, \tag{14}$$

where E_{init} is initial energy and E_{con} is consumed energy of a node n_i at time t. E_{con} can be evaluated by Eq. 15.

$$E_{con} = E_{n_t} + E_{n_r}, \tag{15}$$

where E_{n_t} indicates energy consumption at the time of transmitting packets and E_{n_r} indicates energy consumption at the time of receiving packets.

$$P_4 = \sum_{i=1}^{l_1} M\ (n_i, n_{i+1})\ \forall\ nodes\ n_i \in R_i, \tag{16}$$

where n_i to n_{i+1} are preceding and succeeding nodes in any route R_i where B, D, E, and M indicate several parameters such as bandwidth, delay, energy, and mobility, respectively. The notation l_1 is the number of links available in route R_i.

Depending on the energy, player is divided into two parts, high-level energy enable nodes, i.e., Player A and low-level energy enabled nodes, i.e., Player B given in Eq. 17.

$$N = \{\text{Player A, Player B}\}. \tag{17}$$

3.4 Strategy Mapping for Route Selection

The applications of SDANET is not finite, it increases day by day. So, nature of payoff matrix may be crisp or fuzzy depending on the situation. The game between two players may be cooperative or noncooperative. The cooperative game is a coalition game which consists of limited players. They can easily agree for mutual understanding. But in noncooperative game player does not have mutual understanding. They select their strategy based on decision-making process. Fuzzy cooperative game indicates partial coalition between players. Here, the range of participation level is lies between 0 and 1. Tables 2, 3, 4, and 5 represent crisp and fuzzy payoff matrix for situation 1 and situation 2 where situation 1 represents when nodes are playing cooperative game and situation 2 represents when nodes are playing noncooperative game. The notations γ_1 and γ_2 indicate two strategies such as cooperation and noncooperation.

From the above payoff matrices, there are four possible states are evaluated as follows:

State 1: If Player A cooperates, then Player B also cooperates.
State 2: If Player A does not cooperate, then better for Player B to cooperate.
State 3: If Player B does not cooperate, then better for Player A to cooperate.
State 4: If Player B cooperates, then Player A also cooperates.

In situation 1, according to the utility function, the optimal solution of the problem when both the players agree to cooperate. Eq. 18 shows isolation function (Ψ) which is used to set cooperation between situation 1 and situation 2 for both players.

Table 2 Crisp payoff matrix for situation 1

Player A	Player B	
	γ_1	γ_2
γ_1	(10, 10)	(15, 4)
γ_2	(4, 15)	(7, 7)

Table 3 Fuzzy payoff matrix for situation 1

Player A	Player B	
	γ_1	γ_2
γ_1	(0.9, 0.9)	(0.7, 0.2)
γ_2	(0.2, 0.7)	(0.1, 0.1)

Table 4 Crisp payoff matrix for situation 2

Player A	Player B	
	γ_1	γ_2
γ_1	(4, 4)	(2, 7)
γ_2	(7, 2)	(9, 9)

Table 5 Fuzzy payoff matrix for situation 2

Player A	Player B	
	γ_1	γ_2
γ_1	(0.4, 0.4)	(0.2, 0.7)
γ_2	(0.7, 0.2)	(0.8, 0.8)

Table 6 Payoff matrix with mixed strategy for condition 1

Player A	Player B	
	γ_1	γ_2
γ_1	(11, 11)	(5, 8)
γ_2	(8, 5)	(3, 3)

Table 7 Payoff matrix with mixed strategy for condition 2

Player A	Player B	
	γ_1	γ_2
γ_1	(11, 2)	(3, 10)
γ_2	(5, 9)	(8, 7)

$$\Psi_{ij} = \begin{cases} 1, \ if \ (\gamma_i \ \&\& \ \gamma_j) \geq \frac{1}{2} \\ 0, \ \text{otherwise} \end{cases} \tag{18}$$

where Ψ_{ij} is the isolation function at γ_i for Player A and γ_j for Player B, && is the logical and operator.

According to Eq. 18, in situation 2, both players have optimal outcomes at the state when both players wish not to cooperate. The topology of the SDANET is dynamic, so decision-maker used mixed strategy instead of pure strategy. Therefore, courses of action are to be selected by the players for a particular occasion with some fixed probability. Let one example for two conditions shown in Tables 6 and 7 for payoff matrix with mixed strategy where γ_3 and γ_4 are two different strategies.

To deal both conditions, let Player A and Player B select strategy at equilibrium manner at rate 50%, then the expected utility of Player A for selecting strategies γ_3 and γ_4 are given in Eqs. 19 and 20.

$$u_1 = E_{rate}(Pay_{\Phi_{11}} + Pay_{\Phi_{12}})_{Player_A}, \tag{19}$$

$$u_2 = E_{rate}(Pay_{\Phi_{21}} + Pay_{\Phi_{22}})_{Player_A}, \tag{20}$$

where E_{rate} is the equilibrium rate, $Pay_{\Phi_{11}}$, $Pay_{\Phi_{12}}$, $Pay_{\Phi_{21}}$, and $Pay_{\Phi_{22}}$ are payoff of Player A at Nash equilibrium points 11, 12, 21, and 22.

Here, $u_1 > u_2$, so, Player A chooses the strategy γ_3. Now, the expected utility of Player B for selecting strategies γ_3 and γ_4 are given in Eqs. 21 and 22.

$$u_3 = E_{rate}(Pay_{\Phi_{11}} + Pay_{\Phi_{21}})_{Player_B}, \tag{21}$$

$$u_4 = E_{rate}(Pay_{\Phi_{12}} + Pay_{\Phi_{22}})_{Player_B}, \tag{22}$$

where E_{rate} is the equilibrium rate, $Pay_{\Phi_{11}}$, $Pay_{\Phi_{21}}$, $Pay_{\Phi_{12}}$, and $Pay_{\Phi_{22}}$ are payoff of Player B at Nash equilibrium points 11, 21, 12, and 22.

Here, $u_3 > u_4$, so Player B also chooses the strategy γ_3.

Therefore, it is concluded that in the above game the best decision is for both players to select strategy γ_3. In real life, in most of the situations, equilibrium rate is not fixed due to high rate of uncertainty. Hence, it is necessary to find the probability for each γ_i for both players. Let Player B use the strategies γ_3 and γ_4 with probabilities q and (1−q), and Player A uses the strategies γ_3 and γ_4 with the probabilities p and (1−p). The expected utility of the Player A is given in Eqs. 23 and 24.

$$u_5 = Pay_{\Phi_{11}} \times q + Pay_{\Phi_{12}} \times (1 - q) \tag{23}$$

$$u_6 = Pay_{\Phi_{21}} \times q + Pay_{\Phi_{22}} \times (1 - q) \tag{24}$$

By solving Eqs. 23 and 24, the value of q is 0.4545. Now, the expected utility of the Player B given in Eqs. 25 and 26.

$$u_7 = Pay_{\Phi_{11}} \times p + Pay_{\Phi_{21}} \times (1 - p) \tag{25}$$

$$u_8 = Pay_{\Phi_{12}} \times p + Pay_{\Phi_{22}} \times (1 - p) \tag{26}$$

By solving Eqs. 25 and 26, the value of p is 0.2. So, in a mixed strategy for the above game the probabilities should be ((0.4545, 0.5455), (0.2, 0.8)).

3.5 Nonlinear Formulation for Route Selection

The topology of the network is dynamic, so the proposed payoff matrix does not contain saddle point as well as dominance rule. Hence, here formulation of geometric programming is used with fuzzy game theory method.

Let V, α_j, and β_i are the value of the game and probability of selecting strategies of Player A and Player B, where $\alpha_j = \{A_1, A_2, \ldots, A_\delta\}$ and $\beta_i = \{B_1, B_2, \ldots, B_\delta\}$.

Player A's and Player B's objectives are to maximize the expected gains and minimize the expected losses. The optimizing equation of Player A is shown in Eqs. 27 and 28 and minimizing and inverse formulation of the game is shown in Eqs. 29–31. And same for Player B is shown in Eqs. 32–36.

$$\text{Max} \quad \text{V}. \tag{27}$$

$$\sum_{i=1}^{\delta} C_{ji}\alpha_j \geq V, \tag{28}$$

where j = 1, 2, …, δ; $\alpha_j \geq 0$.

$$\sum_{i=1}^{\delta} C_{ji}\frac{\alpha_j}{V} \geq 1. \tag{29}$$

$$\text{Min} \quad \text{V}^{-1} = \sum_{i=1}^{\delta} x_i, \tag{30}$$

where i = 1, 2, …, δ.

$$\sum_{i=1}^{\delta} C_{ji}x_j \geq 1, \tag{31}$$

where j = 1, 2, …, δ; $x_j \geq 0$.

$$\text{Min} \quad \text{V}. \tag{32}$$

$$\sum_{i=1}^{\delta} C_{ij}\beta_j \leq V, \tag{33}$$

where j = 1, 2, …, δ; $\beta_j \geq 0$.

$$\sum_{i=1}^{\delta} C_{ij}\frac{\beta_j}{V} \leq 1. \tag{34}$$

$$\text{Max} \quad \text{V}^{-1} = \sum_{i=1}^{\delta} y_i, \tag{35}$$

where i = 1, 2, …, δ.

$$\sum_{i=1}^{\delta} C_{ij} y_j \leq 1, \tag{36}$$

where j = 1, 2, …, δ; $y_j \geq 0$.

In real life, rigid goal is not used due to several imprecise information in uncertain environment. The coordination of different boxes and variation of emerging software possess the system administrator to make the actual goal as imprecise goal. To make imprecise objective with constraint an operator is used with the help of membership functions in Eqs. 37 and 38. Equation 37 is the membership function of imprecise objectives and Eq. 38 is the membership function for imprecise constraints. Hence, Eqs. 30 and 31 summarized as nonlinear fuzzy game model in Eqs. 39 and 40 to achieve the purpose of imprecise objectives of Player A's and same Eqs. 35 and 36 converted into Eqs. 41 and 42.

$$\mu z_i(x) = \begin{cases} 0 & : z_i(x) \leq (p_i - \tau_i) = \lambda_i, \\ \frac{(z_i(x) - \lambda_i)}{\tau_i} & : \lambda_i \leq z_i(x) \leq p_i, \\ 1 & : z_i(x) = p_i, \\ \frac{(\gamma_i - z_i(x))}{\varphi_i} & : p_i \leq z_i(x) \leq (p_i + \varphi_i) = \gamma_i, \\ 0 & : p_i + \varphi_i \leq z_i(x), \end{cases} \tag{37}$$

where i = 1 to K is conflicting objectives; λ_i and γ_i are aspiration levels for upper and lower boundaries respectively; and τ_i and φ_i are tolerance limit for imprecise objectives.

$$\mu g_j(x) = \begin{cases} 0 & : g_j(x) \leq (b_j - \tau_{j'}) = \lambda_{j'}, \\ \frac{(g_j(x) - \lambda_{j'})}{\tau_{j'}} & : \lambda_{j'} \leq g_j(x) \leq b_j, \\ 1 & : g_j(x) = b_j, \\ \frac{(\gamma_{j'} - g_j(x))}{\varphi_{j'}} & : b_j \leq g_j(x) \leq (b_j + \varphi_{j'}) = \gamma_{j'}, \\ 0 & : b_j + \varphi_{j'} \leq g_j(x), \end{cases} \tag{38}$$

where j = 1 to m are constraints; $\lambda_{j'}$ and $\gamma_{j'}$ are aspiration levels for upper and lower boundaries, respectively; and $\tau_{j'}$ and $\varphi_{j'}$ are different tolerance limit for imprecise constraints.

$$\text{Min} \quad \underset{\sim}{\overset{\sim}{\text{V}}}^{-1} = \sum_{i=1}^{\delta} \overset{\sim}{x_i}, \tag{39}$$

where i = 1, 2, …, δ.

$$\sum_{i=1}^{\delta} \overset{\sim}{C_{ji}} \overset{\sim}{x_j} \underset{\sim}{\geq} 1, \tag{40}$$

where j = 1, 2, …, δ; $x_j \underset{\sim}{\geq} 0$.

$$\text{Max} \quad \underset{\sim}{\overset{\sim}{\text{V}}}^{-1} = \sum_{i=1}^{\delta} \underset{\sim}{\overset{\sim}{y_i}}, \tag{41}$$

where i = 1, 2, …, δ.

$$\sum_{i=1}^{\delta} \underset{\sim}{\overset{\sim}{C_{ij}}} \underset{\sim}{\overset{\sim}{y_j}} \underset{\sim}{\leq} 1, \tag{42}$$

where j = 1, 2, …, δ; $y_j \underset{\sim}{\geq} 0$.

4 Simulation Environment and Performance Analysis

The performance of the SDANET depends on several types of linear and nonlinear parameters due to adaptation of hardware into software. In this paper, four nonlinear objectives are considered as optimization such as network lifetime, throughput, overhead, and value of the game. The behavior of each objective in conflicting one to another depends on the dissimilar operations of the network. This multi-objective optimization provides lower level functionality of the network. So, the network administrator efficiently manage, change, and control the system operations by reducing operating costs, maintenance of hardware, network overhead, and system downtime. In this paper, the features of the proposed method are compared with some existing methods EMDH [38], EASRP [40], RECI [41], NSG [42], EN-AODV [43]. All of these methods are ad hoc routing protocols. The simulation of the proposed method is compared with two methods such as EMDH [38] and NSG [42]. The reasons for selecting these two methods for simulation are that both methods are based on optimization techniques. The method NSG is based on game theory technique with single-objective optimization and the method EMDH is based on multi-objective optimization technique. But both methods are used linear formulation to formulate the actual goal of the problem. The proposed method is the combination of geometric programming and game theory. The main aims of the proposed method enhance the conflicting network metrics along with network lifetime by estimating nonlinear parameters. The feature comparison of the proposed method with other existing methods is shown in Table 8. It illustrates several linear and nonlinear features of the proposed method and other existing methods. The topology of the proposed method is hybrid. But, topology of other existing methods are dynamic. In the proposed method, the players of the game optimize multiple conflicting objectives of the network. So, optimization level of the proposed method is better than other existing methods. The method EMDH used binary linear programming and the method NSG used game theory approach, so their optimization level is moderate. The fusion of fuzzy logic in the proposed multi-objective model helps the players to produce flexible goals instead of rigid goals. It helps to recognize uncertainty in the network parameters that helps to control software model at the network administrator

Table 8 Comparison of proposed model with other methods

Sl. no.	Characteristics	Proposed model	EMDH [38]	EASRP [40]	RECI [41]	NSG [42]	EN-AODV [43]
(1)	Topology	Hybrid	Dynamic	Dynamic	Dynamic	Dynamic	Dynamic
(2)	Multipath handling	Yes	No	No	No	No	No
(3)	Network lifetime	Much better	Better	Medium	Medium	Medium	Medium
(4)	Optimization used	Yes	Yes	No	No	No	No
(5)	Optimization level	Standard	Moderate	No	No	Moderate	No
(6)	Managing imprecise information	Very good	No	No	No	No	No
(7)	Managing mutual interference	Very good	No	No	No	No	No
(8)	Managing high traffic load	Very good	Good	Less	Less	Moderate	Less
(9)	Managing high mobility	Very good	Good	Less	Less	Moderate	Less
(10)	Managing polynomial information	Yes	Yes	No	No	No	No
(11)	Managing minimax and maximin	Yes	No	No	No	Yes	No
(12)	Managing controllable factors	Yes	No	No	No	No	No
(13)	Support loss aversion	Yes	No	No	No	No	No
(14)	Estimates imprecise parameters	Yes	No	No	No	No	No
(15)	Managing non-controllable factors	Yes	No	No	No	No	No
(16)	Communication feasibility analysis	Efficiently	Moderate	Less	Less	Moderate	Less
(17)	Robustness	Much more	More	Less	Less	Moderate	Less
(18)	Reliability	Much more	More	Less	Less	Moderate	Less

level. The inherent of fuzzy logic with its membership functions in actual objective of the proposed method helps to estimate conflicting information efficiently and selects the optimal solution in uncertain environment of the network.

4.1 Simulation Model

In this work, LINGO optimization software is used and complete flowchart is shown in Fig. 4. To design the proposed model in LINGO optimization software, first proposed problem is identified, then identified the related strategies and payoff matrices. Several conflict strategies help to design objective functions and its related constraints. Finally, it determines the related decision variables, value of the objective functions, and network metrics. The solver window given is in Fig. 5 and summarized simulation setup is given in Table 9. In this work, LINGO optimization software is used as main simulator where MS Excel is used for graph designing purpose. Both are used in Window 8 platform. All graphs are used as 2D. The model of the optimization is nonlinear in random waypoint view at traffic type CBR for TCP. The total iteration is 7 with 13 linear and nonlinear variables with 23 K used memory.

4.2 Performance Metrics

To validate the proposed work some metrics are evaluated such as network lifetime, throughput, and overhead apart from this value of the game in one of the most metrics for game optimization. The combination of all metrics indicates the performance of the proposed work.

4.2.1 Network Lifetime

The network metric network lifetime indicates some duration of time when network is in fully active mode. This active mode depends on some network resources that is also known as network parameters. Figure 6 indicates network lifetime of the proposed work with other methods, where δ_1 to δ_5 indicate several conflicting strategies of the network. The performance of the proposed method is superior due to standard fusion of some techniques. The connectivity of the network is better due to better network parameters during operational time [44–46].

4.2.2 Throughput

Throughput indicates actual received packets by the destination node based on sent packets. Figure 7 shows throughput of three methods in some iterations. From Fig. 7,

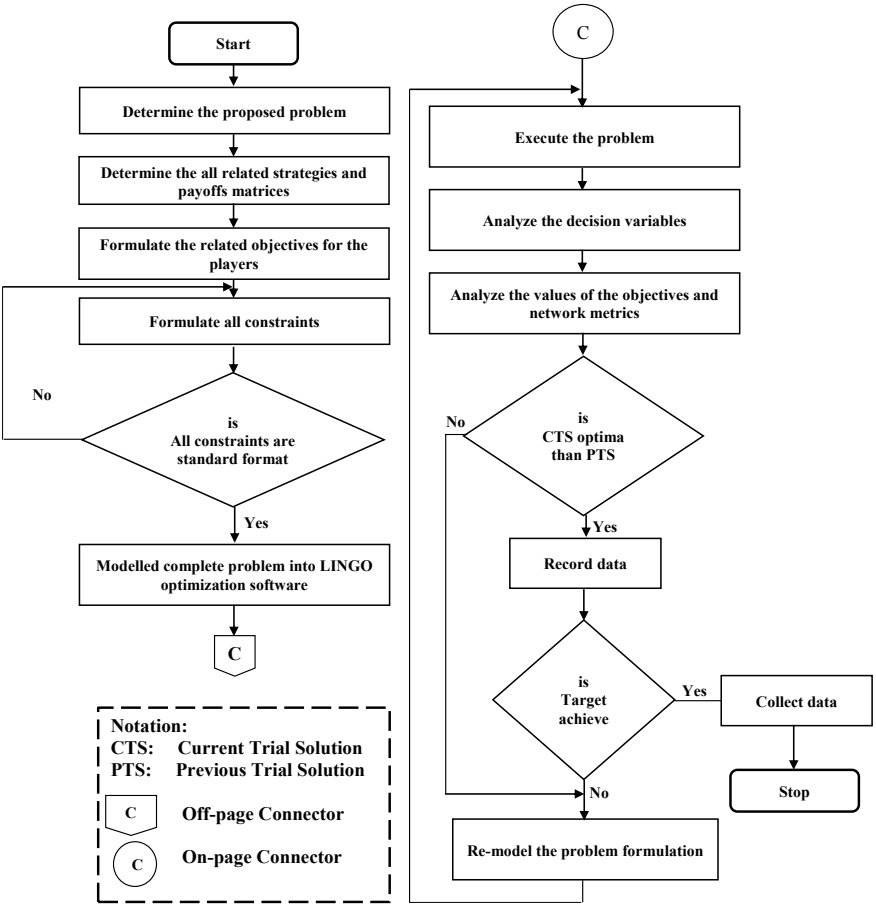


Fig. 4 Flowchart of simulation model

it has been observed that throughput of the proposed model is higher than existing two methods. NSG is based on game theory and it optimizes only energy consumption of the network, whereas EMDH is used linear formulation technique based binary optimization with objective function involvement of nodes and message delivery delay. But both approaches cannot be considered imprecise objective and different conflicting strategies which is most important to estimate nonlinear parameters in uncertain environment. The proposed model is based on nonlinear programming with game theory based on imprecise objective of the players. So, it easily optimizes multiple conflict objectives of the players and solves the game in both cooperative and noncooperative situations. Hence, the proposed model paves the gap of existing two approaches.

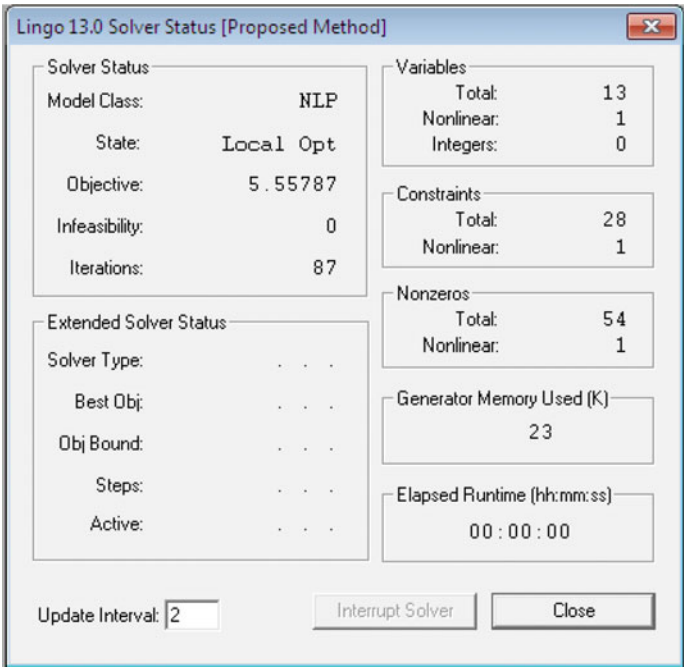


Fig. 5 Solver status window

Table 9 Simulation environment

Parameter	Value
Chart	Column and line
MS Excel version	MS Excel-2013
LINGO simulator version	LINGO-15.0
Platform	Window 8
Dimension	2D
Optimization model class	Nonlinear programming
MAC layer type	IEEE 802.11
Mobility model	Random waypoint model
Traffic type	CBR (TCP)
Total iterations	7
Total variable used	13
Generator memory used	23 K

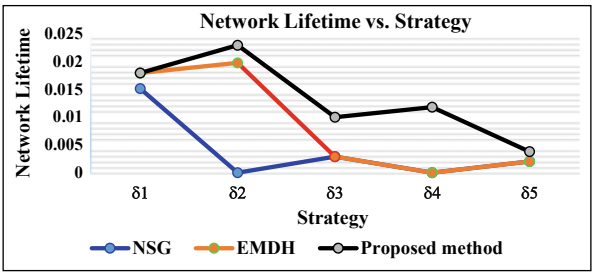


Fig. 6 Network lifetime versus strategies

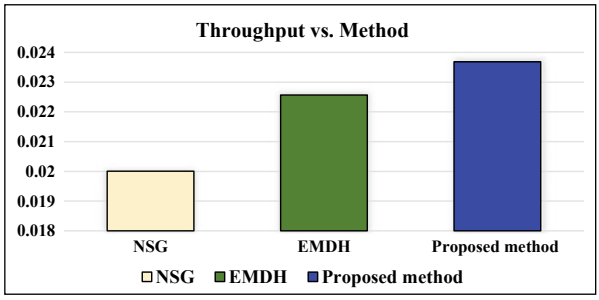


Fig. 7 Throughput versus methods

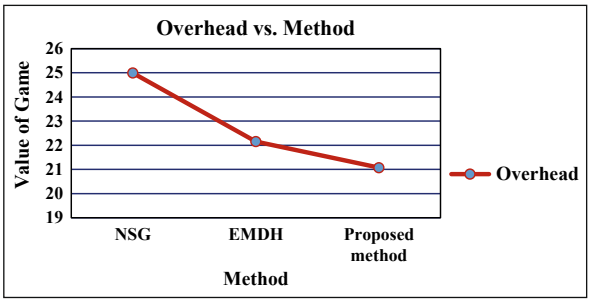


Fig. 8 Overhead versus method

4.2.3 Overhead

Overhead is one of the network metrics that indicates extra memory used, computation time, network resource which is useless for the network lifetime. The proposed technique is the mix-up of nonlinear programming with game theory where the existing methods are based on only linear formulation. Hence, overhead of the proposed method is lesser than other approaches. This scenario is illustrated in Fig. 8.

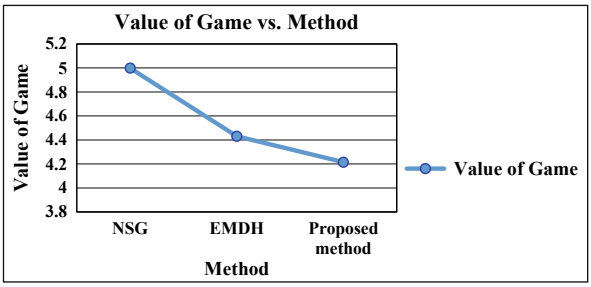


Fig. 9 Value of game versus method

4.2.4 Value of Game

The proposed game model is the fusion of noncooperative and cooperative two person with zero-sum game. Hence, gain and loss of first and second player are equal due to zero-sum operation. The Player A would prefer to maximize its least secure profit and second player would wish to diminish its fatalities. So, final goal of the proposed method is to minimize the value of the game. So, final outcome of the game decreases simultaneously. This scenario is illustrated in Fig. 9. This value of the game quantitatively defined in this figure based on y-axis.

5 Conclusion

In this article, the proposed model which is the combination of several artificial intelligence techniques such as game theory, nonlinear programming, and fuzzy logic is studied. The fusion of stated techniques helps to illustrate several strategies of the nodes and mapped into actual goal of the players. The fuzzy logic technique has been used to make the actual goal as imprecise goal and find the optimal solutions in uncertainty environment of the network. The simulation experiment highlighted that the proposed technique is slightly improved than existing techniques. The future work is same but in nonlinear multi-objective environment.

References

1. Kaswan, A., Nitesh, K., & Jana, P. K. (2017). Energy efficient path selection for mobile sink and data gathering in wireless sensor networks. *AEU-International Journal of Electronics and Communications*, *73*, 110–118.
2. Li, Z., Zhang, J., Shen, X., & Fan, J. (2017). Prediction based indoor fire escaping routing with wireless sensor network. *Peer-to-Peer Networking and Applications*, *10*(3), 697–707.

