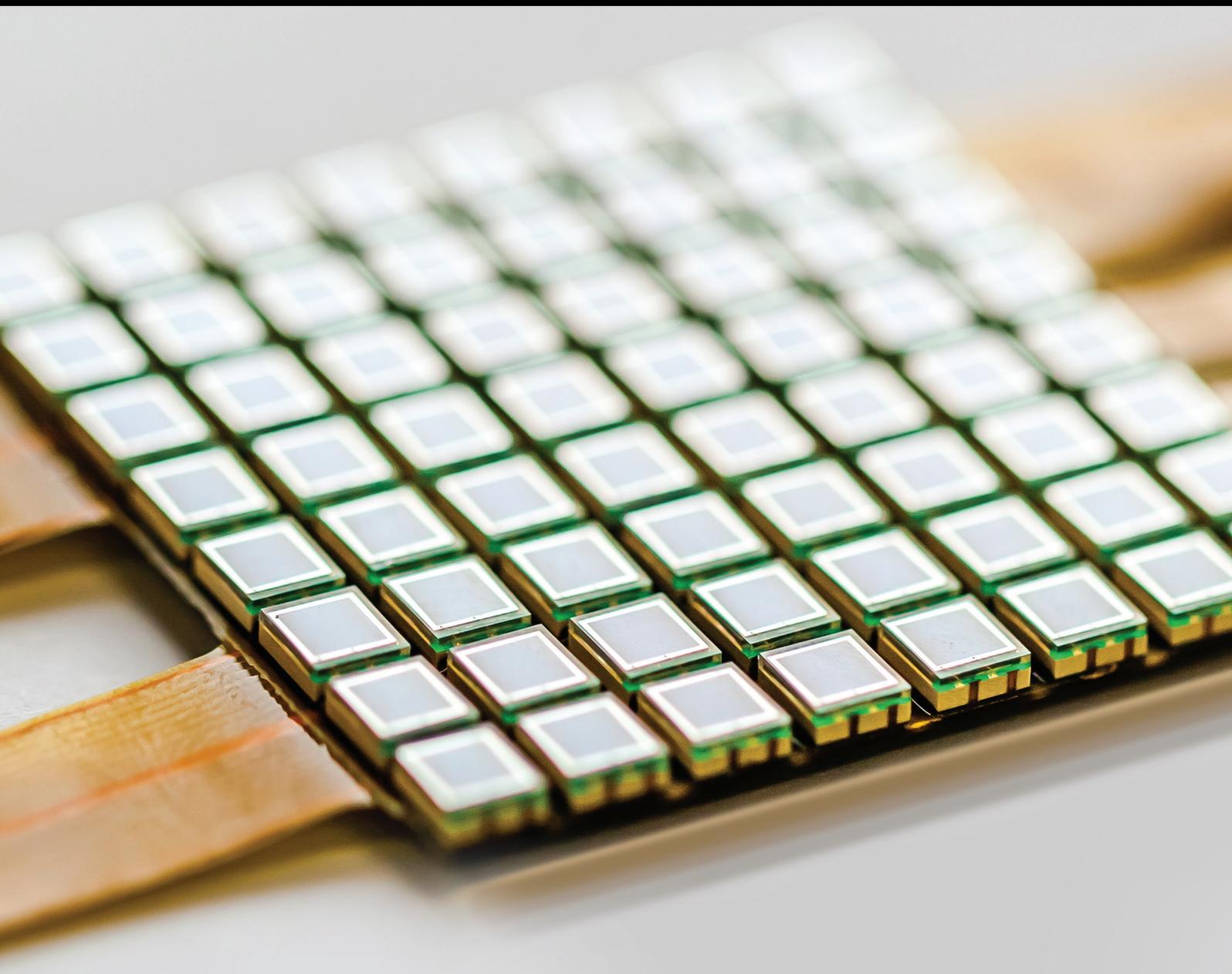


Recent Advances in Security and Privacy for Wireless Sensor Networks 2016

Guest Editors: Fei Yu, Chin-Chen Chang, Jian Shu, Iftikhar Ahmad, Jun Zhang, and Jose M. De Fuentes





**Recent Advances in Security and Privacy
for Wireless Sensor Networks 2016**

**Recent Advances in Security and Privacy
for Wireless Sensor Networks 2016**

Guest Editors: Fei Yu, Chin-Chen Chang, Jian Shu,
Iftikhar Ahmad, Jun Zhang, and Jose M. De Fuentes



Copyright © 2017 Hindawi Publishing Corporation. All rights reserved.

This is a special issue published in "Journal of Sensors." All articles are open access articles distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Editorial Board

Harith Ahmad, Malaysia
Bruno Andò, Italy
Francisco J. Arregui, Spain
Francesco Baldini, Italy
Fernando Benito-Lopez, Ireland
Romeo Bernini, Italy
Shekhar Bhansali, USA
Wojtek J. Bock, Canada
Hubert Brändle, Switzerland
Davide Brunelli, Italy
Paolo Bruschi, Italy
Belén Calvo, Spain
Stefania Campopiano, Italy
Domenico Caputo, Italy
Sara Casciati, Italy
Gabriele Cazzulani, Italy
Chi Chiu Chan, Singapore
Nick Chaniotakis, Greece
Nicola Cioffi, Italy
Elisabetta Comini, Italy
Marco Consales, Italy
Jesus Corres, Spain
Andrea Cusano, Italy
Antonello Cutolo, Italy
Dzung Dao, Australia
Manel del Valle, Spain
Francesco Dell'Olio, Italy
Utkan Demirci, USA
Nicola Donato, Italy
Junhang Dong, USA
Abdelhamid Errachid, France
Stephane Evoy, Canada
Vittorio Ferrari, Italy

Luca Francioso, Italy
Laurent Francis, Belgium
Wei Gao, Japan
Michele Giordano, Italy
Banshi D. Gupta, India
Clemens Heitzinger, Austria
María del Carmen Horrillo, Spain
Wieslaw Jakubik, Poland
Hai-Feng Ji, USA
Kouros Kalantar-Zadeh, Australia
Sher Bahadar Khan, KSA
Sang Sub Kim, Republic of Korea
Challa Kumar, USA
Laura M. Lechuga, Spain
Chengkuo Lee, Singapore
Chenzhong Li, USA
Eduard Llobet, Spain
Jaime Lloret, Spain
Yu-Lung Lo, Taiwan
Oleg Lupan, Moldova
Frederick Mailly, France
Eugenio Martinelli, Italy
J. R. Martinez-De-Dios, Spain
Yasuko Y. Maruo, Japan
Mike McShane, USA
Igor L. Medintz, USA
Fanli Meng, China
Aldo Minardo, Italy
Joan Ramon Morante, Spain
Lucia Mosiello, Italy
Masayuki Nakamura, Japan
Heinz C. Neitzert, Italy
Calogero M. Oddo, Italy

M. Palaniswami, Australia
Alberto J. Palma, Spain
Lucio Pancheri, Italy
Alain Pauly, France
Giorgio Pennazza, Italy
Michele Penza, Italy
Andrea Ponzoni, Italy
B. Pradhan, Malaysia
Ioannis Raptis, Greece
Armando Ricciardi, Italy
C. Riziotis, Greece
M. L. Rodríguez-Méndez, Spain
Albert Romano-Rodriguez, Spain
Carlos Ruiz, Spain
Josep Samitier, Spain
Giorgio Sberveglieri, Italy
Luca Schenato, Italy
Andreas Schütze, Germany
Woosuck Shin, Japan
Pietro Siciliano, Italy
Vincenzo Spagnolo, Italy
Vincenzo Stornelli, Italy
Weilian Su, USA
Tong Sun, UK
Raymond Swartz, USA
Hidekuni Takao, Japan
Isao Takayanagi, Japan
Guiyun Tian, UK
Suna Timur, Turkey
Hana Vaisocherova, Czech Republic
Qihao Weng, USA
Matthew J. Whelan, USA
Hai Xiao, USA

Contents

Recent Advances in Security and Privacy for Wireless Sensor Networks 2016

Fei Yu, Chin-Chen Chang, Jian Shu, Iftikhar Ahmad, Jun Zhang, and Jose Maria de Fuentes
Volume 2017, Article ID 3057534, 3 pages

An Intelligent and Secure Health Monitoring Scheme Using IoT Sensor Based on Cloud Computing

Jin-Xin Hu, Chin-Ling Chen, Chun-Long Fan, and Kun-hao Wang
Volume 2017, Article ID 3734764, 11 pages

Identity Recognition Using Biological Electroencephalogram Sensors

Wei Liang, Liang Cheng, and Mingdong Tang
Volume 2016, Article ID 1831742, 9 pages

Privacy Models in Wireless Sensor Networks: A Survey

J. M. de Fuentes, L. González-Manzano, and O. Mirzaei
Volume 2016, Article ID 4082084, 18 pages

A Lightweight Authentication and Key Management Scheme for Wireless Sensor Networks

Danyang Qin, Shuang Jia, Songxiang Yang, Erfu Wang, and Qun Ding
Volume 2016, Article ID 1547963, 9 pages

WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks

Iman Almomani, Bassam Al-Kasasbeh, and Mousa AL-Akhras
Volume 2016, Article ID 4731953, 16 pages

Supporting Business Privacy Protection in Wireless Sensor Networks

Nan Feng, Zhiqi Hao, Sibao Yang, and Harris Wu
Volume 2016, Article ID 7638149, 11 pages

WDARS: A Weighted Data Aggregation Routing Strategy with Minimum Link Cost in Event-Driven WSNs

Omar Adil Mahdi, Ainuddin Wahid Abdul Wahab, Mohd Yamani Idna Idris, Ammar Abu Znaid, Yusor Rafid Bahar Al-Mayouf, and Suleman Khan
Volume 2016, Article ID 3428730, 12 pages

R-bUCRP: A Novel Reputation-Based Uneven Clustering Routing Protocol for Cognitive Wireless Sensor Networks

Mingchuan Zhang, Ruijuan Zheng, Ying Li, Qingtao Wu, and Liang Song
Volume 2016, Article ID 5986265, 9 pages

A Passenger Flow Risk Forecasting Algorithm for High-Speed Railway Transport Hub Based on Surveillance Sensor Networks

Zhengyu Xie and Yong Qin
Volume 2016, Article ID 5647909, 6 pages

Routing Algorithm with Uneven Clustering for Energy Heterogeneous Wireless Sensor Networks

Ying Zhang, Wei Xiong, Dezhi Han, Wei Chen, and Jun Wang
Volume 2016, Article ID 7542907, 9 pages

Low Complexity Signed Response Based Sybil Attack Detection Mechanism in Wireless Sensor Networks

M. Saud Khan and Noor M. Khan
Volume 2016, Article ID 9783072, 9 pages

A Novel Nonlinear Multitarget k -Degree Coverage Preservation Protocol in Wireless Sensor Networks

Zeyu Sun, Xiaofei Xing, Chuanfeng Li, Yalin Nie, and Yangjie Cao
Volume 2016, Article ID 3434961, 13 pages

AR-RBFS: Aware-Routing Protocol Based on Recursive Best-First Search Algorithm for Wireless Sensor Networks

Farzad Kiani
Volume 2016, Article ID 8743927, 10 pages

An Improved μ TESLA Protocol Based on Queuing Theory and Benaloh-Leichter SSS in WSNs

Haiping Huang, Tianhe Gong, Tao Chen, Mingliang Xiong,
Xinxing Pan, and Ting Dai
Volume 2016, Article ID 9021650, 13 pages

Disjoint Key Establishment Protocol for Wireless Sensor and Actor Networks

AtaUllah Ghafoor, Muhammad Sher, Muhammad Imran, and Imran Baig
Volume 2016, Article ID 5071617, 15 pages

System for Malicious Node Detection in IPv6-Based Wireless Sensor Networks

Kresimir Grgic, Drago Zagar, and Visnja Krizanovic Cik
Volume 2016, Article ID 6206353, 20 pages

Adaptive Cross-Layer Multipath Routing Protocol for Mobile Ad Hoc Networks

Zeeshan Iqbal, S. Khan, Amjad Mehmood, Jaime Lloret, and Nabil Ali Alrajeh
Volume 2016, Article ID 5486437, 18 pages

Security Analysis and Improvements of Session Key Establishment for Clustered Sensor Networks

Jiye Kim, Jongho Moon, Jaewook Jung, and Dongho Won
Volume 2016, Article ID 4393721, 17 pages

RESH: A Secure Authentication Algorithm Based on Regeneration Encoding Self-Healing Technology in WSN

Wei Liang, Zhiqiang Ruan, Yuntao Wang, and Xiaoyan Chen
Volume 2016, Article ID 2098680, 11 pages

Multilevel Modeling of Distributed Denial of Service Attacks in Wireless Sensor Networks

Katarzyna Mazur, Bogdan Ksiezopolski, and Radoslaw Nielek
Volume 2016, Article ID 5017248, 13 pages

Study of Wireless Authentication Center with Mixed Encryption in WSN

Yiqin Lu, Jing Zhai, Ronghuan Zhu, and Jiancheng Qin
Volume 2016, Article ID 9297562, 7 pages

Enhancing Energy Efficiency of Wireless Sensor Network through the Design of Energy Efficient Routing Protocol

Noor Zaman, Low Tang Jung, and Muhammad Mehboob Yasin

Volume 2016, Article ID 9278701, 16 pages

Information Security of PHY Layer in Wireless Networks

Weidong Fang, Fengrong Li, Yanzan Sun, Lianhai Shan, Shanji Chen, Chao Chen, and Meiju Li

Volume 2016, Article ID 1230387, 10 pages

Prediction Approach of Critical Node Based on Multiple Attribute Decision Making for Opportunistic Sensor Networks

Qifan Chen, Linlan Liu, Zhiyong Yang, and Kai Guo

Volume 2016, Article ID 8246030, 8 pages

Multitask Learning-Based Security Event Forecast Methods for Wireless Sensor Networks

Hui He, Dongyan Zhang, Xing Wang, Min Liu, Weizhe Zhang, and Junxi Guo

Volume 2016, Article ID 6047023, 11 pages

Editorial

Recent Advances in Security and Privacy for Wireless Sensor Networks 2016

**Fei Yu,¹ Chin-Chen Chang,² Jian Shu,³ Iftikhar Ahmad,⁴
Jun Zhang,⁵ and Jose Maria de Fuentes⁶**

¹*Peoples' Friendship University of Russia, Moscow, Russia*

²*Feng Chia University, Taichung, Taiwan*

³*Nanchang Hangkong University, Nanchang, China*

⁴*King Saud University, Riyadh, Saudi Arabia*

⁵*Deakin University, Melbourne, Australia*

⁶*Universidad Carlos III de Madrid, Madrid, Spain*

Correspondence should be addressed to Fei Yu; hunanyufei@126.com

Received 8 February 2017; Accepted 8 February 2017; Published 23 February 2017

Copyright © 2017 Fei Yu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Wireless networks have experienced explosive growth during the last few years. Nowadays, there are a large variety of networks spanning from the well-known cellular networks to noninfrastructure wireless networks such as mobile ad hoc networks and sensor networks. Communication security is essential to the success of wireless sensor network applications, especially for those mission-critical applications working in unattended and even hostile environments. However, providing satisfactory security protection in wireless sensor networks has ever been a challenging task due to various network and resource constraints and malicious attacks.

In this special issue, we concentrate mainly on security and privacy as well as the emerging applications of wireless sensor network. It aims to bring together researchers and practitioners from wireless and sensor networking, security, cryptography, and distributed computing communities, with the goal of promoting discussions and collaborations. We are interested in novel research on all aspects of security in wireless sensor networks and tradeoff between security and performance such as QoS, dependability, and scalability. The special issue covers industrial issues/applications and academic research into security and privacy for wireless sensor networks.

This special issue includes a collection of 25 papers selected from 97 submissions to 21 countries or districts

(Australia, China, Croatia, France, India, Iraq, Jordan, Korea, Malaysia, Morocco, Oman, Pakistan, Poland, Russia, Saudi Arabia, Spain, Taiwan, Tunisia, Turkey, UK, and USA).

In the paper entitled “Multitask Learning-Based Security Event Forecast Methods for Wireless Sensor Networks,” H. He et al. propose a sensor network security event forecast method named Prediction Network Security Incomplete Unmarked Data (PNSIUD) method to forecast missing attack data in the target region according to the known partial data in similar regions.

In the paper entitled “Prediction Approach of Critical Node Based on Multiple Attribute Decision Making for Opportunistic Sensor Networks” by Q. Chen et al., the conceptions of critical nodes, region contribution, and cut-vertex in multiregion OSN are defined; then an approach to predict critical node for OSN is proposed, which is based on multiple attribute decision making (MADM).

The paper entitled “Information Security of PHY Layer in Wireless Networks” by W. Fang et al. firstly identifies and summarizes the threats and vulnerabilities in PHY layer of wireless networks. Then, we give a holistic overview of PHY layer secure schemes, which are divided into three categories: spatial domain-based, time domain-based, and frequency domain-based.

The paper entitled “Enhancing Energy Efficiency of Wireless Sensor Network through the Design of Energy Efficient

Routing Protocol” by N. Zaman et al. proposes a new routing protocol entitled “Position Responsive Routing Protocol (PRRP)” and compares its performance with the well-known LEACH and CELRP protocols. The simulation results show a significant improvement over the aforementioned protocols in terms of energy efficiency and the overall performance of the WSN.

In the paper entitled “Study of Wireless Authentication Center with Mixed Encryption in WSN,” Y. Lu et al. propose a wireless authentication center with mixed encryption named “MEWAC” according to shortcomings of the current schemes. MEWAC has the advantages of low cost, low power consumption, good performance, and stability; moreover, the authentication protocol improves the security of sensor nodes and reduces the overhead in node authentication.

The paper entitled “Multilevel Modeling of Distributed Denial of Service Attacks in Wireless Sensor Networks” by K. Mazur et al. proposes a model of a structural health monitoring network, being disturbed by one of the most common types of DDoS attacks, the flooding attack.

The paper entitled “RESH: A Secure Authentication Algorithm Based on Regeneration Encoding Self-Healing Technology in WSN” by W. Liang et al. considers the regeneration encoding self-healing and secret sharing techniques and proposes an effective scheme to authenticate data in WSN. The data is encoded by regeneration codes and then distributed to other redundant nodes in the form of fragments.

In the paper entitled “Security Analysis and Improvements of Session Key Establishment for Clustered Sensor Networks” J. Kim et al. propose a session key establishment scheme for clustered sensor networks that is based on elliptic curve Diffie-Hellman (ECDH) key exchange and hash chain. The proposed scheme eliminates vulnerabilities of existing schemes for WSN and has improved security.

The paper entitled “Adaptive Cross-Layer Multipath Routing Protocol for Mobile Ad Hoc Networks” by Z. Iqbal et al. proposes a cross-layer multipath routing protocol for MANET. The proposed protocol has two important features, that is, security and adaptive nature. These important features are achieved by multipath framework using cross-layer interface.

The paper entitled “System for Malicious Node Detection in IPv6-Based Wireless Sensor Networks” by K. Grgic et al. proposes a system for detecting malicious nodes in an IPv6-based WSN. The proposed system is designed for the IPv6 environment and it supports the IPv6 stack in a WSN. It is implemented into the sensor network that uses the IEEE 802.15.4 standard and the 6LoWPAN adaptation layer.

The paper entitled “Disjoint Key Establishment Protocol for Wireless Sensor and Actor Networks” by A. Ghafoor et al. presents a Disjoint Key Establishment Protocol (DKEP) that does not require transmitting keys across the nodes. In DKEP, each node is preloaded with one row and one column from a matrix.

The paper entitled “An Improved μ TESLA Protocol Based on Queuing Theory and Benaloh-Leichter SSS in WSNs” by H. Huang et al. proposes a novel secret key release scheme based on the data flow, which addresses some

problems of traditional key release schemes based on the fixed time interval, effectively improves the efficiency of the utilization of keys, prolongs the life cycle of hash chain, and reduces the network communication overhead and computational cost.

The paper entitled “AR-RBFS: Aware-Routing Protocol Based on Recursive Best-First Search Algorithm for Wireless Sensor Networks” by F. Kiani proposes the design of an AR-RBFS based routing protocol in two different scenarios on WSN. It is used to evaluate the power consumption and packet delivery rate of wireless sensor nodes. The algorithm computes an optimized path to route the packets from the sink to the destination node.

In the paper entitled “A Novel Nonlinear Multitarget k -Degree Coverage Preservation Protocol in Wireless Sensor Networks” by Z. Sun et al., due to the existence of a large number of redundant data in the process of covering multiple targets, the effective coverage of monitored region decreases, causing the network to consume more energy. To solve this problem, this paper proposes a multitarget k -degree coverage preservation protocol.

The paper entitled “Low Complexity Signed Response Based Sybil Attack Detection Mechanism in Wireless Sensor Networks” by M. S. and N. M. Khan proposes a low complexity sybil attack detection scheme that is based on signed response (SRES) authentication mechanism developed for Global System for Mobile (GSM) communications. A probabilistic model is presented which analyzes the proposed authentication mechanism for its probability of sybil attack.

In the paper entitled “Routing Algorithm with Uneven Clustering for Energy Heterogeneous Wireless Sensor Networks” by Y. Zhang et al. in order to solve the problem of “hotspots” in sensor networks, a kind of routing algorithm named EDEUC based on energies and distances was proposed by using the idea of uneven clustering. This method adopts double selection mechanism for cluster-heads and optimizes the competition radius of cluster-heads.

The paper entitled “A Passenger Flow Risk Forecasting Algorithm for High-Speed Railway Transport Hub Based on Surveillance Sensor Networks” by Z. Xie and Y. Qin considered the passenger flow risk forecasting problem in high-speed railway transport hub. Based on the surveillance sensor networks, a passenger flow risk forecasting algorithm was developed based on spatial correlation.

The paper entitled “R-bUCRP: A Novel Reputation-Based Uneven Clustering Routing Protocol for Cognitive Wireless Sensor Networks” by M. Zhang et al. proposes a reputation-based uneven clustering routing protocol (R-bUCRP) considering both energy saving and reputation assessment.

In the paper entitled “WDARS: A Weighted Data Aggregation Routing Strategy with Minimum Link Cost in Event-Driven WSNs” by O. A. Mahdi et al., a comprehensive weight for tradeoff between different objectives has been employed, the so-called weighted data aggregation routing strategy (WDARS) which aims to maximize the overlap routes for efficient data aggregation and link cost issues in cluster-based WSNs simultaneously.

The paper entitled “Supporting Business Privacy Protection in Wireless Sensor Networks” by N. Feng et al. proposes a

business privacy-protection system (BPS) that is modeled as a hierarchical profile in order to filter sensitive information with respect to enterprise-specified privacy requirements. The BPS is aimed at solving a tradeoff between metrics that are defined to estimate the utility of information and the business privacy risk.

The aim of the paper entitled “WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks” by I. Almomani et al. is to design an intelligent intrusion detection and prevention mechanism that could work efficiently to limit DoS attacks with reasonable cost in terms of processing and energy. To achieve this aim, a specialized dataset for WSN was constructed to classify four types of DoS attacks.

In the paper entitled “A Lightweight Authentication and Key Management Scheme for Wireless Sensor Networks” by D. Qin et al., a lightweight authentication and key management protocol AKMS have been proposed for wireless sensor networks. It uses the symmetric cryptographic primitives with keyed-hash functions (HMAC) and bidirectional encryption algorithm to provide message confidentiality and authenticity for WSN and reduces the encryption overhead to the minimum as well with just a few bytes to be performed for once per authentication attempt.

The paper entitled “Privacy Models in Wireless Sensor Networks: A Survey” by J. M. de Fuentes et al. proposes a set of guidelines to build comprehensive privacy models so as to foster their comparability and suitability analysis for different scenarios.

The paper entitled “Identity Recognition Using Biological Electroencephalogram Sensors” by W. Liang et al. proposes several brain wave-based identity recognition techniques for further studies.

The paper entitled “An Intelligent and Secure Health Monitoring Scheme Using IoT Sensor Based on Cloud Computing” by J.-X. Hu et al. proposes a scheme with IoT sensor based on cloud computing to make the elder safely and conveniently monitored.

Acknowledgments

In particular, we would like to acknowledge the program committee members of Ninth International Symposium on Information Processing (ISIP 2016). This issue contains revised and expanded versions of selected quality papers presented at the Ninth International Symposium on Information Processing (ISIP 2016). ISIP 2016 took place on August 20-21, 2016, in Changsha, China, and was cosponsored by Jishou University, China; Peoples’ Friendship University of Russia, Russia; South China University of Technology, China; Feng Chia University, Taiwan; Henan Polytechnic University, China; Nanchang Hangkong University, China; and Jiangxi University of Science and Technology, China. We wish to express our deepest thanks to the program committee members for their help in selecting papers for this issue and especially the referees of the extended versions of the selected papers for their thorough reviews under a tight time schedule. In closing, we would like to take this opportunity to thank the authors for the efforts they put in the preparation of the

manuscripts and in keeping the deadlines set by editorial requirements. We hope that you will enjoy reading this special issue as much as we did putting it together.

*Fei Yu
Chin-Chen Chang
Jian Shu
Iftikhar Ahmad
Jun Zhang
Jose Maria de Fuentes*

Research Article

An Intelligent and Secure Health Monitoring Scheme Using IoT Sensor Based on Cloud Computing

Jin-Xin Hu,¹ Chin-Ling Chen,^{2,3} Chun-Long Fan,¹ and Kun-hao Wang³

¹*School of Computer Science, Shenyang Aerospace University, Shenyang City, Liaoning Province, China*

²*Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung, Taiwan*

³*School of Information Engineering, Changchun University of Science and Technology, Changchun 130600, China*

Correspondence should be addressed to Chin-Ling Chen; clc@mail.cyut.edu.tw

Received 3 June 2016; Accepted 28 November 2016; Published 3 January 2017

Academic Editor: Hai-Feng Ji

Copyright © 2017 Jin-Xin Hu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Internet of Things (IoT) is the network of physical objects where information and communication technology connect multiple embedded devices to the Internet for collecting and exchanging data. An important advancement is the ability to connect such devices to large resource pools such as cloud. The integration of embedded devices and cloud servers offers wide applicability of IoT to many areas of our life. With the aging population increasing every day, embedded devices with cloud server can provide the elderly with more flexible service without the need to visit hospitals. Despite the advantages of the sensor-cloud model, it still has various security threats. Therefore, the design and integration of security issues, like authentication and data confidentiality for ensuring the elderly's privacy, need to be taken into consideration. In this paper, an intelligent and secure health monitoring scheme using IoT sensor based on cloud computing and cryptography is proposed. The proposed scheme achieves authentication and provides essential security requirements.

1. Introduction

With the rapid development of the Internet of Things (IoT), medical sensors, and Internet applications, online medical service has become possible in recent years. It is noteworthy that the number of elders with chronic disease is increasing every year. An aging society refers to a population structure model in which the aging population reaches or exceeds a certain proportion. According to the UN's traditional standard a region is regarded as an aging society when people over 60 years old account for 10% of the total population, while the new standard is people over 65 years old representing 7% of the total population. Between 2015 and 2050, the proportion of the world's population over 60 years will nearly double, from 12% to 22% [1]. An aging society means low fertility, aging population structure, and social security system lag. In the meantime, the health of the elderly has become a highlighted social issue. While more and more elders need long-term care, they also want to remain independent and active and reside in their own homes for as long as possible.

Due to the lack of medical resources, they cannot be treated appropriately. The hospitals are filling up with an aging population, recovery groups and high risk groups. Continuous monitoring of critical vital signs of patients is a key process in hospitals. Today, this is usually performed via different cabled sensors attached to the patient and connected to bedside monitors [2]. The limitation here is that the elders are tied to bedside devices. Consequently, it has become feasible and necessary to perform personal diagnoses of medical diseases with the measurement repository without visiting hospitals [3]. With the increasing availability of medical sensors and IoT devices for personal use, this situation opens up a new application area for body sensor networks.

Wireless sensor networks (WSNs) are an emerging technology that possesses a huge potential to play an important role in many applications [4]. The rapid growth in physiological sensors, low-power integrated circuits, and wireless communication has enabled a new generation of wireless sensor networks, now used for purposes such as monitoring traffic, crops, infrastructure, and health. The body

area network field is an interdisciplinary area which could allow inexpensive and continuous health monitoring with real-time updates of medical records via the Internet [5].

However, with the presence of sensor networks, many challenges have emerged in terms of flexibility, scalability, and heterogeneous information services. The integration of WSN with cloud provides greater flexibility, unlimited resources, immense processing power, and the ability to provide quick response to the user [6]. Cloud computing provides scientists with a completely new model for utilizing the computing infrastructure. Computer resources and storage resources and applications can be dynamically provisioned (and integrated within the existing infrastructure) on a pay-per-use basis [7]. To provide more suitable and convenient network services, cloud computing has become even more flexible for personal use. Since the cloud is a broad collection of services, organizations can choose where, when, and how they use cloud computing [8]. There are different types of cloud computing services commonly referred to as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Many studies [3, 9] pointed out that cloud computing services are clearly the future trend. Cloud computing services are provided through a browser to access online programming applications, software, and data [9]. Cloud providers have to adhere to security and privacy policies to ensure their users' data remain confidential and secure [10].

Moreover, since the number of smart phones is estimated to reach 1 billion, traditional phones started to be gradually eliminated in 2015. The rapid development of smart phones and the related technology means that mobile computing is no longer the priority; we should also focus on reducing the computation cost and communication cost to achieve the optimal efficiency. Despite the agreement and certification of parties to browse medical information, the public still has concerns about the electronic medical record (EMR) system because of the information security issues, such as hacking, information transfer time, and long-term data management problems.

In recent years, many medical resources have been implemented for people seeking medical advice conveniently [11]. In the literature [12], researchers combine mobile devices and body sensors but do not sufficiently discuss security issues. Security issues of IoT sensors and medical systems have always been a vital aspect part of active research. It is important to consider security solutions to guarantee data authenticity, freshness, replay protection, integrity, and confidentiality. Some research, such as [13–15], specifically address security issues with respect to healthcare applications. In 2014, Ben Othman et al. proposed an efficient solution for securing data transmission, which combines compressive sensing with encryption and integrity checking [16]. In 2015, an ECC-based mutual authentication protocol for secure communication between embedded devices and cloud servers was presented in a paper by Kalra and Sood [17]. In 2016, Lounis et al. proposed a new cloud-based architecture for medical wireless sensor networks which can ensure the security of medical data without patients/doctors interventions [18]. However, these schemes still fail to ensure

a patient's privacy and nonrepudiation. In this paper, we propose an intelligent and secure monitoring scheme using IoT sensors based on cloud computing to protect the elders' privacy.

The main problem here is that the elderly population is increasing every day and they should not be tied to their bed with monitoring machines, causing them inconvenience and entailing the waste of medical resources. On the other hand, the elderly with chronic conditions also have a high probability of suffering some acute diseases or episodes, such as heart attacks. Without the appropriate medical assistance, the consequences will be very serious. The EMR will be used in our scheme to provide more flexible and appropriate medical service. Due to the importance of the elders' privacy, the proposed scheme should focus on the advantages offered by the characteristics of cloud computing and the security of the elders' information.

The remainder of the paper is organized as follows: Section 2 describes the current approaches on the configuration of medical sensor networks. Section 3 introduces our scheme architecture for a wireless IoT sensor network and the set-up procedure. In Section 4, we analyze the security issues of our scheme and compare it with other schemes. Section 5 contains some conclusions and offers some ideas for future work.

2. The Proposed Scheme

In our scheme, each party should register at the key generation center which will issue a pair of public key and private key, to communicate with other parties. The user also gets the pregenerated key; it can be used to encrypt the private health information. The elders can use a mobile device to connect to the IoT medical sensor which can collect the biological data. Seven parties are involved in our scheme as follows.

(1) *Elder (E)*. The aging population with chronic disease (e.g., heart disease, diabetes, and hypertension) wears the IoT medical sensor which can collect biological data.

(2) *Cloud (C): Intelligent Data Storage*. The elder can access the cloud service to upload/download the health information via authentication. It can provide smart applications and send private health reports to the elder at set periods of time. Once there is an emergency situation, the cloud will notify the hospital.

(3) *Hospital (H)*. It is a hospital where the elder can get physical inspection and the report. Once the elder's biological data are over a threshold, the hospital will notify the elder and dispatch an ambulance after it gets the cloud's notification.

(4) *Key Generation Center (KGC)*. The key generation center will issue a pair of public key and private key for the registered parties. The user's pregenerated key and the time of the key's generation are stored in the database.

(5) *IoT Medical Sensor (MS)*. It is the collecting device of the elder's biological data. The IoT medical sensor can also

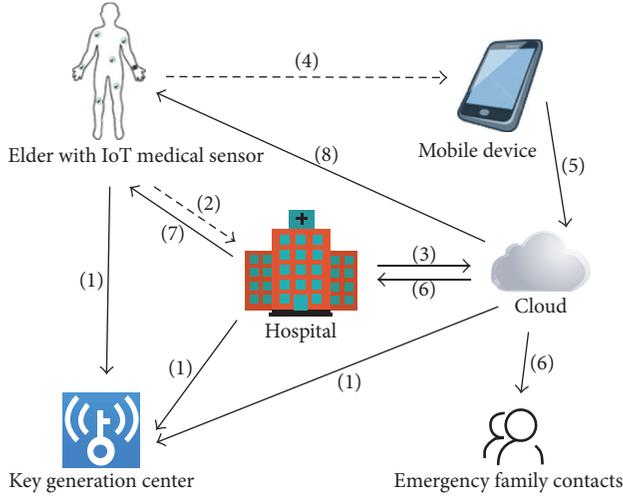


FIGURE 1: The system architecture.

transfer the collected data to the mobile device via Bluetooth (Bluetooth 4.0) and the mobile device can transfer the data to the cloud.

(6) *Mobile Device (MD)*. A portable computing device with a unique International Mobile Equipment Identity (IMEI) which can connect with the IoT medical sensor. It can locate the elder with Global Positioning System (GPS) when there is an emergency and get the reports for normal situation.

(7) *Emergency Family Contacts (EFC)*. They are the elder's family members.

The elder goes to the hospital for a health inspection and the report will be uploaded to the cloud. Every set period of time, the IoT medical sensor will collect the elder's biological data and transfer them to the cloud via mobile device. The hospital and the cloud process authentication procedure. The scenarios are described in Figure 1.

- (1) The elder, the hospital, and the cloud must register at the key generation center in advance via secure channel.
- (2) The elder goes to hospital for a physical inspection.
- (3) The hospital uploads the elder's physical inspection report to the cloud.
- (4) The IoT medical sensor gets the elder's biological data via set periods of time and sends it to the mobile device.
- (5) The mobile device uploads the biological data to the cloud.
- (6) The cloud compares the data sent from the mobile device with the standard values stored in the database. Once there is an emergency, the cloud notifies the hospital and contacts the elder's family in an acceptable time.
- (7) After the hospital gets the notification, it sends messages and dispatches an ambulance to the elder.

- (8) If the data collected by the IoT medical sensor are normal, the cloud sends a health report to the elder at set periods of time.

2.1. *Notations*. The following lists notations that will be used in our scheme:

ID_X : X 's identity.

s : the secret value.

x : the KGC's private key.

$h_0(\cdot)$: the hash function $h_0 : \{0, 1\}^* \rightarrow h_1\{0, 1\}^l, l = 256$.

$h_1(\cdot)$: the hash function $h_1 : G_2 \times \{0, 1\}^* \times G_1 \rightarrow \{0, 1\}^l, l = 256$.

ΔT : the valid transmission time interval.

T_{X_i} : the i th timestamp generated by X .

$Data_{H_i}$: the elder's physical inspection report generated by the hospital.

$Data_{MS_i}$: the elder's biological data collected by the IoT medical sensor, for example, EGC, heart rate, oxygen saturation, blood pressure, body temperature, and blood glucose.

$Cert_X$: X party's identity certification being issued by the KGC.

IMEI: International Mobile Equipment Identity.

PK_X/SK_X : X 's public/private key.

key_{X-Y} : the session key between X and Y .

$SE_K(M)/SD_K(M)$: using the symmetric key K to encrypt/decrypt a message M .

$S_{SK_x}(M)/D_{SK_x}(M)$: using the private key SK_x to sign/decrypt a message M .

$V_{PK_x}(M)/E_{PK_x}(M)$: using the public key PK_x to verify/encrypt a message M .

MSG_X : the patient's health information being generated by X .

MSG_{EM} : the emergency message.

MSG_{NM} : the normal report.

$A \stackrel{!}{=} B$: checking if A is equal to B .

—————>: insecure channel

----->: secure channel.

2.2. *Registration Phase*. Both the elder and the hospital must register at the key generation center in advance. The KGC will issue a pair of public key and private key for each party. The user will get the cloud's public key and use the pregenerated key to encrypt/decrypt the medical information. The KGC will also record the key's generation time in the database. The flowchart of the registration phase is shown in Figure 2.

(1) The elder, the hospital, and the cloud choose the identity $ID_E/ID_H/ID_C$ and send it to the key generation center through a secure channel. The elder should also send his/her

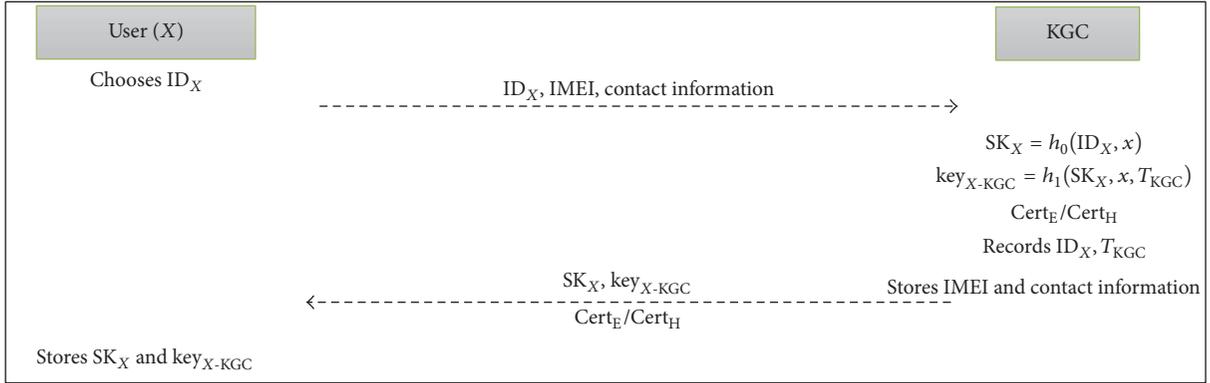


FIGURE 2: The registration phase.

mobile devices IMEI and personal contact information to the KGC, including emergency family contacts.

(2) After receiving the message, the KGC uses the private key x to compute the user's public key $PK_E/PK_H/PK_C$, the private key $SK_E/SK_H/SK_C$, and the pregenerated session key $key_{E-KGC}/key_{H-KGC}/key_{C-KGC}$ as follows:

$$\begin{aligned}
 SK_E &= h_0(ID_E, x), \\
 SK_H &= h_0(ID_H, x), \\
 SK_C &= h_0(ID_C, x), \\
 key_{E-KGC} &= h_1(SK_E, x, T_{KGC}), \\
 key_{H-KGC} &= h_1(SK_H, x, T_{KGC}), \\
 key_{C-KGC} &= h_1(SK_C, x, T_{KGC}).
 \end{aligned} \tag{1}$$

Then, the KGC sends $(PK_E, SK_E, key_{E-KGC})$, $(PK_H, SK_H, key_{H-KGC})$, and $(PK_C, SK_C, key_{C-KGC})$ to the elder, the hospital, and the cloud, respectively. In addition, the KGC generates the certification $Cert_E/Cert_H$ for the elder and hospital, respectively.

(3) Each party stores $(PK_E, SK_E, key_{E-KGC})$, $(PK_H, SK_H, key_{H-KGC})$, and $(PK_C, SK_C, key_{C-KGC})$, respectively. The elder and hospital can use the certification $Cert_E/Cert_H$ to process authentication.

2.3. The Health Data Uploading Phase

2.3.1. The Hospital Uploads Physical Inspection Report Case.

The elder goes to the hospital for a physical inspection. After the hospital and the cloud process authentication, the hospital uploads the physical inspection report to the cloud. The flowchart of the hospital uploading physical inspection report case is shown in Figure 3.

(1) The hospital uses the session key key_{H-C} to encrypt the physical inspection report and makes a timestamp T_{H1} . The

hospital uses the cloud's public key PK_C to encrypt key_{H-C} and makes a signature Sig_1 as follows:

$$\begin{aligned}
 MSG_{H1} \\
 = (ID_H, ID_E, Data_{H1}, Data_{H2}, \dots, Data_{Hn}, T_{H1}),
 \end{aligned} \tag{2}$$

$$C_1 = SE_{key_{H-C}}(MSG_{H1}), \tag{3}$$

$$C_2 = E_{PK_C}(key_{H-C}), \tag{4}$$

$$Sig_1 = S_{SK_H}(h_1(MSG_{H1})). \tag{5}$$

Then, the hospital sends Sig_1 , ID_H , ID_E , $Cert_H$, C_1 , C_2 , and T_{H1} to the cloud.

(2) The cloud verifies the hospital's signature according to the hospital's identity ID_H and checks if the timestamp T_{H1} is valid or not as follows:

$$T_{C_1} - T_{H1} \leq \Delta T. \tag{6}$$

If (6) holds, the cloud uses the KGC's public key PK_{KGC} to verify the hospital's certification $Cert_H$. Then, the cloud finds $SD_{key_{H-C}}$ according to ID_H and uses the private key SK_C and session key key_{H-C} to decrypt C_1 and C_2 :

$$V_{PK_H}(Sig_1) \stackrel{\Delta}{=} h_1(MSG_{H1}), \tag{7}$$

$$key_{H-C} = D_{SK_C}(C_2), \tag{8}$$

$$\begin{aligned}
 (ID_H, ID_E, Data_{H1}, Data_{H2}, \dots, Data_{Hn}, T_{H1}) \\
 = SD_{key_{H-C}}(C_1).
 \end{aligned} \tag{9}$$

Afterwards, the cloud stores MSG_{H1} and Sig_1 .

2.3.2. The Mobile Device Uploads Biological Data Case. In this phase, we consider the IoT medical sensors embedded into an elder's body. The elder uses the mobile device to transfer the biological data which are measured by IoT medical sensors to the cloud. The flowchart of the mobile device uploading biological data case is shown in Figure 4.

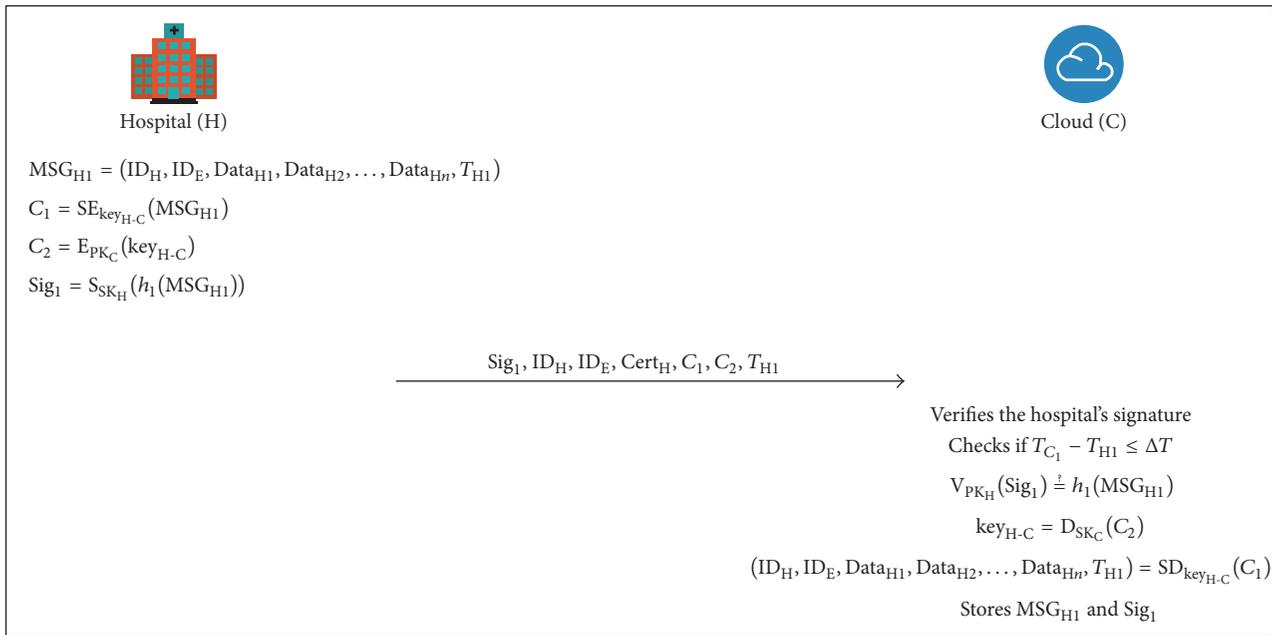


FIGURE 3: The hospital uploads physical inspection report case.

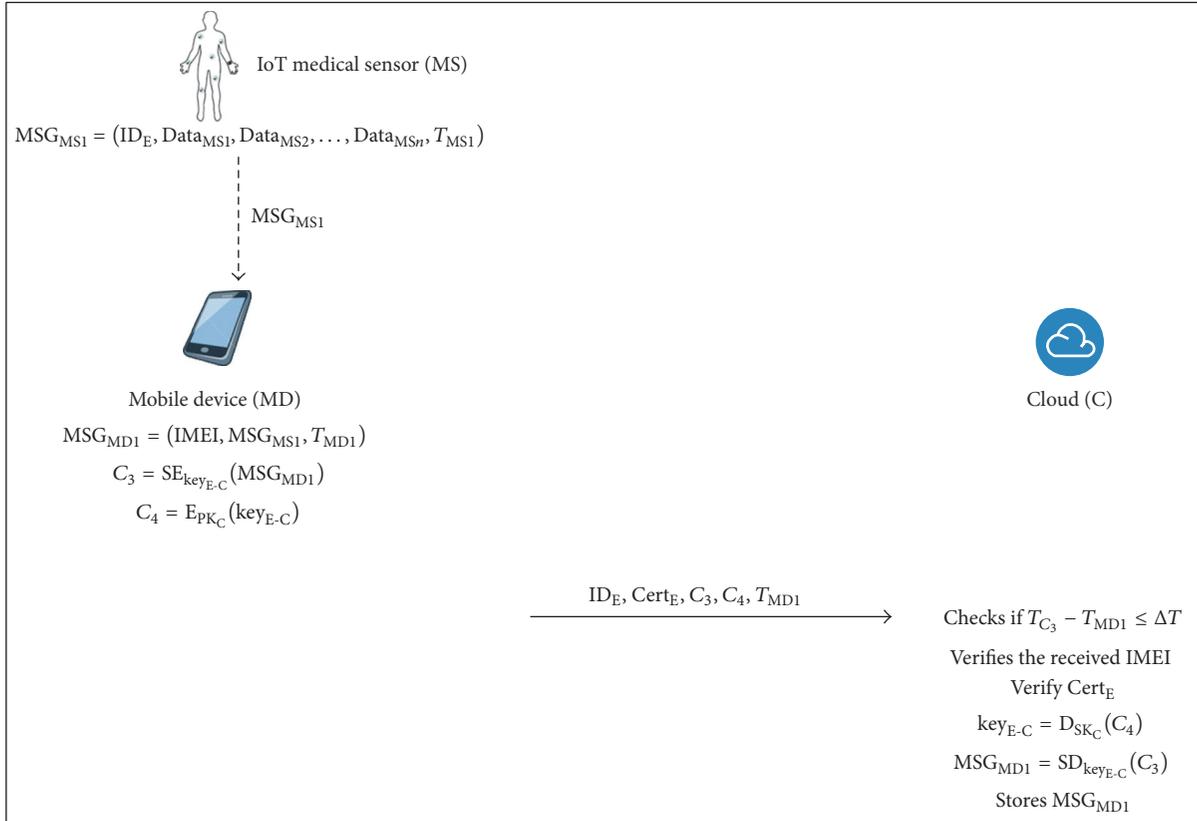


FIGURE 4: The mobile device uploads biological data case.

(1) The IoT medical sensor collects the biological data MSG_{MS1} and sends them to the elder's mobile device through a secure channel:

$$MSG_{MS1} = (ID_E, Data_{MS1}, Data_{MS2}, \dots, Data_{MSn}, T_{MS1}). \quad (10)$$

(2) After receiving the message, the mobile device uses the session key key_{E-C} to encrypt the elder's health information MSG_{MD} and makes a timestamp T_{MD} . Afterwards, the mobile device uses the cloud's public key PK_C to encrypt key_{E-C} :

$$MSG_{MD1} = (IMEI, MSG_{MS1}, T_{MD1}), \quad (11)$$

$$C_3 = SE_{key_{E-C}}(MSG_{MD1}), \quad (12)$$

$$C_4 = E_{PK_C}(key_{E-C}). \quad (13)$$

Then, the mobile device sends ID_E , $Cert_E$, C_3 , C_4 , and T_{MD1} to the cloud.

(3) The cloud checks if the timestamp T_{MD1} is valid or not:

$$T_{C_3} - T_{MD1} \leq \Delta T. \quad (14)$$

If (14) holds, the cloud verifies the received IMEI by finding the mobile device's registered IMEI which is stored in the database according to the elder's identity ID_E . If it holds, the cloud uses the public key PK_{KGC} to verify the elder's certification $Cert_E$. Then, the cloud uses the private key SK_C and session key key_{E-C} to decrypt C_3 and C_4 , respectively:

$$key_{E-C} = D_{SK_C}(C_4), \quad (15)$$

$$MSG_{MD1} = SD_{key_{E-C}}(C_3). \quad (16)$$

Afterward, the cloud stores MSG_{MD1} .

2.4. The Notification Phase

2.4.1. The Emergency Case. When the cloud gets the elder's biological data from the mobile device, the cloud compares the data with the standard values stored in the database. If there is an emergency situation, the cloud sends the alert message to the hospital and contacts the emergency family simultaneously. Then, the hospital will contact the elder and dispatch an ambulance to help the elder, if necessary. The flowchart of the emergency case is shown in Figure 5.

(1) The IoT medical sensor collects the elder's biological data, such as ECG, oxygen saturation, blood pressure, and body temperature. The IoT medical sensor sends the biological data to the mobile device through a secure channel and makes a timestamp T_{MS2} :

$$MSG_{MS2} = (ID_E, Data_{MS1}, Data_{MS2}, \dots, Data_{MSn}, T_{MS2}). \quad (17)$$

(2) After receiving the message, the mobile device makes a timestamp T_{MD2} and integrates IMEI and MSG_{MS2} :

$$MSG_{MD2} = (IMEI, MSG_{MS2}, T_{MD2}). \quad (18)$$

The mobile device then uses the session key key_{E-C} to encrypt MSG_{MD2} and the cloud's public key PK_C to encrypt key_{E-C} . In the meantime, the elder uses the private SK_E and a signature Sig_2 via mobile device as follows:

$$C_5 = SE_{key_{E-C}}(MSG_{MD2}), \quad (19)$$

$$C_6 = E_{PK_C}(key_{E-C}), \quad (20)$$

$$Sig_2 = S_{SK_E}(IMEI). \quad (21)$$

The mobile device sends Sig_2 , ID_E , $Cert_E$, C_5 , C_6 , and T_{MD2} to the cloud.

(3) After receiving the message, the cloud checks if the timestamp T_{MD2} is valid or not:

$$T_{C_5} - T_{MD2} \leq \Delta T. \quad (22)$$

If (22) holds, the cloud uses the private key SK_C and session key key_{E-C} to decrypt C_6 and C_5 as follows:

$$key_{E-C} = D_{SK_C}(C_6), \quad (23)$$

$$(IMEI, MSG_{MS2}, T_{MD2}) = SD_{key_{E-C}}(C_5).$$

The cloud then uses the KGC's public key PK_{KGC} to verify the elder's certification $Cert_E$ and check if the mobile device's IMEI is the same as the registered IMEI:

$$V_{PK_p}(Sig_2) \stackrel{!}{=} IMEI. \quad (24)$$

The cloud then compares the elder's biological data with the standard value stored in the database. If some of the inspection data is beyond the threshold, the cloud uses the hospital's public key PK_H to encrypt the emergency message MSG_{C1} and make a timestamp T_{C1} :

$$MSG_{C1} = (ID_C, ID_E, MSG_{EM}, T_{C1}), \quad (25)$$

$$C_7 = E_{PK_H}(MSG_{C1}). \quad (26)$$

The cloud sends ID_C , ID_E , $Cert_E$, $Cert_C$, C_7 , and T_{C1} to the hospital.

(4) After receiving the message, the hospital checks if the timestamp T_{C1} is valid or not as follows:

$$T_{C_7} - T_{C1} \leq \Delta T. \quad (27)$$

If (27) holds, the hospital uses the public key PK_{KGC} to verify the cloud's and the elder's certification. Then, the hospital uses the private key SK_H to decrypt C_7 :

$$MSG_{C1} = D_{SK_H}(C_7). \quad (28)$$

(5) The hospital gets the elder's identity and obtains his/her contact information which is stored in the database. The hospital then gets the elder's location via the mobile device. According to MSG_{C1} , the hospital evaluates the elder's situation to determine whether to dispatch the ambulance to help the elder. If the elder is able to receive the message,

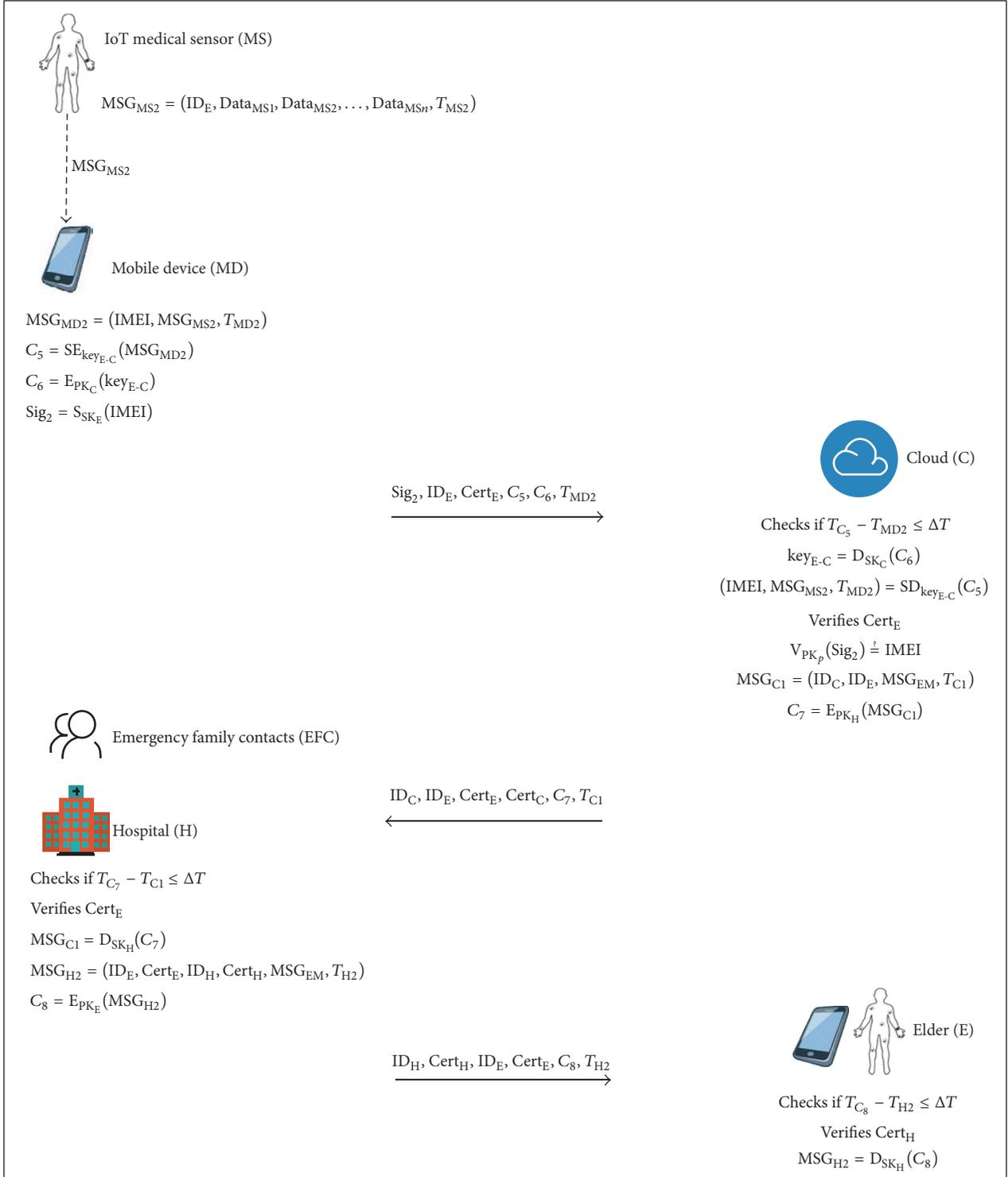


FIGURE 5: The emergency case.

the hospital uses the elder's public key PK_E to encrypt the notification MSG_{H2} and makes a timestamp T_{H2} :

$$MSG_{H2} = (ID_E, Cert_E, ID_H, Cert_H, MSG_{EM}, T_{H2}), \quad (29)$$

$$C_8 = E_{PK_E}(MSG_{H2}). \quad (30)$$

The hospital then sends $ID_H, Cert_H, ID_E, Cert_E, C_8$, and T_{H2} to the elder.

(6) The elder checks if the timestamp T_{H2} is valid or not when he/she receives the message:

$$T_{C_8} - T_{H2} \leq \Delta T. \quad (31)$$

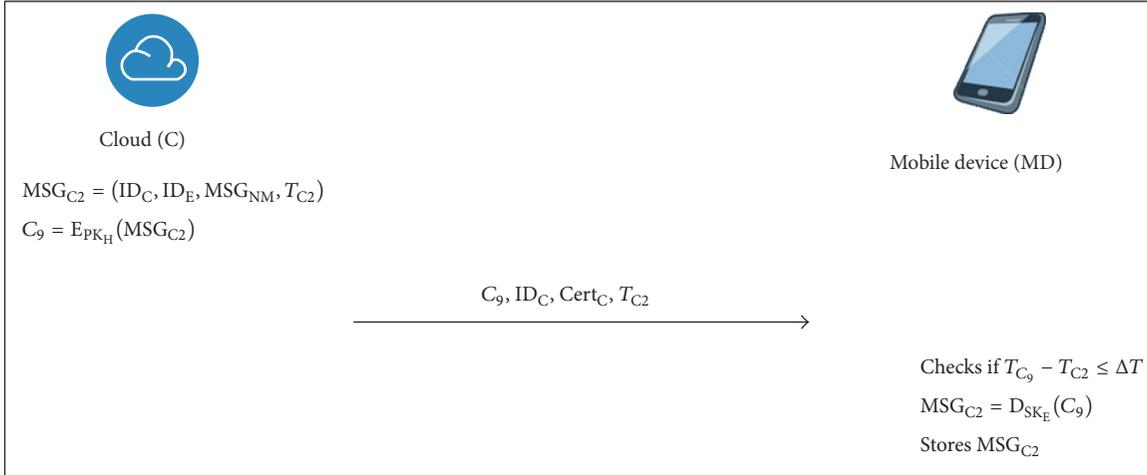


FIGURE 6: The normal case.

If (31) holds, the elder uses the public key PK_{KGC} to verify the hospital's certification and uses the private key SK_E to decrypt C_8 :

$$MSG_{H2} = D_{SK_H}(C_8). \quad (32)$$

(7) If the elder is unconscious and cannot respond to the hospital's notification, the hospital gets the elder's location via GPS and dispatches an ambulance to help him/her directly.

2.4.2. The Normal Case. If the elder's biological data fall in the average scope, the cloud will send a report back to the elder via period of time. The flowchart of the normal case is shown in Figure 6.

(1) The cloud uses the elder's public key PK_E to encrypt the normal health report MSG_{C2} and makes a timestamp T_{C2} :

$$MSG_{C2} = (ID_C, ID_E, MSG_{NM}, T_{C2}), \quad (33)$$

$$C_9 = E_{PK_H}(MSG_{C2}). \quad (34)$$

The cloud sends the encrypted health information C_9 , ID_C , $Cert_C$, and T_{C2} to the elder via set period time.

(2) After receiving the message, the elder checks if the timestamp T_{C2} is valid or not as follows:

$$T_{C_9} - T_{C2} \leq \Delta T. \quad (35)$$

If (35) holds, the elder uses the public key PK_{KGC} to verify the cloud's certification $Cert_C$. The elder then uses the private key SK_E to decrypt C_9 .

$$MSG_{C2} = D_{SK_E}(C_9). \quad (36)$$

The elder stores MSG_{C2} .

3. Security Analysis

In this section, we present a security analysis to discuss how our scheme can defend against various attacks.

3.1. Replay Attack. In our scheme, we use the timestamp mechanism to defend against the replay attack. The receiver will verify if the timestamp is valid or not by checking the valid time interval via (6), (14), (22), (27), (31), and (35). Therefore, our scheme can defend against replay attack.

3.2. Man-in-Middle Attack. If there is a man-in-middle attack, our scheme will be able to resist it by checking the timestamps to verify if the messages are valid.

The elder, the hospital, and the cloud can prove his/her identity via certification in our scheme. The elder sends the certification $Cert_E$ to the cloud and the hospital. The hospital sends the certification $Cert_H$ to the cloud and the elder. The cloud sends the certification $Cert_C$ to the elder and the hospital. Every party will check if the received certification is valid or not.

In our scheme, during the health data uploading phase, the hospital and the mobile device use the session key key_{H-C}/key_{E-C} and the public key PK_C to encrypt the information via (3), (4), (12), (13), (19), (20), (26), (30), and (34).

Other parties cannot decrypt the message without the private key or the session key, so attackers cannot achieve the man-in-middle attack.

3.3. Integrity. In the transmission process, the mobile device's IMEI is authenticated:

$$V_{PK_E}(\text{Sig}_2) \stackrel{!}{=} \text{IMEI}. \quad (37)$$

Therefore, tampering behaviors can be rapidly detected, so the proposed scheme can ensure data integrity.

3.4. Data Security. Our scheme involves the digital envelope mechanism. In order to ensure the elder's privacy, we use the public key to encrypt the symmetric key via (3), (12), (19), (26), (30), and (34), emergency information MSG_{EM} , and normal report MSG_{NM} . We use the symmetric key to protect the elder's secret biological data, via (4), (13), and (20).

TABLE 1: The nonrepudiation proof.

Nonrepudiation proof	Issuer	Holder	Nonrepudiation verification
$\text{Sig}_1 = S_{\text{SK}_H}(h_1(\text{MSG}_{H1}))$	Hospital	Cloud	$V_{\text{PK}_H}(\text{Sig}_1) \stackrel{!}{=} h_1(\text{MSG}_{H1})$
$\text{Sig}_2 = S_{\text{SK}_E}(\text{IMEI})$	Elder	Cloud	$V_{\text{PK}_E}(\text{Sig}_2) \stackrel{!}{=} \text{IMEI}$

TABLE 2: The security comparisons of related works.

Security issue	Proposed scheme			
	Ben Othman et al. [16]	Kalra and Sood [17]	Lounis et al. [18]	Our scheme
Replay attack	N/A	Yes	N/A	Yes
Man-in-middle attack	N/A	Yes	Yes	Yes
Integrity	Yes	N/A	Yes	Yes
Data security	N/A	Yes	Yes	Yes
Confidentiality	Yes	Yes	Yes	Yes
Nonrepudiation	N/A	N/A	N/A	Yes
Privacy	N/A	N/A	N/A	Yes

3.5. Confidentiality. In our scheme, we use the asymmetric/symmetric key to ensure the safety of the patient's personal information as shown in (3), (4), (12), and (13).

In the notification phase, the mobile device uses the session key key_{E-C} and cloud's public key PK_C to encrypt the information as shown in (19) and (20).

Then, the cloud uses the hospital's public key PK_H to encrypt the emergency message as shown in (26).

Afterwards, the hospital uses the elder's public key PK_E to encrypt the notification as shown in (30).

In the normal case, the cloud uses the elder's public key PK_E to encrypt the normal health report as shown in (34).

The elder's privacy information is protected. Therefore, our scheme can achieve confidentiality.

3.6. Nonrepudiation. The cloud can use the hospital's public key to verify the uploaded data via (7). The hospital cannot deny the uploading fact. The cloud can verify the correctness of the mobile device's IMEI via (24). The mobile device cannot deny the transmission. Every party can use the KGC's public key PK_{KGC} to verify whether the sender's certification is valid or not. The nonrepudiation proof is shown in Table 1.

3.7. Privacy. Data transmission on the Internet is insecure and the elder's private information may be revealed in the transmission process. In this paper, we use symmetric encryption to protect his/her personal privacy from unauthorized access. The elder's privacy is ensured.

3.8. Transmission Continuity. The elder's physical report and the biological data which are measured by IoT medical sensors will be stored in the cloud. In order to ensure transmission continuity, the receiver will send information to the sender. If the cloud has not received the elder's biological data in an acceptable time, which is recommended by the doctor, the cloud will notify the elder and contact his/her emergency family.

3.9. Security Analysis Comparison. According to the security issue, we make a comparison with other schemes in Table 2. In Table 2, Ben Othman et al.'s scheme [16] and Lounis et al.'s scheme [18] have some weaknesses. They cannot resist the replay attack. Ben Othman et al.'s scheme cannot ensure the security of data. And Kalra and Sood's scheme [17] cannot achieve integrity. The proposed scheme can resist the replay attack and man-in-middle attack and provide integrity and data security.

4. Discussions

4.1. The Computation Cost of Our Scheme. In this subsection, we present the proposed scheme's computation cost in Table 3. We use SHA-256 hash function, AES-symmetric encryption, Menezes-Vanstone cryptosystem, and signature generated by the ECDSA [20].

4.2. The Communication Cost of Our Scheme. In this subsection, we show the communication cost of the proposed scheme in Table 4. The highest communication cost in our scheme is for emergency case, while the cost is $5T_{\text{ID}} + 3T'_{\text{AS}} + 1T'_S + 1T'_{\text{Sig}} + 3T_T + 5T_{\text{Cert}} = 5 * 80 + 3 * 1024 + 1 * 256 + 1 * 1024 + 3 * 16 + 5 * 8192 = 45,760$ bits. The time of transmitting these messages is $45,760/20 * 10^{-6} = 0.9152$ ms under the 20 Mbps bandwidth network environment. Fast transmission makes our scheme feasible and efficient.

5. Conclusions

The elder's continuous medical monitoring is a serious problem. In this paper, we proposed a scheme with IoT sensor based on cloud computing to make the elder safely and conveniently monitored. In our scheme, the digital envelope, digital certification, signature, and timestamp mechanisms are involved. We also use the cloud's characteristics to make

TABLE 3: The computation cost of our scheme.

Case	Party		
	Elder	Hospital	Cloud/key generation center
The case when hospital uploads physical inspection report	N/A	$2T_{AS} + 1T_{Sig} + 1T_S + 1T_H$	$1T_{AS} + 1T_{Sig} + 1T_S$
The case when mobile device uploads biological data	$1T_{AS} + 1T_S$	N/A	$1T_{AS} + 1T_S$
The emergency case	$3T_{AS} + 1T_{Sig} + 1T_S$	$2T_{AS}$	$2T_{AS} + 1T_{Sig} + 1T_S$
The normal case	$1T_{AS}$	N/A	$1T_{AS}$

T_H : the time to execute a one-way hash function.

T_S : the time to execute a symmetric encryption/decryption operation.

T_{AS} : the time to execute an asymmetric encryption/decryption operation.

T_{Sig} : the time to execute/verify a signature.

TABLE 4: The communication cost of our scheme.

Case	Cost
The case when hospital uploads physical inspection report	$2T_{ID} + 1T'_{AS} + 1T'_S + 1T'_{Sig} + 1T_T + T_{Cert}$
The case when mobile device uploads biological data	$1T_{ID} + 1T'_{AS} + 1T'_S + 1T_T + T_{Cert}$
The emergency case	$5T_{ID} + 3T'_{AS} + 1T'_S + 1T'_{Sig} + 3T_T + 5T_{Cert}$
The normal case	$1T_{ID} + 1T'_{AS} + 1T_T + T_{Cert}$
Total	$8T_{ID} + 6T'_{AS} + 3T'_S + 2T'_{Sig} + 6T_T + 8T_{Cert}$

T_{ID} : the time to transmit the identity (80 bits).

T_T : the time to transmit a timestamp (16 bits).

T_S : the time to transmit a symmetric encryption, ciphertext (256 bits).

T_{AS} : the time to transmit an asymmetric encryption, ciphertext (1,024 bits).

T'_{Sig} : the time to transmit a signature (1024 bits).

T_{Cert} : the time to transmit a certificate (8192 bits) [19].

sure that the elder can get the available medical service conveniently. The asymmetric/symmetric encryption technology is used to protect the inspection report and the biological data of the elder. The elder's biological data and other personal information can be uploaded to the cloud via authentication. The hospital can notify the elder or dispatch an ambulance directly to him/her if there is an emergency situation. The elder can receive his/her personal health reports via set periods of time and browse the reports on their mobile device. Therefore our scheme can provide more flexible and accurate medical service as well as reduce the waste of medical resource.

Besides, our scheme can defend against the replay attack and man-in-middle attack and offer data security, integrity, nonrepudiation, and confidentiality in a cloud environment. As a result, the elder need not worry about the insecure access of medical records in our proposed medical environments.

In the future, we will focus on the bioinformatics certification to make the whole process easier for the elderly.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research was supported by the Ministry of Science and Technology, China, under Contract nos. MOST 103-2632-E-324-001-MY3, MOST 105-2221-E-324-007, and MOST105-2622-E-305-004-CC2.

References

- [1] World Health Organization, <http://www.who.int/mediacentre/factsheets/fs381/en/>.
- [2] H. Baldus, K. Klabunde, and G. Müsch, "Reliable set-up of medical body-sensor networks," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2920, pp. 353–363, 2004.
- [3] H. J. La, H. T. Jung, and S. D. Kim, "Extensible disease diagnosis cloud platform with medical sensors and IoT devices," in *Proceedings of the 3rd International Conference on Future Internet of Things and Cloud (FiCloud '15)*, pp. 371–378, IEEE, Rome, Italy, August 2015.
- [4] Z. Zhang and X. Hu, "ZigBee based wireless sensor networks and their use in medical and health care domain," in *Proceedings of the 7th International Conference on Sensing Technology (ICST '13)*, pp. 756–761, Wellington, New Zealand, December 2013.
- [5] https://en.wikipedia.org/wiki/Body_area_network.
- [6] F. Banaie and S. A. H. Seno, "A cloud-based architecture for secure and reliable service provisioning in wireless sensor network," in *Proceedings of the International Conference on Computer and Knowledge Engineering (ICCKE '14)*, pp. 96–101, Mashhad, Iran, October 2014.
- [7] C. Vecchiola, S. Pandey, and R. Buyya, "High-performance cloud computing: a view of scientific applications," in *Proceedings of the 10th International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN '09)*, pp. 4–16, IEEE, Kaohsiung, Taiwan, December 2009.
- [8] <https://support.rackspace.com/white-paper/understanding-the-cloud-computing-stack-saas-paas-iaas>.
- [9] C.-L. Chen, T.-T. Yang, M.-L. Chiang, and T.-F. Shih, "A privacy authentication scheme based on cloud for medical environment," *Journal of Medical Systems*, vol. 38, article no. 143, 2014.
- [10] A. Hendre and K. P. Joshi, "A semantic approach to cloud security and compliance," in *Proceedings of the IEEE 8th International Conference on Cloud Computing (CLOUD '15)*, pp. 1081–1084, New York, NY, USA, June 2015.