3. Amgoth, T., & Jana, P. K. (2017). Coverage hole detection and restoration algorithm for wireless sensor networks. *Peer-to-Peer Networking and Applications*, *10*(1), 66–78.
4. Mazumdar, N., & Om, H. (2017). Distributed fuzzy logic based energy-aware and coverage preserving unequal clustering algorithm for wireless sensor networks. *International Journal of Communication Systems*. https://doi.org/10.1002/dac.3283.
5. Das, S. K., Yadav, A. K., & Tripathi, S. (2017). IE2M: Design of intellectual energy efficient multicast routing protocol for ad-hoc network. *Peer-to-Peer Networking and Applications*, *10*(3), 670–687. https://doi.org/10.1007/s12083-016-0532-6.
6. Yadav, A. K., Das, S. K., & Tripathi, S. (2017). EFMMRP: Design of efficient fuzzy based multi-constraint multicast routing protocol for wireless ad-hoc network. *Computer Networks*, *118*, 15–23. https://doi.org/10.1016/j.comnet.2017.03.001.
7. Das, S. K., & Tripathi, S. (2016). Intelligent energy-aware efficient routing for MANET. *Wireless Networks*, 1–21. https://doi.org/10.1007/s11276-016-1388-7.
8. Das, S. K., & Tripathi, S. Energy efficient routing formation technique for hybrid ad hoc network using fusion of artificial intelligence techniques. *International Journal of Communication Systems*. https://doi.org/10.1002/dac.3340.
9. Schlosser, D., & Hoßfeld, T. (2009). Mastering selfishness and heterogeneity in mobile P2P content distribution networks with multiple source download in cellular networks. *Peer-to-Peer Networking and Applications*, *2*(3), 252–266.
10. Feng, G., Li, Y., Zhao, Q., Wang, H., Lv, H., & Lin, J. (2017). Optimizing broadcast duration for layered video streams in cellular networks. *Peer-to-Peer Networking and Applications*, *10*(3), 765–779.
11. Nguyen, H. V., Duong, Q., Nguyen, V.-D., Shin, Y., & Shin, O.-S. (2016). Optimization of resource allocation for underlay device-to-device communications in cellular networks. *Peer-to-Peer Networking and Applications*, *9*(5), 965–977.
12. Chen, J., Wu, Y., Qian, L. P., Peng, H., & Zhou, H. (2017). Energy-efficient content distribution via mobile users cooperations in cellular networks. *Peer-to-Peer Networking and Applications*, *10*(3), 750–764.
13. Meng, S., Wang, Y., Miao, Z., & Sun, K. (2017). Joint optimization of wireless bandwidth and computing resource in cloudlet-based mobile cloud computing environment. *Peer-to-Peer Networking and Applications*, 1–11.
14. Wang, J., Liu, A., Yan, T., & Zeng, Z. (2017). A resource allocation model based on double-sided combinational auctions for transparent computing. *Peer-to-Peer Networking and Applications*, 1–18.
15. Lu, T., Chang, S., & Li, W. (2017). Fog computing enabling geographic routing for urban area vehicular network. *Peer-to-Peer Networking and Applications*, 1–7.
16. https://www.opennetworking.org.
17. Das, S. K., & Tripathi, S. (2018). Adaptive and intelligent energy efficient routing for transparent heterogeneous ad-hoc network by fusion of game theory and linear programming. *Applied Intelligence*, *48*(7), 1825–1845.
18. Das, S. K., & Tripathi, S. (2019). Energy efficient routing formation algorithm for hybrid ad-hoc network: A geometric programming approach. *Peer-to-Peer Networking and Applications*, *12*(1), 102–128.
19. Chowdhuri, S., Chaudhuri, S. S., Banerjee, P., Dey, N., Mandal, A., & Santhil, V. (2016). *Secure minimum loss route selection of MIMO-based MANET in combined (indoor, outdoor, and forest) terrain*. Technical report, working paper, International Journal Advanced Intelligence Paradigms.
20. Fong, S., Li, J., Song, W., Tian, Y., Wong, R. K., & Dey, N. (2018). Predicting unusual energy consumption events from smart home sensor network by data stream mining with misclassified recall. *Journal of Ambient Intelligence and Humanized Computing*, 1–25.
21. Chowdhuri, S., Roy, P., Goswami, S., Azar, A. T., & Dey, N. (2014). Rough set based ad hoc network: A review. *International Journal of Service Science, Management, Engineering, and Technology (IJSSMET)*, *5*(4), 66–76.

22. Chowdhuri, S., Chakraborty, S., Dey, N., Azar, A. T., Salem, M. A.-M. M., Chaudhury, S. S., & Banerjee, P. (2014). Recent research on multi input multi output (mimo) based mobile ad hoc network: A review. *International Journal of Service Science, Management, Engineering, and Technology (IJSSMET)*, *5*(3), 54–65.
23. Mukherjee, A., Keshary, V., Pandya, K., Dey, N., & Satapathy, S. C. (2018). Flying ad hoc networks: A comprehensive survey. In *Information and decision sciences* (pp. 569–580). Berlin: Springer.
24. Chowdhuri, S., Das, S. K., Roy, P., Chakraborty, S., Maji, M., & Dey, N. (2014). Implementation of a new packet broadcasting algorithm for MIMO equipped mobile ad-hoc network. In *International Conference on Circuits, Communication, Control and Computing* (pp. 372–376). IEEE.
25. Chowdhuri, S., Dey, N., Chakraborty, S., & Baneerjee, P. K. (2015). Analysis of performance of MIMO ad hoc network in terms of information efficiency. In *Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2* (pp. 43–50). Springer.
26. Chowdhuri, S., Chakraborty, S., Dey, N., Chaudhuri, S. S., & Banerjee, P. (2017). Propagation analysis of MIMO ad hoc network in hybrid propagation model and implement less propagation loss algorithm to find the minimum loss route. *International Journal of Information and Communication Technology*, *10*(1), 66–80.
27. Mukherjee, A., Dey, N., Kausar, N., Ashour, A. S., Taiar, R., & Hassanien, A. E. (2019). A disaster management specific mobility model for flying ad-hoc network. In *Emergency and disaster management: Concepts, methodologies, tools, and applications* (pp. 279–311). IGI Global.
28. Binh, H. T. T., & Dey, N. (2018). *Soft computing in wireless sensor networks*. Boca Raton: CRC Press.
29. Tuysuz, M. F., Ankarali, Z. K., & Gözüpek, D. (2017). A survey on energy efficiency in software defined networks. *Computer Networks*, *113*, 188–204.
30. Chahal, M., Harit, S., Mishra, K. K., Sangaiah, A. K., & Zheng, Z. (2017). A survey on software-defined networking in vehicular ad hoc networks: Challenges, applications and use cases. *Sustainable Cities and Society*. https://doi.org/10.1016/j.scs.2017.07.007.
31. Wang, J., Miao, Y., Zhou, P., Hossain, M. S., & Rahman, S. M. M. (2017). A software defined network routing in wireless multihop network. *Journal of Network and Computer Applications*, *85*, 76–83.
32. Tahaei, H., Salleh, R., Khan, S., Izard, R., Choo, K.-K. R., & Anuar, N. B. (2017). A multi-objective software defined network traffic measurement. *Measurement*, *95*, 317–327.
33. Awad, M. K., Rafique, Y., & M'Hallah, R. A. Energy-aware routing for software-defined networks with discrete link rates: A benders decomposition-based heuristic approach. *Sustainable Computing: Informatics and Systems*, *13*, 31–41.
34. Zhang, S. Q., Zhang, Q., Tizghadam, A., Park, B., Bannazadeh, H., Boutaba, R., & Leon-Garcia, A. (2017). TCAM space-efficient routing in a software defined network. *Computer Networks*, *125*, 26–40.
35. Lin, H., Jia, H., Li, X., Tian, Y. L., Liu, L., & Blakeway, S. (2016). A trustworthy and energy-aware routing protocol in software-defined wireless mesh networks. *Computers & Electrical Engineering*. https://doi.org/10.1016/j.compeleceng.2016.10.015.
36. Manisekaran, S. V., & Venkatesan. R. (2016). An analysis of software-defined routing approach for wireless sensor networks. *Computers & Electrical Engineering*, *56*, 456–467.
37. Lee, M.-C., & Sheu, J.-P. (2016). An efficient routing algorithm based on segment routing in software-defined networking. *Computer Networks*, *103*, 44–55.
38. Sadou, M., & Louiza, B.-M. (2016). Efficient message delivery in hybrid sensor and vehicular networks based on mathematical linear programming. *Computers & Electrical Engineering*. https://doi.org/10.1016/j.compeleceng.2016.11.032.
39. Alishahi, M., Moghaddam, M. H. Y., & Pourreza, H. R. (2016). Multi-class routing protocol using virtualization and SDN-enabled architecture for smart grid. *Peer-to-Peer Networking and Applications*, 1–17.

40. Ravi, G., & Kashwan, K. R. (2015). A new routing protocol for energy efficient mobile applications for ad hoc networks. *Computers & Electrical Engineering*, *48*, 77–85.
41. Gu, C., & Zhu, Q. (2014). An energy-aware routing protocol for mobile ad hoc networks based on route energy comprehensive index. *Wireless Personal Communications*, *79*(2), 1557–1570.
42. Zarifzadeh, S., & Yazdani, N. (2013). Neighbor selection game in wireless ad hoc networks. *Wireless Personal Communications*, *70*(2), 617–640.
43. Sridhar, S., Baskaran, R., & Chandrasekar, P. (2013). Energy supported AODV (EN-AODV) for QoS routing in MANET. *Procedia-Social and Behavioral Sciences*, *73*, 294–301.
44. Siddiqui, F., & Zeadally, S. (2006). Mobility management across hybrid wireless networks: Trends and challenges. *Computer Communications*, *29*(9), 1363–1385.
45. Amah, T. E., Kamat, M., Moreira, W., Bakar, K. A., Mandala, S., & Batista, M. A. (2016). Towards next-generation routing protocols for pocket switched networks. *Journal of Network and Computer Applications*, *70*, 51–88.
46. Xie, B., Yu, Y., Kumar, A., & Agrawal, D. P. (2008). Load-balanced mesh router migration for wireless mesh networks. *Journal of Parallel and Distributed Computing*, *68*(6), 825–839.

Image Encryption in IoT Devices Using DNA and Hyperchaotic Neural Network

Krishnendu Rarhi and Sukanya Saha

Abstract Encryptions on IoT devices are important because such type of network requires security at its best. In the research conducted by us, we have designed an encryption scheme for images which uses the three techniques, namely, chaos, neural networks, and the DNA encoding scheme. It is a chaos-based pseudorandom sequence generator which uses the neural network for generating the sequence. The chaotic algorithm for encryption is a heterogeneous system as it uses the two types of hyperchaotic maps which are the Lorenz attractor and the Rossler system. In the encryption algorithm, the neural network controls various operations of the encryption scheme. The algorithm further incorporates the use of DNA-based bit permutation and substitution methods for the pixel bits of the image. Every neuron of the neural network uses the equation of chaotic maps as its transfer function. The system performs comparatively better as the two hyperchaotic maps have been used in the process with their nonlinearity property. Security analyses prove the fact with more evidence.

Keywords Chaotic maps · Color image encryption · Hyperchaotic maps · Neural network · DNA encoding

1 Introduction

Internet of Things (IoT) is said to be that important invention which is changing each and every aspect of life. There are certain industries and technologies ranging from consumer to commercial owners of devices and the operators of certain

K. Rarhi (✉)
National Institute of Science and Technology, Biju Patnaik University of Technology, Brahmapur, India
e-mail: krarhi@nist.edu

S. Saha
Institute of Engineering and Management, Maulana Abul Kalam Azad University of Technology, Kolkata, India
e-mail: sukanyash441@gmail.com

S. K. Das et al. (eds.), *Design Frameworks for Wireless Networks*,
Lecture Notes in Networks and Systems 82,
https://doi.org/10.1007/978-981-13-9574-1_15

infrastructures who are discovering the need for protection against various security threats and a rid from the nightmares. There is a drive to create every device a bit smarter and this in turn creates an opportunity for the bunch of cyber criminals and the researchers in security field. As a result of these growth patterns that are seen in the era of rapidly growing features of technology, impacts could be seen falling on the corporations, economy, transactions in businesses, privacy, and safety of the individuals. Major vulnerabilities exist in the traditional cybersecurity. Security breaches are quite evident and prominent in some of the major information management systems of the world as well as certain insurance providers. Such security breaches have proven to be fatal for certain companies and have resulted in the tarnished image of their CEOs. These also caused high damages to the individuals who were concerned and connected. It can be stated with evidence supporting the fact that the cybersecurity needs much concrete structure and improvement.

Considering the world of Internet of Things (IoT), there are many devices like smart refrigerators which are embedded with Linux-based OS, smart automobiles, robotics systems, etc. Anything which is new and connected over the networks is the element of IoT. However, it can be surely stated that many of such industries in the past years were not much concerned about security. The tendency of these industries of being much anxious about security has emerged and gained strength as there has been a notion of increased competition in the market of newer products and their advanced features.

The motivation behind this work has been the better utilization of the three spheres of knowledge, namely, neural networks, chaos theory, and DNA encoding in order to develop a better encryption scheme. The work that has been performed is using three aspects and has been capable of securing an image with better randomness property than the existing systems.

The whole chapter has been organized into six sections. The first section discusses the chapter basics, and the second section elaborates the relevant literature that has been referred by us in order to perform a better experiment. Coming to the third section, it is where we have proposed our actual work; fourth section describes the analysis of the results; fifth section presents the application of the encryption scheme; and the last but not least, sixth section concludes the chapter.

1.1 Internet of Multimedia Things

Internet of Things can be described as a straggled bunch of technology and a subject or topic which does not have a single definition with clarity. These devices are connected well to the network that is in the job of providing valuable information which they collect from the outer surroundings via sensors, or at times, it allows the other systems to connect with and act on through some actuators. Each of these Internet of Things (IoT) is endowed with the ability of converting these valuable information taken from the real world into digital form which could give a hiked

visibility into matters of how one user interacts with the products, applications, and services which the other provides.

Apart from the general discussion on IoT, in order to be more specific, there are palpable types of information and files transferred by each of these devices which are center of interest. Certain smart devices not only transfer data but also pass on multimedia elements like image files. We may consider the quadcopter being an IoT device which has the capability of storing and transferring images over the network. It can be stated in this context that image and video files transmission and exchange have become highly crucial in sundry applications in the era of IoT. A quadcopter which has a secure digital camera can capture images. The stratagem is to capture the image and transmit it to other intended users in a secure mode. Such kind of secure transmission requires certain encryption techniques which are to be applied in order to hide the original image from adversaries during transference through the insecure channel. This is where the role of cryptography comes into play [1]. Several cryptographic algorithms exist in the literature which are devoted to the task of securing these images or other multimedia files.

1.2 Encryption Techniques in Images

There are several encryption schemes and mechanisms which are used to encipher the plaintext or the original source of information which is vulnerable to certain attacks [2]. The Internet and the Vibe of information technology have sprouted in a very swift manner. As a consequence, people have been in the tasks of widely utilizing these interactive media in the zone of communication. As it has been discussed above that the main focus of this chapter is subjected to the cryptography in images, certain techniques which exist in the literature are mandatorily needed to be known to the reader.

Images cover an extensive area within multimedia. Images play vital roles in many fields such as military, diplomatic affairs, and agencies functioning for national security. Taken the seriousness of these fields into consideration, it is important for these images to be protected when transmitted through the unreliable passage. The very primary intention behind keeping any sort of information protected is to maintain the three essential parameters, namely, confidentiality, authenticity, and integrity of the information.

Apart from the above discussion based on the need for cryptography in image files, let us discuss encryption. Encryption is the name given to the procedure of transforming an image into a cryptic form with the use of a key. The user at the other end or at the receiving end is able to retrieve the original image by the application of the decryption process on the encrypted form. Furthermore, it can be stated evidently that there exist the following encryption techniques in the literature of research:

- Encryption using affine transformation and XOR operation.
- Chaotic systems for image encryption.

- Encryption based on one-dimensional random scrambling.
- Encryption based on explosive n*n block displacement followed by inter-pixel displacement of RGB attribute of a pixel.
- The neural network approach for digital data encryption.
- Cryptographic approach for image encryption using RC4 and Blowfish.
- Encryption based on multidimensional chaotic system and pixels location.
- Approach with neural network for authentication, security, and compression of image.

The above methods of encryption [3] are prevailing in the research area as well as in the academia and are preferred by the scientists in order to make certain assumptions about the encryption of image files. A brief discussion on each of the above techniques of encryption will provide valuable insights into the nature and characteristics of each.

Encryption using affine transformation and XOR operation is a kind of encryption technique which uses the operation of affine transformations in order to disperse the pixels by the application of four subkeys of 8 bits. The algorithm intends to break apart an image into 2*2 block size with respect to the pixel values. After doing so, it applies the XOR operation on each of the blocks using the four subkeys in order to remold the pixel values.

Chaotic system for image encryption could be described as that chaotic system which is constituted by the three different one-dimensional chaotic maps. The techniques which we are talking about are using the logistic map which controls the selection of tent map in order to generate sequences that are random. Furthermore, the algorithm uses the substitution–permutation network in order to obtain the desired levels for confusion and diffusion. It has been evident from the literature that this scheme uses keys of larger sizes that has all the settings for the other parameters as well as the initial values of new chaotic system. As a consequence, the scheme provides excellent levels of security from the brute force attack with good key sensitivity and better chaotic behavior.

Encryption based on one-dimensional random scrambling is that technique of encryption which uses the scheme of transforming the two-dimensional image into one-dimensional vector. In addition to that, application of one-dimensional random shuffling is made on this transformed image.

*Encryption based on explosive n*n block displacement followed by inter-pixel displacement of RGB attribute of a pixel* is a research paper from the year back in 2012, which have put focus on the system that uses the technique of decomposition of the original image into n*n block. Furthermore, the mechanism utilizes the algorithm of transformation in order to lessen the correlation among the pixels. The mechanism basically consists of two prime phases. The first phase comprises the technique where the steps perform the block displacement in a horizontal manner later followed by vertical manner displacement. In the second stage, an inter-pixel displacement is done among the values of red, green, and blue. It is must to be stated in this context that every phase or stage has its own key that is used in the procedure.

The neural network approach for digital data encryption is that technique of image encryption that uses the stepwise scanning of an image on a pixel-by-pixel

basis. After the scanning process, a transformation is carried out on the pixels in the form of substitution and permutation. The process of encryption performs the task of adding impurities in the transformed image in order to confuse. The mechanism also uses an artificial neural network in order to decrypt the encrypted form.

Cryptographic approach for image encryption using RC4 and Blowfish is the encryption mechanism which uses the algorithm Blowfish in MATLAB in order to achieve encryption and decryption. The results show that such techniques of image encryption are faster and secure. Moreover, the RC4 stream cipher along with the chaotic maps like the logistic chaos map is utilized in order to perform encryption of a digital color image. The scheme of encryption is split up into three different stages. In the first stage, the key is transformed into initial value, and in the second stage, the initial value is applied to the logistic map in order to give rise to a pseudorandom number. At the last stage, the pseudorandom number is XORed with the byte stream of plain image.

Encryption based on multidimensional chaotic system and pixels location is a technique used for image encryption that is intended to offer a prelude that is dependent on the multidimensional chaotic system. The system has been designed in a way so that it remolds the pixels and alters the value of these pixels. It uses two substitution methods and two scrambling procedures in order to disperse the pixels. The stepwise procedure follows certain phases of action like the first substitution scheme is applied using column index and the first scrambling method uses the Rossler equation. After this, the second phase uses the row index and a shuffling employing the Rossler equations X, Y, Z planes.

Approach with neural network for authentication, security, and compression of image is a proposed methodology which utilizes the artificial neural network in order to attain its tasks. The universal approximation is used in this scheme for compression. Additionally, the system also uses the feedforward neural network for the job of compression. In this, the hidden layer comprises the minimum number of neurons if compared with the input layer and output layer. Furthermore, the system also has the property of detecting the tinkered part of any image.

1.3 Latest Trends in Image Encryption Using DNA and Neural Networks

The significant change that has come to the cryptographic research has been caused due to the emergence of the subject and concept of artificial intelligence [4, 5]. The subject of artificial intelligence refers to the branch of study which leads to the structure and design of intelligent systems. These intelligent systems are those which has the ability to interpret its environment and act accordingly which enhances the chances of success of such systems.

Revolutionary era in the field of artificial intelligence began with the advent of concepts like neural networks. As per the definition provided by the researchers, it

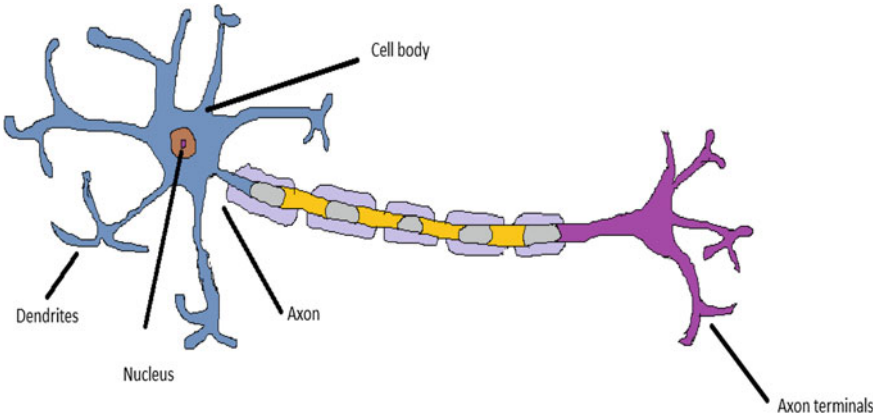


Fig. 1 Biological neuron

has been evident that an artificial neural network is that which could be perceived as an interlinked bunch of nodes, similar to a boundless network of neurons in a human brain. In order to interpret the term neural network, we can refer to the image that is created in our minds which looks something similar to what is presented in Fig. 1.

The picture above is that of the neuron inside the human body. It is the very basic unit of the nervous system. The functionality can be described as the head neuron receiving signals from the brain and based on how intense the signal is, it is passed via various neurons connected to the head neuron and executes the proper job.

Hence, an artificial neural network could be perceived to be as that model which has been designed by taking inspiration from the human brain and the nervous system. In this context, a point must be stated clearly that the neurons in the human brain are way more complicated in structure and operation as compared to the artificial neural networks. However, complex structure and operations can be achieved in artificial neural networks too. Although it can be stated that the neural architecture of the human brain is yet not fully explored, below is the diagram showing an artificial neural network (Fig. 2).

The below diagram is a single-layer neural network. However, neural networks exist which has multiple hidden layers. Furthermore, feedforward and backpropagation neural networks also exist in the literature.

I. DNA cryptography

The term "DNA Cryptography" could be recognized as that latest and new mechanism for securing data in communication systems which is being proved to be of much use. This technique uses the biological sciences as the structure of neuron does. In this case, the biological structure of DNA is utilized and the field of study introduced is known as DNA computing. It has been evident that DNA can be utilized for storage and transmission of data. The notion of DNA cryptography has been spotted as that technology which has the complete power to bring in a brand new feeling of trust for algorithms that are unbreakable [6].

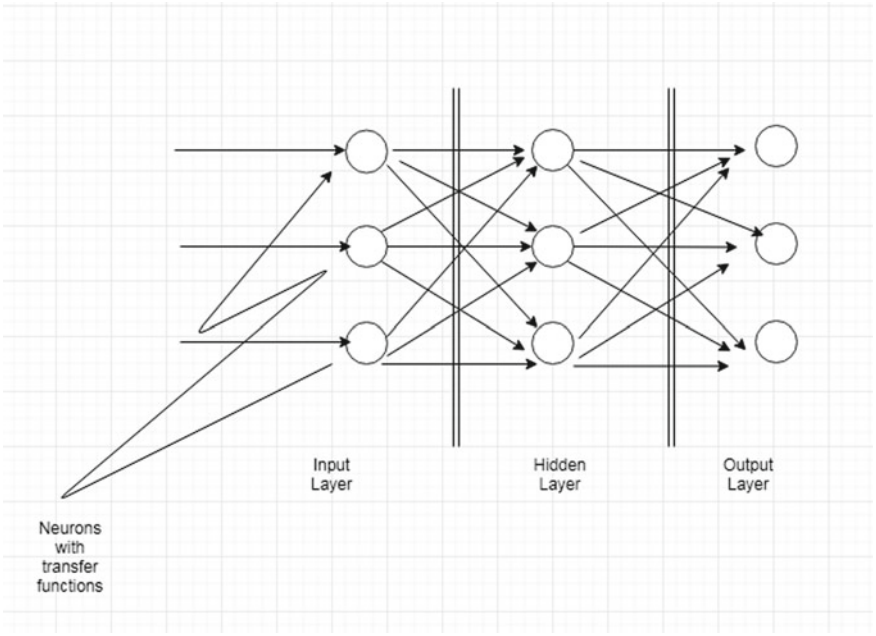


Fig. 2 Artificial neural network

DNA strands are large and lengthy polymers having linked nucleotides in millions. The nucleotides consist of one or more bases, five carbon sugars, and a group of phosphates. These nucleotides which structures the polymers are named according to the nitrogen bases which it comprises. Hence, these are named as Adenine (A), Cytosine (C), Guanine (G), and Thymine (T). Furthermore, one more sentence of knowledge could be added to the context that DNA cryptography is the data hiding which is done in terms of DNA sequences.

II. Fundamentals of image encryption

Image encryption refers to the act of encrypting an image rather than data [7]. We are by now well familiar with the fact that in the real world transmission of secret messages, cryptography is used as a vital tool. Hence, as data being transmitted could be anything starting from audios, text as well as images, there are various methods of encryption that are in existence within the literature [8].

Image encryption follows certain techniques which may be different from the techniques that are generally used to encrypt text or data in other forms. Images are often consisting of more bits than as compared to textual messages. These could consist of dimensions ranging from 10 to 512 pixels. A plain image is enciphered to form an encrypted image which is made to pass through the insecure transmission channel. The following figures show the process.

In Fig. 3, the plain image could be recognized as the variable p which is passed through a function or a function is applied to it in order to get certain operations

Fig. 3 Encryption of images

done. After performing those operations, the resultant that is obtained in the form of image is the c in the below equation:

$$p \oplus key = c \tag{1}$$

$$c \oplus key = p \tag{2}$$

In Eqs. (1) and (2), the term "key" is that which is mixed with the plain image in order to generate the enciphered image. The key is used again at the time of decryption to get back the original image.

Furthermore, it is important to state in this regard that every image consists of a matrix, whose elements are the bytes of 8 bits. However, it is also to be noted that there exist two forms of images; they are grayscale images and the color images. Grayscale image comprises bytes as the elements of the matrix which are known as pixels. Color images comprise three different images or image matrices. They are the red, green, and blue image matrices. The three matrices are just like the grayscale image in the sense that they too, consisting of the bytes as elements of the matrix and those are termed as pixels.

III. **Fundamentals of DNA cryptography**

DNA stands for deoxyribonucleic acids. This kind of cryptography refers to the encryption of the bitstreams in the form of DNA nucleic acids. The bitstream is encoded as per the four acids, ATGC [9]. Hence, the bitstreams are treated as amino acids. There are several rules of performing addition, subtraction, and complement on these DNA strands which follows the general binary arithmetic at the core [10]. The idea is to change the pattern of bitstreams which are encoded as DNA strands into some other pattern. Description has been provided in Fig. 4.

IV. **Chaos and hyperchaotic maps**

The term "chaos" refers to the phenomena which could be illustrated as a situation where the present condition dictates the fate; however, the approximate existing condition does not approximately dictate the fortune. Simply put, when the behavior of a system is dynamic in nature and has high reactivity to the initial conditions,

Fig. 4 Encryption using DNA acids

it is called as a chaotic system. The very familiar butterfly effect emphasizes the whole scenario of chaos by showing a small distraction in one state of the nonlinear deterministic system which could cause a huge difference in a consecutive state later. In words from the butterfly effect, a butterfly if flaps its wings in Brazil could cause a hurricane in Texas.

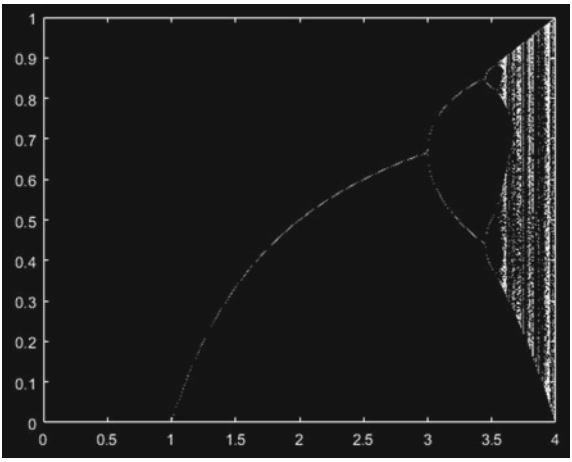
Within cryptography, chaos is utilized as a great source of tool for image encryption [11]. There exist several kinds of chaotic dynamical systems which helps in the generation of sequences that cause to produce complete chaos [5]. These chaotic systems range from one to fourth dimensions. The chaotic systems with three or more dimensions are known as hyperchaotic systems or chaotic attractors. Figures 5 and 6 show the one- and three-dimensional chaotic maps, namely, the chaos map for one-dimensional logistic map and chaos map for three-dimensional Lorenz map.

Description of corresponding equations:

Difference equation of logistic system:

$$x_{n+1} = r x_n (1 - x_n) \tag{3}$$

Fig. 5 Logistic map



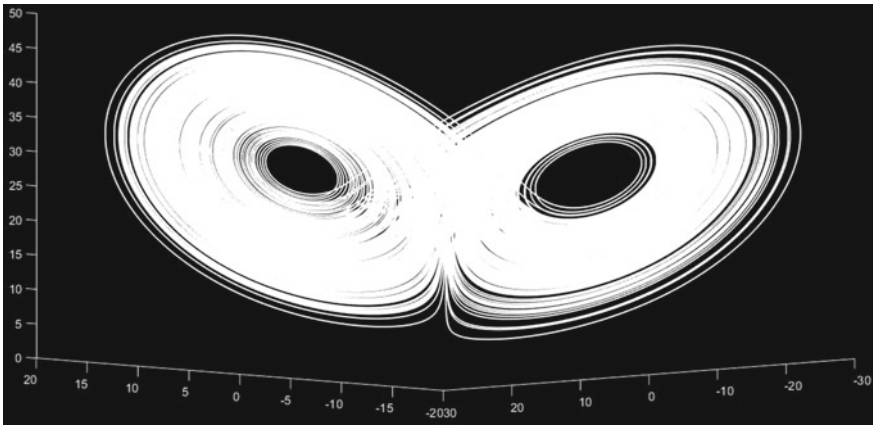


Fig. 6 Lorenz map

Differential equation of Lorenz system:

$$\begin{aligned} dx/dt &= \sigma(y - x) \\ dy/dt &= x(\rho - z) - y \\ dz/dt &= xy - \beta z \end{aligned} \tag{4}$$

2 Relevant Sources of Literature

In order to perform the research in a specific area, a relevant literature review was carried out by us. There are several papers out there in the online libraries and are constantly being disseminated every day through several sources. These are accessed by the researchers to know the latest developments and analytical results through the authenticity of their conducted experimentations. In the below paragraphs, we have presented the literature from relevant academic papers from which we have adopted the various ideas that have been used and applied in our work to produce a better system of encryption.

2.1 Neural Network-Based Chaotic System for Encryption

In [12], the work describes a newer concept of neural network in cryptography. Cryptography used chaos theory since a long time. However, with the advent of artificial intelligence, the subject of neural networks came into the picture. These neural net-

works are used in order to make the encryption of image more complex as they involve a complicated structure. Moreover, chaos theory's chaotic one-dimensional map called the logistic system and piecewise linear chaotic map are those which exhibits a chaotic behavior [13]. The algorithm stated in the paper [12] of encrypting an image involves the usage of neural network. The neural network used four layers. They are the input layer, two hidden layers, and one output layer. There are eight neurons in the first layer, four neurons in the second layer, two in the third layer, and only one in the fourth layer. Each of these neurons uses a transfer function. In the neural network, all the neurons use the same transfer function. Transfer function specifies the chaotic map that has been used in the system and in this case, it is the piecewise linear chaotic map. The cipher algorithm uses a 64-bit key. The output of the input layer has been defined as

$$C = F^{n0}(\Sigma W_0 P + B_0 Q_0) \tag{5}$$

In Eq. (5), n_0 is a random number which is generated by a so-called key generation algorithm. F() is the transfer function of the neurons. The equations which describe the PWLCM have been given below:

$$x(k+1) = F(x(k), q) = \begin{cases} x(k)/q, 0 < x(k) \leq q \\ 1 - x(k)/(1-q), q < x(k) < 1 \end{cases} \tag{6}$$

In Eq. (6), *x(k)* is known as the state of chaotic system and q is the control parameter. The control parameter, in this case, satisfies $0 < x(k) < 1$, $0 < q < 1$. The control parameter of PWLCM specifies the highest Lyapunov exponent which is 0.5. A neural network has weights and biases which are applied along with the inputs to the transfer functions [14–16]. The weight matrix of the input layer is W_0 which is of size 8×8. B_0 is the bias matrix which is of size 8×1. The control parameter matrix is also of size 8×1. The output of the input layer neurons is calculated as first; the elements of the weight matrix are multiplied with the inputs to the function and the obtained value is added with the elements of the bias matrix. Again, the obtained value from this operation is used as the current state x along with the control parameter q in order to iterate the map. The matrices for the consecutive layers of the neural network are given by the following:

$$\begin{aligned} M2 &= F(W_1 M1 + B_1, Q_1) \\ M3 &= F(W_2 M2 + B_2, Q_2) \\ M4 &= F(W_3 M3 + B_3, Q_3) \end{aligned} \tag{7}$$

The matrixes W_1, W_2, and W_3 are of 4×8, 2×4, and 1×2 dimensions, respectively. B_1, B_2, and B_3 are of 4×1, 2×1, and 3×1. Q matrices follow the same dimensions as B. All these matrices and the number of iterations of the transfer functions at each layer have been determined by the key generation algorithm.

Furthermore, the key generation algorithm is said to be using the cubic map. Cubic map is the chaotic map which is given by the following difference equation:

$$y(n+1) = \lambda.y(n).(1 - y(n).y(n)) \tag{8}$$

In Eq. (8), λ is the control parameter which should be set as 2.59. The state of the map is said to be satisfying $0 \leq y(n) \leq 1$.

In the key generation algorithm, the key is given to the system and the chaotic system is iterated 50 times. After 50 iterations, it is once again iterated and the values are taken into consideration. This time the values are used for the matrices to initialize the number of iterations for each layer. Then, a seed 64-bit key is processed through the neural network. This is the another half of the key. Finally, the neural network is operated to obtain the output.

This proposed scheme was found to be secure through 0/1 balancedness test, autocorrelation test, NIST randomness test for the pseudorandom sequence generated by the neural network, and encryption tests. The pseudorandom sequence generator was compared with the LFSR-based generator and the former was proved to be more efficient. Further studies confirm that the properties of the generated pseudorandom sequence are closely linked to that of a perfect sequence of noise. Hence, it is strong for cryptographic applications.

2.2 Heterogenous Chaotic Neural Network and DNA Encoding

In [17], the paper presents a newer neural network combined with chaos-based pseudorandom sequence generator and application of DNA rule-based chaotic algorithm [18, 19] for securing a grayscale image during transmission and storage.

The scheme that has been proposed uses two hidden layer neural networks, which is heterogeneous with respect to the chaotic maps used in every layer. The system uses the logistic map and PWLCM alternatively in each layer. It uses a 64-bit key. This key is made to go through the neural network and the cubic map taken as two halves. The first half 32-bit part is used as the initial condition to the input layer chaotic map function which acts as the transfer function. The other half of 32 bit of the key goes through the cubic map and provides the values for the weight and bias matrices which are used in the neural network. The neural network here uses logistic map in the input layer, PWLCM in the first hidden layer, and so on alternatively. There are four outputs used in this system of neurons. These four outputs are used for the pixel position permutation, pixel bit substitution, pixel bit permutation, and updating the values of the number of iterations of the system. Control parameters for each transfer function are updated after every iteration of the function. The initial condition for the input layer is updated using the XOR of the first three outputs and the number of iterations of the neural network is determined by the fourth output.

The application of DNA encoding lies in the operations of pixel bit substitution and pixel bit permutation [17].

2.3 Color Image Encryption Based on Fractional-Order Hyperchaotic Systems

In paper [20], it has been illustrated that a combination of the outputs generated from three hyperchaotic maps could be utilized to encrypt the three-component matrix of a color image, namely, R, G, and B. The encryption system uses the three maps, namely, Lorenz, Chen, and Lu. The system of equations has been modified to make it four-dimensional in order to increase the randomness and chaotic property of the scheme.

3 Our Proposed Work

The proposed algorithm intends to design an encryption scheme using the techniques which have been used in the literature before as discussed above in the relevant literature readings. The proposed scheme addresses the issues which could arise in the above systems and hence, tries to overcome those and aims to structure a mechanism which is more complicated in terms of if one tries to break the system of encryption. In order to proceed with detailed description of the work we have carried out, it is important to give proper illustration of various mathematical knowledge that have been used. It has been already stated above that there is a huge application of chaotic maps in cryptographic algorithms. In the above two papers, we have seen the usage of one-dimensional chaotic systems. The third paper used three hyperchaotic multidimensional maps or chaotic systems which possessed the chaotic properties for the encryption system. In the work done by us, we have used the hyperchaotic maps as well as the one-dimensional logistic map. Let us illustrate each of these maps one by one by their chaotic functions and chaotic maps.

Logistic Map:
It is the simplest chaotic map that is in usage since a long time in the literature and has the following difference equation:

$$x_{n+1} = p x_n (1 - x_n) \tag{9}$$

Here, p is the control parameter which is in the range of [3.58, 4]. Both x_n and x_{n+1} are the input and output states of the chaotic map. n and $n + 1$ are the iterations of the chaotic system. Figure 7 shows the map given in the simulations from MATLAB.

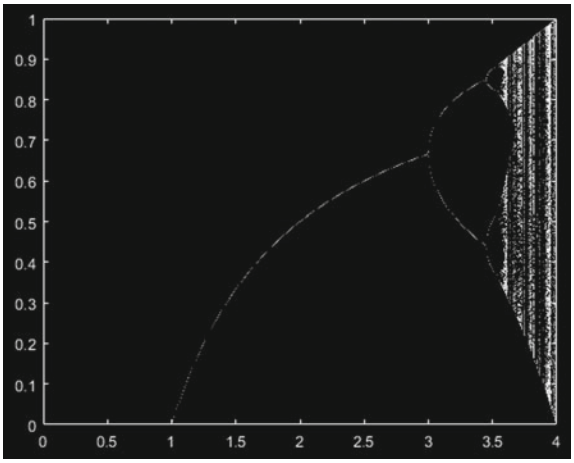


Fig. 7 Logistic map

Lorenz Map:
It is the three-dimensional chaotic map which has the potential to exhibit a higher chaotic behavior. The generated map looks a lot like a butterfly. It is given by the following three differential equations:

$$\begin{aligned} dx/dt &= \sigma(y - x) \\ dy/dt &= x(\rho - z) - y \\ dz/dt &= xy - \beta z \end{aligned} \tag{10}$$

In Eq. (10), *x, y, and z* are the states of the chaotic system and are given as the initial conditions to the system. σ, ρ, *and* β are the three control parameters which have values 28, 10, and 8/3, respectively, when the system is at complete chaos (Fig. 8).

Rossler Map:
The Rossler chaotic system is also a three-dimensional nonlinear differential equations. This is a continuous-time dynamical system which shows the chaotic behavior linked with the fractal properties of the attractor. The associated differential equations are given below:

$$\begin{aligned} dx/dt &= -y - z \\ dy/dt &= x + ay \\ dz/dt &= b + z(x - c) \end{aligned} \tag{11}$$

In the above equations, x, y, and z are the initial conditions which are passed to the chaotic system as inputs and these are the states of the system in every iteration. *a, b, and c* are the control parameters. The system is highly chaotic when the values

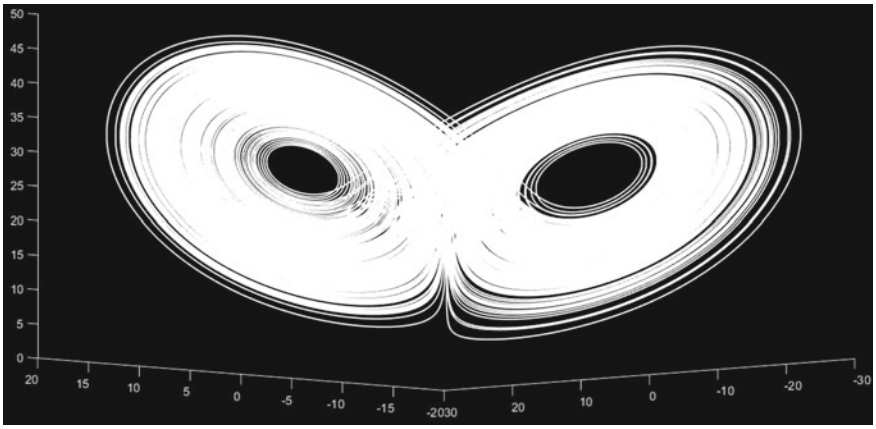


Fig. 8 Lorenz chaotic attractor

of the control parameters are a = 0.2, b = 0.2, and c = 14. Below is the map of the Rossler chaotic attractor (Fig. 9).

Zhou Map:
Zhou's chaotic system is also a three-dimensional chaotic system which is autonomous as per the simulation in both numerical and theoretical ways. The chaotic attractor map of this system, just like the Lorenz system, exhibits the butterfly-like shape. However, topologically, these are different. The system of differential equations is as stated below:

$$\begin{aligned} dx/dt &= a(y - x) \\ dy/dt &= bx - xz \\ dz/dt &= xy + cz \end{aligned} \tag{12}$$

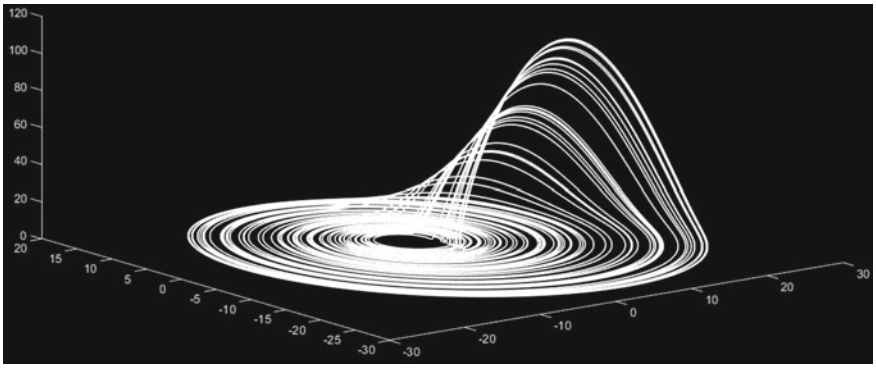


Fig. 9 Rossler chaotic attractor

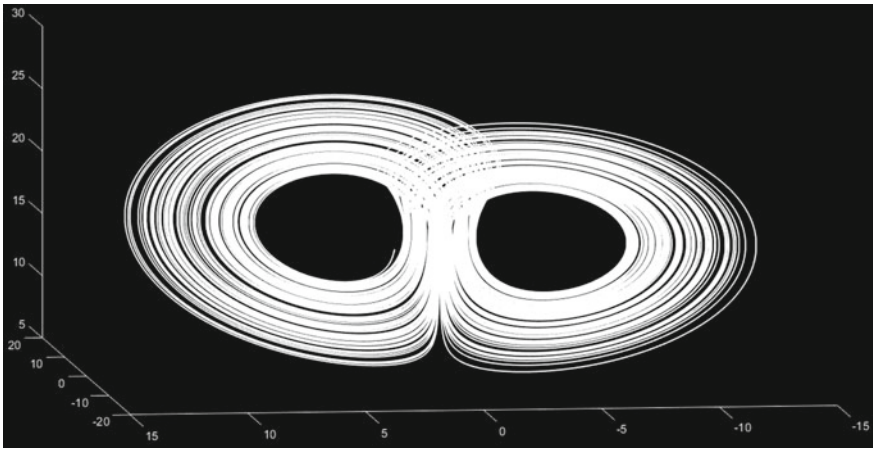


Fig. 10 Zhou chaotic attractor

Similarly, *x, y, and z* decide the subsequent states and the initial conditions. *a, b, and c* are the control parameters which if kept as 10, 16, and −1, respectively, allow the system to be at the utmost chaos. Above is the chaotic map plotted (Fig. 10).

In order to get the maps, we simulated the three sets of nonlinear differential equations in MATLAB using the function ode45, whose underlying method for solving differential equations is the Runge Kutta method [21]. The fourth-order Runge Kutta method can be used in general to iterate the chaotic systems and reach the ultimate chaotic state.

Using the above four maps in the algorithm, we have created a system of enciphering a color image which is made to be transferred through and stored in an IoT device. The algorithm mainly consists of a neural network which is heterogeneous and certain DNA rule-based encoding scheme tables. The heterogeneous neural network has been shown in the diagram below (Fig. 11).

In Fig. 11, a 48-bit key is used to give inputs to the chaotic map in the input layer. As has already been stated above that the neural network consists of the alternate layers of the two chaotic maps, namely, Lorenz and Rossler, we may see the alternate layers using the alternate maps. Moreover, it is important to state at this point that the neural network consists of only one hidden layer. This has been done in order to keep the size of the circuit considerably small so that the system could be used in IoT devices. Due to the fact that IoT devices are subject to certain constraints regarding the fact that they consume less power and time, and has less memory too, there is a requirement of designing circuits that are simple. The working principle of the neural network can be elaborated as follows: the three inputs to each of the neurons are processed by iterating the set of nonlinear differential equations corresponding to each of the chaotic maps. The three inputs are of 16 bits each. Outputs of each chaotic map proceed toward the input of chaotic maps in the next layer as shown in Fig. 11.

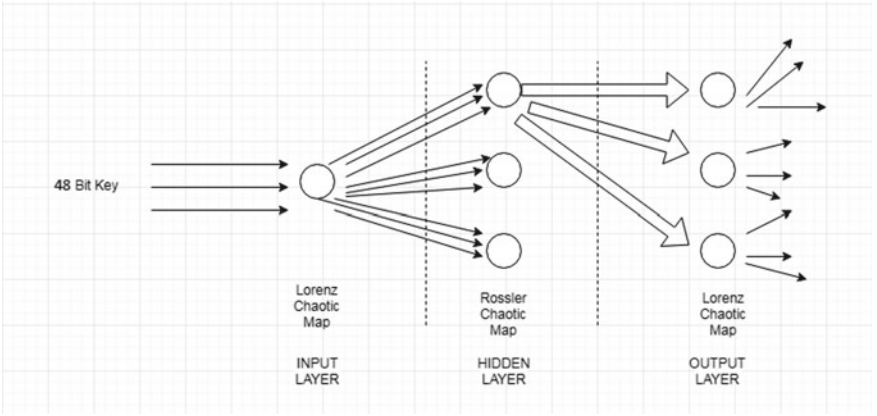


Fig. 11 Heterogeneous hyperchaotic neural network

In addition to the 48 bits of the whole key, another 48 bits of the complete 128-bit key used is processed through a Zhou chaotic map function. The iteration of this system is done after getting the inputs in three 16 bits for x, y, and z, respectively. The map is iterated for thousand iterations in MATLAB simulator, and the values arrived in the last 50 iterations were utilized to fill the elements of the weight and bias matrices. These were done in a random manner considering the round values of the arrived values.

The input layer Lorenz map is first iterated 700 times and the values from the last 300 iterations were passed as inputs to the three Rossler maps in the hidden layer. As in our case, we have taken the 500th iteration of values to the middle most Rossler map, the 600th to the first Rossler map, and the 700th to the last Rossler map. Again, the hidden layer Rossler maps are iterated 700 times and the values are distributed and passed onto the next layer Lorenz systems picking the values from 500th, 600th, and 700th iterations. It is to be noted that the number of iterations was chosen depending on the chaotic behavior possessed by the system being higher in the chosen iterations. It is also to be noted that the control parameters have been kept predefined and are constant, having values at which the respective maps will exhibit the highest chaotic behavior. Inputs to the maps are first multiplied with the weights and are added with the bias values. Thereafter, they are processed by the chaotic functions.

The Lorenz maps at the output layer are each iterated for 5000 times. We have encrypted a 50×50 color image using the random number sequence resulted from the final output layer. There are nine output sequences generated in total from the three chaotic Lorenz maps. These have been illustrated as below:

$$Lorenz1 = \left(x_1^1, y_1^1, z_1^1\right), \left(x_2^1, y_2^1, z_2^1\right), \left(x_3^1, y_3^1, z_3^1\right)$$
$$Lorenz2 = \left(x_1^2, y_1^2, z_1^2\right), \left(x_2^2, y_2^2, z_2^2\right), \left(x_3^2, y_3^2, z_3^2\right)$$
$$Lorenz3 = \left(x_1^3, y_1^3, z_1^3\right), \left(x_2^3, y_2^3, z_2^3\right), \left(x_3^3, y_3^3, z_3^3\right)$$

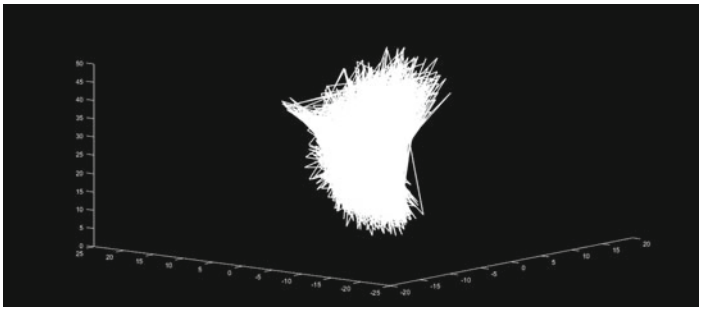


Fig. 12 Chaotic map for $\left(x_1^1, y_1^1, z_1^1\right)$

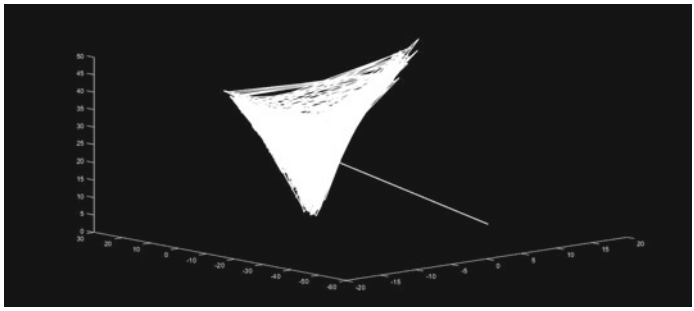


Fig. 13 Chaotic map for $\left(x_1^2, y_1^2, z_1^2\right)$

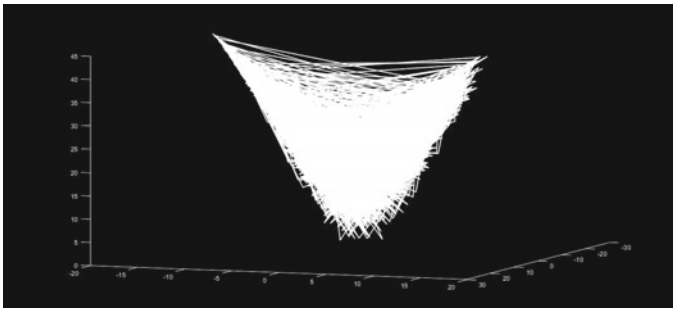


Fig. 14 Chaotic map for $\left(x_1^3, y_1^3, z_1^3\right)$

The chaotic maps have been presented in Figs. 12, 13 and 14 for the sequences $\left(x_1^1, y_1^1, z_1^1\right)$, $\left(x_1^2, y_1^2, z_1^2\right)$ and $\left(x_1^3, y_1^3, z_1^3\right)$.

The steps of encryption have been described below:

- Take the last 2500 values from the whole generated sequences of the final layer maps.
- Take the absolute values of these numbers in the sequences.

- Convert them to unsigned integers.
- Multiply each value by 10.
- Now, perform the following:

$$\begin{aligned} \text{Sum1} &= \left(x_1^1 + y_2^2 + z_3^3\right) \\ \text{Sum2} &= \left(y_1^1 + z_2^2 + x_3^3\right) \\ \text{Sum3} &= \left(z_1^1 + x_2^2 + y_3^3\right) \end{aligned}$$

- Perform the following:

$$\begin{aligned} \text{Sum1} &= \text{Sum1 MOD 256} \\ \text{Sum2} &= \text{Sum2 MOD 256} \\ \text{Sum3} &= \text{Sum3 MOD 256} \end{aligned}$$

Take a plain 50×50 Lena image. Convert it into three different images, namely, P_R, P_G, and P_B.

- Now, perform the following:

$$\begin{aligned} C_R &= \text{Sum1 XOR } P_R \\ C_G &= \text{Sum2 XOR } P_G \\ C_B &= \text{Sum3 XOR } P_B \end{aligned}$$

The above mentioned steps are half of the algorithm specified. It has a DNA encoding part which will be discussed in the next paragraphs.

DNA encoding schemes are used in this algorithm to introduce substitution and permutation in the cipher image obtained in the steps described above.

Substitution through DNA encoding rules:
In order to meet the necessary requirement of confusion and diffusion, it is important to incorporate the techniques of substitution and permutation. It has been found from the literature that DNA encoding rules are very efficient in making the bitstream confusing for the attacker. Hence, we have tried to implement this in designing substitution and permutation techniques for our encryption scheme. We have used the DNA rules in tables which have been stated in [22].

In Table 1 [22], there are eight DNA encoding rules specified. The encoding schemes are chosen from these rules. After selection of the encoding rule, bits inside the bytes are taken in pairs of two and they are encoded as per the rule. Thereafter,

Table 1 Results

NIST test name	P-values obtained	Result of tests
Frequency	0.5814	Pass
Block frequency	0.5465	Pass
Cumulative sums	0.6214	Pass
Runs	0.9983	Pass
Longest runs	0.9987	Pass
Rank	0.5214	Pass
Serial	0.7256	Pass

other operations like complement, addition, or even subtraction are performed to change the existing bit patterns and introduce some confusion in this way. Below we have illustrated the DNA bit substitution and permutation in the encryption scheme in a stepwise approach:

- The remaining 32 bits of the 128-bit key are utilized taken into two halves. Hence, put the first half into the logistic map and iterate it 50 times.
- Consider the value of last iteration. Multiply it by 100.
- Perform mod() on the product by 8.
- The number obtained in the previous step is used to select the DNA rule.
- Encode the whole image matrix according to the selected rule.
- Now, consider the last row of the image matrix and the very first row. Add the elements of these rows using DNA addition rules for the particular encoding scheme.
- Perform the operation of the previous step for the second and third rows, third and fourth rows, and so on, till second last row.

The above steps are the implementation of bit-level substitution for the encryption scheme designed by us. The addition operation will substitute the bit values inside every pixel of the C_R, C_G, and C_B. In this scheme, the larger image will see more additions as the number of rows will increase.

The below steps tell about the bit permutation operation:

1. Give the other half of the 16-bit key to the logistic map. Iterate the map 50 times and eliminate the values.
2. Again iterate the map to the number of rows in the image matrix and consider these values for the next steps.
3. Multiply each of these by 10 and store the values. These values will be considered later.
4. Multiply each of these values by 100 and now perform the next step.
5. Perform mod () on these values by 6.
6. Correspond these values to the DNA complementary transformation rules table given in [17]. After this, select the corresponding rule for complement operation.
7. Now take each of the values for each of the rows, like first value for the first row, the second value for the second row, and so on. Here, value means rule number selected for complement operation from the table.

8. Apply this complement rule to each row of DNA codes for the number of times calculated in step 3 for each.
9. Finally, after doing the operation for every row, convert the DNA codes into binary form using the same rule selected so far for encoding.

The above steps show permutation operation using DNA complement rules. The table for DNA complement rules has been studied from [17].

Pseudocode of the implementation algorithm has been provided below:

let I be the plain image. The following is the pseudo code for the steps:

I) K1 is the 48 bit key given to the neural network as the initial condition.

II) the weights and bias matrices are W11,W12,W13,W21,W22,W23, B11,B12,B13,B21,B22,B23.

III) output of neural networks are as follows:

Lorenz 1 = (x11 , y11, z11), (x12,y12, z12), (x13, y13, z13)
Lorenz 2 = (x21 , y21, z21), (x22,y22, z22), (x23, y23, z23)
Lorenz 3 = (x31 , y31, z31), (x32,y32, z32), (x33, y33, z33)

1) convert(I) --> PlainimageRED,
--> PlainimageGREEN and
--> PlainimageBLUE.

2) Perform the following using the outputs of the neural network:

Sum1 = (x11 + y22 + z33)
Sum2 = (y11 + z22 + x33)
Sum3 = (z11 + x22 + y33)

3) perform:

Sum1 = Sum1 MOD 256
Sum2 = Sum2 MOD 256
Sum3 = Sum3 MOD 256

4) perform:

CipherimageRED = Sum1 XOR PlainimageRED
CipherimageGREEN = Sum2 XOR PlainimageGREEN
CipherimageBLUE = Sum3 XOR PlainimageBLUE

Here is the DNA encryption part of the algorithm:

let 16 bits of the another 32 bit key be denoted by K2.

1) put K2 into the Logistic map.
logistic_map(K2);

2) iterate i=50 { logistic_map(K2) }

3) val = 50th iteration of (logistic_map(K2)

4) val = val*100

5) val = val MOD 8

6) rule = select the DNA rule using val

7) perform:

rule --->encode(CipherimageRED, CipherimageGREEN, CipherimageBLUE)

8) let the last row of the encoded image matrix be denoted by lrow.
let first row be frow.

9) perform:

select(DNA addition rules for the encoding scheme)
add(lrow_elelments , frow_elements)

10) Perform:

step 9 for second and third, third and fourth and so on till second-last row.

11) let the remaining 16 bit key be K3. Perform steps 1 and 2 with K3.

12) iterate i= (no. of rows in the image matrix)

13) val2 = iterate i{
logistic_map(K3)}

14) store (val3 = val2*10) // for later consideration.

15) perform :
val2 = (val2*100) // for performing next steps.

16) val2 = val2 MOD 6

17) choose transformation rules :
DNA_complementary(val2)

18) apply each rule to each of the rows as below:

rule1 --> row1
rule2 --> row2
.
.

19) refer to the values calculated and stored (step 14). Let these be "num".
for every num,do
i=1 to num, perform :
apply(rule --> row_elements)

20) convert_to_binary(row_elements) // use the same DNA decoding scheme.