- [11] C.-L. Chen, T.-T. Yang, and T.-F. Shih, "A secure medical data exchange protocol based on cloud environment," *Journal of Medical Systems*, vol. 38, no. 9, article 112, 2014.
- [12] P. Tudor, W. Martin, B. Natalia, P. Zeeshan, and B. Leon, "Ambient Health Monitoring: the smartphone as a body sensor network component," *Innovation in Medicine and Healthcare Immed*, vol. 6, no. 1, pp. 62–65, 2013.
- [13] Z.-Y. Wu, Y.-C. Lee, F. Lai, H.-C. Lee, and Y. Chung, "A secure authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1529–1535, 2012.
- [14] S. Sahaa and S. Kumar Tomar, "Issues in transmitting physical health information in m-healthcare," *International Journal of Current Engineering and Technology*, vol. 3, no. 2, pp. 411–413, 2013.
- [15] Q. Pu, J. Wang, and R.-Y. Zhao, "Strong authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 4, pp. 2609–2619, 2012.
- [16] S. Ben Othman, A. Trad, and H. Youssef, "Security architecture for at-home medical care using Wireless Sensor Network," in *Proceedings of the 10th International Wireless Communications and Mobile Computing Conference (IWCMC '14)*, pp. 304–309, IEEE, Nicosia, Cyprus, August 2014.
- [17] S. Kalra and S. K. Sood, "Secure authentication scheme for IoT and cloud servers," *Pervasive and Mobile Computing*, vol. 24, pp. 210–223, 2015.
- [18] A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal, "Healing on the cloud: secure cloud architecture for medical wireless sensor networks," *Future Generation Computer Systems*, vol. 55, pp. 266–277, 2016.
- [19] X.509—Wikipedia, <https://en.wikipedia.org/wiki/X.509>.
- [20] D. Johnson and A. Menezes, "The elliptic curve digital signature algorithm (ECDSA)," Tech. Rep. CORR 99-34, Department of C & O, University of Waterloo, 1999.

Research Article

Identity Recognition Using Biological Electroencephalogram Sensors

Wei Liang,^{1,2} Liang Cheng,³ and Mingdong Tang²

¹College of Mathematics and Econometrics, Hunan University, Changsha, Hunan 410082, China

²School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China

³Department of Computer Science and Engineering, Lehigh University, Bethlehem, PA 18015, USA

Correspondence should be addressed to Liang Cheng; cheng@cse.lehigh.edu

Received 30 June 2016; Accepted 19 September 2016

Academic Editor: Fei Yu

Copyright © 2016 Wei Liang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Brain wave signal is a bioelectric phenomenon reflecting activities in human brain. In this paper, we firstly introduce brain wave-based identity recognition techniques and the state-of-the-art work. We then analyze important features of brain wave and present challenges confronted by its applications. Further, we evaluate the security and practicality of using brain wave in identity recognition and anticounterfeiting authentication and describe use cases of several machine learning methods in brain wave signal processing. Afterwards, we survey the critical issues of characteristic extraction, classification, and selection involved in brain wave signal processing. Finally, we propose several brain wave-based identity recognition techniques for further studies and conclude this paper.

1. Introduction

Human biological features include various intrinsic physiological features (e.g., fingerprint) and behavioral features (e.g., signature). The emerging technology of mobile crowd sensing [1] and the recent rise of social bots [2] have added fuels to the research of identity recognition based on human biological features, which is a technique to authenticate human identity by using biosensors, fundamentals of biostatistics, and/or human biological features [3–6]. Generally, any physiological or behavioral feature can be used in identity recognition systems as long as it meets the following conditions: (1) universality, that is, every human being has this feature, (2) uniqueness, that is, different people present this feature differently, (3) stability, that is, it will not change within a period of time, and (4) collectability, that is, it can be quantitatively measured.

Traditional identity authentication techniques such as access codes, passwords, or IC (Integrated Circuit) cards may be vulnerable to identity loss, forgery, theft, or compromise since they are separated from human biological features. These techniques are widely used in information system

or web environment [7]. However, they have limitations in handling the challenges of forging. For example, one may use forged biological features, such as fingerprint, hand shape, palm print, face, iris, and human ear, to crack such systems [8]. Therefore, more research needs to be done and new approaches should be studied to address this challenge that throttles the development speed of identity recognition systems based on human biological features.

Brain wave is a unique biological feature that is hard to be forged. Recently, researchers attempt to apply brain wave techniques in identity recognition. Brain waves, as general bioelectrical phenomena, are generated by the ever-changing bioelectrical field in the human brain. Electroencephalogram (EEG) records brain waves along the scalp. Stimulations of different external signals will lead to different brain waves. Researchers may record the change of the bioelectric fields by inserting electrode(s) into the brain or using an electrode cap on the scalp to collect EEG data.

In an identity recognition system, as illustrated in Figure 1, there are multiple steps in processing the collected brain wave data, such as preprocessing, characteristic extraction, and validation. The classified characteristics will be matched

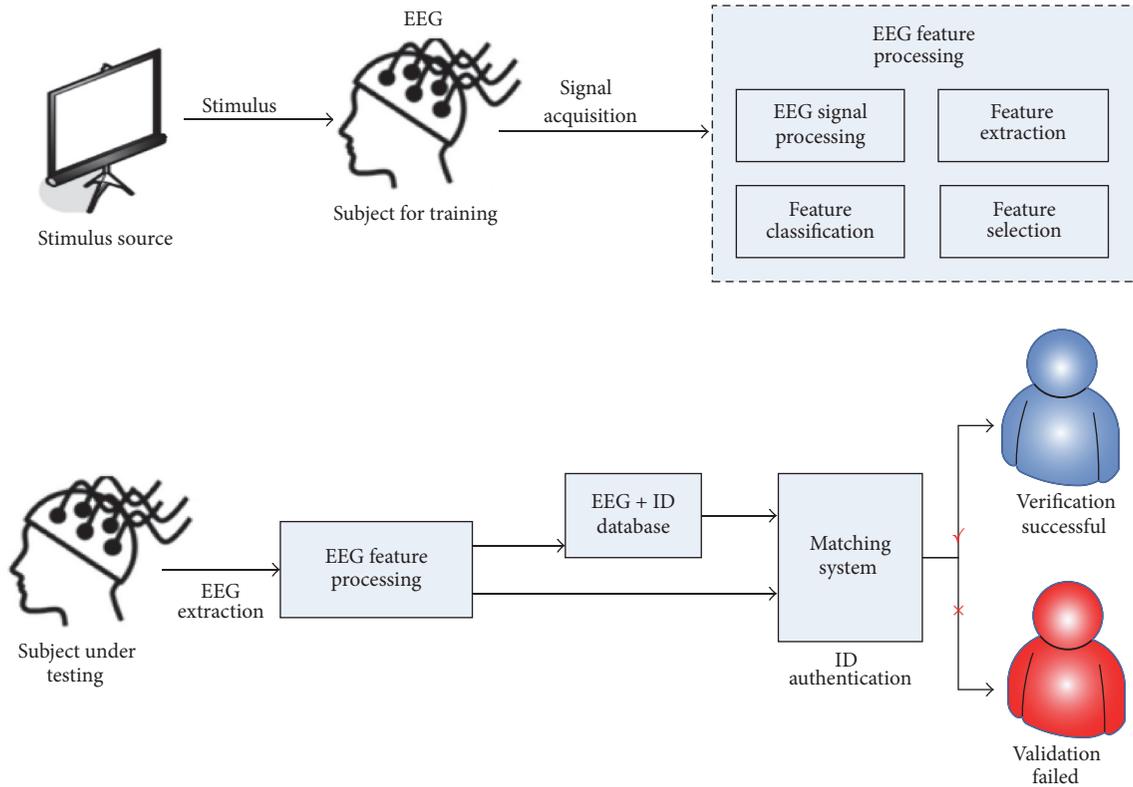


FIGURE 1: Brain wave-based identity recognition system.

with the data in a characteristic database. After calculating the posterior probability of each testing sample under an established model of human subjects, one can implement human identity recognition and authentication by using brain waves.

The rest of the paper is organized as follows. Firstly, we introduce the state-of-the-art brain wave-based identity recognition technologies by discussing the features and electrophysiological basics of human brain waves. Then, we describe the fundamentals and processes of collecting, extracting, selecting, and classifying brain wave features. Then we discuss how machine learning methods are applied in brain wave-based identity recognition systems. Finally, we conclude this paper with future work.

2. Electrophysiological Basics of EEG

Human brain is an important part of the central neural system, including cerebrum, cerebellum, and brain stem. Cerebrum is the most complex component with the largest brain volume and highest growth level. The surface of cerebral hemisphere is uneven and full of sulci and gyri. Several deep sulci divide cerebral hemisphere into four regions: the frontal, parietal, temporal, and occipital lobes. There are many small sulci developed across each lobe region, which extend the surface area of cerebral cortex. Different cortical regions control different nerve centers and undertake different tasks. Thus each region of cerebral cortex has its own function. Researchers have standardized the placement of electrodes for collecting and recording brain waves. The international

TABLE 1: Five frequency bands of EEG signal.

Activity	Frequency (HZ)	Characteristic of signals	Behavior
Delta	0.5–4	Slow wave	Sleeping
Theta	4–8	Slow wave Low frequency	Falling
Alpha	8–13	Fast wave	Relaxing
Beta	13–30	Fast wave high frequency	Psychical activity
Gamma	30–40	Fast wave high frequency	Stress mechanism

standard of 10–20 scalp electrode placement [9] is shown in Figure 2.

In different regions of cerebral cortex, the distribution of nerve cells is uneven and they have diverse structures. The potential collected by placing electrodes on scalp is not a reflection of potential variations of a single nerve cell but a synthetic effect of abundant neural activities. Therefore, the recorded brain wave signals of a series of potentials are regarded as an overlap of brain waves of different types generated in different brain regions. Generally, features of the potential series such as frequency, amplitude, and phase are used to describe brain waves. Under different states of brain activity, brain wave features will be different. As shown in Table 1 (five frequency bands of EEG signal), researchers categorize brain waves into multiple types based on their frequencies and locations, respectively, α , β , γ , δ , and μ waves.

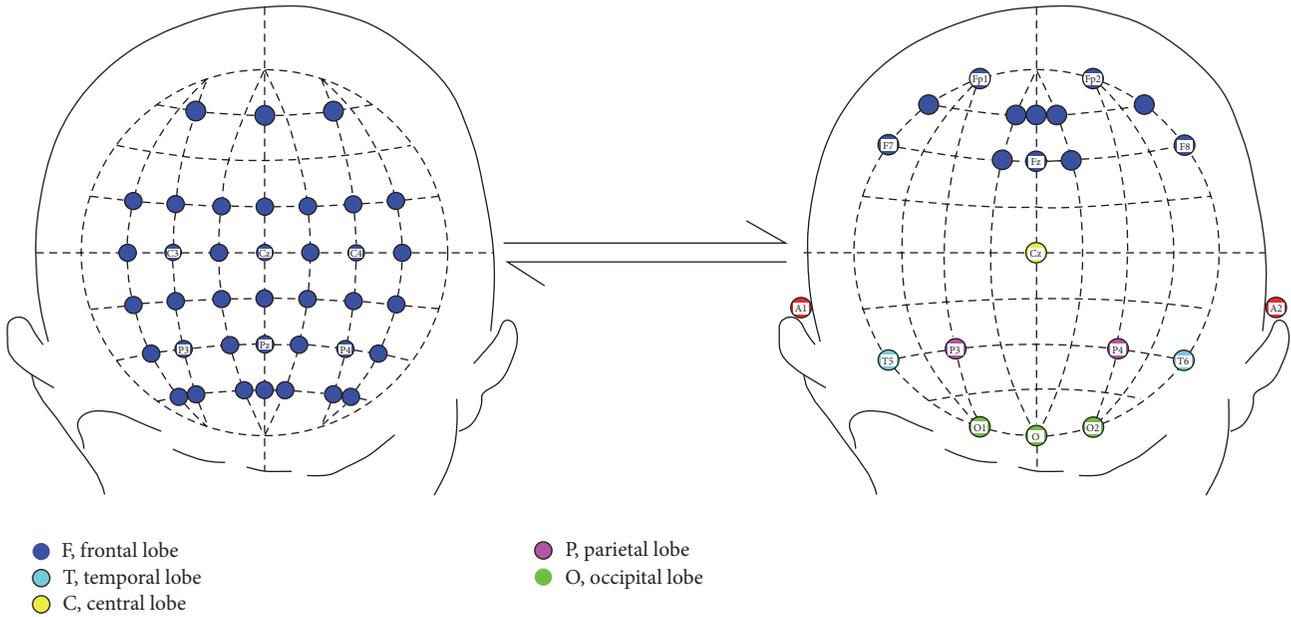


FIGURE 2: Placement of scalp EEG electrodes.

In previous work, researchers have tested different acquisition protocols for human recognition tasks such as relaxation with eye closed, EEG recordings based on visual stimuli, and performing mental tasks.

The blockage of μ rhythm is related to the ready state of movement. For example, human body movements, imagination, or behavior consciousness has great effects on μ rhythm. The amplitude of μ rhythm may be controlled by trained subjects. The use of μ rhythm for authentication control has received wide attention from researchers. β wave of relatively high frequencies is another commonly used wave in research and it is ubiquitous in human brain particularly in central and frontal areas. It is regarded to be closely associated with human thinking activities. For instance, β wave can be observed in EEG signals when a person is nervous or excited. γ wave is generated when a lot of nerve cells carry out an intensive cognitive activity or movement. It has the highest frequency and minimum amplitude among all types of brain waves. Appearance of γ wave demonstrates that the human brain is performing complex thinking activities or experiencing extreme excitements.

3. State of the Art

At present, research on individual identity recognition using EEG is still in its infancy. Existing studies can be roughly classified into two categories: EEG signal recognition during resting state and evoked EEG signal recognition. An overview of relevant research is illustrated in Figure 3.

3.1. Evaluation Criteria of EEG-Based Identity Recognition. There are three major criteria for evaluating the performance of EEG-based identity recognition systems.

(1) *Classification Accuracy.* Classification accuracy is defined as the ratio of the number of accurately classified samples

to the number of all samples. It is the most commonly used evaluation criterion to show the system feasibility.

(2) *Kappa Value.* Kappa value is a quantitative assessment to evaluate statistical consistence of EEG biological features. It takes into account accuracy of sample statistics and accuracy of random classification when samples are random. Moreover, Kappa can also be used to evaluate classification accuracy, robustness, and performance comparison as well. For multiple-category classifications, Kappa is better than classification accuracy. Kappa testing belongs to consistency testing method. It is utilized to test the difference between real consistency rate and random consistency rate. The calculation is described as formula (1). Here, p_0 denotes the real consistency rate and p_e is the theoretical consistency.

$$\text{Kappa} = \frac{p_0 - p_e}{1 - p_e},$$

$$p_0 = \frac{a + d}{n}, \quad (1)$$

$$p_e = \frac{(a + b)(a + c) + (c + d)(b + d)}{n^2}.$$

(3) *Rate of Security Recognition.* An EEG identity recognition system needs to recognize identity of each individual from brain wave, which entails high classification accuracy. High recognition accuracy is hard to achieve when brain waves have low signal to noise ratio. In this case, complexity of identity recognition algorithm will be improved by adding the number of recognizable tasks. Recognition rate of EEG data is an important index to measure the superiority of EEG identity recognition algorithm.

3.2. Analysis. Approaches proposed in references recognize an individual's identity by analyzing brain waves in her/his

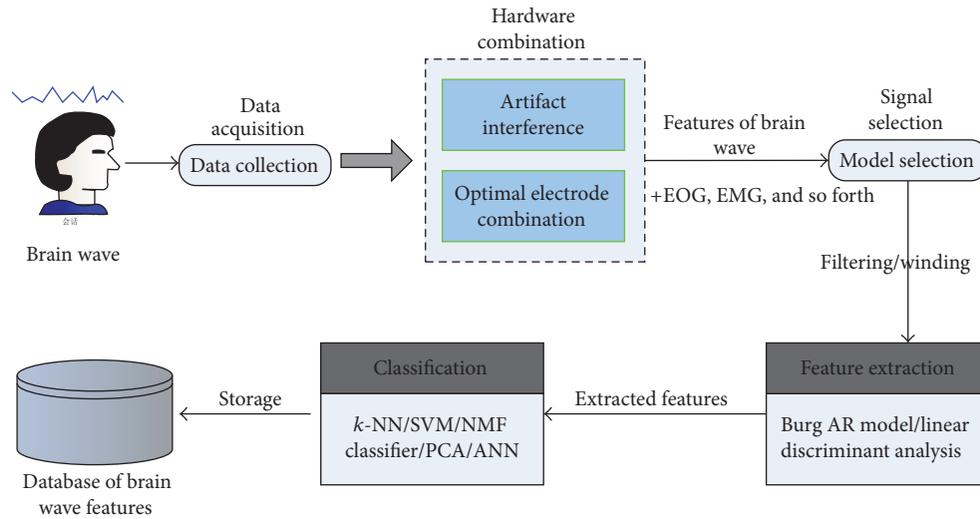


FIGURE 3: Overview of identity recognition based on EEG.

resting state, leveraging features of collected brain waves when the individual is sober and relaxed with eyes closed or open. Reference [10] utilizes principles of Lattice Equivalent Model and Levinson Recursion to generate autoregressive (AR) models with 3–21 orders. Nonlinear analysis is employed to analyze brain waves of forty persons in their resting states with eyes open and with eyes closed. Recognition is conducted using the data collected by one of the electrodes (P4 electrode). The security of recognition system is evaluated according to statistics of forty persons under coefficients of different orders. Bai et al. [11] proposed identifying a person by using the Visual Evoke Potential (VEP) of EEG signals. In this work, several techniques, such as Fisher Discriminant, Recursive Feature Elimination, and Genetic Algorithm, were introduced to reduce the utilized electrodes for less-intrusive user experience. They use a self-collected database of twenty subjects and select the data of 32 electrodes in experiment. The experimental results show that the best identification rate is 97.25% by using a Support Vector Machine classifier. Furthermore, the classification accuracy achieves 85% in experiments. In [12], the authors use variance and density of power spectrum to create characteristic vectors. Data from 23 participants are used in security evaluation. Finally, it achieves the security recognition rate of 79%. After that, Hema et al. [13] proposed an improved scheme. A modality for biometric authentication technique is reported by using brain EEG signals recorded during the performance of three mental tasks to identify six individuals. Using a three-layer feed-forward neural network, they classify brain wave data from six subjects according to thinking activities into four states (Multiplication Task, Reading Task, Spell Task, and Relax Task). Experimental results show that the average security recognition rate reaches 94.4% to 97.5%, significantly improving the performance on security recognition rate. In [14], an individual identity recognition algorithm based on brain waves is devised using a Gaussian mixture model. In the experiment, the subjects need to complete three repeated body tasks with uniform rhythm,

including left hand movement, right hand movement, and two-hand movement. Their results have verified that the Gaussian mixture model can remove noise signals such as those related to electromyography and eye movements when the subject is relaxed and thinking. The paper also shows that there are some mental tasks that are more appropriate for person authentication than others.

In the research of evoked brain wave recognition techniques, an approach proposed in [15] recognizes identity using Visual Evoked Potential (VEP). VEP is a bioelectricity activity induced by visual stimulations to the central neural system. It is an electrical signal of cerebral cortex that responded to visual stimulation, which represents the change of bioelectrical behavior after receiving external information. In [16], the authors propose that different VEP signals in time domain will be triggered by showing the subject with self-face and non-self-face. It could be utilized in person recognition. The prototype system is simple and with low recognition rates, indicating a great room for improvement. In [17], the authors conduct experiments based on 3,560 sets of VEP signals from 102 persons. There was a minimum of 10 and a maximum of 50 eye-blink-free VEP signals from each subject. Techniques used for feature classification include the k -Nearest Neighbors (kNN), Elman Neural Network (ENN) classifiers, and 10-fold Cross Validation Classification (CVC). Notably, it reaches the highest recognition accuracy rate of 98.12%. The experiments had clearly indicated the significant potential of brain electrical activity as biometrics. In [18], the authors synthesize individual brain waves of multiple tasks and extract data features in brain waves for identity recognition. This method matches brain waves with those from nine persons in database. The highest recognition rate is 95.6%.

In [19], the authors use Fast Johnson-Lindenstrauss Transform for robust EEG mAR coefficients hashing. The promising results suggest that hashing may open new research directions and applications in the emerging EEG-based biometry area. The authors of [20] adopt VEP signals

with frequency of 30–50 Hz and implement identity recognition by matching these signals against those of twenty persons in database. The feature vector utilizes coefficients of AR model and the peak value of power spectral density. Dimensionality reduction of features is performed using Fisher linear discriminate analysis. Finally, the kNN technique is employed to classify the data and the leave-one-out cross validation method is used for accuracy assessment, which leads to a correct classification rate of 100% [21].

4. System Analysis

4.1. EEG Data Collection

4.1.1. Hardware Sensor System for EEG Data Collection. Generally, EEG signal collection methods can be classified into three categories: embedding, semiembedding, and nonembedding [22]. An embedding collection method inserts microelectrode(s) or a microelectrode array into the cerebral cortex and collects electrical activities in aggregation of nerve cells, called Local Field Potentials (LFPs). This method can achieve high precision but may cause damage to nerve cells. In the semiembedding methods, electrodes are placed at the surface of cerebral cortex. Compared with the embedding method it has no damage to nerve cells. But both the embedding and the semiembedding methods are intrusive to the subject's body. Consequently, both ways usually apply in research on BCI technologies with subjects using animals or human beings with serious brain damage. Nonembedding methods use electrodes placed on the scalp surface and no intrusive operation is necessary. It has no damage to nerve cells and has advantages like usage convenience and device affordability. These advantages make the nonembedding way popular in BCI research. However, the drawbacks of nonembedding methods are obvious as well. For example, electrical signals of nerve cells which are detected at the scalp surface are weak due to signal attenuations across cerebral tissues, endocranium, skull, soft tissues, and so forth. The signals in different encephalic regions are mixed with interference signals, such as electromyography (EMG), electronystagmogram (ENG), and electrocardiogram (ECG). Thus the signal noise ratio of the collected EEG signals decreases, causing difficulty in extracting the useful EEG signals.

4.1.2. Available EEG Data Sets

- (i) EEG experiments can be conducted on basis of EEG data set on the website [23, 24]. EEGLAB is an open MATLAB tool box developed by Neural Computing Institute in University of California, San Diego, USA. Users can use independent component analysis or time/spectrum domain analysis in this tool box to analyze EEG signals.
- (ii) EEG data analysis and modeling center in Thredbo University, Germany, has provided many original EEG benchmarks (<http://www.fdm.uni-freiburg.de/EpilepsyData>) [25]. The benchmark suit contains many data about dynamic EEG analysis and prediction of epileptics.

4.2. EEG Data Processing. EEG signal processing can be divided into three steps: preprocessing, feature extraction, and classification [26]. Preprocessing is used to reduce noise interference and improve signal noise ratio, which includes band-pass filters, and so forth. The processed signals will be used for feature extraction, which extracts features from EEG signals to reflect intention of subjects. The classifier will classify features signals of EEG.

Original EEG data contains interference signals from sources other than brain activities. Therefore, it is necessary to process original EEG signals for noise reduction and SNR improvement. In different EEG systems, there are various preprocessing algorithms utilized, mostly antinoise filtering and optimal electrode combination.

4.2.1. Antinoise Interference. The procedure of EEG signal collection is easily affected by ocular artifacts, including nonphysiological and physiological interference. The former is interference caused by the environment or equipment, such as power frequency interference, environmental interference, variation of contact resistance between electrode and scalp, and relative slippage. Power frequency interference can be eliminated by 50 Hz trap filter or low-pass filter. Environmental interference may be noise distracting subjects or electromagnetic radiation in space. Moreover, when EEG signals are collected by wet electrodes, conductive paste is required between the electrodes and the scalp to reduce contact resistance, which may change during the experiment. In this case, researchers introduce anti-contact-resistance and anti-ocular-artifact approaches to address this issue. Interference of nonphysiological ocular artifact, including relative slippage caused by head movement, can be controlled by improving experiment methods while the majority of nonphysiological interference can be eliminated by filter technologies [27].

4.2.2. Optimal Electrode Combination. EEG signals are collected by multiple electrodes at different scalp spots of subjects. Each lead data reflects different neural activities [28]. However, not every lead data is helpful in improving the performance of identity recognition system. For example, in a visually evoked EEG experiment, lead data far from the visual cortex cannot be used to recognize identity. In addition, there may exist redundant EEG information among EEG lead data sets. Consequently, researchers utilize electrode selection algorithms for optimal electrode combination to reduce the number of electrodes needed, the preparation time of experiment, the cost of experiment, the EEG data size, and the computational complexity of EEG signal processing [29].

4.3. Applications of Machine Learning in EEG-Based Identity Recognition. As illustrated in Figure 1, after preprocessing EEG signals, for example, by methods described in Section 4.2, EEG feature selection, extraction, and classification are the next steps for EEG-based identity recognition as detailed in Figure 4.

As shown in Figure 4, the original EEG signals and stego data set are initialized. The features are effectively extracted and classified by using classification algorithms in machine learning. The classified features are matched and analyzed

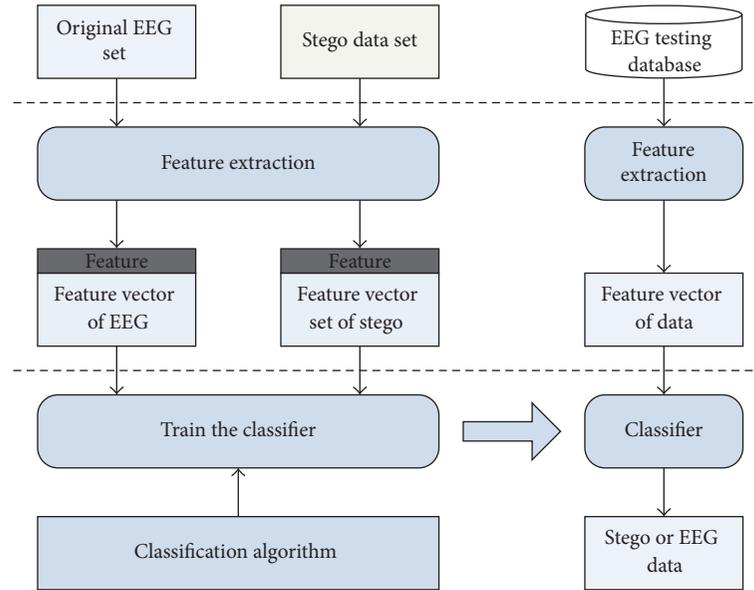


FIGURE 4: Flow of EEG signal processing.

with EEG testing database. Finally, the EEG-based identity authentication is implemented by comparison.

In this section we focus on discussing applications of machine learning methods for EEG-based identity recognition, in the feature signal preprocessing, selection, extraction, and classification, respectively.

4.3.1. EEG Signal Preprocessing. There are large amounts of high dimensional data in collected EEG signals, including noise, expression profile, and wave data. High dimensional data call for higher requirements of hardware storage and classifier selection. Dimension reduction technology can be employed to deal with dimension disaster and improve precision of classification algorithms. It also helps to improve visualization and data compression ratio. Generally, dimension reduction is required to reserve the effective expression of original data. Existing dimension reduction algorithms can be roughly classified into feature selection algorithms and feature extraction (subspace learning) algorithms. The former directly remove unrelated data from the original data, whereas the latter project high dimensional data into low dimensional spaces and fulfill dimension reduction transformation.

In existing EEG dimension reduction methods, data features of spatial samples in linear or nonlinear data set are usually projected in low dimensional spaces. The subset learning algorithms for dimension reduction can be divided into linear algorithms and nonlinear algorithms. The linear subset learning algorithms are based on traditional data optimization methods and the obtained data always have single variation. However, EEG dimension reduction under regularization framework should consider fusion of multiple features. For nonlinear dimension reduction, traditional algorithms mainly focus on study of flow learning. Regular nonlinear dimension reduction technologies usually concentrate on kernel method. In [30], the authors fulfill dimension

reduction by using a sparse subset learning method. Orthogonal discriminate information is added into sparse neighborhood preserving projects. It makes the data after dimension reduction keep a similar partial reconfiguration relationship with sparse neighborhood preserving projects. Meanwhile, margin maximization and partial reconfigurable relationship can be utilized to process EEG samples of the same kind.

4.3.2. EEG Feature Extraction. EEG is electrical signal of cerebral cortex responsible for stimulation and is biological activity variation of central nervous system after receiving external information. However, due to the delay from receiving stimulation to generating EEG signal, EEG amplitude and width are different for each person. So the time domain characteristic can be obtained. Since EEG has short duration time, the signal length is insufficient to evaluate frequency features.

EEG features extraction is among the key issues in identity recognition systems. Through measurements or computations, the objects to be recognized or classified usually yield many original features. In this situation, samples require a procedure of high dimensional spatial feature extraction. In other words, samples will be expressed in low dimensional spaces via projections. During this procedure, the most effective similar features will be extracted from original EEG features. Since features of different categories are usually different from each other, the noise elimination and dimensionality reduction technologies can be studied according to EEG features in time and frequency domains, as well as their application conditions. After eliminating noise, EEG signals record the amplitudes during a period, which cannot be used in identity recognition. In this scenario, it is necessary to classify and transform the time domain signals in order to obtain stable and unique features, autoregressive model coefficients, and power spectral density. These are common features of EEG identity recognition systems.

Another scenario is to mine the high-pass data of EEG signals. Previous feature selection algorithms mainly employ statistical approaches and boundary information. Reference [31] proposes selecting features by using sparse norm and demonstrates the rotation invariance of norm. Authors in [32] propose a generalized assistant function method to solve structural sparsity. This method greatly improves the efficiency of solving the structural sparsity problem, via taking advantage of parallelization. Authors in [33] exploit both global structure and partial structure of data in feature selection. It demonstrates that this way can improve recognition effects in supervised or unsupervised model size recognition. Reference [34] indicates that the recognition performance based on both partial boundary structure and global boundary structure is encouraging. However, the simulation parameters of the partial structure are required to be set manually. Results in [35] demonstrate that the 2 : 1 feature subset based on structural sparse norm has low redundancy.

In EEG feature selection, the high-efficient feature selection algorithms can be taken into consideration. An available method is to combine multiobjective regression and graph embedding using a uniform optimization model. This method is suitable for EEG feature selection, since constraints of structural sparse norm are added. The method is different from other methods and has two advantages: (1) it considers the features of global boundary information and partial structure of the EEG feature data when selecting EEG feature subset. Thus, the global structure and partial structure can be effectively maintained in EEG feature selection. Consequently, feature matching can be completed efficiently in EEG identity recognition. (2) The mutual interactions between data features are considered in the procedure of reducing dimension of EEG features. Thus, the reduction of processing efficiency caused by greedy methods is avoided. A batching method can be introduced for EEG features, in order to improve the processing speed and decrease the time complexity.

4.3.3. EEG Feature Selection. Feature selection is to select a group of distinguishing characteristic subsets from the original feature collection according to some optimization measurement(s). Usually, EEG data has multifeatures. The purpose of feature selection is to find the most effective features from the feature set of original EEG. The features in different classifications may also be aggregated using clustering methods. For example, with the extensive study on EEG feature data, authors of [36] consider the correlation between feature and response and the redundancy between features. A selection criterion algorithm based on the correlation and redundancy is proposed, which maximizes the correlation between feature subset and response.

4.3.4. EEG Classification. The design of classifier is a hot topic in EEG data processing and applications [37–40]. Traditional methods for EEG classifier design face the challenge caused by high dimension of EEG data sets, thus the classification result may have large deviations. Small sample size problem of EEG could lead to the overfitting phenomenon, which limits the application of traditional classifier. To address this issue, [41]

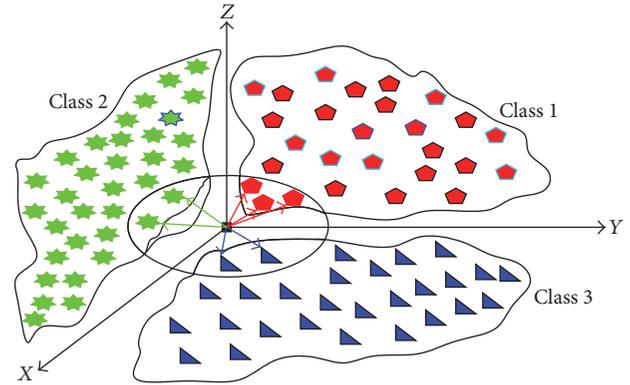


FIGURE 5: kNN query starts at the test point and grows a spherical region until it encloses k training samples, and it labels the test point by a majority voting of these samples. In this case, where $k = 7$, the test point would be labeled by the category of the red points.

has designed a no-argument sparse expression classifier by using a regularization method. This classifier has good robustness and does not need to set sparsity parameters manually. In EEG collection for different individuals, researchers can design effective crossing verification methods according to different sparsity parameters and select the optimal parameter model to address the small sample problem.

Authors of [42] have classified data features in database of epilepsy patients with brain disease. A classification method is proposed to distinguish normal and abnormal (epilepsy) EEG. Data mining of epilepsy EEG and complex signal processing are fulfilled by using theories such as chaos, the nearest neighbor, and systematic statistic time analysis. Results indicate that the proposed method can correctly classify normal and abnormal EEG data with sensitivity of 81.29% and specificity of 72.86%. As shown in Figure 5, the KNN method is employed to query in test point area of training data. Unknown test point will be marked red when $k = 7$. In this case, we can see “trained” data collection test points. Optimal positions of test points can be found quickly. Furthermore, the performance of EEG classification can also be greatly improved.

4.3.5. Discussion. EEG signals belong to biometric modality, which may be affected by multiple factors. It is not enough for the alone metric such as accuracy rate to represent the performance. In order to address these biological problems of EEG, an optimization model can be established for EEG identity recognition. Studies on this problem have developed several models. The models and their optimization not only can provide theoretical evidence for data processing in EEG identity recognition but also can offer a good practical reference for detection departments that engage in identity recognition for living bodies. In the research of EEG classification method, the high-pass technology makes the collection of EEG samples become easier. However, in practical sample analysis and application, low correlation and flexibility still exist in sample data. The reasons lie in two aspects. On one hand, deviations of techniques, hardware, and software reduce reliability of disease data, thus greatly

impairing the correlation of EEG data. On the other hand, biochemical experiments are usually expensive; thus only a small number of samples are used for mark. This issue raises a higher requirement for EEG data selection. Consequently, it becomes a key issue to select typical EEG samples for sample label design. A mathematical model for EEG sample selection is proposed.

Let F denote the characteristic function model of EEG, $X_c \in R^{m \times n}$ denote a sample dataset, and m and n , respectively, denote the number of samples and the characteristic dimension; a mathematical model for the original problem can be established as follows:

$$F = \min_{\beta, \alpha} \sum_{i=1}^m \|x_i - X_c^t \alpha_i\|^2 + \sum_{j=1}^n \frac{\alpha_{i,j}^2}{\beta_j} + \gamma \|\beta\|, \quad (2)$$

where $\chi^i \in X$, $\beta \geq 0$, $i = 1, 2, \dots, m$, and $j = 1, \dots, n$. $\alpha = [\alpha_{i,1}, \dots, \alpha_{i,m}]^T$ is a linear combination coefficient vector. The optimization model (2) has introduced a slack variable $\beta \in R^m$. The features of L_1 norm make vectors β and α sparse. Otherwise, the optimization process will fail.

As indicated in this model, (2) is a convex optimization problem. An alternative and iterative method can be employed to address this problem. The method, however, cannot be directly applied to feature dimension reduction of EEG due to its low convergence rate. In this regard, in order to improve the scaling ability of the original model, an assistant function should be found and further optimized to avoid excessive computation of gradient information.

5. Conclusions and Prospects

As understanding of the uniqueness of EEG signals increases, EEG is applied to more and more fields. It can not only realize anticounterfeiting and bioassay but also overcome the security issue of traditional biometric-based identity recognition. In this paper, we have highlighted the following perspectives. (1) Concerning EEG processing, we have reviewed a number of EEG preprocessing techniques and identified the limitation of existing methods. We have also discussed how to maximize the preservation of EEG characteristics when removing noises such as EMG and EOG. (2) Concerning feature selection and extraction, various common features of EEG are reported. We have also elaborated the advantages of supervised and unsupervised selection methods in dimension reduction of EEG data features. (3) We have placed an emphasis on the description of the design of various classifiers for EEG. Machine learning for EEG identity recognition systems is discussed as well. In summary, identity recognition based on EEG is still in its infancy and there is much work to be done in this area. Though various algorithms have been proposed, there is still significant room for improvement in both theory and practice, so as to meet the performance and cost requirements of person authentication using EEG under different states or from different devices.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work is supported by the National Science Foundation of China (Grant 61572188), Hunan Provincial Natural Science Foundation of China (Grant 2016jj2058), the China Postdoctoral Science Foundation funded project (Grant 140778), Scientific Research Project of Hunan University of Science and Technology (E51697), and Scientific Research Fund of Hunan Provincial Education Department (Grants 14A047 and 10C0689).

References

- [1] B. Guo, Z. Wang, Z. Yu et al., "Mobile crowd sensing and computing: the review of an emerging human-powered sensing paradigm," *ACM Computing Surveys*, vol. 48, no. 1, article 7, 2015.
- [2] E. Ferrara, O. Varol, C. Davis, F. Menczer, and A. Flammini, "The rise of social bots," *Communications of the ACM*, vol. 59, no. 7, pp. 96–104, 2016.
- [3] K. A. Nixon, V. Aimale, and R. K. Rowe, "Spoof detection schemes," in *Handbook of Biometrics*, pp. 403–423, Springer, Berlin, Germany, 2008.
- [4] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial gummy fingers on fingerprint systems," in *Proceedings of the Optical Security and Counterfeit Deterrence Techniques IV*, vol. 4677 of *Proceedings of SPIE*, pp. 275–289, Seoul, South Korea, May 2002.
- [5] B. Y. Hiew, A. B. J. Teoh, and O. S. Yin, "A secure digital camera based fingerprint verification system," *Journal of Visual Communication and Image Representation*, vol. 21, no. 3, pp. 219–231, 2010.
- [6] L. Zhang, L. Zhang, D. Zhang, and H. Zhu, "Online finger-knuckle-print verification for personal authentication," *Pattern Recognition*, vol. 43, no. 7, pp. 2560–2571, 2010.
- [7] S.-G. Wang, Q.-B. Sun, and F.-C. Yang, "Web service dynamic selection by the decomposition of global QoS constraints," *Ruan Jian Xue Bao/Journal of Software*, vol. 22, no. 7, pp. 1426–1439, 2011.
- [8] P. Kumari and A. Vaish, "Brainwave based authentication system: research issues and challenges," *International Journal of Computer Engineering and Applications*, vol. 4, no. 1, pp. 89–108, 2014.
- [9] R. W. Homan, "The 10–20 electrode system and cerebral location," *American Journal of EEG Technology*, vol. 28, no. 4, pp. 269–279, 1988.
- [10] R. B. Paranjape, J. Mahovsky, L. Benedicenti, and Z. Koles, "The electroencephalogram as a biometric," in *Proceedings of the Canadian Conference on Electrical and Computer Engineering*, Toronto, Canada, May 2001.
- [11] Y. Bai, Z. Zhang, and D. Ming, "Feature selection and channel optimization for biometric identification based on visual evoked potentials," in *Proceedings of the 2014 19th International Conference on Digital Signal Processing (DSP '14)*, pp. 772–776, Hong Kong, August 2014.
- [12] C. Miyamoto, S. Baba, and I. Nakanishi, "Biometric person authentication using new spectral features of electroencephalogram (EEG)," in *Proceedings of the International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS '08)*, pp. 1–4, February 2009.

- [13] C. R. Hema, M. P. Paulraj, and H. Kaur, "Brain signatures: a modality for biometric authentication," in *Proceedings of the International Conference on Electronic Design (ICED '08)*, pp. 1–3, Penang, Malaysia, December 2008.
- [14] S. Marcel and J. D. R. Millán, "Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 743–752, 2007.
- [15] S.-H. Liew, Y.-H. Choo, Y. F. Low, and Z. I. Mohd Yusoh, "Identifying Visual Evoked Potential (VEP) electrodes setting for person authentication," *International Journal of Advances in Soft Computing and Its Applications*, vol. 7, no. 3, pp. 85–99, 2015.
- [16] R. Palaniappan and D. P. Mandic, "EEG based biometric framework for automatic identity verification," *Journal of VLSI Signal Processing Systems for Signal, Image, and Video Technology*, vol. 49, no. 2, pp. 243–250, 2007.
- [17] R. Palaniappan and D. P. Mandic, "Biometrics from brain electrical activity: a machine learning approach," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 738–742, 2007.
- [18] S. Sun, "Multitask learning for EEG-based biometrics," in *Proceedings of the 19th International Conference on Pattern Recognition (ICPR '08)*, pp. 1–4, December 2008.
- [19] C. He, X. Lv, and Z. J. Wang, "Hashing the mAR coefficients from EEG data for person authentication," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '09)*, pp. 1445–1448, Taipei, Taiwan, April 2009.
- [20] R. Palaniappan, "Method of identifying individuals using VEP signals and neural network," *IEE Proceedings: Science, Measurement and Technology*, vol. 151, no. 1, pp. 16–20, 2004.
- [21] A. Yazdani, A. Roodaki, S. H. Rezatofighi, K. Misaghian, and S. K. Setarehdan, "Fisher linear discriminant based person identification using visual evoked potentials," in *Proceedings of the 2008 9th International Conference on Signal Processing (ICSP '08)*, pp. 1677–1680, Beijing, China, October 2008.
- [22] M. T. Arun, R. Am, K. Umar, and M. S. Owjany, "Human Brain Signals (EEG) based experimental authentication for secured devices," *International Journal of Scientific Engineering and Technology Research*, vol. 3, no. 27, pp. 5557–5560, 2014.
- [23] "UCI Machine Learning Repository: EEG Database Data Set," <https://archive.ics.uci.edu/ml/datasets/EEG+Database>.
- [24] <http://www.mathworks.com/products/matlab>.
- [25] "European Epilepsy Database," <http://epilepsy-database.eu/>.
- [26] R. B. Paranjape, J. Mahovsky, L. Benedicenti et al., "The electroencephalogram as a biometric," *Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering*, vol. 2, pp. 1363–1366, 2001.
- [27] R. Palaniappan, "A new method to identify individuals using signals from the brain," in *Proceedings of the Joint Conference of the 4th International Conference on Information, Communications and Signal Processing, and 4th Pacific Rim Conference on Multimedia*, pp. 1442–1445, Singapore, December 2003.
- [28] R. Palaniappan, "Recognizing individuals using their brain patterns," in *Proceedings of the 3rd International Conference on Information Technology and Applications (ICITA '05)*, vol. 2, pp. 520–523, Sydney, Australia, 2005.
- [29] R. Palaniappan and P. Raveendran, "Individual identification technique using visual evoked potential signals," *Electronics Letters*, vol. 38, no. 25, pp. 1634–1635, 2002.
- [30] L. Scrucca, "A geometric approach to subset selection and sparse sufficient dimension reduction," in *New Perspectives in Statistical Modeling and Data Analysis*, S. Ingrassia, R. Rocci, and M. Vichi, Eds., pp. 569–576, Springer, Berlin, Germany, 2011.
- [31] L. Du, Z. Shen, X. Li, P. Zhou, and Y.-D. Shen, "Local and global discriminative learning for unsupervised feature selection," in *Proceedings of the 13th IEEE International Conference on Data Mining (ICDM '13)*, pp. 131–140, Dallas, Tex, USA, December 2013.
- [32] D. Cai, C. Zhang, and X. He, "Unsupervised feature selection for multi-cluster data," in *Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 333–342, ACM, Washington, DC, USA, July 2010.
- [33] S. Gao, I. W.-H. Tsang, L.-T. Chia, and P. Zhao, "Local features are not lonely—Laplacian sparse coding for image classification," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR '10)*, pp. 3555–3561, June 2010.
- [34] D. Kong and C. Ding, "Efficient algorithms for selecting features with arbitrary group constraints via group lasso," in *Proceedings of the 13th IEEE International Conference on Data Mining (ICDM '13)*, pp. 379–388, Dallas, Tex, USA, December 2013.
- [35] C. Hou, F. Nie, D. Yi et al., "Feature selection via joint embedding learning and sparse regression," in *Proceedings of the 22nd International Joint Conference on Artificial Intelligence (IJCAI '11)*, vol. 22, pp. 13–24, 2011.
- [36] Y. Sun, S. Todorovic, and S. Goodison, "Local-learning-based feature selection for high-dimensional data analysis," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 32, no. 9, pp. 1610–1626, 2010.
- [37] S.-H. Liew, Y.-H. Choo, and Y. F. Low, "Fuzzy-rough nearest neighbor classifier for person authentication using EEG signals," in *Proceedings of the 2013 International Conference on Fuzzy Theory and Its Applications (iFUZZY '13)*, pp. 316–321, Taipei, Taiwan, December 2013.
- [38] B. W. Heumann, "An object-based classification of mangroves using a hybrid decision tree-support vector machine approach," *Remote Sensing*, vol. 3, no. 11, pp. 2440–2460, 2011.
- [39] K. Baskar, R. Kathirvel, and J. Sundararajan, "A novel classifier algorithm for EEG signal based person authentication from Cz channel with 2D-wavelet compression for the online voting system using touch panel," *Australian Journal of Basic and Applied Sciences*, vol. 8, no. 5, pp. 399–409, 2014.
- [40] M. Poulos, M. Rangoussi, N. Alexandris, and A. Evangelou, "Person identification from the EEG using nonlinear signal classification," *Methods of Information in Medicine*, vol. 41, no. 1, pp. 64–75, 2002.
- [41] B. Liao, Y. Jiang, G. Yuan, W. Zhu, L. Cai, and Z. Cao, "Learning a weighted meta-sample based parameter free sparse representation classification for microarray data," *PLoS ONE*, vol. 9, no. 8, Article ID e104314, 2014.
- [42] W. A. Chaovalitwongse, Y.-J. Fan, and R. C. Sachdeo, "On the time series K-nearest neighbor classification of abnormal brain activity," *IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans*, vol. 37, no. 6, pp. 1005–1016, 2007.

Review Article

Privacy Models in Wireless Sensor Networks: A Survey

J. M. de Fuentes, L. González-Manzano, and O. Mirzaei

Carlos III University of Madrid, Avenida de la Universidad 30, Leganés, 28911 Madrid, Spain

Correspondence should be addressed to J. M. de Fuentes; jfuentes@inf.uc3m.es

Received 23 February 2016; Accepted 8 September 2016

Academic Editor: Christos Riziotis

Copyright © 2016 J. M. de Fuentes et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Wireless Sensor Networks (WSNs) are attracting attention from the research community. One of the key issues is to provide them with privacy protection. In recent years, a huge amount of contributions has been focused on this area. Surveys and literature reviews have also been produced to give a systematic view of the different approaches taken. However, no previous work has focused on privacy models, that is, the set of assumptions made to build the approach. In particular, this paper focuses on this matter by studying 41 papers of the last 5 years. We highlight the great differences appearing among related papers that could make them incompatible to be applied simultaneously. We propose a set of guidelines to build comprehensive privacy models so as to foster their comparability and suitability analysis for different scenarios.

1. Introduction

The widespread network availability in modern societies, as well as the proliferation of connected devices that are routinely carried out by people, highlights the ubiquitous facet of today information technologies [1].

As a result of the abovementioned trend, our world is being transformed into a smart environment. Almost everywhere, there is a small sensor, receiver, or transponder with communication and processing capabilities. In order for this *smartification* to take place, sensors become a key element. Thanks to sensors, it is possible to perceive environmental conditions (temperature, humidity, etc.).

In order for these sensors to be effectively deployed, the concept of Wireless Sensor Networks (WSNs) comes into play. WSNs have received a great attention from the research community. As of January 2016, a general survey from Akyildiz et al. collected more than 15,000 cites on Google Scholar [2]. Thus, it is clear that there is a huge community behind this topic.

In this regard, WSN privacy needs have already been surveyed by several authors. Chow et al. [3], Tayebi et al. [4], Rios et al. [5], Gupta and Chawla [6], Oualha and Olivereau [7], Conti et al. [8], Bista and Chang [9], Alemdar and Ersoy [10], or Al Ameen et al. [11] are representative examples of systematic literature reviews on the matter. All of them focus

on the different techniques that are proposed by authors to address typical security and privacy needs.

The goal of this paper is rather different from previous ones. Instead of focusing on the approaches taken, this survey concentrates on the considered *models*. Models are formed of all assumptions made over the system. In a WSN scenario, three main sets of decisions can be identified (see Figure 1). First, general issues such as goals and threats have to be stated. Afterwards, how the network is supposed to operate has to be defined. Finally, the attacker capabilities and resources need to be specified.

It must be noted that different contributions may not work properly together if they rely upon different models. Thus, it is critical to have a clear view on the considered models to identify whether two or more mechanisms are compatible. To the best of the authors' knowledge, there is no such a survey in this field. The last contribution of this paper is a set of guidelines to build comprehensive privacy-related models. They will help to clearly define these models to improve the comparability (and compatibility, if it is the case) of different proposals.

To ensure the timeliness of our results, we have focused on 41 papers published in the last 5 years. Figure 2 shows the temporal distribution of the considered papers. It is clear that there are several papers (4 at a minimum) per considered year, which supports the soundness of our analysis.

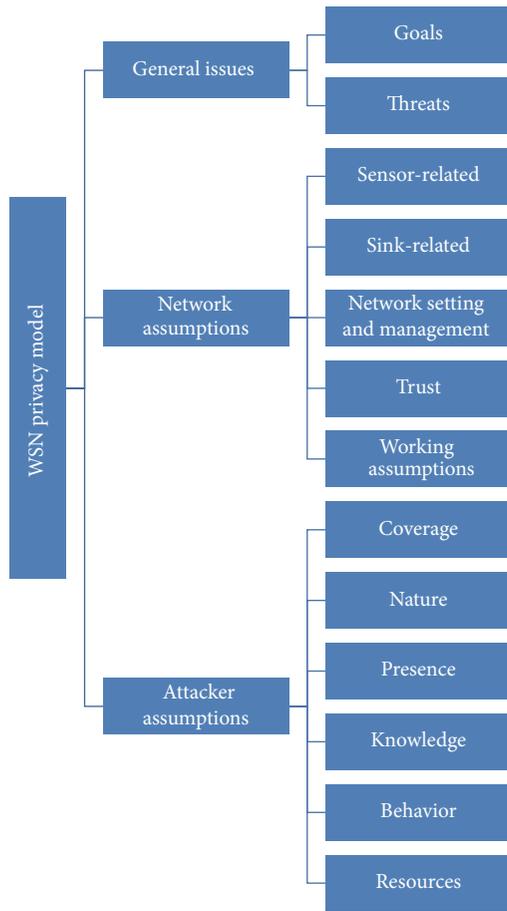


FIGURE 1: Privacy models in WSNs. Scheme of main decisions.

The paper is organized as follows. Section 2 gives a brief background on WSNs and the surveyed papers. Afterwards, the analysis is structured according to the decision sets shown in Figure 1. Thus, Section 3 focuses on the security goals and attacks that are at stake in the studied papers. Section 4 focuses on the assumptions made over the network itself. Section 5 describes the attacker capabilities. After the analysis on current works, Section 6 focuses on the guidelines to build privacy models. Finally, Section 7 concludes the paper.

2. Background

This section introduces the main concepts related to WSNs. Afterwards, the set of papers considered in this survey are briefly described. In particular, they are classified according to the followed approach. This enables showing the diversity of applied techniques, which supports the significance of the conducted survey.

2.1. Wireless Sensor Networks. A Wireless Sensor Network is formed by a set of sensors which are interconnected in an ad hoc fashion. Typically, it is assumed that sensors have a limited and nonremovable battery storage [2]. Their connectivity is usually ad hoc, so that they need to have a decentralized

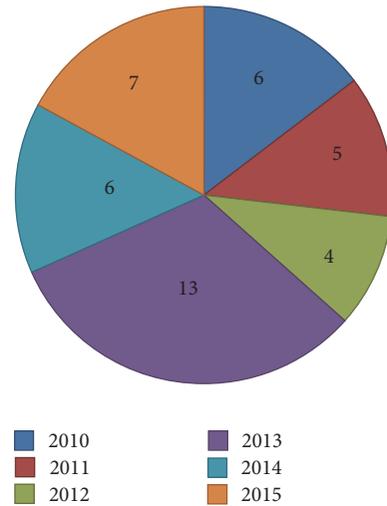


FIGURE 2: Distribution of papers per year.

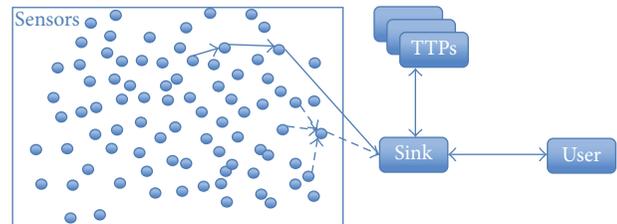


FIGURE 3: Scheme of a Wireless Sensor Network (WSN).

coordination. Thus, nodes share some information and carry out processing tasks in a distributed fashion. This is a typical feature of WSNs.

Apart from sensors, there are typically four entities in a WSN (Figure 3). On the one hand, the server or *sink* is the node that collects sensorial data. As it will be explored later on, this information may reach the sink either through direct routing (straight lines in Figure 3) or through some special sensors that collect data from surrounding ones (dotted lines in Figure 3). In order to make use of the network, the presence of a user is also assumed. Finally, Trusted Third Parties (TTPs) may also be considered to manage credentials and resolve disputes, among other issues.

These networks have been successfully applied in different applications and environments. Akyildiz et al. proposed a comprehensive enumeration of scenarios, ranging from military applications (e.g., reconnaissance) and environmental ones (e.g., tracking animals) to home uses (e.g., smart environments) [2]. In the last years, researchers have also explored their security issues related to their use in automated factories [12].

2.2. Classification of Considered Papers. The set of considered papers are devoted to different privacy-preserving goals. This section analyses the approaches followed on each work. This ensures that diverse techniques are considered and thus that

TABLE 1: Techniques. (x): technique assumed by authors as already existing.

	Encryption	Routing	Aggregation	Packet injection	Anonymity/ k -anonymity/pseudonymity	Statistics
[44]		x		x	Anonymity	
[39]		x				
[30]	x	x				
[22]			x	x		
[28]					k -anonymity	
[25]	x					x
[52]		x		x		
[29]				x		
[31]		x	x		Anonymity	
[21]		x				
[34]					Pseudonymity	
[20]		x		x		
[49]	x		x			
[53]	x					
[16]	x (+ ring signature)				Pseudonymity	
[46]		x		x		
[50]					Pseudonymity	
[35]				x		
[54]			x			
[13]	(x)	(x)				
[14]	x			x	Pseudonymity	
[24]				x	Anonymity	
[38]		x				
[18]	(x)	x		x		
[47]		x				
[48]			x			
[26]			x			x
[42]	x				Pseudonymity	
[27]		x	x			
[45]	x		x			
[15]	(x)	x		x		
[19]	x	x		x	Pseudonymity	
[32]	x					
[23]	x	x		x		
[17]	x				Pseudonymity	
[43]	x		x			
[36]	x					
[33]	x					
[37]	x					
[40]	x	x	x			
[41]	x	x	x			

the survey is representative of the different directions in this field. Additionally, since papers are from the last 5 years, this section gives an up-to-date vision on the research trends in WSN privacy.

Figure 5 summarizes the different considered techniques, namely, encryption, routing, packet injection, aggregation, pseudonymity, anonymity/ k -anonymity, and statistics. At a first glance, it may be seen that the total sum of techniques

appearing in papers exceeds the size of the studied sample (i.e., 41 papers). This is because 25 out of 41 papers combine two or more techniques. Table 1 details this issue.

Around half of the papers make use of encryption. It is a reasonable decision since these mechanisms have already been applied to different network scenarios for long time ago. Therefore, existing algorithms may be adapted to the WSN constraints with relative easiness. One important remark is

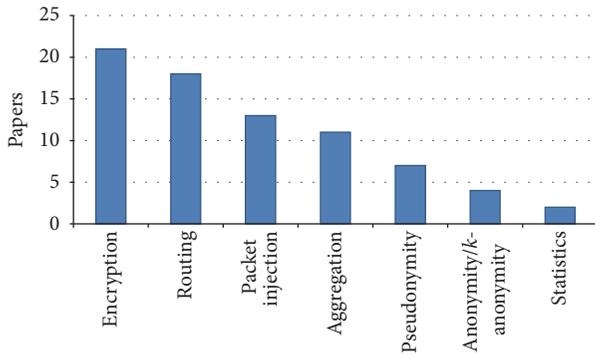


FIGURE 4: Classification of applied techniques.

that [13–15] do not explicitly adopt this mechanism as part of their approach. However, considering their description, it is clear that it comes into play.

Encryption is not the only pure-cryptographic mechanism at stake. Papers [16, 17] combine it with digital signatures. In particular, [16] applies ring signatures whereas [17] uses signcryption. This technique combines both digital signature and encryption at once. In both cases, the goal is to offer both sender anonymity and authenticity of data and its origin.

The second most popular technique is routing. More precisely, the preferred choice is to design a novel routing algorithm to demonstrate that the attacker cannot track a given packet back to its source. For this purpose, [15, 18–20] make use of fake sources and sinks to mislead the attacker. Another alternative is to use special kinds of routing such as tree routing. In particular, [20] proposes a diversionary tree routing in which packet paths cross themselves so that it is difficult for the attacker to track the actual path.

Proposed routing approaches may also leverage on the different types of considered nodes (see Section 4.1). As an example, in [21], routing is performed by specific nodes (called data mules) which are able to move around the network. This enables proposing algorithms which do not need to only rely upon static nodes.

Related to routing is the use of packet injection. In fact, most papers apply both techniques together. This approach bases on creating fake messages that are sent in the network. This technique comes at the cost of wasting some network and computation resources. Given that these are constrained aspects in WSNs, approaches are focused on how to apply this technique while maximizing the network lifetime. On the other hand, a critical aspect is to suitably inject messages to avoid real events tracking. Thus, papers such as [22] or [23] involve an opportunistic approach in which fake packets are only inserted when events come into play. Another option is taken by [24], in which packets are injected following a particular probability distribution. Systematic approaches in which randomness is not considered have also been proposed. For example, [18] makes a node to inject as many dummy packages as children nodes have.

Combining packet injection and encryption is not straightforward. One important remark in this regard appears

in [25]. In that work, authors propose that encryption mechanism must be semantically secure, since it prevents the attacker from distinguishing between relevant messages and useless ones. This statement should be considered in all papers combining the two said techniques.

As the fourth most common technique, aggregation has gained research attention in the last years. One of the main reasons is that it allows reducing the amount of transmitted data. This procedure requires some form of organization among nodes. Thus, some of them become aggregators and have to carry out their operations. The process of selecting nodes as aggregators may either be done randomly or be the consequence of the applied routing algorithm. For example, aggregation trees are chosen in [26].

Another key reason for aggregating is that the sink might not always be present. This situation especially happens when the sink is moving around the network. Thus, in [27], a buffer-based aggregation is proposed while the sink is out of range.

The use of anonymity and pseudonymity is among the least applied techniques. It is worth mentioning that [28] focuses on a particular type of anonymity, called k -anonymity, in which each node becomes unidentifiable in a set of at least k elements. This lack of acceptance among researchers may be due to two reasons. On the one hand, it requires an additional identity management infrastructure to set pseudonyms for each node. This assumption may not be suitable for big-scale or harsh scenarios. On the other hand, full anonymity may not be required since nodes may get compromised. Thus, it may be potentially necessary to reveal the identity of the node in case it spreads false information or performs malicious actions.

The last technique is the use of statistical procedures for privacy preservation. This is only applied by [25, 26]. On the one hand, [25] proposes a statistical metrics to determine how private the location of the source is. For this purpose, it analyses the packets exchanged by the node. As the outcome is a metrics, [25] does not aim to solve the privacy problem by itself, but it is helpful to measure the effectiveness of other proposals. On the other hand, [26] enables determining whether a WSN is compromised or not by examining the result of an aggregation. To this end, the said result is statistically analysed, checking the likelihood of having been produced by a collusion of malicious nodes. Thus, [26] is a relevant complement for other aggregation mechanisms.

3. Privacy Goals and Threats

From a broader point of view, the most general aspects that have to be addressed by a privacy model are the pursued goals and the considered threats. This section focuses on each of these aspects for all the surveyed works. For the sake of clarity, goals are addressed in Section 3.1 whereas threats are studied in Section 3.2. Refer to Tables 2 and 3 for an in-depth comparison among papers.

3.1. Goals. Even if privacy seems a single requirement, it involves several goals that may be achieved to a different extent.

TABLE 2: Goals analysis.

	Location privacy: source/sink/both	Data confidentiality	Anonymity	Access control	Authentication
[44]	Both				
[39]	Source				
[30]		x (query)			
[22]		x (sensor data)			
[28]	Source				
[25]			x (source)		
[52]	Sink				
[29]		x (events)			
[31]		x (query)	x (aggregator)		
[21]	Source				
[34]			x		
[20]	Source				
[49]		x			
[53]		x			
[16]		x (events)			
[46]	Source				
[50]	Source				
[35]			x (source)		
[54]		x			
[13]				x	
[14]	Both				
[24]	Source				
[38]	Source				
[18]	Source				
[47]	Both				
[48]					
[26]		x			
[42]	Source				
[27]	Sink				
[45]					
[15]	Both				
[19]	Source				
[32]		x (query and query results)			x
[23]	Source				
[17]				x (query and query results)	
[43]					
[36]					x
[33]				x (query and query results)	
[37]					x
[40]		x			
[41]					

TABLE 3: Threat analysis.

	Eavesdropping/traffic analysis	Query revealing	Authentication and privacy: tracking (default)/impersonation (when noted)
[44]	x		x
[39]			x
[30]	x		x
[22]	x		
[28]			x
[25]			
[52]	x		x
[29]	x		
[31]	x		
[21]	x		x
[34]	x		x
[20]	x		
[49]	x		
[53]	x		
[16]	x		x
[46]	x		
[50]	x		
[35]	x		x
[54]	x		
[13]	x		x
[14]	x		x
[24]	x		x
[38]			x
[18]	x		x
[47]	x		
[48]	x		
[26]	x		
[42]	x		x
[27]			x
[45]	x		
[15]	x		x
[19]			
[32]		x	
[23]	x		x
[17]	x	x	x (impersonation)
[43]	x		
[36]			x (impersonation)
[33]	x		
[37]			x (impersonation)
[40]	x		
[41]			

Particularly, the considered papers address five privacy-related goals (Figure ??): location privacy, data confidentiality, anonymity, access control, and authentication. We discuss each one separately.

The most common privacy goal in WSN-related contributions is source location privacy. The main reason behind it is that WSNs are usually devoted to detecting events. These events depend on the particular sensor capabilities: a fire may

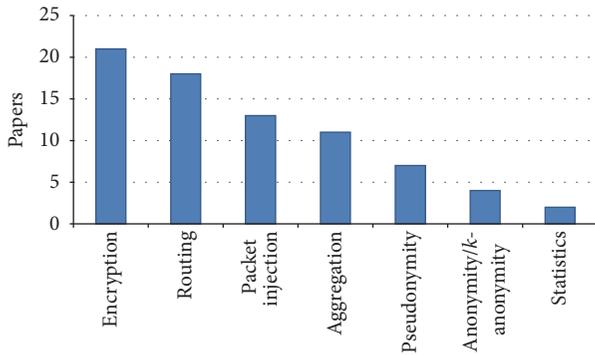


FIGURE 5: Classification of applied techniques.

be the event if temperature sensors are in place, or a burglar appearance may be the target when presence sensors are used. One key remark is that the location of events may be relevant for unauthorized parties. For example, knowing where the alarm has been raised makes it easier for attackers to predict which zones may receive less attention for a period of time, since the staff will be focused on stopping the detected threat.

A similar reasoning can be applied to the sink node location. Given that most WSNs rely upon a unique node to collect their perceived events, discovering the location of such a node is critical to destroy the network. A typical example is the military scenario, in which sensors make alert on the presence of enemy troops. Once the sink is neutralized, all defenses will be unaware of the events perceived by perimetral detectors. Despite its potential practical relevance, it is the privacy goal with the lowest research attention. However, the interest rises when addressed jointly with source location privacy.

The second need in terms of relevance is data confidentiality. This is the focus of several papers, although they refer to different information pieces. There are three elements to protect. First, sensor data may be relevant itself [22]. Second, events, that is, special reporting by sensors when their perceptions are beyond a given threshold, are also critical [16, 29]. The third information element are queries and their results. The concept of query appears in WSNs in which there is a stakeholder (e.g., a supervisor) that can retrieve the network information on demand. Therefore, privacy preservation may be applied over the query itself, as it may leak hints on the interests of the stakeholder [30, 31]. On the other hand, given that query results show the network status according to that request, it is also a relevant matter for attackers [32].

Mainly related to queries, access control is a privacy-preserving goal in WSNs for a small subset of works. Particularly, only [13, 17, 33] are concerned with queries. The issue here is not only related to the confidentiality of information but also ensuring that only authorized parties may have access to that information.

Anonymity and authentication are among the least relevant goals. Papers [25, 34, 35] focus on providing sensor anonymity. This feature is related to the location privacy mentioned so far: if the node remains anonymous, it is not

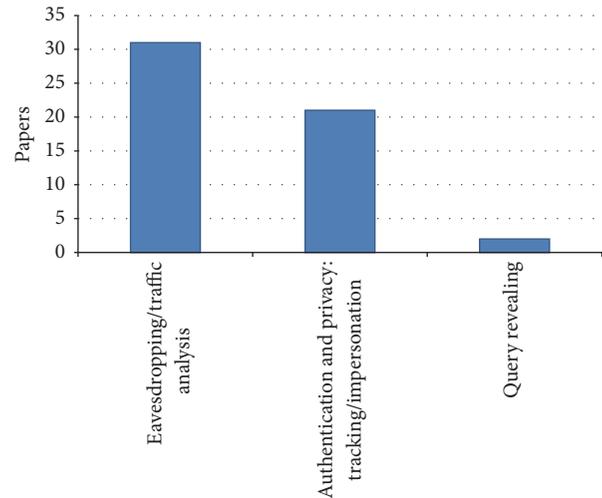


FIGURE 6: Considered threat distribution.

possible to distinguish it from others, thus avoiding location tracking. A similar approach is taken by [31], in which it is the aggregator node that remains anonymous. In this way, it is not possible to determine which node performed an aggregation. This is a similar protection to avoid compromising such a critical node within the network. However, this guarantee may be removed in case of misbehavior.

With respect to authentication, there are two possible variants, namely, entity authentication and data authentication. Papers [36, 37] offer mutual entity authentication, which means that both parties are sure on the identity of their counterpart. Data authentication is on the focus of [32]. It is noteworthy that this goal is specially relevant in aggregation-related approaches, since it is important to verify if the result of the operation is trustworthy.

3.2. Threats. Goals addressed in these papers have a direct link with the types of threats that WSNs may face. From a general point of view, the goals deal with data privacy and entities privacy. As a result, there are three main threats in this context (Figure 6): eavesdropping and query revealing (for data privacy) and authentication threats (for entities privacy).

Regarding data privacy, eavesdropping is by far the most common threat. It refers to the fact that an unauthorized entity may observe the contents of communication. One important aspect is that this threat might not be useful for learning the content itself but for discovering the involved nodes. This threat is usually referred to as *traffic analysis*, as it involves studying all traffic-related factors (e.g., sending-destination nodes, route taken, and frequency).

On the other hand, query revealing is at stake in a small subset of works. This trend is reasonable taking into account that only a reduced sample of considered papers dealt with the goal of access control to queries (recall Section 3.1).

Regarding entities' privacy, authentication threats are divided into tracking and impersonation issues. Tracking refers to the ability of the attacker to follow the physical situation of a given node. Recalling that location privacy is

the most relevant goal to achieve (cf. Section 3.1), the high impact of this threat is coherent. Most works are devoted to either rendering tracking impossible or at least reducing its success rate.

On the other hand, impersonation is addressed in [17, 36, 37]. This threat deals with the chance of a given entity to pretend to be another one. These works focus on avoiding this threat for access control purposes, thus ensuring that only authorized entities (and not third parties instead of them) can access some data.

4. Network Assumptions

Once goals and threats have been stated, the next issue to consider in a WSN privacy model is the network setting. Network assumptions may refer to the different elements that form the WSN or to external conditions in which the system is supposed to operate. This section focuses on these aspects. Sections 4.1 and 4.2 concentrate on sensors and sinks. How the network is managed is addressed in Section 4.3. Trusted elements are shown in Section 4.4 and finally Section 4.5 focuses on working assumptions. For the sake of clarity, tables contain an in-depth description of each aspect (Tables 4 and 5).

4.1. Sensor Assumptions. Sensor assumptions particularly focus on the type of sensor to apply, the information known by sensors, and sensors behavior.

The main aspect is that most works do not make any consideration regarding the type of sensors. In particular, only 4 papers mention that sensors must be static. On the other hand, paper [29] specifies that sensors are moving but at a uniform constant speed. The rest of the papers simply make no distinction. It must be noted that this decision has a direct impact in the soundness of the approach taken. One example is proposing a routing-based solution, that is, a specific mechanism to route packets in such a way that they avoid typical threats such as eavesdropping. If nodes are moving, there is a nonstraightforward need to maintain the routes. Without an explicit decision on this matter, this aspect may be overlooked.

Regarding the information known by sensors, a total amount of 16 papers makes a statement in this regard. There are three main elements that are explicit, namely, location, cryptographic keys, and identifiers. With respect to location, 4 papers assume that sensors know their own location (e.g., [38]) whereas 2 also consider that of the sink. Additionally, two papers determine that sensors know the identifier of the area in which they are placed; this is a relaxed form of location knowledge. Concerning keys, 9 papers assume that nodes know (from the beginning) either a shared key with the sink (e.g., [39]) or at least the sink's public key (e.g., [30]). In both cases, this is necessary to allow a confidential communication between these parties. Finally, 3 papers mention that each sensor has a unique identifier. This has direct implications in terms of the degree of privacy that has to be achieved; if sensors need to use such an identifier, it is necessary to build a mechanism to avoid revealing it to unauthorized parties.

With respect to the sensors behavior, there are two issues to note. First, several papers consider different classes (or roles) among sensors. These classes are linked to the type of mechanism, that is, considered. One typical assumption is that there are specific roles with extended attributions. As an example, aggregation nodes are in charge of receiving and putting together all information received from regular sensors [40, 41]. The second note regarding their behavior is that three papers assume that sensors are synchronized with the sink. Given that these networks may involve hundreds or thousands of nodes, such an assumption heavily limits the applicability of the proposal to specific scenarios.

4.2. Sink Assumptions. Sinks have particular properties to study. Specifically, the amount of entities that play the sink role, as well as the sink behavior, are analysed in the following.

The existence of a sink is mentioned in the vast majority of considered papers. However, they have great differences concerning its nature. One of the first aspects is that the amount of sinks is not usually explicit. Although several authors highlight that this is a single entity (e.g., [42, 43]), [30, 32] assume that there are several instances of it. Moreover, this issue is also part of the approach taken by authors in [18], as they propose several fake sinks to protect the single actual one.

The sink behavior is also subject to assumptions. Particularly, papers such as [15] consider that it is a static entity, whereas other authors [27] consider a moving one. In between, [44] admits both variants.

4.3. Network Setting and Management. WSNs are usually characterized by their simplistic network scheme in which the information flows between two entities, namely, sensors and sink(s) (recall Section 2). However, this vision hides different network topologies that are assumed by authors.

One outstanding organization scheme is the use of clusters or cells. In this way, sensors are separated into groups, usually based on their actual location. The typical setting is that there is one cluster head which is in charge of intercluster communication, whereas intracluster communication is direct among members. This setting is adopted by 9 of the considered papers, such as [45].

Apart from clusters, ring schemes are also considered in [31, 46]. Thanks to rings, nodes are virtually connected to another pair of neighbours (precedent and posterior in the ring). It is clear that this organization has a great impact on routing. However, to decrease predictability, some authors consider that sensors are organized into several rings and messages may flow from one to another.

It is noteworthy that an explicit mention to the network topology is not always given. Moreover, two papers state that their approach is applicable to any network topology [28, 47].

The last critical mention in this regard is the routing assumptions. Even if routing is one of the key mechanisms proposed by authors in recent years (see Section 2.2), there are several routing-related assumptions in the considered papers. Particularly, [44] assumes that communication from sensors to sink is done by flooding. In order to route packets, they rely

TABLE 4: Network assumptions: source and sink issues.

	Sensors: static/moving	Sensors: known info	Sensors: behavior	Sensors: capabilities	Server/sink
[44]					One, static, or moving
[39]		Shared key with sink	Cluster head and cluster members		
[30]		PK server			Set of independent, mutually untrusted servers
[22]		Global secret			
[28]		Own location Server location	Cooperate among themselves		Untrusted server
[25]			They broadcast fake messages		
[52]					
[29]	Moving sensors (uniform constant speed)				
[31]		Shared key with an "operator" which works through a gateway (or directly if it is close enough)	Leaf nodes and aggregator nodes		
[21]	Static ones and moving ones (data mules)	Own location (data mules)	Data mules do not communicate with each other. They move randomly	Greater communication coverage (data mules)	
[34]					
[20]		Own location, neighbours location, sink location			
[49]			Leaf nodes and aggregator nodes		One
[53]	Moving				
[16]					
[46]					One
[50]	Static	Unique ID	Cluster heads randomly chosen		
[35]		Predistributed shared key with any other node and with the base station			
[54]	Static (same cluster)		Cluster head and cluster members		Unconstrained
[13]					Privacy-enhanced base station
[14]			They can masquerade their MAC They are synchronized		One
[24]		Cell ID	Cluster head and cluster members		
[38]		Area ID			
[18]					One real, several fake
[47]	Static ones and moving ones			From low resources to high resources	
[48]					
[26]					
[42]		ID and location			One
[27]		Shared key with sink			Moving

TABLE 4: Continued.

	Sensors: static/moving	Sensors: known info	Sensors: behavior	Sensors: capabilities	Server/sink
[45]			Cluster heads and cluster members		
[15]	Static			Limited	Static
[19]	Static	Unique ID, shared key with sink, key for IBC		Limited	Static
[32]		Unique ID, shared key with user	Synchronized with sink		Several, untrusted
[23]					One but several allowed
[17]		Public key of owner and TTP			One
[43]		Shared key with neighbours			High resource, tamper-resistant
[36]		Long-term key shared with the sink		Vulnerable to tampering	One
[33]			Synchronized with sink		Unconstrained Secure channel with authentication server
[37]					
[40]			Leaf nodes and aggregator nodes		
[41]			Leaf nodes and aggregator nodes		

on an initial beacon sent by the sink at the beginning. In order to prevent overloading the network and, more specifically, the capacity of nodes, each one applies a policy to decide on whether to accept or reject the packet.

4.4. Trust Issues. Trust issues are also controversial. These are specially relevant since they identify which elements are reliable. Sensors and sinks are two of the elements that may or may not be trusted. In particular, [28, 48] assume that sensors and their connectivity are trusted, whereas [23, 36] do the same for the sink. On the contrary, papers such as [30, 32] consider that they are untrusted.

On the other hand, the network itself (i.e., communication channels) may be trusted as well. In particular, [44] assumes that the network is trusted for a period of time T_{\min} after deployment of nodes. The last aspect to consider in this regard is the use of third parties and, in particular, the existence of Trusted Third Parties (TTPs). Several papers assume that there are authentication managers or other related entities. However, it is remarkable that [33] does not assume the existence of TTPs. This is interesting to ensure the applicability of the proposal in harsh environments (e.g., military scenarios).

4.5. Working Assumptions. Working assumptions are statements made about the status of the system, particular features of the scenario, or elements that are supposed to exist for the mechanism to operate properly. There are essentially two aspects: cryptographic and contextual aspects. Regarding cryptography, key management is sometimes taken for granted [20, 37]. A similar assumption is made in [49], which

considers that a random key distribution scheme has already been applied.

Contextual aspects are related to how the scenario has to be. In this regard, the main issue is to define how events will happen. Two main decisions are taken in this regard. First, [31, 50] consider that time is slotted and that only one event may happen per slot. On the other hand, [29] assumes that events follow a probability distribution, initiate in the WSN perimeter, and end at some point inside the network. Thanks to these decisions, simultaneous or truly random events are not considered. Even if they impact the suitability of approaches for some realistic settings, other scenarios are totally applicable. For example, WSN-enhanced monitoring facilities in which measurements are taken periodically (say 5 seconds) may be compatible with the slotted-time assumption.

5. Attacker-Related Assumptions

Previous sections have focused on the privacy goals and threats and how the network is organized. This section addresses the last group of assumptions (recall Figure 1): attacker capabilities. They are critical to assess the degree of impact that threats may have. To make this analysis, the criteria by Back et al. (coverage, nature, and presence) are taken as a basis [51]. Furthermore, its assumed knowledge and behavior are also studied. Table 6 shows the analysis per paper.

The attacker coverage refers to its area of influence. Typical assumptions in this regard are that the attacker is *local* or *global* (Figure 7). The most common assumption is to have global attackers that can affect the whole network

TABLE 5: Network issues: management and trust.

	Network	Clusters/regions	Trusted issues	Working assumptions
[44]	Sensor-sink communication by flooding Routing bases on an initial beacon Each neighbour decides to accept/reject a packet using policy		Network is trusted for a period T_{\min} after deployment	Set of authentication-encryption protocols in use
[39]		x		
[30]		x		
[22]	Tree routing			
[28]	No need for any specific topology Communication with server is anonymous		Sensors and sensor-sensor connectivity	
[25]				
[52]	The destination ID for each packet (i.e., the sink) is encrypted			
[29]				Events follow a probability distribution; initiate on a random location of the WSN perimeter; eventually terminate within the network
[31]	Ring	x		Time is slotted, one event per slot
[21]		x		
[34]				
[20]				Key management exists
[49]				Random key distribution scheme (e.g., Gligor)
[53]				Mobile environment
[16]				
[46]	Ring			
[50]		x		
[35]				Time is slotted, one event per slot
[54]	Sensors randomly scattered	x		
[13]	WSN-suitable routing			
[14]				
[24]		x		
[38]				
[18]				
[47]	Arbitrary topology			
[48]			All components are trusted	Set of authentication-encryption protocols in use
[26]				
[42]		x		
[27]				
[45]		x		
[15]				
[19]				
[32]				
[23]	Homogeneous distribution of nodes		Sink is trusted	Encrypted messages are sent periodically
[17]				
[43]				Random key distribution scheme (e.g., Gligor)
[36]			Sink is trusted	To query a sensor data: need to be registered in the sink and have a smartcard
[33]			No TTPs. Law authority has limited trust	
[37]				Key management exists
[40]				
[41]				

TABLE 6: Attacker-related assumptions. (*): guessed from the text.

	Active/passive/both	Global/local	Static/moving	Insider/outsider/both	Knowledge	Behavior and capabilities	Unique/several-independent/colluding
[44]		Local	Moving	Insider			Several
[39]	Passive						
[30]							
[22]						Honest but curious	Several-colluding
[28]		Global		Insider			
[25]	Passive	Global		Outsider			
[52]	Passive	Local	Moving	Outsider			
[29]	Passive	Global		Outsider			
[31]	Both	Global		Insider			
[21]	Passive	Semiglobal	Moving				
[34]	Passive						
[20]	Passive	Local	Moving				
[49]	Passive	Local		Insider			
[53]							
[16]	Passive	Global		Outsider (*)		Deployment and protocol-aware	Several-colluding
[46]	Passive	Global					
[50]	Passive	Local		Outsider (*)	Location for each ID	The same communication range as sensors	
[35]	Passive	Global		Outsider			
[54]	Passive	Local		Both		Honest but curious	Several-colluding
[13]							
[14]	Both	Multilocal	Moving	Both	Knows everything except keys and IDs	Unlimited resources (memory, processing, energy)	Several-colluding
[24]	Passive	Global		Outsider	Knows everything except keys and IDs	Unlimited resources (memory, processing, energy)	Several-colluding
[38]	Passive						
[18]	Passive	Global		Outsider			
[47]							
[48]	Active			Insider			
[26]				Insider		Honest but curious	Several-colluding
[42]	Both	Global		Both		Attacker works when network is already set up	
[27]	Both						
[45]							
[15]	Passive	Global		Outsider	Knows origin destination for each observed packet		Several-colluding (parallel sensor network)

TABLE 6: Continued.

	Active/passive/both	Global/local	Static/moving	Insider/outsider/both	Knowledge	Behavior and capabilities	Unique/several-independent/colluding
[19]	Passive	Multilocal			Sink location and crypto mechanism in use		
[32]	Active	Local		Insider		Honest but curious and dishonest	
[23]	Passive	Local	Moving	Outsider		The same communication range as sensors	
[17]	Both			Both		Honest but curious	
[43]	Passive			Both			
[36]	Active	Global		Both			
[33]	Both	Local		Both			
[37]							
[40]	Both	Global		Both			
[41]	Both	Global		Both			

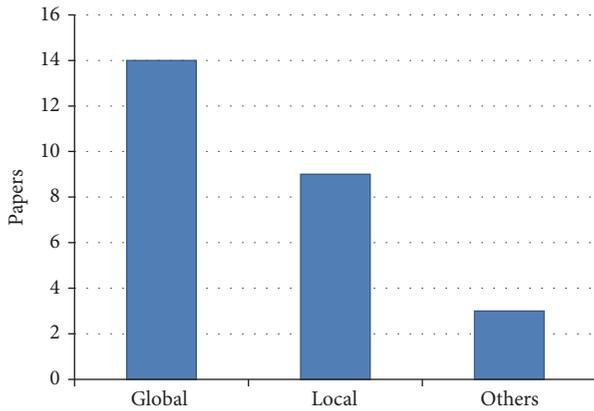


FIGURE 7: Attacker coverage distribution.

at once. Afterwards, less papers consider that the attacker is local, meaning that the attacker only interacts with a small portion of the WSN at a time. In between global and local attackers, several settings appear. Paper [21] adopts a semiglobal attacker since authors state that a global one is not realistic. Papers [14, 19] consider a multilocal attacker, in which it may cover several network portions simultaneously.

The static/moving nature of the attacker is not relevant to global attackers, by definition. However, this is relevant to local attackers, since it makes their coverage (i.e., covered region) vary over time. In particular, [20, 23, 52] consider that attacker may be moving. Note that this is different from a multilocal attacker in that only one place may be visited at a time. Considering this aspect, the static/moving condition of the attacker should be carefully stated in papers. However, only 7 papers make this assumption explicit.

Another issue to note is how the coverage is achieved. Local attackers are sometimes assumed to have similar communication range to regular sensors (e.g., [50]). Nevertheless, in order to have global coverage, some works consider that the attacker is not a single entity but a set of colluding nodes which collectively bring this feature [15, 16]. It is noticeable that this situation cannot always be reached, since it is not always easy to manage a set of nodes within the network. Thus, this aspect should be made clear to clarify the chances for adoption for a particular use case. However, only 6 papers explicitly state it.

With respect to the attacker nature, two main classes are identified. Thus, *passive* attackers can only eavesdrop communication whereas *active* ones are able to interfere with the system itself. This distinction is made by 30 papers, which shows that the research community agrees on that this issue cannot be disregarded. Among these, passive attackers appear in most cases whereas active ones are present in the minority of them. In between, the remaining papers consider an active and passive attacker (Figure 8). Even if it could be said that active attacker capabilities already include those from the passive attacker, we have kept this distinction for the sake of clarity.

Another important dimension of the attacker is its degree of presence. In particular, *outsiders* are those attackers which

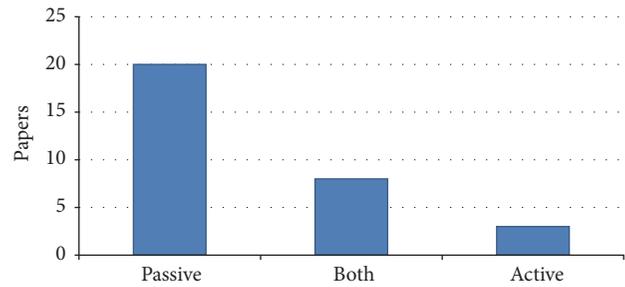


FIGURE 8: Attacker nature distribution.

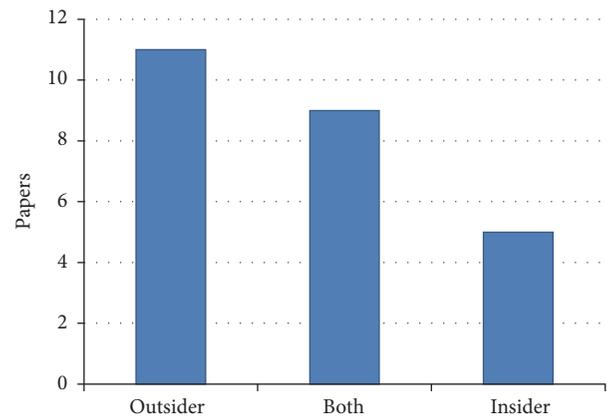


FIGURE 9: Attacker presence distribution.

perform their actions from outside the network. On the contrary, *insiders* are part of the network and may have access to other elements as any other internal member. As it happened with nature, the majority of papers qualify the attacker in this criterion (Figure 9). Among them, the majority consider outsiders whereas only a few of them adopt the insider model. The remaining papers assume that the attacker is formed by entities inside and outside the network. One important aspect is to define how many nodes are insiders. To this extent, [14] specifies that only a small portion of nodes are insiders.

The last aspect that describes an attacker is based on what it knows and which are its resources. Concerning its knowledge, [50] assumes that it knows the location for each ID. Even further, [14, 24] consider that the attacker knows everything about the system except cryptographic keys and IDs. A more relaxed version is found in [19], in which the attacker knows the sink location as well as the cryptographic system in use.

With respect to the attacker behavior, 5 papers assume an honest but curious model. This decision is tailored for internal attackers which follow the rules (e.g., the proposed mechanism) but try to guess as much information as possible. It must be noted that by definition only insider attackers may be honest but curious; outsiders cannot be honest as they are not intended to follow the proposed mechanism.

Attacker resources are also controversial. Papers [14, 24] work under the assumption that the attacker has unlimited

resources in terms of computation, battery, and storage. On the contrary, [32, 50] assume that it has the same coverage range as regular sensors.

6. Guidelines for Privacy-Related Model Definition in WSNs

Based on the observations made in the studied papers, this section focuses on proposing a set of guidelines to foster the adoption of more comprehensive and detailed models in privacy-related research works. For the sake of clarity, these suggestions are divided following the same structure as the analysis conducted in this paper. Our guidelines for privacy-related models in WSNs come in the form of a checklist for usability purposes (see Table 7).

Recalling Figure 1, the most general issues to address are goals and threats. Thus, our guidelines include two questions for each matter, aiming to spot which are the actual privacy goals, which are the data at stake, and which threats are related to data or entities.

Clarifying network and attacker assumptions involves several questions to be addressed. Thus, each of these issues are studied separately.

6.1. Network Decisions. Network-related decisions are related to the assumptions over sources, sink(s), network management, and trusted elements. For the sake of brevity, each aspect is independently covered in what follows.

Concerning sensors, most works agree on that they are resource-constrained, battery-powered devices. However, given that this technology is evolving, it is convenient to clarify the extent of these limitations. On the other hand, it is critical to define whether sensors are static, nonstatic but within a limited range, or fully mobile. This heavily impacts the suitability of approaches. Another factor to set is the distribution of nodes; if they are randomly distributed or they are arranged following some strategy.

With respect to sinks, it is commonly accepted that they are more powerful than sensors. They are sometimes qualified as unconstrained, but this category is rather unrealistic. It is advisable to determine their minimal features. Another important feature is the amount of sinks. Particularly, the less common architecture is to have several sinks. This may be an interesting research niche.

Concerning network management, the election of the topology is not straightforward. Thus, the topology at stake (e.g., ring, multiring, and tree) must be stated. On the contrary, if there is no need for a specific topology, it is convenient to clarify it. If the network has to be organized in a given way, for example, divided in clusters, it is important to determine if these clusters are statically or dynamically created. This issue has to be in consonance with the mobility of nodes and their geographical distribution.

Finally, the choice of trusted elements is a limiting factor. They set the ground base upon which the approach must be built. It is important to determine which elements belong to this condition (e.g., sensor, sink, or TTPs) and to what extent

(e.g., they cannot be compromised, they cannot exfiltrate data).

6.2. Attacker-Related Decisions. Concerning the attacker-related decisions, there are two main aspects to consider: location and capabilities. Each issue is addressed below.

Related to location, the attacker placement is of utmost relevance. There are three decisions that are worth considering: its inclusion in the network, its static/nonstatic condition, and its global-local coverage. These issues differentiate against a local threat and a global one and if this condition changes over time. One related issue is to identify how the global coverage is achieved, when appropriate. If the scenario is small enough, it is reasonable to assume that it is a single entity with great coverage. However, for large-scale scenarios, it may require several-colluding nodes. Thus, stating the amount of attackers and their cooperation level is important.

With respect to the attacker capabilities, apart from the classical distinction between active and passive actions, relevant decisions must be taken regarding the attacker knowledge and behavior. Thus, it must be stated whether the attacker has some advantageous information, such as location of nodes and/or their IDs. Similarly, determining if its knowledge grows with time is important. On the other hand, the attacker behavior may follow a particular pattern, for example, honest but curious and rational/irrational. This puts a limit on the type of threats that the contribution may face.

7. Conclusion

Wireless Sensor Networks (WSNs) have received great attention in the last years. In particular, privacy preservation is of utmost importance in several application scenarios. A plethora of contributions have been produced in this regard. Although several surveys have recently focused on the internals of the proposed approaches, this paper has focused on their underlying models. Thus, the network assumptions, the considered goals, the attacker nature, and its associated threats have been analysed. For this purpose, a set of 41 papers from the last 5 years have been considered. It has been made clear that different papers take assorted decisions in these central aspects. Even worse, sometimes authors do not make explicit statements over some of these critical factors. Thus, our survey shows that many aspects remain unclear in most papers. This makes comparing approaches or even deciding whether they could be simultaneously applied impossible.

To contribute to addressing this situation, this paper has proposed a set of guidelines to build privacy-related models in WSNs. Thus, we believe that this paper will foster the adoption of more comprehensive and detailed models in future contributions from the research community.

Appendix

See Tables 1, 2, 3, 4, 5, and 6.

TABLE 7: Guidelines for privacy-related models in WSNs.

General issues	Goals
	Which particular aspect of privacy is at stake?
	Which kind of data are privacy-sensitive?
	Threats
Network decisions	Which are the data privacy threats (if any)?
	Which are the entity privacy threats (if any)?
	Sensor
	How limited their resources are?
	May they move? If so, are there any boundaries?
	Are they placed following any strategy or randomly scattered?
	Sink
	How many of them are there?
	If they are several, do they cooperate?
	How powerful is it?
	Network
	Is any topology assumed (e.g., ring, tree) or it may work for any topology?
	Is the network organized in some way (e.g., cluster, areas)?
	If so, is this organization permanent?
	Trusted elements
	Are sensors trusted? If so, to what extent?
	Are sinks trusted? If so, to what extent?
	Are communications trusted? Which ones (e.g., sensor-sensor, sensor-sink, and sensor-user)? To what extent?
Are there Trusted Third Parties? If so, what are they trusted for?	
Attacker-related decisions	Coverage
	Where is it placed? Is it internal, external, or both?
	Does it have global view? If so, how?
	Does it move over time?
	Nature
	Is it active, passive, or both?
	Presence
	If it involves internal nodes, is there any upper/lower limit?
	Knowledge
	Which information does it know? Does this information change over time?
	Behavior and resources
	Does it have any attack pattern? Is it honest?
Does it attack for a given benefit to a particular subset of nodes?	
If it involves several entities, do they cooperate? To what extent?	

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work was supported by the MINECO Grant TIN2013-46469-R (Security and Privacy in the Internet of You (SPINY)) and the CAM Grant S2013/ICE-3095 (Cybersecurity, Data, and Risks (CIBERDINE)), which is cofunded by European Funds (FEDER). Furthermore, J. M. de Fuentes and L. González-Manzano were also partially supported by the

Programa de Ayudas a la Movilidad of Carlos III University of Madrid.

References

- [1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.
- [2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.
- [3] C. Y. Chow, W. Xu, and T. He, "Privacy enhancing technologies for wireless sensor networks," in *The Art of Wireless Sensor Networks*, pp. 609–641, Springer, 2014.

- [4] A. Tayebi, S. Berber, and A. Swain, "Wireless sensor network attacks: an overview and critical analysis," in *Proceedings of the 7th International Conference on Sensing Technology (ICST '13)*, pp. 97–102, Wellington, New Zealand, December 2013.
- [5] R. Rios, J. Lopez, and J. Cuellar, "Location privacy in WSNs: solutions, challenges, and future trends," in *Foundations of Security Analysis and Design VII*, vol. 8604 of *Lecture Notes in Computer Science*, pp. 244–282, Springer, 2014.
- [6] P. Gupta and M. Chawla, "Privacy preservation for WSN: a survey," *International Journal of Computer Applications*, vol. 48, no. 3, pp. 11–16, 2012.
- [7] N. Oualha and A. Olivereau, "Sensor and data privacy in industrial wireless sensor networks," in *Proceedings of the Conference on Network and Information Systems Security*, pp. 1–8, 2011.
- [8] M. Conti, J. Willemsen, and B. Crispo, "Providing source location privacy in wireless sensor networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 1238–1280, 2013.
- [9] R. Bista and J.-W. Chang, "Privacy-preserving data aggregation protocols for wireless sensor networks: a survey," *Sensors*, vol. 10, no. 5, pp. 4577–4601, 2010.
- [10] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2688–2710, 2010.
- [11] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *Journal of Medical Systems*, vol. 36, no. 1, pp. 93–101, 2012.
- [12] K. Islam, W. Shen, and X. Wang, "Wireless sensor network reliability and security in factory automation: a survey," *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews*, vol. 42, no. 6, pp. 1243–1256, 2012.
- [13] D. Christin, A. Reinhardt, S. Kanhere, and M. Hollick, "Fine-grained access control enabling privacy support in wireless sensor networks," in *Proceedings of the 9th KuVS Fachgespräch Drahtlose Sensornetze*, vol. 1, pp. 29–32, Würzburg, Germany, September 2010.
- [14] A.-S. Abuzneid, T. Sobh, M. Faezipour, A. Mahmood, and J. James, "Fortified anonymous communication protocol for location privacy in WSN: a modular approach," *Sensors*, vol. 15, no. 3, pp. 5820–5864, 2015.
- [15] K. Mehta, D. Liu, and M. Wright, "Protecting location privacy in sensor networks against a global eavesdropper," *IEEE Transactions on Mobile Computing*, vol. 11, no. 2, pp. 320–336, 2012.
- [16] A. Debnath, P. Singaravelu, and S. Verma, "Efficient spatial privacy preserving scheme for sensor network," *Central European Journal of Engineering*, vol. 3, no. 1, pp. 1–10, 2013.
- [17] C. Ma, K. Xue, and P. Hong, "Distributed access control with adaptive privacy preserving property for wireless sensor networks," *Security and Communication Networks*, vol. 7, no. 4, pp. 759–773, 2014.
- [18] B. Di Ying, D. Makrakis, and H. T. Mouftah, "Anti-traffic analysis attack for location privacy in WSNs," *EURASIP Journal on Wireless Communications and Networking*, vol. 2014, article 131, 2014.
- [19] M. M. E. A. Mahmoud and X. Shen, "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 10, pp. 1805–1818, 2012.
- [20] J. Long, M. Dong, K. Ota, and A. Liu, "Achieving source location privacy and network lifetime maximization through tree-based diversionary routing in wireless sensor networks," *IEEE Access*, vol. 2, pp. 633–651, 2014.
- [21] M. Raj, N. Li, D. Liu, M. Wright, and S. K. Das, "Using data mules to preserve source location privacy in Wireless Sensor Networks," *Pervasive and Mobile Computing*, vol. 11, no. 1, pp. 244–260, 2014.
- [22] M. M. Groat, W. Hey, and S. Forrest, "KIPDA: k-indistinguishable privacy-preserving data aggregation in wireless sensor networks," in *Proceedings of the IEEE INFOCOM*, pp. 2024–2032, IEEE, Shanghai, China, April 2011.
- [23] W. Tan, K. Xu, and D. Wang, "An anti-tracking source-location privacy protection protocol in WSNs based on path extension," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 461–471, 2014.
- [24] Y. Yang, M. Shao, S. Zhu, and G. Cao, "Towards statistically strong source anonymity for sensor networks," *ACM Transactions on Sensor Networks*, vol. 9, no. 3, article 34, Article ID 2480737, 2013.
- [25] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Toward a statistical framework for source anonymity in sensor networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 2, pp. 248–260, 2013.
- [26] J. Wu and F. Zhang, "Privacy-preserving regression modeling and attack analysis in sensor network," in *Cloud Computing and Big Data*, W. Qiang, X. Zheng, and C.-H. Hsu, Eds., vol. 9106 of *Lecture Notes in Computer Science*, pp. 354–366, Springer, New York, NY, USA, 2015.
- [27] E. C.-H. Ngai and I. Rodhe, "On providing location privacy for mobile sinks in wireless sensor networks," *Wireless Networks*, vol. 19, no. 1, pp. 115–130, 2013.
- [28] C.-Y. Chow, M. F. Mokbel, and T. He, "A privacy-preserving location monitoring system for wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 94–107, 2011.
- [29] S. Ortolani, M. Conti, B. Crispo, and R. Di Pietro, "Events privacy in WSNs: a new model and its application," in *Proceedings of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM '11)*, pp. 1–9, IEEE, Lucca, Italy, June 2011.
- [30] B. Carbutar, Y. Yu, W. Shi, M. Pearce, and V. Vasudevan, "Query privacy in wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 6, no. 2, article 14, pp. 1–12, 2010.
- [31] L. Buttyán and T. Holczer, "Perfectly anonymous data aggregation in wireless sensor networks," in *Proceedings of the IEEE 7th International Conference on Mobile Ad hoc and Sensor Systems (MASS '10)*, pp. 513–518, November 2010.
- [32] X. Liao and J. Li, "Privacy-preserving and secure top-k query in two-tier wireless sensor network," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM '12)*, pp. 335–341, IEEE, Anaheim, Calif, USA, December 2012.
- [33] D. He, S. Chan, and M. Guizani, "Accountable and privacy-enhanced access control in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 1, pp. 389–398, 2015.
- [34] J.-H. Park, Y.-H. Jung, H. Ko, J.-J. Kim, and M.-S. Jun, "A privacy technique for providing anonymity to sensor nodes in a sensor network," *Communications in Computer and Information Science*, vol. 150, no. 1, pp. 327–335, 2011.
- [35] Y. Zhang, M. Price, L. Opyrchal, and K. Frikken, "All Proxy Scheme for event source anonymity in wireless sensor networks," in *Proceedings of the 6th International Conference on*

- Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP '10)*, pp. 263–268, IEEE, Brisbane, Australia, December 2010.
- [36] P. Kumar, A. Gurtov, M. Ylianttila, S.-G. Lee, and H. J. Lee, “A strong authentication scheme with user privacy for wireless sensor networks,” *ETRI Journal*, vol. 35, no. 5, pp. 889–899, 2013.
- [37] N. Bruce, Y. S. Lee, S. G. Lee, and H. J. Lee, “A privacy preserving security protocol-based application for wireless communication system,” in *Proceedings of the IEEE 17th International Conference on High Performance Computing and Communications (HPCC '15), the IEEE 7th International Symposium on Cyberspace Safety and Security (CSS '15) and the IEEE 12th International Conference on Embedded Software and Systems (ICSS '15)*, pp. 1651–1656, New York, NY, USA, August 2015.
- [38] L. Zhou, Q. Wen, and H. Zhang, “Protecting sensor location privacy against adversaries in wireless sensor networks,” in *Proceedings of the 5th International Conference on Computational and Information Sciences (ICIS '13)*, pp. 1384–1387, Shiyang, China, June 2013.
- [39] Y. Li and J. Ren, “Source-location privacy through dynamic routing in wireless sensor networks,” in *Proceedings of the IEEE INFOCOM*, pp. 1–9, March 2010.
- [40] S. B. Othman, A. A. Bahattab, A. Trad, and H. Youssef, “Confidentiality and integrity for data aggregation in WSN using homomorphic encryption,” *Wireless Personal Communications*, vol. 80, no. 2, pp. 867–889, 2014.
- [41] K. Xie, X. Ning, X. Wang et al., “An efficient privacy-preserving compressive data gathering scheme in WSNs,” in *Algorithms and Architectures for Parallel Processing*, G. Wang, A. Zomaya, G. M. Perez, and K. Li, Eds., vol. 9528 of *Lecture Notes in Computer Science*, pp. 702–715, Springer, New York, NY, USA, 2015.
- [42] R.-H. Hu, X.-M. Dong, and D.-L. Wang, “Protecting data source location privacy in wireless sensor networks against a global eavesdropper,” *International Journal of Distributed Sensor Networks*, vol. 2014, Article ID 492802, 17 pages, 2014.
- [43] G. Yang, S. Li, X. Xu, H. Dai, and Z. Yang, “Precision-enhanced and encryption-mixed privacy-preserving data aggregation in wireless sensor networks,” *International Journal of Distributed Sensor Networks*, vol. 9, no. 4, Article ID 427275, pp. 1–12, 2013.
- [44] X. Luo, X. Ji, and M.-S. Park, “Location privacy against traffic analysis attacks in wireless sensor networks,” in *Proceedings of the International Conference in Information Science and Applications (ICISA '10)*, pp. 1–6, Seoul, South Korea, April 2010.
- [45] B. Ntirenganya, Z. Zhang, L. Zhu, Y.-A. Tan, Z. Yang, and C. Guo, “Enhanced privacy preserving pattern-code based data aggregation in wireless sensor networks,” in *Proceedings of the 9th IEEE International Conference on Mobile Ad-Hoc and Sensor Networks (MSN '13)*, pp. 336–341, December 2013.
- [46] L. Yao, L. Kang, F. Deng, J. Deng, and G. Wu, “Protecting source-location privacy based on multirings in wireless sensor networks,” *Concurrency and Computation: Practice and Experience*, vol. 27, no. 15, pp. 3863–3876, 2015.
- [47] J. E. Tapiador, M. Srivatsa, J. A. Clark, and J. A. McDermid, “Decorrelating WSN traffic patterns with maximally uninformative constrained routing,” in *NETWORKING 2011 Workshops*, vol. 6827 of *Lecture Notes in Computer Science*, pp. 207–218, Springer, Berlin, Germany, 2011.
- [48] X. Yang, X. Ren, S. Yang, and J. McCann, “A novel temporal perturbation based privacy-preserving scheme for real-time monitoring systems,” *Computer Networks*, vol. 88, pp. 72–88, 2015.
- [49] C. Li and Y. Liu, “ESMART: energy-efficient slice-mix-aggregate for wireless sensor network,” *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 134509, 9 pages, 2013.
- [50] A. Gurjar and A. R. B. Patil, “Cluster based anonymization for source location privacy in wireless sensor network,” in *Proceedings of the 3rd International Conference on Communication Systems and Network Technologies (CSNT '13)*, pp. 248–251, IEEE, Gwalior, India, April 2013.
- [51] A. Back, U. Möller, and A. Stiglic, “Traffic analysis attacks and trade-offs in anonymity providing systems,” in *Information Hiding*, I. S. Moskowitz, Ed., vol. 2137 of *Lecture Notes in Computer Science*, pp. 245–257, Springer, London, UK, 2001.
- [52] L. Yao, L. Kang, P. Shang, and G. Wu, “Protecting the sink location privacy in wireless sensor networks,” *Personal and Ubiquitous Computing*, vol. 17, no. 5, pp. 883–893, 2013.
- [53] K.-J. Kim and S.-P. Hong, “Privacy care architecture in wireless sensor networks,” *International Journal of Distributed Sensor Networks*, vol. 9, no. 5, Article ID 369502, 2013.
- [54] X. Zhang, H. Chen, K. Wang, H. Peng, Y. Fan, and D. Li, “Rotation-based privacy-preserving data aggregation in wireless sensor networks,” in *Proceedings of the 1st IEEE International Conference on Communications (ICC '14)*, pp. 4184–4189, IEEE, Sydney, Australia, June 2014.

Research Article

A Lightweight Authentication and Key Management Scheme for Wireless Sensor Networks

Danyang Qin, Shuang Jia, Songxiang Yang, Erfu Wang, and Qun Ding

Key Lab of Electronic and Communication Engineering, Heilongjiang University, Harbin, China

Correspondence should be addressed to Danyang Qin; qindanyang@hlju.edu.cn

Received 3 June 2016; Revised 6 September 2016; Accepted 21 September 2016

Academic Editor: Jose Maria de Fuentes

Copyright © 2016 Danyang Qin et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Security problem is one of the most popular research fields in wireless sensor networks for both the application requirement and the resource-constrained essence. An effective and lightweight Authentication and Key Management Scheme (AKMS) is proposed in this paper to solve the problem of malicious nodes occurring in the process of networking and to offer a high level of security with low cost. For the condition that the mobile sensor nodes need to be authenticated, the keys in AKMS will be dynamically generated and adopted for security protection. Even when the keys are being compromised or captured, the attackers can neither use the previous keys nor misuse the authenticated nodes to cheat. Simulation results show that the proposed scheme provides more efficient security with less energy consumption for wireless sensor networks especially with mobile sensors.

1. Introduction

Wireless sensor networks (WSNs) [1] consist of a large number of nodes in a self-organized manner, where there are no central control nodes, and the nodes lying out of the transmitting range can communicate in a multihop way. As the wireless sensor network is independent of the predeploy infrastructure, it has broad application prospects in the battlefield environment, disaster relief, and environmental threats exploration, which make the security and efficiency the most basic requirements and the most popular research areas [2].

The characteristics of wireless sensor networks determine the network security threats, the security systems, and security algorithms that are quite different from those in traditional networks [3], and the traditional network security systems and security algorithms cannot be introduced directly. Meanwhile, the inherent essence of limited storage space, computational capabilities [4], bandwidth, and communication energy does not make the computational data encryption and public key cryptography based on the traditional cryptographic techniques adapt to wireless sensor networks. The security system and algorithm for WSN are mainly focused on in this paper to design an effective

Authentication and Key Management Scheme with low computing and energy cost.

2. Related Work

With the development of security technology in wireless sensor networks, the research on routing protocols has been increasing in recent years. This section describes the three existing master key-based key management protocols: LOCK [5], SPINS [6], and BROSK [7]. These protocols have been widely discussed in this area.

The Localized Combinatorial Keying (LOCK) proposed by Eltoweissy is an Exclusion-Based Systems (EBS) dynamic key management approach for cluster-based sensor networks. LOCK takes use of three keys, including the administrative key, the group session key, and the cluster session key. A special node selected by the cluster head is called a key generation node and will perform a key generation process. LOCK is for static networks. But the proposed scheme in this paper will be suitable for dynamic networks.

SPINS is a famous security framework for wireless sensor networks. Although it contains two protocols, SNEP and TESLA, which are used to achieve the confidentiality and

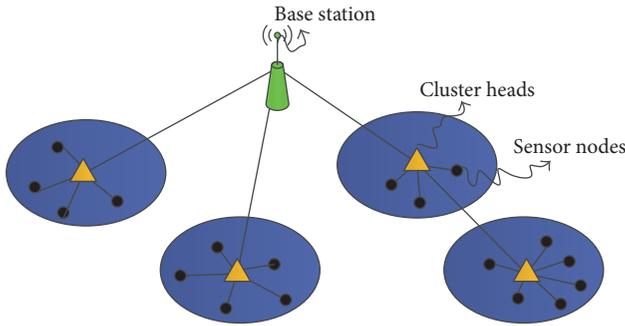


FIGURE 1: Wireless sensor network model.

authentication of data broadcasting, respectively, we will concentrate on the key agreement protocols [8].

BROSK can be considered as a more recent ad hoc key agreement protocol compared to SPINS. There are no trusted parties or servers in this scheme, in which each node negotiates the session key directly with its neighbor node by broadcasting key agreement message.

3. Network Model and Key Generation

This part briefly introduces the network model, the importance of authentication, and the idea of CPK system based on ECC.

3.1. Network Model. The members of wireless sensor network are BS (base station), CH (cluster head), and resource-constrained nodes, which are deployed in a geographical area to perform some special monitoring functions. In most applications, especially for large scale deployment, the sensors are arranged in multiple static clusters, as shown in Figure 1. The members' changing makes the authentication and key management always a key research point in wireless network. Considering the resource-constrained essence of WSN, a lightweight scheme is badly needed, which keeps the key changeless to save the limited energy. Many applications, however, require the mobility of network nodes to support. In such a mobile sensor network, there will be always the condition that a node from an existing cluster moves into another cluster. The separated nodes may be the cluster heads or cluster members. The main reason causing the changes in cluster heads and cluster members is the mobility. The mobility of nodes together with the transient nature of the wireless media often leads to a highly dynamic network topology. In this case, security protection with moving sensors must be incorporated into wireless sensor network.

Authentication is one of the security practices to verify the identity of the sensor nodes. Public key cryptography is a popular way to provide authentication for WSN. Though the easy design and effective operation make it attractive, the disadvantage of more energy requirement greatly restricts the network performance. Thus, the sensor node has to use elliptic curve digital signature algorithm to generate a digital signature authentication. The combination of pairwise, global key, cluster key, and preloaded secret information is also used

to verify the sensor nodes in the network. The node mobility will lead to random topology changes, which affects the security of mobile sensor networks. The lightweight Authentication and Key Management Scheme (AKMS) proposed in this paper will adopt a Hash Message Authentication Code (HMAC) algorithm [9] and a Combined Public Key (CPK) password system based on ECC to authenticate the moving nodes within the network effectively.

Sensor network has many features that make them more vulnerable to attack than the traditional computing devices. For example, the nature of the broadcasting allows the information to be intercepted, eavesdropped on, tampered with, or exchanged easily. Besides suffering the same threats with the conventional wireless networks, WSN is vulnerable to resource depletion attacks, which attempt to run out of resources, such as node battery and network bandwidth, and causes more damage. Finally, most devices in WSN cannot be tamper-resistant typically, which facilitates the physical manipulation and keys being stolen. To approach the real condition, the attack model is assumed as follows:

- (1) The sensors are not tamper-resistant, so an attacker is able to access the stored information and the keys in the node storage directly.
- (2) The attackers may appear not only before the network deployment but also during all the network life cycle without any assumptions about the quantity or the physical location of the attackers.
- (3) The attackers may easily intercept and modify the exchanged information among the network nodes.

3.2. The Idea of CPK System Based on ECC. Combined Public Key (CPK) password system based on ECC is a way of authentication based on the identity. According to the mathematical principle of elliptic curve discrete logarithm, we build public key matrix and private key matrix and use the hash function to map the entity's identity for the row and column coordinates sequence of the matrix; it is used for the selection and combination of matrix element, and it can generate a large number of public and private key pairs, so as to realize the large scale of identity-based key generation and distribution. Entity nodes need to know each other's identity to calculate its public key, which can easily achieve authentication and security features. Among them, identify key is generated by the entity's identity through combination matrix. The CPK system based on ECC has the following advantages.

- (1) In wireless sensor network (WSN), the only legitimate nodes have the private key, and, according to the other identity ID and segmentation key, we can calculate the other Combined Public Keys (CPK), so the simple and efficient authentication process can be realized without the participation of the third party.
- (2) The CPK system based on ECC can combine large public/private key pair through a small amount of public/private key matrix; nodes only need to store a small matrix to achieve a large number of nodes' security authentication in the network.

Point multiplication operation is the foundation of CPK algorithm. ECC Signature Algorithm (ECDSA) is the elliptic curve version of digital signature algorithm (DSA); it is the basis for the CPK digital signature algorithm. This paper adopts ECC algorithms based on Montgomery type curve [10]. We use point multiplication operation of Montgomery type elliptic curve and the binary shift NAF coding algorithm to solve the large amount of calculation generated by ECC point multiplication. We use the point addition and times point fast operation where the value of y is not calculated to avoid modular inversion algorithm under the projective coordinates.

Point addition formula is as follows:

$$\begin{aligned} X_{m+n} &= Z_{m-n} [(X_m - Z_m)(X_n + Z_n) + (X_n - Z_n) \\ &\quad \cdot (X_m + Z_m)]^2 \\ Z_{m+n} &= X_{m-n} [(X_m - Z_m)(X_n + Z_n) - (X_n - Z_n) \\ &\quad \cdot (X_m + Z_m)]^2. \end{aligned} \quad (1)$$

Times point formula is as follows:

$$\begin{aligned} 4X_n Z_n &= (X_n + Z_n)^2 - (X_n - Z_n)^2 \\ X_{2n} &= (X_n + Z_n)^2 (X_n - Z_n)^2 \\ Z_{2n} &= (4X_n Z_n) \left[(X_n - Z_n)^2 + \left(\frac{A+2}{4} \right) 4X_n Z_n \right]. \end{aligned} \quad (2)$$

Calculating coordinates (X, Z) of the times point dP of point $P = (x, y)$ in projective coordinates, where “ \leftarrow ” denotes mapping and (S1) means step 1, the specific algorithm is as follows:

$$(S1) \ i \leftarrow |d| - 1;$$

(S2) Calculate the integer:

$$X_1 \leftarrow x,$$

$$Z_1 \leftarrow 1;$$

$$T_1 \leftarrow (X_1 + Z_1)^2 - (X_1 - Z_1)^2 \quad (3)$$

$$X_2 \leftarrow (X_1 + Z_1)^2 (X_1 - Z_1)^2;$$

$$Z_2 \leftarrow T_1 \left((X_1 - Z_1)^2 + \left(\frac{A+2}{4} \right) T_1 \right);$$

(S3) If $i = 0$, then jump to (S12), else go to (S4);

(S4) $i \leftarrow i - 1$;

(S5) If $d_i = 0$, then go to (S6), else jump to (S9).

(S6) Calculate the integer:

$$T_1 \leftarrow X_2;$$

$$X_2 \leftarrow [(T_1 - Z_2)(X_1 + Z_1) + (T_1 + Z_2)(X_1 - Z_1)]^2 \quad (4)$$

$$Z_2$$

$$\leftarrow x [(T_1 - Z_2)(X_1 + Z_1) - (T_1 + Z_2)(X_1 - Z_1)]^2;$$

(S7) Calculate the integer:

$$T_1 \leftarrow X_2;$$

$$T_2 \leftarrow (T_1 + Z_1)^2 - (T_1 - Z_1)^2$$

$$X_1 \leftarrow (T_1 + Z_1)^2 (T_1 - Z_1)^2; \quad (5)$$

$$Z_1 \leftarrow T_2 \left((T_1 - Z_1)^2 + \left(\frac{A+2}{4} \right) T_2 \right);$$

(S8) Jump to (S3);

(S9) Calculate the integer;

$$T_1 \leftarrow X_1;$$

$$X_1 \leftarrow [(X_2 - Z_2)(T_1 + Z_1) + (X_2 + Z_2)(T_1 - Z_1)]^2 \quad (6)$$

$$Z_1$$

$$\leftarrow x [(X_2 - Z_2)(T_1 + Z_1) - (X_2 + Z_2)(T_1 - Z_1)]^2;$$

(S10) Calculate the integer:

$$T_1 \leftarrow X_2;$$

$$T_2 \leftarrow (T_1 + Z_2)^2 - (T_1 - Z_2)^2$$

$$X_2 \leftarrow (T_1 + Z_2)^2 (T_1 - Z_2)^2; \quad (7)$$

$$Z_2 \leftarrow T_2 \left((T_1 - Z_2)^2 + \left(\frac{A+2}{4} \right) T_2 \right);$$

(S11) Jump to (S3);

(S12) Output integer X_1, Z_1 , as dP corresponding X, Z .

4. Proposed Authentication and Key Management Scheme

The lightweight AKMS proposed in this paper consists of three main phases: key predistribution phase, network initialization phase, and authentication protocol. The first phase is enabled before the nodes are being deployed. The second phase sets the security of network, and it is enabled during the network deployment. The last phase is enabled when a new node joins the network with the previous stage being over.

4.1. Key Predistribution Phase. Key predistribution phase is a key step for dynamic key management with moving nodes in WSN. For reasons of clarity, the symbols used in this paper are listed in the Notations.

In this phase, a network-wide symmetric master key will be generated and stored securely. This key should be long enough to destroy the common attack, namely, a minimum of 128 bits. During the networking stage, each node is preinstalled with an initial authenticator. The i th cycle authenticator ∇^i can be used by a node to identify

another node, the superscript symbol of which indicates the cycle where the authenticator takes. It consists of the random number of n tuples and the results of using a keyed-hash function with the current authentication key over them.

During the first authentication cycle, the authentication key is equal to the master key $k_{\text{auth}}^0 = k_M$ before the deployment; therefore

$$\nabla^0 = \left\{ \left(r_i, [r_i]_{k_M} \right) \right\}, \quad i = 0, \dots, n-1. \quad (8)$$

In general, the authentication key of the first cycle is $k_{\text{auth}}^j = [k_M]^j$; then the authenticator set is

$$\nabla^j = \left\{ \left(r_i, [r_i]_{k_{\text{auth}}^j} \right) \right\}, \quad i = 0, \dots, n-1; \quad (9)$$

when the tuples are exhausted at this time, the authenticator will transmit to the next cycle.

4.2. Network Initialization Phase. This phase is enabled during the network deployment. In such operating environment, each node can find its neighbors within the communication range. Specific steps are as follows:

- (1) Each node i generates its unique symmetric key by the CPK system based on ECC, k_{enc}^i , called the node encryption key, which is obtained by generating a random number and performing $k_{\text{enc}}^i = [k_M, r_i]$. For example, the encryption key of some node A can be calculated as $k_{\text{enc}}^A = [k_M, r_A]$.
- (2) For a very short time, each node broadcasts its random value r_i with the unit as seconds [11]. In this way, the attackers listening to the broadcast communication will get the random values.
- (3) Each node receives a random value from its neighbor node and uses common master key to calculate their encryption key. In this case, each node will store a list of paired keys of its neighbor nodes.
- (4) Each node hashes the common master key and keeps it with the first forms of authentication key as $k_{\text{auth}}^1 = [k_M]$, for the easy reason that storing master key in node's storage space has great potential danger if a node is captured. This is mainly because of the existence of the authenticator, which will help to authenticate other nodes and to verify the information of common master key without storing master key.
- (5) In this stage, each node stores its encryption key k_{enc}^i , the set of encryption keys of its neighbor nodes, and the keys of the next authentication cycle k_{auth}^1 , which is hash function of the master key and the current authenticator, ∇^0 consisting of the set of n tuples.
- (6) Now, the node begins to communicate with other nodes using the encryption key in pair.

4.3. Authentication Operator. Authentication operation is used for network nodes to authenticate each other. The

operator's goal is to provide the ability to verify the new node in the network once the deployment phase of nodes is over. Retaining the master key in the node internal memory could cause the whole network security to be damaged. To avoid this situation, AKMS precalculates the necessary authentication material (excitation/response tuple) and the authentication key which will be deleted later. Therefore, the new node will be verified by the knowledge of the authentication key without being stored in the memory. As mentioned above, the authentication operation will adopt two encryption primitives, as the excitation/response scheme [12] and the key chain [13].

4.3.1. Authenticator Generation. The authentication of any cycle j is constructed from the keys of the previous cycle $j-1$. In this way, the node can verify the master key, because the authentication key of the cycle $j-1$ can only be derived rather than storing the master key itself. If a node is destroyed, the attacker will only obtain the identity of the current cycle but not compromise the authentication and the exchange of keys performed using the previous cycles of the authenticator. As a node runs out of authenticators' instances, it will simply generate a new set; that is, it will start a new cycle of the authenticators set. The cycle should be composed of the following steps:

- (1) A new authenticators set with n tuples of random numbers is calculated and the current authentication key k_{auth}^j is applied to each of them to obtain

$$\nabla^{j+1} = \left\{ \left(r_i, [r_i]_{k_{\text{auth}}^j} \right) \right\}, \quad i = 0, \dots, n-1. \quad (10)$$

- (2) The current authentication key is updated and hashed to obtain

$$k_{\text{auth}}^{j+1} = [k_{\text{auth}}^j]. \quad (11)$$

- (3) The new key is generated by

$$\left[k_{\text{auth}}^{j+1}, \nabla^{j+1} = \left\{ \left(r_i, [r_i]_{k_{\text{auth}}^j} \right) \right\} \right], \quad i = 0, \dots, n-1. \quad (12)$$

4.3.2. Implementation Issues. Each of these tuples has a status label to describe its current status in the authentication process. The possible values of status are as follows:

UNUSED: the tuple is unused

ASSIGNED: the tuple is temporarily assigned to a node in an ongoing process of authentication; if the process fails, the label will change to UNUSED, and the tuple can be used again

USED: the tuple is used in a successful authentication process, which cannot be adopted by any other processes; in this way, the replay attack will be avoided efficiently

In addition to these labels, there is another domain in authenticator structure, called the current tuple index denoted as δ to store the first UNUSED tuple, which will

TABLE 1: Example of the authenticator with $\delta = 3$.

Authenticator ∇^2	Status label of each tuple
$(r_0, [r_0]_{k_{\text{auth}}^2})$	USED
$(r_1, [r_1]_{k_{\text{auth}}^2})$	USED
$(r_2, [r_2]_{k_{\text{auth}}^2})$	ASSIGNED
$(r_3, [r_3]_{k_{\text{auth}}^2})$	UNUSED
...	...

increase when each tuple changes its status from UNUSED to ASSIGNED.

Finally, another important issue to be analyzed is the size of the authenticator n . As a system parameter, the value of n should be carefully set according to the number of nodes and the moving rate. Of course, if the network status is changing dramatically, the value of n will be adjusted dynamically. A typical value of n is about 10, which is relatively reasonable taking into account the expected authentication rate and the number of the neighbor nodes in such a network [14].

Although it has no direct security consequences, a very small value of n may cause some performance problems if the network has a high new nodes ingress rate. In order to avoid these drawbacks, a new authentication cycle has to be calculated [15].

An example in Table 1 includes the values of the second authentication cycle. There is $k_{\text{auth}}^2 = [[k_M]] = [k_M]^2$ in this situation. From the value of the current tuple index δ , it can be inferred that the authenticator has carried out two successful authentications.

4.4. Authentication Protocol. A new node, A , wants to join in the network; excitation/response based mutual authentication protocol will be performed after deployment [16]. As a new node, node A can be regarded as the node first entering into the network in some certain sense, so the authenticator will be the first cycle ∇^1 . Assuming node B is the authentication node to node A , which can be adopted at any cycle j , the authentication protocol between node A and node B can be described as follows:

- (1) Node A produces an excitation to node B by generating a random number r_A . Then, it will send a message to node B with the following format:

$$M_1 = r_A. \quad (13)$$

- (2) After receiving M_1 from node A , node B will perform the following operations:

- (i) to open the first unused tuple and mark it by the current tuple index δ , so as to extract the corresponding random number r_B and the random pair $[r_B]_{k_{\text{auth}}^{j-1}}$, as well as change the status label of tuple δ from UNUSED to ASSIGNED;
- (ii) to respond to an excitation from node A using the defined keyed-function with k_{auth}^{j-1} over the excitation r_A to obtain $[r_A]_{k_{\text{auth}}^{j-1}}$;

- (iii) to recover its own encryption keys k_{enc}^B and the ciphers of the current authentication key to obtain $\{k_{\text{enc}}^B\}_{k_{\text{auth}}^j}$;

- (iv) to restore the current cycle j of authenticator for the later synchronization with node A and send the message to node A with the following format:

$$M_2 = \left\{ r_B, [r_A]_{k_{\text{auth}}^{j-1}}, \{k_{\text{enc}}^B\}_{k_{\text{auth}}^j}, j \right\}. \quad (14)$$

- (3) After receiving M_2 from node B , node A will perform the following operations:

- (i) to calculate the current cycle j of node B (node A is considered to be a new node, so the current cycle is 1; therefore node A needs to perform $j-1$ times hash over k_M to obtain $k_{\text{auth}}^j = [k_M]^{j-1}$ to synchronize with node B);

- (ii) to check whether the response from node B is correct or not by comparing its own computation with the received value (passing the checks means node B has demonstrated the original master key and is successfully authenticated);

- (iii) to calculate the imaginary part of the excitation r_B to obtain $[r_B]_{k_{\text{auth}}^{j-1}}$;

- (iv) to generate its own encryption key k_{enc}^A and the ciphers of the current authentication key so as to obtain $\{k_{\text{enc}}^A\}_{k_{\text{auth}}^j}$;

- (v) to send the message to node B with the following format:

$$M_3 = \left\{ [r_B]_{k_{\text{auth}}^j}, \{k_{\text{enc}}^A\}_{k_{\text{auth}}^j} \right\}. \quad (15)$$

- (4) Finally, after receiving M_3 from node A , node B will compare each response of the authenticator in use with the status label ∇_k^j :

- (i) if they are equal, the status label ∇_k^j is changed from ASSIGNED to USED, and the new joining node is authenticated to access the network;
- (ii) if they are not equal, the status label is changed to UNUSED again, which means the new joining node fails in authentication and is not allowed to access the network.

The whole information exchange process can be summarized as in Figure 2.

Being observed in steps (2) and (3), this exchange process provides simple key establishment procedures and effective transfers of the appropriate encryption key k_{enc}^A or k_{enc}^B to the corresponding groups.

Figure 2 shows a full implementation example of the proposed authentication scheme. Node A and node B are regarded as the requester and the authenticator, respectively. The authentication parameters of node B are ∇^3 and $\delta = 2$, which means that the authenticator is in the third cycle and two tuples have been successfully used. Node A is a new node, so its authenticator is in the first cycle.

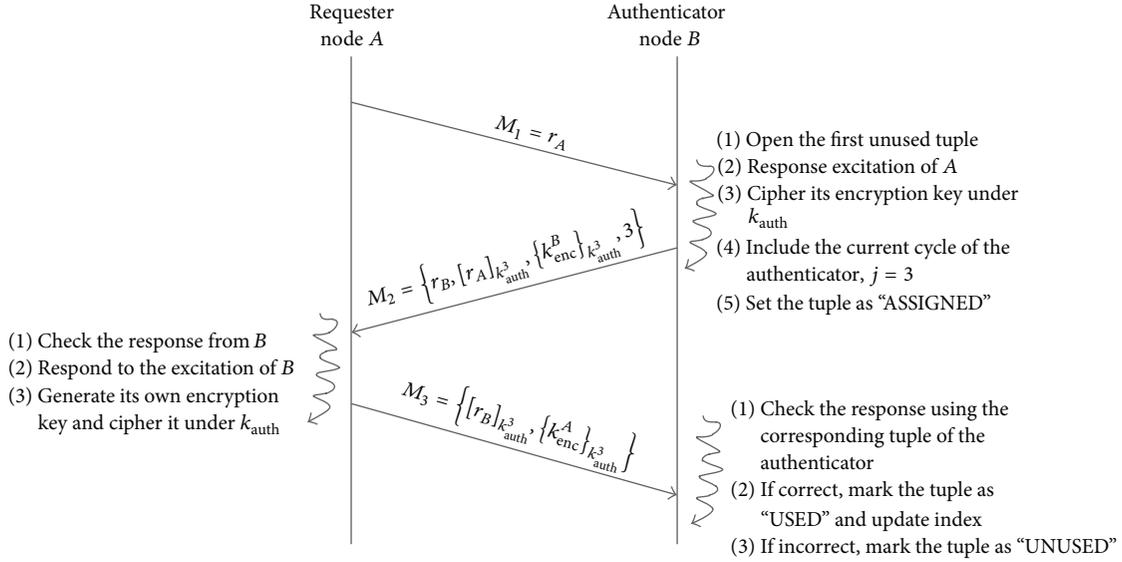


FIGURE 2: Authentication protocol running example.

TABLE 2: Summarization of the simulation parameters (CH: cluster head; SN: sensor node).

Parameters	Values
Number of nodes	100, 101, 102, ..., 500
Area size (m ²)	500 × 500
Wireless bandwidth (Mbps)	2
Simulation duration (sec)	300
Traffic source	CBR
Mobility speed (m/s)	0, 1, 2, ..., 25
Initial energy (J)	CH = 50, SN = 5
Initial V _{BP} (J)	CH = 500, SN = 50
Radio range (m)	CH = 150, SN = 50
Number of internal attackers	90% of attackers
Number of external attackers	10% of attackers
Number of CHs	6% of nodes

5. Performance Evaluations

In this section, the performance of AKMS will be evaluated and analyzed in terms of the average packet delivery rate, the average energy consumption, and the networking success rate with different types of attackers.

5.1. Simulation Settings. The performance of AKMS proposed in this paper is assessed by NS2 [17]. The simulations have been carried out 20 times in different scenarios with the results being averaged for each [18]. The simulation parameters are shown in Table 2.

5.2. Simulation Results. The number of nodes remains 200 with the number of attackers being 5, 10, 15, 20, and 25, respectively [19]. Firstly, the average packet delivery rate (PDR) of AKMS is simulated compared with that of LOCK, SPINS, and BROSK, and the results are shown in Figure 3.

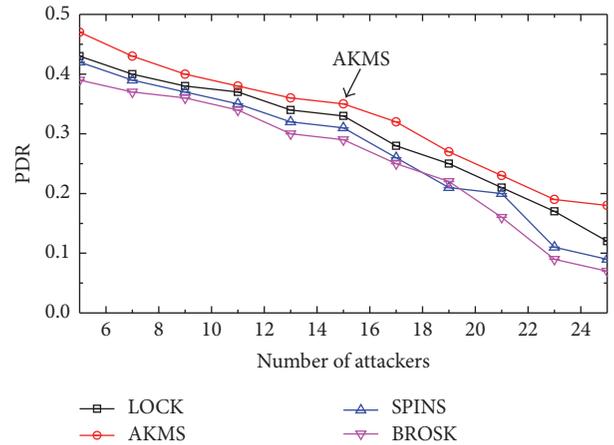


FIGURE 3: Packet delivery ratio.

Because of the bidirectional malware detection technology to eliminate malicious node cluster members and CH, AKMS will reduce the error packets effectively, so as to be able to send more legitimate packets to the destination compared to other schemes. Besides, AKMS adopts multipath propagation routing technology to eliminate the selective forwarding attacks, which makes the PDR even higher.

Secondly, the average energy consumption of all the nodes is measured during transmission, including the energy consumption by sending, receiving, and calculating. Figure 4 shows the average energy consumption comparisons of AKMS, LOCK, SPINS, and BROSK. When the number of attackers is growing, the average energy consumption will also increase. This is because the increasing attackers will cause more error packets. CH will filter out error packets based on AKMS to avoid the spreading of the packets from attackers throughout the network, so as to reduce the energy consumption. In LOCK, the CH node must initiate the key updating if it is captured. A new CH is selected as the new BS,

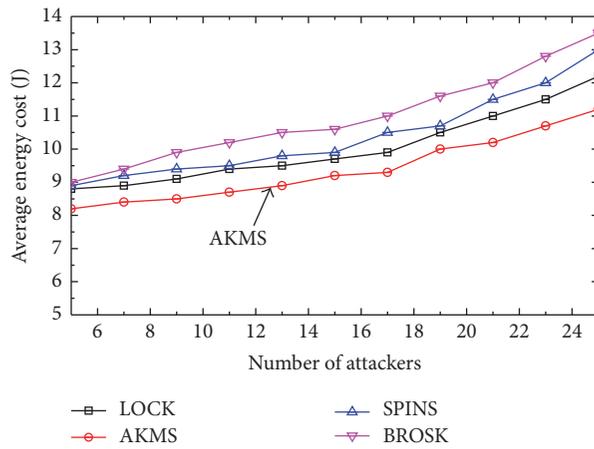


FIGURE 4: Energy consumption.

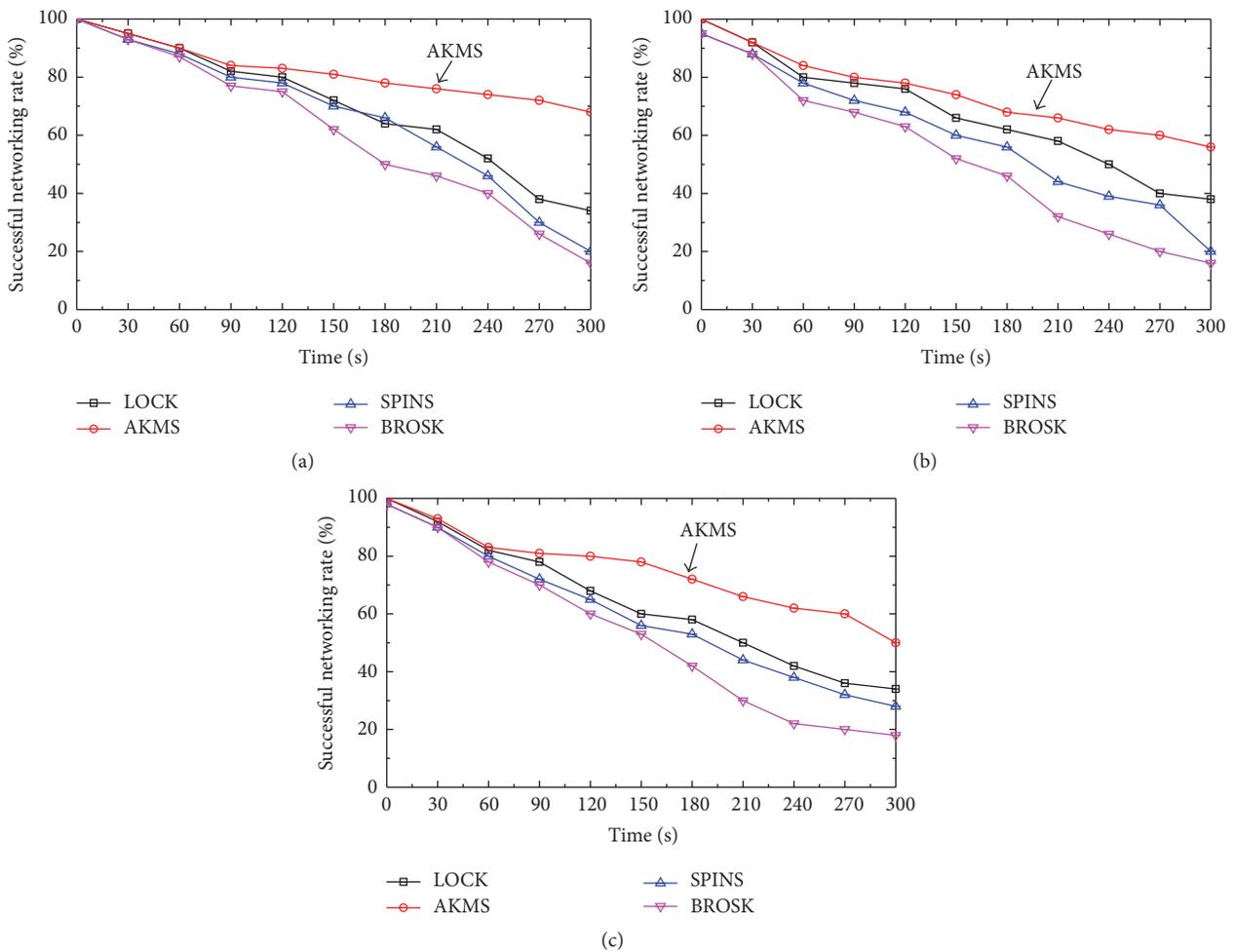


FIGURE 5: (a) Successful networking rate with 25 static attackers. (b) Successful networking rate with 25 mobile attackers. (c) Successful networking rate with static and mobile attackers.

and it will distribute new keys to its cluster members with the help of key generation node (KGN) [20], which will consume more energy.

Thirdly, the impact of network resilience ability has been analyzed and evaluated by the percentage of successful

networking in the network of 500 nodes with 25% being the attacker. Three types of attack scenarios are set with only static attackers, only mobile attacker, and combination of both, and the simulating results are shown in Figures 5(a), 5(b), and 5(c), respectively. AKMS will detect the malicious nodes and

exclude them from the network to avoid them participating in the network activities. Moreover, network environment variation based dynamic key scheme makes it difficult for the attackers to capture node. Even if the nodes are compromised by attackers, it cannot affect the entire network with AKMS.

Figure 5(a) shows the successful networking rate in the presence of 25 static attackers. In LOCK, the key updating is initiated only if the node-capturing rate reaches the Network Resilience Point (Nc). If a certain node in the network is attacked before the key updating, it will be further used by the attacker to destroy the rest of the nodes in the network. Therefore, the proportion of the mobile nodes will be decreasing rapidly. AKMS, however, is able to capture the key that is hidden before distribution or stored in each node in the cluster. Once these keys are captured, the attacker will further attempt to compromise more nodes until AKMS reinitiates the key updating. Since AKMS support mobility, the neighbors of any attacker may move to another cluster, so the performance of AKMS will be better than other schemes, especially in mobile WSN.

Figure 5(b) shows the successful networking rate in the presence of 25 mobile attackers. The attackers in the network are moving with different speed. Generally, the attacker with the maximum speed is able to attack the most nodes by moving from one to another cluster quickly and continuously launching attacks before being recognized and separated. Simulating results and analysis both indicate that the performance of AKMS is better than that of LOCK, SPINS, and BROSK, because AKMS can identify the malicious nodes and isolate them from the network at the same time.

Figure 5(c) shows the successful networking rate in the presence of 10 mobile and 15 static attackers. From the simulation it can be seen that the static attackers are able to be identified before the network becomes stable; the mobile attackers will attack by moving from one to another cluster. AKMS will perform better because of the mobility-support characteristics.

6. Conclusions

The resource-constrained essence of WSN makes the attack threat, security system, and algorithm quite different from those in traditional wireless network. In this paper, a lightweight authentication and key management protocol AKMS has been proposed for wireless sensor networks. It uses the symmetric cryptographic primitives with keyed-hash functions (HMAC) and bidirectional encryption algorithm to provide message confidentiality and authenticity for WSN and reduces the encryption overhead to the minimum as well with just a few bytes to be performed for once per authentication attempt. Simulation results show that the proposed scheme AKMS will provide more efficient security with less energy consumption, control overhead, and packet loss rate than other typical schemes, and the advantages will become remarkable with the number of nodes, attackers, and cycles increasing. Moreover, for the condition that there are mobile sensors in the network, the proposed scheme AKMS performs quite well compared to LOCK, SPINS, and BROSK.

Future research will focus on the way to resist various attacks and robust routing in ubiquitous communication network.

Notations

- k_M : Master key in the whole network
- k_{enc}^A : Encryption key of node A
- $\{M\}_k$: Encryption of message M with key k
- $[M]^i$: Message M is hashed i times without key
- ∇^j : The j th tuple of the i th cycle authenticator
- $[M]$: Hash of message M
- V_{BP} : Virtual battery power
- $[M]_k^i$: Message M is hashed i times with key k
- $[M]_k$: Hash of message M with key k (HMAC)
- k_{auth}^j : Authentication key of the j th authentication cycle; that is, $k_{auth}^j = [k_M]^j$.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (61302074, 61571181), Natural Science Foundation of Heilongjiang Province (QC2013C061), Modern Sensor Technology Research and Innovation Team Foundation of Heilongjiang Province (2012TD007), Postdoctoral Research Foundation of Heilongjiang Province (LBH-Q15121), and Postgraduate Innovation Research Foundation of Heilongjiang University (YJSCX2016-019HLJU).

References

- [1] I. F. Akylidiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.
- [2] Z. Chen, M. He, W. Liang, and K. Chen, "Trust-aware and low energy consumption security topology protocol of wireless sensor network," *Journal of Sensors*, vol. 2015, Article ID 716468, 10 pages, 2015.
- [3] S. Verma and Prachi, "Key pre-distribution scheme for WSNs," *Ad-Hoc and Sensor Wireless Networks*, vol. 23, no. 1-2, pp. 47–67, 2014.
- [4] S. Bag, "A new key predistribution scheme for grid-group deployment of wireless sensor networks," *Ad Hoc and Sensor Wireless Networks*, vol. 27, no. 3-4, pp. 313–329, 2015.
- [5] M. Eltoweissy, M. Moharrum, and R. Mukkamala, "Dynamic key management in sensor networks," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 122–130, 2006.
- [6] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "Spins: security protocols for sensor networks," *Wireless Networks*, vol. 8, no. 5, pp. 521–534, 2002.
- [7] B. C. Lai, D. D. Hwang, S. P. Kim, and I. Verbaauwhede, "Reducing radio energy consumption of key management protocols for wireless sensor networks," in *Proceedings of the ACM International Symposium on Low Power Electronics and Design (ISLPED '04)*, pp. 351–356, Newport Beach, Calif, USA, 2004.

- [8] O. D. Mohatar, A. F. Sabater, and J. M. Sierra, "A light-weight authentication scheme for wireless sensor networks," *Ad Hoc Networks*, vol. 9, no. 5, pp. 727–735, 2011.
- [9] F. Ishmanov, A. S. Malik, S. W. Kim, and B. Begalov, "Trust management system in wireless sensor networks: design considerations and research challenges," *Transactions on Emerging Telecommunications Technologies*, vol. 26, no. 2, pp. 107–130, 2015.
- [10] A. Yener and S. Ulukus, "Wireless physical-layer security: lessons learned from information theory," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1814–1825, 2015.
- [11] J. Rabaey and J. Ammer, "Distributed framework for correlated data gathering in sensor networks," *IEEE Transactions on Mobile Computing*, vol. 57, no. 1, pp. 578–593, 2010.
- [12] K. C. Egemen, B. Dan, and D. Amit, "Modelling communication network challenges for future internet resilience, survivability, and disruption tolerance: a simulation-based approach," *Telecommunication Systems*, vol. 2, no. 6, pp. 751–768, 2013.
- [13] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.
- [14] O. Bazan and M. Jaseemuddin, "A survey on MAC protocols for wireless adhoc networks with beamforming antennas," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 2, pp. 216–239, 2012.
- [15] H. Wang, J. Lai, M. Hu, and Y. Liang, "Research on key technologies for implementing network security situation awareness," *Geomatics and Information Science of Wuhan University*, vol. 33, no. 10, pp. 995–998, 2008.
- [16] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1728–1740, 2013.
- [17] D. Lucas and J. Joel, "A survey on cross-layer solutions for wireless sensor networks," *IEICE Transaction on Journal of Network and Computer Applications*, vol. 5, no. 34, pp. 523–534, 2011.
- [18] C. Wang, X.-Y. Shi, and Z.-H. Niu, "The research of the promotion for ECDSA algorithm based on Montgomery-form ECC," *Journal on Communications*, vol. 31, no. 1, pp. 9–13, 2010.
- [19] K. Okeya and K. Sakurai, "A scalar multiplication algorithm with recovery of the y-coordinate on the montgomery form and analysis of efficiency for elliptic curve cryptosystems," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 85, no. 1, pp. 84–93, 2002.
- [20] G. Anastasi and M. Conti, "Data collection in sensor networks with data mules: an intergrade simulation analysis," *IEEE Symposium on Computers and Communications*, vol. 3, no. 7, pp. 1096–1102, 2012.

Research Article

WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks

Iman Almomani,^{1,2} Bassam Al-Kasasbeh,² and Mousa AL-Akhras^{2,3}

¹Computer Science Department, College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia

²Computer Science Department/Computer Information Systems Department, King Abdullah II School for Information Technology (KASIT), The University of Jordan, Amman, Jordan

³Computer Science Department, College of Computation and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia

Correspondence should be addressed to Iman Almomani; imomani@psu.edu.sa

Received 25 March 2016; Accepted 28 August 2016

Academic Editor: Hana Vaisocherova

Copyright © 2016 Iman Almomani et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Wireless Sensor Networks (WSN) have become increasingly one of the hottest research areas in computer science due to their wide range of applications including critical military and civilian applications. Such applications have created various security threats, especially in unattended environments. To ensure the security and dependability of WSN services, an Intrusion Detection System (IDS) should be in place. This IDS has to be compatible with the characteristics of WSNs and capable of detecting the largest possible number of security threats. In this paper a specialized dataset for WSN is developed to help better detect and classify four types of Denial of Service (DoS) attacks: Blackhole, Grayhole, Flooding, and Scheduling attacks. This paper considers the use of LEACH protocol which is one of the most popular hierarchical routing protocols in WSNs. A scheme has been defined to collect data from Network Simulator 2 (NS-2) and then processed to produce 23 features. The collected dataset is called WSN-DS. Artificial Neural Network (ANN) has been trained on the dataset to detect and classify different DoS attacks. The results show that WSN-DS improved the ability of IDS to achieve higher classification accuracy rate. WEKA toolbox was used with holdout and 10-Fold Cross Validation methods. The best results were achieved with 10-Fold Cross Validation with one hidden layer. The classification accuracies of attacks were 92.8%, 99.4%, 92.2%, 75.6%, and 99.8% for Blackhole, Flooding, Scheduling, and Grayhole attacks, in addition to the normal case (without attacks), respectively.