4 Analysis of the Test Results

The above algorithm was tested with certain tests which proved that the algorithm performs well as compared to other existing chaotic algorithms. The neural network makes unpredictability of the key more rigid. Moreover, maps like Rossler and Lorenz have introduced hyperchaos into the system and the usage of these in the structure and architecture of a neural network has made the system more complicated. The incorporation of heterogeneity and hyperchaos have caused the generation of the random sequence to become more chaotic in nature. Moreover, the DNA encoding scheme has made the bit substitution and permutation more capable of increasing the cross-correlation between the plain image and the encrypted image. The method of using the actual 128-bit key is an efficient one as it has been utilized in broken form of 16 bits and passed through the chaotic functions in order to get the outputs. Below are the various tests which have been done with respect to the randomness [23], gray value distribution of pixels, and cross-correlation tests.

In order to get into more detailed explanation, about the complexity involved while tracing back from ciphertext to plaintext, for an attacker, aspects like key space and image size have greater significance.

The complexity of the cryptographic system has been improved by incorporating the multiple layers of neural networks holding the chaotic functions as their transfer functions. It can be evidently stated that we have used the initial conditions in a dynamic manner which has been determined by the outputs of the chaotic system in the previous layer. Hence, the dynamic nature makes the outputs of the transfer functions unpredictable. Moreover, the DNA encoding as well as the transformation rules selection has been governed by the outputs of the chaotic map functions depending upon the key initially feeded. The weights and biases introduce a greater amount of randomness, and these are determined in a dynamic manner as well. Gradually, it becomes complex for the attacker to decrypt the cipher as the complexity of the algorithm will increase with the increase in the dimensions of the image that is to be encrypted. This can be stated in more detail, as the number of attempts to get the actual values will consist of a huge set. Even when the size of the image is smaller, the algorithm introduces effective complexity in the system as the key space is larger. Furthermore, the randomness incorporated adds up to the scenario.

NIST randomness tests

We have tested the random sequences [24] which have been generated by the three Lorenz maps of the neural network using the runs test for randomness in MATLAB. Along with runs test, other NIST tests were performed, which are listed in the test suit. Table 1 states the results of our analysis:

The highest p-value was found to be 1. This ranged from $p = 0.6$ to complete 1. Hence, it outperformed many random sequences out there and also, MATLAB's own *rand()* function was found to be lagging behind the randomness of these sequences.

Encryption test and probability density functions

The encryption test was done using the histogram analysis which shows the gray value distributions in the two images, which are the plain image and the cipher image. These have been shown in Figs. 15, 16, 17, and 18.

It can be evidently said that the gray value distribution of the encrypted image in Fig. 18 is more uniformly distributed and hence, it may be considered to be a noise image.

The probability density distribution has been obtained for the three R, G, and B components of the plain color image. Three of them exhibits the uniform distribution of gray values in their respective cipher images. As per the literature, it has been quite evident that the attacker can take good advantage of the probability density function associated with the pixels, resulting in a statistical attack. In this case, when the randomness in the pixel values is introduced, then different probability density

Fig. 15 Plain image P_R

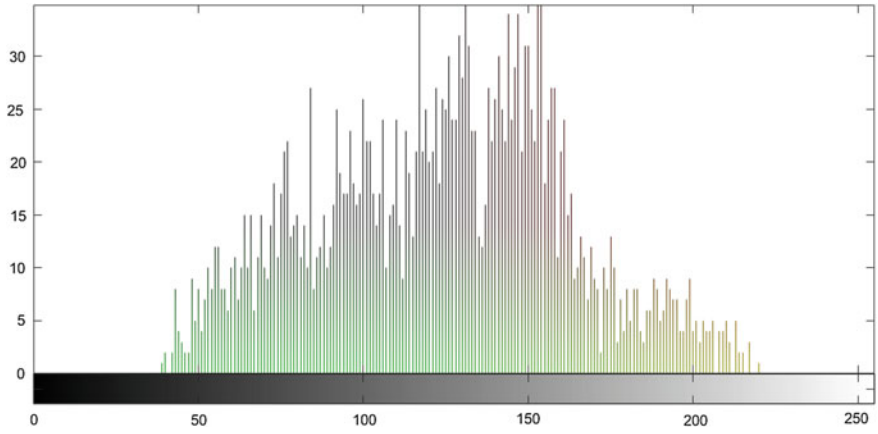


Fig. 16 Histogram of P_R

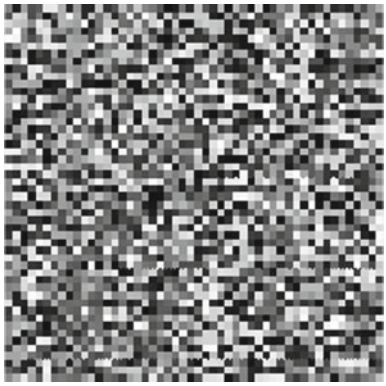


Fig. 17 Cipher image C_R

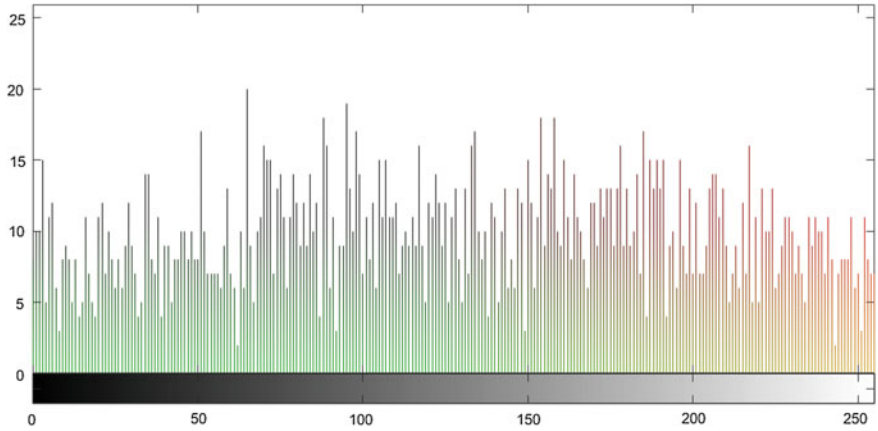


Fig. 18 Histogram of C_R

distributions of distinct plain images result in the similar uniform density of their cipher images.

The encryption test also provides information about the low gray level and higher gray levels of the images. However, it was found that the randomness incorporated within the image pixels after the encryption process has resulted in the scenario, where the higher gray levels have been converted to medium values. Furthermore, lower gray levels have either resulted in a bit higher or a medium gray value.

Cross-correlation testing

The cross-correlation test shows an inclination toward the zero line. The correlation coefficient was found to be 0.0312 within the two images. Hence, a very less amount of correlation exists between the two. See Fig. 19.

Security analyses prove that the algorithm designed by us is capable of encrypting a multimedia image that is to be transferred over an IoT device and through an

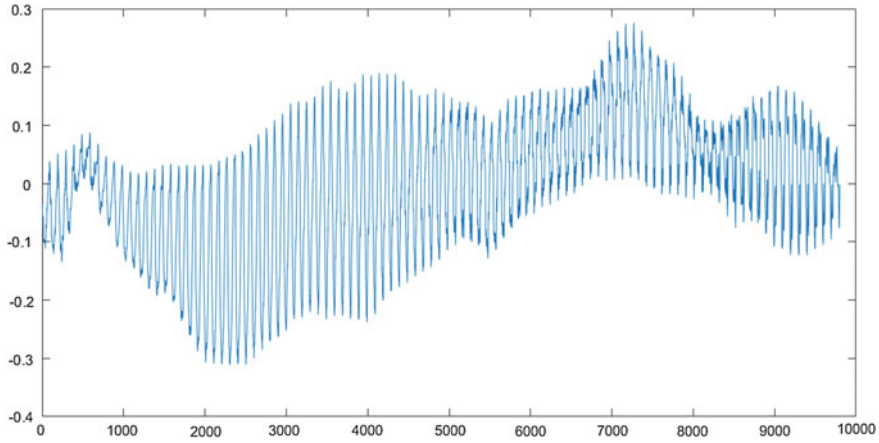


Fig. 19 Cross correlation

insecure wireless sensor network. The algorithm in [17] is the system which uses a neural network structure and performs efficiently. However, the structure selected and implemented by us has proved to be giving better randomness. This is because hyperchaotic maps have been used.

5 Application

As application of IoT devices has been eminent nowadays, multimedia files like images are transferred in nearly most of the smart devices [25]. Be it smartphones, quadcopter, or a Spycam, there are images, which are captured and transferred. The transmission of images through the wireless sensor network in IoT requires these images to be encrypted using such encryption schemes [26, 28]. The significant application of our algorithm and its design has been structured to be utilized in such spheres.

The future scope and next-generation application of such encryption algorithms will help in the secure processing of essential information in the form of images [27]. Also, a lightweight form of such encryption techniques would result in more appealing security requirement.

6 Conclusion

The algorithm that was designed by us is an effort toward making a system of color image encryption that shows better resistibility toward known attacks. It has been evident from the tests of the encryption and other analyses that the encryption scheme

is good to perform in cryptographic applications. The design of the neural network is kept simpler with just one hidden layer so as to keep the circuit structure simplified as the algorithm is made to run on IoT devices. Furthermore, it is designed for color images which are not converted to grayscale. However, the three components R, G, and B matrices have been encrypted. It can be evidently said that any error in the decryption would result in the wrong color image, as the combination would not give the same original image. The better usage of the 128-bit key has proved to be fruitful in the whole encryption process as it had been used in an indirect way in every step of encryption. The architecture of the neural network contributes much to the unpredictability of the key at the outputs, making it hard to break. As a future scope for the experiment conducted by us, it can be said that more security analyses are needed to be done and in order to make the system completely foolproof, there needs to be carried out better cryptanalysis.

References

1. Hossain, M. B., Rahman, M. T., Rahman, A., Islam, S. (2014). A new approach of image encryption using 3D chaotic map to enhance security of multimedia component. In *2014 International Conference on Informatics, Electronics & Vision (ICIEV)* (pp. 1–6). IEEE.
2. Daemen, J., & Rijmen, V. (2013). *The design of Rijndael: AES-the advanced encryption standard*. Berlin: Springer Science & Business Media.
3. Kumar, M., Aggarwal, A., & Garg, A. (2014). A review on various digital image encryption techniques and security criteria. *International Journal of Computer Applications, 96*(13).
4. Burak, D. (2013). Parallelization of encryption algorithm based on chaos system and neural networks. In *Parallel Processing and Applied Mathematics* (pp. 364–373). Springer.
5. Chauhan, M., Prajapati, R. Image encryption using chaotic based artificial neural network.
6. Zhang, Y., Xiao, D., Wen, W., Wong, K.-W. (2014). On the security of symmetric ciphers based on DNA coding. *Information Sciences, 289*, 254–261.
7. Zhang, J. (2015). An image encryption scheme based on cat map and hyperchaotic lorenz system. In *2015 IEEE International Conference on Computational Intelligence & Communication Technology (CICT)* (pp. 78–82). IEEE.
8. Zhou, Y., Bao, L., & Chen, C. P. (2014). A new 1d chaotic system for image encryption. *Signal Process, 97,* 172–182.
9. Zhang, Q., Liu, L., & Wei, X. (2014). Improved algorithm for image encryption based on dna encoding and multi-chaotic maps. *AEU International Journal Electronics and Communications, 68*(3), 186–192.
10. Awad, A., Miri, A. (2012). A new image encryption algorithm based on a chaotic dna substitution method. In *2012 IEEE International Conference on Communications (ICC)* (pp. 1011–1015). IEEE.
11. Avasare, M. G., Kelkar, V. V. (2015). Image encryption using chaos theory. In *2015 International Conference on Communication, Information & Computing Technology (ICCICT)* (pp. 1–6). IEEE.
12. Singla, P., Sachdeva, P., & Ahmad, M. (2014, February). A chaotic neural network based cryptographic pseudo-random sequence design. In *2014 Fourth International Conference on Advanced Computing & Communication Technologies* (pp. 301–306). IEEE.
13. Hu, Y., Zhu, C., Wang, Z. (2014). An improved piecewise linear chaotic map based image encryption algorithm. *The Scientific World Journal*. Cairo.
14. Kassem, A., Hassan, H. A. H., Harkouss, Y., & Assaf, R. (2014). Efficient neural chaotic generator for image encryption. *Digital Signal Process, 25,* 266–274.

15. Li, X., Li, C., Lee, I.-K. (2016). Chaotic image encryption using pseudo-random masks and pixel mapping. *Signal Process, 125*, 48–63.
16. Lian, S. (2009). A block cipher based on chaotic neural networks. *Neurocomputing, 72*(4), 1296–1301.
17. Maddodi, G., Awad, A., Awad, D., Awad, M., & Lee, B. (2018). A new image encryption algorithm based on heterogeneous chaotic neural network generator and DNA encoding. *Multimedia Tools and Applications*, 1–25.
18. Liu, H., Wang, X., et al. (2012). Image encryption using DNA complementary rule and chaotic maps. *Applied Soft Computing, 12*(5), 1457–1466.
19. Liu, Y., Tang, J., & Xie, T. (2014). Cryptanalyzing a RGB image encryption algorithm based on dna encoding and chaos map. *Optics & Laser Technology, 60,* 111–115.
20. He, J., Yu, S., & Cai, J. (2015). A method for image encryption based on fractional-order hyperchaotic systems. *Journal of Applied Analysis and Computation, 5*(2), 197–209.
21. Roslan, U. A. M., Salleh, Z., & Kılıcman, A. (2012). Solving Zhou's chaotic system using Euler's method. *Thai Journal of Mathematics, 8*(2), 299–309.
22. Zhang, J., Hou, D., & Ren, H. (2016). Image encryption algorithm based on dynamic DNA coding and Chen's hyperchaotic system. *Mathematical Problems in Engineering*, *2016*.
23. Wu, Y., Noonan, J. P., Agaian, S. (2011). NPCR and UACI randomness tests for image encryption. *Cyberjournals: Multidisciplinary Journals in Science and Technology*. *Journal of Selected Areas in Telecommunications (JSAT)*.
24. Bassham III, L. E., Rukhin, A. L., Soto, J., Nechvatal, J. R., Smid, M. E., Barker, E. B., … & Heckert, N. A. (2010). Sp 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications.
25. Bhatt, C., Dey, N., & Ashour, A. S. (Eds.). (2017). *Internet of things and big data technologies for next generation healthcare*.
26. Dey, N., Hassanien, A. E., Bhatt, C., Ashour, A., & Satapathy, S. C. (Eds.). (2018). *Internet of things and big data analytics toward next-generation intelligence*. Berlin: Springer.
27. Hassanien, A. E., Dey, N., & Borra, S. (Eds.). (2018). *Medical big data and internet of medical things: Advances, challenges and applications*. Boca Raton: CRC Press.
28. Chen, J.-X., Zhu, Z.-L., Fu, C., Yu, H., & Zhang, L.-B. (2015). A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. *Communications in Nonlinear Science and Numerical Simulation, 20*(3), 846–860.

Design and Implementation of Efficient Routing Protocol

Implementation of Traffic Priority Aware Medium Access Control Protocol for Wireless Body Area Networks

Kanhu Charan Gouda, Subhra Priyadarshini Biswal, Sourabh Debnath and Sagar Kumar Sahu

Abstract Wireless Body Area Networks (WBANs), which are a sub domain of Wireless Sensor Networks (WSNs), can undoubtedly improve in various fields of medical service like health care, diagnostic monitoring, patient monitoring and other activity related to health. Recently, the use of WBANs has increased in small amount of time. Design of effective and adaptability use of Medium Access Control (MAC) protocol is one of the fundamental themes in wireless body area networks (WBANs). The MAC protocol is based on various access techniques. Wireless Body Area Network is a very exciting technology, which has attracted on the whole world. It plays an important role in the future of e-health and the development of smart. Hence, the proposed protocol is designed for WBANs. In this paper, a new routing protocol is proposed for traffic management. In this paper, we first categorized patient data to emergency and non-emergency data depend on high and low threshold value and then we develop a superframe structure, which consists of contention access period, contention free period, low power listening mode and beacon period. The threshold value support classification which includes a number of parameters like medical sensors, body placement and data transmission. Then we implement data traffic prioritization to give priority to patient data to reduce the average delay time in superframe structure so that contention will be reduced, also minimize energy consumption and increase throughput.

Keywords Wireless sensor networks · Superframe structure · Medium access control · Wireless body area network · TAMAC

K. C. Gouda (✉) · S. P. Biswal · S. Debnath · S. K. Sahu
Department of Computer Science, National Institute of Science and Technology (Autonomous), Institute Park, Pallur Hills, Brahmapur 761008, Odisha, India
e-mail: kanhu325@nist.edu

S. P. Biswal
e-mail: subhrapriyadarshini033@gmail.com

S. Debnath
e-mail: dsourabh@nist.edu

S. K. Sahu
e-mail: sagarsahu030@gmail.com

S. K. Das et al. (eds.), *Design Frameworks for Wireless Networks*,
Lecture Notes in Networks and Systems 82,
https://doi.org/10.1007/978-981-13-9574-1_16

1 Introduction

Wireless Sensor Network (WSN) has developed significantly in research as well as in product development and in numerous fields like military, health care, domestic system and home system because of increasing number of sensors based applications [1]. Wireless Body Area Network (WBAN) is a special designed WSN [2] which is capable of connecting various Medical Sensors (MSs) and monitoring patient for long period of time for diagnosing and treating health issues at an early stage. WBAN is a sub domain of WSN. As per each day, according to World Health organization (WHO) around 55.3 million people die each year and 151,160 people die each day because of many incurable diseases like cancer, heart diseases and paralysis. The heart disease is the leading cause death in each and every country around the world. So the old people and patient need to be monitoring continuously of their disease and health which cost them high and also for developing country like India [3].

So another domain of WSN that is WBAN, which is cost affordable solution and can be used for early detection of disease and has witnessed significant attention in healthcare domain. The WBAN is the new technology in health application and can collect patient data and provide it to medical service provider. The sensor used in WBAN can collect data from one sensor to another sensor and can send it from one sensor to another sensor. WBAN is very exciting technology which has attracted on the whole world. WBANs consist of many MSs. These MSs can be deployed inside the body or implanted on outside body or it can be wearable sensors like ECG, EEG sensors. In this paper, two algorithms are proposed that is Data Severity on vital sign of Patient (DVP) and Emergency data Transfer Slots (ETS) slot allocation based on Severity of Vital sign (ETSVS) for calculation of threshold value based on patient data.

Different types of protocol used in WBAN but among them use MAC protocol, which has two subcategories that is IEEE 802.15.4 [4] and IEEE 802.15.6 [5, 6]. Among these two protocols, first protocol is used for WSN and second protocol is used for WBAN, but the first protocol is precedence over the second protocol. IEEE 802.15.4 is more supple in coverage and support more sensors as compared to IEEE 802.15.6 but consumes high energy than IEEE 802.15.6. The MAC protocols used in our project should be energy efficient, reliability with less data loss and delay. MAC protocol is responsible for connecting different sensors inside the network. With the help of this MAC protocol, sensors can communicate with other sensors in the same networks or in different networks.

1.1 Wireless Body Area Network (WBAN)

Recent development and technological advancement in wireless communication, Microelectro Mechanical System (MEMS) technology and nanotechnology has brought low-powered nano and micro technology which strategically placed inside or outside of human body for various applications such as health monitoring and diagnosing. The main aim of the WBAN is to simplify and increase the speed of

communication between sensors nodes between them and inside the body also. For example, patient need not have to stay in hospital during treatment; he/she can move freely or may leave the hospital. This reduces the cost and can improve the lifestyle of the patient.

1.2 Architecture of WBAN

WBANs are mostly used in medical field and communication. WBANs consist of many tiny MSs. Basically three types of methods are available for implantation of these sensors in human body. The use of MSs includes in-body, on the surface of skin of human body and placement near human body for monitoring vital sign of patients (blood pressure, oxygen, heart rate). In implantation sensors are placed inside the body for monitoring lungs, kidney and liver. In off-body, sensors are placed on the body for monitoring ECG, EEG and EMG.

These sensors also portable and can be carried in different positions. These sensors can more effective than other two methods and it is a key technology in health monitoring case. These sensors are connected to medical server. The primary functions of the sensors is to sample vital sign of patient. Medical server collects information from different types of sensors and forward it to hospital and according to the priority of information, patient gets its needs.

1.3 Application of WBAN

WBANs are used in the medical field for the monitoring and detecting the internal diseases of the human body. WBANs are used for the detection of various chronic diseases such as heart attacks, asthma, etc. The application of WBANs is as shown in Fig. 1 [7]. Following are the application of WBANs.

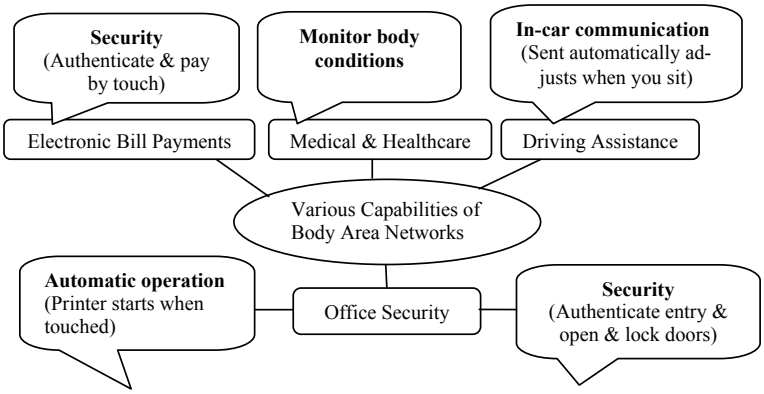


Fig. 1 Application of WBANs

1.3.1 Remote Patient Monitoring

Remote health monitoring and telemedicine are the main application of wireless body area network. Telemedicine means diagnosis and treatment of using telecommunication and information technology from a distance. WBAN has now made it possible. Using telemedicine more and more patients can be served in less time and reduce cost also. Body sensors gather data from patient and send those data to doctor for further process. Doctor can also use that information for health checkup treatment. This will create a smart health treatment.

1.3.2 Rehabilitation

By rehabilitative method, you can keep and improve abilities that a person needs in his/her daily life. You may have lost them because of disease or serious injury. These patients need to continuous monitor for better health. So WBANs make it easy, WBAN continuously keep the track of different vital signs of patient and send it to doctor. The feature of WBANs includes sensor variation, data fusion, real-time comment and household improvement health through a device that continuously and constantly monitors bodily activities.

1.3.3 Biofeedback

WBAN can do monitoring of human body remotely. People can take care their health all the way through biofeedback analysis like body temperature analysis, blood pressure finding, ECG, EEG, etc. It means maintaining and upgrading health through wireless/wired devices that constantly monitors all activities of a human body.

1.3.4 Assisted Living

This application of WBAN helps to improve the virtue of life. This technology enables elderly and old aged citizens to be monitored at their home. This will also reduce their hospital costs.

1.4 Superframe Structure

This section represents superframe structure of IEEE 802.15.4 and IEEE 802.15.6 [8]. Both of these superframe structure contains CAP, CEP and beacon and active and inactive period. Both protocols are requiring for data transmission which contains number of allocation slots. Both protocols are used in wireless communication on behalf of short-range communication. However, a few studies were conducted to find

Table 1 Contrast and compare between IEEE 802.15.4 and IEEE 802.15.6

Feature	IEEE 802.15.4	IEEE 802.15.6
Specific task	Designed for medical field, to monitor environment events like temperature and also for military application	Specially built for health care and medical application
Nature of data	Homogenous	Heterogeneous
Network coverage	Scalable	Medium
Network deployment range	10–100 m	3–6 m
Frequency band	ISM	ISM and other bands approved by medical authorities
Data transmission medium	Air	Air, inside body and on-body
Data transmission rate	20–200 kb/s	50 kb/s to 100 mb/s
Scheduling access scheme	CSMA/CA, TDMA, FDMA, Aloha	CSMA/CA, TDMA, FDMA

similarities and difference between these two protocols [9] as given in Table 1. In this table, two protocols, i.e. IEEE 802.15.4 and IEEE 802.15.6 are compared with several features. The proposed method is based on IEEE 802.15.4, where it is used for WSN and IEEE 802.15.6 used for WBANs.

1.4.1 IEEE 802.15.4 Superframe Structure

The MSs are placed on the surface of human body for determining sign of a patient. These MSs are attached to a coordinator of body network. Here there are three classifications of patient data that is emergency, periodic and normal data. The periodic data are generally glucose reading and blood pressure and normal data are temperature and emergency data are critical vital sign like heartbeat, ECG, EEG. Further, the IEEE 802.15.4 superframe structure comprises a beacon, CEP, CAP and LPL/IP. Here all MSs follow CSMA/CA method and based on contention to acquire all channel of CAP. The coordinator of body network passes a notification to every MSs in the network consisting data about synchronization and logical address of coordinator of body network. In synchronization, MSs transmit request for channels allocation and deallocation. The Beacon Interval (BI) is the time interval where Medical Sensor transmits sensory data for a specific period. The Inactive Period (IP) is used when there is no transmission and for saving energy.

IEEE 802.15.6 operates in 3 frequencies which are 16 channels in 2.4 GHz ISM band, 10 channel in 951 MHz ISM band and 1 channel in European 868 MHz. IEEE 802.15.4 has 2 operational modes that us beacon enabled and non-beacon enabled mode. There are also some few limitations in this superframe structure.

- It is restricted up to 16 (0–15) channels.
- All MSs execute contention to acquire channel in CAP period.

- There is no priority based slots are dedicated for emergency data.
- MSs perform contention and also consume higher energy.
- Due to collision higher delay occurs in emergency data and as a result it retransmits the collided packets and require limited time interval of a BI.

The above drawbacks decrease the performance of MAC superframe structure due to low consistency, conflict and high energy consumption.

1.4.2 IEEE 802.15.6 Superframe Structure

This superframe structure was first published in 2012 [10]. There are two methods available for propagating data existence in WBANs, one-hop and two-hop communication. In these two types of communication, the nodes are structured in mesh and star topologies [11]. In one-hop, the coordinator of body network is a central controller which is in charge of allocations of slots to MSs. Similarly in two-hop, there is a broadcast sensor or intermediate sensor is there and the work of broadcast sensor is to exchange frames among various sender sensors and coordinator of body network when they are not at closer range. The usage of the coordinator sensors consumes a huge energy for the duration of communication of the patient's information. Hence, IEEE 802.15.6 was determined to create low power device to check patient's data and vital sign and psychological condition to overcome the limitation of IEEE 802.15.4 which was discussed before. The first version of IEEE 802.15.6 categorize the superframe structure to various channels and beacons. It defines a MAC that supports physical layers such as Narrow Band (NB), Ultrawide Band (UB), Human Body Communication (HBC). This superframe structure defines three ways of data transmission and these are enabled beacon superframe structure, non-enabled beacon superframe structure, non-enabled beacon without superframe structure. There is also some limitation as follows.

- During critical situations, there is no dedicated slot for transmission of emergency data as well as no categorization of this data into high and low priority values.
- In non-beacon MAC superframe structure, BNC cannot transmit data directly into MSs.
- MAC allows only one type of patient data for slot allocation at same time.

1.5 Objective of MAC Layer

MAC protocol defines a specific way of a medium which is accessed for transmission. It belongs to Data Link layer (DLL) of OSI model. This DLL consists of two layers one is MAC layer and another is logical link layer (LLC). While MAC is responsible for medium access then LLC is responsible for logical link control. LLC provide end-to-end flow, error control and multiplexing different protocols over the MAC layer and demultiplexing those.

Each node which needs to become a part of network communication has a MAC address or some time called physical address, which makes them unique and distinct from others. This makes data possible to send to correctly to destination through the network. Different protocols have been developed by IEEE (Institute of Electrical and Electronics Engineers, USA) and some of them are IEEE 802.15.4 and IEEE 802.15.2. MAC layer handle frame authentication, guaranteeing time slots and monitor node.

The roadmap of the manuscript as follows. Section 2 defined the literature review, Sect. 3 highlights the main problem statement, Sect. 4 describes performance evaluation, and Sect. 5 concludes the proposed work.