1. Introduction

Wireless Sensor Networks (WSN) have become increasingly an important field of research due to their wide range of real-time applications like critical military surveillance, battlefields, building security monitoring, forest fire monitoring, and healthcare [1]. A WSN consists of large number of autonomous sensor nodes, which are distributed in different areas of interest to gather important data and cooperatively transmit the collected data wirelessly to a more powerful node called sink node or Base Station (BS) [2, 3]. The data transmitted across the network depend on specialized WSN protocols. Therefore, protecting WSN from different security threats is essential. Unfortunately, achieving this objective becomes a major challenge because of the constrained resources of

WSNs including battery energy, memory, and processing capabilities [4]. Such limiting characteristics make traditional security measures like cryptography not always sufficient for such networks.

WSNs are highly vulnerable to attacks, due to their open and distributed nature and limited resources of the sensor nodes. Moreover, in WSNs packets broadcasting has to be done frequently, sensor nodes can be deployed randomly in an environment so an attacker adversary can be easily injected to a WSN [5].

An attacker can compromise a sensor node, eavesdrop messages, inject fake messages, alter the integrity of the data, and waste network resources. Denial of Service (DoS) attack is considered one of the most general and dangerous attacks that threaten WSN security. This attack has several forms

and its main objective is to interrupt or suspend the services provided by WSNs [6, 7].

Because the process of avoiding or preventing security threats cannot be always successful, an Intrusion Detection System (IDS) is needed to detect known and unknown attacks and alert sensor nodes about them [3, 4]. IDS allows detecting suspicious or abnormal activities and triggers an alarm when an intrusion occurs. The implementation of IDSs for WSNs are more difficult than other systems because sensor nodes are usually designed to be tiny and cheap, and they do not have enough hardware resources. Additionally, there is no specialized dataset that contains normal profiles and attacks in WSN that can be used to detect an attacker signature [3]. Considering the above challenges, there are mainly two conditions while designing IDS for WSNs: The IDS must be of high degree of accuracy in detecting an intruder that includes unknown attacks, and it also must be lightweight to ensure minimum overhead on the infrastructure of WSNs [8].

In this paper a specialized WSN dataset is constructed to characterize four types of DoS attacks in addition to the normal behavior when no attacks exist. WSNs' characteristics and challenges were considered when Low Energy Aware Cluster Hierarchy (LEACH) [9] routing protocol was used in this study. This choice was made since LEACH is one of the most popular hierarchical routing protocols in WSNs that consumes limited energy and is characterized by its simplicity. The constructed dataset is called WSN-DS.

The rest of paper is organized as follows. Section 2 provides an overview of LEACH protocol, IDSs, and reviews related work. Section 3 analyzes LEACH protocol mathematically; Section 4 describes the extracted features of the constructed dataset. Section 5 models different attacks. Section 6 presents the experimental results obtained from IDS and discusses the importance of the achieved results. Conclusions and avenues for future work are presented in Section 7.

2. Background and Related Works

This section presents an overview of LEACH protocol, LEACH-based protocols, DoS, and IDS in WSNs.

2.1. LEACH Protocol Overview. LEACH is a hierarchical routing protocol used in WSNs to increase the network's lifetime [9–11]. LEACH is a clustering, adaptive, and self-organizing protocol. LEACH assumes that BS is fixed and located far from sensor nodes. Additionally, all sensor nodes are homogeneous and have limited energy and memory. Sensors can communicate among each other and they can communicate directly with the BS. The main idea of LEACH protocol is to organize nodes into clusters to distribute the energy among all nodes in the network. Also, in each cluster there is a node called Cluster Head (CH) which aggregates the data received from sensors within its cluster and forward them to the BS. Figure 1 shows the structure of nodes in LEACH routing protocol. Each round in LEACH protocol consists mainly of two phases: setup phase and steady-state phase. In the setup phase, clusters are formed, whereas in the

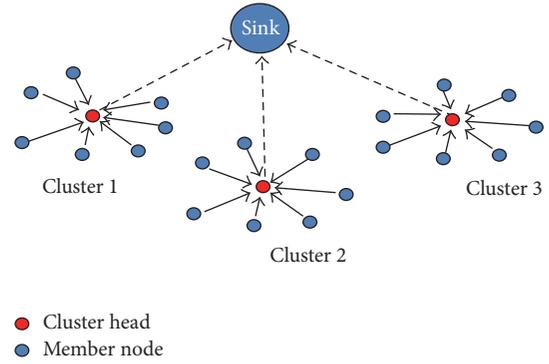


FIGURE 1: Nodes structure in LEACH routing protocol.

steady-state phase, sensed data will be transferred to the sink node [12].

At the beginning of the setup phase, every node generates a random number between 0 and 1, and it then computes a threshold formula $T(n)$, as shown in (1). If the selected random number is less than the threshold value, the node becomes a CH:

$$T(n) = \begin{cases} \frac{0}{1 - p \times (r \bmod p^{-1})}, & \forall n \in N \\ 0, & \text{otherwise,} \end{cases} \quad (1)$$

where p is the CH probability (usually in LEACH a node becomes CH with a probability of 0.05), N : is the set of nodes that have not been a CH, in the last $1/p$ rounds, and r is the current round.

CH in the first round cannot be CH again in the next $1/p$ rounds. After $1/p - 1$ rounds, the threshold value becomes 1 for any sensor node that has not been CH yet, and after $1/p$ rounds, all nodes are eligible again to become CHs. Once CHs are assigned for all clusters, each CH will broadcast an advertisement message (ADV_CH) to the rest of nodes using Carrier Sense Multiple Access-Media Access Control (CSMA-MAC) protocol [9]. After receiving ADV_CH message, each node decides to which cluster it belongs by selecting a CH based on the Received Signal Strength Indication (RSSI) of the advertisement message, the node then sends a (JOIN_REQ) message to the selected CH with the highest RSSI. Each node uses CSMA-MAC protocol to transmit its selection [9, 10]. During the setup phase, all CHs keep their receivers ON. After clusters formation, each CH creates a Time Division Multiple Access (TDMA) schedule according to the number of nodes in its cluster called Cluster Members (CM) and broadcasts it to them.

During steady-state phase, each sensor node collects data and transmits them to its CH during its allocated time slot according to the TDMA schedule. CHs receive all the data and aggregate them before sending them to the BS. After a predetermined time, the network starts another round by going back to the setup and steady-state phases again [9].

2.2. LEACH-Based Protocols. LEACH was and still is studied in enormous number of research articles. The authors in [13]

provided a review of 27 clustering and routing techniques based on LEACH protocol for WSNs that includes a comprehensive discussion and comparisons among them. The authors in [14, 15] highlighted LEACH protocol and presented fifteen LEACH improved versions introduced in the literature. The papers have compared some features of several variants of LEACH protocol not empirically but based on their descriptions. In [16] the author proposed and evaluated two new clustering-based protocols for heterogeneous WSNs that were built based on LEACH protocol by considering three types of nodes with different battery energies, which was the source of heterogeneity in the author's protocols.

LEACH-ICE (LEACH Inner Cluster Election) algorithm based on LEACH algorithm was introduced in [17]. The threshold function of the node selected as CH is adjusted. Also, direct communication with the BS occurs when a node is closer to the BS. To improve the clustering mechanism, LEACH-ICE elects a new CH inside the cluster when the resident energy of the current CH is lower than a predefined threshold.

In [18] the authors proposed an energy efficient secondary CH selection algorithm for WSN. By controlling the distances among the CHs, a uniform distribution of CHs is satisfied. Two-level hierarchy mode was applied to transmit data to the BS. LEACH is compared with the improved LEACH-TLCH method. Simulation results show that the improved method can reduce the network consumption of energy and lengthen the network's lifetime.

In [19], a distributive Energy Neutral Clustering (ENC) protocol was proposed to group the network into several clusters, with the goal of providing perpetual network operation. ENC employs a novel Cluster Head Group (CHG) mechanism that allows a cluster to use multiple CHs to share heavy traffic load and to reduce the frequency of cluster reformation. An extension to ENC based on convex optimization techniques of the number of clusters was proposed to group the network into equal-sized clusters to maximize network information gathering. According to the authors' experiments, the proposed protocol can successfully prevent sensors from shutting down due to excessive usage of energy.

2.3. DoS and IDS in WSN. As mentioned earlier, DoS is a common attack that could have a severe impact on WSN's functionalities and services [20]. Many different types of DoS attacks have been identified so far, for example, Blackhole attack, Grayhole attack, Flooding attack, and Wormhole. The seriousness of DoS attack stems from the fact that most WSN applications require the deployment of a sensor node in harsh environments where they are far away and difficult to be controlled [20, 21]. Recently, many researches are going on in an attempt to find solutions for DoS attacks, but mainly they have tackled one or two forms of these attacks but not the majority [2, 22–24]. Moreover, they offer partial solutions and they cannot be applied concurrently because they will consume high energy, which is not practical in WSNs [2, 25]. Therefore, a mechanism should be found to identify different behaviors of DoS attacks and classify them to take effective countermeasures.

Cryptography is a security mechanism that is used for protecting WSN against external attacks. It ensures many security services including integrity and authentication by checking the data packet source and its contents using several techniques such as symmetric encryption, public key cryptography, and hash functions [25]. These techniques cannot be used to detect internal attacks when security keys are exposed to the attacker which uses them to perform encryption and decryption of messages' contents. Consequently, such techniques serve as first line of defense [5]. Attackers always attempt to launch new and unknown attacks in more than one way; therefore, it is necessary to create an efficient IDS, which acts as a second line of defense to detect known and unknown attacks and alert sensor nodes about them. IDS allows detecting suspicious or abnormal activities and triggers alarms when intrusions are detected [26].

The National Institute of Standards and Technology (NIST) [27] categorized intrusion detection into two main approaches: anomaly detection and misuse detection. In anomaly detection the system depends on prior knowledge of normal behavior of the network which will be then compared with its current activities. In misuse detection, the system depends on prior knowledge of attack signatures. It compares the signature with the current activities in the network.

IDS has become an important security component of WSNs; however, the implementation of IDS in WSNs introduces number of challenges that can have negative impact on WSN performance [28]. It is inefficient to use IDS in every sensor node due to the resource-constrained nature of such nodes. IDS components should be installed in places where sensor nodes can be followed to be able to defend against certain threats to the network. IDS is also used in WSNs where huge amount of traffic is transmitted; therefore, there is a possibility an intrusion could be missed as sensor nodes generally have restrictions in handling huge data in the network.

There are two main components of IDS, features extraction and modeling algorithm. Features extraction defines measured attributes that are linked to the IDS functionalities. Modeling algorithm is the main component; the accuracy and the efficiency of detecting and responding to intrusions depend on the modeling algorithm. IDS may have components that depend on the network characteristics and possible intrusions [29]. Most of IDSs have six common components as shown in Figure 2:

- (1) Monitoring component: which is used for local activity monitoring or for monitoring neighbor sensor nodes. This component mostly monitors internal activities, traffic patterns, and resource utilization.
- (2) Analysis component: which contains all records of normal and abnormal behaviors for all nodes in the network [30].
- (3) Detection component: which is the main component that is built based on the modeling algorithm. It works after analyzing network behaviors. Decisions are made to declare such behaviors as malicious or not [31].

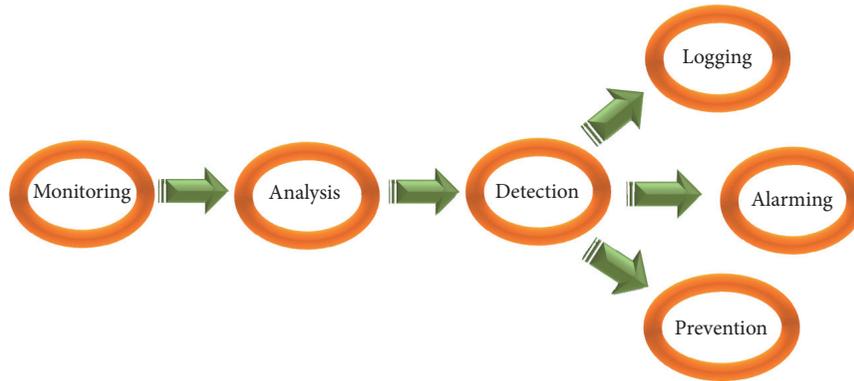


FIGURE 2: IDS components.

The other three components of IDS consist of actions that can be taken, either one, two, or all of them [32]:

- (4) Logging: storing each packet in a log file so that security administrator can use it for later analysis.
- (5) Alarming: a responding generating component in case of detection of an intrusion. The response may trigger an alarm to announce the misbehaving node(s).
- (6) Prevention: an advanced step that can be added to IDS to enable it to take an action to prevent dealing with an attack once detected. This can be done, for example, by excluding harmful nodes from the network [30].

Designing a specialized dataset for WSN to achieve better detection and classification of DoS attacks is the main aim of this paper. The authors in [30] presented current IDSs and a comparison among them. The authors revised mechanisms, attacks, and evaluation metrics but without mentioning the use of specialized datasets. The comparison depended on the type of IDSs, whether it is anomaly-based, signature-based, hybrid, or cross layer.

Knowledge Discovery and Data Mining Tools Competition (KDD) dataset [33] was constructed for Local Area Network (LAN). KDD is not specialized for wireless in general and WSN in particular, even though many researchers have used it to deal with fraud and intrusion detection [34].

Anomaly, signature, and hybrid-based IDSs have been reviewed in [35]. Mainly KDDCup-99 was used in these IDSs. For example, in the eight studied hybrid-based IDSs, four of them have used KDDCup-99 and the rest have used real data samples.

Other researches which also considered KDD in their analysis and classifications can be found in [36–38].

It can be concluded that there is no specialized dataset for WSN that has been reported in the literature for detecting and classifying as many DoS as possible. Therefore, there is an urgent need to define a labelled, specialized dataset that successfully characterizes WSN to help in studying normal and anomaly behaviors. The construction and testing of such dataset are proposed in this paper.

3. LEACH Mathematical Analysis

To ensure the correctness of the constructed dataset called WSN-DS, a mathematical analysis has been conducted to all LEACH phases and then has been compared to the results of simulation in case of normal situation when there is no DoS attack. The terms used in LEACH's mathematical model are listed as follows:

LEACH Mathematical Model Terms

N : number of sensor nodes in WSN

S_i : sensor node i

NC : number of CHs

CM : number of members within a cluster

$ADV-CH-SENT$: number of advertisement messages sent by CH

$ADV-CH-RCVD$: number of advertisement messages received by sensor nodes

$JOIN-REQ-SENT$: number of join request messages sent by sensor nodes

$JOIN-REQ-RCVD$: number of join request messages received by CHs

$TDMA-SENT$: number of TDMA schedules sent by CHs

$TDMA-RCVD$: number of TDMA schedules received by sensor nodes

$NO-DATA-PKT$: number of data packets received by a CH

3.1. Advertisement Phase. Theorem 1 calculates the number of advertisement messages that are sent by CHs and received by CMs in a specific round as follows.

Theorem 1. *In the advertisement phase of LEACH, maximum $ADV-CH-SENT$ in a specific round is NC and the maximum $ADV-CH-RCVD$ is $(N - 1) * NC$.*

TABLE 1: Comparison between the mathematical model and simulation results.

Round	Number of clusters	ADV-CH-Sent		ADV-CH-Rcvd		Join-Req-Sent		Join-Req-Rcvd		BS receives	
		Math	Sim.	Math	Sim.	Math	Sim.	Math	Sim.	Math	Sim.
1	4	4	4	396	396	96	96	96	96	238	238
2	2	2	2	198	198	98	98	98	98	53	53
3	3	3	3	297	297	97	97	97	97	126	126
4	2	2	2	198	198	98	98	98	98	59	59
5	7	7	7	693	693	93	93	93	93	563	563
6	6	6	6	594	594	94	94	94	94	516	516
7	4	4	4	396	396	96	96	96	96	268	268
8	4	4	4	396	396	96	96	96	96	291	291
9	5	5	5	495	495	95	95	95	95	447	447
10	7	7	7	693	693	93	93	93	93	695	695
11	6	6	6	594	594	94	94	94	94	456	456
12	6	6	6	594	594	94	94	94	94	363	363
13	1	1	1	99	99	99	99	99	99	13	13
14	7	7	7	693	693	93	93	93	93	629	629

TABLE 2: Applying Theorem 3 equation to round 1 of simulation round.

Cluster number	Number of nodes within CH	Number of packets received(No-DATA-PKT)	Number of packets sent to BS
Cluster 1	25	1200	48
Cluster 2	30	1230	41
Cluster 3	8	880	111
Cluster 4	33	1254	38
Applying Theorem 3 equation $\sum_{i=1}^{NC}(\text{NO-DATA-PKT}/\text{CM of CH}_i)$			Total: 238

Proof. According to LEACH, each CH in each round is supposed to broadcast an advertisement message to the rest of nodes. Therefore, in case of having NC cluster heads, then ADV-CH-SENT equals NC. On the other hand, these advertisement messages (NC) will be received by all sensor nodes (N) except the CH node itself which equals $(N - 1) * NC$. \square

3.2. Cluster Setup Phase. Theorem 2 calculates the number of join request messages sent by sensor nodes and received by CHs in order to associate with them.

Theorem 2. In clusters setup phase of LEACH, the maximum JOIN-REQ-SENT equals JOIN-REQ-RCVD which is $N - NC$.

Proof. According to LEACH, once each sensor node has decided to which cluster it will belong, then it informs its CH by sending a (JOIN_REQ) message. Therefore, all sensor nodes (N) except CHs (NC) will send (JOIN_REQ) messages $(N - NC)$ and these messages will also be received by CHs. \square

3.3. Data Transmission Phase. Theorem 3 calculates the amount of sensed data packets that are delivered to the BS at the end of each round.

Theorem 3. In the data transmission phase of LEACH, at the end of each round, BS receives $\sum_{i=1}^{NC}(\text{NO-DATA-PKT}/\text{CM of CH}_i)$ packets.

Proof. According to LEACH, when the CH receives the sensed data from the sensors nodes (CMs) according to their time slots assigned by TDMA schedule, it aggregates them into one packet and sends it to the BS. Throughout the round, the number of packets sent to the CH from CMs is (NO-DATA-PKT) but due to the aggregation process only $(\text{NO-DATA-PKT}/\text{CMs of CH}_i)$ packets will be sent to the BS. Having NC of CHs, then the overall data packets received by BS are $\sum_{i=1}^{NC}(\text{NO-DATA-PKT}/\text{CM of CH}_i)$. \square

3.4. Comparison between Mathematical Model and Simulation Results. To confirm the correctness of the simulation which is used to collect data to construct the dataset, a comparison is performed between the mathematical analysis and simulation results. The comparison will be based on sample of the simulation results representing the first 14 rounds as after this round nodes start to die. In the first 14 rounds, the number of alive nodes is 100. Table 1 shows this comparison. The mathematical results were obtained by applying the equations in Theorems 1–3, while the simulation results were obtained from Network Simulator 2 (NS-2) simulator.

For more clarification, Table 2 presents how the mathematical formula of Theorem 3 is applied to a sample round (Round 1) in one of the simulation scenarios to calculate the number of received data packets by BS.

Table 1 shows 100% match between the mathematical model and the simulation results. This is due to the behavior of LEACH protocol which implements dynamic

TABLE 3: Observations for five different simulation scenarios (A–E) when determining the number of nodes monitored by each node.

Number of neighbors to watch	Max number of monitors for a specific node					Min number of monitors for a specific node					Number of overall monitored nodes				
	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E
3	6	7	7	6	7	0	0	0	1	0	97	99	99	100	97
4	7	9	8	8	9	0	0	0	1	0	99	99	99	100	99
5	10	9	10	10	10	1	1	1	1	2	100	100	100	100	100
6	11	12	11	10	13	1	1	1	2	2	100	100	100	100	100

TDMA Scheduling technique at the data transmission level. Additionally, it uses both Code Division Multiple Access (CDMA) and CSMA codes to avoid and reduce collisions and interferences that may exist in the network.

4. WSN-DS Dataset Description and Creation

In order to build the dataset and collect the required data from the sent and received packets within WSN, a monitoring service is needed with minimum cost. On the other hand, we need to guarantee that necessary data related to the network which help in detecting, classifying, and then preventing different possible attacks are collected. In this research, to distribute the load among sensor nodes, each sensor will take part in the monitoring process and should be able to monitor set of its neighbors. The challenge was how to find the suitable number of nodes to be watched by a sensor node in order to monitor all network sensors. Many experiments have been conducted to decide on this number and the summary of the results is shown in Table 3.

When each sensor node has watched 3 nodes of its neighbors, it has been noticed that the largest number of sensor nodes which could be monitored by a single node was seven. In other words, the BS has received seven different reports about the same node from seven different watching nodes. To make sure that the received information are correct, these reports could be checked for consistency. In some scenarios, some sensor nodes were not monitored by any sensor. This indicates that monitoring 3 neighboring nodes is not enough to get information about all network sensor nodes.

Additionally, an improvement has occurred when 4 neighbors are being watched. But only when the number is 5, all sensor nodes are being watched in all 5 scenarios. Similar results have been obtained when a sensor node was watching 6 of its neighbors. Consequently, it has been found that monitoring 5 neighbors is enough to get information about all nodes in the network and there is no need to increase the computational complexity by going further.

Choosing 5 neighbors to be monitored is done at the beginning of the simulation. All nodes broadcast a *Hello* message. Accordingly, each node selects the first 5 nodes it heard from. Then it monitors them over the simulation period, so that each node sends a report to its CH at the end of each round. Then the CH sends the received reports to the BS. For security purposes and in case of suspecting the CH and having one monitor for this node (one report),

these reports could be sent directly to the BS at the expense of consuming more energy if this node is further from the BS than the CH. After deep study of LEACH routing protocol, we have succeeded to extract 23 attributes to help in identifying the status of each node in the network, These attributes are listed as follows.

WSN-DS Dataset Attributes

Node ID: a unique ID to distinguish the sensor node in any round and at any stage. For example, node number 25 in the third round and in the first stage is to be symbolized as 001 003 025.

Time: the current simulation time of the node.

Is CH? A flag to distinguish whether the node is CH with value 1 or normal node with value 0.

Who CH? The ID of the CH in the current round.

RSSI: Received Signal Strength Indication between the node and its CH in the current round.

Distance to CH: the distance between the node and its CH in the current round.

Max distance to CH: the maximum distance between the CH and the nodes within the cluster.

Average distance to CH: the average distance between nodes in the cluster to their CH.

Current energy: the current energy for the node in the current round.

Energy consumption: the amount of energy consumed in the previous round.

ADV_CH send: the number of advertise CH's broadcast messages sent to the nodes.

ADV_CH receives: the number of advertise CH messages received from CHs

Join_REQ send: the number of join request messages sent by the nodes to the CH.

Join_REQ receive: the number of join request messages received by the CH from the nodes.

ADV_SCH send: the number of advertise TDMA schedule broadcast messages sent to the nodes.

ADV_SCH receives: the number of TDMA schedule messages received from CHs.

Rank: the order of this node within the TDMA schedule.

```

 $N$  → Network Size
 $SN$  → Sensor Node
 $MN$  → Malicious Node
 $CH$  → Cluster Head
 $BS$  → Base Station
 $CM$  → Cluster Member
 $NC$  → Cluster Heads list
 $x$  → Integer value between 0 and  $N - 1$ 
 $\forall SN_i, 0 < i \leq N$ , compute  $T(SN_i)$  and random  $r_{SN_i}$ 
IF ( $r_{SN_i} < T(SN_i)$ ) THEN
     $SN_i = CH$ 
ELSE
     $SN_i = CM$ 
ENDIF
 $\forall CH_j, j \in NC$ 
{
     $CH_j$  broadcasts the advertisement message (ADV_CH)
     $x$  CMs will join  $CH_j$ 
     $CH_j$  creates TDMA schedule
     $x$  CMs send data to  $CH_j$  in the corresponding TDMA time slot
}
IF  $CH_j = MN$  THEN
    Performs the attack by dropping all packets
ELSE
    Sends aggregated data to BS
ENDIF

```

ALGORITHM 1: Model of Blackhole attack.

Data sent: the number of data packets sent from a sensor to its CH.

Data received: the number of data packets received from CH.

Data sent to BS: the number of data packets sent to the BS.

Distance CH to BS: the distance between the CH and the BS.

Send Code: the cluster sending code.

Attack Type: type of the node. It is a class of five possible values, namely, Blackhole, Grayhole, Flooding, and Scheduling, in addition to normal, if the node is not an attacker.

5. Attack Models

Four types of DoS attacks in LEACH protocol are implemented in the constructed dataset; Blackhole, Grayhole, Flooding, and Scheduling attacks. This section models each one of these attacks. To ensure proper distribution of the attacker nodes, the network terrain has been divided into 10 regions. Then the attackers' ratios according to the simulation scenario were distributed randomly within these regions.

5.1. Blackhole Attack. Blackhole attack is a type of DoS attack where the attacker affects LEACH protocol by advertising itself as a CH at the beginning of the round. Thus, any node that has joined this CH during this round will send the data

packets to it in order to be forwarded to the BS. The Blackhole attacker assumes the role of CH and it will keep dropping these data packets and not forwarding them to the BS [39–41]. Algorithm 1 shows the algorithm of Blackhole attack.

To implement this attack in the simulation environment, several attackers' intensities (10%, 30%, and 50%) have been injected randomly to perform Blackhole attack. These attackers which act as CHs will drop all the packets relayed through them in their way to the BS.

5.2. Grayhole Attack. Grayhole attack is a type of DoS attack where the attacker affects LEACH protocol by advertising itself as a CH for other nodes. Therefore, when the forged CH receives data packets from other nodes, it drops some packets (randomly or selectively) and prevents them from reaching the BS [40–42]. Algorithm 2 shows the algorithm of Grayhole attack.

Similar to Blackhole attack, 10%, 30%, and 50% of the sensor nodes are injected randomly to implement the Grayhole attack. The decision whether to forward a specific packet or not is also devised randomly. But the decision can be done selectively based on the sensitivity of the sensed data carried by the packet.

5.3. Flooding Attack. Flooding attack is a type of DoS attack where the attacker affects LEACH protocol in more than one way. This research studies the impact of Flooding attack by sending large number of advertising CH messages (ADV_CH) with high transmission power. Consequently, when sensors receive large number of ADV_CH messages,

```

N → Network Size
SN → Sensor Node
MN → Malicious Node
CH → Cluster Head
BS → Base Station
CM → Cluster Member
NC → Cluster Heads list
x → Integer value between 0 and N - 1
∀ SNi, 0 < i ≤ N, compute T(SNi) and random rSNi
IF (rSNi < T(SNi)) THEN
    SNi = CH
ELSE
    SNi = CM
ENDIF
∀ CHj, j ∈ NC
{
    CHj broadcasts the advertisement message (ADV_CH)
    x CMs will join CHj
    CHj creates TDMA schedule
    x CMs send data to CHj in the corresponding TDMA time slot
}
IF CH = MN THEN
    Performs the attack by dropping some packets (randomly or selectively)
ELSE
    Sends aggregated data to BS
ENDIF

```

ALGORITHM 2: Model of Grayhole attack.

this will consume sensors' energy and waste more time to determine which CH to join. Moreover, the attacker attempts to cheat victims to choose it as a CH, especially those nodes that are located on a far distance from it in order to consume their energy [40, 43]. Algorithm 3 shows the algorithm of Flooding attack.

Flooding attack has been implemented in several ways in the simulation environment. In some experiments 10 ADV_CH messages were sent by the attacker; other scenarios consider 50 ADV_CH messages to be sent or a random number between 10 and 50. The idea is when more ADV_CH messages are sent, more messages will be received and more energy will be consumed. We have already studied in [44] the impact of Flooding attack on WSN lifetime. The energy consumption was shown in each round using several attackers' ratios.

5.4. Scheduling Attack. Scheduling attack was introduced in a previous study of the authors [44]. Scheduling attack occurs during the setup phase of LEACH protocol, when CHs set up TDMA schedules for the data transmission time slots. The attacker which acts as a CH will assign all nodes the same time slot to send data. This is done by changing the behavior from broadcast to unicast TDMA schedule. Such change will cause packets collision which leads to data loss. Algorithm 4 shows the algorithm of Scheduling attack.

The implementation of Scheduling attack is performed by setting the same time for all Cluster Members to send their data packets. Other scenarios assign every two nodes the same time or every five nodes the same time.

In [44] it has been shown that the risk of DoS attackers on LEACH protocol services could be significant. The attackers can influence the network in more than one way, through wasting the nodes' energy or dropping their data packets. This badly affects the services provided by WSN. Therefore, a methodology to detect such attacks and protect different services provided by WSN is urgently required.

Section 6 illustrates the importance of studying normal and anomaly (under attack) behaviors of WSN protocols and presenting them through a specialized dataset (WSN-DS). WSN-DS allows several intelligent and data mining approaches to be applied for the aim of better detection and classification of DoS attacks. As a result, sensor nodes will be more experienced with the normal behaviors and attackers' signatures and will be able to make proper decisions at the right time. In this research ANN is applied to test the constructed dataset and measure its accuracy in detecting and classifying four types of DoS attacks.

6. Experiments and Results

In this paper, WSN-DS, a specialized dataset for WSN to detect DoS attacks, was constructed. LEACH protocol was used to collect the dataset because it is one of the most common and widely used routing protocols in WSNs. WSN-DS contains 374661 records that represent four types of DoS attacks: Blackhole, Grayhole, Flooding, and Scheduling attack, in addition to the normal behavior (no-attack) records. Table 4 shows sample from WSN-DS dataset to help in detecting and classifying DoS attacks.

```

N → Network Size
SN → Sensor Node
MN → Malicious Node
CH → Cluster Head
BS → Base Station
CM → Cluster Member
NC → Cluster Heads list
x → Integer value between 0 and N - 1
∀ SNi, 0 < i ≤ N, compute T(SNi) and random rSNi
IF (rSNi < T(SNi)) THEN
    SNi = CH
ELSE
    SNi = CM
ENDIF
∀ CHj, j ∈ NC
{
    IF CHj = MN THEN
        CHj broadcasts a lot of advertisement messages (ADV_CH) with
        high transmitting power.
    ELSE
        CHj broadcasts normal advertisement message (ADV_CH)
    ENDIF
    x CMs will join CHj
    CHj creates TDMA schedule
    x CMs send data to CHj in the corresponding TDMA time slot
}

```

ALGORITHM 3: Model of Flooding attack.

```

N → Network Size
SN → Sensor Node
MN → Malicious Node
CH → Cluster Head
BS → Base Station
CM → Cluster Member
NC → Cluster Heads list
x → Integer value between 0 and N - 1
∀ SNi, 0 < i ≤ N, compute T(SNi) and random rSNi
IF (rSNi < T(SNi)) THEN
    SNi = CH
ELSE
    SNi = CM
ENDIF
∀ CHj, j ∈ NC
{
    CHj broadcasts the advertisement message (ADV_CH)
    x CMs will join CHj
    IF CHj = MN THEN
        CHj performs the attack by creating the TDMA schedule and give all nodes
        same time slot to send data
    ELSE
        CHj creates normal TDMA schedule
    ENDIF
    x CMs send data to CHj in the corresponding TDMA time slot
    CHj sends aggregated data to BS
}

```

ALGORITHM 4: Model of Scheduling attack.

TABLE 4: Sample from WSN-DS dataset.

Id	Time	Is_CH	Who_CH	CH_To_CH	ADV_S	ADV_R	JOIN_S	JOIN_R	SCH_S	SCH_R	Rank	DATA_S	DATA_R	Data_Sent_To_BS	Dist_CH_To_BS	Send_code	Consumed energy	Attack type
106079	303	1	106079	0	1	3	0	0	75	1	0	0	1350	7	108.34705	0	1.64035	Grayhole
107033	353	1	107033	0	1	3	0	0	71	1	0	0	1349	9	162.5505	0	2.03296	Grayhole
115021	753	1	115021	0	1	5	0	0	59	1	0	0	1298	0	0	0	0.00721	Blackhole
117044	853	1	117044	0	1	4	0	0	54	54	0	0	0	0	0	0	0.00723	Scheduling
103043	153	1	103043	0	1	4	0	0	47	1	0	0	1269	14	145.08942	0	1.88023	Grayhole
105005	253	1	105005	0	1	9	0	0	47	1	0	0	1170	7	137.59248	0	0.92063	Grayhole
110024	503	1	110024	0	1	9	0	0	35	1	0	0	1200	15	113.27654	0	2.0577	Grayhole
101041	53	1	101041	0	1	0	0	0	34	1	0	0	1258	0	0	0	0.00225	Blackhole
102040	103	1	102040	0	1	2	0	0	31	1	0	0	1240	0	0	0	0.00728	Blackhole
201061	1003	1	201061	0	1	7	0	0	31	1	0	0	1240	0	0	0	0.00719	Blackhole
118058	903	1	118058	0	1	5	0	0	27	27	0	0	0	0	0	0	0.00724	Scheduling
103003	153	1	103003	0	1	4	0	0	22	1	0	0	1166	29	85.19787	0	2.06959	Grayhole
111050	553	0	111093	15.17406	0	2	1	0	0	0	1	10	22	0	0	1	0.04156	Normal
111057	553	0	111093	15.91573	0	2	1	0	0	0	1	3	22	0	0	1	0.04172	Normal
402054	1253	1	402054	0	6	22	0	0	0	0	0	0	0	13	142.10787	0	0.24255	Flooding
402063	1253	1	402063	0	6	28	0	0	0	0	0	0	0	13	123.96292	0	0.23082	Flooding
402069	1253	1	402069	0	6	22	0	0	0	0	0	0	0	13	93.93772	0	0.21998	Flooding
118046	903	1	118046	0	1	5	0	0	21	21	0	0	0	0	0	0	0.00722	Scheduling
110044	503	1	110044	0	1	9	0	0	20	1	0	0	1087	23	121.40806	0	1.92349	Grayhole
117061	853	1	117061	0	1	9	0	0	20	1	0	0	1131	0	0	0	0.00728	Blackhole
201021	1003	1	201021	0	1	7	0	0	20	1	0	0	1140	0	0	0	0.0072	Blackhole
101021	53	1	101021	0	1	0	0	0	17	1	0	0	1105	0	0	0	0.00225	Blackhole
117039	853	1	117039	0	1	4	0	0	14	14	0	0	0	0	0	0	0.00723	Scheduling
117095	853	1	117095	0	1	4	0	0	14	14	0	0	0	0	0	0	0.00722	Scheduling
103029	153	1	103029	0	1	3	0	0	10	1	0	0	960	0	0	0	0.00724	Blackhole
118031	903	1	118031	0	1	5	0	0	5	5	0	0	0	0	0	0	0.00736	Scheduling
111053	553	0	111028	19.42763	0	2	1	0	0	0	1	37	32	0	0	2	0.1789	Normal
111051	553	0	111028	21.35118	0	2	1	0	0	0	1	33	32	0	0	2	0.057	Normal
111055	553	0	111028	36.99519	0	2	1	0	0	0	1	31	32	0	0	2	0.0582	Normal
111054	553	0	111028	43.03687	0	2	1	0	0	0	1	24	32	0	0	2	0.05904	Normal
111060	553	0	111028	40.20187	0	2	1	0	0	0	1	20	32	0	0	2	0.05894	Normal

TABLE 5: Ns-2 simulation parameters.

Parameter	Value
Number of nodes	100 nodes
Number of clusters	5
Network area	100 m × 100 m
Base station location	(50, 175)
Size of data packet	500 bytes
Size of packet header	25 bytes
Maximum transmission range	200 m
Routing protocol	LEACH
MAC protocol	CSMA/TDMA
Simulation time	3600 s
Initial energy (in joule)	5, 50
Attackers' intensities	10%, 30%, 50%

In order to gather the required data, NS-2 was used [45]. Simulation parameters are summarized in Table 5.

This section shows the results obtained from the dataset collected as described in Section 4. Waikato Environment for Knowledge Analysis (WEKA) Toolbox was used in the simulation experiments to evaluate the proposed dataset. WEKA is an open source data mining software suite built using Java programming language and developed at the University of Waikato in New Zealand. Data mining algorithms in WEKA could be applied to datasets and be called using either WEKA's interface or user customized Java code. WEKA contains a lot of algorithms for data preprocessing, clustering, classification, association rules, regression, and visualization [46, 47].

Experiments were conducted on an Intel® Core™ i5-4210U CPU @ 1.70 GHz 2.40 GHz, 8.00 GB RAM with Windows 8.1 64-bit Operating System.

Because different performance metrics are appropriate in different settings, in this paper seven performance metrics are used: True Positive Rate (TPR), True Negative Rate (TNR), False Positive Rate (FPR), False Negative Rate (FNR), Overall Accuracy (A), Precision (P), and Root Mean Square Error (RMSE).

TPR represents the rate of attack cases identified correctly, TNR represents the rate of normal (no-attack) cases identified correctly, FPR represents the rate of no-attack cases identified as attacks by the system, and FNR represents the rate of attack cases identified as normal ones. A is the total rate of correct decisions whether identifying an attack correctly or deciding there is no attack when really there is no attack. P represents the predicted positive cases that were correctly classified; RMSE provides information on the efficiency that indicates the difference between the outputs and the targets. Lower values of RMSE indicates more accurate evaluation. Zero means no error:

$$TPR = \frac{TP}{TP + FN}, \quad (2)$$

$$TNR = \frac{TN}{FN + TP}, \quad (3)$$

$$FPR = \frac{FP}{FP + TN}, \quad (4)$$

TABLE 6: Dataset separated 60% training set and 40 testing sets using holdout method.

The attack type	Training set (60%)	Testing set (40%)
Blackhole	6029	4020
Grayhole	8758	5838
Flooding	1988	1324
Scheduling	3982	2656
Normal	204039	136027
<i>Sum</i>	<i>224796</i>	<i>149865</i>

$$FNR = \frac{FN}{FN + TP}, \quad (5)$$

$$A = \frac{TP + TN}{TP + TN + FP + FN}, \quad (6)$$

$$P = \frac{TP}{TP + FP}, \quad (7)$$

$$RMSE = \sqrt{\frac{\sum_{i=1}^n (O_i - T_i)^2}{n}}, \quad (8)$$

where TP is the number of attack cases classified correctly as attacks. TN is the number of normal (no-attack) cases classified correctly as normal (no-attack). FP is the number of normal (no-attack) cases classified incorrectly as attacks. FN is the number of attack cases classified incorrectly as normal (no-attack). O_i and T_i are the output and target values, respectively, and n is the total number of data points.

The classification results of this dataset were obtained through a number of test cases applied using Artificial Neural Networks (ANNs), which can be built in several ways. ANN is used as a classifier were the 23 attributes extracted from the simulation experiments are used as inputs and the type of attack, including the normal case, is used as output. ANN training algorithm includes a built-in procedure to help minimizing the error between the neural network output and the desired output. Its iterative training procedure terminates when that error reaches a value below a predetermined threshold. After the training phase, the trained neural network is used on the test dataset to check its generalization accuracy.

We are extracting different results with two ANNs test options. The first one is by using holdout method where the dataset is separated to 60% training data and 40% testing data. Table 6 shows data separation using holdout method.

The second option is by using 10-Fold Cross Validation which separates the training dataset into 10 equal parts. This method trains ANN using nine of the 10 parts and evaluates it with the remaining part. The same process is repeated for all 10 parts using a sliding window to determine the test set and the remaining parts are used for training the ANN. After the completion of the 10 iterations, the results are compiled and averages are computed. The main advantage of the 10-Fold Cross Validation is using all records in the dataset alternately for both training and testing. On the other hand, it is computationally expensive.

TABLE 7: Parameters for MLP neural network classifier.

Parameter	Explanation	Used value
L	Learning rate: used for weight adjustment on each iteration. (The value should be between 0 and 1.)	0.3
M	Momentum: used for weight adjustment during backpropagation, in order to speed up convergence and avoid local minima. (The value should be between 0 and 1.)	0.2
N	The number of epochs or passes through training data.	500
V	The percentage of the validation set from the training data.	20%
S	Seed for random number generator. Random numbers are used for setting initial weights for the connections between nodes. (The value should be ≥ 0 .)	0
E	Threshold for consecutive errors allowed during validation testing before the neural network terminates. (The value should be > 0 .)	20
H	Number of nodes in the hidden layer which is represented as follows: number of hidden layers (number of neurons in each layer).	1 (11) 2 (11, 5) 3 (11, 5, 2)

An important parameter of ANNs is the used transfer function. In this study the most common activation (transfer) function which is the logistic sigmoid function was used. This function is also called log-sigmoid. The function is defined as

$$a = \frac{1}{1 + e^{-n}}. \quad (9)$$

The logistic sigmoid function accepts any value and returns a value between 0 and 1. Because of the nonlinear characteristics of this function, it allows ANNs to model complex data with possible built-in nonlinearities.

Table 7 shows the parameters and the values used in this paper for WEKA toolbox Multilayer Perceptron (MLP) ANN classifier configuration. MLP is the most popular ANN variation that allows configuration of multilayer ANN which is able to model complex relations between the input and output parameters.

Several ANN architectures were attempted in this paper, an ANN with one hidden layer and 11 neurons is used. Moreover, an ANN with two hidden layers with 11 neurons in the first layer and 5 neurons in the second hidden layer was used. Finally, ANN with three hidden layers with 11 neurons in the first layer, 5 neurons in the second hidden layer, and two neurons in the third hidden layer was also attempted.

By using the holdout method to train the ANN with one hidden layer, an overall classification accuracy of 97.5431% was achieved. This corresponds to correctly classifying 146184 out of 149865 in the testing set as can be noticed from Table 6.

Table 8 shows the Confusion matrix for this method. For example, there are 2656 records in the testing set for Scheduling attack as shown in Table 6. 2620 records were classified correctly as Scheduling attack, 23 records were

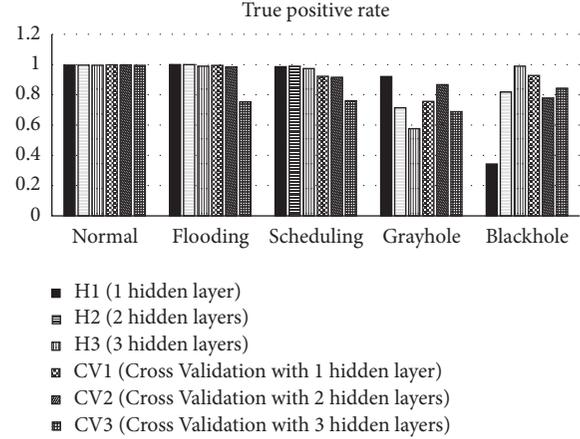


FIGURE 3: True positive results.

classified as no-attack, 3 records were classified as Grayhole attacks, and 10 records were classified as Blackhole attack. This means that the percentage of positive classification of Scheduling attack is 98.6%. The percentage of samples that were incorrectly classified as positive while they are normal is 0.4%.

Table 9 shows the results of the remaining metrics for the holdout method. RMSE as calculated in (8) is 0.073 which is an acceptable value.

From Table 9, it can be concluded that the accuracy of detecting Blackhole attack was (34.3%), which is a low percentage. For that reason, an ANN architecture that has two hidden layers was attempted. In this case, 98% (avg. of TPR) of DoS cases were correctly classified with an error of 0.0817. Table 10 shows summary of the metrics of using this architecture. From Table 10, it can be shown that the accuracy rate decreased for Grayhole attack and significantly increased for Blackhole attacks.

When the ANN was trained on the dataset with three hidden layers, 97.8% of DoS cases were correctly classified with an error of 0.0791. Table 11 shows summary of results of using holdout method with three hidden layers.

More decrease in the accuracy rate of Grayhole attack can be seen in Table 11.

An ANN was trained on the WSN-DS dataset using 10-Fold Cross Validation method with one hidden layer. In this case, 98.52% of DoS attacks were correctly classified with an error of 0.0636. Table 12 shows the summary results of using this method with one hidden layer.

Table 12 shows an improvement in the results for all types of attacks. We have trained the ANN using 10-Fold Cross Validation with two hidden layers. Having two hidden layers, 98.53% of the DoS cases were classified correctly with an error of 0.0643. Table 13 summarizes the results of using this method.

Using 10-Fold Cross Validation to train an ANN architecture that has three hidden layers on WSN-DS dataset, 97.18% of the cases were correctly classified with an error of 0.0914. Table 14 summarizes the results of using this method.

Figures 3, 4, and 5 summarize the previous results. Figure 3 shows the True positive rate. On average the best

TABLE 8: Confusion matrix of holdout method with one hidden layer.

	Normal	Flooding	Scheduling	Grayhole	Blackhole
Normal	135483	350	32	152	10
Flooding	0	1325	0	0	0
Scheduling	23	0	2620	3	10
Grayhole	29	0	9	5379	421
Blackhole	0	0	3	2640	1377

TABLE 9: Summary results of holdout method with one hidden layer.

	TPR	FPR	FNR	TNR	<i>P</i>
Normal	0.996	0.004	0.004	0.996	1.000
Flooding	1.000	0.002	0	0.998	0.791
Scheduling	0.986	0.000	0.014	1	0.983
Grayhole	0.921	0.003	0.079	0.997	0.658
Blackhole	0.343	0.004	0.657	0.996	0.757
Avg.	0.975	0.021	0.025	0.979	0.978

TABLE 10: Summary results of holdout method with two hidden layers.

	TPR	FPR	FNR	TNR	<i>P</i>
Normal	0.996	0.008	0.004	0.992	0.999
Flooding	1	0.003	0	0.997	0.753
Scheduling	0.984	0	0.016	1	0.991
Grayhole	0.714	0.006	0.286	0.994	0.838
Blackhole	0.818	0.011	0.182	0.989	0.669
Avg.	0.98	0.008	0.02	0.992	0.982

TABLE 11: Summary results of holdout method with three hidden layers.

	TPR	FPR	FNR	TNR	<i>P</i>
Normal	0.995	0.016	0.005	0.984	0.998
Flooding	0.989	0.003	0.011	0.997	0.734
Scheduling	0.973	0.001	0.027	0.999	0.954
Grayhole	0.576	0.001	0.424	0.999	0.965
Blackhole	0.989	0.016	0.011	0.984	0.631
Avg.	0.978	0.015	0.022	0.985	0.984

TABLE 12: Summary results of 10-Fold Cross Validation with one hidden layer.

	TPR	FPR	FNR	TNR	<i>P</i>
Normal	0.998	0.018	0.002	0.982	0.998
Flooding	0.994	0.001	0.006	0.999	0.904
Scheduling	0.922	0	0.078	1	0.995
Grayhole	0.756	0.003	0.244	0.997	0.911
Blackhole	0.928	0.009	0.072	0.991	0.730
Avg.	0.985	0.017	0.015	0.983	0.987

method for classifying the attacks is Cross Validation with one hidden layer (CV1). It was the best in classifying all attacks except for Scheduling and Grayhole attack where it

TABLE 13: Summary results of 10-Fold Cross Validation with two hidden layers.

	TPR	FPR	FNR	TNR	<i>P</i>
Normal	0.998	0.02	0.002	0.98	0.998
Flooding	0.985	0.001	0.015	0.999	0.900
Scheduling	0.915	0	0.085	1	0.992
Grayhole	0.867	0.007	0.133	0.993	0.832
Blackhole	0.778	0.005	0.222	0.995	0.810
Avg.	0.985	0.019	0.015	0.981	0.985

TABLE 14: Summary results of 10-Fold Cross Validation with three hidden layers.

	TPR	FPR	FNR	TNR	<i>P</i>
Normal	0.994	0.045	0.006	0.955	0.995
Flooding	0.754	0.001	0.246	0.999	0.855
Scheduling	0.761	0.001	0.239	0.999	0.946
Grayhole	0.689	0.01	0.311	0.99	0.743
Blackhole	0.843	0.013	0.157	0.987	0.638
Avg.	0.972	0.041	0.028	0.959	0.974

was slightly more accurate to use holdout method with one hidden layer (H1).

Figure 4 shows FPR. In FPR the smaller the rate, the better the performance. On average H1 was the best method; it is slightly better than CV1; however, CV1 was better than H1 in classifying Flooding, Scheduling, and Grayhole attacks. H1 was better in classifying the normal behavior and the Blackhole attack.

Figure 5 shows the error rate of all methods using Root Mean Squared Error (RMSE).

Figure 5 shows that CV1 was the best in terms of RMSE. From the results of TPR, FPR, and RMSE in Figures 3–5, it is concluded that the use of CV1 architecture outperforms other ANN architectures in classifying DoS attacks in WSN.

From the previous results obtained from applying ANN to WSN-DS dataset, high accuracy was achieved in the task of classifying four DoS attacks to determine whether the protocol is in its normal mode or exposed to any type of attack.

7. Conclusions and Future Work

The aim of this paper is to design an intelligent intrusion detection and prevention mechanism that could work efficiently to limit DoS attacks with reasonable cost in terms

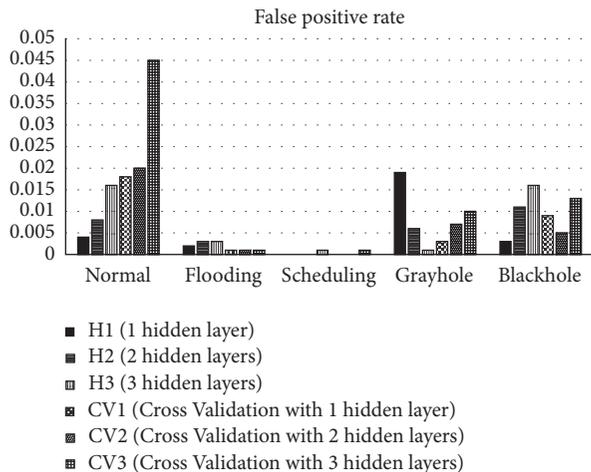


FIGURE 4: False positive results.

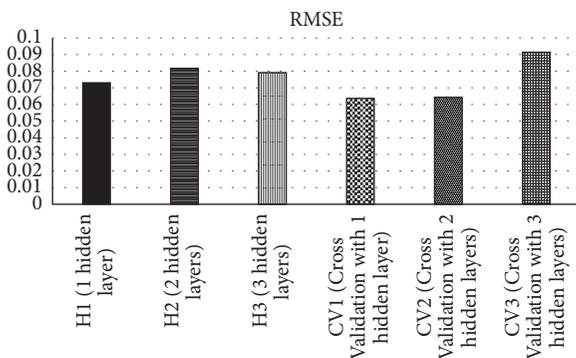


FIGURE 5: Root Mean Squared Error (RMSE) in each method.

of processing and energy. To achieve this aim, a specialized dataset for WSN was constructed to classify four types of DoS attacks. The considered attacks are Blackhole, Grayhole, Flooding, and Scheduling attacks. The data were collected using NS-2. In addition to including normal behavior, it was also able to collect 374661 records containing the signatures of these four attacks. The dataset containing normal and malicious network traffic was used to obtain the experimental results shown. In this paper, mathematical validation of the created dataset has been provided to ensure its correctness. The constructed dataset is called WSN-DS.

ANN-MLP model using WEKA toolbox was built; attacks were classified using two methods, holdout and 10-Fold Cross Validation, with one, two, and three hidden layers used in each case. We have found that, using 10-Fold Cross Validation with one hidden layer, the percentages of classification accuracies of attacks were 92.8%, 99.4%, 92.2%, 75.6%, and 99.8 in Blackhole, Flooding, Scheduling, and Grayhole attacks, in addition to the normal case (without attacks), respectively. From these results, it can be concluded that ANN trained using WSN-DS dataset is very useful in classifying DoS attacks as it was able to achieve high classification accuracy in the presence of more than one attack.

This work, which compares a number of distinct DoS attacking models, provides additional insights. Specifically,

it would draw conclusions in terms of selecting the best protocol to be employed in a precisely predefined real-time application in WSN. This research reemphasizes the importance of considering security early in the network protocol development process. Without this, inherited vulnerabilities in these network protocols and other software will increasingly become targets for malicious attacks.

In future, this work can be extended to include other types of DoS attacks in data link layer such as Wormhole or Sybil. In addition, attacks on protocols other than LEACH and in different layers of WSN can be considered. It is also possible to attempt the use of other classifiers and data mining approaches. The current and future versions of WSN-DS will be posted to the researchers.

Competing Interests

The authors declare that they have no competing interests.

References

- [1] N. Marriwala and P. Rathee, "An approach to increase the wireless sensor network lifetime," in *Proceedings of the World Congress on Information and Communication Technologies (WICT '12)*, pp. 495–499, IEEE, Trivandrum, India, October–November 2012.
- [2] V. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 10, pp. 3557–3564, 2010.
- [3] M. A. Rassam, M. A. Maarof, and A. Zainal, "A survey of intrusion detection schemes in wireless sensor networks," *American Journal of Applied Sciences*, vol. 9, no. 10, pp. 1636–1652, 2012.
- [4] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 266–282, 2014.
- [5] H. Modares, R. Salleh, and A. Moravejsharieh, "Overview of security issues in wireless sensor networks," in *Proceedings of the 2nd International Conference on Computational Intelligence, Modelling and Simulation (CIMSIm '11)*, pp. 308–311, September 2011.
- [6] J. Sen, "Security in wireless sensor networks," in *Wireless Sensor Networks: Current Status and Future Trends*, S. Khan, A.-S. K. Pathan, and N. A. Alrajeh, Eds., CRC Press, New York, NY, USA, 2012.
- [7] N. Farooq, I. Zahoor, S. Mandal, and T. Gulzar, "Systematic analysis of DoS attacks in wireless sensor networks with wormhole injection," *International Journal of Information and Computation Technology*, vol. 4, no. 2, pp. 173–182, 2014.
- [8] A. Mitrokotsa and T. Karygiannis, "Intrusion detection techniques in sensor networks," in *Wireless Sensor Network Security, Cryptology and Information Security Series*, pp. 251–272, IOS Press, 2008.
- [9] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd IEEE Annual Hawaii International Conference on System Sciences*, pp. 1–10, Maui, Hawaii, USA, January 2000.

- [10] H. Liu, L. Li, and S. Jin, "Cluster number variability problem in LEACH," in *Ubiquitous Intelligence and Computing*, pp. 429–437, Springer, Berlin, Germany, 2006.
- [11] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660–670, 2002.
- [12] S. B. Alla, A. Ezzati, and A. Mohsen, "Hierarchical adaptive balanced routing protocol for energy efficiency in heterogeneous wireless sensor networks," in *Energy Efficiency—The Innovative Ways for Smart Energy, the Future Towards Modern Utilities*, InTech, 2012.
- [13] S. Tyagi and N. Kumar, "A systematic review on clustering and routing techniques based upon LEACH protocol for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 36, no. 2, pp. 623–645, 2013.
- [14] A. Braman and G. R. Umaphathi, "A comparative study on advances in LEACH Routing protocol for wireless sensor networks: a survey," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 3, no. 2, pp. 5883–5890, 2014.
- [15] H. Dhawan and S. Waraich, "A comparative study on LEACH routing protocol and its variants in wireless sensor networks: a survey," *International Journal of Computer Applications*, vol. 95, no. 8, pp. 21–27, 2014.
- [16] D. Kumar, "Performance analysis of energy efficient clustering protocols for maximizing lifetime of wireless sensor networks," *IET Wireless Sensor Systems*, vol. 4, no. 1, pp. 9–16, 2014.
- [17] Y. M. Miao, "Cluster-head election algorithm for wireless sensor networks based on LEACH protocol," *Applied Mechanics and Materials*, vol. 738–739, pp. 19–22, 2015.
- [18] S. Taneja, "An energy efficient approach using load distribution through LEACH-TLCH protocol," *Journal of Network Communications and Emerging Technologies (JNCET)*, vol. 5, no. 3, pp. 20–23, 2015.
- [19] S. Peng, T. Wang, and C. P. Low, "Energy neutral clustering for energy harvesting wireless sensors networks," *Ad Hoc Networks*, vol. 28, pp. 1–16, 2015.
- [20] G. Padmavathi and D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *International Journal of Computer Science and Information Security*, vol. 4, no. 1-2, 2009.
- [21] D. Mansouri, L. Mokdad, J. Ben-Othman, and M. Ioualalen, "Detecting DoS attacks in WSN based on clustering technique," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '13)*, pp. 2214–2219, IEEE, Shanghai, China, April 2013.
- [22] A. Garofalo, C. Di Sarno, and V. Formicola, "Enhancing intrusion detection in wireless sensor networks through decision trees," in *Dependable Computing*, pp. 1–15, Springer, Berlin, Germany, 2013.
- [23] S.-S. Wang, K.-Q. Yan, S.-C. Wang, and C.-W. Liu, "An integrated intrusion detection system for cluster-based wireless sensor networks," *Expert Systems with Applications*, vol. 38, no. 12, pp. 15234–15243, 2011.
- [24] D. Wu, G. Hu, and G. Ni, "Research and improve on secure routing protocols in wireless sensor networks," in *Proceedings of the 4th IEEE International Conference on Circuits and Systems for Communications (ICCS '08)*, pp. 853–856, IEEE, Shanghai, China, May 2008.
- [25] G. Wang, J. Hao, J. Mab, and L. Huang, "A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering," *Expert Systems with Applications*, vol. 37, no. 9, pp. 6225–6232, 2010.
- [26] M. Xie, S. Han, B. Tian, and S. Parvin, "Anomaly detection in wireless sensor networks: a survey," *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1302–1325, 2011.
- [27] R. Bace and P. Mell, *NIST Special Publication on Intrusion Detection Systems*, Booz-Allen and Hamilton, McLean, Va, USA, 2001.
- [28] J. Xu, J. Wang, S. Xie, W. Chen, and J.-U. Kim, "Study on intrusion detection policy for wireless sensor networks," *International Journal of Security and Its Applications*, vol. 7, no. 1, pp. 1–6, 2013.
- [29] S. Khan and K.-K. Loo, "Real-time cross-layer design for a large-scale flood detection and attack trace-back mechanism in IEEE 802.11 wireless mesh networks," *Network Security*, vol. 2009, no. 5, pp. 9–16, 2009.
- [30] N. A. Alrajeh, S. Khan, and B. Shams, "Intrusion detection systems in wireless sensor networks: a review," *International Journal of Distributed Sensor Networks*, vol. 9, no. 5, pp. 1–7, 2013.
- [31] A. Abid, A. Kachouri, and A. Mahfoudhi, "Anomaly detection in WSN: critical study with new vision," in *Proceedings of the International Conference on Automation, Control, Engineering and Computer Science (ACECS '14)*, pp. 37–46, 2014.
- [32] H. Jadidoleslamy, "A high-level architecture for intrusion detection on heterogeneous wireless sensor networks: hierarchical, scalable and dynamic reconfigurable," *Wireless Sensor Network*, vol. 3, no. 7, pp. 241–261, 2011.
- [33] KDD, <https://kdd.ics.uci.edu>.
- [34] J. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. K. Chan, "Cost-based modeling and evaluation for data mining with application to fraud and intrusion detection," Results from the JAM Project by Salvatore, 2000.
- [35] A. Ananthakumar, T. Ganediwal, and A. Kunte, "Intrusion detection system in wireless sensor networks: a review," *International Journal of Advanced Computer Science and Applications*, vol. 6, no. 12, pp. 131–139, 2015.
- [36] A. Alsadhan and N. Khan, "A proposed optimized and efficient intrusion detection system for wireless sensor network," *International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering*, vol. 7, no. 12, pp. 1621–1624, 2013.
- [37] Y. El Mourabit, A. Bouirden, A. Toumanari, and N. E. Moussaid, "Intrusion detection techniques in wireless sensor network using data mining algorithms: comparative evaluation based on attacks detection," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 6, no. 9, pp. 164–172, 2015.
- [38] S. Sumitha Pandit and B. Kalpana, "Hybrid technique for detection of denial of service (DOS) attack in wireless sensor network," *International Journal of Advanced Networking and Applications*, vol. 7, no. 2, pp. 2674–2681, 2015.
- [39] S. Athmani, D. E. Boubiche, and A. Bilami, "Hierarchical energy efficient intrusion detection system for black hole attacks in WSNs," in *Proceedings of the World Congress on Computer and Information Technology (WCCIT '13)*, pp. 1–5, IEEE, Sousse, Tunisia, June 2013.
- [40] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293–315, 2003.
- [41] M. Tripathi, M. S. Gaur, and V. Laxmi, "Comparing the impact of black hole and gray hole attack on LEACH in WSN," *Procedia Computer Science*, vol. 19, pp. 1101–1107, 2013.

- [42] A. P. Renold, R. Poongothai, and R. Parthasarathy, "Performance analysis of LEACH with gray hole attack in Wireless Sensor Networks," in *Proceedings of the International Conference on Computer Communication and Informatics (ICCCI '12)*, pp. 1–4, January 2012.
- [43] S. Magotra and K. Kumar, "Detection of HELLO flood attack on LEACH protocol," in *Proceedings of the 4th IEEE International Advance Computing Conference (IACC '14)*, pp. 193–198, IEEE, Gurgaon, India, February 2014.
- [44] I. Almomani and B. Al-Kasasbeh, "Performance analysis of LEACH protocol under Denial of Service attacks," in *Proceedings of the 6th IEEE International Conference on Information and Communication Systems (ICICS '15)*, pp. 292–297, Amman, Jordan, April 2015.
- [45] The Network Simulator—ns-2, <http://www.isi.edu/nsnam/ns/>.
- [46] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. H. Witten, "The WEKA data mining software: an update," *ACM SIGKDD Explorations Newsletter*, vol. 11, no. 1, pp. 10–18, 2009.
- [47] R. R. Bouckaert, E. Frank, M. A. Hall et al., "WEKA—experiences with a Java open-source project," *The Journal of Machine Learning Research*, vol. 11, pp. 2533–2541, 2010.

Research Article

Supporting Business Privacy Protection in Wireless Sensor Networks

Nan Feng,¹ Zhiqi Hao,¹ Siboyang,¹ and Harris Wu²

¹Department of Information Management, Tianjin University, Tianjin 300072, China

²Old Dominion University, Norfolk, VA 23529, USA

Correspondence should be addressed to Siboyang; yangsibo@tju.edu.cn

Received 15 March 2016; Revised 19 May 2016; Accepted 21 June 2016

Academic Editor: Jose M. De Fuentes

Copyright © 2016 Nan Feng et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the pervasive use of wireless sensor networks (WSNs) within commercial environments, business privacy leakage due to the exposure of sensitive information transmitted in a WSN has become a major issue for enterprises. We examine business privacy protection in the application of WSNs. We propose a business privacy-protection system (BPS) that is modeled as a hierarchical profile in order to filter sensitive information with respect to enterprise-specified privacy requirements. The BPS aims at solving a tradeoff between metrics that are defined to estimate the utility of information and the business privacy risk. We design profile, risk assessment, and filtration agents to implement the BPS based on multiagent technology. The effectiveness of our proposed BPS is validated by experiments.

1. Introduction

Wireless sensor networks (WSNs) are highly distributed networks that are enabled with wireless communication technologies and composed of devices with sensing capabilities [1, 2]. The rapid development of WSNs is changing the way people live and work. Extensive research has focused on a broad range of applications of WSNs, including both the military and civilian domains [3, 4]. However, it is the issue of privacy protection that has drawn considerable attention from the research community. This is because of the implementation of WSNs in commercial scenarios involving businesses and individuals.

Privacy protection has been studied in many fields associated with the applications of WSNs. Nevertheless, the following inherent characteristics lead to some challenges for privacy protection in WSNs.

- (i) Uncontrollable environment: sensors are commonly employed in an environment without sufficient security control.
- (ii) Resource constraints: the ability of a sensor node to store, process, and transmit the sensed data is generally limited by its power supply.

- (iii) Topological constraints: due to the limited communication range of sensor nodes, multiple hops are required for transmitting data. Such a transmission scheme may cause an unbalanced network load.

In addition to the above challenges, employers must pay much attention to the threat of business privacy leakage due to the accessibility of WSNs [5, 6]. The attributes of WSNs may lead to the disclosure of sensitive information regarding the enterprise. This is susceptible to being collected and analyzed by an adversary, who can in turn harm the enterprise's business privacy [7]. Thus, when an enterprise employs a WSN for commercial transactions, the disclosure of sensitive or confidential information will be inevitable without effective business privacy protection.

Although business privacy protection is imperative in the applications of WSNs, there has been minimal attention devoted to the threat of business privacy leakage for enterprises. Existing studies focus mainly on how to protect the individual's privacy in the context of WSNs [8–11]. Therefore, in this paper, we propose a business privacy-protection system (BPS) that is designed specifically for enterprises in order to reduce the threat of business privacy leakage in WSNs. The BPS is implemented by three types of agent:

a profile agent, a risk assessment agent, and a filtration agent, all based on multiagent technology. Integrating the current risk level of privacy leakage, the BPS makes a tradeoff between the utility of information transmitted in a WSN and the risk of privacy leakage and finally generates the optimal filtered profile that satisfies the security requirements.

The remaining sections of this paper are organized as follows. We first review the relevant literature. Then, Section 3 presents the components of our proposed BPS in detail. In Section 4, the BPS is validated further by extensive experiments. Finally, we summarize our contributions.

2. Literature Review

Privacy protection in WSNs can be categorized as data-oriented and context-oriented [12]. Data-oriented privacy protection focuses on protecting the privacy of the data sensed by the nodes [13] and the queries posted to the WSN [14]. Context-oriented privacy protection focuses instead on protecting the metadata related to the transmission of data, such as the information of time and location. This paper aims at solving the issues in data-oriented privacy protection.

To understand the challenges of privacy protection in WSNs, it is necessary first to review the privacy issues and privacy-protection approaches as follows.

Privacy concerns related to sensed-data management have been proposed in several different systems [15]. (1) Data-collection system: the privacy-protection methods commonly employed in data-collection systems are random-perturbation techniques [16, 17]. (2) Information-sharing system: such systems commonly use cryptographic secure multiparty computation techniques [18, 19]. (3) Data-publishing system: the system's purpose is to facilitate data-analysis applications. In these systems, algorithms based on k -anonymity [20] and l -diversity [21] are widely used to protect privacy. Privacy issues have also been investigated in privacy-protection schemes. In [22, 23], the researchers emphasized that the sender's location information is the most important data that need to be protected. Some researchers have tried to hide the origin of the message [24]. Mehta et al. [25] first focused on the location privacy of sensor networks in the global environment, the assumption which became the basis for future research. In order to protect the location privacy, some scholars proposed a new approach for network topology discovery that allows the sink to obtain a global view of the topology without revealing its own location [26]. Some scholars addressed the importance of location privacy of both the source and sink and proposed four schemes, respectively, to deliver messages from source to sink, which can protect the end-to-end location privacy against local eavesdropper [27]. In order to resist the attacks targeted at the base station of WSNs, some scholars present HISP-NC (Homogenous Injection for Sink Privacy with Node Compromise Protection), a receiver-location privacy solution that consists of two complementary schemes which protect the location of the base station [10].

In recent years, multiagent technology has been widely applied in the field of privacy protection. A multiagent system (MAS) is a system consisting of several agents. Agents

TABLE 1: Comparison between BPS and other approaches.

	BPS	DCARP	FRW	HISP-NC
Risk level evaluation	Yes	No	No	No
Information filtration	Yes	No	No	No
Location privacy protection	Yes	Yes	Yes	Yes
Resisting traffic analysis	No	Yes	No	Yes
Tool support	Hugin expert	NA	TOSSIM	MATLAB

coordinate among the various members, provide service for one another, and together complete a task. The goal of a MAS is to convert large and complex systems into small, well-communicated, well-coordinated, and easy-to-manage systems [28]. In a MAS, each agent is independent, autonomous, and able to solve a given problem. Simultaneously, it is a coordinated system in which agents solve large complex problems in coordination with one another. As for the privacy protection related to privacy leakage, some researchers have focused on a secure model that shows how to maintain the secrecy in a cloud environment by using a MAS. Yang et al. [29] focused on developing an active defense for emergency-management system engineering using a MAS. Bishop et al. [30] proposed a mobile agent-based approach to automate the process of detecting and monitoring a colored file system for privacy protection. In this paper, we utilize multiagent technology to build our proposed BPS. There are three agents, profile, risk assessment, and filtration agents, that interact with each other for the common goal of privacy protection in a WSN.

In this paper, we examine the business privacy protection in a WSN. We model the sensed information as a hierarchical profile. Furthermore, we utilize multiagent technology to build our proposed BPS. There are three agents, profile, risk assessment, and filtration agents, that interact with each other for the common goal of privacy protection in a WSN. In the filtration agent, a filtration is developed to filter sensitive information from the profile with respect to enterprise-specified privacy requirements. In addition, the effectiveness and the scalability of the filtration are validated by experiments.

Table 1 shows the comparison results between our proposed BPS and other widely used three approaches, namely, DCARP [26], FRW [27], and HISP-NC [10], where NA means information not found in the related references.

The first issue is the capability of risk level evaluation. In WSN, the entire system faces many risks, and we need to assess the risk and determine the risk level that the enterprise is now facing. As a result, it can be determined which appropriate measures need to be taken immediately to reduce the risks. In BPS, based on BN, we can analyze the current risk level of the enterprise. The second issue is about the information filtration. Faced with the risk, enterprise must

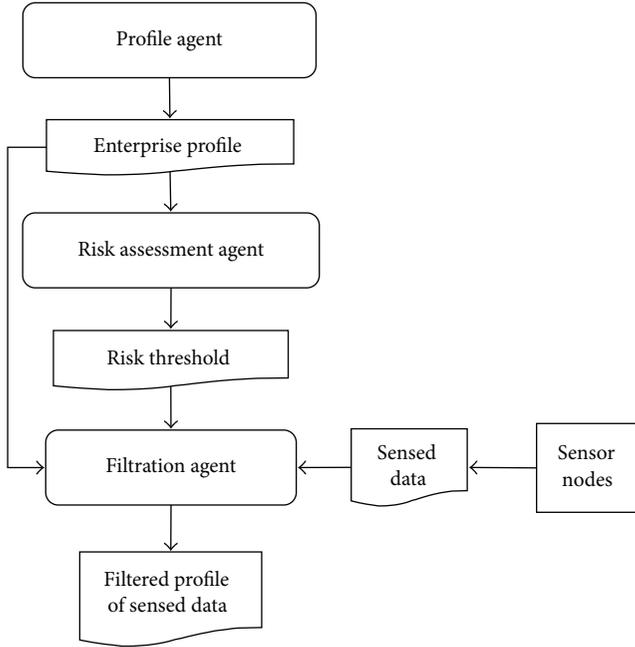


FIGURE 1: BPS architecture.

make adjustment to change the situation. In WSN, a lot of data is related to enterprise's sensitive information, so we have to make filtration before it is published. In the BPS, we have established a filtration agent which seeks a tradeoff between risk and utility to carry out this work. The third issue is the location privacy protection that refers to the sensors' location information in WSN. It is vital because it is related to the source and sink. In BPS, we consider this problem in the enterprise profile as the case in chapter 5 described. The fourth issue is about resisting traffic analysis. Both of DCARP and HISP-NC are good at resisting traffic analysis. We will do some work about it later to enrich our BPS. The fifth issue is about tool support. Hugin expert is used in BPS and TOSSIM is used in FRW, whereas MATLAB is used in HISP-NC. Supporting tools for DCARP have not been found.

3. Business Privacy-Protection System

In this section, we propose a business privacy-protection system (BPS) based on multiagent technology and discuss the characteristics and functions for each of the agents. Figure 1 demonstrates the BPS architecture and shows the agents and their interactions.

A Bayesian network (BN) is a directed acyclic graph (DAG), composed of representatives of the variable nodes and edges connecting these nodes. Nodes represent random variables and directed edges represent the mutual relationship between the nodes (by the parent node to its child nodes). The intensity of the relationship is expressed by the conditional probability between nodes and the no parent nodes express information with a priori probability. A BN can be used to learn causal relationships and hence can be used to gain understanding about a problem domain and to predict

the consequences of intervention. Also, the BN is an ideal representation for combining prior knowledge (which often comes in causal form) and data because it has both causal and probabilistic semantics. Based on these characteristics of BN, it is suitable to predict the risk of privacy leakage.

In the BPS, there are three types of agents to be considered for simulating the process of business privacy risk protection in a WSN. These agents are described as follows:

- (1) The profile agent is responsible for establishing the enterprise profile E . It includes two phases: constructing profile and customizing privacy requirement.
- (2) The risk assessment agent encapsulates a BN that is employed to estimate the risk of privacy leakage. The nodes of the BN are variables that describe the risk environment for privacy leakage. The outcome of this agent is used to determine the risk threshold.
- (3) The filtration agent aims to work out all possible filtered profiles to find the optimal filtration. The process of the filtration is based on two conflicting metrics named utility and risk. The outcome of this agent is a filtered profile that has highest utility and satisfies the business privacy requirement.