2 Literature Review

In the past few decades, several works have been proposed, some of them are described as. In [1], TAMAC provides a dedicated time slots to emergency data without contention. As compared to existing MAC, suggested TAMAC reduce delay, thus increasing throughput and also minimize energy consumption and also resolves conflict slot allocation. In [6], Modelling and Simulation of WBANs for Monitoring Sick Patient Remotely has been proposed. In this paper, one architecture was proposed which conveys a united telemedicine service that automates the process from data gathering to information distribution. Many advantages have been discussed and some of them are providing real-time data collection, simplifying the deployment process. In [8], the QoS routing protocol uses routing table constructor algorithm, path selector algorithm to calculate the communication cost, path delay and all possibilities path from sender to receiver and after that decide the finest way with QoS requirements consideration. Omnet++-based simulator Castalia is used to evaluate the performance of suggested QoS protocol. In [12], it focuses on Continuous Health Monitoring System for wearable body sensor network. In support of a wearable, continual health observing system, a self-configured body sensor network controller and a higher efficiency wirelessly powered sensor are required. The sensor chip used Adaptive Threshold Rectifier (ATR) for harvesting its power from the surrounding health monitoring. The ATR is implemented with a CMOS process to reduce its cost. The network controller spontaneously detects the sensor position, arrange the type of sensor (self-configuration), wirelessly supplies power to the configured sensors and conduct data with only the elected sensors. In [13], it focuses on study of existing/proposed MAC protocols for Wireless Body Area Networks. Different mechanisms like LPL, schedule contention and TDMA mechanism were examined and analysed in the WBAN. The CSMA/CA come across many unreliable issuesand faces heavy collision. So that TDMA is observed as most consistent and capable protocol for WBAN. But there is also limitation of TDMA in terms of dynamic slot allocation, synchronization and many more. So, a low-power MAC is developed basically based on TDMA to satisfy the traffic heterogeneity and correlation. This study can be used for development of low-power MAC protocol. In [14],

a routing protocol for multicast ad hoc network was proposed. It creates a power effective pathway from source to every multicast set built on two vague parameters such as distance and energy. It uses fuzzy inference system to deal with imprecise data. As other parameters were not considered by this proposed work which leads to its limitation. In [15], fuzzy-based multi-constraints multicast routing protocol was proposed. They have considered three parameters that are delay, bandwidth and energy as they vary frequently. It supports to elect the best route along with the help of fuzzy cost. In the past few years, several techniques are proposed for WSNs as well as ad hoc network for network lifetime enhancement [16–19]. But the proposed method is especially for WBANs traffic management technique.

3 Problem Statement

Nowadays, various incurable diseases like cancer, diabetes are the major cause of the death of the patient. So these types of disease need early detection so that it can decrease the death rate around the world. With a very high speed improvement in physiological sensors and wireless communication, wireless sensor networks have developed remarkably and also support a large range of applications including health care and medical services. So WBANs consist of many MSs to monitor the vital sign of the patient. These vital signs of the patients are heterogeneous in nature. So that various kinds of sensors are necessary to intellect and examine human beings' various health parameters, which may also be different in performance, storage capacity and energy consumption.

To put the sensors in human body, basically there are three types of procedure for implantation of these sensors in human body. Implantation of MSs include in-body, on the surface of skin of human body and placement near human body for monitoring vital sign of patients like ECG, EMG, EEG. In near-body placement, the sensors are placed near the body to monitor motion of different body parts like arm and leg position and other physical health conditions. All of these sensors are connected to a BNC in star topology. BNC is like a router in Body Area Network (BAN). BNC is to facilitate to patient so that it was not necessary for patients to keep on in hospital. In these, implementation radio-frequency parts of the sensor play a key role in energy consumption. So MAC protocol reduces energy consumption.

In [5, 20] IEEE 802.15.4 and IEEE 802.15.6 have been proposed. An MAC protocol is responsible for increasing error-free data transmission, maximizing throughput, increasing network lifetime and minimizing transmission delay, hence increasing the network lifetime. There is also important factor of BAN that we need to take care of and some of are limited bandwidth, energy efficiency, QoS (Quality of Service), transmit power.

In [21] QoS, flexibility and cost efficiency are main goal in WBAN. The MSs are placed during BAN formation is a manual process. Sensors are placed on different positions on human body manually which cannot be disturbed by noise. Generally, BAN routing protocol is responsible for providing a reliable and dynamic pathway to

send patient's normal data and critical data. QoS (Quality of Service) [4] are of two types, one type is delay tolerant and reliability. In delay-tolerant, packets are needed to be delivered before the deadline. The reliability protocol ensures that maximum packets are delivered to the destination.

In [8], Medical Sensor Network is created by physiological parameter sensor located in human body. Sensors are of two types that is accelerometer which is used to monitor ECG, EEG, detect blood pressure and another type is glucose sensor which is used to detect temperature and glucose level. Monitoring of patient data has been categorized into emergency and non-emergency data. These categorizations include Ordinary Data (OD), Critical Data (CD), Normal Data (ND) and Reliable Data (RD). BNC assigns guarantee time slot allocation in Contention Empty Period (CEP) for data transmission. We can use IEEE 802.15.4 and IEEE 802.15.6 for slot allocation and for superframe structure.

In IEEE 802.15.4, the slot allocation of data is based on contention in Contention Access Period (CAP) [9, 16]. Due to this contention, it degrades the performance of the above protocol due to the finite number of channel in superframe structure which results collision, high delay of data and lower consistency of data during transmission. CAPs have been classified into four slots and provision is based on contention, IEEE 802.15.4 cannot fulfil all requirements. So we have specific requirement for health and medical field and also does not carry QoS for various from of coexisting in WBAN. QoS-aware MAC protocol is required for WBAN in ISM (Institute of Science and Medical) band.

So, to fulfil the requirement of WBAN, IEEE 802.15.6 is published in 2012. IEEE 802.15.4 defines the physical layer and MAC to serve a variety of services for medical and non-medical application. IEEE 802.15.6 was the first international WBAN that supports inside the human body to provide a variety of medical applications and non-medical applications. IEEE 802.15.6 operates in low power and can communicate in small range and mainly supply human data to evaluate human physiological condition. The IEEE 802.15.6 is designed in such a way to provide low complicacy, low price, low power utilization and highly reliable wireless communication [22].

3.1 Traffic Priority Aware Medium Access Control Protocol (TAMAC)

The authors in this work have proposed an adaptive MAC protocol based upon traffic priority. They have used superframe structure, traffic prioritization and severity recognition along with slot allotment algorithm. They have considered both normal data and emergency data [23, 24]. Here, all classified data execute contention to acquire all channels of CAP. But there are some disadvantages in both protocols. They do not assign wedded slot allocation to emergency data without contention. So due to these disadvantages, it results in collision and medical sensor consumes huge energy which leads to performance degradation of the MAC protocol. So to avoid

this problem, a Traffic Load Sensor (TLS) protocol was suggested which classifies information into low-load, moderate-load and high-load. But during implementation, we classified the patient data into CD, OD, RD and DP. The CD is the high priority data which is allocated to first available channel, RD is the next highest priority data to access channel without loss of packet, The DP is the third highest priority which must be transferred on time and the OP is the last priority of data that can be delayed. But the recommended MAC solves contention of slot allocation when same value of vital sign received.

3.2 Suggested Superframe Structure

The Traffic-Aware Medium Access superframe structure contains beacon, BI (Beacon Interval), CAP, CEP, Emergency Data Transfer Slots (ETS), Critical data Transfer slots (CTS), Normal Data Transfer slots (NTS), Low Power Listening (LPL) or Inactive Period (IP). The proposed superframe structure provides 42 slots by access point(coordinator), that is, 8 slots for ETS, 10 slots for CTS, 8 Slots for NTS, 7 slots for CAP, 1 slots for B, N, EB and LPL/IP [1]. The inactive period is represented as LPL mode because this is used by wireless body sensors to minimize energy consumption when there is no data propagation. Beacon determines the time interval between two beacons. Patient data is categorization into CD, OD, RD and DP.

OD refers to the normal reading of vital signs which is the normal temperature of body and calorie level. This data can be delayed without consistency compulsion, similarly DP is generally audio or video depending on information about a patient such as body movement, which can be minimum delay with less loss. So, for OD and DP we assign in NTS. RP comprises reading of great variation of vital signs that are high blood pressure and low sugar level. The RP data is needed to be transmitted with less loss of packet and delay, similarly CD consists of different vital signs like low heart rate and high sugar level, this type of data is required to be delivered without any delay and packet loss and with higher reliability. So RD and CD are assigned to CTS. The active period in superframe structure is represented as SD (Superframe Duration). CAP scans sensor or vital sign of patient data before entering into CEP. CAP is required to carry a huge number of data packets to BNC.

After knowing the Notification (N) from wireless body sensor node, the CP and RP allocate the ETS. Further, the coordinator will take priority among two data packets which will be allocated the packet in CTS at first priority. At that time the Emergency Beacon (BE) signal occurs for allocated data packet in which is allocated first in CTS according to the priority. BE is basically tracking transmitter used to send signal of location of MSs used in human body.

The Back Off Exponent (BOE) time evaluates the back off interruption for accessing CAP and attempt to decrease collision on BOE based on volume of the Contention Window (CW) as shown in Eq. 1.

$$\mathrm{CW} = 0 \text{ to } 2^{\mathrm{BE}} - 1 \tag{1}$$

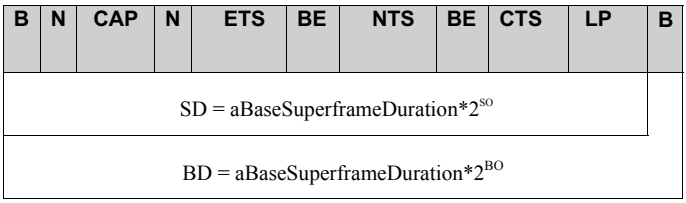


Fig. 2 Superframe structure of TAMAC

Superframe Duration (SD) and Beacon Interval (BI) are related with Superframe Order (SO) and Beacon Order(BO). SO manages the duration of active period of TAMAC as described in Eqs. 2 and 3 the duration of the entire Superframe of TAMAC is managed by BO

$$\mathrm{SD} = \mathrm{aBaseSuperframeDuration}^{*}\, 2^{\mathrm{SO}} \tag{2}$$

$$\mathrm{BI} = \mathrm{aBaseSuperframeDuration}^{*}\, 2^{\mathrm{BO}} \tag{3}$$

After knowing the Notification (N) from wireless body sensor node, the CP and RP allocate the ETS. Minimum duration of slots is represented by a Base Superframe Duration in Eqs. 2 and 3. IEEE 802.15.4 supplies minimum value of BOE is 3 and maximum value of BOE is 5. BE depends on contention window size (Fig. 2).

3.2.1 Traffic Prioritization and Reduce Slot Allocation Contention

The patient's traffic is divided into E1, E2, E3 and E4, which represent emergency data, on-demand data, normal data and non-medical data. In contention E1, every phase of CAP period was acquired, E2 type of traffic can only access phase 2–4, E3 traffic data resides in channel of slots of 3 and 4 and E4 traffic occupies only channel of phase 4. The proposed approach categorizes the patient's data into OD, DP, RD and CD. OD contains normal reading of vital sign while CD contains severity of vital sign. DP basically based on different information of a patient such as body movement, sleeping posture, hand shaking, etc.; it receives least delay with loss. RD is the low priority value like blood pressure, heart beat rate and need to be delivered with minimum loss and CD is high priority value need to be delivered with no loss of data like low blood pressure, ECG.

The contention-based slot allocation results in collision of patient's data, which causes delay due to retransmission of collided information and also acquires high amount of energy. So, in this paper to provide a Detection of Vital sign of Patient data (DVP) and ETSVS algorithm to reduce contention-based slot allocation and for traffic prioritization of data.

In emergency situation, medical sensor detects abnormal reading of vital sign of patient data low priority and high priority value like blood pressure, high heart beat rate. The emergency data needs to be delivered without contention. If contention occurs, then collision of data results higher delay due to retransmission of data and consumes higher energy. For this, to classify patient data into low priority and high priority data value. High priority data value like CD, RD and low priority value like OD, DP. To minimize contention slot allocation and efficient traffic, prioritization of data two algorithms are proposed which is given in Algorithms 1 and 2.

Algorithm1: Detection vital Sign of Patient Data (DVP)

NS_{ith}= no of sensors in Wireless network
NS_off=sensor $_{1\ to\ i}$in LPL
Monitor_Vsign
LP=lower priority value
HP=High priority value
NS_{ith}_TRAS=sensor transmit signal to BNC
BNC_ETS=BNC allocate ETS to sensor
ETS=emergency data transfer slot
NS_{ith}_HP_LP=sensor transmit high and low priority value
UEC=Unusual event occur

Input- blood pressure, Heart beat
Process-
1.START
2.BEGIN NS_{ith}
3.NS_{ith}←NS_off
4.NS_{ith} ← Monitor_Vsign
5.NS_{ith}←1;
6.While (NS_{ith}← Monitor_Vsign)
7.If ($NS_{ith==}$LP or $NS_{ith==}$HP) then
BNC_{BE}← NS_{ith}_TRANS_VAL

ETS ← BNC_NS_{ith}
Else
8.Print (Unusual event occur);
9. End if
10.End loop
11.EXIT

Algorithm2: ETS Slot Allocation on Emergency Vital Sign (ETSVS)

NS_{ith}= number of sensors in wireless network
NS_{ith}_off=number of sensors allocated in inactive period
NS_{ith}_on=number of sensors allocated in active period
NS_{ith}_on_CD=number pf sensors allocated in active period for CD
NS_{ith}_on_RD=number pf sensors allocated in active period for RD
NS_{ith}_on_OD=number pf sensors allocated in active period for OD
NS_{ith}_on_DP=number pf sensors allocated in active period for DP
LP=Low Priority Value
HP=High priority Value
ETS=Emergency data Transfer slots
NTS=Normal Data Transfer slots
CTS=Critical Data Transfer Slots
HP_CD=High priority value CD
LP_RD=Low priority value RD
HP_OD=High priority value OD
LP_DP=Low priority value DP
UEC=Unusual Event Occur

Input= Heart Beat, Blood Pressure, ECG

Process

1. While ($NS_{ith=}NS_{ith}$_on or NS_{jth}_off) do // when BNC receives only one signal from sensors
2. if (BNC ← NS_{ith}_on_HP || BNC <- NS_{jth}_on_HP) then
   ETS ← NS_{ith}_on_HP or NS_{jth}_off_HP;
   Else
   Goto sleep mode
3. END if

while (BNC ← NS_{ith}_on&&NS_{jth}_on) // (when BNC receives two emergency data simultaneously \\

4. if (NS_{ith}_on == HP_CD or NS_{jth}_on=HP_CD) // when both sensors $NS_{ith}$and NS_{jth}has high priority value //
5. CTS= NS_{ith}_on_CD or CTS= NS_{jth}_on_CD;
6. Elseif (NS_{jth}_on==LP_RD or NS_{ith}_on_LP_RD)
7. CTS= NS_{jth}_on_RD or NS_{ith}_on_RD;
8. Else
9. Print (Unusual Event Occur);
10. END if
11. END if
12. Elseif (NS_{ith}_on==LP or NS_{jth}_on==LP)

```
13.            If (NS_ith_on==HP_OD or NS_jth_on==HP_OD)
                        NTS← NS_ith_on_OD or NS_ith_on_DP;
14. Elseif (NS_ith_on_LP_DP or NS_jth_on_LP_DP)
15.                     NTS ← NS_ith_on_DP or NS_ith_on_DP;
16.             Else
17.              Print (Unusual event occur);
18. End if
19. End if
20. End  loop
21. While (NS_ith=NS_ith_off&&NS_jth_off)
          Goto IP;
          END if
    END while
    EXIT
```

There are (n) no. of sensors for monitoring vital sign of patient data. The first part of the algorithm is based on one single MSs, while the other part is based in the two MSs when two emergency data is received by BNC simultaneously. In the first of the algorithm, when BNC receives only one single value from the sensor, then according to priority value, BNC transmits an alert signal to BE slots of the superframe structure of TAMAC. Then BNC allocates ETS slots according to priority based. In the second part of the algorithm, when BNC receives two emergency data from sensors simultaneously. From line 4 to 18, it allocates critical data according to priority of data. It first checks, between two data which of the data has more priority than other, like CD and RD, between these two data, always CD has more priority value than RD. SO BNC assigns CD type data to CTS and then after allocation of CD, it assigns second slot to RD data. Similarly, when Low priority data arrived in BNC or when BNC received low priority data then it allocates the two data in the above described method.

4 Performance Evaluation

Our proposed protocol is simulated by using OMNET++ considering various parameters and compared with the existing protocol, i.e. IEEE 802.15.4. The data which is generated is transmitted through different frequencies due to its heterogeneous nature.

4.1 Simulation Implementation

In this section, in order to explain in TAMAC protocol for WBANs implementation of OMNET++ network simulator is explained. Low power sensor device is implanted in wireless network or wireless BAN which is to be implemented by the simulation through Castalia framework. It is built on the OMNET++ platform, OMNET++ is the basic concept of object oriented of the modular approach to accept the message from one module to another module. The proposed method is compared with some existing methods [1, 6, 8, 12–15] which is shown in Table 2 and categorization of threshold values of vital signs shown in Table 3.

We used OMNET++ as the base to implement and construct a decent and fast simulator. Using OMNET++, we can focus on the models and overall blue print.

Table 2 Comparison of proposed method with other methods

Algo. versus Char.	Characteristics				
	Network type	Topology	Setup	Network lifetime	Delay
Proposed	WBAN	Dynamic	Infrastructure-less	Very High	Very Less
Reference [1]	WBAN	Dynamic	Infrastructure-less	Moderate	Medium
Reference [6]	WBAN	Dynamic	Infrastructure-less	Moderate	Medium
Reference [8]	BAN	Dynamic	Infrastructure-less	Moderate	Medium
Reference [12]	BAN	Dynamic	Infrastructure-less	Moderate	Medium
Reference [13]	WBAN	Dynamic	Infrastructure-less	Moderate	Medium
Reference [14]	WANET	Dynamic	Infrastructure-less	High	Less
Reference [15]	WANET	Dynamic	Infrastructure-less	High	Less

Caption:
Algo. Algorithm. *Char.* Characteristic. *WBAN* Wireless Body Area Network
BAN Body Area Network. *WANET* Wireless Ad hoc Network

Table 3 Categorization of threshold values of vital signs

Vital sign	Low values	Normal values	High values
Heart beat (beats/min)	0–45	68–72	100–120
Blood pressure	(70–90)/(40–60)	(90–120)/(60–80)	(140–190)/(95–105)
Temperature	NIL	96.7 Fahrenheit	100–105 Fahrenheit

Here we have decided to capture realistic node behaviour beyond the channel and build an open expandable and reliable simulator that has a chance of becoming a de facto standard for certain WSN simulation needs.

4.2 Analysis of Results

The performance of the TAMAC is analysed and compared with IEEE 802.15.4, which is MAC protocol for delivery and throughput.

4.2.1 Delay Time

The sensor based on non-emergency data performs contention to access channel while sensors based on emergency data access channel without contention. So the delivery delay of packet is defined as in Eq. 4.

$$\text{Delay} = \frac{\sum(\text{TR} - \text{TD})}{\sum(\text{BN})} \tag{4}$$

4.2.2 Throughput

Throughput is basically the generated packet of MSs to successfully receive by BNC per second in its allocated slots. It can be stated as given in Eq. 5.

$$\text{Throughput} = \frac{\sum\text{Packet received}}{\sum\text{Packets generated}} \tag{5}$$

4.2.3 Average Delay Versus No. of MSs

From this below result, we see that in TAMAC, the emergency data received by BNC and allocated to ETS slots with less delay as compared with IEEE 802.15.4. In proposed approach, the average delay time got minimized in compared to the existing protocol. So this reduces the contention slot allocation in suggested superframe structure as given in Fig. 3.

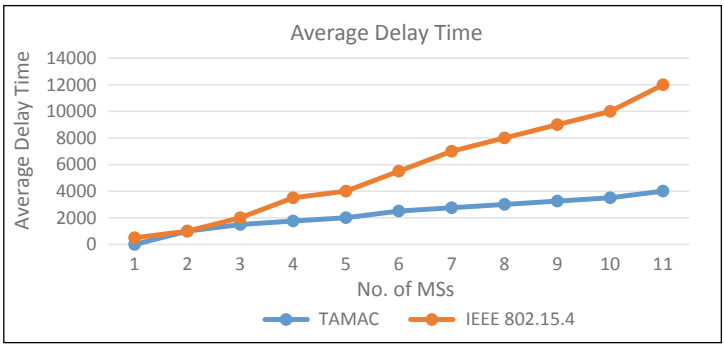


Fig. 3 Average delay versus no. of MSs

4.2.4 Throughput Versus No. of MSs

The RD and CD data are considered as emergency data in TAMAC. So, these types data should be delivered with no packet loss. MSs do not perform contention for slot allocation but then send a signal using BE slot for ETS slot allocation to BNC. BNC allocates MSs, if it receives a notification from MSs. If BNC receives two signals from two MSs simultaneously, then according to priority, it allocates to TAMAC as described in ETS algorithm. But the existing MAC does not have capability to resolve conflict slot allocation which is solved in suggested MAC that is TAMAC. The energy consumption in TAMAC is minimized and also reduces average delay time as shown in Fig. 4. The throughput of TAMAC also increased as compared to IEEE 802.15.4 as shown in Fig. 4.

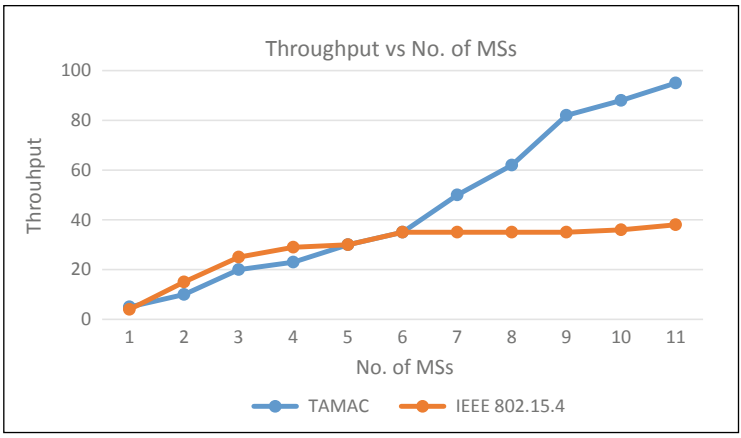


Fig. 4 Throughput versus no. of MSs

5 Conclusion

In this paper, a suggested MAC that is TAMAC has been suggested for better efficient use of slot allocation for emergency and non-emergency data. This also reduces contention-based slot allocation of non-emergency data, which increase performance of the MAC. Also the emergency data do not perform contention for slot allocation. This paper also focuses on traffic prioritization of data of patient. Suggested MAC protocol also resolves the conflict of slot allocation when two emergency data arrive simultaneously. Simulation has been performed to analyse the result and also the output is compared with existing MAC protocol. From this chapter, we conclude that the suggested MAC performs better than existing protocol and also reduce average delay time, hence increase the better data flow and also increase throughput and also consume less energy. In future work, the proposed method will be applied with the help of machine learning algorithm.

References

1. Ullah, F., Abdullah, A. H., Kaiwartya, O., & Cao, Y. (2017). TraPy-MAC: Traffic priority aware medium access control protocol for wireless body area network. *Journal of Medical Systems, 41*(6), 93.
2. Binh, H. T. T., & Dey, N. (Eds.). (2018). *Soft computing in wireless sensor networks*. CRC Press.
3. Ullah, S., Higgins, H., Braem, B., Latre, B., Blondia, C., Moerman, I., et al. (2012). A comprehensive survey of wireless body area networks. *Journal of Medical Systems, 36*(3), 1065–1094.
4. IEEE802.org, IEEE 802.15 WPAN Task Group 4 (TG4), EEE 802.15 WPAN Task Group 4 (TG4). (2016). http://www.ieee802.org/15/pub/TG4.html.
5. Kwak, K. S., Ullah, S., & Ullah, N. (2010, November). An overview of IEEE 802.15.6 standard. In *2010 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL 2010)* (pp. 1–6). IEEE.
6. Ali, A., & Khan, F. A. (2014). A broadcast-based key agreement scheme using set reconciliation for wireless body area networks. *Journal of Medical Systems, 38*(5), 33.
7. Sensors Network-Know all about BAN Body Area Network, EL-PRO-CUS (Electronics Projects Focus).
8. Khan, Z. A., Sivakumar, S., Phillips, W., & Robertson, B. (2014). ZEQoS: A new energy and QoS-aware routing protocol for communication of sensor devices in healthcare system. *International Journal of Distributed Sensor Networks, 10*(6), 627689.
9. Bouayad, A., Chaoui, N. E. H., & El Ghazi, M. (2015). Modeling and simulation of a wireless body area network for monitoring sick patient remotely.
10. Shuai, J., Zou, W., & Zhou, Z. (2013, September). Priority-based adaptive timeslot allocation scheme for wireless body area network. In *2013 13th International Symposium on Communications and Information Technologies (ISCIT)* (pp. 609–614). IEEE.
11. Bhandari, S., & Moh, S. (2016). A priority-based adaptive MAC protocol for wireless body area networks. *Sensors, 16*(3), 401.
12. Yoo, J., Yan, L., Lee, S., Kim, Y., Kim, H., Kim, B., et al. (2009, February). A 5.2 mW self-configured wearable body sensor network controller and a 12 μW 54.9% efficiency wirelessly powered sensor for continuous health monitoring system. In *2009 IEEE International Solid-State Circuits Conference-Digest of Technical Papers* (pp. 290–291). IEEE.

13. Ullah, S., Shen, B., Riazul Islam, S. M., Khan, P., Saleem, S., & Sup Kwak, K. (2010). A study of MAC protocols for WBANs. *Sensors, 10*(1), 128–145.
14. Das, S. K., Yadav, A. K., & Tripathi, S. (2017). IE2M: Design of intellectual energy efficient multicast routing protocol for ad-hoc network. *Peer-to-Peer Networking and Applications, 10*(3), 670–687.
15. Yadav, A. K., Das, S. K., & Tripathi, S. (2017). EFMMRP: Design of efficient fuzzy based multi-constraint multicast routing protocol for wireless ad-hoc network. *Computer Networks, 118,* 15–23.
16. Das, S. K., & Tripathi, S. (2019). Energy efficient routing formation algorithm for hybrid ad-hoc network: A geometric programming approach. *Peer-to-Peer Networking and Applications, 12*(1), 102–128. https://doi.org/10.1007/s12083-018-0643-3 (Springer).
17. Das, S. K., & Tripathi, S. (2018). Adaptive and intelligent energy efficient routing for transparent heterogeneous ad-hoc network by fusion of game theory and linear programming. *Applied Intelligence, 48*(7), 1825–1845. https://doi.org/10.1007/s10489-017-1061-6.
18. Das, S. K., & Tripathi, S. (2017). Energy efficient routing formation technique for hybrid ad hoc network using fusion of artificial intelligence techniques. *International Journal of Communication Systems, 30*(16). https://doi.org/10.1002/dac.3340.
19. Das, S. K., & Tripathi, S. (2018). Intelligent energy-aware efficient routing for MANET. *Wireless Networks, 24*(4), 1139–1159. https://doi.org/10.1007/s11276-016-1388-7 (Springer).
20. IEEE Computer Society LAN MAN Standards Committee. (1999). Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. ANSI/IEEE Std. 802.11-1999.
21. Djenouri, D., & Balasingham, I. (2009, September). New QoS and geographical routing in wireless biomedical sensor networks. In *2009 Sixth International Conference on Broadband Communications, Networks, and Systems* (pp. 1–8). IEEE.
22. Nepal, S., Pudasaini, A., Pyun, J. Y., Hwang, S. S., Lee, C. G., & Shin, S. (2016, July). A new MAC protocol for emergency handling in wireless body area networks. In *2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN)* (pp. 588–590). IEEE.
23. Li, C., Hao, B., Zhang, K., Liu, Y., & Li, J. (2011). A novel medium access control protocol with low delay and traffic adaptivity for wireless body area networks. *Journal of Medical Systems, 35*(5), 1265–1275.
24. Rahim, A., Javaid, N., Aslam, M., Qasim, U., & Khan, Z. A. (2012, June). Adaptive-reliable medium access control protocol for wireless body area networks. In *2012 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)* (pp. 56–58). IEEE.

Enhanced Shortest Path Routing Protocol Using Fuzzy C-Means Clustering for Compromised WSN to Control Risk

Ranjit Kumar, Sachin Tripathi and Rajeev Agrawal

Abstract In military, agriculture, industrial and commercial areas the wireless sensor network (WSNs) is broadly utilized. The safety of WSNs is a significant problem and they are attracting greater attention. WSNs are very susceptible for inner attacks from the cooperated nodes. In WSN, this is a frequent way for the conflict to attack some nodes to interrupt, tamper with/leave valued packages. To find the Compromised Nodes (CNs), we can hire a reputation system. This article shows the regions which cover the dense set of CNs named Compromised Regions (CRs) and obviously it is a major threat to networks as compared to only CNs. For preventing the attacks of CRs, we plan an Enhanced Secure Shortest Path Routing Algorithm (ESPRA) to carry bundles correctly everywhere, instead of CRs. As previous works have used K-means and DBSCAN algorithm for selection of cluster head but failed to opt optimal cluster head. Therefore, we have proposed a fuzzy C-means clustering to split the sensor hubs to prolong network lifetime along with optimal cluster head and QuickHull algorithm to construct convex hull for each cluster. Simulation outcomes demonstrate that ESPRA could always discover the short routing pathways, whereas assuring the packages safety and improving the accuracy.