3.1. Profile Agent. The formal definition of enterprise profile is presented as follows.

Definition 1 (enterprise profile). The enterprise profile E is a hierarchical representation of the topic domain of an enterprise.

The enterprise profile E satisfies the assumption that, given a topic t related to the enterprise, a corresponding node can be found in E , with the subtree (t, E) as the taxonomy accompanying t . Furthermore, for each topic $t \in E$, a *profile support*, denoted by $\text{sup}_E(t)$, represents the frequency of the topic t mentioned in E . If the topic t can be considered as the result of a random walk from its parent topic $\text{Par}(t, E)$ in E , the profile support can be recursively aggregated as the following equation:

$$\text{sup}_E(t) = \sum_{t' \in C(t, E)} \text{sup}_E(t'), \quad (1)$$

where $C(t, E)$ is the children of t within the tree E .

The procedure of profile agent consists of the following two steps:

- (1) Constructing profile.
- (2) Customizing privacy requirement.

(1) Constructing Profile. The original enterprise profile E is constructed in a form of topic hierarchy as follows:

- (1) Build the enterprise profile as a topic path trie with the topic set T ; that is, $E = \text{trie}(T)$.
- (2) For topic $t \in T$, initialize the profile support $\text{sup}_E(t)$ with (1).

```

Input: Set of all/candidate edges
Output: Bayesian network
//Initialization
(1) define  $m$  as the number of ants;
(2) pheromones  $\tau$ : initialize each entry of  $\tau$  with  $\tau_0$ ;
(3) define  $N_{\max}$  as max number of iterations;
(4)  $N_{\text{iter}} = 0$ ;
(5)  $G^* = \text{empty graph}$ ;
    //Optimization
(6) repeat
(7)   for  $k = 1$  to  $m$  do
(8)     for  $i = 1$  to  $n$  do  $Pa(x_i) = \phi$ ;
(9)     for  $i = 1$  and  $j = 1$  to  $n$  do
(10)      if ( $i \neq j$ ) then  $\eta_{ij} = f(x_i, x_j) - f(x_i, \phi)$ ;
(11)     end
(12)     repeat
(13)      Select two indexes  $i$  and  $j$  by using (5) and (6) and assign edge  $e_{ij}$  to  $G_k$ ;
(14)      if ( $\eta_{ij} > 0$ ) then  $Pa(x_i) = Pa(x_i) \cup \{x_j\}$ ;
(15)       $\eta_{ij} = -\infty$ ;
(16)      for all  $x_a \in \text{Ancestors}(x_j) \cup \{x_j\}$  and  $x_b \in \text{Descendants}(x_i) \cup \{x_i\}$  do
(17)        $\eta_{ab} = -\infty$ ;
(18)       for  $k = 1$  to  $n$  do
(19)        if ( $\eta_{ik} > -\infty$ ) then  $\eta_{ij} = f(x_i, Pa(x_i) \cup \{x_k\}) - f(x_i, Pa(x_i))$ ;
(20)       end
(21)        $\tau_{ij} = (1 - \rho) \cdot \tau_{ij} + \rho \cdot \tau_0$ ;
(22)      until  $\forall i, j$  ( $\eta_{ij} \leq 0$  or  $\eta_{ij} = -\infty$ );
(23)     end
(24)      $G_b = \arg \max_{k=1 \dots m} f(G_k : D)$ ;
(25)     if  $f(G_b : D) \geq f(G^* : D)$  then  $G^* = G_b$ ;
(26)     Update pheromone according to (3) using  $f(G^* : D)$ ;
(27)      $N_{\text{iter}} + +$ ;
(28) until  $N_{\text{iter}} = N_{\max}$ ;
(29) return Bayesian network with structure  $G^*$ 

```

ALGORITHM 1: The ACO-based algorithm for learning the BN structure.

(2) *Customizing Privacy Requirement.* A vulnerable node set $V \in E$ and the sensitivity $\text{sen}(v)$ for each $v \in V$ are specified by the enterprise in this step. A vulnerable node set means that a node set belongs to the enterprise profile and may lead to privacy leakage risk to the enterprise. The *sensitivity* $\text{sen}(v)$ represents the severity of the business privacy leakage for the enterprise due to disclosing v .

3.2. *Risk Assessment Agent.* This part involves risk assessment, and the risk threshold applied in profile filtration can accompany the outcome of the agent.

Ant colony optimization (ACO) algorithm [31] is an algorithm that solves the problem by simulating the embodied intelligent behavior of artificial ants groups in the process of foraging. It is a method used to find the optimal path in graph. ACO was originally used to solve TSP problem. After years of development, it has gradually penetrated other areas.

With the risk assessment agent, a BN is developed to represent the factors related to assessing the risk of business privacy leakage. To indicate the relationships among privacy risk factors, an algorithm (see Algorithm 1) based on ant colony optimization (ACO) is generated to learn the BN structure that best fits the environment of enterprise.

In each iteration, a network structure is built collaboratively by the ants on the basis of a candidate network. Each ant picks an edge at random and then decides the state of that edge based on the pheromones and heuristics in iteration. More specifically, the performances consisting of two steps of each ant are as follows.

- (1) Random selection of the next edge: all edges of the graph are candidates, and the next edge will be evaluated from the set of candidates.
- (2) Assignment of an edge state: this assignment is made based on probability and searches for the balance between the pheromone information and the locally computed heuristic information.

The network is changed by the ant when it finds the assignment with the highest score improvement, but the premise is that the change does not lead to any cycle in the network structure. If no higher scoring network can be found, the pheromone information is updated with the current network G and the best network found so far, G^* , to lead the ants in the next iterations to higher quality networks.

When $N_{\text{iter}} = N_{\max}$, that is, when the current number of iterations is equal to the maximum number of iterations, the

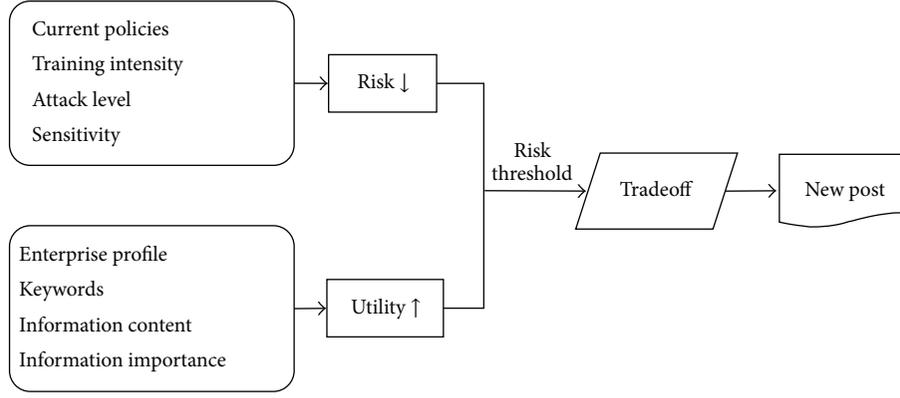


FIGURE 2: The filtration procedure.

process of iteration ends. N_{\max} should be set to a value high enough to allow the pheromone matrix to become saturated.

The equations shown in Algorithm 1 are as follows.

(1) *Heuristic Information*. One has

$$\eta_{ij} = f(x_i, Pa(x_i) \cup \{x_j\}) - f(x_i, Pa(x_i)). \quad (2)$$

(2) *Pheromone Updating Rule*. One has

$$\tau_{ij} \leftarrow (1 - \rho)\tau_{ij} + \rho\Delta\tau_{ij}, \quad (3)$$

where

$$\Delta\tau_{ij} = \begin{cases} \frac{1}{|f(G^* : D)|} & \text{if } x_j \rightarrow x_i \in G^* \\ \tau_{ij} & \text{if } x_j \rightarrow x_i \notin G^*, \end{cases} \quad (4)$$

where τ_{ij} is the level of pheromone in the arc $x_j \rightarrow x_i$, ρ ($0 < \rho \leq 1$) is a parameter controlling the pheromone, and G^* is the best graph found so far.

(3) *Probabilistic Transition Rule*. Select $x_r \rightarrow x_l$ such that

$$r, l = \begin{cases} \arg \max_{i, j \in F_G} \{[\tau_{ij}]^\alpha [\eta_{ij}]^\beta\} & \text{if } q \leq q_0 \\ I, J & \text{if } q > q_0, \end{cases} \quad (5)$$

where I, J are two nodes chosen based on the following equation:

$$p_k(i, j) = \begin{cases} \frac{[\tau_{ij}]^\alpha [\eta_{ij}]^\beta}{\sum_{u, v \in F_G} [\tau_{uv}]^\alpha [\eta_{uv}]^\beta} & \text{if } i, j \in F_G \\ 0 & \text{otherwise.} \end{cases} \quad (6)$$

In this agent, maximum likelihood estimation (MLE) is employed to calculate the parameters (conditional probability tables) of each node in the BN based on the expert's knowledge.

After the construction of the BN of privacy leakage risk, the BN begins to act as a risk assessment tool and provides

TABLE 2: The risk threshold.

Risk level	Risk threshold (β)
Very low	0.9
Low	0.7
Medium	0.5
High	0.2
Very high	0.1

updated information about each observable node in the BN as inference evidence. The BN finally yields the occurrence probability of the risk of privacy leakage.

To update previous estimates, the new evidence should be plugged into the BN by probabilistic inference whenever it is available in the process of the risk assessment. In BN, probabilistic inference is a task that computes all posterior marginals of nonevidence variables based on the given evidence. In this paper, an inference engine based on a junction tree is introduced.

The result of privacy risk assessment is used to determine the risk threshold, which is applied in the filtration agent. The relationship between the risk threshold and the risk level is shown in Table 2.

3.3. Filtration Agent. This agent filters the enterprise profile E in an iterative manner based on the utility and privacy risk metrics. The filtration agent is to work out all possible filtered profiles for sensed data in a WSN to find the optimal filtration. The specific procedure is as in Figure 2.

Based on the risk level estimated by risk assessment agent, the enterprise faces different levels of the privacy leakage risk. The risk may come from following four aspects.

Policy making is the first step of prevention and the enterprise must implement a policy that specifies how to manage the WSN firstly. An effective policy for WSN usage should describe permissible usage, impermissible usage, and behavioral regulations on WSN as well as access rights. In addition, the penalties for violations of the policy, including security violations and system vandalism, should also be covered. Before deploying WSN, enterprises should be required to sign a policy declaration, avowing that they

TABLE 3: Motivation of attacker.

Level	Definition
Weak	Out of curiosity or having no obvious motivation
Intensive	Having a strong desire to attack to benefit from valuable privacy

TABLE 4: Skill of attacker.

Level	Definition
Low	Collecting the public privacy on social networks
Medium	Obtaining objective privacy by text-mining or data analysis
High	Aggregating data and stealing privacy by hacking into the database of social networks

understand that it will be kept on file as a legally binding document.

Training is another proactive measure that can prevent data misuse in the company. Enterprises can effectively convey and update policies to employees by means of training, which is aimed at increasing awareness of the issues, reducing occurrence of possible incidents, and decreasing corporate liability. The components that the training focuses on are topics such as defining accessible and inaccessible data, identifying the warning signs of misuse in the workplace, and identifying risk factors that may contribute to privacy leakage. Furthermore, comprehensive employee training should cover how the company will address incidents of misuse.

The attack events are modeled with an exponential probability distribution. A successful attack on the social network is based on hackers' motivations and skills and on the vulnerability of the social network. As shown in Tables 3 and 4, the motivation range is (Weak, Intensive) and the skill range is (Low, Medium, High), both of which are obtained by expert evaluation based on the information from monitor agent.

What is more, the profile sensitivity is an important factor because different nodes have different privacy concerns. The severity of the business privacy leakage for the enterprise due to disclosure is various. Therefore, the sensitivity has a certain impact on risk. Enterprise should control the profile's sensitivity.

When confronted with the utility of the profile, the enterprise profile should be established firstly. The basic information and data about enterprise are contained. It is constructed as a tree and we can find the node in certain layer. Then we can list the keywords for every profile. The keywords help us find the current node in the tree. Based on the profile, we can also determine the information content and information importance. All these are about the utility of the profile.

Based on the risk assessment agent, we can get a risk threshold about the current situation. It is necessary to control the risk level value lower than the risk threshold. Under the premise of guaranteed risk threshold value, we

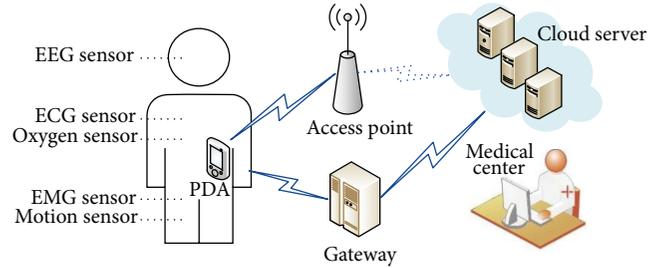


FIGURE 3: System architecture of medical WSN.

establish the tradeoff to mitigate the risk and improve the utility as much as possible. Then some sensitive keywords in the profile are filtrated and the new profile is formed.

4. BPS Validation

Recently, the application scope of wireless sensor networks (WSNs) is wide. Many enterprises take advantage of WSN technology to expand their business [31]. In this section, the proposed BPS is applied to an Internet medical enterprise to control its privacy leakage threat.

By placing sensor nodes in the human body surface or in vivo, patients use the personal smart terminal equipment (such as PDA, smartphones) to build up WSN through self-organizing method. The network structure is shown in Figure 3. The sensors distributed in various parts of the body are used to detect physiological data (such as ECG, EEG, Pulse IPI, and Blood pressure) or peripheral status information. This collected physiological data is sent to the personal handheld devices via short-range wireless communication. Then it will be transmitted to a remote database server through the remote network. Remote medical personnel and care officers analyze the local electronic medical data to detect abnormal physiological condition of the patients and perform remote feedback treatment.

The specific workflow of the application of WSN is described as follows. By placing biological sensor nodes in patient's body, the system can detect physiological data and surrounding circumstances. Then the collected data is transmitted by wireless network to remote databases and services. After the data processing, the patients and doctors will receive the patient's current physical condition information on their personal smart terminal equipment (such as smartphone) through wireless network. Remote doctors analyze the received medical data and contact the patients in abnormal physiological conditions, and then the remote treatment and communication through the intelligent terminal are formed.

The Internet medical enterprise must attach great importance to privacy protection in WSN, because the patients' privacy disclosure will lead to very serious consequences. For example, if a patient's identification information, location information, or physical conditions are intercepted by illegal persons, it is a serious problem. Based on the patient's information, medicine marketing or some spam may be caused. Of course, these will affect people's normal life.

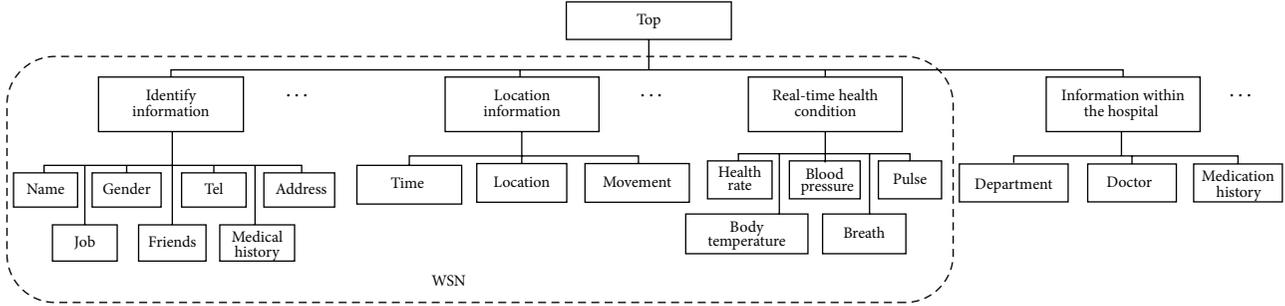


FIGURE 4: Sample of Internet medical enterprise profile.

TABLE 5: Privacy of threat node in BN.

ID	Threat node	State space	Parent nodes	Children nodes
R1	Privacy leakage threat	{High, Medium, Low}	{RF_4, RF_5, RF_6}	\emptyset

TABLE 6: Privacy of threat factor nodes in BN.

ID	Threat factor	State space	Parent nodes	Children nodes
RF_1	Skill of attackers	{High, Medium, Low}	\emptyset	{RF_5}
RF_2	Vulnerabilities of the WSN	{High, Medium, Low}	\emptyset	{RF_5}
RF_3	Motivation of attackers	{Intensive, Weak}	\emptyset	{RF_5}
RF_4	Enterprise security measures	{Effective, Average, Ineffective}	\emptyset	{RF_6, R1}
RF_5	Threat of privacy leakage through WSN	{High, Medium, Low}	{RF_1, RF_2, RF_3}	{R1}
RF_6	Awareness of privacy security	{High, Medium, Low}	{RF_4}	{R1}

A sample of the enterprise profile is illustrated in Figure 4, which is established according to the domain knowledge about the enterprise.

As shown in Figure 4, there is some information about patients in the enterprise, and here we just list a portion of distinct information that sensors in WSN can accept. When patients and doctors interact, they would generate incomplete information. For example, a patient may use vague words to describe his feelings, so that it will produce medium and ambiguous keywords. These keywords may contain sensitive information that patients do not want more people to know. Thus, every node in the tree has its own sensitivity value that represents the loss amount once privacy leakage happens.

4.1. Implementation. Based on the ACO-based algorithm presented in Section 4.2, we develop the BN encapsulated in the risk assessment agent. For the algorithm, different parameter levels are examined, following the research presented in [32]. There are six different ant colony sizes, $m \in \{5, 10, 20, 30, 40, 50\}$; four different evaporation rate levels, $\rho \in \{0, 0.25, 0.5, 0.75\}$; three different pheromone weighting parameters, $\alpha \in \{0, 1, 5\}$; and three different desirability parameters, $\beta \in \{0, 1, 5\}$. The arbitrary positive constant Q is set to 100. The initial pheromone intensity on all arcs τ_0 is fixed at 1. Meanwhile, different numbers of iterations were tested, and we found that the algorithm’s performance no longer improved significantly after 500 iterations. Thus, the maximum number of iterations was set to $N_{\max} = 500$. In sum, our experiments show that $m = 30$, $\alpha = 1$, $\beta = 5$, and

TABLE 7: The risk level.

Risk level	Risk state	Probability range
Very low	Low	≥ 0.7
Low	Low	≥ 0.5
Medium	Medium	≥ 0.5
High	High	≥ 0.5
Very high	High	≥ 0.7

TABLE 8: The probabilities of threat occurrence.

Threat node	State	Probability	Risk level
R1. Privacy leakage threat	High	0.6152	High
	Medium	0.2413	
	Low	0.1435	

$\rho = 0.75$ are the best choices for the parameter values for the algorithm.

The details of the privacy leakage risk node that security threat managers hope to predict ultimately are shown in Table 5, whereas Table 6 presents the information regarding the factor nodes of the risk node R1, that is, the causes that lead to the privacy leakage. Figure 5 shows the BN structure of privacy leakage risk and the conditional probability tables of the nodes are shown in Appendix. Moreover, the IDs of the BN nodes in Tables 9–11 and Figure 5 are explained in Tables 5 and 6.

TABLE 9: CPT of $P(RF_5|RF_1, RF_2, \text{ and } RF_3)$.

RF_1	RF_2	RF_3	RF_5 = high	RF_5 = medium	RF_5 = low
High	High	Intensive	0.9727	0.0273	0
Medium	High	Intensive	0.7933	0.1978	0.0089
Low	High	Intensive	0.7169	0.2653	0.0178
High	Medium	Intensive	0.7896	0.1601	0.0503
Medium	Medium	Intensive	0.7016	0.2198	0.0786
Low	Medium	Intensive	0.5607	0.3401	0.0992
High	Low	Intensive	0.6195	0.2602	0.1203
Medium	Low	Intensive	0.5538	0.3394	0.1068
Low	Low	Intensive	0.4939	0.3489	0.1572
High	High	Weak	0.7149	0.1962	0.0889
Medium	High	Weak	0.5950	0.2547	0.1503
Low	High	Weak	0.5499	0.2789	0.1703
High	Medium	Weak	0.5674	0.3011	0.1315
Medium	Medium	Weak	0.3021	0.4125	0.2854
Low	Medium	Weak	0.2201	0.3601	0.4198
High	Low	Weak	0.4650	0.3004	0.2346
Medium	Low	Weak	0.1929	0.3198	0.4873
Low	Low	Weak	0.0109	0.1688	0.8203

TABLE 10: CPT of $P(RF_6|RF_4)$.

RF_4	RF_6 = high	RF_6 = medium	RF_6 = low
Effective	0.0056	0.1368	0.8576
Average	0.3028	0.5786	0.1186
Ineffective	0.8924	0.1062	0.0014

The relationship between the risk level and the probability of each risk state is shown in Table 7. We offer the updated information about each observable node in the BN as inference evidence. With regard to the privacy leakage risk, the estimated probabilities of risk state and risk level by security threat assessment are shown in Table 8. Since the privacy risk level is high, the risk threshold is set as 0.2 according to Table 2.

4.2. Experiment Results. In this section, the experimental results of BPS are presented. In this experiment, we analyze and compare the results of utility and privacy risk in the iterative process of the filtration.

Figures 6 and 7 demonstrate the results of the utility and risk during the filtration, respectively. In order to show the trend of the results clearly, we link the results on each iteration with dotted line.

In Figure 6, the graph means that, with the number of iterations increasing, the amounts of utility are gradually decreased. We can observe that the utility displays an incremental decrease during filtration. This means that the higher level topics improve the sensed information strength more effectively. Figure 7 shows the results of the metric of risk during the filtration. We observe that the privacy risk first decreases incrementally, but the decline becomes slow as more vulnerable node is pruned from the profile of sensed data.

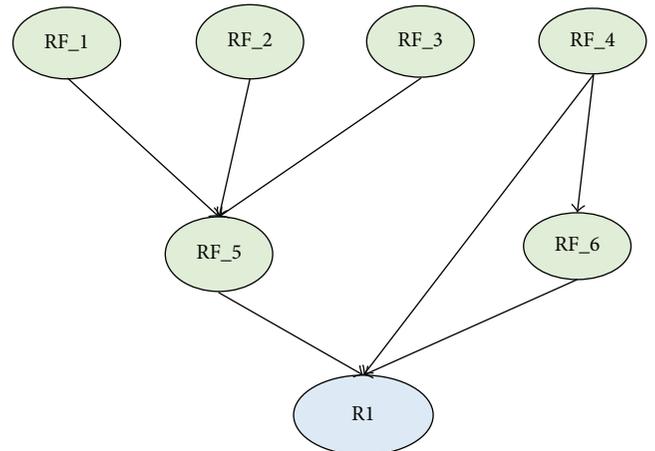


FIGURE 5: BN structure of privacy leakage risk.

Figure 8 illustrates the tradeoff between the utility (i.e., IS) and the privacy risk. For the keywords issued to the WSN, we can find that the utility increases incrementally with slight compromise on risk, while, after a turning point, any small utility will be improved at the cost of a great increase in privacy risk. Therefore, the turning point is a near-optimal solution for the tradeoff.

5. Conclusions

This paper proposes a business privacy-protection system called BPS to mitigate the threat of enterprise's privacy leakage in the application of wireless sensor networks (WSNs). The main contributions are summarized as follows.

- (1) In the BPS, we develop a filtration to filter sensitive information from sensed data transmitted in a WSN

TABLE 11: CPT of $P(R_1|RF_4, RF_5, \text{ and } RF_6)$.

RF_4	RF_5	RF_6	R1 = high	R1 = medium	R1 = low
Effective	High	High	0.4253	0.2732	0.3015
Average	High	High	0.5435	0.2432	0.2142
Ineffective	High	High	0.6012	0.2441	0.1547
Effective	Medium	High	0.3186	0.2816	0.3998
Average	Medium	High	0.3972	0.2984	0.3044
Ineffective	Medium	High	0.5048	0.2699	0.2253
Effective	Low	High	0.0147	0.1002	0.8851
Average	Low	High	0.1738	0.3017	0.5245
Ineffective	Low	High	0.4244	0.2874	0.2882
Effective	High	Medium	0.4987	0.2671	0.2432
Average	High	Medium	0.5548	0.2883	0.1569
Ineffective	High	Medium	0.6943	0.2089	0.0968
Effective	Medium	Medium	0.4007	0.3012	0.2981
Average	Medium	Medium	0.5142	0.2844	0.2014
Ineffective	Medium	Medium	0.7045	0.1808	0.1147
Effective	Low	Medium	0.2918	0.3067	0.4015
Average	Low	Medium	0.4312	0.2555	0.3133
Ineffective	Low	Medium	0.5413	0.2498	0.2089
Effective	High	Low	0.6872	0.1883	0.1245
Average	High	Low	0.8325	0.1186	0.0489
Ineffective	High	Low	0.9701	0.0299	0
Effective	Medium	Low	0.6303	0.1972	0.1725
Average	Medium	Low	0.7152	0.1800	0.1048
Ineffective	Medium	Low	0.8047	0.1628	0.0325
Effective	Low	Low	0.5217	0.2128	0.2655
Average	Low	Low	0.6045	0.2413	0.1542
Ineffective	Low	Low	0.7012	0.2001	0.0987

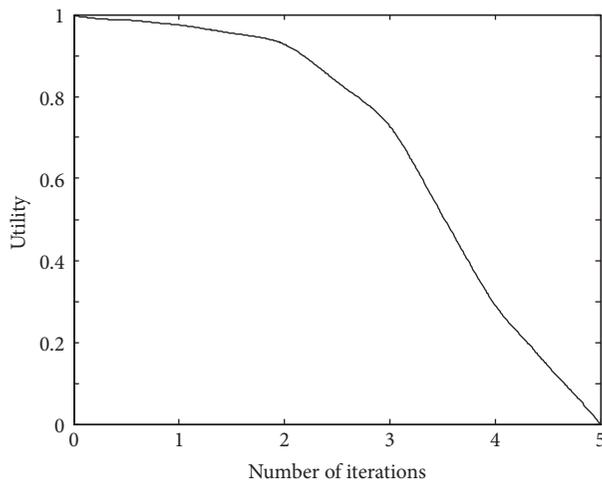


FIGURE 6: Results of utility.

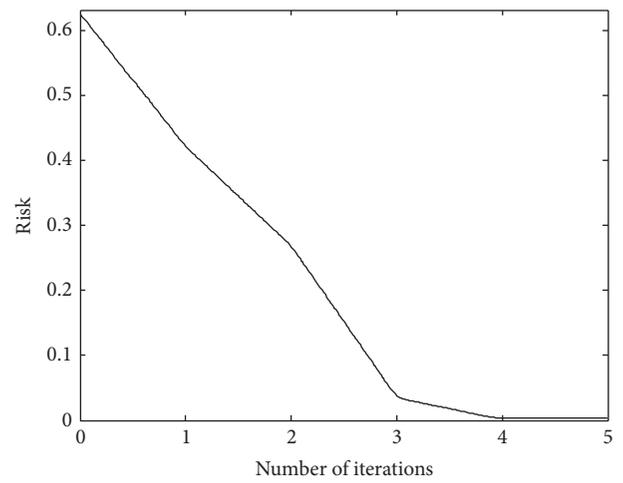


FIGURE 7: Results of privacy risk.

with respect to enterprise-specified privacy requirements.

- (2) We formulate a tradeoff between two conflicting metrics named *utility* and *risk* in the process of profile filtration. The former one is defined as the

information strength of the filtered profile of sensed data, while the latter one represents the risk of the profile exposure.

- (3) We design three agents, profile agent, risk assessment agent, and filtration agent, which are interrelated and

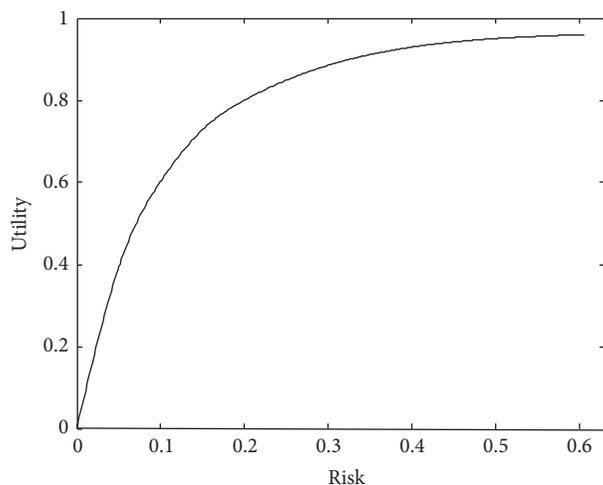


FIGURE 8: Utility versus risk.

interact with each other to implement the BPS based on multiagent technology.

In future work, we will focus on the automatic retrieval of the profile of sensed data based on the enterprise profile. In addition, we also try to improve the current metrics to test the performance of our proposed BPS.

Appendix

The conditional probability tables of the nodes (i.e., RF_5, RF_6, and R1) in Figure 5 are shown in Tables 9–11.

Competing Interests

The authors declare that there are no competing interests.

Acknowledgments

The research was supported by the National Natural Science Foundation of China (no. 71271149) and the Program for New Century Excellent Talents in University.

References

- [1] F. Yu, C.-C. Chang, J. Shu, I. Ahmad, J. Zhang, and J. M. de Fuentes, "Recent advances in security and privacy for wireless sensor networks," *Journal of Sensors*, vol. 2015, Article ID 169305, 2 pages, 2015.
- [2] Q. Yang, X. Zhu, H. Fu, and X. Che, "Survey of security technologies on wireless sensor networks," *Journal of Sensors*, vol. 2015, Article ID 842392, 9 pages, 2015.
- [3] L. Ding, F. Yu, Z. Yang, and G. Yue, "The system design of a node of p2p networks for intrusion detection," *Journal of Networks*, vol. 8, no. 8, pp. 1920–1927, 2013.
- [4] A. Ramos and R. H. Filho, "Sensor data security level estimation scheme for wireless sensor networks," *Sensors*, vol. 15, no. 1, pp. 2104–2136, 2015.
- [5] M. Shariati, F. Bahmani, and F. Shams, "Enterprise information security, a review of architectures and frameworks from interoperability perspective," *Procedia Computer Science*, vol. 3, pp. 537–543, 2011.
- [6] D. He, C. Chen, S. C. Chan, J. Bu, and L. T. Yang, "Security analysis and improvement of a secure and distributed reprogramming protocol for wireless sensor networks," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 11, pp. 5348–5354, 2013.
- [7] H. Huang, T. Gong, P. Chen, G. Qiu, and R. Wang, "Secure two-party distance computation protocols with a semihonest third party and randomization for privacy protection in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID 475150, 15 pages, 2015.
- [8] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Toward a statistical framework for source anonymity in sensor networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 2, pp. 248–260, 2013.
- [9] R. Rios and J. Lopez, "Exploiting context-awareness to enhance source-location privacy in wireless sensor networks," *Computer Journal*, vol. 54, no. 10, pp. 1603–1615, 2011.
- [10] R. Rios, J. Cuellar, and J. Lopez, "Probabilistic receiver-location privacy protection in wireless sensor networks," *Information Sciences*, vol. 321, Article ID 11369, pp. 205–223, 2015.
- [11] J. D. Zhang and C. Y. Chow, "REAL: a reciprocal protocol for location privacy in wireless sensor networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 4, pp. 458–471, 2015.
- [12] L. Zhang, H. Zhang, M. Conti, R. Di Pietro, S. Jajodia, and L. V. Mancini, "Preserving privacy against external and internal threats in WSN data aggregation," *Telecommunication Systems*, vol. 52, no. 4, pp. 2163–2176, 2013.
- [13] R. D. Pietro and A. Viejo, "Location privacy and resilience in wireless sensor networks querying," *Computer Communications*, vol. 34, no. 3, pp. 515–523, 2011.
- [14] K. Islam, W. Shen, and X. Wang, "Wireless sensor network reliability and security in factory automation: a survey," *IEEE Transactions on Systems, Man and Cybernetics C: Applications and Reviews*, vol. 42, no. 6, pp. 1243–1256, 2012.
- [15] N. Zhang and W. Zhao, "Privacy-preserving data mining systems," *Computer*, vol. 40, no. 4, pp. 52–58, 2007.
- [16] N. Zhang, S. Wang, and W. Zhao, "A new scheme on privacy preserving association rule mining," in *Knowledge Discovery in Databases: PKDD 2004: 8th European Conference on Principles and Practice of Knowledge Discovery in Databases, Pisa, Italy, September 20–24, 2004. Proceedings*, vol. 3202 of *Lecture Notes in Computer Science*, pp. 484–495, Springer, Berlin, Germany, 2004.
- [17] N. Zhang, S. Wang, and W. Zhao, "A new scheme on privacy-preserving classification," in *Proceedings of the 11th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '05)*, pp. 374–383, Chicago, Ill, USA, August 2005.
- [18] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 48, no. 4, pp. 393–422, 2012.
- [19] E. De Cristofaro, X. Ding, and G. Tsudik, "Privacy-preserving querying in sensor networks," in *Proceedings of the 18th International Conference on Computer Communications and Networks (ICCCN '09)*, pp. 1–6, San Francisco, Calif, USA, August 2009.

- [20] L. Sweeney, “ k -anonymity: a model for protecting privacy,” *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 5, pp. 557–570, 2002.
- [21] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkatasubramanian, “ L -diversity: privacy beyond k -anonymity,” *ACM Transactions on Knowledge Discovery from Data*, vol. 1, no. 1, article 3, Article ID 1217302, 2007.
- [22] R. Di Pietro, P. Michiardi, and R. Molva, “Confidentiality and integrity for data aggregation in WSN using peer monitoring,” *Security and Communication Networks*, vol. 2, no. 2, pp. 181–194, 2009.
- [23] Y. Xi, L. Schwiebert, and W. Shi, “Preserving source location privacy in monitoring-based wireless sensor networks,” in *Proceedings of the 20th International Parallel and Distributed Processing Symposium (IPDPS '06)*, IEEE, Rhodes Island, Greece, April 2006.
- [24] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, “Enhancing source-location privacy in sensor network routing,” in *Proceedings of 25th IEEE International Conference on Distributed Computing Systems*, pp. 599–608, IEEE Computer Society, Washington, DC, USA, June 2005.
- [25] K. Mehta, D. Liu, and M. Wright, “Location privacy in sensor networks against a global eavesdropper,” in *Proceedings of the 15th IEEE International Conference on Network Protocols (ICNP '07)*, pp. 314–323, Beijing, China, October 2007.
- [26] A. A. Nezhad, A. Miri, and D. Makrakis, “Location privacy and anonymity preserving routing for wireless sensor networks,” *Computer Networks*, vol. 52, no. 18, pp. 3433–3452, 2008.
- [27] H. Chen and W. Lou, “On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks,” *Pervasive and Mobile Computing*, vol. 16, pp. 36–50, 2015.
- [28] A. Das and M. M. Islam, “SecuredTrust: a dynamic trust computation model for secured communication in multiagent systems,” *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 2, pp. 261–274, 2012.
- [29] Q. Yang, H. Ma, and Y. Yu, “Multi-agent risk identifier model of emergency management system engineering based on immunology,” *Systems Engineering Procedia*, vol. 4, pp. 385–392, 2012.
- [30] S. Bishop, H. Okhravi, S. Rahimi, and Y.-C. Lee, “Covert channel resistant information leakage protection using a multi-agent architecture,” *IET Information Security*, vol. 4, no. 4, pp. 233–247, 2010.
- [31] S. Jiang, Y. Cao, S. Iyengar et al., “CareNet: an integrated wireless sensor networking environment for remote healthcare,” in *Proceedings of the 3rd International ICST Conference on Body Area Networks (BODYNETS '08)*, Tempe, Ariz, USA, March 2008.
- [32] T. Liao, K. Socha, M. A. M. De Oca, T. Stutzle, and M. Dorigo, “Ant colony optimization for mixed-variable optimization problems,” *IEEE Transactions on Evolutionary Computation*, vol. 18, no. 4, pp. 503–518, 2014.

Research Article

WDARS: A Weighted Data Aggregation Routing Strategy with Minimum Link Cost in Event-Driven WSNs

**Omar Adil Mahdi,^{1,2} Ainuddin Wahid Abdul Wahab,¹ Mohd Yamani Idna Idris,¹
Ammar Abu Znaid,¹ Yusor Rafid Bahar Al-Mayouf,^{2,3} and Suleman Khan¹**

¹Faculty of Computer Science & Information Technology, University of Malaya, 50603 Lembah Pantai, Kuala Lumpur, Malaysia

²Department of Computer Sciences, College of Education for Pure Sciences-Ibn Al-Haytham, University of Baghdad, Baghdad, Iraq

³Faculty of Engineering and Built Environment, Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, Malaysia

Correspondence should be addressed to Omar Adil Mahdi; omar_1980117@yahoo.com
and Ainuddin Wahid Abdul Wahab; ainuddin@um.edu.my

Received 15 March 2016; Revised 9 May 2016; Accepted 25 May 2016

Academic Editor: Fei Yu

Copyright © 2016 Omar Adil Mahdi et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Realizing the full potential of wireless sensor networks (WSNs) highlights many design issues, particularly the trade-offs concerning multiple conflicting improvements such as maximizing the route overlapping for efficient data aggregation and minimizing the total link cost. While the issues of data aggregation routing protocols and link cost function in a WSNs have been comprehensively considered in the literature, a trade-off improvement between these two has not yet been addressed. In this paper, a comprehensive weight for trade-off between different objectives has been employed, the so-called weighted data aggregation routing strategy (WDARS) which aims to maximize the overlap routes for efficient data aggregation and link cost issues in cluster-based WSNs simultaneously. The proposed methodology is evaluated for energy consumption, network lifetime, throughput, and packet delivery ratio and compared with the InFRA and DRINA. These protocols are cluster-based routing protocols which only aim to maximize the overlap routes for efficient data aggregation. Analysis and simulation results revealed that the WDARS delivered a longer network lifetime with more proficient and reliable performance over other methods.

1. Introduction

Wireless sensor networks (WSNs) are formed by a collaboration of sensors through data sensing, processing, and wireless communication among the sensor nodes. These networks are organized for sensing event-driven information and transmitting it to the base station for in-depth evaluation [1–3]. WSNs have delivered beneficial outcomes in several applications such as environmental monitoring, surveillance missions, health monitoring, home automation, target tracking, traffic monitoring, fire management, agriculture monitoring, industrial failure detection, and energy management [4–8]. WSNs are often deployed in the form of thousands of nodes in remote and hostile areas which are inaccessible or unsafe for humans. Therefore, the formation of autonomous and energy efficient network among the sensor nodes becomes vital to ensure prolonged network lifetime and controlled energy depletion [9–12].

Energy efficiency is directly related to effective data routing wherein cluster of nodes is formed to reduce the energy consumption and control overhead while limiting the interference among the sensor nodes [13]. Generally, the energy is consumed during data sensing, processing, and transmission. Among these activities, data transmission consumes the most energy [14]. Thus, efficient data forwarding and processing techniques must be developed to extend the network lifetime. One possible solution is by using in-network data aggregation schemes (e.g., see [15]). This approach reduces a significant number of bytes transmitted during the network operation by aggregating data at intermediate nodes and thus helps in bandwidth and energy savings. Data aggregation involves combining data from various sources so that aggregated information is received at the base station and circulation of redundant information is eliminated. By employing data aggregation, the issues of

redundancy and numbers of transmissions are reduced. For execution of common tasks, the nodes within the network must communicate with each other or through intermediate nodes [16, 17].

To develop a data aggregation scheme, three main constituents of data aggregation should be considered, which are (1) aggregation function used by the protocol, (2) data aggregation scheduling which defines the waiting period before a node aggregates and forwards the received data, and (3) routing scheme which defines the routing protocol used to send the aggregated data towards the sink by generating a network structure [18]. This paper focuses on the routing scheme of data aggregation which potentially optimizes the routing procedure by utilizing the available processing capability of the intermediate sensor nodes.

The aggregation task in our network is achieved by formation of cluster-based data aggregation in a three-level hierarchy. This reduces the processing and communication cost for randomly distributed nodes. When in-network overlapping of routes occurs inside the cluster, the member nodes of that cluster perform aggregation (aggregation via cluster members). Moreover, aggregated data are sent to sink by the cluster head node (aggregation via cluster head). If overlapping of two or more events paths occurs outside the cluster, the relaying nodes will perform the data aggregation (aggregation via relay nodes).

In the context of WSNs, efficient in-network data aggregation will require an adaptive forwarding paradigm that allows intermediate nodes to forward the data packets towards the sink node through different paths. The paths are estimated based on comprehensive weights and choosing the next hop with the maximum overlap routes to ensure the efficiency of in-network data aggregation. This forwarding paradigm is different from the classic routing which only considers the shortest path between sources and sink nodes.

In event-driven WSNs, the monitoring capability deteriorates when the over-overlapping paths of uncorrelated events perform extensive data aggregation. Hence, the improved network performance is not obtained. Inefficient data aggregation neglects the network state and causes the early energy depletion of the backbone nodes and uneven network structure due to various dead nodes. Therefore, a balance between maximizing data aggregation and energy is necessary.

In this paper, a novel strategy of weighted data aggregation routing is proposed by analyzing the existing problems. The algorithm uses hop-tree to attain maximum data aggregation. To build and update hop-tree, the local state of the nodes is considered so that adaptive behavior can be obtained for event-driven WSNs. Moreover, the proposed strategy finds the ideal point for route overlapping through the shortest paths from events to sink and optimally balanced the energy consumption. Each node chooses its next hop to forward the data in accordance with innovative triple cost functions, which are distributed, adaptive, and comprehensive weights.

The rest of this paper is organized as follows: in Section 2, the related works are discussed. In Section 3, the network model and scenario assumptions are outlined, and the proposed methodology and strategy are presented in

detail. Section 4 discusses the performance of the proposed algorithm by comparing it with other approaches. Finally, in Section 5, conclusions are drawn and possible future directions are described.

2. Related Work

2.1. Flat Network Based Aggregation. In the literature, many earlier approaches employ the flat sensor networks for data aggregation [19, 20]. For instance, many studies have used parent and child association based simpler topology for tree-based data aggregation technique [21]. The data sent by the children are aggregated by the parent node which in turn sends it to its own parent node. The key restrictions of the tree-based data aggregation methodologies are discussed as follows: (1) this technique provides a simpler approach to aggregate data but results in a high latency because the data aggregation is not performed until the packets have arrived at the parent node or grandparent node. (2) High possibility of data is not aggregated near the event of interest because any two nodes that sense the same event might have different parent nodes. This reduces proficiency of data aggregation as the data transmitted over a long path to grandparent node. (3) The tree-based data aggregation schemes require a high number of control messages to build and update the routing tree which consumes more energy. (4) The prior construction of the tree is based on the assumption that the source nodes in the network are fixed and predetermined. Hence, it fails to exhibit the flexible behavior. (5) Its main drawback is when the packet loses due to bad channel links. In this case, the entire aggregated data from the children nodes are lost.

Hierarchical tree structures are costly to maintain and prone to damage due to limited network strength. However, they are still used in designing optimal data aggregation function, energy efficient network, and proficient data aggregation at intermediate nodes. For example, Li et al. developed the data aggregation protocol using Steiner minimum tree [22]. Data centric routing approach employs shortest path tree (SPT) routing protocol [23]. This algorithm is a simple approach to construct the trees in ad hoc fashion and promotes the energy awareness in the parent nodes. When an event is detected by any node, it uses the shortest path to transmit the information towards the sink. This condition is true if the overlapping paths of data aggregation occur (i.e., opportunistic data aggregation).

Issues in tree-based data aggregation due to correlation of sensed information have been considered in [24]. The authors demonstrated the data gathering problem as an NP-complete problem and found the ideal result to be between shortest path tree (SPT) and Traveling Salesman Problem (TSP). A hybrid scheme proposed by Park and Sivakumar [25] combines the shortest path tree and clustering in which the data are aggregated in each minimum dominating set by a head node and all head nodes are linked through a global shortest path tree.

In [26], an energy-aware spanning tree algorithm (Espan) has been proposed for data aggregation exhibiting the feature of energy awareness. This algorithm selects the source node with the highest available energy as the root while other nodes

use the residual energy and distance from the root node as metrics to select their parent node from the neighbors. However, the nodes will tend to select the neighboring nodes with the least distance to the root as parent nodes. This will cause a rapid energy depletion in the parent nodes with the least distance to the root and they will be failed sooner as compared to the other network nodes due to their frequent selection as parent nodes. To achieve a long network lifespan and eliminate the dead nodes in the network, an algorithm based on left over energy in node and distance parameters has been proposed in [27]. The node with the highest energy is selected as the parent node with a reasonable distance to the root. The energy along the path and length is used to maintain a balance between energy and distance parameters.

2.2. Cluster-Based Aggregation. Clustering is a well-established approach in hierarchical data aggregation. This method involves division of network into small sets of nodes called clusters. Within each cluster, the hierarchy is divided into a cluster head node and member nodes [28]. The data from the member nodes are collected by the cluster head. Then, the data are aggregated and forwarded to the upstream node. The clustering algorithms can be either a static or dynamic.

The static clustering is the clusters that are formed prior to network operation [29–31] and based on network parameters (e.g., the remaining energy in the nodes [32] and physical distance as in the Voronoi diagram-based method in [33]). Moreover, the reestablishments or updates of cluster do not occur adaptively. LEACH [34] and HEED [35] are two classic models of static clustering. They differ in the selection method of cluster head as follows; LEACH is formulated on the assumption that energy of all nodes is equal during the election while HEED considers the variation of energy in nodes to optimize the network lifetime.

A dynamic cluster architecture [33, 36, 37] is formed reactively within the proximity of the event sensing nodes. Once the event is located, a specific sensor node is chosen as a cluster head (ideally the node with the maximum energy or adjacent to the event) and the nodes that are one hop away are assigned as the member nodes. The main benefit of this approach is that only the participated nodes are active in the aggregation of the data. Thereby, it conserves the energy of the idle nodes.

Nakamura et al. [38] discussed the reactive algorithm of the Information Fusion Based Role Assignment (InFRA). The roles such as sink, collaborator, coordinator, and relay are assigned when any event takes place. In this protocol, clusters are formed when similar event is detected by various nodes. Then, the coordinator aggregates the data from all collaborated clusters and sends the event data towards the sink in multihop fashion. InFRA discovers the shortest path tree linking all source nodes to sink in a manner that the intra cluster data aggregation is possible. InFRA provides a role migration policy; that is, role of coordinator is transferred from one node to another so that the load of energy consumption is distributed evenly between nodes in the cluster. InFRA used intracluster and intercluster in its data aggregation schemes. A disadvantage of InFRA is that, each time a new

event is detected, the information of the event is broadcasted all over the network to notify other nodes and the paths from the available coordinators to the sink node are updated. These processes are costly and limit the network scalability.

Data Routing for In-Network Aggregation (DRINA) in WSNs [39] provides reliable and improved data aggregation. It reduces the control overhead for building routing trees and maximizes the formation of overlapping paths. The main aim of DRINA is to reduce the energy depletion and minimize the message exchanges during the network operation. However, there are few disadvantages in DRINA as follows. (1) Lacks of load balance, a heavy load in the nodes on the prior built path, will cause those nodes to expire prematurely. (2) Correlated events are ignored due to the assumption that the data from differing event areas could be aggregated adequately. (3) Sometimes the data have to be routed over the lengthier paths, which increase the total energy depletion.

In this work, we proposed a novel algorithm for in-network data aggregation which takes into account the trade-offs between routes overlapping and total link cost for data transmission. Further, the proposed algorithm exploits the local node state to construct and update the hop-tree for efficient data aggregation and efficient control of energy consumption.

3. WDARS: Weighted Data Aggregation Routing Strategy

3.1. The Network Model and Scenario Assumptions. In this study, we consider the features of sensor nodes in the simulated scenario as follows:

- (1) A 2D space has been filled with randomly deployed sensor nodes. The nodes exhibit static and homogeneous behavior in terms of storage, processing abilities, battery power, sensing, and communication capabilities.
- (2) A symmetric radio channel has been considered for modeling so that the energy needed to conduct a data transmission from sensor node S_i to sensor node S_j is equal to the energy used for the same data transmission from sensor node S_j to sensor node S_i .
- (3) The single base station is considered to be at a distant location from the sensor field. It is connected to the power supply while the sensor nodes are non-rechargeable and may die after their energy are exhausted.
- (4) Every node possesses a unique ID and forwards the data at any time during the network operation.
- (5) It is assumed that every node has the capability to calculate its remaining energy and existing buffer size (available memory to store the data before being serviced).
- (6) The network employs a dynamic cluster architecture. A cluster is formed reactively within the proximity of the sensing nodes event and terminated at the end of the event.

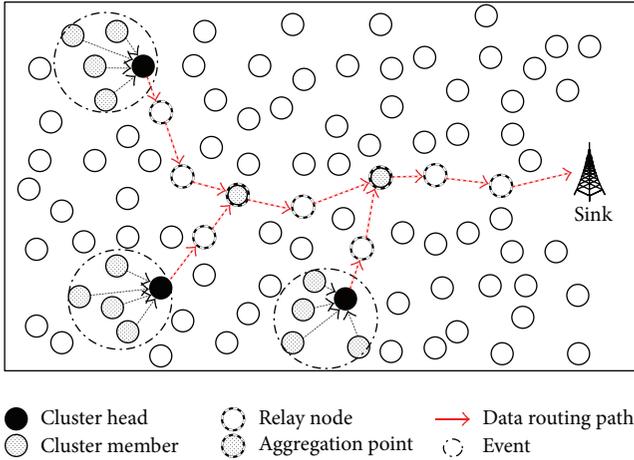


FIGURE 1: Network model diagrams for routing towards the sink node.

3.2. Proposed Model. The event-driven applications are often used in a wide network and enforced dissimilar load to the various parts of the network. This is due to the arbitrarily occurrence of the events. In order to consider such applications, the protocol should be designed to adopt ad hoc features, energy efficiency (i.e., effective management of energy resource for each node), maximum connectivity, a simple controlled processing, and transmissions.

Most existing in-network data aggregation protocols maximize the route overlapping for efficiency of data aggregation. However, such approach may adversely affect the network stability. Therefore, we proposed a protocol to provide a trade-off between the data aggregation cost and the total link cost to solve the excessive route overlapping problem which could cause transfer of the data along longer paths and unbalance of data load on the backbone nodes. The proposed protocol builds a fully distributed cluster and efficient routing tree with the maximum energy conservation and congestion avoidance. It connects all the sensor nodes that detect the event to the sink while maximizing the data aggregation. Also, the proposed protocol optimally balanced the energy depletion paths leading to the sink from the cluster head. Figure 1 depicts the suggested approach and the roles in the routing arrangement are described as follows:

- (i) *Cluster Member (CM)*. This node is responsible for the discovery of an event and forwarding the gathered data to the cluster head.
- (ii) *Cluster Head (CH)*. The responsibility of the cluster head includes the event detection and it performs the data aggregation. Then, the gathered data are transmitted towards the sink.
- (iii) *Relay*. It is a node whose duty is to forward the received data towards its next possible hop. In some cases, relay nodes represent a data aggregation point when the data paths are overlapped on it.
- (iv) *Sink*. It is a collection of nodes or personal computers having high computational energy and processing

TABLE 1: The header of HCM.

Number	Parameter	Description
1	Node-ID	Identification of the node that transmitted/retransmitted the HCM
2	Type	Description of HCM messages
3	HtT	The distance from the node to the hop-tree (in hops)
4	HtS	The distance from the node to the sink (in hops)
5.1	ER	Energy residual of the node
5.2	AB	Available buffer memory size of the node

capability. The sink is liable to receive all the data from the cluster head and other member nodes.

The algorithm proposed in this study consists of three phases. The first phase involves establishment of a hop-tree between sensor nodes and sink. The second phase starts as soon as any event is sensed by a node. In this phase, formation of clusters and selection of cluster head take place. In the third phase establishment of routes, data aggregation, and routing process take place.

3.2.1. Phase I: Hop-Tree Building Process. The input of the initialization phase is a set of nodes which are deployed in the predetermined sensor field. Consequently, each node will identify its neighbors as possible parents within its radio frequency (broadcast) region, hop distance to reach the sink, their residual energy, and available buffer size. The initialization algorithm begins by broadcasting a Hop Configuration Message (HCM) from the sink to all the sensors in the network (Step 1, Algorithm 1). In addition to the common message fields, it contains five key parameters including Node-ID, Type, Hop-to-Tree (HtT), Hop-to-Sink (HtS), and Status (ER, AB) as explained in Table 1.

In addition to Hop-to-Tree, each node has Hop-to-Sink parameter that maintains a minimum number of hops between the node and the sink. At the beginning of the tree formation, the same values are assigned to Hop-to-Tree and Hop-to-Sink. The value of Hop-to-Tree parameter change immediately after the first event is detected. It will continuously change with the occurrence of the new events. Contrarily, the value of Hop-to-Sink remains the same in every node. However, Hop-to-Tree of any node may change due to the occurrence of following two events: (i) the member node is included in the backbone structure, which is the Hop-to-Tree of the sink node, and other nodes belonging to the backbone structure are zero. (ii) a HCM is received by the member node and gives a more accurate information about the distance.

At the beginning of the process, when the hop-tree begins to form, the value of HtT at sink node is stored as zero and infinity for other nodes, the node energy is set to actual value, and the node available buffer memory size is conceded maximum. Once the neighboring nodes of the sink receive the HCM (Step 2, Algorithm 1), a node performs the following tasks: verifies if its HtT value is greater than the

value of HtT in the HCM message (Step 3.1, Algorithm 1); this condition will guarantee that each node records the minimum number of hops to the sink. Depending on the validity of the condition, the node maintains the information of its neighbors whose HCM are received in neighbors table (Step 3.1.1, Algorithm 1). This node also updates the routing table as stated in Steps 3.1.2 and 3.1.3 in Algorithm 1 by exploiting the weights function to compute the link cost of their next hop neighbors and selects the node with the lowest cost as its next hop is depending on (4). This follows incrementing the values of HtT and HtS by one in a sensor node. The sensor node then computes its residual energy after one complete transmission and updates the ER field. Moreover, it computes the obtainable buffer size and updates the AB field and finally circulates the HCM to further neighbors, as shown in Algorithm 1 (Steps 3.1.4–3.1.11).

Otherwise, in Step 3.2, Algorithm 1, the HCM message will be dropped if the condition in Step 3.1, Algorithm 1, is false, which indicates the stored path is the shortest distance to sink.

This procedure is repeated until all the nodes in the network join the tree topology, with the sink node as the root node of the tree.

The weights for packet transmission from node x to node y are defined as follows:

$$W_1 = \left(1 - \frac{E_{\text{res}}(y)}{E_{\text{init}}(y)}\right)^2 + \left(1 - \frac{B_{\text{ava}}(y)}{B_{\text{total}}(y)}\right)^2 \quad (1)$$

$$W_2 = \frac{((\text{HtT}(y) - \text{HtT}(x)) + 1)}{\text{HtT}(y)} \quad (2)$$

$$W_3 = \frac{((\text{HtS}(y) - \text{HtS}(x)) + 1)}{\text{HtS}(y)} \quad (3)$$

$$W_f = \text{alpha} * W_1 + \text{beta} * W_2 + \text{meu} * W_3 \quad (4)$$

$$\text{alpha} + \text{beta} + \text{meu} = 1. \quad (5)$$

The weight (W_1) consists of leftover energy and average buffer size of node. In the first part of (1), when the remaining energy of node y reduces, the result approaches 1. Conversely, when the remaining energy is high, the resulting value approaches zero and the cost reduces. Furthermore, if the node energy does not change (i.e., same as the starting energy), zero cost will be obtained. Likewise, in the second part of the equation, when the buffer is spacious, the cost approaches 0 and when the buffer size has reached its maximum capacity, the cost approaches 1.

Further, W_2 and W_3 are the distance based on number of hops to calculate the next hop neighbor. These weights have the same initial values during the establishment of the tree. In (2), when the node y is one hop closer to already established path, 0 cost is obtained. If the node y is far from the earlier

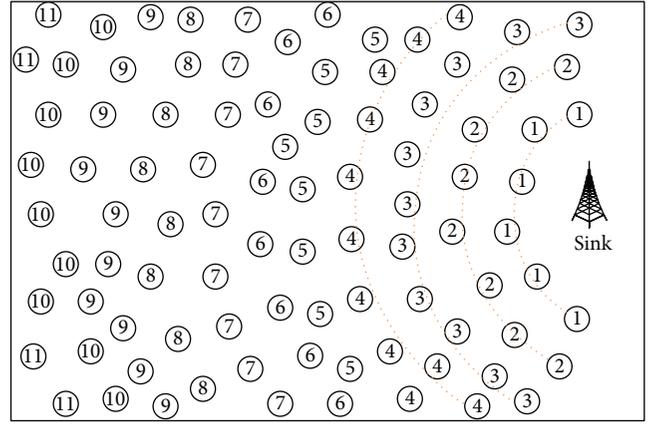


FIGURE 2: The hop-tree building process.

path, the cost is higher than 0, and if the hop distance is the same, the cost is 1. The same principle is applied to (3), but the variables are representing the distance to the sink. The weights are represented by alpha, beta, meu and their summation is equal to unity. The final weight (W_f) is obtained by combining W_1 , W_2 , and W_3 together, which represents the overall cost of the packet transmission from node x to node y .

Figure 2 shows the hop-tree building process, where the labels in the sensors indicate the Hop-to-Tree in increasing order as it moves away from the sink.

Algorithm 1. Hop-tree building process.

Step 1. The sink node broadcasts the initialization message HCM.

Step 2. “ N ” is the set of nodes in a network that receive HCM such that $x \in N$.

// x represents any member node

Step 3. Foreach $x \in N$

Step 3.1. If $\text{HtT}(x) > \text{HtT}(\text{received HCM})(x)$
← true then

Step 3.1.1. Insert Neighbortable (Node-ID, HtT, HtS, ER and BM);

Step 3.1.2. Node x compute the final link cost (W_f) for $NE(x)$;

// $NE(x_i) = \{x_j / d(l_i, l_j) \leq r_c \text{ and } l_j \leq l_i\}$ is the set of neighbor nodes of sensor node x_i , where l_i is the location of x_i and $d(l_i, l_j)$ is the Euclidean distance between x_i and x_j

Step 3.1.3. NextHop(x) ← ID(Bestneighbour);

//Bestneighbour = The neighbour with smallest weight

Step 3.1.4. $\text{HtT}(x) \leftarrow \text{HtT}(\text{HCM}) + 1$;

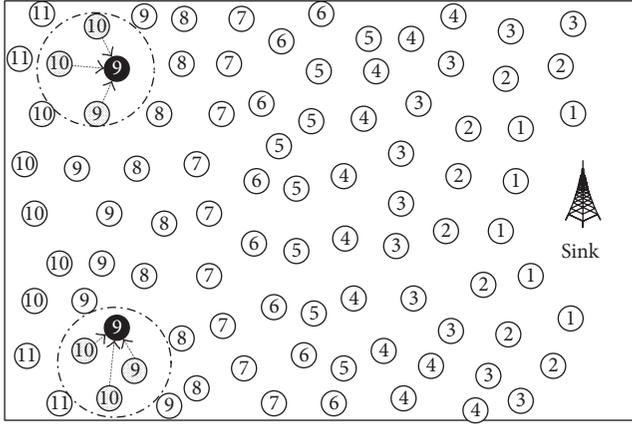
Step 3.1.5. $\text{HtS}(x) \leftarrow \text{HtT}(\text{HCM}) + 1$;

Step 3.1.6. Update the HCM;

Step 3.1.7. ID(HCM) ← ID(x);

Step 3.1.8. $\text{HtT}(\text{HCM}) \leftarrow \text{HtT}(x)$;

Step 3.1.9. $\text{HtS}(\text{HCM}) \leftarrow \text{HtS}(x)$;



- Cluster head
- ⊙ Cluster member
- Event

FIGURE 3: Example of cluster formation.

Step 3.1.10. Status (HCM) \leftarrow Status (x);
 //State contain ER & AB
 Step 3.1.11. Broadcast (HCM);
 Step 3.2. Else Discard HCM message;
 Step 3.3. End.

Step 4. End.

3.2.2. Phase II: Event-Driven Cluster Formation and Cluster Head Election. In phase II, a formation of dynamic cluster architecture takes place. Once the event is located, all the nodes that detect the event will be input to the cluster formation algorithm. At the end, the algorithm will choose a specific sensor node as the cluster head (ideally the one with the minimum weight cost) while nodes within the range of the cluster head will be designated as member nodes. In this process, any node that has detected the event sets its role to cluster head and calculates its weight (W_f) as stated in Steps 1.1 and 1.2 in Algorithm 2. Then, all event nodes propagate their information by Cluster Configuration Message (CCM) (Step 1.3, Algorithm 2), where CCM also constitutes quantities (Node-ID, Type, HtT, HtS, and Status). Cluster head is selected considering the final weight function (4) and minimum weight node will be assigned as the cluster head (Step 3, Algorithm 2). Finally, the decision is broadcasted to the all member nodes. The member nodes then remember their cluster head and all the events detection reports are sent directly to the cluster head. In the case of two or more concurrent nodes having the same weight, the node with the lowest ID is considered eligible, as shown in Step 3.2, Algorithm 2.

Every cluster head is liable to collect information from the member nodes and forward the aggregated data towards sink. Figure 3 shows an example of cluster formation.

Algorithm 2. Event-driven cluster formation and cluster head election.

Input. S // S is the set of nodes that detects the event.

Output. u // A node of the set S is elected as a cluster head.

Step 1. Foreach $x \in S$ do

Step 1.1. Role(x) \leftarrow Cluster head;

Step 1.2. $W_f(x) \leftarrow \alpha * W_1 + \beta * W_2 + \mu * W_3$;

//Each node calculate its weight W_f .

Step 1.3. Node x broadcast (CCM);

//Each node after create CCM broadcast it to its one hop neighbors.

Step 1.4. End.

Step 2. " N " is the set of nodes in a network that received CCM and detects the event.

Step 3. Foreach $u \in N$

Step 3.1. If $W_f(u) > W_f(\text{CCM})$ then

Step 3.1.1. Role(u) \leftarrow Member Node;

Step 3.1.2. Node u retransmits the CCM received from x ;

Step 3.2. ElseIf $W_f(u) == W_f(\text{CCM})$ && ID(u) > ID(CCM) then

Step 3.2.1. Role(u) \leftarrow Member Node;

Step 3.2.2. Node u retransmits the CCM received from x ;

Step 3.3. Else Node u discards the CCM received from x ;

Step 4. End.

3.2.3. Phase III. Route Establishment in Consideration of Nodes Weight. In phase III, a group of cluster heads which were established during phase II is considered as input and the new route to transfer the event data will be the outcome of this process. In this phase, routing tree formation is based on the saved weights in neighbor table which was created during Phase I. Each node will be well aware of all its neighbors, the possible parent nodes within its radio range, number of hops required to approach sink or former routing path, remaining energy of those nodes, and obtainable buffer memory. This implies that each node can use the information in neighbors table to send the data packet to the sink node.

In the first step of this process, the cluster head is now responsible for routing tree formation and routing packets of the new event towards the sink (Step 1, Algorithm 3). The cluster head will check if its HtT is zero and this means it is apart from the backbone of the hop-tree, so creating a fresh route as hop-trees' new backbone is not required (Step 2, Algorithm 3).

In order to acquire even energy dissipation and avoid congestion delay which is caused by data collisions, the WDARS scheme keeps track of the remaining energy level and accessible buffer memory of the nodes in the backbone, which if it gets larger than the set weight limit, the new

routing path formation is initiated, as shown in Step 3, Algorithm 3. During the reformation process, the neighbor node that relatively has less HtT and HtS, higher energy level, and available buffer memory in comparison to other candidates is chosen as the alternative next hope. Also in the reformation of routing path process, the weight-threshold level for (W_1) in every node is slightly increased if no suitable node can be found.

The cluster head starts to create a route establishment message (REM) and sends the REM to its next hop as shown in Step 4, Algorithm 3. If a route establishment message is received by the next hop node, it will retransmit and initiate the process of updating the hop-tree (Steps 5 and 6, Algorithm 3). The repetition of these steps occurs until the sink is approached or a node that took part in a formerly constructed route is discovered. The creation of routes occurs by selecting the best neighbor at every hop.

The updating of hop-tree is required so that all source nodes can be connected via shortest paths, data aggregation can be maximized, and energy dissipation can be balanced as events befall in succession. In the proposed scheme, HtT, HtS, ER, and AB values are updated at each node to fulfill these objectives. Correlation among data is of great concern in data aggregation and hence higher degree of correlation generates better results. Spatial distance between nodes determines the spatial correlation of sensed data by nodes. So, if the two events are closer, the sensed data is highly correlated whereas when the events are far apart the sensed data exhibits lower degree of correlation. Usually, efficient data aggregation could not be performed for events that are far apart. In WDARS, the purpose of using varied weights especially for HtT and HtS in route establishment is to achieve the ideal point for path overlapping for different events. When events are close, the data path will overlap as early as possible at the nearest ideal point for aggregating event's data. In contrast, when the events are far apart the data routes overlapping will occur at the point where the shortest path will be selected to reach the destination and avoid transferring the data over the long tracks.

Algorithm 3. Routing establishment in consideration of nodes weight.

Step 1. The leader node v of new event starts to establish routing tree;

Step 2. If $HtT(v) == 0$ then

Step 2.1. Start send data to its NextHop(v);

//There is no need to routing formation; node v is already on the backbone of the Hop-Tree.

Step 3. If $W_1(\text{NextHop}(v)) > \text{Weight-Threshold}$ then

Step 3.1. Node v find a new NextHop with less weight that satisfy the predefined limits by exploiting the neighbors table.

Step 4. The leader node v sending REM to its next hop.

Step 5. Repeat

Step 5.1. Node x is NextHop(v) that received REM.

Step 5.2. $HtT(x) \leftarrow 0$;

//node x becomes a part from new routing structure

Step 5.3. $\text{Role}(x) \leftarrow \text{Relay}$;

Step 5.4. If $W_1(\text{NextHop}(x)) > \text{Weight-Threshold}$ then

Step 5.4.1. Node x find a new NextHop with less weight that satisfy the predefined limits by exploiting the neighbors table.

Step 5.5. Node x send route establishment message REM to its NextHop(x);

Step 5.6. Node x broadcasts the HCM with value of $HtT = 0$;

Step 6. Until finds the sink node or a node belongs to the routing structure for previous event.

Step 7. End.

Figure 4(a) shows the formation of the new path and the updated hop-tree based on HtT only [39]. Their technique forces the paths from the events that occur far apart to overlap and aggregate the data from two consistent events. This results in a poor data formation, the overload in overlapping paths that causes imbalance of energy consumption in the network, and increase in the number of dead nodes. Moreover, the data transmission over the lengthier path will boost the total energy consumption. In WDARS, the state of route overlapping depends on HtT and HtS as an addition to the node status as shown in Figure 4(b). It can be observed that the route overlapping is linearly related to the distance between the two events and guaranteed the data transmission over the shortest route possible.

4. Simulation Results and Performance Evaluation

4.1. Simulation Environment. The simulation of the proposed model was conducted using MATLAB with IEEE 802.15.4 as the MAC layer protocol. This simulation was based on a wireless sensor network in event-based environment with an area of $500 \text{ m} \times 500 \text{ m}$ in which the nodes are randomly placed. If two sensors are within the range of each other, they are considered neighbors. A circular event space is considered with random position, time, and event duration. The size of the nodes varies from [100, 300] with a step size of 50 nodes while the sensor field, communication range, and event radius remain constant. As the number of nodes increases, the time taken for simulation also increases gradually. All parameters used in this simulation are listed in Table 2.

4.1.1. Description of Adopted Energy Consumption Model. The energy consumption model can be categorized into three energy consumption submodules: communication, computation, and sensing [14]. Among these activities, the communication phase consumes a significant amount of energy

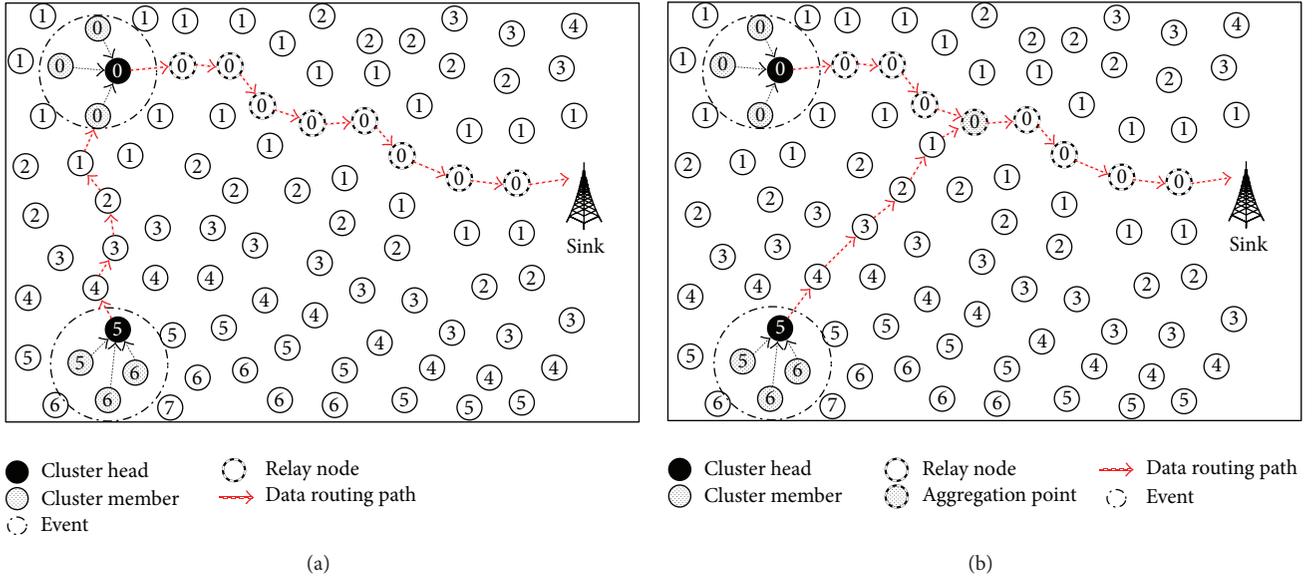


FIGURE 4: (a) and (b) The formation of the new path based on the former hop-tree when another event happens for DRINA and WDARS, respectively.

TABLE 2: Simulation parameter.

Parameter	Value
Channel	Wireless channel
Sink node	Fixed coordinates
Deployment area	500 m × 500 m
Antenna	Omni directional
Initial node energy	2 J
Number of sensor nodes	100, 150, 200, 250, 300
Number of events	3
Event radius	80 m
Communication radius	80 m
Simulation time (sec)	3000
Topology	Dynamic cluster
Bandwidth	10 Mbps
Data packet size	1024 byte
Control packet size	56 byte
Alpha	0.250
Beta	0.375
Meu	0.375

in the sensor nodes depending on the distance between source and destination node. In this simulation, we utilize the radio transceiver model as in [40]. According to the communication energy consumption model in Figure 5, the energy consumed to transmit an ℓ -bit packet over a distance d by the radio can be described in the following equation:

$$E_{Tx}(\ell, d) = \ell * E_{\text{node (Tx)}} + \ell * \epsilon_{\text{op-amp}} * d^n. \quad (6)$$

Furthermore, a sensor node is responsible for forwarding other sensor nodes' data. In this procedure, the data packets are received by the sensor nodes and their energy is not

affected by variation of distance between communication pairs. Therefore, the energy required for receiving an ℓ -bits packet over a distance d is given by the following equation:

$$E_{Rx}(\ell) = \ell * E_{\text{node (Rx)}}. \quad (7)$$

The sensing structure of each sensor node is activated and data is collected from the surroundings by consuming sensing energy denoted by E_s . It is assumed that a constant amount of energy $E_{\text{node (sensing)}}$ is dissipated to sense one bit. Hence, the overall energy dissipation for ℓ -bits is given by the following equation:

$$E_s = E_{\text{node (sensing)}} * \ell. \quad (8)$$

Finally, the sensor network has been structured into distributed clusters. The sensor nodes not only forward the data but also contribute in making key decisions regarding the network operation. Furthermore, the computation of data aggregation consumes extra energy $E_{\text{node (aggregation)}}$ but it is relatively low in comparison to the energy dissipated during communication [14]. For simplicity, we assume the energy dissipated for computation and sensing energy are the same and equal to 50 nJ/bit, while communication (sending/receiving) is assumed to be 100 nJ/bit. The following list defines the meaning of different energy terms in this work and their typical values.

Energy consumption model parameters are presented as follows.

Term and meaning are given:

$E_{\text{node (Tx)}}$: energy consumed in transmitter electronics per bit (taken to be 100 nJ/bit);

$E_{\text{node (Rx)}}$: energy consumed in receiver electronics per bit (taken to be 100 nJ/bit);

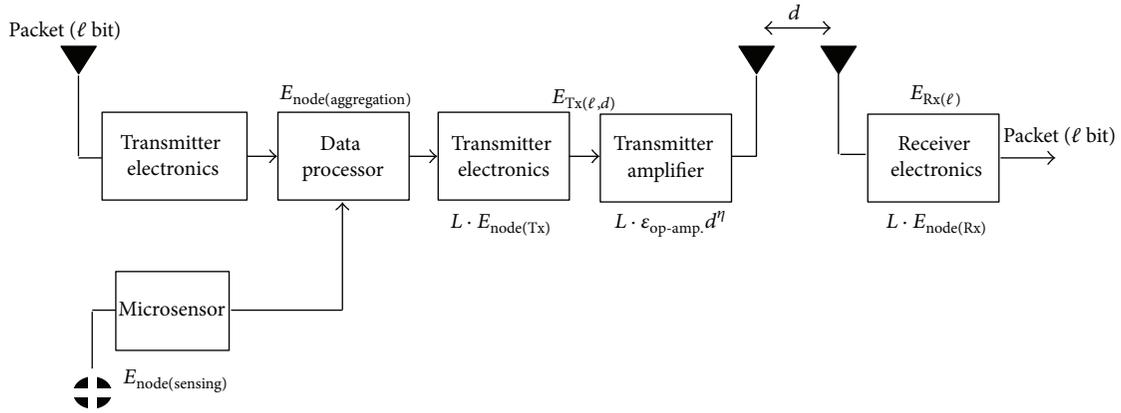


FIGURE 5: Energy consumption model.

$E_{\text{node (sensing)}}$: energy consumed in sensing one bit (taken to be 50 nJ/bit);

$E_{\text{node (aggregation)}}$: energy consumed for aggregating one bit (taken to be 50 nJ/bit/signal);

$\epsilon_{\text{op-amp}}$: energy consumed in the transmitter amplifier for either a free-space channel or a multipath fading channel (taken to be 10 pJ/bit/m² and 0.0013 pJ/bit/m⁴, resp.);

d : distance that the data has to travel;

l : data packet size in bits (taken to be 8192 bit);

η : path loss exponent that ranges between 2 and 6.

4.2. Performance Evaluation. The performance of the proposed WDARS has been evaluated with various network test cases and compared against DRINA and InFRA protocols. Figure 6 illustrates the energy consumption of the nodes for various network densities between WDARS, DRINA, and InFRA protocols. The InFRA recorded the highest energy consumption followed by DRINA and WDARS. This is due to the fact that the InFRA sends more control packets throughout the network during the event detection to inform the nodes and update the routes from existing coordinators to the sink node. This process results in a high communication cost in InFRA. In DRINA, lengthier paths are formed due to unwanted overlapping of distant and uncorrelated events. Therefore, a significant energy is wasted by forwarding the data through the longer paths. On the contrary, the suggested methodology of WDARS consumes less energy by taking into consideration the residual energy of the nodes to stabilize the energy consumption among the nodes. Moreover, the weights of HtT and HtS play an important role in energy saving through the selection of the proper overlapping points. Consequently, a balanced trade-off between the data aggregation and link cost is achieved. The average of the total energy consumption for all tested protocols is depicted in Figure 7. The proposed WDARS recorded the lowest energy consumption with 11.65% compared to the DRINA (21.75%) and the InFRA (35.71%).

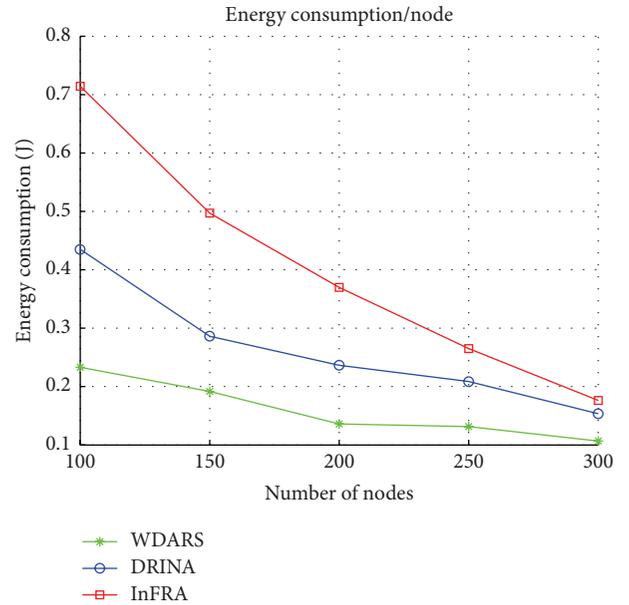


FIGURE 6: Comparison of average energy consumption for different node density.

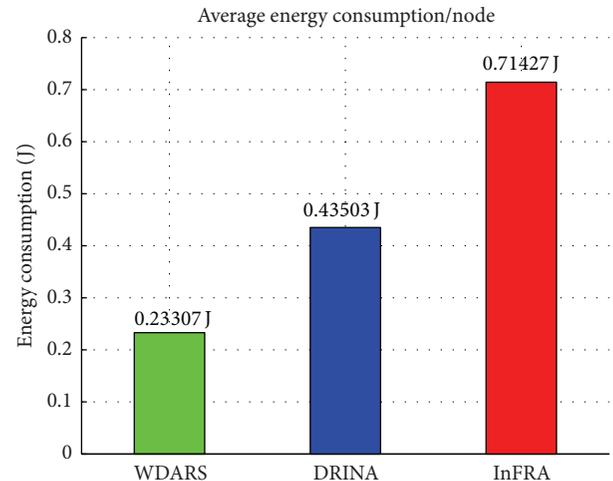


FIGURE 7: Comparison of total energy consumption.

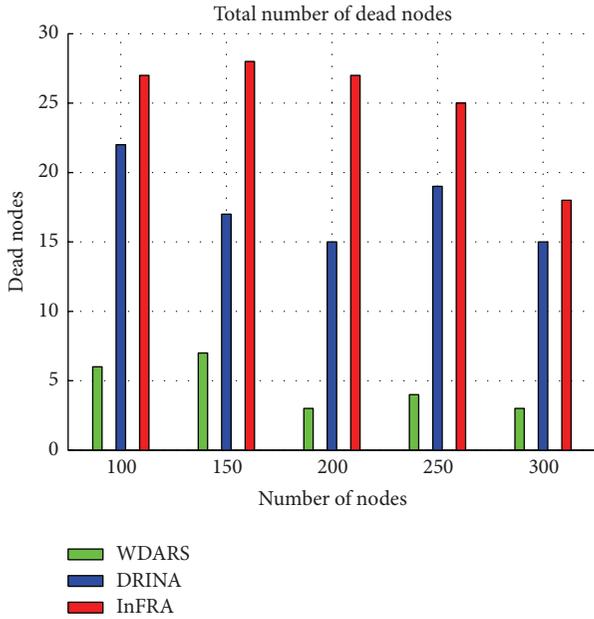


FIGURE 8: Comparison of the dead nodes number.

Next, the rates of dead nodes for each algorithm during the network operation were evaluated and compared as shown in Figure 8. Again, the WDARS had the lowest number of the dead nodes followed by the DRINA and InFRA in ascending order. This can be explained as follows: InFRA ignores the node status in decision to forward the nodes. Only the shortest path tree is considered to link the source and sink node and enable the intracluster data aggregation. Consequently, the nodes which are located at the shortest path are extensively utilized during the data transmission. This causes excessive energy consumption by those nodes and in turn generates a lot of dead nodes in the network. In DRINA, the maximization of the route overlapping is irrespective to the actual status of the network nodes and the spatial correlation between the events. Such approach has placed an immense load on the overlapping area and a very low aggregation ratio. As a result, the energy of the nodes in these areas is rapidly depleted and contributed to the early death of the backbone nodes. Contrarily, WDARS minimized the dead nodes by setting the weights rationally. Furthermore, the scenario of low hop distance and extensive energy depletion were successfully avoided in WDARS. Thus, the energy consumption of the nodes in the network is well balanced.

The network lifetime is highly depending on the routing protocol and influence by two factors: energy consumed over time and the initial node energy. If the initial energy capacity of a node is E and the energy consumed by each node is e_i , then the time up to which the node can work is given as ($t_i = E/e_i$). All such arrays of t_i provide us with the information about network lifetime. As depicted in Figure 9, the network lifetime of all algorithms increased as the node density increased. The lifetime of the WDARS exceeded other algorithms at all node densities. When the node density was minimum, the difference of lifetime between WDARS and DRINA and InFRA was 8.89% and 9.44%, respectively. At

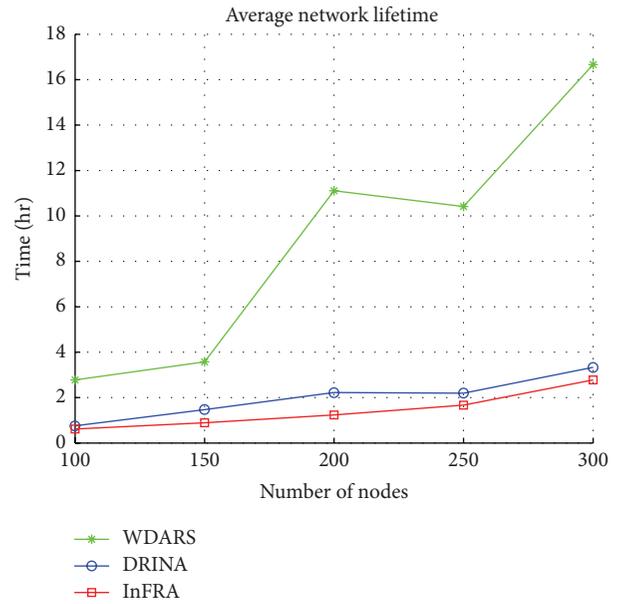


FIGURE 9: Comparison of network lifetime.

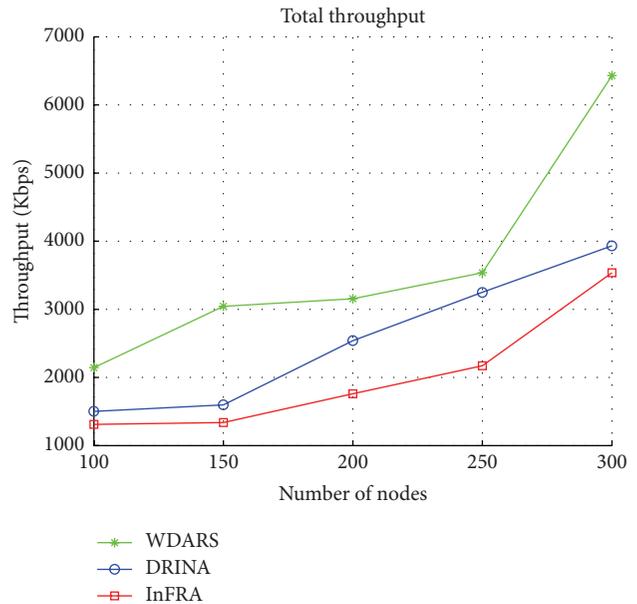


FIGURE 10: Comparison of throughput.

node size of 300, the WDARS scored 91.11% which was higher as compared to DRINA and InFRA with 75.55% and 77.78%, respectively. Moreover, the approach of the energy balance adopted by the WDARS appears to be beneficial with the increase of network density.

Figure 10 shows the throughput of WDARS, DRINA, and InFRA in different network density. It can be observed that the total throughput is increased with the increasing of node density. Overall, the WDARS achieved 8.22% and 13.07% more throughput at the lowest density network and 39.31% and 41.90% at the highest density network as compared with DRINA and InFRA, respectively. Such performance of

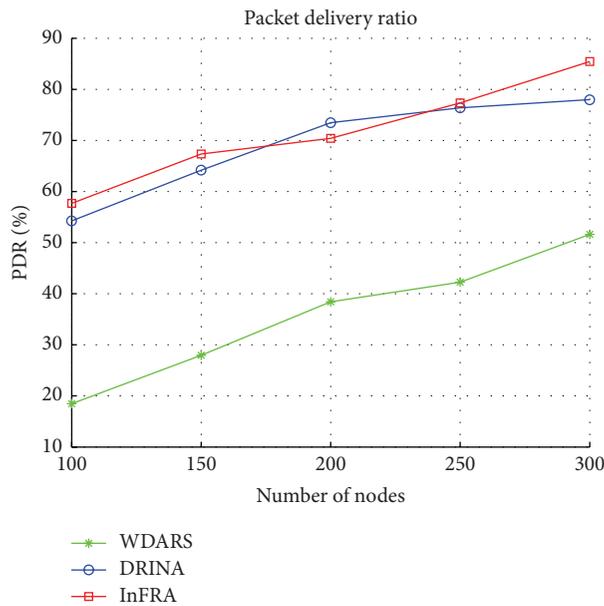


FIGURE 11: Comparison of packet delivery ratio.

WDARS is contributed by its protocol that tracks the level of the available buffer memory in the backbone and effectively avoids the congestion delay caused by data collisions.

Another evaluation metric that quantifies the quality of routing tree built by the algorithms is measured by the packet delivery ratio (PDR). A low PDR implies a greater aggregation rate of the built tree. In Figure 11, the PDR for all algorithms is increased as the network density increased. At the lowest network density, the WDARS has low PDR with 36.10% and 39.80% whereas at highest density it has a 26.50% and 33.10% as compared to DRINA and InFRA, respectively. The WDARS selects the ideal point for routes overlapping which results in fewer relay nodes in the routing tree as compared to DRINA and InFRA for varying network density. The perfect aggregation results were achieved via minimal Steiner tree [23].

5. Conclusion and Future Recommendations

This paper presented a multiobjective clustered-based routing protocol by utilizing the comprehensive weights. The proposed WDARS, successfully maximized the route overlapping via ideal aggregation point while simultaneously ensuring the data transmission across a lightweight route in WSNs. The performance of WDARS was compared with well-known DRINA and InFRA algorithms in terms of scalability, aggregation rate, data delivery rate, energy consumption, and network lifetime. For a set of different test instances, the simulation results showed that WDARS-based clustering protocol outperformed the DRINA and InFRA. Also, our WDARS attained a better performance in the network lifetime by providing a route structure with lower energy consumption for in-network communication. Furthermore, WDARS demonstrated an acceptable level in balancing the energy load among all nodes. This reflects that the proposed algorithm

can provide considering aggregation cost. Also, a trade-off between network load and network lifetime was established while considering residual node energy and obtainable buffer size. Other improvements in route structures exhibiting delay and fault tolerance abilities will be investigated in future work.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research is supported by Research Grant RP036(A,B,C)-15AET and HIR MoE Grant UM.C/625/1/HIR/MoE/FCSIT/17 from the Ministry of Education Malaysia.

References

- [1] K. Matrouk and B. Landfeldt, "RETT-gen: a globally efficient routing protocol for wireless sensor networks by equalising sensor energy and avoiding energy holes," *Ad Hoc Networks*, vol. 7, no. 3, pp. 514–536, 2009.
- [2] M. H. Anisi, G. Abdul-Salaam, M. Y. I. Idris, A. W. A. Wahab, and I. Ahmedy, "Energy harvesting and battery power based routing in wireless sensor networks," *Wireless Networks*, 2015.
- [3] H. Modares, R. Salleh, and A. Moravejsharieh, "Overview of security issues in wireless sensor networks," in *Proceedings of the 3rd International Conference on Computational Intelligence, Modelling and Simulation (CIMSIM '11)*, pp. 308–311, September 2011.
- [4] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, 2002.
- [5] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.
- [6] M. Y. I. Idris, A. M. A. Abu Znaid, A. W. A. Wahab, L. K. Qabajeh, and O. A. Mahdi, "Low communication cost (LCC) scheme for localizing mobile wireless sensor networks," *Wireless Networks*, 2016.
- [7] M. Ahmed, M. R. Sattari, M. K. Nasir et al., "Vehicle adhoc sensor network framework to provide green communication for urban operation rescue," *Lecture Notes on Information Theory*, vol. 1, no. 2, pp. 77–82, 2013.
- [8] S. Khan, A. Gani, A. W. Wahab, M. Shiraz, and I. Ahmad, "Network forensics: review, taxonomy, and open challenges," *Journal of Network and Computer Applications*, vol. 66, pp. 214–235, 2016.
- [9] S. Park, "Performance evaluation of data aggregation schemes in wireless sensor networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '06)*, vol. 1, pp. 413–418, Las Vegas, Nev, USA, April 2006.
- [10] M. H. Anisi, A. H. Abdullah, and S. A. Razak, "Energy-efficient and reliable data delivery in wireless sensor networks," *Wireless Networks*, vol. 19, no. 4, pp. 495–505, 2013.
- [11] S. A. A. Shah, M. Shiraz, M. K. Nasir, and R. B. M. Noor, "Unicast routing protocols for urban vehicular networks: review, taxonomy, and open research issues," *Journal of Zhejiang University: Science C*, vol. 15, no. 7, pp. 489–513, 2014.

- [12] G. Abdul-Salaam, A. H. Abdullah, M. H. Anisi, A. Gani, and A. Alelaiwi, "A comparative analysis of energy conservation approaches in hybrid wireless sensor networks data collection protocols," *Telecommunication Systems*, vol. 61, no. 1, pp. 159–179, 2016.
- [13] S. Halawani and A. W. Khan, "Sensors lifetime enhancement techniques in wireless sensor networks—a survey," *Journal of Computing*, vol. 2, no. 5, pp. 34–47, 2010.
- [14] V. Raghunathan, C. Schurgers, S. Park, and M. B. Srivastava, "Energy-aware wireless microsensor networks," *IEEE Signal Processing Magazine*, vol. 19, no. 2, pp. 40–50, 2002.
- [15] M. Gasser, "In-Network Aggregation Techniques in Wireless Sensor Networks," *Internet Economics VIII*, p. 7, 2014.
- [16] B. Abid, T. T. Nguyen, and H. Seba, "New data aggregation approach for time-constrained wireless sensor networks," *The Journal of Supercomputing*, vol. 71, no. 5, pp. 1678–1693, 2015.
- [17] C. Chen, K. Lee, J.-S. Park, and S. J. Baek, "Minimum cost data aggregation for wireless sensor networks computing functions of sensed data," *Journal of Sensors*, vol. 2015, Article ID 506909, 17 pages, 2015.
- [18] M. Bagaa, Y. Challal, A. Ksentini, A. Derhab, and N. Badache, "Data aggregation scheduling algorithms in wireless sensor networks: solutions and challenges," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1339–1368, 2014.
- [19] L. Chitnis, A. Dobra, and S. Ranka, "Aggregation methods for large-scale sensor networks," *ACM Transactions on Sensor Networks*, vol. 4, no. 2, article 9, 2008.
- [20] R. Rajagopalan and P. K. Varshney, "Data-aggregation techniques in sensor networks: a survey," *IEEE Communications Surveys and Tutorials*, vol. 8, no. 4, pp. 48–63, 2006.
- [21] C. Castelluccia, A. C.-F. Chan, E. Mykletun, and G. Tsudik, "Efficient and provably secure aggregation of encrypted data in wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 5, no. 3, article 20, 2009.
- [22] J. Li, A. Deshpande, and S. Khuller, "On computing compression trees for data collection in wireless sensor networks," in *Proceedings of the IEEE INFOCOM*, pp. 1–9, IEEE, San Diego, Calif, USA, March 2010.
- [23] B. Krishnamachari, D. Estrin, and S. Wicker, "The impact of data aggregation in wireless sensor networks," in *Proceedings of the 22nd IEEE International Conference on Distributed Computing Systems Workshops*, pp. 575–578, Vienna, Austria, 2002.
- [24] R. Cristescu, B. Beferull-Lozano, M. Vetterli, and R. Wattenhofer, "Network correlated data gathering with explicit communication: NP-completeness and algorithms," *IEEE/ACM Transactions on Networking*, vol. 14, no. 1, pp. 41–54, 2006.
- [25] S.-J. Park and R. Sivakumar, "Energy efficient correlated data aggregation for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 4, no. 1, pp. 13–27, 2008.
- [26] M. Lee and V. W. Wong, "An energy-aware spanning tree algorithm for data aggregation in wireless sensor networks," in *Proceedings of the IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM '05)*, IEEE, August 2005.
- [27] Z. Eskandari, M. H. Yaghmaee, and A. Mohajerzadeh, "Energy efficient spanning tree for data aggregation in wireless sensor networks," in *Proceedings of the 17th International Conference on Computer Communications and Networks (ICCCN '08)*, pp. 1–5, IEEE, St. Thomas, Virgin Islands, USA, August 2008.
- [28] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Computer Communications*, vol. 30, no. 14-15, pp. 2826–2841, 2007.
- [29] R. Ghosh and S. Basagni, "Napping backbones: energy efficient topology control for wireless sensor networks," in *Proceedings of the IEEE Radio and Wireless Symposium*, pp. 611–614, January 2006.
- [30] Y. Chen and S. H. Son, "A fault tolerant topology control in wireless sensor networks," in *Proceedings of the 3rd ACS/IEEE International Conference on Computer Systems and Applications*, pp. 269–276, January 2005.
- [31] M. Busse, T. Haenselmann, and W. Effelsberg, "TECA: a topology and energy control algorithm for wireless sensor networks," in *Proceedings of the 9th ACM Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM '06)*, pp. 317–321, October 2006.
- [32] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660–670, 2002.
- [33] W.-P. Chen, J. C. Hou, and L. Sha, "Dynamic clustering for acoustic target tracking in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 3, no. 3, pp. 258–271, 2004.
- [34] W. B. Heinzelman, *Application-Specific Protocol Architectures for Wireless Networks*, Massachusetts Institute of Technology, 2000.
- [35] O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE Transactions on Mobile Computing*, vol. 3, no. 4, pp. 366–379, 2004.
- [36] S. Park, *Performance analysis of data aggregation schemes for wireless sensor networks static-cluster aggregation and dynamic-cluster aggregation section [Ph.D. dissertation]*, North Carolina State University, Raleigh, NC, USA, 2006.
- [37] J.-Y. Cheng, S.-J. Ruan, R.-G. Cheng, and T.-T. Hsu, "PADCP: power-aware dynamic clustering protocol for wireless sensor network," in *Proceedings of the IFIP International Conference on Wireless and Optical Communications Networks*, 6 pages, IEEE, Bangalore, India, April 2006.
- [38] E. Nakamura, H. de Oliveira, L. Pontello, and A. Loureiro, "On demand role assignment for event-detection in sensor networks," in *Proceedings of the 11th IEEE Symposium on Computers and Communications (ISCC '06)*, pp. 941–947, Cagliari, Italy, 2006.
- [39] L. A. Villas, A. Boukerche, H. S. Ramos, H. A. de Oliveira, R. B. de Araujo, and A. A. Loureiro, "DRINA: a lightweight and reliable routing approach for in-network aggregation in wireless sensor networks," *IEEE Transactions on Computers*, vol. 62, no. 4, pp. 676–689, 2013.
- [40] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, IEEE, Maui, Hawaii, USA, January 2000.

Research Article

R-bUCRP: A Novel Reputation-Based Uneven Clustering Routing Protocol for Cognitive Wireless Sensor Networks

Mingchuan Zhang, Ruijuan Zheng, Ying Li, Qingtao Wu, and Liang Song

Information Engineering College, Henan University of Science and Technology, Luoyang 471023, China

Correspondence should be addressed to Mingchuan Zhang; zhang_mch@haust.edu.cn and Ruijuan Zheng; rjwo@163.com

Received 23 March 2016; Revised 17 June 2016; Accepted 28 June 2016

Academic Editor: Iftikhar Ahmad

Copyright © 2016 Mingchuan Zhang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Energy of nodes is an important factor that affects the performance of Wireless Sensor Networks (WSNs), especially in the case of existing selfish nodes, which attracted many researchers' attention recently. In this paper, we present a reputation-based uneven clustering routing protocol (R-bUCRP) considering both energy saving and reputation assessment. In the cluster establishment phase, we adopt an uneven clustering mechanism which controls the competitive scope of cluster head candidates to save the energy of WSNs. In the cluster heads election phase, the residual energy and reputation value are used as the indexes to select the optimal cluster head, where the reputation mechanism is introduced to support reputation assessment. Simulation results show that the proposed R-bUCRP can save node energy consumption, balance network energy distribution, and prolong network lifetime.

1. Introduction

As a new ubiquitous network, Wireless Sensor Networks (WSNs) are widely used in various fields, such as ecological protection, energy conservation and emission reduction, and food security. As a huge network, WSNs have diverse sensor nodes and multifarious communication protocols. The resource management for WSNs is difficult and the application fields are extensive. Meanwhile, the complexity and uncertainty promote the idea that cognition becomes an important characteristic for WSNs.

In 1999, Dr. Mitola and Maguire Jr. [1] proposed the concept of cognitive radio and integrated “cognitive” elements into radio networks, which has attracted a lot of researches and has achieved many research results. The thought of cognition promoted the development of network intelligence greatly. Cognitive radio network [2, 3], cognitive network [4–6], and Cognitive Internet of Things [7, 8] have greatly interested the researchers, and large numbers of achievements have been attained, which greatly promoted the evolution of network intelligence.

In recent years, with the rapid development of the WSNs, the WSNs' intelligent feature has been involved in more and more researches. The concept of the Cognitive Wireless

Sensor Networks (CWSNS) is derived from the autonomic computing [9] and bioinspired theory [10], which puts the “cognitive” element into the WSNs. Since its core idea is to put the intelligent characteristic into IoT, CIoT has the characteristics of self-perception, self-decision, self-learning, self-optimization, and self-adjustment. For network communications, although nodes should cooperate with each other and provide services for others, the existing research shows that a large number of nodes only want to enjoy the services provided by other nodes due to the limited energy of nodes but do not want to provide services for others [11]. Since CWSNS is a large scale network with limited energy and different performance goals in different regional network, there could be many selfish nodes which would cause negative forwarding of packets. Scientific researches prove that forward selfish behavior will affect seriously the network performance—just only a small number of selfish nodes (10%–40%) will lead to a significant decrease (16%–32%) of network performance [12]. Therefore, how to design a reliable routing mechanism is a key problem to be solved in the information transmission field of CWSNS.

Considering the characteristics of scalability and energy saving in networks, the clustering method is always applied to the heterogeneous Wireless Sensor Network protocols,

especially in the large scale network. The clustering method provides a hierarchical structure for the network, which has two members, the cluster head nodes and the cluster member nodes. The cluster head nodes have better basic conditions and manage their cluster member. They fuse the information that cluster member nodes collected and then send it to the base station. In the early stage, the route clustering often used even clustering method. The typical even clustering protocols include LEACH [13], TEEN [14], and APTEEN [15]. Subsequently, Bhasker [16] proposes a genetically derived secure cluster-based data aggregation in WSN which minimizes the energy consumption, ensures data security, and reduces the transmission overhead. Lin and Uster [17] consider a mixed-integer linear programming (MILP) model to optimally determine the sink and CH locations as well as the data flow in the network, which could prolong the network lifetime. Quang and Kim [18] propose a clustering algorithm to enhance the performance of fixed wireless sensor and actuators networks (WSANs). In each cluster, a multilevel hierarchical structure can be applied to reduce the energy consumption. In addition to the cluster head, some nodes can be selected as intermediate nodes, which manages a subcluster. Li and Hua [19] propose a clustering algorithm for energy-efficiency in Wireless Sensor Networks, which is partially similar to this paper. The requirements of even clustering method are even size of clusters in networks and the same number of nodes in the cluster. Polling method used in cluster head election could balance the energy consumption. However, data collection, data fusion, and communication with the base station are usually completed alone by the cluster head node, which will cause premature death, energy consumption imbalance, and short network lifetime.

In order to solve the problem, many researchers have focused in their works on the uneven clustering method to balance the energy consumption. EECS [20] not only considers the distance between cluster member nodes and cluster head nodes, but also considers the distance of the cluster head nodes to the base station and constructs uneven size of clusters to ease the problem of the uneven energy consumption. UCS [21] balanced the energy consumption of the cluster head nodes and adjusted the size of the cluster according to the expected forwarding load of the cluster head nodes. EEUC [22] made use of the uneven size of competitive radius. The number of the cluster members near the base station is relatively small, so that the cluster head nodes could save energy for the cluster data forwarding. It optimizes the energy consumption of nodes and prolongs the network lifetime significantly. CEB-UC [23] showed the reasonable partition of the network area. The closer to the base station clusters are, the less sensor nodes in each cluster are, so that the energy consumption of nodes in the network is balanced. Jiang et al. [24] achieved the uneven clustering by uneven layering of the sensor network model. Each layer forms the cluster independently to balance the energy consumption of cluster head nodes and prolong the network lifetime. Buchegger and Le Boudec [25] used cluster head competitive algorithm based time rules. The broadcast time depends on the residual energy of the cluster head candidate nodes and

their neighbor nodes. The energy consumption of the nodes could be compensated by each other.

The above researches use energy and distance to elect cluster heads and clustering. However, the reliability of the cluster head nodes is also very important. The reputation value of the nodes is often used to measure the reliability of the nodes. The higher the reputation value of the cluster head nodes is, the more reliable the nodes are and the higher the quality of service provided by the nodes in the cluster is. Naghizadeh and Liu [26] describe the reputation problem in a distributed multiuser system by using a mechanism design theoretic approach. They introduce a number of utility models representing users' strategic behavior and design a mechanism that achieves the optimal performance. Due to the node collusion impairing the effectiveness of reputation systems in trustworthy node selection, Li et al. [27] identify suspicious collusion behavior by examining the overstock transaction trace of reputation ratings and propose the Social Trust mechanism that leverages a social network to combat collusion. Refaei et al. [28] introduce a time-slotted approach to allow the evaluation function to quickly and accurately capture changes in node behavior and show the ability to achieve high accuracy and promptness in dynamic environments. Labraoui et al. [29] propose a Risk-aware Reputation-based Trust (RaRTrust) model for WSNs, using both reputation and risk to evaluate trustworthiness of a sensor node. Capossele et al. [30] propose a reputation-based channel aware routing protocol (R-CARP) for underwater acoustic sensor networks (UASNs). It was tailored to such communication constrained environment. The confident protocol proposed in [31] is a kind of ad hoc nodes reputation evaluation mechanism. Through the monitoring of the neighbor nodes, the reputation value is calculated and compared with the presetting threshold to judge the reliability of the nodes. Heinzelman et al. [13] used the watchdog mechanism to monitor the next hop node's forwarding behavior. If the next node would not transmit the data packet, it is indicated that the node's reliability is low. Moreover, the reputation values recommended by other nodes are taken into account for collaborative computing node's reputation value.

We presented a next hop selecting algorithm for static sensor nodes in [32], a "*Physarum* and ants" based hybrid routing algorithm for WSNs [33], and a reputation revision algorithm in cloud circumstance [34]. In this paper, we propose a reputation-based uneven cluster routing protocol (R-bUCRP) based on the prior works. The proposed protocol introduces the reputation mechanism firstly; next calculates the value of the node's direct reputation and relative reputation according to the node's historical interaction information and the similarity of the collected data; then evaluates comprehensively the reputation in consideration of the node's income and expenses value when it joins into the cluster; and finally details the cluster heads election method according to the weight value of the cluster head candidate node's residual energy and reputation value. The proposed method could efficiently decrease the dead speed of the nodes, balance the energy consumption of all nodes, and prolong the network lifetime.

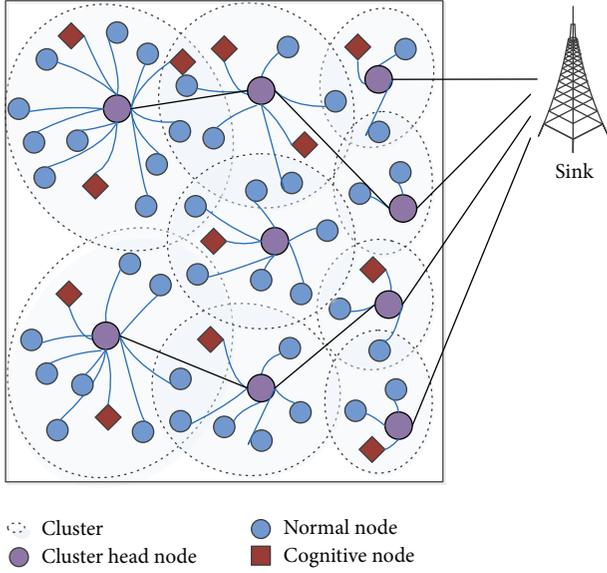


FIGURE 1: Network model.

The rest of the paper is organized as follows. Section 2 introduces network clustering model, energy model, and the reputation model. Section 3 details the proposed R-bUCRP. Section 4 evaluates our models and algorithms with extensive simulations. Finally, the conclusion is presented in Section 5.

2. System Models

2.1. CWSNS Model. In this paper, we construct a network model for CWSNS, as shown in Figure 1. The CWSNS is divided into multiple clusters based on the cluster model of Wireless Sensor Network. We use the uneven clustering method in this paper. The closer to the base station a cluster is, the smaller its radius is. Nodes in the network are divided into cluster head nodes and cluster member nodes. The cluster head is elected according to the cluster head competitive rules, such as more residual energy and less energy consumption. The cluster head node manages cluster member nodes, fuses the information collected by cluster members, and sends it to the base station. The cluster member nodes include cognitive nodes and normal nodes. Cognitive nodes are special normal nodes where “cognitive” element is introduced. Cognitive nodes have the characteristics of wisdom, perceive the change of environment, and make the corresponding decision.

Here, we present some assumptions for the network model used in the proposed method as follows.

- (i) Each node has a unique ID.
- (ii) The energy of the node is heterogeneous, is limited, and cannot be supplied, and the node could obtain its own current energy.
- (iii) The base station cannot be moved, which has infinite energy and strong capacity of computing and storage.
- (iv) The data fusion technology is used to reduce the amount of data transmission.

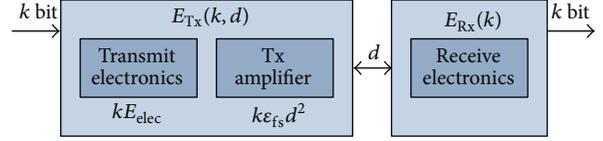


FIGURE 2: Circuit model of sending and receiving data.

- (v) The node is not provided with Global Positioning System (GPS) function module, so it has no position sensing capability.

2.2. Energy Consumption Model. In this paper, the energy consumption model of wireless communication is adopted from [22], where both the free space and multipath fading channels are used depending on the distance between the transmitter and receiver node. If the communication distance is less than a threshold value d_0 , the free space model is used. Otherwise, the multipath fading model is considered. The receiving and sending circuit models of the wireless sensor nodes are shown in Figure 2.

As shown in Figure 2, the energy consumption for transmitting data is mainly composed of two parts, that is, transmitting circuit and power amplifier circuit. The energy consumed by node i to transmit k bit data packet to node j with the distance d is given in

$$E_{Tx}(k, d) = \begin{cases} kE_{elec} + k\epsilon_{fs}d^2, & d < d_0 \\ kE_{elec} + k\epsilon_{mp}d^4, & d \geq d_0. \end{cases} \quad (1)$$

The energy consumption for receiving data comes mainly from receiving circuit, so the energy consumed by node to receive k bit data packet is shown in

$$E_{Rx}(k) = kE_{elec}, \quad (2)$$

where E_{elec} is the radio frequency energy consumption coefficient and ϵ_{fs} and ϵ_{mp} are energy required by amplifier in free space and multipath, respectively. Through (1), d_0 is given as $d_0 = \sqrt{\epsilon_{fs}/\epsilon_{mp}}$.

2.3. Reputation Model. Reputation mechanism provides an effective way to judge the trust relationship between nodes. The introduction of reputation can help determine the degree of cooperation between the nodes, identify the selfish nodes efficiently, and punish or incent the selfish nodes in some way. The so-called selfish nodes are the nodes which do not forward data or forward selectively data in order to maintain their own energy. Assuming that the node i is the neighbor node of node j , if i wants to know whether j is reliable or not, it could determine by computing the reputation value of j .

The traditional node reputation calculation mainly considers two aspects: direct reputation value and indirect reputation value. The reputation evaluation process is shown in Figure 3. Direct reputation means that the reputation value of j is evaluated based on the direct historical interaction between nodes i and j , while indirect reputation value of j is

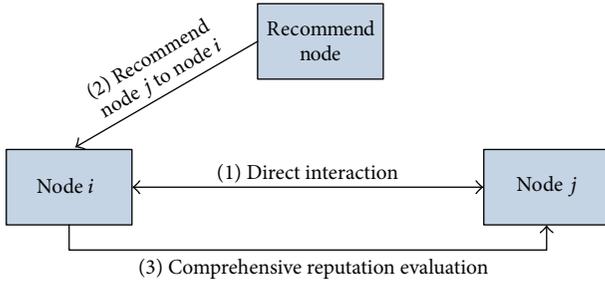


FIGURE 3: Reputation evaluation process.

formed from the recommended value according to the other nodes' reputation to j .

3. R-bUCRP Description

In the network establishment phase, the base station needs to broadcast a signal with a given transmit power. Each sensor node calculates the approximate distance to the base station based on the intensity of the received signal. The distance is not only helpful for the nodes to select the appropriate transmit power to save energy consumption, but also as one of the necessary pieces of information to construct clusters.

The basic process of the R-bUCRP in each round is illuminated as follows. Firstly, each node in the cluster selects a random number between 0 and 1. If the number is below a certain threshold, the node becomes the cluster head candidate. Then, the final cluster heads are determined by using the competitive algorithm, and new cluster heads broadcast the messages to the surrounding nodes. Each node determines which cluster to join in based on the competitive function and replies to the messages to the cluster head.

In the data transmission phase, all nodes in the cluster send data to the cluster head in accordance with TDMA (Time Division Multiple Access) slots. Cluster head fuses the data and then transmits to the base station. After a period of continuous operation, the network reenters the start-ups phase and begins the next round of the cluster heads selection and reestablishes the clusters.

3.1. Reputation Evaluation. Due to the limited energy, some nodes are selfish in order to save their own energy. So it is important to consider the reputation paradigm for network nodes. The lower the reputation value is, the more selfish the nodes are. Therefore, the node's reputation value is one of the factors that need to be considered in the selection of cluster head.

Node reputation value could be computed by similarity of collected data and the historical interaction experience between nodes. Moreover, when the nodes compete to become the cluster head, they can charge a certain reputation value from other nodes as the compensation of energy consumption.

3.1.1. Calculation of Direct Reputation Value. Direct reputation is obtained by listening to the direct interaction of two

nodes. It uses the historical interaction experience between nodes. The more successful interactions of node i to node j are, the higher reliability of node i to node j is. In a period of time, if the number of interactions from node i to node j is N and the number of successful interactions is k , the reputation by direct interaction of node i to node j could be expressed as

$$\varphi_{ij} = \begin{cases} 0.5 + \frac{k - (N - k)}{2N_0}, & N < N_0 \\ \frac{k}{N}, & N \geq N_0, \end{cases} \quad (3)$$

where N_0 is the threshold of interaction frequency.

Generally, interaction time is very important to the reliability of the evaluation and reputation value. Therefore, the interaction time of node i and node j is divided into R segments. For the collected information in paragraph r of node i , the time attenuation factor ρ_r and the importance factor V_r are introduced to calculate the direct reputation value. Direct reputation value of node i could be expressed as

$$\text{DRV}_i = \frac{\sum_{j=1}^M \sum_{r=1}^R \varphi_{ij} \cdot \rho_r \cdot V_r}{R}, \quad (4)$$

where M is the number of neighbor nodes of node i .

3.1.2. Calculation of Relative Reputation Value. In CWSNS, since the distribution of nodes is relatively dense, the observational data by the neighboring nodes often has a lot of similarities. Comparing the data of the neighbor nodes in the same period, we can see that the higher degree of similarity is, the more reliable it is.

Assume that the feature vector of environmental data collected by node i in a period of time is expressed as $D_i = (t, e, a, v)$, where t represents the type of object (the value range is set as T), e represents the event type (the value range is set as E), a represents the attribute of the observation area (the value range is set as A), and v represents the value of perceptual information (the value range is set as V).

The relative reputation between nodes is calculated by the similarity of data feature vectors. There are two adjacent nodes i and j . Their data feature vectors are $\text{DF}_i = (t_i, e_i, a_i, v_i)$ and $\text{DF}_j = (t_j, e_j, a_j, v_j)$. The similarity of data feature vectors of node i and node j in a period of time is

$$\text{Sim}(\text{DF}_i, \text{DF}_j) = \cos(\overrightarrow{\text{DF}_i}, \overrightarrow{\text{DF}_j}) = \frac{\overrightarrow{\text{DF}_i} \cdot \overrightarrow{\text{DF}_j}}{|\overrightarrow{\text{DF}_i}| |\overrightarrow{\text{DF}_j}|}. \quad (5)$$

The relative reputation value of i in this period of time is

$$\text{RRV}_i = \frac{\sum_{j=1}^M \lambda (1 + \text{Sim}(\text{DF}_i, \text{DF}_j))}{M}, \quad (6)$$

where M is the number of nodes adjacent to node i and $\lambda > 0$ is similar parameters to calculate relative reputation value.

3.1.3. Calculation of Reputation Value. The reputation value of node i is composed of direct reputation value (DRV), relative reputation value (RRV), and income and expenses value (IEV). It is expressed as

$$RV_i = \omega_1 DRV_i + \omega_2 RRV_i + \omega_3 IEV_i, \quad (7)$$

where $\omega_1 + \omega_2 + \omega_3 = 1$. If the node i is a cluster head node, when member nodes want to join into the cluster, they need to pay some virtual reputation value to the cluster head node, where $IEV_i \geq 0$; on the contrary, if node i is a normal node and requests to join into the cluster, $IEV_i < 0$.

3.2. Establishment of Cluster

3.2.1. Competitive Radius of Cluster Head. The energy consumption of cluster head is different in even clustering multihop routing. The cluster head nodes near the base station take on more data forwarding tasks and consume more energy. In order to balance the energy consumption of cluster head nodes and prolong the network life, R-bUCRP uses uneven clustering in the stage of cluster establishment. The closer to the base station a cluster is, the smaller its size is. The communication radius of the cluster head node is related to the distance to the base station. Competitive radius of cluster head node is defined as

$$R_i = \left(1 - \mu \frac{d_{\max} - d(s_i, BS)}{d_{\max} - d_{\min}} \right) R_{\max}, \quad (8)$$

where R_i represents the competitive radius of cluster head node i , R_{\max} represents the maximum competitive radius of system setting, and μ is a constant whose value is $[0, 1]$.

3.2.2. Competitive Function of Cluster Head. In the cluster head selection process, this paper constructs a competitive function to avoid the excessive energy consumption or the selfish nodes elected as the cluster head. The competitive function is shown in

$$W_i = \alpha \frac{E_{\text{res}}}{E_{\text{res}}} + \beta \frac{RV}{\overline{RV}}, \quad (9)$$

where W_i is the comprehensive weight value of energy and reputation and the larger the value is, the more competitive to be cluster head the node is, E_{res} represents the current residual energy of node i , $\overline{E_{\text{res}}}$ represents the average residual energy of nodes in the network area, RV represents the current reputation value of node i , and \overline{RV} represents the average reputation value of nodes in the network area.

3.2.3. Competitive Function of Joining into the Cluster. After the cluster heads are determined, the cluster head nodes broadcast the *Cluster_Msg* packet and then wait for other nodes to join in. In this paper, when a node selects a cluster to join in, we consider not only the residual energy of cluster head, but also the distance to the cluster head and distance

between cluster head and base station. The competitive function of node i is given as

$$F(i, CH_i) = \frac{E_{\text{res}}}{d(i, CH_i)^2 + d(CH_i, BS)^2}, \quad (10)$$

where CH_i is the cluster head node, E_{res} is the residual energy of the cluster head node, $d(i, CH_i)$ is the distance between the nodes i and the cluster head node CH_i , and $d(CH_i, BS)$ is the distance between the cluster head CH_i and the base station.

The cluster establishment process is to achieve the purpose of load balancing. When a node wants to join into a cluster, it considers the energy residual of cluster head and transmission distance. From (10), it can be seen that there are three factors to determine the probability of joining into the cluster, that is, energy residual of cluster head, the distance between the cluster head and the normal node, and distance between the cluster head and the base station. In order to avoid the extreme situations of difficult choice (a node encounters a long distance with large energy or a short distance with low energy), especially in the later period of the network lifetime, the algorithm could give priority to the cluster head with the large signal strength when the energy of cluster head candidate is less than a certain threshold.

3.2.4. Establishment Process of Cluster. Network node cluster establishment process includes the cluster head election process and the process of normal nodes joining into the cluster. The corresponding pseudocode is described as in Algorithm 1.

4. Simulation and Result Analysis

4.1. Simulation Environment. In order to evaluate the performance of the proposed algorithms, we use MATLAB to simulate LEACH, EEUC, MADSEC, and our R-bUCRP under the same conditions and compare their performances. Simulation scene is set as follows: 1500 nodes are distributed in the network area of $400 \text{ m} \times 400 \text{ m}$, the coordinates of the base station are $(200, 500) \text{ m}$, and each node moves towards a random direction at a speed uniformly distributed $[0, 20 \text{ m/s}]$. We use energy model of literature [22] in the simulation. Detailed parameter settings are shown in Table 1.

4.2. Result Analysis. Since R-bUCRP introduces the concept of the reputation into the clustering process of CWSNS, reducing energy consumption of normal nodes when they communicate with the selfish nodes, at the same time, it balances the energy consumption of nodes in the network by using uneven clustering method. Therefore, it can be seen from Figure 4 that the first node death time and network death time of R-bUCRP are significantly later than those of the LEACH protocol, EEUC protocol, and MADSEC protocol.

Figure 5 compares the changes of network residual energy by using four protocols over time. Smaller slope shows a slower rate of energy consumption and indicates a longer survival time. As can be seen from Figure 5, the energy

```

For every node in the network
(1)  $t \leftarrow \text{RAND}(0, 1)$ 
(2) if  $t < T$ 
(3)    $\text{beCluserHeadCandidate} \leftarrow \text{TRUE}$ 
(4) end if
(5) if  $\text{beCluserHeadCandidate} = \text{TRUE}$ 
(6)   compute  $R_i$  and  $W_i$  following (8) and (9)
(7)    $\text{CompetitiveHeadMsg}(ID, R_i, W_i)$ 
(8) else
(9)   sleep
(10) end if
For every candidate node  $i$ 
(11) receiving a  $\text{CompetitiveHeadMsg}$  from candidate  $j$ 
(12) if  $d(i, j) < R_i$  OR  $d(i, j) < R_j$ 
(13)   add  $j$  to  $i$  neighbor set  $NS_i$ 
(14) end if
For every candidate node  $j$ 
(15) if  $W_j < W(NS_i)$ 
(16)    $j$  give up the competition and become a normal node
(17) end if
For every normal node  $i$ 
(18) if  $i$  is in one cluster_coverage
(19)    $i$  apply to join into the cluster
(19)    $i$  pay reputation value to the cluster head
(20) else
(21)    $i$  select cluster following (10)
(22)    $i$  pay reputation value to the cluster head
(23) end if

```

ALGORITHM 1: Cluster establishment.

TABLE 1: Network parameters and values.

Parameter	Value
Network coverage	(0,0)~(400, 400) m
Base station location	(200, 500) m
Node number	1500
Initial energy	0.5 J
Data packet size	4000 bits
Speed distribution	[0, 20] m
E_{elec}	50 nJ/bit
ϵ_{fs}	10 pJ/(bit·m ²)
ϵ_{mp}	0.0013 pJ/(bit·m ²)
E_{fusion}	5 nJ/bit

consumption rate by using R-bUCRP is significantly smaller than the other three kinds of protocols, and the network has a longer survival time, with the better network quality.

Figure 6 shows the changes of node average energy by using four kinds of protocols over time. The node average energy by using R-bUCRP is higher than the other three kinds of protocols, which means R-bUCRP has a better performance in energy balance.

Figure 7 compares the changes of node average energy by using four kinds of protocols over the number of nodes in round 1000. With the increase of the node number in the network area, the node average energy is decreased.

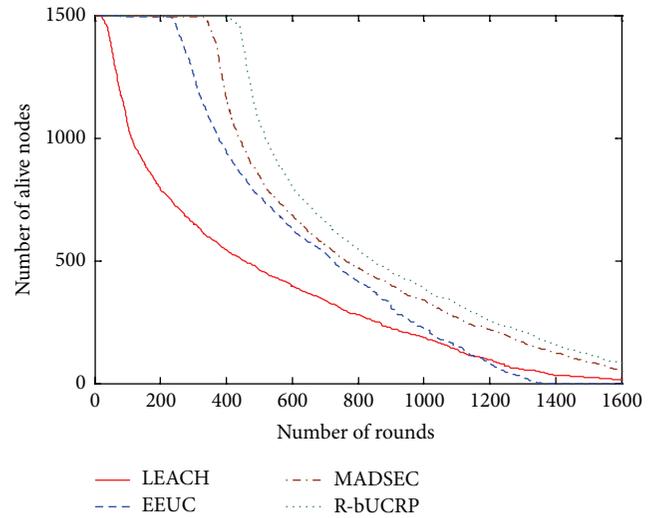


FIGURE 4: The relationship between the alive node number and round number.

As shown from Figure 7, the speed of energy consumption by using R-bUCRP is slower than the other three kinds of protocols, which means R-bUCRP has a better performance in scalability.

Figures 8, 9, 10, and 11 illustrate the stability of the algorithm. A stable clustering algorithm should also generate

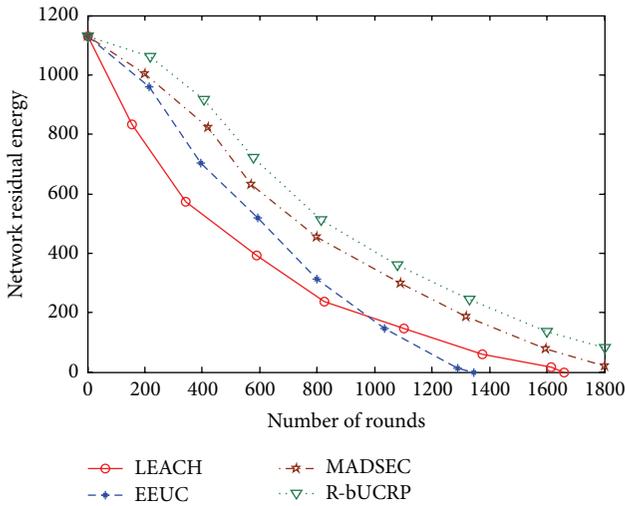


FIGURE 5: The relationship between network residual energy and round number.

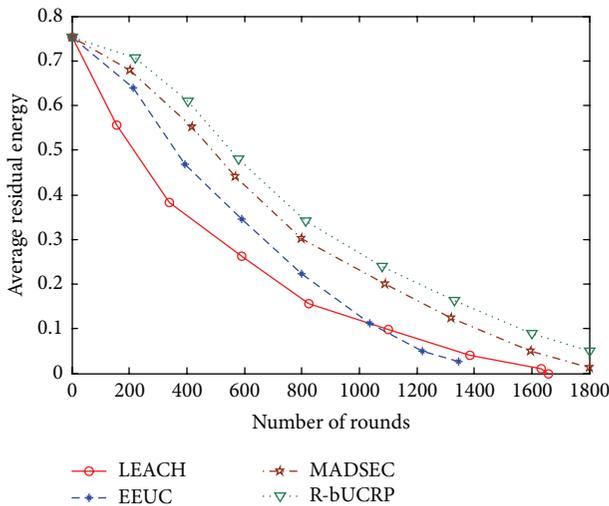


FIGURE 6: The relationship between average residual energy and round number.

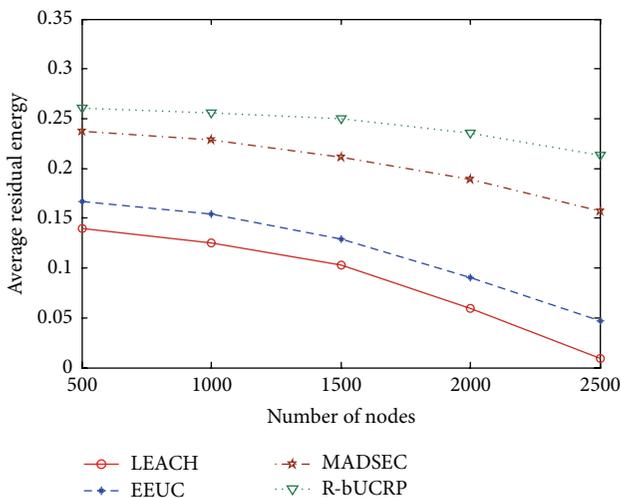


FIGURE 7: The relationship between average residual energy and node number.

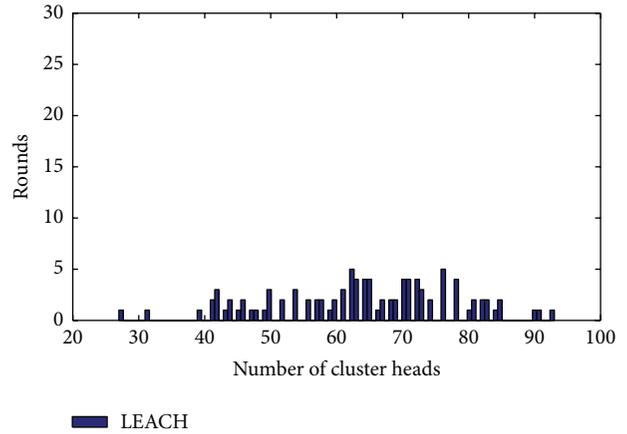


FIGURE 8: Cluster head number distribution of LEACH.

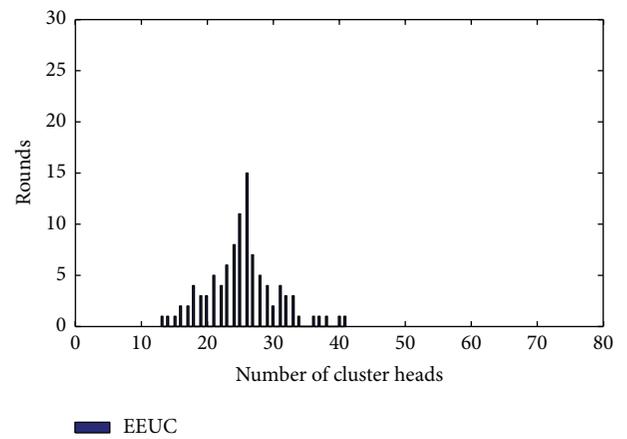


FIGURE 9: Cluster head number distribution of EEUC.

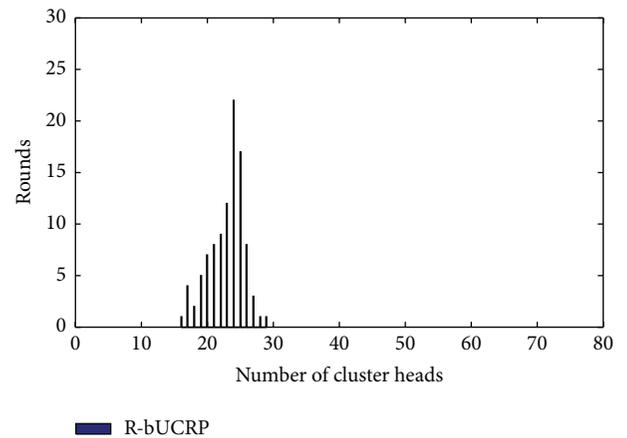


FIGURE 10: Cluster head number distribution of R-bUCRP.

more consistent number of clusters in order to balance the energy consumption of the network. Randomly select 100 rounds from the experimental processes of LEACH protocol, EEUC protocol, MADSEC protocol, and R-bUCRP, and count the distribution of cluster heads' number and the results are shown in Figures 8–11. Among these, LEACH

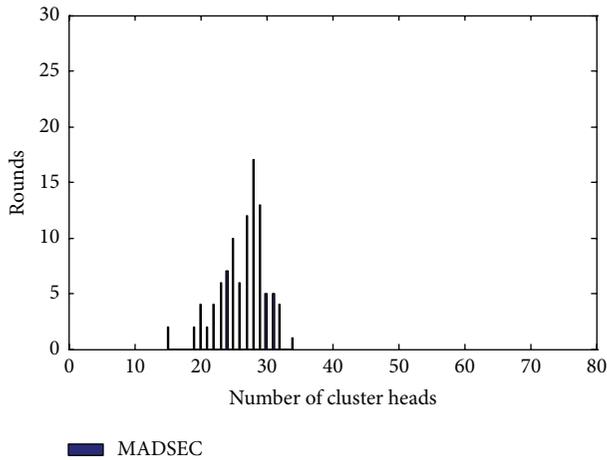


FIGURE 11: Cluster head number distribution of MADSEC.

protocol only uses the random number and threshold mechanism in the cluster head election; therefore, the range of cluster head number is large by using LEACH protocol. MADSEC protocol uses the K -means algorithm to divide the network area. EEUC protocol and R-bUCRP use the competitive function of cluster head candidates, and the number of cluster heads is controlled effectively within a certain range. In addition, R-bUCRP generates a more stable number of the cluster heads, which has better reliability.

5. Conclusion

A reputation-based uneven cluster routing protocol R-bUCRP is proposed in this paper. The protocol adopts an uneven clustering method and introduces the reputation mechanism to reduce the communicational energy consumption between normal nodes and selfish nodes and increase the reliability of the network effectively. The algorithm optimizes the process of cluster head selection by competing for the cluster head among cluster head candidate nodes according to the residual energy and reputation value. Simulation results show that R-bUCRP can balance the network energy consumption, prolong the network lifetime, and increase the network reliability effectively.

Competing Interests

The authors declare that there are no competing interests regarding the publication of this paper.

Acknowledgments

This work is partially supported by the National Natural Science Foundation of China (NSFC) under Grants no. U1404611, no. U1204614, and no. 61370221, in part by the Program for Science & Technology Innovation Talents in the University of Henan Province under Grants no. 16HASTIT035 and no. 14HASTIT045, in part by Program for Science & Technology Innovative Research Team in University of Henan Province under Grant no. 14IRTSTHN021,

and in part by Henan Science and Technology Innovation Outstanding Talent under Grant no. 164200510007.

References

- [1] J. Mitola III and G. Q. Maguire Jr., "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18, 1999.
- [2] R. Uргаonkar and M. J. Neely, "Opportunistic scheduling with reliability guarantees in cognitive radio networks," in *Proceedings of the IEEE Conference on Computer Communications (INFOCOM '08)*, Phoenix, Ariz, USA, April 2008.
- [3] E. Dall'Anese, S.-J. Kim, G. B. Giannakis, and S. Pupolin, "Power allocation for cognitive radio networks under channel uncertainty," in *Proceedings of the IEEE International Conference on Communications (ICC '11)*, pp. 1–6, Kyoto, Japan, June 2011.
- [4] R. W. Thomas, D. H. Friend, L. A. DaSilva, and A. B. MacKenzie, "Cognitive networks: adaptation and learning to achieve end-to-end performance objectives," *IEEE Communications Magazine*, vol. 44, no. 12, pp. 51–57, 2006.
- [5] C. Fortuna and M. Mohorcic, "Trends in the development of communication networks: cognitive networks," *Computer Networks*, vol. 53, no. 9, pp. 1354–1376, 2009.
- [6] A. Rabbachin, T. Q. S. Quek, H. Shin, and M. Z. Win, "Cognitive network interference," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 2, pp. 480–493, 2011.
- [7] M. Zhang, H. Zhao, R. Zheng, Q. Wu, and W. Wei, "Cognitive internet of things: concepts and application example," *International Journal of Computer Science Issues*, vol. 9, no. 6, pp. 151–158, 2012.
- [8] M. Zhang, Y. Qiu, R. Zheng, X. Bai, W. Wei, and Q. Wu, "A novel architecture for cognitive internet of things," *International Journal of Security and Its Applications*, vol. 9, no. 9, pp. 235–252, 2015.
- [9] R. Zheng, Q. Wu, M. Zhang, G. Li, J. Pu, and H. Wang, "A self optimization mechanism of system service performance based on autonomic computing," *Computer Research and Development*, vol. 48, no. 9, pp. 1676–1684, 2011 (Chinese).
- [10] M. Zhang, R. Zheng, Q. Wu, W. Wei, X. Bai, and H. Zhao, "Bi-ITRS: a bio-inspired trusted routing scheme for wireless sensor networks," *Journal of Sensors*, vol. 2015, Article ID 156843, 8 pages, 2015.
- [11] R.-I. Ciobanu, C. Dobre, M. Dascălu, Ș. Trăușan-Matu, and V. Cristea, "SENSE: a collaborative selfish node detection and incentive mechanism for opportunistic networks," *Journal of Network and Computer Applications*, vol. 41, no. 1, pp. 240–249, 2014.
- [12] W. Guo, R.-Z. Xu, and B. Liu, "Research on subjective trust routing algorithm for mobile ad hoc networks," in *Proceedings of the 6th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '10)*, pp. 1–6, IEEE, Chengdu, China, September 2010.
- [13] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences (HICSS '33)*, Maui, Hawaii, USA, January 2000.
- [14] A. Manjeshwar and D. Agrawal, "TEEN: a protocol for enhanced efficiency in wireless sensor networks," in *Proceedings of the 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing*, San Francisco, Calif, USA, 2001.

- [15] A. Manjeshwar and D. P. Agarwal, "APTEEN: a hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks," in *Proceedings of the International Parallel and Distributed Processing Symposium (IPDPS '02)*, pp. 195–202, Fort Lauderdale, Fla, USA, April 2002.
- [16] L. Bhasker, "Genetically derived secure cluster-based data aggregation in wireless sensor networks," *IET Information Security*, vol. 8, no. 1, pp. 1–7, 2014.
- [17] H. Lin and H. Uster, "Exact and heuristic algorithms for data-gathering cluster-based wireless sensor network design problem," *IEEE/ACM Transactions on Networking*, vol. 22, no. 3, pp. 903–916, 2014.
- [18] P. T. A. Quang and D.-S. Kim, "An energy efficient clustering in heterogeneous wireless sensor and actuators networks," in *Proceedings of the IEEE Globecom Workshops (GC Wkshps '12)*, pp. 524–528, Anaheim, Calif, USA, December 2012.
- [19] K. Li and K. A. Hua, "Mobility-assisted distributed sensor clustering for energy-efficient wireless sensor networks," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM '13)*, pp. 316–321, IEEE, Atlanta, Ga, USA, December 2013.
- [20] M. Ye, C. Li, G. Chen, and J. Wu, "EECS: an energy efficient clustering scheme in wireless sensor networks," in *Proceedings of the 24th IEEE International Performance, Computing, and Communications Conference (PCCC '05)*, pp. 535–540, Phoenix, Ariz, USA, April 2005.
- [21] S. Soro and W. Heinzelman, "Prolonging the lifetime of wireless sensor networks via unequal clustering," in *Proceedings of the 5th IEEE International Workshop on Algorithms for Wireless, Mobile, Ad Hoc and Sensor Networks (WMAN '05)*, Denver, Colo, USA, 2005.
- [22] C. F. Li, M. Ye, G. H. Chen, and J. Wu, "An energy-efficient unequal clustering mechanism for wireless sensor networks," in *Proceedings of the 2nd IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS '05)*, pp. 597–604, IEEE, Washington, DC, USA, November 2005.
- [23] T. Chen, Y. Luo, F. Xiao, D. Shi, and S. Zhang, "Uneven clustering algorithm based on clustering optimization for wireless sensor networks," *Computer Science*, vol. 41, no. 6A, pp. 289–292, 2014 (Chinese).
- [24] C.-J. Jiang, W.-R. Shi, X.-L. Tang, P. Wang, and M. Xiang, "Energy-balanced unequal clustering routing protocol for wireless sensor networks," *Journal of Software*, vol. 23, no. 5, pp. 1222–1232, 2012 (Chinese).
- [25] S. Buchegger and Y. J. Le Boudec, "The selfish node: increasing routing security for mobile ad hoc networks," LCA-Report 2001-008, 2001.
- [26] P. Naghizadeh and M. Liu, "Perceptions and truth: a mechanism design approach to crowd-sourcing reputation," *IEEE/ACM Transactions on Networking*, vol. 24, no. 1, pp. 163–175, 2016.
- [27] Z. Li, H. Shen, and K. Sapra, "Leveraging social networks to combat collusion in reputation systems for peer-to-peer networks," *IEEE Transactions on Computers*, vol. 62, no. 9, pp. 1745–1759, 2013.
- [28] M. T. Refaei, L. A. DaSilva, M. Eltoweissy, and T. Nadeem, "Adaptation of reputation management systems to dynamic network conditions in ad hoc networks," *IEEE Transactions on Computers*, vol. 59, no. 5, pp. 707–719, 2010.
- [29] N. Labraoui, M. Gueroui, and L. Sekhri, "A risk-aware reputation-based trust management in wireless sensor networks," *Wireless Personal Communications*, vol. 87, no. 3, pp. 1037–1055, 2016.
- [30] A. Caposelle, G. De Cicco, and C. Petrioli, "R-CARP: a reputation based channel aware routing protocol for underwater acoustic sensor networks," in *Proceedings of the International Conference on Underwater Networks & Systems*, Arlington, Va, USA, October 2015.
- [31] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Advanced Communications and Multimedia Security*, B. Jerman-Blažič and T. Klobučar, Eds., vol. 100 of *IFIP—The International Federation for Information Processing*, pp. 107–121, Springer, New York, NY, USA, 2002.
- [32] M. Zhang, C. Xu, J. Guan, R. Zheng, Q. Wu, and H. Zhang, "A novel *Physarum*-inspired routing protocol for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 483581, 12 pages, 2013.
- [33] M. Zhang, C. Xu, J. Guan, R. Zheng, Q. Wu, and H. Zhang, "A novel bio-inspired trusted routing protocol for mobile wireless sensor networks," *KSII Transactions on Internet and Information Systems*, vol. 8, no. 1, pp. 74–90, 2014.
- [34] Q. Wu, X. Zhang, M. Zhang, Y. Lou, R. Zheng, and W. Wei, "Reputation revision method for selecting cloud services based on prior knowledge and a market mechanism," *The Scientific World Journal*, vol. 2014, Article ID 617087, 9 pages, 2014.

Research Article

A Passenger Flow Risk Forecasting Algorithm for High-Speed Railway Transport Hub Based on Surveillance Sensor Networks

Zhengyu Xie^{1,2} and Yong Qin²

¹School of Traffic and Transportation, Beijing Jiaotong University, Beijing 100044, China

²State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing 100044, China

Correspondence should be addressed to Yong Qin; yqin@bjtu.edu.cn

Received 18 March 2016; Revised 14 May 2016; Accepted 7 June 2016

Academic Editor: Iftikhar Ahmad

Copyright © 2016 Z. Xie and Y. Qin. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Passenger flow risk forecasting is a vital task for safety management in high-speed railway transport hub. In this paper, we considered the passenger flow risk forecasting problem in high-speed railway transport hub. Based on the surveillance sensor networks, a passenger flow risk forecasting algorithm was developed based on spatial correlation. Computational results showed that the proposed forecasting approach was effective and significant for the high-speed railway transport hub.

1. Introduction

In the 12th Five-Year Plan (2011–2015) period, high-speed railway in China had a fast development. As of December 31, 2015, the high-speed railway lines amounting to a total length of 19000 km were operated in mainland China, and most cities with more than 50 million populations were covered by the high-speed railway transport networks. With the fast development of high-speed railway, high-speed railway transport hub has become a vital node of passenger transport networks and several transport modes, that is, civil aviation, highway, urban rail transit, and public transport transferred in high-speed railway transport hub. Massive passenger flow collecting and distributing brings several potential risks to the safety management of high-speed railway transport hub.

At present, most of high-speed railway transport hubs have emergency plans for different risks, especially passenger flow risk. When risk values meet the threshold, these plans are activated immediately. But current approach only passively responded for emergency and lacks actively detection and forecasting of risks. With wide application of intelligent video surveillance in high-speed railway transport hubs, a comprehensive surveillance sensor networks is gradually formed, which provides powerful supports for risk detecting and forecasting. Based on real-time passenger flow status obtained by surveillance sensor networks, passenger flow

risk forecasting can effectively prevent risks, reduce risks value, and decrease the negative effects caused by risks. So it is necessary for high-speed railway transport hubs to study on passenger flow risk forecasting approach based on surveillance sensor networks.

The rest of this paper is organized as follows: Section 2 reviews the relevant literature. The passenger flow risk forecasting frame is introduced in Section 3, and Section 4 proposes a passenger flow risk forecasting algorithm based on spatial correlation. Computational experiments are conducted in Section 5 and finally Section 6 covers the conclusion.

2. Literature Review

Currently, video surveillance is the key approach to detect the potential risks in transport hubs. Several passenger image processing and intelligent detecting algorithms were developed for rapid and accurate detection of passenger flow status [1–8]. A real-time system for detecting and tracking multiple people when they appear in a group was proposed. Several computational models, that is, a silhouette-based shape model, a motion model, and correlation-based matching methods were employed to track multiple people before, during, and after occlusion [1]. For automatically

tracking pedestrian, a pedestrian tracking system was proposed, consisting of three subsystems, which calculates the image processing, object tracking, and traffic flow variables. The first subsystem performs image processing analysis while the second subsystem carries out the tracking of pedestrians by matching the features and tracing the pedestrian numbers frame by frame [2]. In order to accurately and promptly detect potential safety hazard, a modified background model based on Dempster-Shafer theory and a passenger flow status recognition algorithm based on features of image connected domain were proposed to improve the accuracy and real-time performance of passenger flow detection [3]. To improve detection accuracy in terms of feature extraction, a novel feature of gradient self-similarity (GSS) was present, which was computed from HOG and was applied to capture the patterns of pairwise similarities of local gradient patches [4]. For the challenging of abrupt illumination, occlusions, out of field of view, and cluttered backgrounds, a novel tracking framework was developed, which consists of two steps: image shadow removal and tracking by association [5]. A sparse representation based approach is proposed for pedestrian detection from thermal images. The approach first adopted the histogram of sparse code to represent image features and then detect pedestrian with the extracted features in a unimodal and a multimodal framework, respectively [6]. In order to accurately detect potential safety hazard hidden in passenger flow, a hybrid forecasting approach was proposed to obtain the passenger flow status [7]. By thoroughly analyzing and optimizing each step of the detection pipeline, a pedestrian detection system was proposed based on deep learning, adapting a general-purpose convolutional network to the task at hand [8].

Some studies focused on causing and handling of the potential risks [9–15]. A pedestrian evacuation simulation model based on the extended cellular automata was proposed with the consideration of heterogeneous behavioral tendencies in humans, and the model was applied to optimize buildings to reduce evacuation times [9]. A more comprehensive conceptual model was introduced for the representation of the impact of fatigue on the performance of evacuees during building stair evacuation. The model was presented considering its conceptual formulation and the issues associated with its implementation [10]. A multigrid model was proposed to simulate evacuation with guiders, and the effects of guider type, guider number, guider distribution, and guidance strategy on evacuation were discussed [11]. The selfish and selfless behaviors were considered as two main factors in evacuation, and selfishness- and selflessness-based model of pedestrian room evacuation was proposed [12]. A new multiagent based congestion evacuation model incorporating panic behavior was proposed for simulating pedestrian evacuation in public places such as a stadium. Pedestrians in this model were divided into four classes and each pedestrian's status can be either normal, overtaken, or casualty [13]. The evacuation process from a room without visibility was investigated by both experiment and modeling. Some typical characteristics of blind evacuation, including the preference of choosing left-hand side direction and following behavior, were found from the experiment

[14]. A pedestrian evacuation modeling framework was developed, which used volunteered geographical information from OpenStreetMap and simplified queuing-network model to estimate evacuation time, detect bottlenecks, and test different evacuation strategies [15].