Keywords WSN · Secure routing · Compromised regions · Energy efficiency · Enhanced secure shortest path routing algorithm

R. Kumar (✉) · S. Tripathi
Department of Computer Science & Engineering, Indian Institute of Technology (Indian School of Mines) Dhanbad, Dhanbad 826004, Jharkhand, India
e-mail: ranjit_kumaruitbu@yahoo.co.in

S. Tripathi
e-mail: var_1285@yahoo.com

R. Agrawal
Department of Computer Science and Engineering, GL Bajaj Institute of Technology & Management, Greater Noida 201301, India
e-mail: rajkecd@gmail.com

S. K. Das et al. (eds.), *Design Frameworks for Wireless Networks*,
Lecture Notes in Networks and Systems 82,
https://doi.org/10.1007/978-981-13-9574-1_17

1 Introduction

Wireless Sensor Network (WSN) establishes an auspicious technique, which allows simple collection and physical data treatment from the atmosphere. Integrated into extensive networks, to the physical world in a simple and dependable method, they provide the connectivity. For several applications they offer attractive resolutions, with sensitive tasks like monitoring of wild animal, target tracking, military surveillance and detection of forest fire and security of industry [1–6]. Inside these networks, sensor nodes are installed in a possibly antagonistic atmosphere wherever in a one-hop/multi-hop method the data is carried out to the sink node [7–9]. Through satellites/internet, collectively data is dispatched via sink node to the remote server and is thus in danger of several kinds of attacks [10]. The most important challenging issues regarding security in WSN is node compromising. The attacks of node capture shows to excerpt the cryptographic vagueness where the opponent attempts to physically tamper with a node. On the basis of network's security architecture, this attack can be very damaging. Apart from this, it can lead to several succeeding influential inner attacks [11]. There are 2-key mechanisms to evade this significant threat. First and foremost is tamper-resistant mechanisms and second one is surveillance-based approach. The tamper-resistant mechanism consists of improving the tampering resistance of the nodes which improves the attacker's efforts. However, the tamper-resistant mechanism is expensive to the trivial sensor nodes and therefore on those tools this does not exist generally. Second, another option usually accepts the surveillance-based method in the network level, that attempts to find measures connected to the node negotiation. Node seizure will incite some noteworthy measures, like a connectivity loss, dislocation/node elimination, a penalty of the node internal state, etc. [11]. Releasing of nodes is noticeable because they could guard low-price sensor tools susceptible to attacks physically by node capture attack. For example, the method implemented in [12–15] such as rescue, wherever a captured node is recognized on the basis of discovery of a distrustful performance and the alteration of its software code, correspondingly.

This article shows Compromised Nodes (CNs) could be recognized through the deployed reputation systems in the networks [16–20]. The main concept of these plans is to recognize the CNs through analysing their unusual behaviours. In order to distribute the packages logically, we have proposed Enhanced Shortest Path Routing Algorithm called ESPRA to overwhelm the Compromised Regions (CRs) through an adequate increase in consumption of the energy. The nodes detected by reputation threshold are separated in the clusters by utilizing fuzzy C-means clustering process [21] for optimal clustering of nodes. The Fuzzy C-means clustering basically associates to each node a corresponding membership value to each cluster number which have to be formed. The clusters are formed according to the highest degree of belongingness (also known as degree of relationship) to a particular cluster number. After the clusters are formed, the cluster heads are chosen based on the maximum residual energy node among the cluster members and also its proximity to corresponding cluster center. The cluster heads further communicate the data collected

through the cluster member sensor nodes to the base station. Also, convex hull of each cluster is constructed using QuickHull algorithm as QuickHull uses less space than most of the randomized incremental algorithms and runs faster for distributions with non-extreme points. Each Compromised Region (CR) is spoken to through a curved polygon that covers a lot of wary hubs. In the article, the sensor hubs on the vertices of the curved polygons are thought to be replicable and this is down to earth thinking about that the polygons' size may be somewhat augmented to certify the unwavering quality of the vertices once constructing these polygons. Finally, the data of CRs is periodically refreshed through the sink hub and only the gradual data of CRs, i.e. the altered data of CRs, is communicated in the entire system to the spare vitality.

The remains sections are described as follows. Phase 2 offers some explanation of the associated performance, Phase 3 explains the implemented work and Phase 4 defines the presentation assessment and outcomes of the implemented methodology. At the end, Phase 5 completes the chapter.

2 Related Work

Routing algorithm is very significant in WSNs and they are the basis of the entire network. As a result, in the literature several routing algorithms are implemented. In WSNs the very extensively utilized routing algorithm is the LEACH algorithm [22], in which whole cluster heads have been chosen in a completely disseminated way. In their own time slots, the affiliates in the cluster deliver their cluster head packages and the cluster heads connect by the sink node directly. In [23], alternative routing algorithm which is based on cluster called HEED is introduced. The cluster heads are chosen sporadically and a subordinate parameter which is permitting to a hybrid of residual energy like node nearness to its node degree/neighbours. In [24] for connectivity of the cluster heads a well effective condition is given. Few processes are constructed to the one-layer networks apart from for cluster-based routing algorithms. The nodes should always be selected as the next node subsequent to the sink node as per the succeeding hop each time viable inside the greedy mode of GPSR [25]. If it miscarries the greedy pattern, then convalesces the face mode and assurances that package is continually send to a node anywhere Greedy mode could be used again. Of course, if the end point node is not linked with the network, then to the Greedy mode, Face mode will not reoccur and will be lost in the end. In order to prevent the coverage fleabags, another way of face routing [26, 27] is planned through employing comparative coordinate systems, evading planarizing networks and preservative the road quality's optimality. In [28], the researcher pays attention over the WSNs of the 1-dimensional and offers the opportunistic algorithm to confirm the minimum rate of the energy throughout the data relay and to defend nodes by comparative minimum residual energy. Alternative typical routing algorithms are guided propagation [29] in which a ready stage is wanted to build the inclinations of whole nodes to the sink node. Inside the direction with the maximum gradient,

the packages are sent always. To protect against black holes, the Active Trust [30] is planned, in that routes detection groups are designed dynamically which is used to find the node trust. Though, this can't be employed directly to protect the CRs, given that this algorithm can't find the nodes being entered. For duty-cycled WSNs, the opportunistic routing algorithm called ORR [31] has been implemented in that forwarding rate and residual energy both are occupied in the consideration at the method of selection of the succeeding hop. Consequently, the ORR could detect continually a better stability between package delays and consumption of energy. For our information, the most current routing algorithms are planned to prevent the ingesting of energy, stability of load and packages delay time and some of them are directly planned to protect the threat model conferred in this article can be done.

3 Proposed Work

3.1 Network Model

First, we suppose that a stationary 2-D n/w is made of laid off SN and every single knob is proficient to performing the transmission of the data, computational processes and storage. All sensor nodes (SNs) are homogeneous and similar communication variety is R_c. In another way, one couple of nodes may communicate at once with every other if and best if their distance isn't bigger than R_c. Sink node is considered tougher than sensor nodes and has enough energy. It is believed that GPS devices/other appropriate etiquette [32] are able to accurately detect themselves. Seemingly, every single node can simply find its neighbours' positions by basic communication performance. After the formation, the node of the sink first transmit their position in the network to entire nodes and could get position of the sink node in each node period. Initially, we believe that entire nodes are dependable and later reputation system is appropriately built. It is advisable to consider that the set of nodes for adverse condition is compromised for a great deal of time.

3.2 Reputation System in WSN

To prevent the inadequacies of cryptography-based WSNs, the idea of reputation created from sociology can be utilized. In the literature [33, 34] numerous reputation systems have been introduced. In this article, we pay attention over beta reputation system [35], in that reputation R_{ij} is calculated through node of the sensor N_i utilizing previous works of beta density function of sensor node N_j's.

For instance, node of the sensor N_i sums numeral of good and bad movements of N_j as r_{ij} and s_{ji}. At that time, N_i records the reputation R_{ij} around node N_j as

$$R_{ij} = Beta(p|r_{ij} + 1; s_{ij} + 1),$$

and the trust

$$T_{ij} = E\left(R_{ij}\right) = \frac{r_{ij} + 1}{r_{ij} + s_{ij} + 2},$$

Wherever, *Beta* denotes the Beta distribution that could be shown through gamma function Γ as

$$Beta\left(p|r_{ij} + 1, s_{ij} + 1\right) = \frac{\Gamma\left(r_{ij} + s_{ij} + 2\right)}{\Gamma\left(r_{ij} + 1\right)\Gamma\left(s_{ij} + 1\right)} p^{r_{ij}}(1 - p)^{s_{ij}} \quad (1)$$

Wherever $0 \leq \mathrm{p} \leq 1$, $r_{ij}, s_{ij} \geq 0$. By the neighbours avg. trust value, we could assess the SN dependability and the smallest trust value nodes from T are known as CNs. Apart from this, constructed on the CNs, we could build CRs in network and in end, ESPRA could hired to protect in contrary to the CRs.

3.3 Enhanced Secure Shortest Path Routing with CRs

Specifically, ESPRA could be alienated in the three stages as algorithms:

- The shortest geometric path evaluation.
- Determining virtual locations.
- Between the agent nodes the packages are delivered.

Before continuing to the diverse periods of ESPRA, let us develop the CR. The accompanying flowchart is introduced in Fig. 1. It very well may be observed that notorieties of the hubs are first determined dependent on the notoriety framework and every hub has a notoriety list pretty much every one of the neighbours. At that point, every hub delivers the notorieties for the sink hub every so often and consequently whole notoriety records are gathered through sink hub to compute the normal notoriety of the hubs in the system. For spare vitality, just the altered notorieties are conveyed and sink hub utilizes chronicled information for the hubs with unaltered reputations. At that point, the suspicious hubs can be identified by a notoriety edge and they can be partitioned into bunches by appropriate grouping algorithms dependent on their areas.

In this article, we are utilizing Fuzzy C- means clustering technique [21] to separate the sensor hub into bunches. The likenesses between the suspicious hubs are characterized as the Euclidean separation. In the addition, the raised frame to each group is built through the QuickHull Algorithm [35] and they are CRs. Each CR is spoken to through a curved polygon that covers a lot of wary hubs. In the article, the sensor hubs on the vertexes of the curved polygons are thought to be replicable and this is down to earth thinking about that the polygons' size may be somewhat

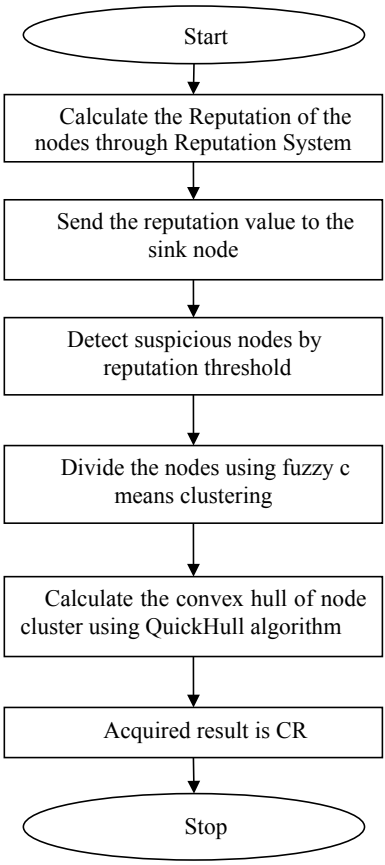


Fig. 1 Flowchart to construct CR

augmented to certify the unwavering quality of the vertexes once constructing these polygons. Finally, the data of CRs is periodically refreshed through the sink hub and only the gradual data of CRs, i.e. the altered data of CRs, is communicated in the entire system to the spare vitality. Steps for constructing convex hull using QuickHull algorithm are as follows:

1. Discover the focuses with least and greatest x arranges. These will dependably be a piece of the raised frame.
2. The line framed by these focuses partition the rest of the focuses into two subsets, which will be prepared recursively.
3. Determine the point, on one side of the line, with the most extreme distance from the line. This point will likewise be a piece of the raised body. The two found before alongside this one structure is a triangle.
4. The focuses lying within that triangle can't be a piece of the arched structure and can in this way be overlooked in the following stages.

5. Rehash the past two stages on the two lines shaped by the triangle (not the underlying line).
6. Stop when no more focuses are left.

STAGE 1: Evaluating the shortest geometric path

Stage1, represent on how to develop the most limited geometric way between source nodes and sink node without intersection of any CRs spoken to by the raised polygons. Truth be told, the geometric way is utilized to direct the transmission of the bundles and it chooses the essential state of the last steering way. Obviously, it frames the vital immoral of SPRA. As appeared in Fig. 2, every CR is spoken to by a polygon and we admit that entirely the apexes of these polygons, the sink hub and the source hub shapes a hub set sensor node. On the off chance that any pair of hubs in sensor node can "watch" one another, we interface an edge amid them which is called as perceptibility edge. Point is, 2 hubs be able to "watch" one another if and just if the edge amid them doesn't cross any piece of the compromised nodes. Entirely the visibility edges make a diagram known as visibility chart. This is clearly demonstrated on most limited geometric way among the source hub and the sink hub must be one way made out of the visibility edges [36–40]. Dijkstra calculation is utilized to locate the briefest way among the source hub and the sink hub.

STAGE 2: Deciding the virtual location

It very well may be seen that few defining moments exist on the geometric way and at every defining moment, the bearing of the way changes with time. In ESPRA, the operator hubs go about as stays to turn the bearings of the steering ways and clearly, approximately every tuning point, a grapple is required. Expect that the geometric way is made out of m line portions, at that point $m - 1$ requested specialist hubs $\{B_1, B_2, \ldots, B_{m-1}\}$ should be chosen around the defining moments.

To guarantee that the bundles don't cross any CR, the specialist hubs ought to be ones a long way from the CRs. Be that as it may, this can build the sizes of steering

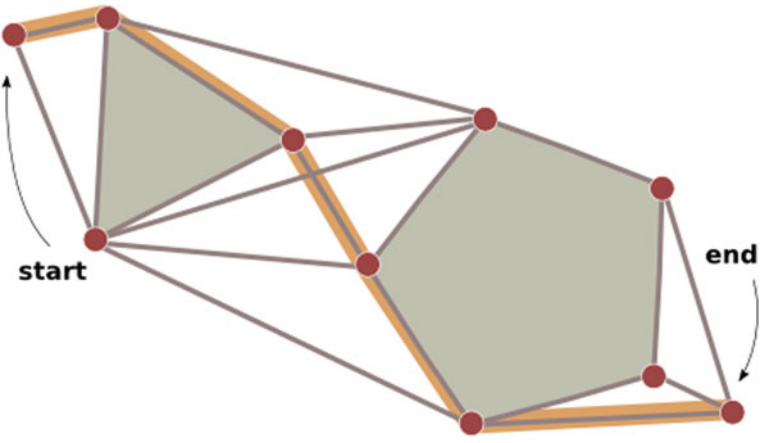


Fig. 2 The shortest geometric path

ways and there is an interchange among safety and productivity. It's illogical to predict a lot of explicit hubs as the specialist hubs, on the grounds that the source hub (SH) doesn't know the whole topology of the network. Luckily, the SH simply desires to choose virtual areas and the operator hubs both are characterized as the closest hubs to these areas. In this work, the virtual areas are picked haphazardly in the virtual circles (VC). To manufacture a virtual hover about a defining moment, we initially figure rakish bisector of the defining moment, and afterward the point $\beta R_c(\beta \geq 0)$ away from the defining moment the other way of the CR is characterized as the focal point of the VC. The range of the VC is characterized as $\gamma R_c(0 \leq \gamma \leq \beta)$ and finally the virtual area is arbitrarily chosen from the VC. For each defining moment, we choose a virtual area similarly and get a lot of requested virtual areas $\{V_1, V_2, \ldots, V_{m-1}\}$. Note that, the SH does not have to know the areas of specialist hubs in the entire directing procedure. Bundle conveyance component is examined in next area.

β and γ are utilized to control the general position of the defining moments and specialist hubs. When we increment β and γ, the security of bundles increments and more vitality is devoured. Despite what might be expected, in the event that we decline β and γ, the security of bundles diminishes and vitality productivity increments. It tends to be seen that there is a trade-off between bundle security and vitality proficiency. Along these lines, the system administrators need to pre-set the parameters as indicated by their necessities. ESPRA picks the specialist hubs in an arbitrary way to different directing ways. This is imperative to adjust remaining tasks at hand of the hubs and improve security of system.

In spite of the fact that it is practically unimaginable that the virtual hover crosses with any CR for legitimate β and γ, if the VC without a doubt covers a piece of any CR, the directing way should be absolutely reconstructed. This is sensible thinking about that the last steering way is probably going to experience a few CRs if the specialist hubs are very near the CNs. For this situation, we can induce that the two CRs must be near one another. To revamp the directing ways, the two contiguous CRs are first thought to be combined and another CR is produced. At that point, another geometric way should be remade dependent on the refreshed polygons. Finally, we rehash the above procedure until a lot of legitimate virtual areas are chosen effectively.

STAGE 3: Delivering packages between the agent nodes (AN)

In this segment, we will talk about how to convey the bundles from the SH to the sink hub dependent on the virtual areas (VA). In particular, upon the m − 1 virtual areas $\{V_1, V_2, \ldots, V_{m-1}\}$ a component to convey the bundles between the specialist hubs $B_1\{B_1, B_1, \ldots, B_{m-1}\}$ should be planned. As discussed already, it is characterized as the closest sensor hub to the VA $V_i(i = 1, 2, \ldots, V_{m-1})$. Presently expect that a bundle is sent from the SH S to the primary operator node B_1. The following jump of the bundle is dependably picked by Greedy mode [25] when conceivable, in which a switch dependably picks the neighbour closest to V_1 as the following bounce. In the interim, the wellspring of the bundle is refreshed to the most recent hub that has gotten the bundle. In the event that no neighbour has a littler separation to V_1 than the switch, Greedy mode falls flat and Face Mode (FM) [27] (i.e. Perimeter

Forwarding in [25]) recuperates. The FM utilizes the "right hand rule" to navigate the polygons in the planar diagram of the network, which is built by the SH in a conveyed way, until finding the goal hub (for this situation, the steering procedure is finished) or an edge E on the chart that crosses the source goal line (neither the SH nor the goal hub situates on E). At that point, at either vertex of the edge E, Greedy mode can be continued. In the event that the FM can't discover the goal hub or the edge E, the directing procedure falls flat. Regardless, it is ensured that the bundle can be constantly transmitted effectively to the hub situated at V_1 or the polygon that covers (V_1 can situate on the edge of the polygon). On the off chance that the FM bombs on a polygon, the closest hub to V_1 on this polygon (i.e. B_1) is only the specialist hub and no other hub in the system can be nearer to V_1. The rightness of this procedure has been broken down and demonstrated in [20]. By this progression, the SH is supplanted by B_1 and V_1 turns into the following goal hub. By repeating the above procedure, the bundle may be conveyed to the sink hub finally. ESPRA may generally discover short steering ways even in extremely complex situations, in light of the fact that the directing ways dependably pursue the briefest geometric way b/w the SH and the sink hub.

ESPRA patterns to choose comparative steering ways and the hubs on the ways dependably go about as the middle hubs. The ESPRA may adjust the remaining burden among each SH via expanding β and γ, however, the scope of β and γ are obliged via appropriation of compromised regions. To additionally recover the decent variety for directing ways, the SH would first be able to build a lot of geometric ways and arrange them dependent on their time-spans. At that point a way is chosen as of the set arbitrarily. When all is said in done, a shorter way ought to be chosen with a higher likelihood. Thus, adjustment in energy weights amid the SH and clearly the length of the steering way increments somewhat. Another test is the means by which to additionally perk up the security of the bundles in the system. The steering ways be built dependent resting on the briefest geometric way and for this situation we generally endeavour to locate the most limited way. Despite the fact that bundles are conveyed in the middle of the CRs instead of through them, it is conceivable that the bundles are caught by the CNs when the street between two CRs is tight. An instinctive methodology is developing the last steering ways dependent on the second or third briefest geometric way in that compromised nodes are dispersive. A going with issue is the means by which to adjust the security of the bundle conveyance and the vitality utilization. A key issue is the means by which to gauge the hazard dependent on top of the dissemination of the CRs and our prospect methodology will explore.

4 Performance Assessment and Result

In our area, we assess the execution of ESPRA. To begin with, the re-enactment setup is introduced in Sect. 4.1. At that point, ESPRA is contrasted with SPRA and dynamic GPSR regarding achievement rate of bundle conveyance, normal bounces

Table 1 Required parameters

S. no	Required statements
1.	MATLAB is utilized as a simulation tool
2.	1000 homogeneous SN are haphazardly positioned in 100 m × 100 m
3.	Initial energy is 5 J
4.	R_c is taken as 7 m
5.	Source node and sink node is at (0, 0) and (100, 100) where sink node is positioned at end side
6.	For every stage, 10 packets of data are conveyed as of the source hub to the sink hub and afterwards another CR is created
7.	Number of CRs increments slowly from 0 to 5
8.	Every CR is made out of 50 CNs and focus (x, y) of every CR is four-sided figure with x ∈ [20, 80] & y ∈ [20, 80]
9.	Length of package is 1024 bits
10.	β *and* γ are chosen from {(0, 0), (2, 1), (4, 2)}
11.	Each simulation is conducted 100 times
12.	Energy consumption is defined as $E_T(l, R_c) = lE_{elec} + l \in R_c^2$, where $E_{elec} = \frac{50\,\text{nJ}}{\text{bit}}$, $\in = 10\,\text{pJ/bit/m}^2$

of steering ways, the measure of information transmission and system lifetime. The reproduction results be introduced and talked about in Sects. 4.2, 4.3, 4.4 and 4.5, individually. Finally, we outline the execution of ESPRA in Sect. 4.6.

4.1 Simulation Setup

Table 1 shows the simulation setup required for our experiment.

4.2 Success Rate of Package Delivery

Here our model utilizes the success rate (SR) of package delivery to gauge the system security with various amounts of compromised regions. It should be kept in mind that the conveyance procedure for a bundle be fizzled suppose the bundle is blocked, altered otherwise fallen. As appeared in Fig. 3, unmistakably the dynamic GPSR and SPRA can't give any insurance on the bundles and the achievement rate altogether diminishes through the expanding of compromised regions. This could be clarified with the way so as a considerable amount bundles are sent to the CNs and subsequently they are altered or dropped. The other three calculations can generally

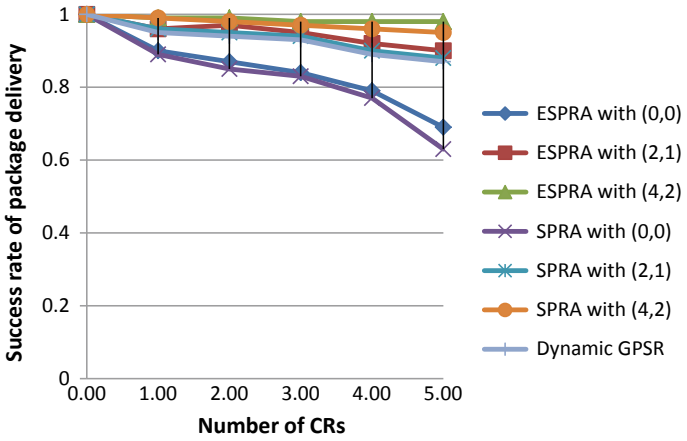


Fig. 3 Success rate of package delivery

give solid insurance and most bundles can be conveyed effectively. This is sensible thinking about that every one of the CRs is considered when planning the directing ways and subsequently the packets aren't broadcasted throughout CRs. By means of expanding the quantity of compromised regions, an ever increasing number of areas in the system are secured by the CNs and it builds the likelihood that the bundles being caught via CNs. In this way, the achievement rate for delivering packets for every one of the plans diminishes with the expanding of quantity of compromised nodes. In addition, the execution of ESPRA is influenced via the parameters β and γ. When values are fixed as β as 0; γ as 0, the achievement rate of ESPRA is a lot inferior than to former powerful calculations, in light of the fact that the operator hubs are excessively near the compromised regions and thus conceivable a few bundles that are delivered to the compromised nodes. Essentially, the bundles in Dynamic GPSR are capable of catching via the compromised nodes now and again. By the way of expanding β and γ, the separations between the specialist hubs and the compromised regions likewise increment and for situation, the likelihood of the bundles being caught via the compromised nodes diminishes. Because of result, the achievement rate of bundle conveyance increments. When values for $\beta = 2$; $\gamma = 1$ or $\beta = 4$; $\gamma = 2$, ESPRA and the SPRA plans have comparable execution as far as progress rate of bundle conveyance (Table 2).

4.3 Average Length of the Routing Paths

Figure 4 shows the average hops of the routing paths which can be observed and stated as the average (avg.) hops of all the algorithms uneventfully increases with the increase in CRs. The reason behind this is that the Compromised Regions chunk the

Table 2 Success rate of package delivery

Number of CR	ESPRA with (0, 0)	ESPRA with (2, 1)	ESPRA with (4, 2)	SPRA with (0, 0)	SPRA with (2, 1)	SPRA with (4, 2)	Dynamic GPSR
0	1	1	1	1	1	1	1
1	0.9	0.96	0.99	0.89	0.96	0.99	0.95
2	0.87	0.97	0.99	0.85	0.95	0.98	0.94
3	0.84	0.95	0.98	0.83	0.94	0.97	0.93
4	0.79	0.92	0.98	0.77	0.9	0.96	0.89
5	0.69	0.9	0.98	0.63	0.88	0.95	0.87

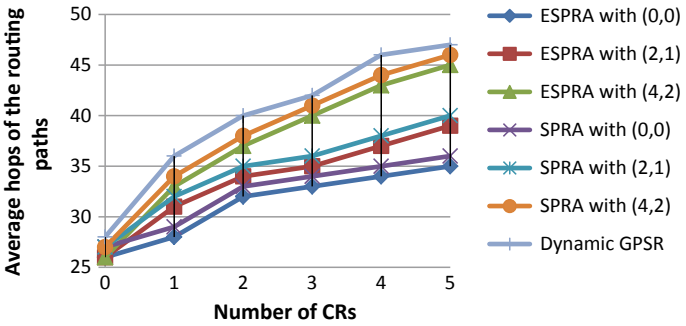


Fig. 4 Avg. hops of the routing paths

routing paths and the data packets which are sent from the source node. ESPRA with $\beta = 0, \gamma = 0$ have similar performance and they achieve much better result than the other methods. One disadvantage of using GPSR is that it get strapped by the local optimums thereafter a quantity of additional hops are essential to conquer it. On the other hand, SPRA and Dynamic DD all the time determine the global optimums and strive in the direction of avoiding the local optimums at the early stage. Nevertheless, the patterns obtained via 2 algorithms are totally different. ESPRA discovers the shortest routing paths by the duration to find the shortest geometric path and it seems that it is an intellectual method; also it considers that the geometric path be able to in the neighbourhood build via the source node. When considering the package safety measures, β and γ also affect the average hops. From Fig. 4, it says that the average hops of ESPRA enhances with the increase in the values of β and γ. So by the above theory, we are capable of summarizing via the information so as to at what time the agent nodes are at a certain distance from the turning points, the geometric paths gets elongated and hence results in the elongation of final routing path (Table 3).