According to the literature review above, current studies only focused on the potential risks detection and risk handling. For passenger flow forecasting, most of studies concerned passenger flow demand, arriving, and departure volume forecasting [16–19]. Specific literature on risk forecasting is scarce. The risk forecasting is an important connection between potential risks detection and risk handling. Based on the detection result, forecasting the passenger flow risk can well master the variation trend of risk and adopt suitable handling operations. So in this paper, we consider the passenger flow risk forecasting in high-speed railway transport hub. Based on surveillance sensor networks, a spatial correlation forecasting algorithm is developed to forecast the passenger flow risk of bottleneck areas.

3. Passenger Flow Risk Forecasting Frame

In this section, the passenger flow risk forecasting frame is described in three aspects. Firstly, surveillance sensor networks of high-speed railway transport hub are introduced. Secondly, forecasting mechanism is described. Based on the previous two parts, the forecasting procedure is designed in the last part.

3.1. Surveillance Sensor Networks of High-Speed Railway Transport Hub. According to the different surveillance purposes and focuses, the sensors in surveillance sensor networks of high-speed railway transport hub can be classified into three types [20], key area monitoring sensors, passenger line monitoring sensors, and complete coverage monitoring sensors, which are shown in Figure 1.

For the three types of sensors (Figure 1), our study mainly focuses on the passenger flow risk forecasting of key area. The forecasting not only use the passenger flow data detected by key area monitoring sensors but also used the passenger flow data obtained by passenger line monitoring sensors.

3.2. Passenger Flow Risk Forecasting Mechanism. The accuracy of passenger flow risk forecasting in key area is influenced by several factors, that is, current risk status of key area, risk status of correlated surveillance areas in passenger line, and service capability of equipment in key area. So it is hard to obtain an accurate risk forecasting value by only using the risk status of key area.

In this paper, we consider the passenger flow risk forecasting of key area under the surveillance sensor networks in high-speed railway transport hub. By analyzing the relationship between key area and correlated surveillance areas in passenger line, a forecasting algorithm is developed based on spatial correlation.

The spatial correlation between key area and correlated areas in passenger line can be defined as the impact on key area risk caused by correlated areas. A sample of spatial

Sensor in surveillance sensor networks	Key area monitoring sensors	(i) Sensors in different key areas are independent and do not have any relevance (ii) Sensors do not need adjustment after setting (iii) Sensors have front-end event detecting software
	Passenger line monitoring sensors	(i) Sensors should be set following the passenger line (ii) Sensors in the same passenger line have association (iii) Sensors do not need adjustment after setting (iv) The data acquired by sensors should be continuously transferred to the control center to process
	Complete coverage monitoring sensors	(i) Sensors should cover all the function areas in HRTH (ii) The monitoring areas of sensors should reduce overlaps as much as possible (iii) Sensors can adjust monitoring areas after setting (iv) The data acquired by sensors should be continuously transferred to the control center to be stored

FIGURE 1: Sensors in surveillance sensor networks.

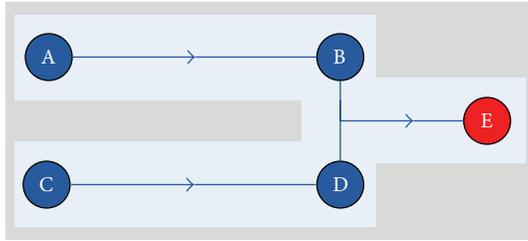


FIGURE 2: A sample of spatial correlation.

correlation is shown in Figure 2. In the figure, the red point is the key area, blue points are correlated surveillance areas, and the blue arrows are passenger line. The passengers moved from A to B and C to D and converge to E. The A, B, C, and D have spatial correlation with E, and the spatial correlation degrees of B and D are larger than the spatial correlation degrees of A and C.

3.3. Passenger Flow Risk Forecasting Procedure. In the surveillance sensor networks of high-speed railway transport hub, based on the spatial correlation, there are three main steps in the passenger flow risk forecasting procedure, which are shown in Figure 3.

Step 1. Calculate the risk value $r(x)$ of correlated surveillance areas by using the passenger flow status of the areas.

Step 2. Calculate spatial correlation degrees $s(x, y)$ between key area and correlated surveillance areas based on the surveillance sensor networks of high-speed railway transport hub.

Step 3. Forecast the risk value $R(e)$ of key area based on the current risk value $r(e)$ of key area, $r(x)$, and $s(x, y)$ obtained by Steps 1 and 2.

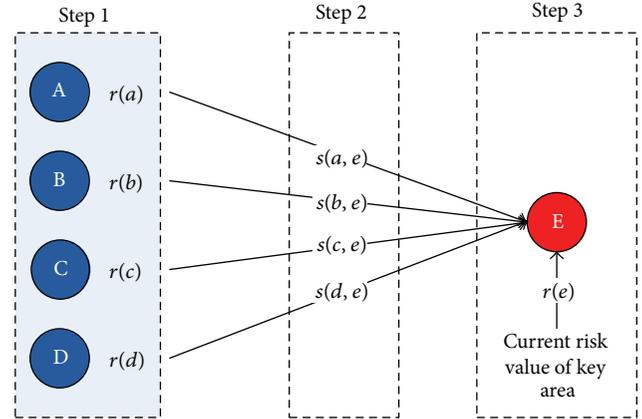


FIGURE 3: Main steps in the passenger flow risk forecasting procedure.

4. A Passenger Flow Risk Forecasting Algorithm Based on Spatial Correlation

According to passenger flow risk forecasting procedure mentioned in Section 3, the calculation method of passenger flow risk value and forecasting algorithm based on spatial correlation will be discussed in this section.

4.1. Passenger Flow Risk Value Calculation. In this paper, we adopt passenger flow amount to calculate the risk value in key area and correlated surveillance areas. And three types of passenger flow status parameters are used, which are current passenger flow amount of area A_1 , average passenger flow amount of area in statistic period A_2 , and max passenger flow amount of area in statistic period A_3 . Based on plenty of data experiments for different areas in high-speed railway transport hubs, the passenger flow risk values in key area and correlated surveillance areas can be calculated as follows.

(1) While current passenger flow amount is less than or equal to average passenger flow amount in statistic period, $A_1 \leq A_2$,

$$r(x) = 3 - 10 \left(\frac{A_2 - A_1}{A_2} \right). \quad (1)$$

(2) While current passenger flow amount is larger than average passenger flow amount in statistic period and less than or equal to max passenger flow amount of area in statistic period, $A_2 < A_1 \leq A_3$,

$$r(x) = \frac{4A_1 + 3A_3 - 7A_2}{A_3 - A_2}. \quad (2)$$

(3) While current passenger flow amount is larger than max passenger flow amount of area in statistic period, $A_1 > A_3$,

$$r(x) = 7 + 10 \left(\frac{A_1 - A_3}{A_3} \right). \quad (3)$$

4.2. Spatial Correlation Degree Calculation. The spatial correlation reflects the risk correlation between key area and correlated surveillance areas. And the spatial correlation degree is an important indicator to represent the impact on passenger flow risk of key area caused by the risk value of correlated surveillance areas.

$r_i = \{r_i(t) \mid t = 1, 2, \dots, n\}$ is a time series set, representing risk values of one key area and i correlated surveillance areas at different time. $r_0(t)$ is the risk values of key area in t period, and $r_i(t)$ is the risk values of the i th correlated surveillance area in t period. The spatial correlation degree between the key area and i th correlated surveillance area in t period can be calculated as follows:

$$s(r_0(t), r_i(t)) = \frac{m + \omega M}{\Delta(0, i) + \omega M}, \quad (4)$$

where $\Delta(0, i) = |r_0(t) - r_i(t)|$, $m = \min_i \min_t \Delta(0, i)$, $M = \max_i \max_t \Delta(0, i)$, and ω is the identification coefficient, $\omega \in (0, 1)$.

According to the incidence extent, each spatial correlation between key area and one correlated surveillance area has a correlation weight coefficient, which can be calculated by

$$\alpha_i = \frac{s(r_0(t), r_i(t))}{\sum_{j=1}^n s(r_0(t), r_j(t))}. \quad (5)$$

4.3. Forecasting Algorithm Based on Spatial Correlation. For a key area k , it has n correlated surveillance areas ck_i , $i = 1, 2, \dots, n$. Based on the passenger flow risk value of k and ck_i and the spatial correlation among their areas, the initial passenger flow risk of k in t period can be forecasted as follows:

$$r'_k(t) = \sum_{i=1}^n \alpha_i r_i(t - t_i), \quad (6)$$

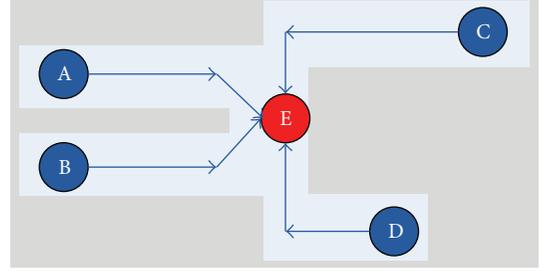


FIGURE 4: Schematic representation of areas.

where α_i is the correlation weight coefficient between k and ck_i and t_i is the correlation time between k and ck_i .

In actual forecasting, for improving the accuracy, we employ the initial forecasting value and actual passenger flow risk values before t period to forecast the passenger flow risk of k in t period. The forecasting algorithm is shown as follows:

$$\begin{aligned} r_k(t) &= r_k(t-1) + \Delta r_k(t) \\ &= r_k(t-2) + r_k(t-1) + \Delta r_k(t) \\ &= r_k(0) + \Delta r_k(1) + \Delta r_k(2) + \dots + \Delta r_k(t). \end{aligned} \quad (7)$$

Set $\Delta r_k(t) = \Delta r'_k(t)$, and $\Delta r'_k(t) = r'_k(t) - r'_k(t-1)$. So the forecasting algorithm can be transferred as follows:

$$\begin{aligned} r_k(t) &= r'_k(t) - r'_k(0) + r_k(0) \\ &= \sum_{i=1}^n \alpha_i r_i(t - t_i) - \sum_{i=1}^n \alpha_i r_i(0) + r_k(0), \end{aligned} \quad (8)$$

where $r_k(0)$ is the actual passenger flow risk value of k at the initial forecasting period and $r_i(0)$ is the actual passenger flow risk value of ck_i at the initial forecasting period.

5. Computational Experiments

In this section, computational experiments are conducted to verify passenger flow risk algorithm proposed above. A specific key area in high-speed railway transport hub is taken as an example. This area is an escalator connecting waiting hall and entrances. The schematic representation of their areas is shown in Figure 4.

The E is the escalator. A and B are two metro transfer points; the passengers arriving by metro enter the hub from these two points. C is an entrance; the passengers arriving by public transport enter the hub from this entrance. D is a park entrance; the passengers arriving by private car enter the hub from this entrance. Both of these areas have intelligent surveillance, which can automatically detect the passenger flow amount and calculate the risk value. Based on the real detection data from intelligent surveillance sensors, the forecasting algorithm developed in Section 3 is employed to forecast the passenger flow risk of area E. We set 10 minutes as a forecasting period, and firstly experiment on 6 hours (12:00 am–6:00 pm) is conducted. The computational result

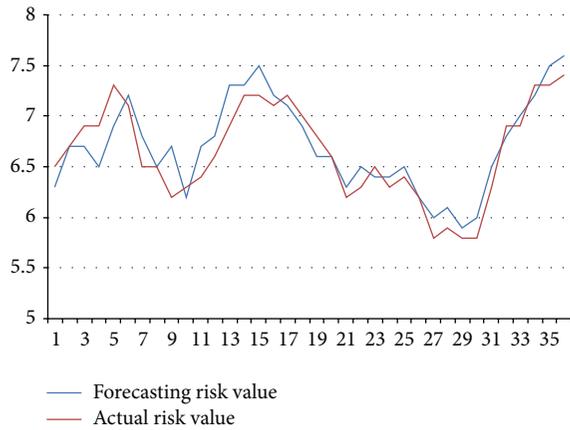


FIGURE 5: Comparison between forecasting risk value and actual risk value.

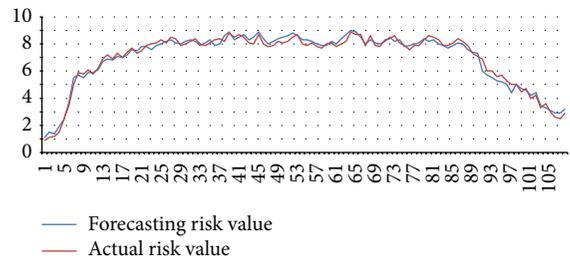


FIGURE 6: Computational result of a festival day.

is shown in Table 1, and comparison between forecasting risk value and actual risk value is shown in Figure 5.

As observed in Figure 5, the forecasting risk values obtained by our approach are close to actual risk value; the average gap between forecasting risk value and actual risk value is 2.6%. And the variation trend of passenger flow risk is well forecasted by our approach. For illustrating the performance of our forecasting approach facing mass passenger flow, a festival day (6:00 am–12:00 pm) is selected as an example. The computational result is shown in Figures 6 and 7.

As observed in Figures 6 and 7, our forecasting approach has a good performance for mass passenger flow in festival days. It can well forecast variation trend of passenger flow risk in a whole day time (6:00 am–12:00 pm is a normal operation time of hub) except some low risk periods. Generally, our forecasting approach can meet the demands of safety management in high-speed railway transport hub.

6. Conclusion

In this paper, we considered the passenger flow risk forecasting problem in high-speed railway transport hub. According to the surveillance sensor network of hub, a spatial correlation degree calculation between the key area and the correlated surveillance area was proposed, and a passenger flow risk forecasting algorithm based on spatial correlation was developed. Computational experiments on a key area in

TABLE 1: Computational result of 6 hours (12:00 am–6:00 pm).

Hour	Period	Forecasting risk value	Actual risk value	Gap
12:00 am	1	6.3	6.5	3.08%
	2	6.7	6.7	0.00%
	3	6.7	6.9	2.90%
	4	6.5	6.9	5.80%
	5	6.9	7.3	5.48%
	6	7.2	7.1	1.41%
1:00 pm	7	6.8	6.5	4.62%
	8	6.5	6.5	0.00%
	9	6.7	6.2	8.06%
	10	6.2	6.3	1.59%
	11	6.7	6.4	4.69%
	12	6.8	6.6	3.03%
2:00 pm	13	7.3	6.9	5.80%
	14	7.3	7.2	1.39%
	15	7.5	7.2	4.17%
	16	7.2	7.1	1.41%
	17	7.1	7.2	1.39%
	18	6.9	7.0	1.43%
3:00 pm	19	6.6	6.8	2.94%
	20	6.6	6.6	0.00%
	21	6.3	6.2	1.61%
	22	6.5	6.3	3.17%
	23	6.4	6.5	1.54%
	24	6.4	6.3	1.59%
4:00 pm	25	6.5	6.4	1.56%
	26	6.2	6.2	0.00%
	27	6.0	5.8	3.45%
	28	6.1	5.9	3.39%
	29	5.9	5.8	1.72%
	30	6.0	5.8	3.45%
5:00 pm	31	6.5	6.3	3.17%
	32	6.8	6.9	1.45%
	33	7.0	6.9	1.45%
	34	7.2	7.3	1.37%
	35	7.5	7.3	2.74%
	36	7.6	7.4	2.70%

high-speed railway transport hub showed that the proposed forecasting approach is effective to forecast the passenger flow risk of key area in hub. In future, considering several key areas risk, forecasting the whole safety status of high-speed railway transport hub is a possibility for further research.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

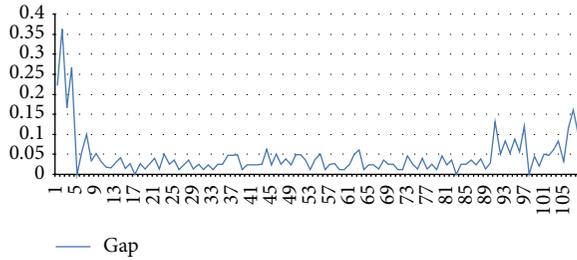


FIGURE 7: Gap between forecasting risk value and actual risk value in a festival day.

Acknowledgments

This research was supported by the Fundamental Research Funds for the Central Universities (Grant no. 2015JBM044) and the Talented Faculty Funds of Beijing Jiaotong University (Grant no. 2014RC005).

References

- [1] I. Haritaoglu, D. Harwood, and L. S. Davis, "Hydra: multiple people detection and tracking using silhouettes," in *Proceedings of the 10th International Conference on Image Analysis and Processing (ICIAP '99)*, pp. 280–285, IEEE, Venice, Italy, September 1999.
- [2] K. Teknomo, Y. Takeyama, and H. Inamura, "Tracking system to automate data collection of microscopic pedestrian traffic flow," in *Proceedings of the 4th Eastern Asia Society for Transportation Studies*, vol. 3, no. 1, pp. 11–25, Hanoi, Vietnam, October 2001.
- [3] S. Wu, R. Laganière, and P. Payeur, "Improving pedestrian detection with selective gradient self-similarity feature," *Pattern Recognition*, vol. 48, no. 8, pp. 2364–2376, 2015.
- [4] Z. Y. Xie, L. M. Jia, Y. Qin, and L. Wang, "Passenger flow detection of video surveillance: a case study of high-speed railway transport hub in China," *Elektronika ir Elektrotechnika*, vol. 21, no. 1, pp. 48–53, 2015.
- [5] X. Shen, X. Sui, K. Pan, and Y. Tao, "Adaptive pedestrian tracking via patch-based features and spatial-temporal similarity measurement," *Pattern Recognition*, vol. 53, pp. 163–173, 2016.
- [6] B. Qi, V. John, Z. Liu, and S. Mita, "Pedestrian detection from thermal images: a sparse representation based approach," *Infrared Physics & Technology*, vol. 76, pp. 157–167, 2016.
- [7] Z. Y. Xie, L. M. Jia, Y. Qin, and L. Wang, "A hybrid temporal-spatio forecasting approach for passenger flow status in Chinese high-speed railway transport hub," *Discrete Dynamics in Nature and Society*, vol. 2013, Article ID 239039, 7 pages, 2013.
- [8] D. Tomè, F. Monti, L. Baroffio, L. Bondi, M. Tagliasacchi, and S. Tubaro, "Deep convolutional neural networks for pedestrian detection," <http://arxiv.org/abs/1510.03608>.
- [9] D. Li and B. Han, "Behavioral effect on pedestrian evacuation simulation using cellular automata," *Safety Science*, vol. 80, pp. 41–55, 2015.
- [10] E. Ronchi, P. A. Reneke, and R. D. Peacock, "A conceptual fatigue-motivation model to represent pedestrian movement during stair evacuation," *Applied Mathematical Modelling*, vol. 40, no. 7–8, pp. 4380–4396, 2016.
- [11] S. Cao, W. Song, and W. Lv, "Modeling pedestrian evacuation with guiders based on a multi-grid model," *Physics Letters, Section A: General, Atomic and Solid State Physics*, vol. 380, no. 4, pp. 540–547, 2016.
- [12] X. Song, L. Ma, Y. Ma, C. Yang, and H. Ji, "Selfishness- and Selflessness-based models of pedestrian room evacuation," *Physica A: Statistical Mechanics and Its Applications*, vol. 447, pp. 455–466, 2016.
- [13] J. Wang, L. Zhang, Q. Shi, P. Yang, and X. Hu, "Modeling and simulating for congestion pedestrian evacuation with panic," *Physica A: Statistical Mechanics and Its Applications*, vol. 428, pp. 396–409, 2015.
- [14] S. Cao, W. Song, W. Lv, and Z. Fang, "A multi-grid model for pedestrian evacuation in a room without visibility," *Physica A: Statistical Mechanics and Its Applications*, vol. 436, pp. 45–61, 2015.
- [15] B. Kunwar, F. Simini, and A. Johansson, "Large scale pedestrian evacuation modeling framework using volunteered geographical information," *Transportation Research Procedia*, vol. 2, pp. 813–818, 2014.
- [16] Z. Ma, J. Xing, M. Mesbah, and L. Ferreira, "Predicting short-term bus passenger demand using a pattern hybrid approach," *Transportation Research Part C: Emerging Technologies*, vol. 39, pp. 148–163, 2014.
- [17] C. Zhou, P. Dai, F. Wang, and Z. Zhang, "Predicting the passenger demand on bus services for mobile users," *Pervasive and Mobile Computing*, vol. 25, pp. 48–66, 2016.
- [18] G. Xie, S. Wang, and K. K. Lai, "Short-term forecasting of air passenger by using hybrid seasonal decomposition and least squares support vector regression approaches," *Journal of Air Transport Management*, vol. 37, pp. 20–26, 2014.
- [19] Y. Wei and M.-C. Chen, "Forecasting the short-term metro passenger flow with empirical mode decomposition and neural networks," *Transportation Research Part C: Emerging Technologies*, vol. 21, no. 1, pp. 148–162, 2012.
- [20] Z. Y. Xie and Y. Qin, "Sensor networks hierarchical optimization model for security monitoring in high-speed railway transport hub," *Journal of Sensors*, vol. 2015, Article ID 951242, 9 pages, 2015.

Research Article

Routing Algorithm with Uneven Clustering for Energy Heterogeneous Wireless Sensor Networks

Ying Zhang,¹ Wei Xiong,¹ Dezhi Han,¹ Wei Chen,² and Jun Wang^{1,3}

¹College of Information Engineering, Shanghai Maritime University, Shanghai 201306, China

²Department of Computer Science, Tennessee State University, Nashville, TN 37209, USA

³Department of Electrical and Computer Engineering, University of Central Florida, Orlando, FL 32816, USA

Correspondence should be addressed to Wei Xiong; xiongwei501@163.com, Dezhi Han; dzhan@shmtu.edu.cn, and Wei Chen; wchen@tnstate.edu

Received 3 June 2016; Accepted 14 August 2016

Academic Editor: Fei Yu

Copyright © 2016 Ying Zhang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Aiming at the “hotspots” problem in energy heterogeneous wireless sensor networks, a routing algorithm of heterogeneous sensor network with multilevel energies based on uneven clustering is proposed. In this algorithm, the energy heterogeneity of the nodes is fully reflected in the mechanism of cluster-heads’ election. It optimizes the competition radius of the cluster-heads according to the residual energy of the nodes. This kind of uneven clustering prolongs the lifetime of the cluster-heads with lower residual energies or near the sink nodes. In data transmission stage, the hybrid multihop transmission mode is adopted, and the next-hop routing election fully takes account of the factors of residual energies and the distances among the nodes. The simulation results show that the introduction of an uneven clustering mechanism and the optimization of competition radius of the cluster-heads significantly prolonged the lifetime of the network and improved the efficiency of data transmission.

1. Introduction

With the extension of detecting areas by human beings, information obtaining, information storage, and information processing, transmission, and application are embedded to every aspect in social production and daily life. Wireless sensor networks (WSNs) [1] integrated with the frontier technologies, such as sensing, microelectromechanical systems (MEMS), wireless communication, and distributed information processing, have emerged as the time requires. A wireless sensor network is comprised of a large number of small and cheap sensor nodes. The nodes communicate with each other by agreement strategies, and the communication strategies are administered by routing protocols [2]. The wireless sensor network has a wide application prospect in real life. It has an important research value and huge practicality value in many fields: environment monitoring, rescue and relief work, remote control in hazardous area, and so on. It will be recommended and applied in many fields with great favor [3, 4].

Nowadays, with the development of marine economy, the huge economic benefit is being brought about from the exploitation of marine resources, and meanwhile this causes environmental disruption in many marine areas. There are frequent occurrences of ocean disasters. How to dynamically detect the environmental factors becomes a serious challenge. With the development of sensors and computer networking, WSNs play an important role in the development of marine environment monitoring and forecasting [5–7]. Sensor nodes deployed in the ocean will change their initial position owing to the effect of ocean currents, and the AUVs (Autonomous Underwater Vehicles) collect the underwater environmental information in moving state. These all cause the dynamical change of the network’s topology.

Normally, the nodes of a wireless sensor network have limited energies. Due to the one-off deployment, it is difficult to replenish the energies [8]. Due to the different duty and equipping for the sensor nodes, the energy consumption will be different among them. So, it is an energy heterogeneous sensor network. Sometimes, the so-called “hotspots” easily

occur in sensor networks with heterogeneous energies in practical application. It is important to find an optimized route for the information transmission of the network. Routing protocols [9, 10] will be responsible for discovering and maintaining energy efficient routes and make communication reliable and efficient. "Hotspots" will make some nodes come to an untimely end due to the excessive energy consumption, and this will shorten the life cycle of the whole network [11]. Therefore, it is necessary to design the energy efficient protocol to adapt the features of this kind of sensor network. For the unbalanced energy consumption of the sensor networks, cluster-based sensor networks enable achieving efficient utilization of the limited energy resources of the deployed sensor nodes. The uneven clustering is suitable to be used in heterogeneous sensor networks [12]. In this way, it can extend the lifetime of the networks the furthest. The cluster-based routing protocol, whose goal is to reduce the node's energy consumption and improve the network lifetime, has become one of the hot topics in the study of wireless sensor networks.

The rest of this article is organized as follows. In Section 2, some related works on cluster-based routing algorithm for sensor networks are introduced. In Section 3, some necessary models are defined. Then, in Section 4, we describe the EDEUC method in detail. Section 5 comprises the simulation and results analysis, and finally we conclude the article in Section 6.

2. Related Work

According to the sensory ability, computing power, communication capacity, and carrying of energies, sensor nodes can be divided into different levels. Heterogeneous sensor networks mean a network composed of a variety of different types of sensor nodes [13]. The form organized into a cluster of sensor nodes can effectively reduce the network energy consumption. Some energy efficient routing protocols are designed based on the cluster structure. Currently, many cluster algorithms, such as LEACH [14, 15], PEGASIS [16], and HEED [17], are all set up based on homogeneous network. However, the pure homogeneous network is inexistent in practical application. It is just an ideal assumption. Each kind of protocol has its own characters. The algorithms used in homogeneous network cannot be duplicated to be used in heterogeneous network directly, so it is necessary to design the clustered-based routing algorithm which is suitable to be used in heterogeneous network [18, 19].

In recent years, many literatures have studied the feasibility of heterogeneous sensor networks in practice application, and some clustering methods for heterogeneous sensor networks were proposed. Solar LEACH [20] was proposed in 2004 by Voigt et al., which is an improved protocol based on extending the ordinary LEACH to two class level heterogeneous sensor networks. EELBC algorithm [21] was proposed by Jayashree et al., who structured the two-class clustering network model with cluster-head based on heterogeneous nodes; this protocol optimizes the deployment of the ordinary sensor nodes and the cluster-head nodes, so it

can extend the life cycle of the network. SEP protocol [22] was proposed in 2004 by Smaragdakis et al. In this protocol, nodes are divided into two kinds of nodes: normal nodes and advanced nodes. The advanced nodes have more chances to become the cluster-head, but this method only considers one factor: residual energy for the choice of cluster-head. Moreover, this method chooses one hop transmission mode for data transferring in inner cluster or among the clusters. The literature [23] proposed DEEC algorithm aiming at ordinary multilevel heterogeneous wireless sensor networks. The cluster-head can be elected based on residual energies of the nodes and the average energy of the network, and it can make the nodes with high initial energy and residual energy have more chances to become the cluster-head, so the energy consumption of the network could be balanced, and the cycle time of the network is prolonged. Cai et al. [24] proposed the RCR (Reliable Clustering Routing) method. It establishes a predictive model of residual energy, REP (Remaining Energy Prediction) applied to multilevel energies heterogeneous network, and it can solve the problem of energy loss for single node due to some kinds of fault. Every cluster will elect multicluster-heads to afford the tasks of cluster-heads jointly, but it has the problem of only considering one factor in the cluster election. Wang et al. [25] proposed the cluster method of load balance, LBCA (Load Balance Clustering Algorithm), which can be applied in multilevel energies heterogeneous sensor networks. It can elect the cluster-heads according to the energies distribution in the detecting area. The nodes with lower average communication energy have high priority to become the cluster-head in the area with homogeneous energy distribution, and the nodes with higher residual energies will have high priority to become the cluster-head in the area with unbalanced distribution of energy. Aiming at the problem of lifetime for heterogeneous network, the literature [26] proposed an optimal algorithm of lifetime for multilevel energies heterogeneous sensor networks: SNLOC (Sensor Network Lifetime Optimization Clustering Algorithm). The literature [27] proposed an uneven cluster-based routing protocol for wireless sensor networks. It makes the nodes near the sink node have a small scale cluster by the uneven competition scope, and the unequal-sized scope is determined by the subjective settings. So, they all do not give a practical algorithm to realize the uneven clustering for this kind of sensor network systematically and effectively.

In this paper, we proposed a routing algorithm for multilevel energies heterogeneous sensor networks based on uneven clustering, EDEUC (Energy-Distance Efficiency Based on Uneven Clustering), which constructs an optimal path to the base station with multihops by cluster-heads. The EDEUC strategy can reduce the energy consumption of the nodes and prolong the life cycle of sensor networks effectively.

The main contribution of the article reflects as follows: the energy heterogeneity is fully considered in the election of cluster-heads, the competition radius of the cluster-heads is optimized according to the residual energy of the nodes, and this improves the stability of clusters. The lifetime of the nodes with lower residual energies or near the sink nodes can be prolonged by this kind of uneven clustering mechanism and this improves the stability of the networks. The hybrid

multihop transmission mode is adopted in data transmission stage. The next-hop routing election fully takes account of the factors of residual energies and the distances among the nodes, and this improves the efficiency of data transmission.

3. Network Model

3.1. Assumption of Network Model. For the heterogeneous network model, we suppose that there are N sensor nodes distributed in a two-dimensional square area: $M \times M$ randomly. The nodes collect environment information periodically. The sensor network has features as follows:

- (1) The sensor network is the static network, and the nodes can only have micromotion or hold still after deployment.
- (2) The energy of the base station is controllable. The energy is heterogeneous for all the nodes, and the energies cannot be supplemented.
- (3) All the nodes have the function of data fusion, and every node has a unique ID.
- (4) The communication between the nodes in cluster and cluster-head adopts single hop mode, and the communication between cluster-head and the sink node adopts multihop mode by relay.

The wireless channel is symmetrical. The energy consumption for transmitting one bit from node A to node B is equal to the energy consumption for transmitting one bit from node B to node A .

3.2. Energy Model for Sensor Networks. In multilevel energy heterogeneous network, the initial energy of nodes is distributed randomly in the closed interval: $[E_0, E_0(1 + \alpha_i)]$, where E_0 is the minimum energy of the nodes and $\alpha_i \in (0, 1)$ is the multiple coefficient of the initial energy of node S_i more than E_0 . Suppose the number of all the nodes in the network is N . The initial energy of the whole multilevel energies heterogeneous network can be presented as the following formula:

$$E_{\text{total}} = \sum_{i=1}^N E_0 (1 + \alpha_i) = E_0 \left(N + \sum_{i=1}^N \alpha_i \right). \quad (1)$$

The calculation of energy loss in the process of wireless communication is in accordance with the energy consumption model in the literature [21]. Suppose the threshold of communication distance $d_0 = \sqrt{\varepsilon_{\text{fs}}/\varepsilon_{\text{mp}}}$; when the distance of nodes transmitting data $d < d_0$, the channel model of free space will be used; when the distance of nodes transmitting data $d \geq d_0$, the multichannel attenuation model will be used as well.

The energy consumption of sensor node transmitting the data of k bit can be described as

$$E_{\text{Tx}}(k, d) = E_{\text{Txelec}}(k) + E_{\text{Txamp}}(k, d) = \begin{cases} kE_{\text{elec}} + k\varepsilon_{\text{fs}}d^2, & d < d_0 \\ kE_{\text{elec}} + k\varepsilon_{\text{fs}}d^4, & d \geq d_0. \end{cases} \quad (2)$$

The energy consumption of sensor node receiving the data of 1 bit can be described as

$$E_{\text{Rx}}(k) = E_{\text{Rxelec}}(k) = kE_{\text{elec}}. \quad (3)$$

The model includes the energy consumption of transmitting data and receiving data. The consumption of transmitting data includes the energy consumption of radiofrequency circuit and signal amplifier. The consumption of receiving nodes is the energy consumption of receiving circuit. Where ε_{fs} and ε_{mp} are the magnifications of amplifier, E_{elec} denotes the energy consumption of transmitting or receiving 1-bit data.

4. EDEUC Algorithm

The core idea of the algorithm is the mechanism of uneven clustering routing which is introduced into the sensor network with heterogeneous energy. The energy factor is introduced to the competition radius of cluster-head, so it can fully make use of the property of heterogeneous energy of the nodes. Before electing the cluster-head of the nodes, the number of the competition cluster-heads can be restrained by electing the candidates of cluster-head, and then the final nodes of cluster-head will be elected from these candidate cluster-heads. The next routing nodes can be chosen by considering energies of nodes and the transmitting distances in the process of data transferring comprehensively.

4.1. Election of Candidate Cluster-Heads. In the time of network running, all the nodes in the network will participate in the competition to become the candidate cluster-heads. Every node S_i ($i = 1, 2, \dots, N$) will produce a random number $\mu \in (0, 1)$. If μ is less than the threshold $T(S_i)$, the relevant node will be the candidate cluster-head, and it is expressed as formula (4). In order to fully make use of the property of heterogeneous energy of nodes, the factor of residual energy of node S_i is introduced into weighting probability of the competition of cluster-heads. It is expressed as formula (5). k_{opt} is introduced into threshold $T(S_i)$ for candidate cluster-heads in the election mechanism. k_{opt} is the optimal cluster number of the network: $k_{\text{opt}} = \sqrt{N/2\pi} \cdot \sqrt{\varepsilon_{\text{fs}}/\varepsilon_{\text{mp}}} \cdot (M/d_{\text{toBS}}^2)$, where d_{toBS} is the distance between the node S_i and base station. This will cause the threshold to become larger, and it will ensure that more nodes have the opportunity to become the candidate cluster-heads. The node sets of candidate cluster-head can be denoted as $S_i \cdot S_{\text{ch}}$:

$$S_i \cdot S_{\text{ch}} = \{S_j \text{ is the candidate cluster-head} \mid S_j \cdot \mu \in (0, 1) < T(S_j)\}. \quad (4)$$

$S_j \cdot \mu$ is the random number produced by node S_j . $T(S_j)$ is the threshold of candidate cluster-head of node S_j accordingly. The average probability for node S_i becoming cluster-head can be calculated as in the following formula:

$$p(S_i) = \frac{p_{\text{opt}} \cdot N \cdot (1 + \alpha_i)}{N + \sum_{i=1}^N \alpha_i} \cdot \frac{E_i(r)}{E_{\text{ave}}(r)}, \quad (5)$$

where $p_{\text{opt}} = k_{\text{opt}}/N$ is the ratio of the optimal cluster-head number for the network, $E_i(r)$ is the residual energy of the node currently, and $E_{\text{ave}}(r)$ is the average residual energy for all the nodes of the network in the r round currently. In this algorithm, the threshold $T(S_i)$ is denoted as in the following formula:

$$T(S_i) = \begin{cases} \frac{p(S_i)}{1 - p(S_i) \cdot (r \cdot \text{mod}(1/p(S_i)))} \cdot k_{\text{opt}}, & S_i \in G \\ 0, & \text{the other,} \end{cases} \quad (6)$$

where $p(S_i)$ is the probability of the node becoming the candidate cluster-head, r is the round currently, $r \cdot \text{mod}(1/p(S_i))$ is the number of the nodes to ever become the candidate cluster-head in this round, and G is the set of the nodes not to become the candidate cluster-head in this round.

4.2. Competition Radius of Candidate Cluster-Head. In order to achieve uneven clustering in the network, the method of designing different competition radius of candidate cluster-head is adopted. However, this traditional method only considers the distance factor among the nodes in the design of cluster-head competition radius, and the energy factor is not considered in the process. For the sensor network with heterogeneous energy, the node with higher residual energy should have larger communication radius, so the energy of nodes could be balanced like this. In order to solve the problem of ‘‘hotspots’’ in sensor network, the factors of energy and distance should be considered comprehensively in the calculation of cluster-head radius. The candidate cluster-heads calculate the cluster-head radius by formula (7) according to their residual energy and the distance between themselves and the base station.

$$R_{c_i} = \left[1 - p_1 \left(\frac{d_{\text{max}} - d(c_i, \text{BS})}{d_{\text{max}} - d_{\text{min}}} \right) - p_2 \left(1 - \frac{E_{c_i}}{E_{\text{ave}}} \right) \right] R_c, \quad (7)$$

where p_1 and p_2 are the regulative parameters of distance and energy, respectively, and they are in the range of (0,1). d_{max} is the farthest distance from the candidate cluster-head to the base station, and d_{min} is the shortest distance from the candidate cluster-head to the base station. E_{ave} is the average residual energy of all the candidate cluster-heads. E_{c_i} is the residual energy of the candidate cluster-head currently. R_c is the maximal competition radius of the candidate cluster-heads. $d(c_i, \text{BS})$ is the distance from candidate cluster-head c_i to base station. From formula (7), we know that the greater the residual energy of the candidate cluster-heads is, the larger the competition radius of the cluster-heads will be. The closer the distance from the candidate cluster-heads to the base station is, the smaller the competition radius of candidate cluster-head will be.

4.3. Election of Cluster-Head. After electing the candidate cluster-heads, these candidate cluster-heads will broadcast

the information (COMPETE_HEAD_MSG) of competing cluster-head in the range of their radius of cluster-head competition. The content of the information includes the node ID and the current residual energy E_i . The candidate cluster-heads begin to compete with the cluster-head by different starting time (T_{c_i}). Energy factor is mainly considered in this kind of election system. If a candidate cluster-head has a shorter starting time to elect the cluster-head, this means it will have higher priority to become the cluster-head. If the time at which the candidate cluster-head starts to elect is longer than the latest time of starting to elect the cluster-head preset by the system, the candidate cluster-head will not be the cluster-head. The time (T_{c_i}) at which the candidate cluster-head starts to elect the cluster-head can be calculated as follows:

$$T_{c_i} = \frac{E_{\text{ave}}(E_{\text{max}} - E_i)}{E_i(E_{\text{max}} - E_{\text{ave}})} \cdot T_c, \quad (8)$$

where E_{max} is the largest initial energy of the candidate cluster-head, E_i is the current residual energy of the node, and T_c is the latest time of starting to elect cluster-head preset by the system.

4.4. Data Transmission Mode. After setting up the cluster, it should enter the phase of data transferring. The mixed multihop transferring mode should be adopted between cluster-head and base station. The transmission mode of multihop may share the energy consumption with multiclusters rather than concentrating on one cluster. It can balance the energy consumption of clusters effectively. Suppose that the cluster-head c_i indirectly sends data to base station via the relay cluster-head c_j ; the set of routing nodes where the cluster-head c_i will choose the next hop can be expressed as $c_i \cdot R_{\text{ch}}$:

$$c_i \cdot R_{\text{ch}} = \left\{ c_j \mid d^2(c_j, \text{BS}) \leq d^2(c_i, \text{BS}) \cup \left(d^2(c_j, \text{BS}) + d^2(c_i, c_j) \right) < d^2(c_i, \text{BS}) \right\}, \quad (9)$$

where $d(c_i, \text{BS})$ is the distance from the cluster-head c_i to base station BS, $d(c_j, \text{BS})$ is the distance from relay cluster-head c_j to base station, and $d(c_i, c_j)$ is the distance from the cluster-head c_i to the relay cluster-head c_j . If the set $c_i \cdot R_{\text{ch}}$ is an empty set, this indicates that the cluster-head c_i has no appropriate relay routing nodes for the next hop, and the cluster-head c_i will directly communicate with the base station. If the set $c_i \cdot R_{\text{ch}}$ is not an empty set, this means that there exist relay routing nodes for the next hop. The cluster-head c_i will choose the appropriate relay routing node from the set according to the parameter weight W_j . The residual energy of the nodes and distance among the cluster-heads will be considered comprehensively in this process.

Definition 1. The distance factor $D_{c_i, \text{BS}}$ is introduced to the mechanism of choosing the routing nodes for the next hop by cluster-head c_i . It can be described as in the following formula:

$$D_{c_i, \text{BS}} = \left(d^2(c_i, c_j) + d^2(c_j, \text{BS}) \right) \times e^{-E_{c_j}/E_{\text{ave}}}, \quad (10)$$

where E_{c_j} is the current residual energy of relay cluster-head c_j and E_{ave} is the current average residual energy of the whole network.

In the mechanism of choosing the relay cluster-heads, the distance factor $D_{c_i,BS}$ will mainly consider two aspects: energy and distance; that is to say, the path and energy consumption for sending data by cluster-head c_i should be considered comprehensively. If we only consider the distance factor for the next-hop routing, we cannot elect the appropriate routing path roundly. The energy factor of all the cluster-heads should be considered sufficiently in this process.

Definition 2. The energy balance factor m_{c_i} is introduced to the process of choosing relay cluster-head c_j by the cluster-head c_i according to its own residual energy. The value of m_{c_i} can be expressed as in the following formula:

$$m_{c_i} = \begin{cases} d^2(c_i, c_j), & E_{c_i} \leq E_{c_j,ave} \\ 0, & E_{c_i} > E_{c_j,ave}, \end{cases} \quad (11)$$

where $E_{c_j,ave}$ is the average residual energy of candidate relay cluster-head c_j .

From formula (11), we know that when the residual energy of current cluster-head c_i is larger than the average residual energy of candidate relay cluster-head c_j , we shall not worry too much about the problem of excessive energy consumption of cluster-head c_i . On the contrary, when the surplus energy of cluster-head c_i is smaller, the factor of distance between cluster-heads c_i and c_j should be fully considered in the election of relay cluster-head. Therefore, in order to reduce the energy consumption of the source cluster-head, the transmission distance $d^2(c_i, c_j)$ between cluster-heads c_i and c_j can be introduced to restrain the election of relay cluster-head.

Definition 3. The energy balance factor m_{c_j} is introduced to the process of electing the relay cluster-head by the candidate relay cluster-head c_j according to its own residual energy. The value of m_{c_j} can be expressed as in the following formula:

$$m_{c_j} = \begin{cases} K, & E_{c_j} \leq E_{c_j,ave} \\ 0, & E_{c_j} > E_{c_j,ave}, \end{cases} \quad (12)$$

where K is a constant. From formula (12), we know that when the residual energy of relay cluster-head c_j is larger, the cluster-head will take on more responsibility in the process of forwarding data. It can avoid the energy being exhausted with taking on the task of forwarding data for the cluster-heads with less residual energy. The energy balance factor m_{c_j} is just introduced to constrain the cluster-heads with lower energy to become the next-hop routing nodes.

Definition 4. On the base of Definition 1 to Definition 3, the parameter weight w_j is introduced to the process of choosing the relay cluster-head c_j from the cluster-head c_i . This weight

TABLE 1: Simulation parameters.

Parameters	Values	Parameters	Values
E_{elec}	50 nJ/bit	ϵ_{fs}	10 pJ/bit/m ²
E_{DA}	5 nJ/bit/message	ϵ_{mp}	0.0013 pJ/bit/m ⁴
E_0	0.5 J	Message size	40000 bits
p	0.1	n	100

considers the relationship of distance factor and energy factor comprehensively. It can be expressed as in the following formula:

$$w_j = pD_{i,BS} + q(m_{c_i} + m_{c_j}), \quad (13)$$

where $D_{i,BS}$ is the factor of distance from the cluster-head c_i to base station, m_{c_i} is the energy balance factor of the cluster-head c_i , m_{c_j} is the residual energy balance factor of the relay cluster-head c_j , p and q are the weight regulation parameters, and $p + q = 1$.

The cluster-head c_i can calculate the weight w_j of candidate relay cluster-heads in the set of $c_i \cdot R_{ch}$ by formula (13). The next-hop relay routing nodes can be chosen in the relay cluster-heads according to the size of the weights. The election law of relay cluster-head is that the smallest of the parameter weights w_j of the cluster-head will be the next-hop routing nodes. In order to reduce the energy consumption of storing information in the node, there are only 3 pieces of routing information stored in the routing table of cluster-head c_i . The routing information in the routing table is stored according to the sequence from the small weight to the large weight. The cluster-head with the smallest weight will be the first routing choice.

5. Simulation Results and Performance Analysis

5.1. Simulation Environment. In order to test and verify the energy saving performance and balance performance of energy loss, EDEUC was compared with some widely used algorithms: SEP and DEEC in this experiment. The simulation environment settings are as follows: supposing 100 nodes with heterogeneous energies are distributed in the square area ($(x = 0, y = 0), (x = 100, y = 100)$) randomly. The base station locates in the point of $(x = 50, y = 150)$. Suppose m , which is the proportion of the nodes with advanced energies to all the nodes, is 0.5. In the heterogeneous network, $E_0 = 0.5J$, $\alpha_{max} = 1$, the nodes of the sensor network are distributed in the closed interval $[E_0, (1 + E_0)]$ randomly, so we can get the initial energy interval of the nodes: $[0.5, 1]$. The other parameters of the simulation environment are listed in Table 1.

p is the proportion of optimizing clusters, E_{DA} is the energy consumption of data fusion by cluster-head, and n is the number of the nodes. These parameters above should be used in the evaluation of energy consumption. Besides these, there are other parameters that need to be configured;

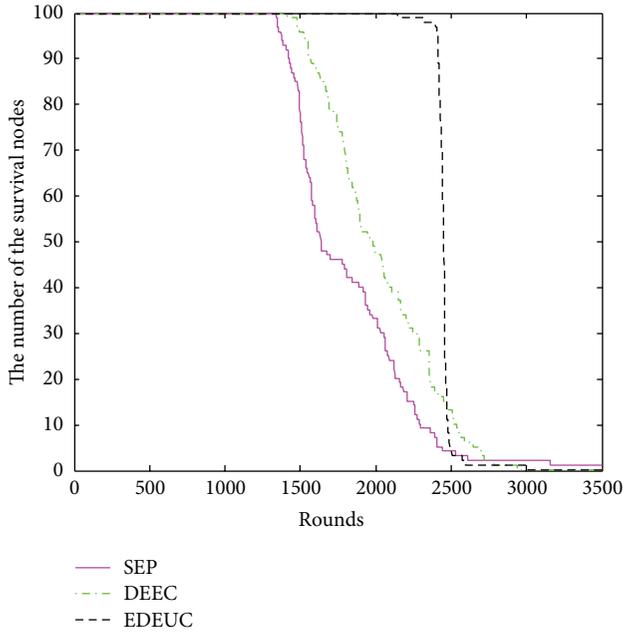


FIGURE 1: The number of survival nodes changes with rounds updating.

for example, p_1 and p_2 can be used to control the size of competition radius of cluster-head and R_c is the largest competition radius of cluster-head. After lots of testing and simulation, the values can be set up as follows: $R_c = 60$ m, $p_1 = 0.3$, and $p_2 = 0.2$. The regulation parameters of distance and energy in the multihop transmission mechanism are set up as $p = 0.6$ and $q = 0.4$.

5.2. Experimental Results and Analysis. The network life cycle is an important index of the performance evaluation for a routing algorithm. Figure 1 indicates the changes of number of the live nodes in the network with rounds updating.

Figure 1 illustrates that the first dead node in EDEUC algorithm can last more rounds than others, so this indicates that EDEUC algorithm has a longer stable life cycle than the others. The first dead node of SEP, DEEC, and EDEUC has died in the round of 1444, 1586, and 2256, respectively. DEEC algorithm has improved by 9.8% compared to DEEC, and EDEUC has improved by 42.2% compared to DEEC. EDEUC has a relative small time span while the network is dying, which is because EDEUC algorithm considers the factors of the residual energy of nodes and the distance of communication, and the proportionality of energy consumption is better than the others. Due to the introduction of the mechanism of uneven clustering to the EDEUC algorithm, the cluster-head can fully make use of the feature of heterogeneous energy of the nodes in the stage of cluster-head structuring and data transferring. It can balance the energy consumption of cluster-head and extend the life cycle of the network effectively.

Figure 2 illustrates that different value assigned to the parameter weight of competition radius of cluster-head will influence the life cycle. When (p_1, p_2) is assigned with

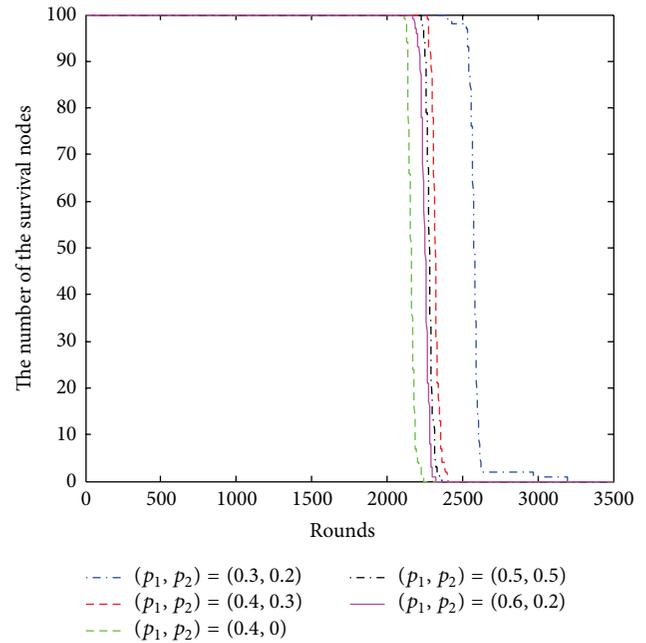


FIGURE 2: Different value assigned to p_1 and p_2 influences the life cycle of the network.

(0.4, 0), this means we only consider the communication distance of the nodes in the process of determining the competition radius of cluster-head and ignore the factor of residual energies. The other assignments of the parameters will optimize the situation of choosing competition radius of cluster-head. Figure 2 illustrates that the life cycle of network will be the shortest one if we do not optimize the competition radius of cluster-head. That is to say, the communication distance and the residual energy of the node should be both considered when we determine the competition radius of cluster-head. When (p_1, p_2) is with the value of (0.3, 0.2), the life cycle of the network will be the longest compared to the other cases. In other cases for (p_1, p_2) , life cycles of the network have relative closer results. So it is reasonable that (p_1, p_2) should be chosen as (0.3, 0.2) in the several groups of data above.

EDEUC method adopts the hybrid multihop transmission mechanism. It can reduce the energy consumption of data transmission for cluster-heads. In order to verify the advantages of energy consumption of cluster-heads, we chose 10 rounds of data randomly in the process of network running and compare the results of energy consumption with DEEC and SEP methods. Figure 3 illustrates the volume of energy consumption of cluster-heads for these three kinds of methods.

Figure 3 illustrates that the energy consumption of cluster-head by using EDEUC method is obviously lower than the energy consumption of cluster-head by using DEEC and SEP methods, and the energy consumption of cluster-head by using SEP method is the largest compared to others. EDEUC method improves two aspects, choice of cluster-head and data transmission, and its multihop transmission mechanism can effectively reduce energy consumption of

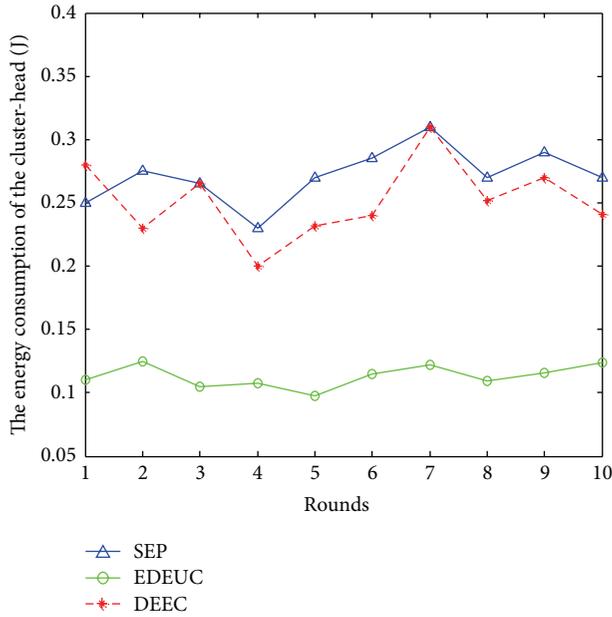


FIGURE 3: The sum of the energy consumption of cluster-heads.

cluster-heads. EDEUC is proposed as a kind of uneven clustering routing algorithm based on the characters of nodes with heterogeneous energies. The residual energy and the distance of transmission data of the nodes are both considered comprehensively in the mechanism of choosing cluster-head and data transferring, so the distribution of cluster-head nodes is more reasonable. This can effectively prevent the occurring of network “hotspots.” The energy consumption of cluster-head by using EDEUC algorithm has better performance than the other two algorithms.

Figure 4 illustrates the analysis results of the algorithm performance from the view of residual energy of the network. The residual energy of network can impliedly indicate the performance of life cycle and the energy consumption of the network. The more residual energy the network has, the less the energy consumption of the network is and the longer the life cycle of the network will be.

Figure 4 also illustrates that the residual energy of the network by using SEP or DEEC algorithm is less than by using EDEUC algorithm in most time stages. Along with the network operation to late stage (after 1000 rounds), the residual energy of network by using EDEUC algorithm is more than the others. So the performance of the two aspects regarding the node energy utilization and the balance of network’s energy consumption is better than the other two algorithms.

Figure 5 illustrates the data volume of network transferring by these three algorithms. It is clear that not only does EDEUC algorithm have better performance of the balance of network energy consumption than the others, but also it can have the network transfer more data volumes to base station. Lower energy consumption of network is in favor of prolonging the lifetime of the network, so the network could keep sending more data in the longer period of time, and

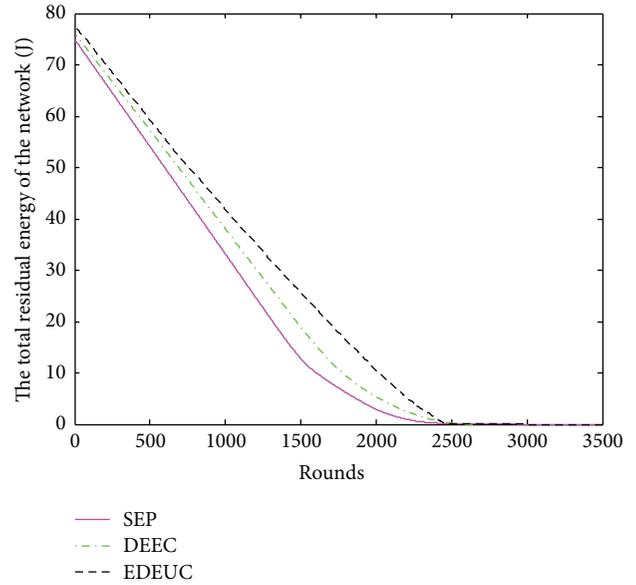


FIGURE 4: The residual energy of the network changes over time.

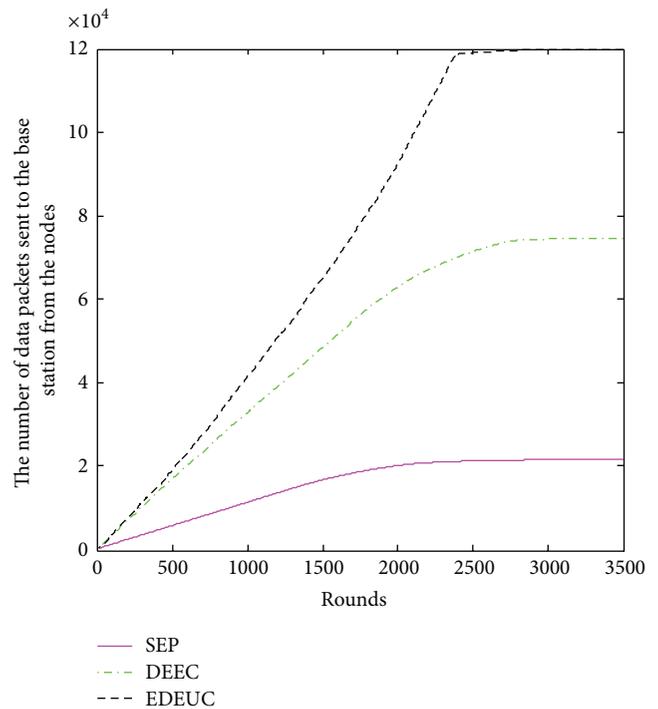


FIGURE 5: The amount of data received by base station with rounds updating.

the amount of data received by base station will be bound to increase.

In order to clearly observe the amount of data transferred by using these different algorithms, we choose four stages of network running time to compare them to each other in the experiments. In the horizontal ordinate of Figure 6, the four stages are the round of 1000, 1500, 2000, and 2500, respectively. We can compare these total data volumes of the four

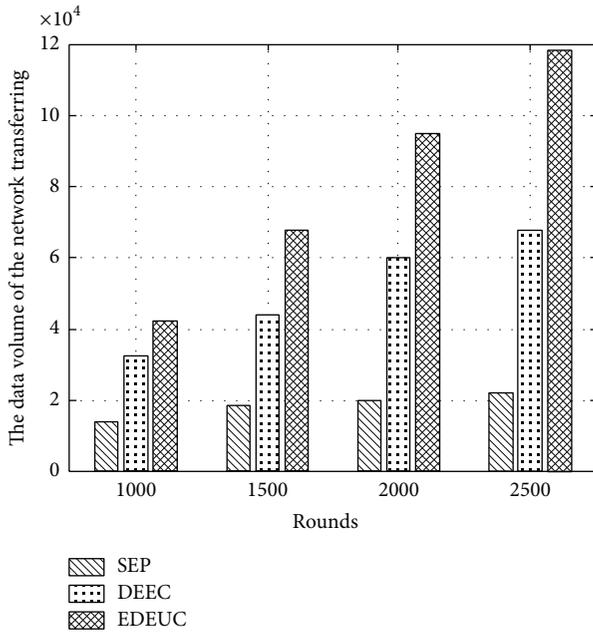


FIGURE 6: Columnar contrast figure of the amount of data transferred by network with different algorithms.

states as columnar contrast figure visually in Figure 6. When the network running time reaches 2000 rounds, the network can transfer more data volumes by using EDEUC algorithm, and it can improve by 380% and 75% compared with SEP and DEEC algorithms, respectively. After 2000 rounds, the data volume transferred by SEP algorithm increases less, and the total data volume transferred by network tends to have stable status. But, for the other two algorithms, the data volume transferred still increases, and obviously the data volume transferred by using EDEUC algorithm increases more than the others.

6. Conclusion

In order to solve the problem of “hotspots” in sensor networks, a kind of routing algorithm named EDEUC based on energies and distances was proposed by using the idea of uneven clustering. This method adopts double selection mechanism for cluster-heads and optimizes the competition radius of cluster-heads. The hybrid multihop transmission is adopted in the stage of data transferring. The simulation result indicates that this kind of uneven clustering mechanism and the optimizing for competition radius of cluster-heads can obviously improve the transmission performance of the network and enhance the life cycle of the network effectively.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (nos. 61273068, 61673259, and 61373028) and the International Exchanges and Cooperation Projects of Shanghai Science and Technology Committee (no. 15220721800).

References

- [1] A. A. Abbasi and M. Younis, “A survey on clustering algorithms for wireless sensor networks,” *Computer Communications*, vol. 30, no. 14-15, pp. 2826–2841, 2007.
- [2] S. P. Singh and S. C. Sharma, “A survey on cluster based routing protocols in wireless sensor networks,” *Procedia Computer Science*, vol. 45, pp. 687–695, 2015.
- [3] A. N. Knaian, “A wireless sensor network for smart roadbeds and intelligent transportation systems,” Tech. Rep., Electrical Science and Engineering, Massachusetts Institute of Technology, 2000.
- [4] Y. Liang and R. Liu, “Routing topology inference for wireless sensor networks,” *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 1, pp. 21–28, 2013.
- [5] Z. Zhou, B. Yao, R. Xing, L. Shu, and S. Bu, “E-CARP: an energy efficient routing protocol for UWSNs in the internet of underwater things,” *IEEE Sensors Journal*, vol. 16, no. 11, pp. 4072–4082, 2015.
- [6] N. Javaid, M. R. Jafri, Z. A. Khan, N. Alrajeh, M. Imran, and A. Vasilakos, “Chain-Based communication in cylindrical underwater wireless sensor networks,” *Sensors*, vol. 15, no. 2, pp. 3625–3649, 2015.
- [7] I. Nevat, G. W. Peters, F. Septier, and T. Matsui, “Estimation of spatially correlated random fields in heterogeneous wireless sensor networks,” *IEEE Transactions on Signal Processing*, vol. 63, no. 10, pp. 2597–2609, 2015.
- [8] S. Dehghani, M. Pourzaferani, and B. Barekatain, “Comparison on energy-efficient cluster based routing algorithms in wireless sensor network,” *Procedia Computer Science*, vol. 72, pp. 535–542, 2015.
- [9] A. Chamam and S. Pierre, “A distributed energy-efficient clustering protocol for wireless sensor networks,” *Computers and Electrical Engineering*, vol. 36, no. 2, pp. 303–312, 2010.
- [10] M. Azharuddin, P. Kuila, and P. K. Jana, “Energy efficient fault tolerant clustering and routing algorithms for wireless sensor networks,” *Computers & Electrical Engineering*, vol. 41, pp. 177–190, 2015.
- [11] S. Soro and W. B. Heinzelman, “Prolonging the lifetime of wireless sensor networks via unequal clustering,” in *Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS '05)*, pp. 1–8, Denver, Colo, USA, April 2005.
- [12] T. C. Karalar, S. Yamashita, M. Sheets, and J. Rabaey, “A low power localization architecture and system for wireless sensor networks,” in *Proceedings of the IEEE Workshop on Signal Processing Systems Design and Implementation*, pp. 89–94, Piscataway, NJ, USA, October 2004.
- [13] H. Xia, R.-H. Zhang, J. Yu, and Z.-K. Pan, “Energy-efficient routing algorithm based on unequal clustering and connected graph in wireless sensor networks,” *International Journal of Wireless Information Networks*, vol. 23, no. 2, pp. 141–150, 2016.

- [14] W. Heinzelman, A. Chandrakasan, and H. Balakrishman, "Energy-efficient communication protocol for wireless micro-sensor networks," in *Proceedings of the 33rd Hawaii International Conference on System Science*, pp. 3005–3014, Maui, Hawaii, USA, January 2000.
- [15] S. Tyagi and N. Kumar, "A systematic review on clustering and routing techniques based upon LEACH protocol for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 36, no. 2, pp. 623–645, 2013.
- [16] S. Lindsey and C. S. Raghavendra, "PEGASIS: power-efficient gathering in sensor information systems," in *Proceedings of the IEEE Aerospace Conference*, pp. 1125–1130, March 2002.
- [17] O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE Transactions on Mobile Computing*, vol. 3, no. 4, pp. 366–379, 2004.
- [18] B. A. Attea and E. A. Khalil, "A new evolutionary based routing protocol for clustered heterogeneous wireless sensor networks," *Applied Soft Computing Journal*, vol. 12, no. 7, pp. 1950–1957, 2012.
- [19] J. Yu, Y. Qi, G. Wang, and X. Gu, "A cluster-based routing protocol for wireless sensor networks with nonuniform node distribution," *AEU—International Journal of Electronics and Communications*, vol. 66, no. 1, pp. 54–61, 2012.
- [20] T. Voigt, A. Dunkels, J. Alonso et al., "Solar-aware clustering in wireless sensor networks," in *Proceedings of the 9th International Symposium on Computers and Communications (ISCC '04)*, vol. 1, pp. 238–243, July 2004.
- [21] L. S. Jayashree, S. Arumugam, and N. Rajathi, "E/sup 2/LBC: an energy efficient load balanced clustering technique for heterogeneous wireless sensor networks," in *Proceedings of the IFIP International Conference on Wireless and Optical Communications Networks*, pp. 1–7, IEEE, Bangalore, India, April 2006.
- [22] G. Smaragdakis, I. Matta, and A. Bestavros, *SEP: A Stable Election Protocol for Clustered Heterogeneous Wireless Sensor Networks*, Computer Science Department, Boston University, Boston, Mass, USA, 2004.
- [23] L. Qing, Q. Zhu, and A. Wang, "A distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks," *Journal of Software*, vol. 17, no. 3, pp. 481–489, 2006.
- [24] H.-B. Cai, X.-M. Ju, and Q.-Y. Cao, "Energy prediction and reliable clustering routing protocol for multilevel energy heterogeneous wireless sensor networks," *Chinese Journal of Computers*, vol. 32, no. 12, pp. 2393–2402, 2009.
- [25] X. Wang, G. Zhang, and X. Xie, "A load balance clustering algorithm for multilevel energy heterogeneous wireless sensor networks," *Journal of Computer Research and Development*, vol. 45, no. 3, pp. 392–399, 2008.
- [26] Y. Liang, "An optimized clustering algorithm for energy heterogeneous wireless sensor networks," *Transactions of Shenyang Ligong University*, vol. 28, no. 2, pp. 57–61, 2009.
- [27] C.-F. Li, G.-H. Chen, M. Ye, and J. Wu, "Uneven cluster-based routing protocol for wireless sensor networks," *Chinese Journal of Computers*, vol. 30, no. 1, pp. 27–36, 2007.

Research Article

Low Complexity Signed Response Based Sybil Attack Detection Mechanism in Wireless Sensor Networks

M. Saud Khan¹ and Noor M. Khan²

¹Department of Computer Science, Capital University of Science and Technology, Islamabad 44000, Pakistan

²Department of Electrical Engineering, Capital University of Science and Technology, Islamabad 44000, Pakistan

Correspondence should be addressed to M. Saud Khan; saud@ciit.net.pk

Received 23 December 2015; Revised 9 May 2016; Accepted 13 July 2016

Academic Editor: Guiyun Tian

Copyright © 2016 M. Saud Khan and N. M. Khan. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Security is always a major concern in wireless sensor networks (WSNs). Identity based attacks such as spoofing and sybil not only compromise the network but also slow down its performance. This paper proposes a low complexity sybil attack detection scheme, that is, based on signed response (SRES) authentication mechanism developed for Global System for Mobile (GSM) communications. A probabilistic model is presented which analyzes the proposed authentication mechanism for its probability of sybil attack. The paper also presents a simulation based comparative analysis of the existing sybil attack schemes with respect to the proposed scheme. It is observed that the proposed sybil detection scheme exhibits lesser computational cost and power consumption as compared to the existing schemes for the same sybil detection performance.

1. Overview and Related Work

Introduction. The wireless sensor networks have been widely applied in various fields in order to monitor the physical world like harvesting, battle field, habitat monitoring, and so forth. The scope of this deployment gets increased day by day due to its low cost, large scaled deployment, and self-configuration nature [1–4]. The existing designs of application for wireless sensors allow a better flexibility in terms of communication and exchange of data but are also establishing communications and increasing system automation, but also the WSNs are lacking security and privacy [3, 5, 6]. The inadequate battery life and communication and processing resources are the main limitation of a sensor node [7]. Due to these reasons, a sensor network becomes vulnerable to different threats which can lead an attacker to access secret information [8]. Sybil attack is one of the most widely launched attacks in wireless sensor networks. The sybil attack is considered very easy to be launched because of the open and broadcast nature of the wireless sensor network. In such attacks, the sybil node creates multiple identities at different locations deceiving the cluster heads (CHs) or the other nodes of the network and tries to become part of the

network. The current mechanisms to detect sybil attacks are mainly based upon centralized and decentralized approaches. In centralized approach, a central entity is responsible for determining the attack and pointing out the attacking node where, as in decentralized approach, a distributed approach is used for this purpose. In [9], the authors proposed an attack detection model for sybil attacks based on RSSI. According to the authors, the model does not require any extra resources like third party or antennas and also the mobility of nodes is supported by the model. One of the implemented solutions is certification of the nodes [10]. This mechanism requires the presence of trusted and authorized third party for the validation of participating entities. The authors in [11] proposed a solution for sybil attacks based upon social networks known as sybil control which is an admission based control designed for distributed WSN. The proposed solution is basically a protocol in which a node calculates the computational work done by the other respective nodes in order to detect a malicious or misbehaving node present in the network. According to the authors, a malicious or attacking node does not have the capability to calculate the computational work of other nodes properly. Similarly, another protocol known as Gatekeeper [12] which is a decentralized admission

control protocol is also based on social network approach. Another RSSI based solution is proposed in [13]. The authors used K -means algorithm for the detection of attacking node. According to the authors, the proposed solution can also detect the location of attacking node and is enough robust to handle the variable transmission power level of attacking nodes. The RSSI based solutions are considered to be lighter in overhead since only one message is communicated but, on the other hand, RSSI being a time varying and unreliable parameter exhibits nonisotropic behavior most of the time. In [14, 15], a ranging method based approach is proposed for sybil attack detection. However, range-based algorithms involve the distance estimations by using the measurement of various physical properties of signal such as RSSI, time of arrival (TOA), and time difference of arrival (TDOA). In [16], a scheme for the detection of sybil attack is proposed on the basis of radio resource testing and registration but such approaches use high power and violate the limitation of battery power consumption. In [17, 18], the authors use Gaussian mixture model to read RSSI readings but the paper does not clearly explain how the sybil attacks are localized. In [19], the authors proposed a defense mechanism for sybil attacks based upon various resource testing like radio resource testing, position verification and registration, and so forth. In [20], a hop-by-hop authentication procedure is proposed. The authors in [21] proposed a key management mechanism that refreshes all authentication keys in order to protect them from being compromised. The authors in [22] proposed a framework, that is, performed by cluster heads in hierarchical WSN.

Problem Statement and Proposed Solution. As discussed earlier, almost every existing protocol proposed for the detection of location based attacks (like sybil attack) in sensor networks focused only on security and protection from attacks neglecting the effect of its computational complexity on the resource-constrained and bottleneck parameters like power consumption, processing capability, traffic intensity, and message latency. These parameters may lead the network towards poor performance if not handled properly. In this paper, we propose an algorithm to protect the sensor network from location based attacks like spoofing attack and sybil and so forth. The scope of this work is intentionally made limited to sybil attack in order to extend simplicity for the reader. The proposed authentication scheme is inherited from the SRES (signed response) authentication mechanism used in second-generation cellular mobile communication system, the Global System for Mobile (GSM) communication [23]. The SRES mechanism is responsible for authenticating the user and encrypting the voice data. In order to implement the SRES in WSNs, we modified the original scheme to fit it into ad hoc scenario. Simulations are performed to validate the performance of the proposed algorithm in MATLAB®. From the simulation results, we prove that the proposed scheme not only is enough efficient to detect the sybil attack but also requires lesser processing and battery power as compared to notable existing authentication schemes. Moreover, the scheme creates little message overhead resulting in negligible

increase in the traffic of the network. In order to prove the efficiency, comparison of the proposed algorithm is carried out with two notable attack detection and authentication schemes, that is, Detecting and Locating Location Based Attack Detection (LBAD) in wireless sensor networks [13] and Lightweight Sybil Attack Detection (LwSAD) in MANETs [9]. Both the schemes are evaluated over probability, processing overhead, and power consumption.

The rest of the paper is organized as follows.

Section 2 explains the procedure of authentication in GSM technology. Section 3 discusses the proposed attack model and defense strategy, respectively. The simulation results and performance comparison are discussed in Section 4 followed by conclusions in Section 5.

2. Working of Authentication Algorithms in GSM

The signed response procedure is originally designed for second-generation GSM based networks. This mechanism is responsible for handset authentication to the network. The A3 algorithm is used to produce a response against the challenge (SRES) as elaborated in Figure 1. The Subscriber Identity Module (SIM) also contains the ciphering key generating algorithm (A8 algorithm). The A8 algorithm is used to calculate the 64-bit ciphering key (K_c) which is used to encrypt the voice data before it is sent over the channel. The ciphering algorithm A5 is used to authenticate and ensure the secure communication between the mobile station (MS) and the network. The GSM network initiates a request and sends to mobile station over the channel. The A3 algorithm which is embedded in the handset is responsible for generating the signed response (SRES). The block diagram of A3 algorithm is shown in Figure 2 which involves the process of creating a 32-bit signed response from 128-bit key (RAND). The detailed step-by-step procedure of mobile authentication and voice encryption in GSM is given below:

- (1) The mobile station (MS) initiates process to sign in to the network.
- (2) A request for 5 triples to Mobile Services Switching Center (MSC) is forwarded from the Home Location Register (HLR).
- (3) With the help of A8 algorithm, the five triples are created by Home Location Register and sent to MSC comprising the following main components:
 - (i) 128-bit random challenge (RAND).
 - (ii) 32-bit matching SRES.
 - (iii) 64-bit ciphering key used as a Session Key (K_c).
- (4) From the first triple, a random challenge is sent to Base Transceiver Station (BTS) from the Mobile Services Switching Center. The BTS then forwards the challenge to mobile station.