Table 3 Avg. hops of the routing paths

Number of CRs	ESPRA with (0, 0)	ESPRA with (2, 1)	ESPRA with (4, 2)	SPRA with (0, 0)	SPRA with (2, 1)	SPRA with (4, 2)	Dynamic GPSR
0	26	26	26	27	27	27	28
1	28	31	33	29	32	34	36
2	32	34	37	33	35	38	40
3	33	35	40	34	36	41	42
4	34	37	43	35	38	44	46
5	35	39	45	36	40	46	47

4.4 Totality in Transmitting the Data

With the addition of the quantity of CRs, the absolute information transmission measure of the considerable number of methods uninterestingly increments, on the grounds that the ideal directing ways can be blocked by the CRs. As we have discussed in above that despite of short routing path, dynamic GPSR has a maximum of transmitted packages than that of ESPRA. Figure 5 clearly shows the above package. One reason for sure is formerly the topology of a system is modernized and gets efficient; a convoluted fundamental stage should be worked in dynamic GPSR to ensure the unwavering quality of the directing ways. In principle, every one of the hubs need to send no less than one bundle and get a few bundles relying upon the quantity of its neighbors to find the gradient towards the sink node. As a result, a more quantity of additional statistics gets transmitted which gets consumed in the preliminary stage therefore dynamic GPSR results in a deprived dynamics. However, the totality in transmitting the amount of data in Dynamic GPSR is pretty big, as the average hops of the paths are huge. Overall, we can say that ESPRA has a maximum performance

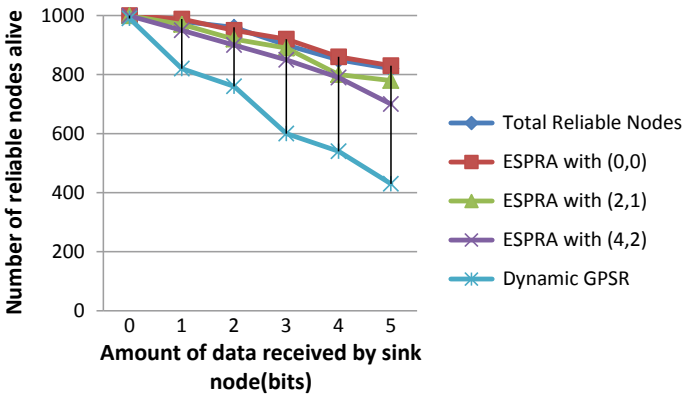


Fig. 5 Number of reliable nodes alive in the network

Table 4 Number of reliable nodes alive in the network

Amount of data received by sink node (bits)	Total Reliable Nodes	ESPRA with (0, 0)	ESPRA with (2, 1)	ESPRA with (4, 2)	Dynamic GPSR
0	1000	1000	999	999	990
1	980	988	970	950	820
2	960	950	920	900	760
3	900	920	890	850	600
4	850	860	800	790	540
5	820	830	780	700	430

with a small β and γ For instance, if we set $\beta = 0$, $\gamma = 0$ or $\beta = 2$, $\gamma = 1$, the amount in sending the data is much smaller than that of other methods. However, it can b observed that with the increase in β and γ, the amount in transmitting the data increases.

4.5 Energy Efficiency of ESPRA

In the end, the total dependable nodes that are alive in the system are utilized for calculating the routing algorithms regarding energy efficiency. Figure 5 shows the totality of live nodes. When we increase the data received by the sink node, the numbers of the reliable nodes (RN) that are alive decreases for the routing algorithms. It is because of the following 2 facts. To begin with, when another compromised node is created, the quantity of RN for every algorithm diminishes by around 50 and it is an extreme alter beneath your suspicion. Next, the quantity of the dependable nodes additionally diminishes via way that a number of nodes come up short on energy as a result of sending and accepting packages. Due to smaller β and γ, ESPRA has an excellent performance thus resulting it as energy efficient. When we change the value of β as 0, γ as 0 or β as 2, γ as 1, our methods perform better than other schemes appreciably. So we can conclude that the 2 dynamic algorithms can assure strong safety to the package security. However, in WSN, ESPRA generally discovers the paths in an energy efficient approach and performs better than other approaches next to the CRs (Table 4).

4.6 Performance Discussion

When analysing the experiment, it can be noticed that the dynamic GPSR cannot give any safety on the package security which is a reason behind avoiding the CNs.

ESPRA can give solid assurance to safeguard alongside the CRs and evidently a number of additional energy is devoured contrasted by static algorithms. These avg. hops of the routing ways produced by ESPRA are comparative among the smaller than that of the dynamic GPSR. In principle, ESPRA plays out the best regarding energy efficiency and incredibly extend the network existence. The overall thing is able to clarify with the way so as to ESPRA be capable of executing in a completely dispersed way and the created routing paths be of smaller lengths.

Also, another thing for noticing from the experimental result is that parameters β and γ have extraordinary effect on the execution of ESPRA. It can also be observed that while increasing β and γ there is an improvement in network security as these two values evade the packages from being attacked via compromised nodes. In interim, it likewise increments the avg. hops of the routing paths, quantity of information transmitted and energy consumption of the networks. As a result, compensation from the network reliability and the energy efficiency of the n/w is present. Auspiciously, when $\beta = 2$ and $\gamma = 1$, ESPRA outperforms the greatest regarding both the reliability and energy efficiency. Overall, ESPRA at all time discovers the shortest routing paths as well as provide safety measures in securing the packages resulting better performance than others.

5 Conclusion

This chapter has proposed an enhanced secure shortest path routing algorithm called ESPRA to preserve against the Compromised Regions in WSNs. The Compromised Nodes that are recognized by the reputation system where fuzzy C-means clustering is used for dividing the clusters and the also we have constructed CRs which are based on the convex hulls structure, i.e. QuickHull algorithm. After that, a geometric shortest path is evaluated so that many turning points can be naturally selected on the path. The selection of the agent nodes is very complex method. In the end, the data packets are delivered from the agent nodes in a relay way throughout a complicated means so that it could not be reached by the opponents. Despite the fact that ESPRA is worked absolutely in an appropriated way, the source node may adaptably switch the states of the routing ways by utilizing a few agent nodes. Simulations results demonstrate that ESPRA at all times discover the secure shortest routing paths and prove energy efficient because clustering prolong the network lifetime. Future work would like to include some equilibrium among the security of the data packet and consumption of energy. Also there should be an extra work for analysing and reducing the loss of energy in constructing the CRs in different situations.

References

1. Gerrigagoitia, K., & Uribeetxeberria, R. (2014). Reputation-based intrusion detection system for wireless sensor networks. In *Complexity in engineering* (pp. 1–5).
2. Das, S. K., Yadav, A. K., & Tripathi, S. (2017). IE2M: Design of intellectual energy efficient multicast routing protocol for ad-hoc network. *Peer-to-Peer Networking and Applications, 10*(3), 670–687. https://doi.org/10.1007/s12083-016-0532-6.
3. Fu, J. S., & Liu, Y. (2015). Double cluster heads model for secure and accurate data fusion in wireless sensor networks. *Sensors, 15*(1), 2021–2040.
4. Niculescu, D., & Nath, B. (2003). Trajectory based forwarding and its applications. In *Proceedings of the 9th Annual International Conference on Mobile Computing and Networking* (pp. 260–272). ACM.
5. Yadav, A. K., Das, S. K., & Tripathi, S. (2017). EFMMRP: Design of efficient fuzzy based multi-constraint multicast routing protocol for wireless ad-hoc network. *Computer Networks, 118,* 15–23.
6. Das, S. K., & Tripathi, S. (2018). Intelligent energy-aware efficient routing for MANET. *Wireless Networks, 24*(4), 1139–1159. https://doi.org/10.1007/s11276-016-1388-7 (Springer).
7. Das, S. K., & Tripathi, S. (2019). Energy efficient routing formation algorithm for hybrid ad-hoc network: A geometric programming approach. *Peer-to-Peer Networking and Applications, 12*(1), 102–128. https://doi.org/10.1007/s12083-018-0643-3 (Springer).
8. Das, S. K., & Tripathi, S. (2018). Adaptive and intelligent energy efficient routing for transparent heterogeneous ad-hoc network by fusion of game theory and linear programming. *Applied Intelligence, 48*(7), 1825–1845. https://doi.org/10.1007/s10489-017-1061-6.
9. Das, S. K., & Tripathi, S. (2017). Energy efficient routing formation technique for hybrid ad hoc network using fusion of artificial intelligence techniques. *International Journal of Communication Systems, 30*(16). https://doi.org/10.1002/dac.3340.
10. Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in wireless sensor networks. *ACM Communication, 47*(6), 53–57.
11. Krauß, C., Schneider, M., & Eckert, C. (2008). On handling insider attacks in wireless sensor networks. *Information Security Technical Report, 13*(3), 165–172.
12. Khalil, I., Bagchi, S., & Nina-Rotaru, C. (2005). DICAS: Detection, diagnosis and isolation of control attacks in sensor networks. In *1st International Conference on Security and Privacy for Emerging Areas in Communications Networks, SECURECOMM*.
13. Conti, M., Pietro, R. D., Mancini, L. V., & Mei, A. (2008). Emergent properties: Detection of the node-capture attack in mobile wireless sensor networks. In *WiSec 2008: 1st Conference on Wireless Network Security* (pp. 214–219). New York: ACM.
14. Seshadri, A., Perrig, A., Van Doorn, L., & Khosla, P. (2004). SWATT: Software-based attestation for embedded devices. In *Proceedings of the IEEE Symposium on Security and Privacy*.
15. Krauß, C., Stumpf, F., & Eckert, C. M. (2007). Detecting node compromise in hybrid WSN using attestation techniques. In F. Stajano, C. Meadows, S. Capkun, & T. Moore (Eds.), *ESAS 2007* (Vol. 4572, pp. 203–217)., LNCS Heidelberg: Springer.
16. Karp, B., & Kung, H. T. (2000). GPSR: Greedy perimeter stateless routing for wireless networks. In *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking* (pp. 243–254). ACM.
17. Intanagonwiwat, C., Govindan, R., & Estrin, D. (2000). Directed diffusion: A scalable and robust communication paradigm for sensor networks. In *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking* (pp. 56–67). ACM.
18. Heinzelman, W. B., & Chandrakasan, A. P. (2002). An application-specific protocol architecture for wireless microsensor networks. *IEEE Transactions on Wireless Communications, 1*(4), 660–670.
19. Johnson, D., Hu, Y., & Maltz, D. (2007). The dynamic source routing protocol for mobile ad hoc networks for IPv4, No. RFC (p. 4728).

20. Zhang, D., Li, G., et al. (2014). An energy-balanced routing method based on forward-aware factor for wireless sensor networks. *IEEE Transactions on Industrial Informatics, 10*(1), 766–773.
21. Su, S., & Zhao, S. (2018). An optimal clustering mechanism based on Fuzzy-C means for wireless sensor networks. ScienceDirect.
22. So, J., & Byun, H. (2017). Load-balanced opportunistic routing for duty-cycled wireless sensor networks. *IEEE Transactions on Mobile Computing, 16*(7), 1940–1955.
23. Ester, M., Kriegel, H. P., Sander, J., et al. (1996). A density-based algorithm for discovering clusters in large spatial databases with noise. In *International Conference on Knowledge Discovery and Data Mining* (pp. 226–231).
24. Huang, H., Yin, H., Min, G., et al. (2017). Coordinate-assisted routing approach to bypass routing holes in wireless sensor networks. *IEEE Communications Magazine, 55*(7), 180–185.
25. Graham, R. L. (1972). An efficient algorithm for determining the convex hull of a finite planar set. *Information Processing Letters, 1*(4), 132–133.
26. Luo, J., Hu, J., Wu, D., et al. (2017). Opportunistic routing algorithm for relay node selection in wireless sensor networks. *IEEE Transactions on Industrial Informatics, 11*(1), 112–121.
27. Liu, Y., Dong, M., Ota, K., et al. (2017). ActiveTrust: Secure and trustable routing in wireless sensor networks. *IEEE Transactions on Information Forensics and Security, 11*(9), 2013–2027.
28. Zhu, C., & Nicanfar, H. (2015). An authenticated trust and reputation calculation and management system for cloud and sensor networks integration. *IEEE Transactions on Information Forensics and Security, 10*(1), 118–131.
29. Berg, M. D., et al. (2000) Computational geometry. In *Computational geometry* (pp. 1–17).
30. Ganeriwal, S., Balzano, L. K., & Srivastava, M. B. (2008). Reputation-based framework for high integrity sensor networks. *ACM Transactions on Sensor Networks, 4*(3), 15.
31. Kuila, P., & Jana, P. K. (2014). Energy efficient clustering and routing algorithms for wireless sensor networks: Particle swarm optimization approach. *Engineering Applications of Artificial Intelligence, 33,* 127–140.
32. Arora, A., Dutta, P., et al. (2004). A line in the sand: A wireless sensor network for target detection, classification, and tracking. *Computer Networks, 46*(5), 605–634.
33. Ozdemir, S. (2008). Functional reputation based data aggregation for wireless sensor networks. In *Proceedings of the WIMOB'08, IEEE International Conference on Wireless and Mobile Computing Networking and Communications* (pp. 592–597).
34. Fang, W., et al. (2015). *BTRES: Beta-based trust and reputation evaluation system for wireless sensor networks*. Elsevier Ltd. ISSN: 1084-8045.
35. Barber, C. B., Dobkin, D. P., & Huhdanpaa, H. (1996). The quickhull algorithm for convex hulls. *ACM Trans Math Software (TOMS), 22*(4), 469–483.
36. Yang, S. L., Li, Y. S., Hu, X. X., et al. (2006). Optimization study on k value of Kmeans algorithm. *Systems Engineering-Theory and Practice, 26*(2), 97–101.
37. Binh, H. T. T., & Dey, N. (Eds.). (2018). *Soft computing in wireless sensor networks*. CRC Press.
38. Fong, S., Li, J., Song, W., Tian, Y., Wong, R. K., & Dey, N. (2018). Predicting unusual energy consumption events from smart home sensor network by data stream mining with misclassified recall. *Journal of Ambient Intelligence and Humanized Computing*, 1–25.
39. Chowdhuri, S., Chaudhuri, S. S., Banerjee, P., Dey, N., Mandal, A., & Santhil, V. (2016). Secure minimum loss route selection of MIMO-based MANET in combined (indoor, outdoor, and forest) terrain (pp. 1–26). Working paper, International Journal Advanced Intelligence Paradigms.
40. Dey, N., & Mukherjee, A. (2018). *Embedded systems and robotics with open source tools*. CRC Press.

Fuzzy Petri Nets-Based Intelligent Routing Protocol for Ad Hoc Network

Asish Samantra, Abhijit Panda, Santosh Kumar Das and Sourabh Debnath

Abstract Ad hoc network is a collection of devices with wireless communications. The issue in this network is energy conservation that is equipped with limited batteries, scalability, low-quality communication, and resource-constrained computation that defines limited amount of network bandwidth. To minimize this uncertainty problem in the network, a soft computing technique is used, i.e., Fuzzy Petri Net. The proposed method consists of two phases such as evaluation of fuzzy cost and route selection. The first phase evaluates fuzzy cost of node and link using fuzzy logic. The second phase is used to evaluate the optimal route with the help of FPN model. The proposed method is simulated in Python in terms of some network resources and validate different feasible paths of the network.

Keywords Ad hoc network · Petri nets · Fuzzy logic · Routing protocol · Membership function

1 Introduction

Mobile Ad hoc Network (MANET) [1, 2] is a unique case of mobile networks, where no fixed links were present to carry out communication between each node. It violates the single-hop cellular network model, which carries out wireless communication from the access point with different Base Stations (BS). Communication between nodes in cellular network totally depends on fixed Base Stations and the

A. Samantra · A. Panda · S. K. Das (✉) · S. Debnath
School of Computer Science and Engineering, National Institute of Science and Technology (Autonomous), Institute Park, Pallur Hills, Berhampur 761008, Odisha, India
e-mail: sunsantosh2014@gmail.com

A. Samantra
e-mail: asishsamantra7@gmail.com

A. Panda
e-mail: abhijitpanda172@gmail.com

S. Debnath
e-mail: dsourabh@nist.edu

S. K. Das et al. (eds.), *Design Frameworks for Wireless Networks*,
Lecture Notes in Networks and Systems 82,
https://doi.org/10.1007/978-981-13-9574-1_18

wired backbone. However, in MANET, each node acts as a router and takes the full responsibility to share the information with the destinations [3, 4]. Due to the mobility nature of nodes, the network topology changes repeatedly and randomly. In wireless communication, as the bandwidth is less as compared to wired architecture, the routing technique in MANET is a challenging task and an active research area [5, 6]. In the past few years, various algorithms for routing techniques have been proposed in MANET, maximum algorithms were based on hop routing apart from selecting a reliable path during route selection process [7–9].

There are many applications of MANETs. Many day to day applications such as electronic mail and file transfer can be considered that are very efficient in deploying in ad hoc network [10–12]. Initially, this technology is developed mainly for military applications and places where human intervention is unreachable for establishing or maintaining infrastructure-based network. In certain situations where other technologies failed to deploy, these self-organizing ad hoc networks are efficiently used. To broadcast and distribute information among members, this ad hoc network can create an immediate link between multimedia network using computers such as conferences [13–15]. Bluetooth facilitates communication within a short range between communicating nodes such as mobile phones, laptops, etc.

In ad hoc network, the network topology changes unpredictably, hence routing is the most challenging task. The network topology behaves as a router for sending and receiving data packets as each node are equipped with limited battery power [16]. If a node failure occurs due to energy loss, then the entire network topology may alter. Any malicious node may be interfere during transmission and affect the communication. In this type of network, nodes are free to move while transmitting the data. So, a node may go out of the range. Similarly, length of path plays an important role in considering route determination, whereas a larger delay in communication is offered by longer paths. Path that contains more number of nodes needs extra resources of in-between nodes for data communication.

To overcome these issue, an intelligent protocol for routing is proposed for ad hoc network which can able to discovery an optimal route between the source and destination by considering different factors like node battery power, node mobility, path length, etc. which helps to increase the network lifetime and finds an optimal path for communication.

2 Related Works

In recent years, several routing algorithms are proposed for MANET such as optimized link state routing protocol, destination sequenced distance vector, and dynamic source routing belong to shortest-path routing protocols [17].

In [18], a fuzzy primarily based intelligent routing algorithm was established to find out the packet loss, best parameters, membership functions, and repairing of path broken. In this work, responsibility inclusion is not considered. In most of the

cases, network performance depends on the responsibility of link similarly as nodes. Link property is properly not maintained during this routing protocol.

Singh et al. [19] has proposed an algorithm named as AODV-Reliability (AODV-R). It's a routing protocol based on Ant Colony Optimization (ACO) for clustering purpose and to remove congestions as well as to search for the shortest path. The proposed algorithm uses ACO concept in order to increase the selection process for finding the shortest route [20]. This algorithm decides and selects the path which is the most reliable and minimizes the probability of link failure during network topology shuffling. However, it does not fulfill the requirements of QoS routing.

Das et al. [21] proposed a routing protocol for multicast ad hoc network in order to create an energy effective path from origin to every multicast set built on two vague parameters such as distance and energy. Whereas, other parameters were not been considered by this proposed work which leads to its limitation. Hence, Yadav et al. [22] stretched the effort placed on multi constraints method. They have considered three parameters that are delay, bandwidth, and energy. It supports to elect the best route with the help of fuzzy cost. Here, two limitations occurred as it is a point-based membership function and fails to hold the fuzziness information. Henceforth, Das and Tripathi [23] proposed an energy conscious-based routing protocol by considering five parameters such as distance, energy, delay, packets, and hop count. The objective of this routing is to search for an optimal route by considering multi-criteria decision-making and intuitionistic fuzzy soft set. As it doesn't use any optimization method, it leads to its limitation. So, by using the above techniques, several contradictory objectives may not be optimized. Das and Tripathi [24] brought up a routing technique based on nonlinear optimization technique. This nonlinear optimization technique is based on geometric programming which works with polynomial environment instead of polynomial environment. It helps to determine nonlinear parameters efficiently and enhance the network lifetime.

In MANET, each node is equipped with inadequate energy and works in an unsupervised mode. Hence, improvement for this network is done by considering energy-efficient multicast routing protocols. Several energy efficient algorithms for multicast has utilized for the appropriate utilization of available resources of the network. The algorithms which follow this technique are an Improved Ant Colony-based Multi-constrained Quality of Service Energy-saving Routing protocol (IAMQER) and algorithm for an efficient routing protocol for multicast based on network coding [25].

Abdel et al. [26] propose an algorithm called as Multi-Route Ad hoc On-Demand Distance Vector (AODV) Ant Routing Algorithm (MRAA). Here, AODV uses to discover routes in reactive manner, i.e., on-demand, whereas ACO discovers route proactively, i.e., not in on-demand basis. This algorithm minimizes the end-to-end interruption through the transmission of the data between the different nodes. In this type of technique, alternative paths have been chosen for data delivery of packets from source to destination with less overhead. As it keeps tracking, the route along with it stores and maintains the backup routes, which are an overhead for the algorithm.

Dhurandher et al. [27] have intended for a well-organized peer-to-peer searching of files in Mobile Ad hoc Network (MANETs), hence proposed an algorithm as Peer-to-Peer Bee Algorithm (P2PBA). This scheme uses the foraging behavior of

honey bees which was a part of swarm intelligence. Here, a file is divided into the form of packets and distributed on selected routes. It doesn't consider parameters such as heterogeneity of node, security, and energy consumption.

Rao et al. [28] have proposed a protocol for routing that has nth backup route in AODV (AODV nth BR). Here, an additional or more backup route is provided to the source node in case any breakout occurs in the network link. It is the improved version of AODV protocol for delivering packets from source to destination having more than one route. Node distance and nodes residual energy are used for selecting a node for routing. In this algorithm, each node is verified or examined with its transmission energy as well as next nearest node is selected using distance vector, if it has sufficient energy for transmission it will again search for the nearest node. It will continue till and until the appropriate node is selected for transmission.

Misra et al. [29] proposed a protocol for routing named as Bird Flight-Inspired Routing Protocol (BFIRP) by considering position and energy. Here, they have considered node energy as well as distance factor for sending data packets from source to destination. It also considers the degree of node closeness that connects the destination nodes with the intermediate nodes. Its main limitation is bandwidth consumption.

A DUCR algorithm for wireless sensor networks was discussed by Mazumdar et al. [30]. This mechanism resolves the hot spot problem. To balance the receiving nodes, DUCR algorithm uses a well-organized approach to distribute the information to its parent nodes. It is scattered in nature and facilitates the preferred performance of energy consumption, alive nodes, and lifetime of network. This algorithm is also stationary in nature; it doesn't have the property of mobility which may increase the network performance.

Mazumdar et al. [31] proposed a distributed fuzzy logic-based energy-aware and coverage safeguarding uneven clustering algorithm (DECUC) for wireless sensor networks. While addressing the problems in wireless sensor networks, it intends to create a transition between coverage parameters and energy competence. It uses a fuzzy logic concept by taking parameters such as distance from base station, enduring energy, and CS of a node for electing cluster heads and cluster radii. This algorithm is distributed in nature and facilitates better conduct in coverage preservation, network's lifetime, and energy efficiency. This algorithm is also stationary in nature; it doesn't have the property of mobility, which may increase the network performance.

The directional sensor models used in the coverage of ROI was proposed by Chaya et al. [32]. The probability estimation method is used to calculate the threshold value. This was elaborated to directional sensor ratio with respect to omnidirectional sensors. The LP formulation for boosting the coverage area was provided. Fixed count in the number of sensors, different orientation ways were implied and the future objective was to achieve the coordinated value of sensors in ROI.

The key research work of CLDs was proposed by Sah et al. [33]. It played an important aspect in the past in context to wireless sensor networks [34]. Irrespective of layer's collaboration, the focus was on minimizing the transference and collecting power, end-to-end delivery improvement, reduction of control packet overhead, and QoS. Apart from this, very small progress was observed in the area of security.

Incentive-based replication strategy was proposed by Singh et al. [35] to provide an incentive to the participating nodes, so that it doesn't act as selfish node. Community-based mechanism was provided for fair incentive to the nodes to carry packets from origin to target. The proposed strategies evaluated in terms of epidemic, prophet, spray and wait, and MaxProp routing algorithms. This strategy works better than the existing strategies.

Singh et al. [36] say IRS provided a better result of delivery ratio when compared to epidemic and prophet routing algorithms. In IRS, incentive policy for selfish nodes was popularized in socially aware DTNs to sacrifice their selfishness and as per incentive value reputation relay nodes can cooperate in the replication process and earn incentive value for transferring packets.

3 Preliminaries

3.1 Fuzzy Logic

Fuzzy logic is a mathematical tool based on soft computing technique that deals with the data which are encountered in an imprecise manner in a real world like very low, low, medium, high, and very high [37, 38]. It has four components, namely fuzzy rule base, inference engine, fuzzifier, and defuzzifier. In the proposed protocol, three variables of a node are given as input in fuzzy logic system: (1) energy, (2) control packet, and (3) speed and then three variables of link (1) distance, (2) delay, and (3) energy is provided. The proposed protocol converts them into two fuzzy costs. The two fuzzy costs are compared with each other and the corresponding path is found out.

3.1.1 Input Fuzzification

The fuzzification is done twice for the crisp variables of node and link. The inputs in this phase are fuzzified. A set of linguistic terms is normally the partition of linguistic variable. In MANET, the terms Low, Medium, and High can be taken as three linguistic variables to each input variables based on the knowledge base rule.

3.1.2 Membership Function

This function is employed in fuzzification and defuzzification process in the theoretical concepts of fuzzy logic systems in order to plot the crisp input into a fuzzy system and vice versa. This procedure includes the conversion of the crisp input to fuzzy input set by using the abovementioned function. The objective of this function

is to measure a linguistic term, and to perform this, we have employed triangular membership function.

3.1.3 Fuzzy Knowledge-Based Rule

Here, a base rule is generated in order to manage the output variable. Basically a fuzzy rule is a simple "IF THEN" rule that consists of antecedent and consequent statements having operators, i.e., either "AND" or else "OR". Both the operators carry out various linguistic statements. The two operators manage various linguistic declaration where "AND" bargain whether different linguistic explanation is applicable and "OR" operator bargains when no less than one of the linguistic expression were justifiable.

3.2 Petri Nets

A Petri Net (PN) is a bipartite graph, which has two types of nodes named as places and transitions that are characterized by circles and rectangles, respectively. Input arcs are the arcs that connect places with the transition, whereas an output arc connects in reverse order, i.e., from transitions to the places. Weights are nonnegative integers that are connected with an arc. Places represent the state variables whereas the transitions correspond to the actions that induce changes of states.

4 Proposed Work

Ad hoc network consists of several nodes that are communicating with each other. At first, all the node and link properties are carried out and stored. The node properties that we have considered here are energy, control packet, and speed. Then, in the route discovery phase, all nodes find its neighbors those are residing in the communication range of the node. Link establishment among them is occurred. All the available paths from the source to the destination can be found out on the basis of their distance. The stated paths are not trusted for the routing. So, in order to decide the trustable paths, we will be processing those paths to find out the paths that can be more trustable than others by fuzzy Petri net [36].

Fuzzy Petri Net (FPN) is the fusion of fuzzy logic and Petri nets. We are combining the fuzzy model and Petri net model to find out the trustable paths. In this model, at first, the variables are fuzzified and the Fuzzy Cost (FC) values, i.e., the output parameter of the inputs is determined. In second phase, the FC values are processed in the FPN model that we have designed to find out the trustable paths from the source to the destination.

The two phases of our work are as follows:

(1) Evaluation of FC(ϕ1),
(2) Route selection by using FPN.

4.1 Evaluation of FC

At first, a source node will be chosen. The source node finds all the neighbor nodes in its range. After finding the neighbor nodes, for each node, the link variables are considered. The ϕ1 value is calculated for the sending node and the link is established between the sending and receiving node. A linguistic variable is typically divided into a lot of linguistic terms or values. Based on learning base standard of MANET, the terms Low, Medium, and High are the three linguistic variables corresponding to every input variables, i.e., energy, control packet, and speed. Likewise, three linguistic variables will be given as input to each input variable of the link such as energy, distance, delay.

Here, we are using triangular membership function for calculating the membership value of each variable. At first, for each property or variable of the node, the membership value is calculated. Here, we are calculating the membership values of the energy, control packet and speed shown in Tables 1, 2, and 3.

Table 1 Triangular membership function for Energy (E)

Linguistic variables	Notation	Range	Value
Low	E_L	[E_{L-}, E_{L+}]	[0–150]
Medium	E_M	[E_{M-}, E_{M+}]	[120–300]
High	E_H	[E_{H-}, E_{H+}]	[250–500]

Table 2 Triangular membership function for Control packet (C)

Linguistic variables	Notation	Range	Value
Low	C_L	[C_{L-}, C_{L+}]	[0–150]
Medium	C_M	[C_{M-}, C_{M+}]	[120–300]
High	C_H	[C_{H-}, C_{H+}]	[250–500]

Table 3 Triangular membership function for Speed (S)

Linguistic variables	Notation	Range	Value
Low	S_L	[S_{L-}, S_{L+}]	[0–100]
Medium	S_M	[S_{M-}, S_{M+}]	[80–200]
High	S_H	[S_{H-}, S_{H+}]	[150–300]

Here, the node properties, i.e., E, C, and S are the network lifetime increasing factors. After calculating the membership values of these three parameters, i.e., $\mu_E(x)$, $\mu_C(x)$ and $\mu_S(x)$, output parameter, i.e., $\phi 1$ calculated by Eq. 1

$$\phi 1 = \max(\mu_E(x), \mu_C(x), \mu_S(x)) \tag{1}$$

For calculation of membership values of the link variables, we are using the same triangular membership function. Here, the membership function of energy is same as node level and membership functions of distance and delay are defined in Tables 4 and 5.

Here, the link properties energy which is a network lifetime increasing factor, whereas distance and delay are the network lifetime decreasing factors. So, we have to convert the membership values of the distance and delay as Reverse Distance (RDS) and Reverse Delay (RDL) by fuzzy complement shown in Eqs. 2 and 3. After calculating the membership values of the energy, distance, and delay of the link, the fuzzy cost $\phi 2$ shown in Eq. 4.

$$\mu_{RDS}(x) = 1 - \mu_{DS}(x) \tag{2}$$

$$\mu_{RDL}(x) = 1 - \mu_{DL}(x) \tag{3}$$

$$\phi 2 = \max(\mu_E(x), \mu_{RDS}(x), \mu_{RDL}(x)) \tag{4}$$

For each of the nodes in the paths, these values will be calculated. On the basis of these values, the route will be established. These values will be further utilized in the fuzzy Petri net phase for route selection.

Table 4 Triangular membership function for Distance (DS)

Linguistic variables	Notation	Range	Value
Low	DS_L	$[DS_{L-}, DS_{L+}]$	[0–100]
Medium	DS_M	$[DS_{M-}, DS_{M+}]$	[80–200]
High	DS_H	$[DS_{H-}, DS_{H+}]$	[150–300]

Table 5 Triangular membership function for Delay (DL)

Linguistic variables	Notation	Range	Value
Low	DL_L	$[DL_{L-}, DL_{L+}]$	[0–100]
Medium	DL_M	$[DL_{M-}, DL_{M+}]$	[80–200]
High	DL_H	$[DL_{H-}, DL_{H+}]$	[150–300]

4.2 Route Selection by Using FPN

The route selection can be done by using FPNs. All the possible paths from the source to destination are evaluated in route discovery phase. Each possible route can be processed through FPNs and reliable routes are designed. FPNs is the fusion of fuzzy logic and Petri nets [27]. Here, we defined the proposed FPN model with seven elements in Eq. 5.

$$\text{FPN} = (\text{P}, \text{T}, \text{F}_{\text{in}}, \text{F}_{\text{out}}, \text{W}, \text{M}_0, \text{L}) \tag{5}$$

where

$\text{P} = \{\text{P}_1, \text{P}_2, \ldots, \text{P}_n\}$ is a finite set of places, i.e., nodes.
$\text{T} = \{\text{T}_2, \text{T}_2, \ldots, \text{T}_n\}$ is a finite set of transitions where $\text{P} \cup \text{T} = \emptyset$ and $\text{P} \cap \text{T} = \emptyset$.
$\text{F}_{\text{in}} \subseteq (\text{P} \times \text{T})$ is an input matrix that consists of arcs from places to transitions (i.e., input arc).
$\text{F}_{\text{out}} \subseteq (\text{T} \times \text{P})$ is an output matrix that consists of arcs from transitions to places (i.e., output arc).
$\text{W} = (\text{F}_{\text{in}} \cup \text{F}_{\text{out}}) \rightarrow \text{R}$ is a weight function that consists of a set of real numbers.
$\text{M}_0 = \text{P} \rightarrow \text{N}$ is the initial marking.
L = Linguistic variable that makes the elements of Petri nets as fuzzy.

At first, for each route, initial node is selected. When the initial node is selected in the process, the $\phi 1$ value of the node is compared with the $\phi 2$ value. If the $\phi 1$ value of the node is greater or equal to the $\phi 2$ of the link, then transition enables the sending and receiving node and they are ready to fire the tokens from one node to the other node. Figure 1 shows the structure of the FPN which consists of two places as nodes that connected with input and output arcs separated by a transition (T_1). Each node consists of four tokens where three black tokens indicate input parameters E, C, and S. The output parameter of node, i.e., $\phi 1$ indicates by white token.

Figure 2 represents the initial stage of the route selection. Then for each path, the initial node is selected for route selection. All the nodes and transitions are ready for the path selection in this phase. An initial node is selected at first and this process is continued till the destination node is found out or till the link breaks. In Fig. 2, node P1 is the initial node and node P4 is the destination node. P1 wants to send data packets to the destination node P4. Initially, communication happens between two

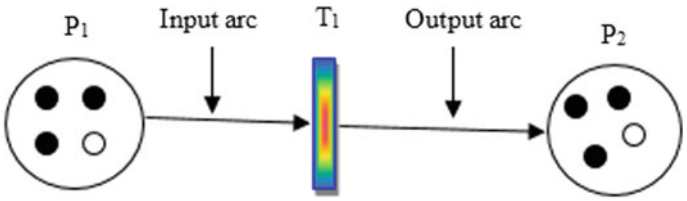


Fig. 1 Structure of the FPN

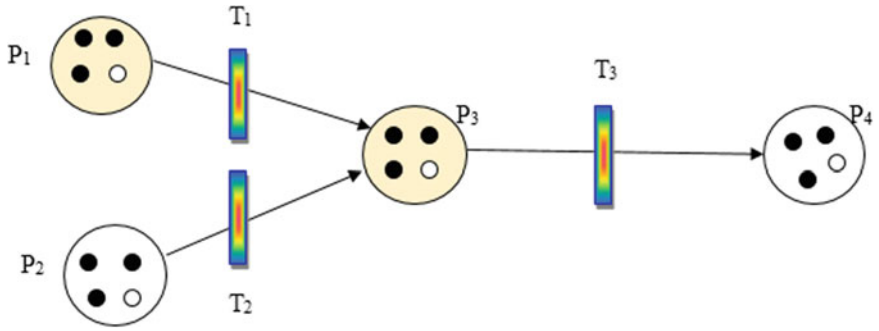


Fig. 2 Initial state of the route selection (i.e., Stage I)

nodes, i.e., P1 and P3. So, these nodes are shaded. The next stage, i.e., Stage II is shown in Fig. 3.

In Fig. 3, $\phi 1$ of P_1 is compared with $\phi 2$ value of the link between P_1 and P_3 in the transition. As $\phi 1$ value of the node P_1 is greater than $\phi 2$ value of the link, the transition enables the node P_1 indicating by green token of $\phi 1$ and transition fire the token from the node P_1 to node P_3 as shown in Fig. 4, i.e., Stage III. Now,

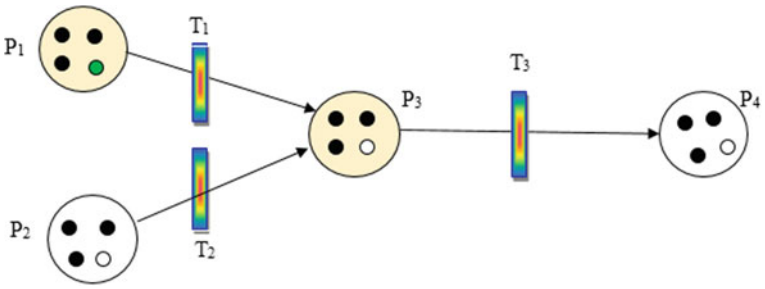


Fig. 3 Stage II of the route selection

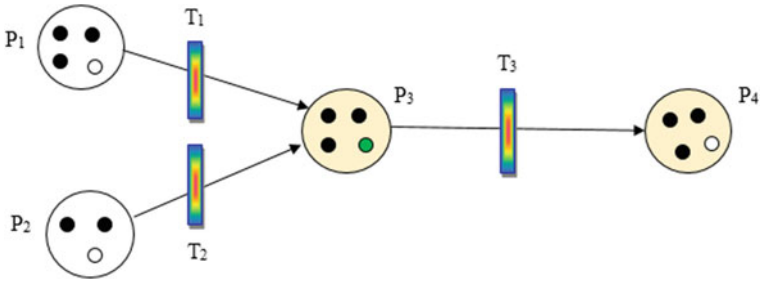


Fig. 4 Stage III of the route selection

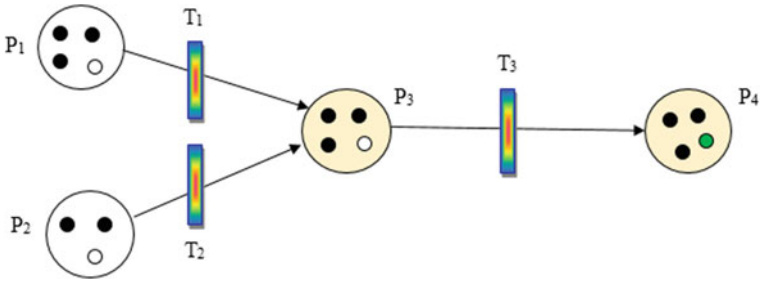


Fig. 5 Stage IV of the route selection

communication happens between nodes P_3 and P_4 and the same process is repeated, which is illustrated between Figs. 4 and 5.

Another node P_2 shown in Fig. 6 is willing to send the data to the destination node P_4. The same process continues in this case also. The $\phi 1$ value of node P_2 and $\phi 2$ value of the link between P_2 and P_3 are compared with the transition T_2. As the condition fails, the transition is not enabled and the firing of the token from the node P_2 to P_3 does not occur. So, the color of main token, i.e., $\phi 1$ of P_2 is red. As the initial link is broken, the process terminates and no further verification is done by using that path.

The green token indicates that the transition has enabled the two nodes and now, node can transfer the tokens to the other node. Here, the red color token indicates that it does not satisfy the condition and the node cannot send data to the other nodes through P_3. In this way, all the paths from the source to the destination node are found out. The proposed algorithm is shown in Algorithm 1, where source node (S) and destination node (D) are the initial input parameters, along with different network parameters are used such as energy, control packet, and mobility (speed) for node properties and energy, distance, and delay for link (edge) properties. Nature of delay and distance are contradictory based on energy, control packet, and speed with respect network lifetime. So, here, reverse distance and reverse delay are calculated.

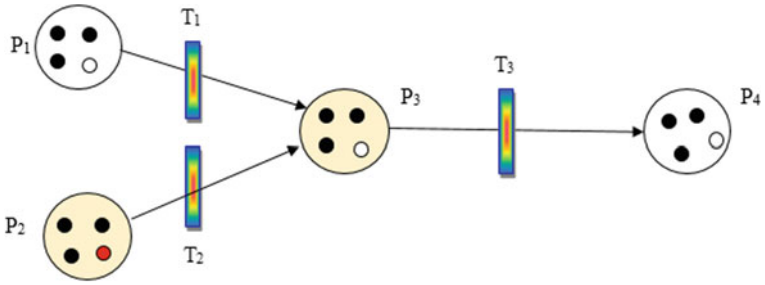


Fig. 6 Stage V of the route selection

All parameters are mapped into FPN model for evaluating feasible as well as optimal path. There are two fuzzy costs are calculated as $\phi 1$ and $\phi 2$ where $\phi 1$ for node and $\phi 2$ for link. Both fuzzy costs are evaluated between place and transition, where node playing the role of place and mediator of link playing the role of transition. Finally, different feasible paths are calculated, and after that, one optimal path is selected for data transmission.

Algorithm 1: Proposed model

Input: Source node (S), and Destination node (D)

Output: An optimal path

Step 1: Start

Step 2: Define FPN = (P, T, F_{in}, F_{out}, W, M_0, L); path_cost=0

Step 3: Select number of nodes

Step 4: Assign the node properties to each node

Step 5: Find each node's neighbour nodes within their range

Step 6: Select Source node (S) and Destination node (D)

Step 7: Select node S with its neighbor as places P_i and P_j

Step 8: Calculate membership values (i.e. $\mu_E(x)$, $\mu_C(x)$ and $\mu_S(x)$) and find $\phi 1$ for Pi

Step 9: Calculate reverse distance and reverse delay (i.e. $\mu_{RDS}(x)$ and $\mu_{RDL}(x)$)

Step 10: Calculate membership values (i.e. $\mu_E(x)$, $\mu_{RDS}(x)$, $\mu_{RDL}(x)$) and find $\phi 2$ for Lj

Step 11: If ($\phi 1 >= \phi 2$), then enable Tk and add Lj in routing table with link properties

Step 12: Increase place as Pi to Pi+1

Step 13: Repeat Step 8 to 12 until Pi=D

Step 14: Find Avg=($\mu_E(x)$, $\mu_{RDS}(x)$, $\mu_{RDL}(x)$) for each route

Step 15: $path_{opt}$=Max(avg_i) where i=1 to n; total path between S to D

Step 16: Stop

5 Performance Evaluation

The proposed work is evaluated in Python programming language. The simulation parameters are shown in Table 6. Figure 7 display scenario of node ID with their properties such as energy, mobility, and control packet. Range of energy is 0–500, range of mobility is 100–400, and range of control packet is 100–200. Dimension of operation is 300 × 300 for x- and y-axis where total nodes is used 12.

Table 6 Simulation parameter

Parameter	Description
Software	Python
Version	3.7.0
Nodes	12
Energy	0–500
Mobility	100–400
Control packet	100–200
X-axis	300
Y-axis	300
Radio range	100

```
Enter no of Nodes: 12
                Node Details
id    Energy   Mobility   Ctrl
=======================================
0       312      372      109      (115, 223)       100
1       32       130      166      (107, 22)        100
2       65       143      110      (107, 92)        100
3       153      343      171      (49, 280)        100
4       55       153      190      (132, 127)       100
5       190      263      164      (155, 89)        100
6       199      141      180      (190, 122)       100
7       168      292      119      (229, 128)       100
8       106      229      125      (69, 103)        100
9       320      146      181      (85, 181)        100
10      410      239      165      (38, 187)        100
11      244      153      102      (225, 76)        100
```

Fig. 7 Scenario of node with their properties

Figure 8 displays node distance of nodes Ni and Nj within radio range (i.e., 100) in 3 × 3 dimension. Figure 9 displays node and link membership, which are also known as fuzzy costs, i.e., $\phi 1$ and $\phi 2$, where $\phi 1$ for node or place and $\phi 2$ for link or edge. These two costs are evaluated with the help of FPN techniques where place and transition of FPN play a vital role. The mathematical modeling help to derive different feasible paths between source node S, i.e., N0 and destination node D, i.e., N4. The whole scenario is illustrated in Fig. 10.

```
Node(i),Node(j),Distance(i,j)
================================================
[[2, 1, 70.0], [3, 0, 33.27], [4, 0, 94.48], [4, 2, 24.49],
6, 1, 55.78], [6, 2, 77.39], [6, 3, 71.3], [6, 4, 57.78],
4, 96.99], [7, 5, 62.89], [7, 6, 38.54], [8, 1, 71.53], [8,
, 86.24], [9, 3, 92.22], [9, 4, 26.59], [9, 5, 59.7], [9,
, 92.35], [10, 4, 72.36], [10, 5, 63.91], [10, 8, 78.07],
[11, 6, 29.85], [11, 7, 51.85], [11, 9, 92.6]]
```

Fig. 8 Scenario of node with their properties

```
Node Membership
 {0: 0.8, 1: 0.6, 2: 0.9, 3: 0.6, 4: 0.8, 5: 0.3, 6: 0.8, 7: 0.6, 8: 0.8, 9: 0.9, 10: 0.9, 11: 0.6}
Link Membership
 {(2, 1): 0.9, (1, 2): 0.9, (3, 0): 0.9, (0, 3): 0.9, (4, 0): 0.6, (0, 4): 0.6, (4, 2): 0.9, (2, 4): 0.9, (5, 1): 0.9, (1
, 5): 0.9, (5, 2): 0.8, (2, 5): 0.8, (5, 4): 0.8, (4, 5): 0.8, (6, 0): 0.9, (0, 6): 0.9, (6, 1): 0.9, (1, 6): 0.9, (6, 2)
: 1.0, (2, 6): 1.0, (6, 3): 0.8, (3, 6): 0.8, (6, 4): 0.8, (4, 6): 0.8, (6, 5): 0.9, (5, 6): 0.9, (7, 0): 0.8, (0, 7): 0.
8, (7, 1): 0.8, (1, 7): 0.8, (7, 3): 1.0, (3, 7): 1.0, (7, 4): 0.6, (4, 7): 0.6, (7, 5): 0.7, (5, 7): 0.7, (7, 6): 1.0, (
6, 7): 1.0, (8, 1): 0.9, (1, 8): 0.9, (8, 2): 0.9, (2, 8): 0.9, (8, 4): 0.9, (4, 8): 0.9, (8, 5): 0.4, (5, 8): 0.4, (9, 0
): 0.9, (0, 9): 0.9, (9, 2): 0.7, (2, 9): 0.7, (9, 3): 0.3, (3, 9): 0.3, (9, 4): 0.8, (4, 9): 0.8, (9, 5): 0.8, (5, 9): 0
.8, (9, 6): 0.8, (6, 9): 0.8, (9, 8): 0.9, (8, 9): 0.9, (10, 0): 0.6, (0, 10): 0.6, (10, 2): 0.7, (2, 10): 0.7, (10, 3):
0.5, (3, 10): 0.5, (10, 4): 0.9, (4, 10): 0.9, (10, 5): 1.0, (5, 10): 1.0, (10, 8): 0.4, (8, 10): 0.4, (10, 9): 1.0, (9,
10): 1.0, (11, 0): 0.8, (0, 11): 0.8, (11, 4): 0.4, (4, 11): 0.4, (11, 5): 0.9, (5, 11): 0.9, (11, 6): 0.9, (6, 11): 0.9,
(11, 7): 1.0, (7, 11): 1.0, (11, 9): 0.3, (9, 11): 0.3}
```

Fig. 9 Scenario of node with their properties

```
Enter the SOURCE and DESTINATION node seperated by a space: 0 4
================================================
Path_ 1 ['0', '4']
Path_ 2 ['0', '7', '4']
Path_ 3 ['0', '10', '2', '4']
Path_ 4 ['0', '10', '2', '9', '4']
Path_ 5 ['0', '10', '2', '9', '6', '4']
Path_ 6 ['0', '10', '2', '9', '11', '4']
Path_ 7 ['0', '10', '3', '9', '2', '4']
Path_ 8 ['0', '10', '3', '9', '4']
Path_ 9 ['0', '10', '3', '9', '6', '4']
Path_ 10 ['0', '10', '3', '9', '11', '4']
Path_ 11 ['0', '10', '4']
Path_ 12 ['0', '11', '4']
Path_ 13 ['0', '11', '9', '2', '4']
Path_ 14 ['0', '11', '9', '2', '8', '10', '4']
Path_ 15 ['0', '11', '9', '2', '10', '4']
Path_ 16 ['0', '11', '9', '3', '10', '2', '4']
Path_ 17 ['0', '11', '9', '3', '10', '4']
Path_ 18 ['0', '11', '9', '4']
Path_ 19 ['0', '11', '9', '6', '3', '10', '2', '4']
Path_ 20 ['0', '11', '9', '6', '3', '10', '4']
Path_ 21 ['0', '11', '9', '6', '4']
Path_ 22 ['0', '11', '9', '8', '10', '2', '4']
Path_ 23 ['0', '11', '9', '8', '10', '4']
================================================
Optimal Path =  ['0', '11', '9', '2', '4']
```

Fig. 10 Scenario of node with their properties

6 Conclusion

In ad hoc, nodes and links are having different properties based on which we have calculated the available paths from the source to destination by using FPNs. In this work, E, C, and S are taken as the node properties and E, DS, and DL are taken as the link property. After fuzzification of these variables, these values are converted into a single output. These output values of the nodes ($\phi 1$) and links ($\phi 2$) are compared through which we are able to find all the paths between the source and destination. All the paths from the source to destination using FPN has been found out in the current work. Future work is to analyze the other factors of the network in terms of overhead, mobility, etc. and compared with other related works.

References

1. Moamen, A. A., Hamza, H. S., & Saroit, I. A. (2014). Secure multicast routing protocols in mobile ad-hoc networks. *International Journal of Communication Systems, 27*(11), 2808–2831.
2. Gautam, S. K., & Om, H. (2016). Computational neural network regression model for host based intrusion detection system. *Perspectives in Science, 8,* 93–95.
3. Das, S. K., & Tripathi, S. (2018). Adaptive and intelligent energy efficient routing for transparent heterogeneous ad-hoc network by fusion of game theory and linear programming. *Applied Intelligence, 48*(7), 1825–1845. https://doi.org/10.1007/s10489-017-1061-6.
4. Das, S. K., & Tripathi, S. (2017). Energy efficient routing formation technique for hybrid ad hoc network using fusion of artificial intelligence techniques. *International Journal of Communication Systems, 30*(16). https://doi.org/10.1002/dac.3340.
5. Chowdhuri, S., et al. (2014). Recent research on multi input multi output (MIMO) based mobile ad hoc network: A review. *International Journal of Service Science, Management, Engineering, and Technology (IJSSMET), 5*(3), 54–65.
6. Mukherjee, A., Keshary, V., Pandya, K., Dey, N., & Satapathy, S. C. (2018). Flying ad hoc networks: A comprehensive survey. In *Information and Decision Sciences* (pp. 569–580). Springer, Singapore.
7. Chowdhuri, S., Dey, N., Chakraborty, S., & Baneerjee, P. K. (2015). Analysis of Performance of MIMO Ad Hoc Network in Terms of Information Efficiency. In *Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2* (pp. 43–50). Springer, Cham.
8. Chowdhuri, S., Chakraborty, S., Dey, N., Chaudhuri, S. S., & Banerjee, P. (2017). Propagation analysis of MIMO ad hoc network in hybrid propagation model and implement less propagation loss algorithm to find the minimum loss route. *International Journal of Information and Communication Technology, 10*(1), 66–80.
9. Das, S. K., Tripathi, S., & Burnwal, A. P. (2015). Intelligent energy competency multipath routing in wanet. In *Information systems design and intelligent applications* (pp. 535–543). Springer, New Delhi.
10. Mukherjee, A., Dey, N., Kausar, N., Ashour, A. S., Taiar, R., & Hassanien, A. E. (2019). A disaster management specific mobility model for flying ad-hoc network. In *Emergency and Disaster Management: Concepts, Methodologies, Tools, and Applications* (pp. 279–311). IGI Global.
11. Chowdhuri, S., Chaudhuri, S. S., Banerjee, P., Dey, N., Mandal, A., & Santhil, V. (2016). *Secure minimum loss route selection of MIMO-based MANET in combined (indoor, outdoor,*

and forest) terrain (pp. 1–26). working paper, International Journal Advanced Intelligence Paradigms.
12. Das, S. K., Tripathi, S., & Burnwal, A. P. (2015, February). Design of fuzzy based intelligent energy efficient routing protocol for wanet. In *Proceedings of the 2015 Third International Conference on Computer, Communication, Control and Information Technology (C3IT)* (pp. 1–4). IEEE.
13. Fong, S., Li, J., Song, W., Tian, Y., Wong, R. K., & Dey, N. (2018). Predicting unusual energy consumption events from smart home sensor network by data stream mining with misclassified recall. *Journal of Ambient Intelligence and Humanized Computing,* 1–25.
14. Chowdhuri, S., Roy, P., Goswami, S., Azar, A. T., & Dey, N. (2014). Rough set based ad hoc network: A review. *International Journal of Service Science, Management, Engineering, and Technology (IJSSMET), 5*(4), 66–76.
15. Das, S. K., Tripathi, S., & Burnwal, A. P. (2015, February). Fuzzy based energy efficient multicast routing for ad-hoc network. In *Proceedings of the 2015 Third International Conference on Computer, Communication, Control and Information Technology (C3IT)* (pp. 1–5). IEEE.
16. Chowdhuri, S., Das, S. K., Roy, P., Chakraborty, S., Maji, M., & Dey, N. (2014, November). Implementation of a new packet broadcasting algorithm for MIMO equipped Mobile ad-hoc network. In *International Conference on Circuits, Communication, Control and Computing* (pp. 372–376). IEEE.
17. Vir, D., Agarwal, S.K., Imam, S.A. and Mohan, L. (2012, October). Performance analysis of MTPR routing protocol in power deficient node. In *proceedings of the International Journal on Ad Hoc Networking Systems (IJANS) 2*(4), 67–75.
18. Budyal, V. R., & Manvi, S. S. (2013). Intelligent agent based delay aware QoS unicast routing in mobile ad hoc networks. *International Journal of Multimedia and Ubiquitous Engineering, 8*(1), 11–28.
19. Singh, H., & Singh, P. (2017). Enhanced new clustering ant colony optimization based routing protocol AODV-R. *International Journal of Computer Applications, 160*(9).
20. Sarkar, D., Choudhury, S., & Majumder, A. (2018). Enhanced-Ant-AODV for optimal route selection in mobile ad-hoc network. *Journal of King Saud University-Computer and Information Sciences.*
21. Das, S. K., Yadav, A. K., & Tripathi, S. (2017). IE2 M: Design of intellectual energy efficient multicast routing protocol for ad-hoc network. *Peer-to-Peer Networking and Applications, 10*(3), 670–687. https://doi.org/10.1007/s12083-016-0532-6.
22. Yadav, A. K., Das, S. K., & Tripathi, S. (2017). EFMMRP: Design of efficient fuzzy based multi-constraint multicast routing protocol for wireless ad-hoc network. *Computer Networks, 118,* 15–23.
23. Das, S. K., & Tripathi, S. (2018). Intelligent Energy-aware Efficient Routing for MANET. *Wireless Networks, Springer, 24*(4), 1139–1159. Retrieved May 2018, from https://doi.org/10.1007/s11276-016-1388-7.
24. Das, S. K., & Tripathi, S. (2019). Energy efficient routing formation algorithm for hybrid ad-hoc network: A geometric programming approach. *Peer-to-Peer Networking and Applications, Springer, 12*(1), 102–128. Retrieved January 2019, from https://doi.org/10.1007/s12083-018-0643-3.
25. Wang, Y. L., Mei, S. O. N. G., Wei, Y. F., Wang, Y. H., & Wang, X. J. (2014). Improved ant colony-based multi-constrained QoS energy-saving routing and throughput optimization in wireless Ad-hoc networks. *The Journal of China Universities of Posts and Telecommunications, 21*(1), 43–59.
26. Abdel-Moniem, A.M., Mohamed, M.H. & Hedar, A. R. (2010, November). An ant colony optimization algorithm for the mobile ad hoc network routing problem based on AODV protocol. In *2010 10th International Conference on Intelligent Systems Design and Applications* (pp. 1332–1337). IEEE.
27. Dhurandher, S. K., Misra, S., Pruthi, P., Singhal, S., Aggarwal, S., & Woungang, I. (2011). Using bee algorithm for peer-to-peer file searching in mobile ad hoc networks. *Journal of Network and Computer Applications, 34*(5), 1498–1508.

28. Rao, M., & Singh, N. (2014). An improved routing protocol (AODV nthBR) for efficient routing in MANETs. In *Advanced Computing, Networking and Informatics-Volume 2* pp. 215–223. Springer, Cham.
29. Misra, S., & Rajesh, G. (2011). Bird flight-inspired routing protocol for mobile ad hoc networks. *ACM Transactions on Autonomous and Adaptive Systems (TAAS), 6*(4), 25.
30. Mazumdar, N., & Om, H. (2017). DUCR: Distributed unequal cluster-based routing algorithm for heterogeneous wireless sensor networks. *International Journal of Communication Systems. 30.* Retrieved from https://doi.org/10.1002/dac.3374.
31. Mazumdar, Nabajyoti, & Om, Hari. (2017). Distributed fuzzy logic based energy-aware and coverage preserving unequal clustering algorithm for wireless sensor networks: Distributed Energy-aware and Coverage preserving Unequal Clustering. *International Journal of Communication Systems, 30,* e3283. https://doi.org/10.1002/dac.3283.
32. Chaya, S., Jayasree, P. V. Y., Kumar, S., & Sah, D. K. (2018) Boolean directional sensor orientation solution for K-coverage in wireless sensor network. In *2018 4th International Conference on Recent Advances in Information Technology (RAIT)* (pp. 1–6). Dhanbad.
33. Sah, D. K., & Amgoth, T. (2018). Parametric survey on cross-layer designs for wireless sensor networks. *Computer Science Review, 27,* 112–134. https://doi.org/10.1016/j.cosrev.2017.12.002.
34. Sah, D. K., Shivalingagowda, C., & Kumar, D. P. (2018). Optimization Problems in Wireless Sensors Networks. In *Soft Computing in Wireless Sensor Networks,* (pp 41–62). Chapman and Hall/CRC.
35. Singh, A. K., Bera, T., & Pamula, R. (2018). PRCP: Packet replication control based prophet routing strategy for delay tolerant network. In *2018 4th International Conference on Recent Advances in Information Technology (RAIT),* (pp. 1–5). IEEE.
36. Singh, A. K., & Pamula, R. (2018). IRS: Incentive Based Routing Strategy for Socially Aware Delay Tolerant Networks. In *2018 5th International Conference on Signal Processing and Integrated Networks (SPIN),* pp. 343–347. IEEE.
37. Binh, H. T. T., & Dey, N. (Eds.). (2018). *Soft Computing in Wireless Sensor Networks.* CRC Press.
38. Hu, Z. G., Ma, H., Wang, G. J., & Liao, L. (2005). A reliable routing algorithm based on fuzzy Petri net in mobile ad hoc networks. *Journal of Central South University of Technology, 12*(6), 714–719.