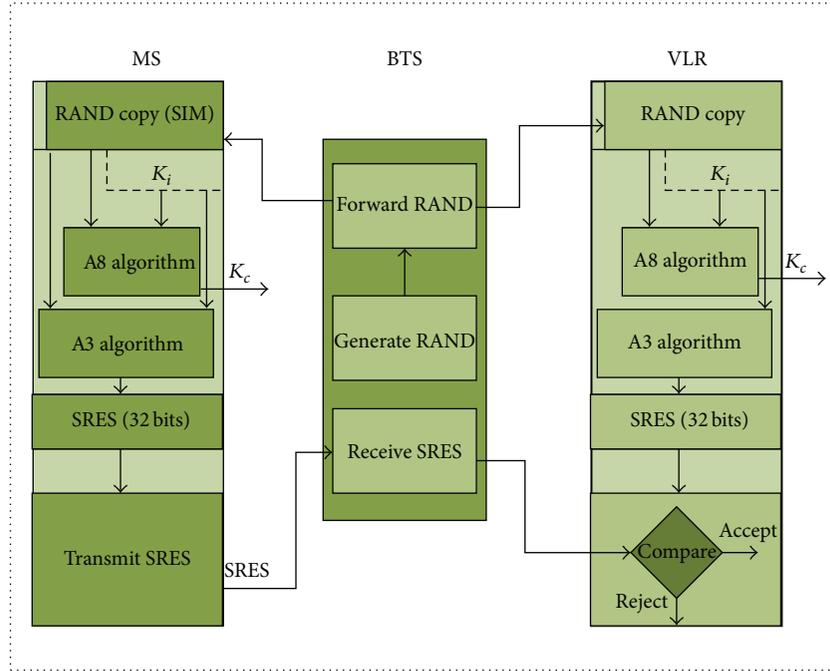


FIGURE 1: Authentication process in GSM.

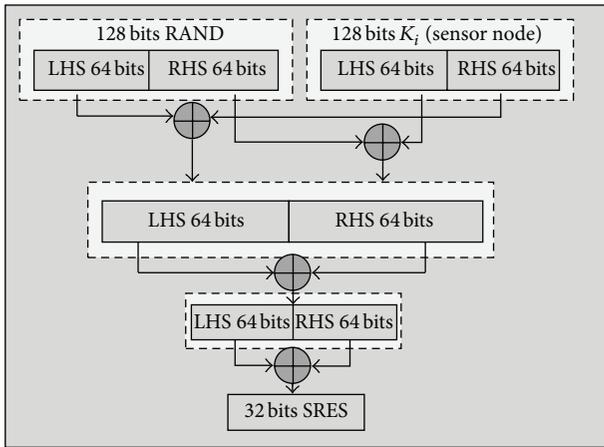


FIGURE 2: Block diagram of A3 algorithm generating 32-bit SRES.

- (5) After receiving the challenge from BTS, the mobile station starts the process of encryption with authentication key K_i assigned to it. The encryption process is carried out with the help of A3 algorithm.
- (6) Mobile station creates a SRES and sends to the BTS.
- (7) The Base Transceiver Station forwards the SRES to the Mobile Services Switching Center.
- (8) The SRES is verified by Mobile Services Switching Center.

The use of A8 algorithm for session creation by a mobile station is not discussed in this section since it does not come in our scope.

3. Low Complexity Signed Response Based Sybil Attack Detection Mechanism

3.1. Network Model and Assumptions. Figure 3 illustrates a distributed network with hierarchical structure having cluster heads (CHs) along with the member sensor nodes. We assume that the CH is a powerful node that may become a sink in case of a centralized network. The sybil nodes S are assumed to be present in the network and they have the complete information of security mechanism of the network. The CH is responsible for monitoring the behavior of sensor nodes in its vicinity and ensuring that there is no attacker or sybil node. The CH sends the attack information to the BS or any controlling entity if determined. Although only one BS is shown in Figure 3 but there could be as many BS as required by the network and environment. The deployment of nodes can be aerial or manual depending upon the nature of physical environment. Each sensor node is assigned an ID and the position of the sensor node is assumed to be known to it. We also assume that the sink or cluster head has all the necessary information about member sensor nodes like sensor ID, sensor MAC address, and the assigned authentication key K_i .

3.2. Proposed Methodology. In order to implement the SRES mechanism in WSN, we make necessary modifications in the existing authentication scheme implemented in GSM. The proposed mechanism can also be used both in centralized and in clustered ad hoc environment. In ad hoc mode, a sink is responsible for coordinating with all the nodes in the network whereas, in clustered mode, a cluster head can authenticate the node. Since data encryption is not covered in this paper,

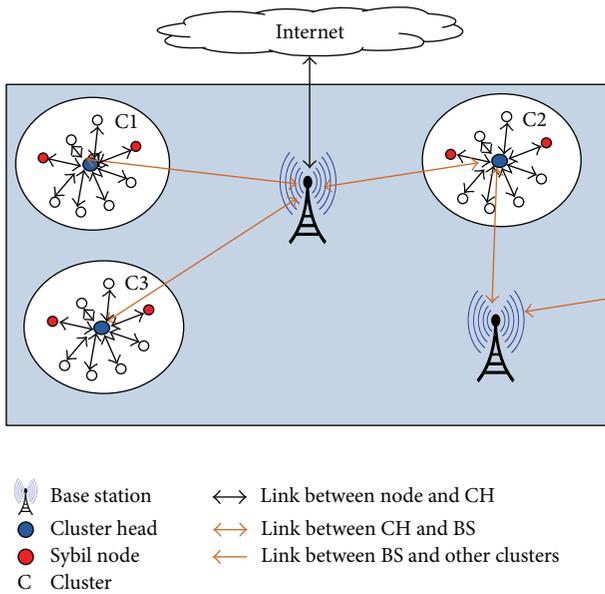


FIGURE 3: An overview of sensor network with sybil nodes.

we will not use the voice encryption algorithm which is also part of the GSM security module. The step-by-step procedure of the proposed algorithm is given below:

- (1) The five triples are generated and provided by the server or cluster head (CH) or sink side. The five triples are comprised of the following:
 - (i) 128-bit random challenge (RAND).
 - (ii) 32-bit matching SRES.
 - (iii) 64-bit ciphering key used as a Session Key (K_c).
- (2) RAND is forwarded to the sensor nodes as a challenge in order to authenticate it.
- (3) This challenge can be sent either as a broadcast if all the nodes need to be authenticated through single challenge number or as a unicast if a specific node is meant to be authenticated.
- (4) Every node has a MAC address and is also provided a preshared key K_i . Thus, a node can produce the SRES with either MAC address or K_i depending upon the implementation.
- (5) The signed response (SRES) can be sent by the node directly to either a server, CH, or SN depending upon the nature of the wireless sensor network.
- (6) The server, CH, or sink verifies the SRES sent by the node and acts accordingly (allowing or disallowing the node).

Figure 4 shows the block diagram of proposed authentication scheme where a sink generates and forwards a challenge to the node(s). The MAC address of each node that can be considered as K_i is required to be registered with the sink or CH. The GSM does not allow a mobile station to authenticate the network. However, in our proposed scheme, we will use

the SRES to authenticate the network by each member node of the network. In order to verify the network, a node N can request the sink or cluster head to resend its already sent SRES to it for confirmation. It means that a node can verify whether it is communicating with the right and authentic network or not. However, this verification can be carried out after a certain number of SRESs have already been generated by the node N . As an extension of this work in the future, we will enable the node to reverse the authentication process without sending any challenge to the network.

3.3. Attack Model and Defense Strategy. In order to launch the attacks and test the efficiency of the proposed scheme, we establish a network of 1000 sensor nodes deployed randomly in an arbitrary area. It is assumed that each node is able to communicate with at least one neighboring node in the network. Since the proposed scheme can work both in centralized and in hierarchical networks, we take both structures on board in our simulations while launching attack and executing defense mechanism. The sybil node present in the network is assumed to be a powerful node with respect to both processing and battery power. A sybil node cannot be registered to the network until it successfully verifies itself as a member sensor node of the network to either the server, CH, or SN. To become a member of the network, the sybil node launches repeated attacks in two ways; it either generates and sends the fake IDs to the respective SN or CH or attempts to steal the ID of a valid member sensor node from the network. If the sybil node with a fake ID achieves success in participating in the network without being identified, we will call it a valid sybil identity. In order to make the situation harder for a sybil node, we will perform validation test. There are two types of validations, direct validation and indirect validation. In direct validation, a node can directly check whether the node in its neighborhood or vicinity is having a valid identity or not based upon the knowledge it possesses. In indirect validation, different nodes can communicate during validating a targeted node so that a globally consistent decision can be made. The indirect validation mechanism is considered to be costly as compared to direct validation because, in the latter case, if a node A having an identity ID_i tries to validate an identity ID_j of a node B , the messages need to be exchanged only between nodes A and B via a single hop, whereas, in the former case, other nodes of the network have to be taken on board for an identity validation. In order to prove the efficiency of the proposed authentication protocol, we evaluate it on both direct and indirect validation processes. To verify a node and its identity in the network through direct validation, the verifier (CH or SN) challenges the identity by sending challenge to the targeted node laying in its one-hop neighborhood. The challenge in our case is a 128-bit random number generated by authenticating party, that is, the server or CH or SN. Upon the reception of challenge number, the targeted node will encrypt it with either its MAC address or K_i with the help of A3 algorithm to generate the SRES. At the same time the authenticating party also calculates the SRES from the random number sent and the same K_i from the database as with the targeted node.

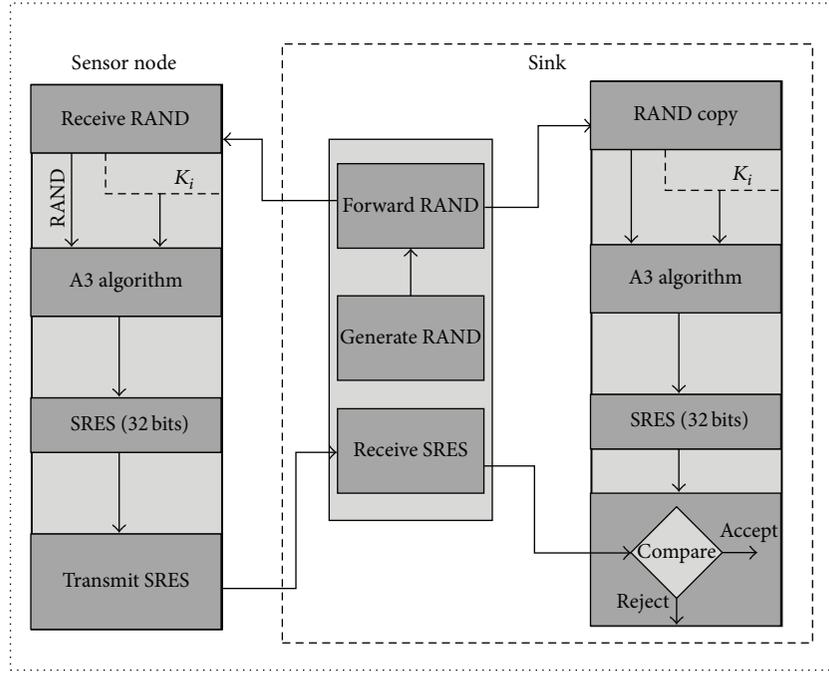


FIGURE 4: Block diagram of the proposed authentication scheme for wireless sensor networks.

When the authenticating party receives the SRES from the targeted node, both the values of SRES are compared. These values must be the same if the node is a valid one; otherwise it will be declared as sybil node. In case of indirect validation, the authenticating node N sends a challenge to a targeted node T which is not in its one-hop neighborhood N . Thus, this challenge has to reach the targeted node in a hop-by-hop manner. Upon the reception of the challenge, the node T will calculate the SRES through A3 algorithm and sends back to node N . The process of calculating the SRES is the same as discussed for direct validation.

The steps involved in the proposed authentication scheme are represented in Algorithm 1. Line (1) generates five vectors of sizes 32, 64, 128, 256, and 512. Note that each value of table T_i ranges from 0 to 2^{4+j-1} , where $j = 1, 2, 5$. In line (4) the sybil node generates and forwards the SRES to the authenticating party through $\Psi_a(T, R_k, \Psi_{r,16}(0 \text{ to } 2^8 - 1))$ whereas the authenticating party validate the SRES received from attacking node through $\Psi_a(T, R_k, K_{i,j})$, where $j = 1$ to Pool Size). Similarly lines (10)–(23) show the step-by-step process of $X \oplus R$ by dividing the RAND and K_i into LHS and RHS to produce the 32-bit SRES.

4. Probabilistic Model of the Proposed Scheme

let the key size be α , and let the pool size in the sink be β .

Consider K_i , where $(1 \leq i \leq n)$ is the predistributed i th key from a vector space $K = K_1, K_2, K_3, \dots, K_n$ of size $n = 2^\alpha$. If the sybil node generates a random key K_a , then the probability of this key being a valid key is

$$P(K_a) = P(K_i) = \frac{1}{|K|}, \quad (1)$$

where $|K|$ is the cardinality of the vector space K . Since $|K| = n$ therefore

$$P(K_i) = \frac{1}{2^\alpha}. \quad (2)$$

This gives us the probability of a randomly generated key to be accepted by the sink. let us suppose that a node uses a pool size of β of predistributed keys, and then S is the subspace of predistributed keys in the pool such that $S \subseteq K$, where $S = \{S_i \in K \mid 1 \leq i \leq \beta\}$. Now, with the probability of any key S_i being in the subspace S , $P(S_i)$ becomes

$$P(S_i) = \beta P(K_i). \quad (3)$$

Probability that a key S_a is being attacked by the sybil node from the pool of β keys is

$$\text{Prob}(S_a) = P(S_i) = P. \quad (4)$$

Suppose that we have M number of sybil nodes attacking on a network. The probability that j attacking sybil nodes are successful out of M nodes is given as

Prob(j sybil nodes are successful out of M nodes)

$$\begin{aligned} &= \binom{M}{j} P^j (1 - P)^{M-j} \\ &= \binom{M}{j} [\beta P(k_i)]^j [1 - \beta P(k_i)]^{M-j} \\ &= \binom{M}{j} \beta^j \frac{1}{2^{\alpha j}} \left[1 - \frac{\beta}{2^\alpha}\right]^{M-j} \end{aligned}$$

```

(1)  $T_{i,1:2^{4+i}} \leftarrow \Psi_r(0 \text{ to } 2^{(4+i-1)} - 1)$ ,  $i \in \{1, 2, 3, 4, 5\}$ 
(2) {Sybel attack}
(3) for 1 to number of attacks do
(4)   if  $\Psi_a(T, R_k, \Psi_{r,16}(0 \text{ to } 2^8 - 1)) = \Psi_a(T, R_k, K_{i,j})$ , where  $j = 1$  to Pool Size then
(5)     useable sybil
(6)   else
(7)     sybel detected
(8)   end if
(9) end for
(10) SRES =  $\Psi_a(T, R_k, K_i)$ 
(11) for  $i \leftarrow 1$  to 8 do
(12)    $X_{1:16} \leftarrow K_i$ 
(13)   for  $j \leftarrow 1$  to 5 do
(14)     for  $l \leftarrow 1$  to  $25 - j$  do
(15)        $m \leftarrow l$ 
(16)        $n \leftarrow m + 25 - j$ 
(17)        $y \leftarrow ((X_m + 2 * X_n) \bmod 29 - j) + 1$ 
(18)        $z \leftarrow ((2 * X_m + X_n) \bmod 29 - j) + 1$ 
(19)        $X_m \leftarrow T_{j,y}$ 
(20)        $X_n \leftarrow T_{j,z}$ 
(21)     end for
(22)   end for
(23) end for
(24) Convert  $X$  to corresponding binary key  $B$ 
(25) Permute  $B$ 
(26) SRES  $\leftarrow B_{1:32}$ 

```

ALGORITHM 1: Algorithm of the proposed authentication scheme.

$$\begin{aligned}
&= \binom{M}{j} \frac{\beta^j}{2^{\alpha j}} \left[\frac{2^\alpha - \beta}{2^{\alpha(m-j)}} \right]^{(M-j)} \\
&= \binom{M}{j} \frac{\beta^j (2^\alpha - \beta)^{M-j}}{2^{\alpha j} \cdot 2^{\alpha M} \cdot 2^{-\alpha j}} = \binom{M}{j} \frac{\beta^j (2^\alpha - \beta)^{M-j}}{2^{\alpha M}}.
\end{aligned} \tag{5}$$

Therefore, probability of total successful sybil attacks if M nodes attack the network is given as

$$P_{\max} = \sum_{j=1}^M \binom{M}{j} \frac{\beta^j}{2^{\alpha M}} (2^\alpha - \beta)^{M-j}. \tag{6}$$

Figure 5 shows the probability that at least one sybil node is successful out of M attacking sybil nodes in the proposed sybil prevention scheme. Moreover, Figure 6 shows the maximum probability when one or more attacking sybil nodes become successful under different sizes of authentication key. This figure shows a sharp exponentially declining trend in the probability as the number of useful sybil nodes increases.

5. Results and Discussion

In this section, we discuss the simulation results and provide a detailed performance analysis of the proposed scheme. As discussed earlier, the simulations are based on a network of 1000 sensor nodes. The parameters that we consider for performance are probability of usable sybil, traffic behavior, power consumption, and probability of attack detection.

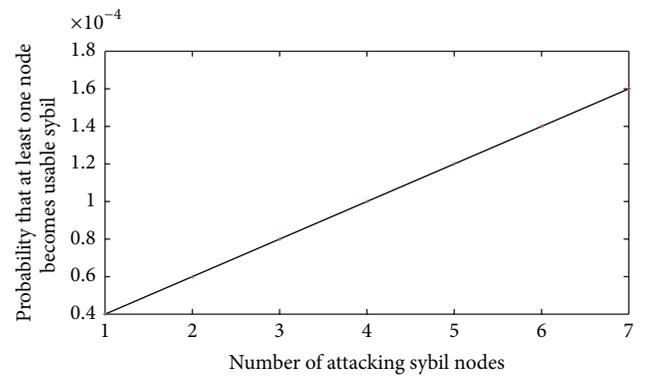


FIGURE 5: Successful probability of at least one sybil node in a pool of M sybil nodes.

5.1. Probability of Usable Sybils. The capability of a security algorithm can be better judged on the basis of its probability of letting sybil nodes successfully utilize the network. Figure 7 shows the probability of successful sybil attacks as exhibited by the proposed and referenced mechanisms. If a sybil node is successfully injected to the network without being detected, we call it usable attack. The attacks are launched and tested with the pool sizes of $N_{K_c} = 1$ and $N_{K_c} = 2$. The case of $N_{K_c} = 2$ is even more harder for sybil node to get through as compared to $N_{K_c} = 1$. However, the earlier case requires relatively more processing overhead than the latter one. The result shows that the proposed scheme provides a better protection

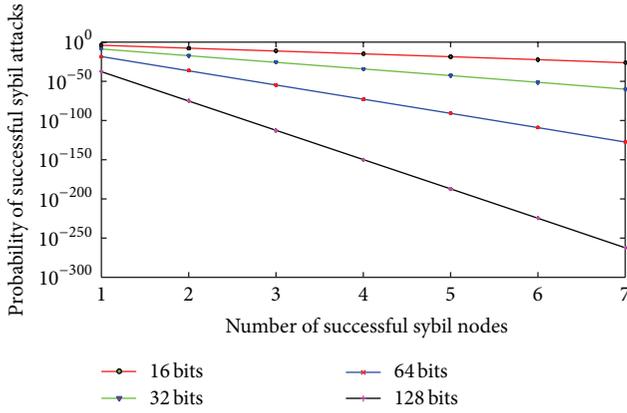


FIGURE 6: Probability of successful attacks by sybil nodes.

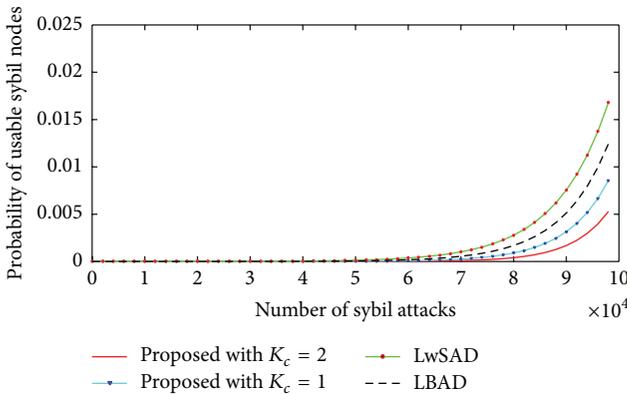


FIGURE 7: Probability that a sybil node will go undetected by the various algorithms.

since the probability of usable sybil node is lower in both cases ($N_{K_c} = 1$ and $N_{K_c} = 2$) than the LBAD and LwSAD.

5.2. Traffic Analysis. The lifetime of a wireless sensor network is directly proportional to the rate of exchange of packets. Excessive amount of packet exchange leads to a rapid battery drain due to which the network may die out. Figure 8 shows the behavior of algorithms against the traffic of the network during authentication process. It can be observed from the figure that the proposed scheme produces lesser number of packets in both cases of $N_{K_c} = 1$ and $N_{K_c} = 2$ as compared to LBAD and LwSAD. The number of packets generated is also directly proportional to the number of authentication rounds launched by a node or CH and will thus be borne at the cost of enhanced security of the network. This result also verifies our claim that the proposed scheme consumes lesser processing power and does not adversely affect the network lifetime.

The little overhead produced as a result of exchange of packets regarding authentication of the nodes can be borne at the cost of secure network. The traffic overhead is directly proportional to the number of authentication procedures launched by CH or SN depending upon the network.

5.3. Node Power Consumption. While designing a protocol for sensor nodes, the power consumption should always

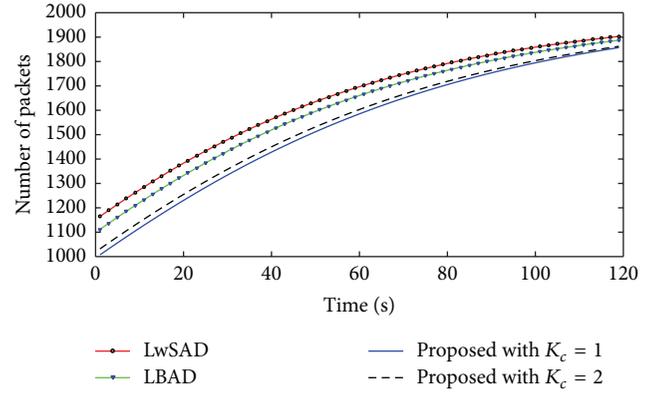


FIGURE 8: Simulated traffic behavior of the WSN while executing the proposed and existing authentication schemes.

be taken on board especially when the network has no resource of additional power supply once deployed. The power consumption of nodes is also calculated in case of direct and indirect validation of the nodes. As already discussed, the indirect validation requires more processing and communication power as compared to direct validation. Figures 9(a) and 9(b) illustrate the results of simulation with respect to power consumption in both direct and indirect validation process against authentication rounds. The graph shows the combined power consumption of all nodes either at both ends of the communication link or at the intermediate nodes during the process of authentication of a node or a set of nodes. The proposed authentication protocol consumes much lesser power in indirect validation as compared to direct validation as shown in Figures 9(a) and 9(b). The power consumption in case of indirect validation is due to information exchange like challenge and SRES between the originating and destination sensor nodes. This operation engages all the nodes that come in the path. Power consumption in case of indirect validation thus depends significantly on nodes population. Larger networks will consume more power in indirect validation and vice versa.

5.4. Probability of Attack Detection. Probability of attack detection is a major parametric criterion to evaluate the performance of a security algorithm. Figure 10 represents the probability of detection shown by each algorithm applied to the network. It can be clearly seen that the proposed algorithm provides a better protection against the sybil attacks. If we increase the pool size of keys in the sensor nodes, the situation will become even harder for the sybil node. However, this may demand more memory and processing capability available at each sensor node. Therefore, we limited the size up to $N_{K_c} = 2$. The pool size thus is subject to the requirement of the desired security level, power availability at the sensor nodes, and number of nodes in the network.

6. Conclusion

The existing approaches of defense against the sybil attacks are becoming incapable day by day due to increase in the

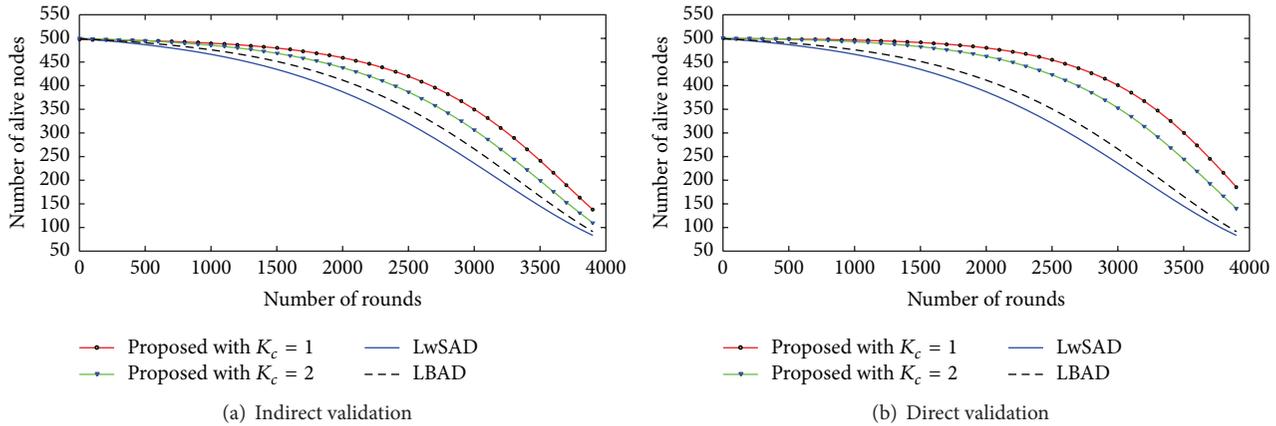


FIGURE 9: Power consumption and remaining number of alive nodes as a result of power consumption by participating nodes during the process of authentication in various algorithms.

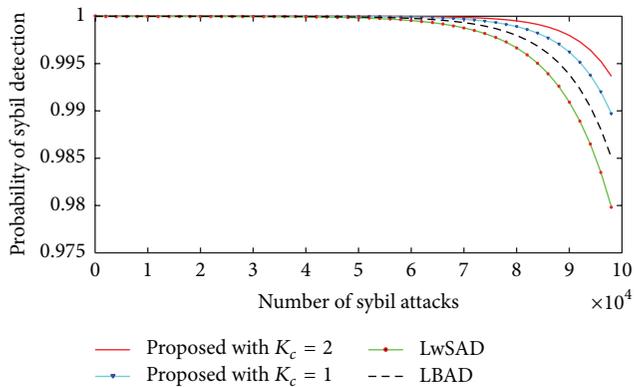


FIGURE 10: Probability of sybil node detection by the proposed algorithm in comparison with the existing algorithms.

processing power and capability of attacking nodes. A sybil node can now launch thousands of attacks before its battery gets drained or its processing capability is exhausted. In this paper, we have proposed a low complexity sybil attack detection mechanism which is based on the SRES authentication mechanism developed for Global System for Mobile (GSM) communications. The SRES mechanism is responsible for authenticating the user and encrypting the voice data. The proposed scheme can be implemented in both hierarchical and centralized wireless sensor networks. The proposed scheme has been analyzed for its performance under various sybil attacks. The scheme has been evaluated for its probability of detecting sybil nodes when different authentication key pool sizes are utilized. After extensive simulations, it has also been observed that the proposed scheme is able to detect sybil attacks with higher probability as compared to existing state-of-the-art existing schemes. It has been observed that the proposed sybil detection scheme exhibits lesser computational cost and power consumption as compared to the existing schemes for the same sybil detection performance.

Competing Interests

The authors declare that they have no competing interests.

References

- [1] H. Chen, W. Lou, Z. Wang, J. Wu, Z. Wang, and A. Xi, "Securing DV-Hop localization against wormhole attacks in wireless sensor networks," *Pervasive and Mobile Computing*, vol. 16, pp. 22–35, 2015.
- [2] M. Winkler, M. Street, K.-D. Tuchs, and K. Wrona, "Wireless sensor networks for military purposes," in *Autonomous Sensor Networks*, D. Filippini, Ed., vol. 13 of *Springer Series on Chemical Sensors and Biosensors*, pp. 365–394, Springer, Berlin, Germany, 2013.
- [3] D. Sun, X. Huang, Y. Liu, and H. Zhong, "Predictable energy aware routing based on dynamic game theory in wireless sensor networks," *Computers & Electrical Engineering*, vol. 39, no. 6, pp. 1601–1608, 2013.
- [4] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *Journal of Medical Systems*, vol. 36, no. 1, pp. 93–101, 2012.
- [5] I. Bekmezci and F. Alagaz, "Energy efficient, delay sensitive, fault tolerant wireless sensor network for military monitoring," *International Journal of Distributed Sensor Networks*, vol. 5, no. 6, pp. 729–747, 2009.
- [6] X. Xu, "Sequential anomaly detection based on temporal-difference learning: principles, models and case studies," *Applied Soft Computing Journal*, vol. 10, no. 3, pp. 859–867, 2010.
- [7] N. Aslam, W. Phillips, W. Robertson, and S. Sivakumar, "A multi-criterion optimization technique for energy efficient cluster formation in wireless sensor networks," *Information Fusion*, vol. 12, no. 3, pp. 202–212, 2011.
- [8] P. Schaffer, K. Farkas, Á. Horváth, T. Holczer, and L. Buttyán, "Secure and reliable clustering in wireless sensor networks: a critical survey," *Computer Networks*, vol. 56, no. 11, pp. 2726–2741, 2012.
- [9] S. Abbas, M. Merabti, D. Llewellyn-Jones, and K. Kifayat, "Lightweight sybil attack detection in MANETs," *IEEE Systems Journal*, vol. 7, no. 2, pp. 236–248, 2013.
- [10] B. Viswanath, M. Mondal, A. Clement et al., "Exploring the design space of social network-based Sybil defenses," in *Proceedings of the 4th International Conference on Communication Systems and Networks (COMSNETS '12)*, pp. 1–8, Bangalore, India, January 2012.
- [11] F. Li, P. Mittal, M. Caesar, and N. Borisov, "SybilControl: practical sybil defense with computational puzzles," in *Proceedings*

- of the 7th ACM Workshop on Scalable Trusted Computing (STC '12), pp. 67–78, October 2012.
- [12] N. Tran, J. Li, L. Subramanian, and S. S. M. Chow, “Optimal Sybil-resilient node admission control,” in *Proceedings of the IEEE Conference on Computer Communications (INFOCOM '11)*, pp. 3218–3226, Shanghai, China, April 2011.
- [13] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, “Detecting and localizing identity-based attacks in wireless and sensor networks,” *IEEE Transactions on Vehicular Technology*, vol. 59, no. 5, pp. 2418–2434, 2010.
- [14] J. Yang and Y. Chen, “A theoretical analysis of wireless localization using RF-based fingerprint matching,” in *Proceedings of the 22nd IEEE International Parallel and Distributed Processing Symposium (IPDPS '08)*, pp. 1–6, Miami, Fla, USA, April 2008.
- [15] M. Demirbas and Y. Song, “An RSSI-based scheme for sybil attack detection in wireless sensor networks,” in *Proceedings of the International Symposium on World of Wireless, Mobile and Multimedia Networks (WOWMOM '06)*, pp. 564–570, IEEE Computer Society, Buffalo, NY, USA, June 2006.
- [16] D. B. Faria and D. R. Cheriton, “Detecting identity-based attacks in wireless networks using signalprints,” in *Proceedings of the 5th ACM Workshop on Wireless Security (WiSe '06)*, pp. 43–52, New York, NY, USA, 2006.
- [17] A. Wool, “Lightweight key management for IEEE 802.11 wireless LANs with key refresh and host revocation,” *Wireless Networks*, vol. 11, no. 6, pp. 677–686, 2005.
- [18] D. Liu, P. Ning, and R. Li, “Establishing pairwise keys in distributed sensor networks,” *ACM Transactions on Information and System Security*, vol. 8, no. 1, pp. 41–77, 2005.
- [19] J. Newsome, E. Shi, D. Song, and A. Perrig, “The sybil attack in sensor networks: analysis & defenses,” in *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks (IPSN '04)*, pp. 259–268, ACM, Berkeley, Calif, USA, April 2004.
- [20] M. Bohge and W. Trappe, “An authentication framework for hierarchical ad hoc sensor networks,” in *Proceedings of the 2nd ACM Workshop on Wireless Security (WiSe '03)*, pp. 79–87, ACM, San Diego, Calif, USA, September 2003.
- [21] S. Zhu, S. Xu, S. Setia, and S. Jajodia, “LHAP: a lightweight hop-by-hop authentication protocol for ad-hoc networks,” in *Proceedings of the 23rd International Conference on Distributed Computing Systems Workshops (ICDCSW '03)*, pp. 749–755, Providence, RI, USA, May 2003.
- [22] P. Bahl and V. N. Padmanabhan, “RADAR: an in-building RF-based user location and tracking system,” in *Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '00)*, vol. 2, pp. 775–784, IEEE, March 2000.
- [23] M. Y. Rhee, *Mobile Communication Systems and Security*, John Wiley & Sons, New York, NY, USA, 2009.

Research Article

A Novel Nonlinear Multitarget k -Degree Coverage Preservation Protocol in Wireless Sensor Networks

Zeyu Sun,^{1,2} Xiaofei Xing,³ Chuanfeng Li,¹ Yalin Nie,¹ and Yangjie Cao⁴

¹School of Computer and Information Engineering, Luoyang Institute of Technology, Luoyang, Henan 471023, China

²School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an, Shaanxi 710049, China

³School of Computer Science and Software Engineering, Guangzhou University, Guangzhou 510006, China

⁴School of Software Technology, Zhengzhou University, Zhengzhou, Henan 450001, China

Correspondence should be addressed to Xiaofei Xing; xxfcsu@163.com

Received 26 May 2016; Revised 18 July 2016; Accepted 21 July 2016

Academic Editor: Fei Yu

Copyright © 2016 Zeyu Sun et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Due to the existence of a large number of redundant data in the process of covering multiple targets, the effective coverage of monitored region decreases, causing the network to consume more energy. To solve this problem, this paper proposes a multitarget k -degree coverage preservation protocol. Firstly, the affiliation between the sensor nodes and target nodes is established in the network model; meanwhile the method used to calculate the coverage expectation value of the monitored region is put forward; secondly, in the aspect of the network energy conversion, use scheduling mechanisms on the sensor nodes to balance the network energy and achieve different network coverage quality with energy conversion between different nodes. Finally, simulation results show that NMCP can improve the network lifetime by effectively reducing the number of active nodes to meet certain coverage requirements.

1. Introduction

With the rapid development of technology [1], wireless sensor network technology has developed exponentially [2, 3]. Wireless sensor network is a network system comprised of a large number of cheap sensor nodes that are randomly deployed and are self-organized [4–6]. A sensor node is characterized with such abilities as computation, perception, communication, storage, and control; the behavior characteristics of sensor nodes indicate that they are part of the network service system fusing the physical world and the information world, realizing collection, computation, communication, and control of data [7, 8]. In the engineering field, wireless sensor networks are widely used in many areas like military surveillance, transportation, health care, environmental monitoring, and rescue work and in other fields [9, 10]. The multilevel (k -degree) coverage is given, as an example, in Figure 1.

Two vital performance criteria that are required are coverage quality and energy management, which are also hot issues in the field of wireless sensor networks [11, 12]. Coverage as

its name implies means effectively covering the target nodes instead of the global monitored region. The coverage quality not only affects the degree of concern to the target nodes directly, but also affects the entire network lifetime and QOS (Quality of Services) directly [13–15]. The k -degree coverage mode is used in the process of covering multitarget nodes. Generally, the sensor nodes are deployed in the monitored region randomly, and, because of this, a large number of sensor nodes may be located in the monitored region [16, 17], which will generate a large number of redundant nodes, interfering with the communication channel and also reducing the communication ability between nodes, thereby speeding up the network energy consumption.

2. Related Works

Coverage control technology is an important basic research issue and is one of the hotspots in the field of wireless sensor network, and coverage quality affects the network lifetime directly [18]. In recent years, many experts at home and abroad have carried out research on the coverage technology

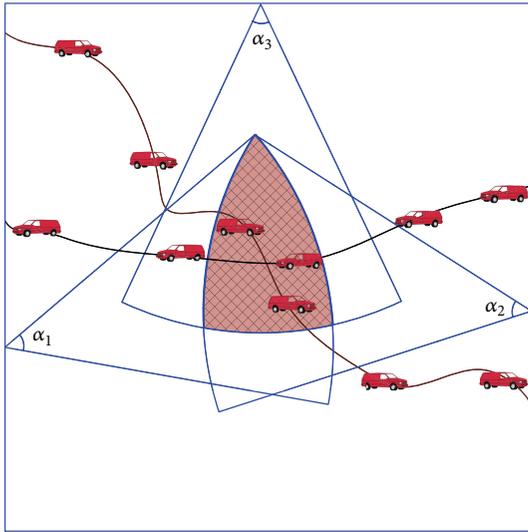


FIGURE 1: k -degree coverage diagram.

in wireless sensor network elaborately and profoundly as it was developed and widely used. Reference [19] proposed the artificial bee colony algorithm and particle swarm algorithm deploying the nodes in the whole monitored network and optimized the global coverage with both the intelligent algorithms in the coverage optimization phase, ultimately finishing the complete coverage over the monitored area. In terms of energy consumption, node energy conversion was scheduled with heuristic node scheduling algorithm, thereby improving the network lifetime. Literature [20] proposed a method to construct connectivity coverage protocol. The protocol defined the ratio between network coverage quality, network connectivity, and the performance indexes of the network infrastructure parameters, as well as constructing the SCA (Scheduling Control Algorithm) to meet the need of ensuring the whole network connectivity with minimum number of nodes in the problem-solving process, ultimately achieving the goal of network energy consumption balancing. Literature [21] put forward a kind of effective coverage area hole repair algorithm based on Voronoi. On the premise of certain coverage quality, this algorithm improved the coverage rate by increasing working nodes to coverage hole; in the meantime, it found the proper location information for mending, guaranteeing the whole network connectivity; by researching the Voronoi diagram, literature [22] also completed covering the monitored region, finding the solution to disc location of sensor nodes formed by the geometric variation parameters in the Voronoi diagram with related geometric theory. Literature [23] introduced local parameter α and formed local α -coverage with the idea of partial coverage optimization and then, after a series of calculations with α , achieved global coverage optimization. The algorithms above can effectively cover the monitored region to some extent. However, the three algorithms have some problems in common: they all need large amount of calculation, the algorithms are highly complex, and they have poor scalability in a wireless sensor network. Literature

[24, 25] proposed methods to calculate coverage rate in different monitored domain by effectively computing target nodes in monitored region, using different angle of sector formed by the sensor node and destination node. The above four algorithms have good feasibility and stability, as well as high network scalability; but their network models are too idealistic in the process of research: literature [22, 23] employed static target nodes as the research object; literature [25] did not consider the k -degree coverage situation of the moving related target nodes. Literature [26] put forward an energy efficient multitarget covering algorithm based on linear rule. The algorithm utilized a clustered structure system to solve the problem of multitarget covering. It presented an optimal solution to covering the target node in a linear fashion by calculating the coverage ability of the sensors and their remaining energy. Literature [27] proposed a coverage algorithm based on event driven mechanism. In this algorithm, the coverage and expectations of the nodes were calculated using the probability model, and then the calculation result was optimized to achieve optimal coverage on target nodes. Although these two algorithms can achieve the goal of optimal coverage on targets nodes and prolong the network lifetime, the requirement conditions for covering are quite strict. Furthermore, the algorithm is highly complex in itself. In order to cover the monitored region more effectively, based on the study in literature [24, 25], we present a nonlinear multiobjective coverage protocol (NMCP) which is given in this paper. This protocol can effectively calculate the coverage expectation value of the sensor nodes for the moving target nodes. In terms of energy, we compare the energy consumption under the multilateral connection and unilateral connection based on global network nodes energy analysis; namely, the energy cost in multipoint transmission is not higher than single-node energy consumption. In terms of energy conversion, it was completed between nodes with self-scheduling mechanism, thereby prolonging the lifetime of the entire network. At last, this paper gives the comparison process between NMCP algorithm and other algorithms in simulation experiments, which show that the NMCP algorithm is more effective and steadier.

3. Network Model and Coverage Quality

To study the wireless sensor network coverage problem better, as well as facilitate studying the NMCP algorithm, in this paper, we make the following assumptions:

- (1) Each sensor node has certain perception ability, and their perception range and communication range are both circles.
- (2) The perception range of a sensor node is far shorter than side length of the monitored region.
- (3) Initially, all sensor nodes have the same energy and are clock synchronized.
- (4) The location information of sensor nodes can be obtained with GPS.
- (5) A sensor node's perception radius is subject to normal distribution.

3.1. Basic Definitions

Definition 1 (target coverage). In the two-dimensional plane, each target node is covered by at least one sensor node, which is called the target coverage.

Definition 2 (k -degree coverage). In a monitored region, if each target node is covered by k sensor nodes, it is called k -degree coverage.

Definition 3 (network lifetime). The time span from when a network begins running to when none target node is covered by the sensor nodes is called the network lifetime.

Definition 4 (coverage quality). In the two-dimensional plane, the ratio of the total perception area of all sensor nodes to the monitored region is known as coverage quality.

3.2. Coverage Quality

Theorem 5. Suppose each sensor node's coverage rate is p . Let $k = 2$ in k -degree coverage, and m, n are the moving frequency of sensor nodes, the occurrence probability of which is $p^2 q^{n-2}$, and the conditional probability is $p q^{n-m-1}$, where $q = 1 - p$.

Proof. Let X be the number the node moves in the first round; let Y be that of the second round. According to the question, the target node is covered by sensor nodes in the m th time during the first round and is covered twice in the n th time, with the remaining $n-2$ times not covered, during the second round.

Therefore, the sensor node probability is

$$P(X = m, Y = n) = p^2 q^{n-2}. \quad (1)$$

The joint probability of both rounds is

$$\begin{aligned} P(X = m) &= \sum_{n=m+1}^{\infty} P(X = m, Y = n) = \sum_{n=m+1}^{\infty} p^2 q^{n-2} \\ &= p q^{m-1}, \end{aligned} \quad (2)$$

$$\begin{aligned} P(X = n) &= \sum_{m=1}^{n-1} P(X = m, Y = n) = \sum_{m=1}^{n-1} p^2 q^{n-2} \\ &= (n-1) p^2 q^{n-2}. \end{aligned}$$

According to multiplication formula of probability, we get

$$\begin{aligned} P(Y = n | X = m) &= \frac{P(X = m, Y = n)}{P(X = m)} = \frac{p^2 q^{n-2}}{p q^{m-1}} \\ &= p q^{n-m-1}. \end{aligned} \quad (3)$$

The process to prove is complete. \square

Theorem 6. If the coverage rate of each sensor node is p , then the coverage rate at any point in a two-dimensional plane is $P(nA) = 1 - (1 - p)^n$.

Proof. We will use mathematical induction in the proof. In the two-dimensional plane, any sensor node is not independent, so, according to the probability theory, when $k = 2$, we have

$$\begin{aligned} P(A + A) &= p(A) + p(A) - p(A)p(A) \\ &= 1 - (1 - p)^2. \end{aligned} \quad (4)$$

When $k = 3$, the joint coverage is

$$\begin{aligned} P(A + A + A) &= p(A + A) + p(A) \\ &\quad - p(A + A)p(A). \end{aligned} \quad (5)$$

Substitute formula (5) into formula (4); we have

$$P(A + A + A) = 1 - (1 - p)^3. \quad (6)$$

When $k = i$, by formula (6), we get

$$P(nA) = 1 - (1 - p)^n. \quad (7)$$

The process to prove is complete. \square

Corollary 7. In the two-dimensional plane, suppose the sensor node coverage rate is p , and N is the maximum value of the continuous coverage number of a sensor node. Until the moving target node is covered, the sensor node coverage expectation is $E(X) = [1 - (1 - p)^N] p^{-1}$.

Proof. In the two-dimensional plane, suppose the frequency a target node moves by is X . Because N is the maximum value of the continuous coverage number of a sensor node, the possible value range of X is $X \in [1, 2, 3, \dots, N]$. When $X = m$, and $1 \leq m \leq N - 1$ is satisfied, namely, in the first $N - 1$ times, the moving target node is not covered by the sensor nodes; we can get the distribution density function of X according to probability theory:

$$P(X = k) = \begin{cases} p(1 - p)^{k-1} & k = 1, 2, 3, \dots, N - 1 \\ (1 - p)^{N-1} & k = N. \end{cases} \quad (8)$$

Namely,

$$E(X) = \sum_{k=1}^{N-1} k p (1 - p)^{k-1} + N (1 - p)^{N-1}. \quad (9)$$

Suppose $q = 1 - p$, $S = \sum_{k=1}^{N-1} k (1 - p)^{k-1}$; then $S = \sum_{k=1}^{N-1} k q^{k-1}$; multiplying both sides of the equation by q , we get

$$qS = \sum_{k=1}^{N-1} k q^k. \quad (10)$$

Namely,

$$\begin{aligned}
(1-p)S &= \sum_{k=1}^{N-2} q^k - (N-1)q^{N-1} \\
&= \frac{1-q^{N-1}}{1-q} - (N-1)q^{N-1}, \\
S &= \frac{1-q^{N-1}}{(1-q)^2} - \frac{(N-1)q^{N-1}}{1-q} \\
&= \frac{1-(1-p)^{N-1}}{p^2} - \frac{(N-1)(1-p)^{N-1}}{p}.
\end{aligned} \tag{11}$$

Substitute S into formula (9); we have

$$\begin{aligned}
E(X) &= p \left(\frac{1-(1-p)^{N-1}}{p^2} - \frac{(N-1)(1-p)^{N-1}}{p} \right) \\
&\quad + N(1-p)^{N-1} = [1-(1-p)^N] p^{-1}.
\end{aligned} \tag{12}$$

After the sensor nodes cover the monitored region during time span t , they will inevitably have some energy consumptions, which results in the change in their coverage areas. In order to improve effective coverage on the target nodes concerned, in the process where sensor nodes consume energy, the total monitored region can be effectively covered, or all the concerned target nodes are effectively covered, as long as the sequence collection of the coverage areas of sensor nodes is not less than the total monitored area after their energy is consumed. \square

Theorem 8. *In the two-dimensional plane, suppose the fitting function of a sensor node energy consumption is $f(x, y)$; the coverage area is S_n after the energy attenuation, where $n \in [1, 2, 3, \dots, N]$; then the bounded closed region formed is able to cover the entire monitored region; namely, $\iint_S f(x, y) dx dy = \lim_{x \rightarrow \infty} \iint_{S_n} f(x, y) dx dy$.*

Proof. Take a bounded closed region sequence S'_n , which covers the whole monitored region. Suppose $S'_1 \subset S'_2 \subset S'_3 \dots S'_n \subset \dots S_n$. Because the energy attenuation function is nonnegative, the integral sequence $\iint_{S'_n} f(x, y) dx dy$ is increasing; suppose the limit is as follows:

$$I = \lim_{x \rightarrow \infty} \iint_{S'_n} f(x, y) dx dy. \tag{13}$$

Therefore, we just need to prove

$$\lim_{x \rightarrow \infty} \iint_{S_n} f(x, y) dx dy = I, \tag{14}$$

where factor I is a finite set of numbers. For any $\varepsilon > 0$, formula (13) shows that there is a number N ; when $n \geq N$, formula (15) is always satisfied:

$$I - \varepsilon < \lim_{x \rightarrow \infty} \iint_{S'_n} f(x, y) dx dy < I + \varepsilon. \tag{15}$$

Suppose there is n_0 , when $n \geq n_0$, $S_n \supset S'_n$. Therefore, according to the nonnegative $f(x, y)$ and formula (15), we know that

$$\iint_S f(x, y) dx dy \geq \lim_{x \rightarrow \infty} \iint_{S'_n} f(x, y) dx dy > I - \varepsilon. \tag{16}$$

For each fixed $n \geq n_0$, on the other hand, there must be a number which tends to infinity; suppose the number is k_n , and $S'_{k_n} \supset S_n$; then by formula (15) we get

$$\begin{aligned}
\iint_S f(x, y) dx dy &\leq \lim_{x \rightarrow \infty} \iint_{S'_{k_n}} f(x, y) dx dy \\
&< I + \varepsilon.
\end{aligned} \tag{17}$$

Namely, when $n \geq n_0$, we get

$$I - \varepsilon < \lim_{x \rightarrow \infty} \iint_{S_n} f(x, y) dx dy < I + \varepsilon. \tag{18}$$

Therefore, formula (14) is satisfied.

Now, let $I = +\infty$; for any $M > 0$, formula (13) shows that there is N_1 and

$$\iint_{S'_{N_1}} f(x, y) dx dy > M. \tag{19}$$

And because there is n_1 , when $n \geq n_1$, $S_n \supset S'_{N_1}$ is always satisfied, so we have

$$\iint_S f(x, y) dx dy \geq \iint_{S'_{N_1}} f(x, y) dx dy > M. \tag{20}$$

The process to prove is complete. \square

4. NMCP Protocol

4.1. Energy Conversion. For a sensor node, the energy consumption mainly happens in the sensing module and the communication module. When collecting l bits data, the energy consumption of sensing module E_T and the communication module E_R is as follows:

$$E_T(l, d) = \begin{cases} lE_{T\text{-elec}} + l\varepsilon_{fs}d^2, & d < d_0 \\ lE_{T\text{-elec}} + l\varepsilon_{\text{amp}}d^4, & d \geq d_0. \end{cases} \tag{21}$$

The energy consumption model for receiver module is

$$E_R(l) = E_{R\text{-elec}}(l) = lE_{\text{elec}}, \tag{22}$$

where l bits are the fixed length of data transmitted, d represents the communication Euclidean distance between sensor nodes, and d_0 represents the threshold or proportional quantity of the communication distance between sensor nodes. When the communication distance between sensor nodes is less than d_0 , the energy attenuation index value is 2; otherwise it is 4.

Definition 9 (optimum subset). Let G be the set of wireless sensor network's sensor nodes; G_1 is called an optimum subset where G_1 is a subset of sensor nodes, namely, $G_1 \subset G$, and all the sensor nodes in G_1 cover target set T entirely.

Definition 10 (energy property). $W = \{w_1, w_2, w_3, \dots, w_n\}$ is the initial energy collection of sensor nodes; W follows $W \sim N(\mu, \sigma^2)$ normal distributions, where w_i denotes the initial energy of sensor node s_i .

Definition 11 (the maximum distortion). On the premise that certain coverage rate is met, the maximum distortion is

$$E \left[(s_1(x, y) - s(x, y))^2 \right] \leq D \quad \forall s_i(x, y) \in A. \quad (23)$$

$s_1(x, y)$ is the estimated Euclidean distance between a sensor node and the target node, while $s(x, y)$ is the average measured distance, Euclidean distance, between the sensor node and the target node.

Theorem 12. *The communication distance between nodes is less than or equal to half the difference between variance and the distortion.*

Proof. Suppose the measured distance at the target node $t(x, y)$ is $s(x, y)$, the data information used contains the measured data, and when multitarget nodes are measured, the average of measured values follows normal distribution. The energy collection set of preset-energy sensor nodes is $W = \{w_1, w_2, w_3, \dots, w_n\}$. Then the Euclidean distance between communication nodes is as follows:

$$\begin{aligned} R((x_1, y_1), (x_2, y_2)) &= \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \\ &= E[(S(x_1, y_1) - u)(S(x_2, y_2) - u)] = R(d). \end{aligned} \quad (24)$$

Let H be the set of sensor nodes which collects information, and let H_1 be the complementary set of H ; the sensor node nearest to the target node in H is used to calculate the measured distance which is then used to estimate a signal data in H_1 . Therefore, the estimated signal value at the target node point (x, y) is $s_1(x_0, y_0)$; namely,

$$s_1(x_0, y_0) = s(x_1, y_2). \quad (25)$$

According to formulas (23) and (24), we have

$$\begin{aligned} E[(s(x_0, y_0) - \mu)(s(u, v) - \mu)] \\ = 2\sigma^2 - 2R(d((x_0, y_0), (u, v))). \end{aligned} \quad (26)$$

Substitute formula (23) into formula (26); we have

$$R(d((x_0, y_0), (u, v))) \leq \sigma^2 - \frac{D}{2}. \quad (27)$$

The process to prove is complete. \square

Theorem 13. *In initial state, when transmitting l -bit data, the energy consumed in multilateral transmission is more than that consumed in unilateral transmission.*

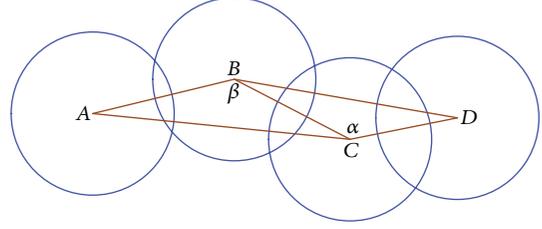


FIGURE 2: Multilateral and unilateral node connection diagram.

Proof. Suppose the current working node S_i has a set of neighbour nodes named Z , in which each node corresponds to neighbour S_z . For convenience, the calculations start with 3, which denotes the number of neighbours in the collection, when $n \rightarrow \infty$. We will prove that using mathematical induction, as shown in Figure 2.

Let A be the source node, let D be the convergence node, let B, C be the neighbour nodes, and let O be the disk centre; the network stores l -bit data of any sequence, which is going to be sent from source A to convergence node D . Two kinds of circumstances are discussed as follows.

The First Case: From A to D Directly. According to formula (21), the energy dissipations are as follows when source node A sends out data:

$$E_{Tx,AD}(l, d_{AD}) = \begin{cases} lE_{T\text{-elec}} + l\varepsilon_{fs}d_{AD}^2, & d_{AD} < d_0 \\ lE_{T\text{-elec}} + l\varepsilon_{amp}d_{AD}^4, & d_{AD} \geq d_0. \end{cases} \quad (28)$$

The Second Case: From A to B, Then From B to D. We prove that with mathematical induction: when $k = 3$, from node A to node B , the energy consumption model of the transmitting module in node A is

$$E_{Tx,AB}(l, d_{AB}) = \begin{cases} lE_{T\text{-elec}} + l\varepsilon_{fs}d_{AB}^2, & d_{AB} < d_0 \\ lE_{T\text{-elec}} + l\varepsilon_{amp}d_{AB}^4, & d_{AB} \geq d_0, \end{cases} \quad (29)$$

$$E_{Rx,B}(l) = lE_{elec}.$$

The energy consumed by node B to receive the information is

$$E_{Tx,BD}(l, d_{BD}) = \begin{cases} lE_{T\text{-elec}} + l\varepsilon_{fs}d_{BD}^2, & d_{BD} < d_0 \\ lE_{T\text{-elec}} + l\varepsilon_{amp}d_{BD}^4, & d_{BD} \geq d_0. \end{cases} \quad (30)$$

So far, the total energy consumption of nodes on the path A - B - D is

$$E_{Total} = E_{Tx,AB} + E_{Rx,B} + E_{Tx,BC}. \quad (31)$$

In their initial state, the nodes work with the same amount of energy and are independent from each other. The basic properties of triangle show that

$$E_{Total} = E_{Tx,AB} + E_{Rx,B} + E_{Tx,BD} < E_{Tx,AD}. \quad (32)$$

Namely, when $k = 3$, node energy consumption in multilateral data transmission is lower than that in unilateral data transmission, so when $k = 3$, the inequality is satisfied.

First, take the path from A to B , then B to C , and C to D (A - B - C - D), as an example to prove, and then add to $n \rightarrow \infty$. Because $\angle \alpha > \angle ACD = \pi/2$, $\angle \alpha$ is an obtuse angle. Conclusion can be drawn with cosine theorem as: $\cos \angle \alpha < 0$; namely, $BC^2 + CD^2 < BD^2$, when $n \rightarrow \infty$. The adjacent neighbour nodes can be combined into an obtuse triangle, in which the square of the length of the side opposite to the acute angle is less than the sum of the squares of the lengths of the sides of the obtuse angles. After $n - 2$ times of superposition calculation, we eventually get $BC^2 + CD^2 < BD^2$; namely,

$$\begin{aligned} E_{Tx_{AB}} + E_{Rx_{B}} + \dots + E_{Rx_{n-1}} + E_{Tx_{n-1,n}} &< \dots \\ &< E_{Tx_{AB}} + E_{Rx_{B}} + E_{Tx_{BD}} < E_{Tx_{AD}}. \end{aligned} \quad (33)$$

The process to prove is complete. \square

Energy consumed in multilateral transmission is not higher than the energy dissipation in unilateral transmission in a multiple hops path in wireless sensor network [28–30]. But practically, it is always hard to implement the single hop transmission between the source node and the convergence node due to the limited communication radius of nodes, obstacles, and the variation of environment.

NMCP algorithm takes the network running time round number as the basic unit, each round containing two aspects, namely, coverage control information and the stable state information of nodes. In working stage, the working nodes remain on, and all redundant nodes are off so as to save the network energy. At stable stage, each node has five kinds of running state, which are judge, compete, wait, start, and sleep states [31–33]. Judge state: at the beginning of each time round, nodes are in the state of judgment. When redundant judging condition of a node is satisfied, the node enters sleep state; otherwise, if the condition is not satisfied, it enters the compete state; compete state: a node which succeeds on the start-up of a competition may convert into the state of working, whereas the unsuccessful nodes enter the state of wait; wait state: those nodes failed in the competition to enter wait state, and when they successfully receive the on-duty message from their neighbours during initiating, they update the message of their own locally and then enter judge state. Start state: when a node wins in the competition, it enters the start state. By calculating the node coverage, whether the nodes which perception regions are in start states satisfy the requirements for coverage is determined. If not satisfied, it sends on-duty message for schedule and then enters judge state; sleep state: while the redundant judging conditions are satisfied, the node enters sleep state to reduce its energy consumption and enters judge state in the unit time round. When the density of nodes is too large in a monitored region, the vast majority of the nodes in the region will satisfy the redundant node judgment conditions. At the moment, all those nodes will enter sleep states. Although this state can reduce the node energy consumption, there are still some deficiencies; the reason for this is that once perceiving neighbour nodes enter sleep state, there will be

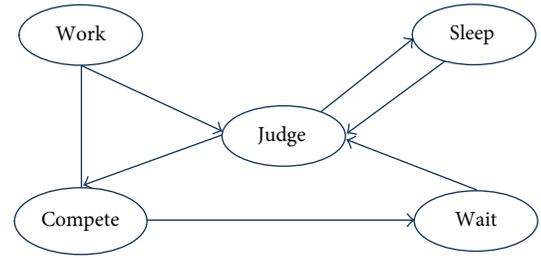


FIGURE 3: The state transition diagram.

large coverage blind area in monitored region; therefore the coverage quality is decreased [34–37]. In order to avoid such kind of situation, NMCP algorithm uses a mechanism that once a node enters sleep state, it wakes up its neighbour nodes immediately and converts them into wait states. The aim is to reduce the density of working nodes first, namely, select a node as a candidate working node directly; the other nodes not selected enter sleep states directly and then schedules in the candidate working nodes [38]. Each candidate working node elects itself with a probability of p , whereas those nodes which are not chosen directly enter sleep state and then work as candidate nodes in the redundant nodes. Each candidate node elects itself to enter the prework state, whereas those candidate nodes which are not elected enter presleep state. The state transition between the five states in the covering control phase is as shown in Figure 3.

4.2. The Basic Idea of NMCP Algorithm. Based on the idea in literature [10] by means of clustering theory, this algorithm divides the coverage region in the monitored region into several clusters, each head node of a cluster being in charge of and controlling the member nodes in its cluster. At the initial stage of the network operation, the cluster members send “ k -degree Coverage” message to their cluster head node first, while the cluster header maintains a linked list CL which receives the messages which are composed of the sensor node ID and such properties as its perception range and energy attenuation. After one or more cycles, the cluster header will collect all the cluster members information, then sort the list according to the size of the residual energy of nodes, as well as assigning to weight the first few nodes in the front of the list; after that, it scans every item in the linked list and marks the sensor nodes which are capable of covering the target node. Finally, the cluster header sends “ k -Notice” messages to those marked member nodes which are responsible for covering the target node. The cluster head node sends on-duty messages to the member nodes and neighbour nodes to awaken those members nodes to enter waiting state and notify the neighbour cluster head nodes of the monitored information of the target. Based on the above information, the weighting of member nodes participating in the monitoring is calculated. If its weighting is greater than the set threshold, the node would enter into active state and monitor any moving target within its sensing range. Active nodes around the target will form an initial dynamic cover group. Member nodes will send an information packet to the cluster head node. The data packet contains information as

```

(1) Input  $N, R_s, E, E_{thr}$  // Initialize the number of sensor nodes, perception radius, sensor nodes energy
and the energy threshold value.
(2)  $CL = \text{Null}$ 
(3)  $i = 0, j = 0, t = 0, k = 0$  // loop variables
(4) While ( $i \leq N$ )
(5)  $E(X) = \cup\{(s_i, L) \mid N(l, \sigma^2)/l^2\}$  // calculating the coverage expectation values of node members
(6) While ( $t_r = t \parallel t_r = nt$ ) // After one or a few rounds
(7) {
(8)   if ( $S_a \leftarrow \text{Coverage}$ ) // the administrator node receives "Coverage" message
(9)    $CL[j].\text{date} = \text{Coverage}$ 
(10)   $j++$ 
(11) }
(12)  $\text{Sort\_order}(CL[j].\text{data})$  // sorting the member nodes
(13) While ( $j < i$ ) // determining the optimal coverage set
(14) {
(15)   if ( $E_r < E_{thr}$ ) // node residual energy is less than node threshold energy
(16)    $S_i \leftarrow \text{Notice}$  // the administrators sends "Notice" to the member nodes
(17)    $\text{Coverage}(t_i) \leftarrow S_i$  // node members complete covering the target nodes
(18) }
(19)  $k = j$ 
(20) While ( $k < j$ )
(21) {
(22)   if ( $CL[k].\text{data} \supset CL[j].\text{data}$ )
(23)   {
(24)      $\text{Close}(CL[k].\text{data})$ 
(25)      $j++$ 
(26)   }
(27) else
(28)   return ()
(29) }

```

ALGORITHM 1

time stamp, node ID, and distance between the nodes and the target. As there may be more than one cluster head node in NMCP, for the convenience of management, one of the cluster head nodes will be selected as managing node and is responsible for the information fusion and data management. Because the target node is moving in the monitoring area, the initial NMCP may not meet the requirements of target monitoring. Therefore, dynamic reconstruction is needed according to the position of the target. Reconstruction process is completed by members updating management and head node reselecting. When the target moves to a new grid, new cluster head node and member nodes that meet the requirements of the threshold weighting joint to the original NMCP, and the newly jointed cluster head node is elected as the leader node. Nodes within the original NMCP that cannot meet the monitoring requirements will quit the NMCP. If the original managing node happens to be a quitting node, at this time, the original managing node needs to send information of target location and member's nodes to the new managing node. When the target moves away from the original location, the cluster head node will broadcast messages to its member nodes to enter into sleep state to save power consumption.

4.3. NMCP Algorithm Description

Step 1. Calculate the perception intensity of cluster members.

Step 2. The cluster member nodes send "k-Coverage" to the cluster header node. After one or more time units, the header node receives the message from cluster members.

Step 3. The cluster head node establishes a linked list and stores the information collected in it and then sorts the list according to the amount of energy in the sensor nodes; at the same time it assigns weights to those nodes which have higher energy.

Step 4. Find qualified sensor nodes, and mark them.

Step 5. If the target node is in the state of k-coverage, the cluster header will traverse the list to turn off those sensor nodes which have weaker perception ability.

Step 6. After the traverse, the cluster header node schedules the optimal subset to finish covering the target node; otherwise, go to Step 2.

4.4. Algorithm Code. See Algorithm 1.

4.5. The NMCP Algorithm Complexity Analysis. In the analysis of NMCP algorithm, n represents the number of sensor nodes; m is equal to the number of edges connecting any two sensor nodes. P_{\min} and P_{\max} are the minimum and maximum coverage value of the monitoring area, respectively. Δp means

the increment of coverage after each covering process. Set $P_{\min} = c$ and $P_{\max} = bn$; c and b are constant coefficient. Assume that, at the initial stage, the coverage rate of sensor node is $p(0) = b/n$, and at time t , the transition probability of a sensor node is greater than $c/2bn$ which also means the minimum probability of sensor node's coverage is $P_{\min} = c/2bn$. Set $R = (1 - e)p(t - 1)$ at time $t + 1$; the coverage of a sensor node is

$$p(t+1) = \frac{p_{t+1}(t+1)}{p_{t+1}(t+1) + p_t(t+1)} \leq \frac{p_{t+1}(t+1)}{c + p_t(t+1)} \leq \frac{b}{(1 - \Delta p)(c + ce + R)}. \quad (34)$$

When $L = b/(1 - e)(c + ce + R)$, the time complexity of NMCP algorithm is $E(T)$, as follows:

$$E(T) = \sum_{m=1}^{n-1} \left(\frac{2bn}{c(n-m)} \cdot \left[1 - \frac{L}{n} \right]^{1-n} \right) = \frac{2bn}{c} \left[1 - \frac{L}{n} \right]^{1-n} \sum_{m=1}^{n-1} \frac{1}{m} \leq \frac{2bn}{c} e^{-L} H_{n-1}. \quad (35)$$

Since $\sum_{m=1}^{n-1} (1/m)$ is the sum of harmonic series of first $n - 1$ terms, let $H_{n-1} = \sum_{m=1}^{n-1} (1/m)$; then $\sum_{x=1}^{n-1} (1/x) - 1 < \int_1^{n-1} (1/x) dx < \sum_{x=1}^{n-1} (1/x)$; that is,

$$H_{n-1} = \sum_{m=1}^{n-1} \frac{1}{x} = \int_1^{n-1} \frac{1}{x} dx = O(\ln n). \quad (36)$$

5. System Evaluation

In order to verify the effectiveness and the stability of algorithm NMCP, we use MATLAB7.0 as the simulation platform for experiment and analysis. With the comparison experiment between NMCP and [26, 27, 34], we give the performance comparison in different evaluation systems. The simulation parameters are as shown in Table 1.

The comparison simulation experiments between algorithms NMCP in this paper and ETCA in [26], ECAPM in [34], and EPDM in [27] are carried out under the same network scale, with different network lifetime, target node scale, number of sensor nodes, network run time, and coverage rate, as shown in Figures 4–7.

Figure 4 shows the comparison simulation diagram of algorithms NMCP, ETCA, and ECAPM in the aspect of network lifetime. In this figure, the three algorithms have similar lifetime at the initial phase, while as time passes by, the ETCA algorithm and ECAPM algorithm rise relatively slower which mainly lies in the fact that ETCA algorithm and ECAPM algorithm monitor the whole network in centralized manner, thus converting the scheduling mechanism between sensor nodes in a linear fashion, which consumes more energy, whereas the NMCP algorithm in this paper mainly finishes the covering process over the monitored region in a fashion of seeking in the linked list and finding the optimal node set. With the same number of sensor nodes, the NMCP

TABLE 1: Performance parameters list.

Parameter	Value
Monitoring area	400 * 400
R_s	10 m
Initial energy	10 J
Time	600 s
e_{\min}	0.005 J
R_c	20 m
$E_{R\text{-elec}}$	50 J/b
$E_{T\text{-elec}}$	50 J/b
ϵ_{fs}	10 (J/b)/m ²
ϵ_{amp}	100 (J/b)/m ²

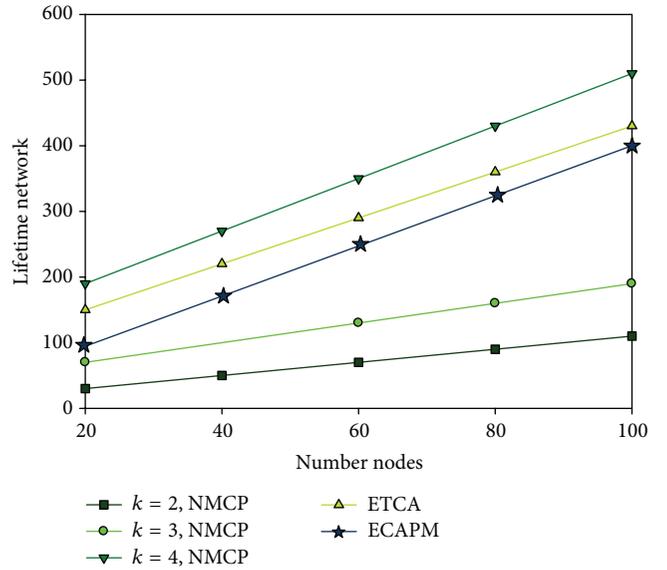


FIGURE 4: Comparison of network lifetime.

algorithm requires longer network run time. Take an example of iterating 200 times, the network lifetime is prolonged by 16.33% and 19.75% averagely compared with the algorithm ETCA.

Figure 5 reflects the different number of target nodes and the corresponding network lifetime variation curve. When the network begins running, the number of sensor nodes is 348, and the number of target nodes is 10. With the increase of network running time and target nodes number, the network lifetime using the three algorithms is all in equilibrium state. When $k = 4$, both the ETCA algorithm and the ECAPM algorithm show slight fluctuations relative to the NMCP algorithm. With the same number of target nodes, the average running time of the network using NMCP algorithm is 7.12%, 9.06% higher than that using the ETCA algorithm.

Figure 6 shows the run time comparison curves of the three algorithms. As can be seen from Figure 4, the run time of NMCP algorithm is less than that of the EPDM or ECAPM algorithm. The main reason is that, using clustered structure, the NMCP algorithm has higher speed than EPCM or ECAPM algorithm when seeking nodes which meet the

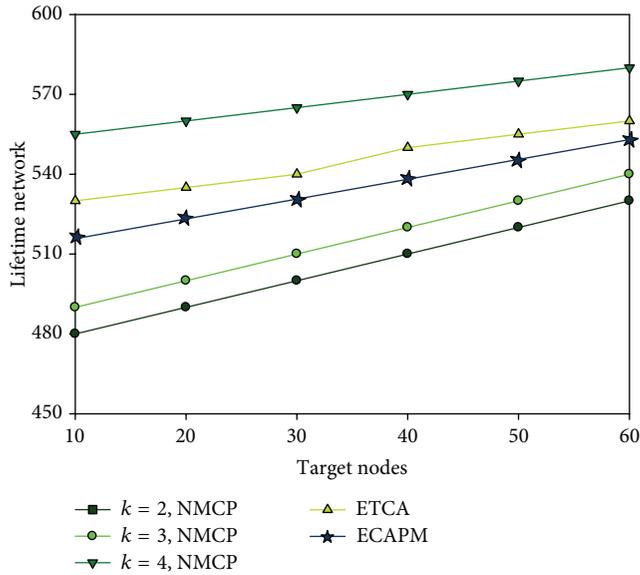


FIGURE 5: The network lifetime and number of target nodes.

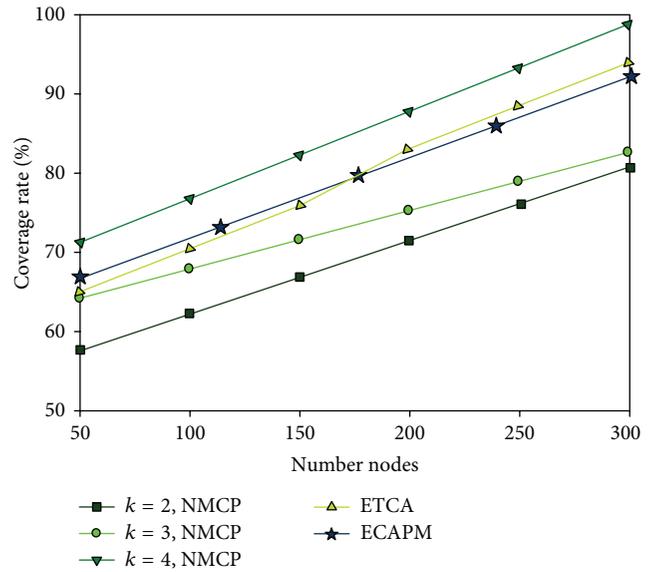


FIGURE 7: Comparison of coverage rate.

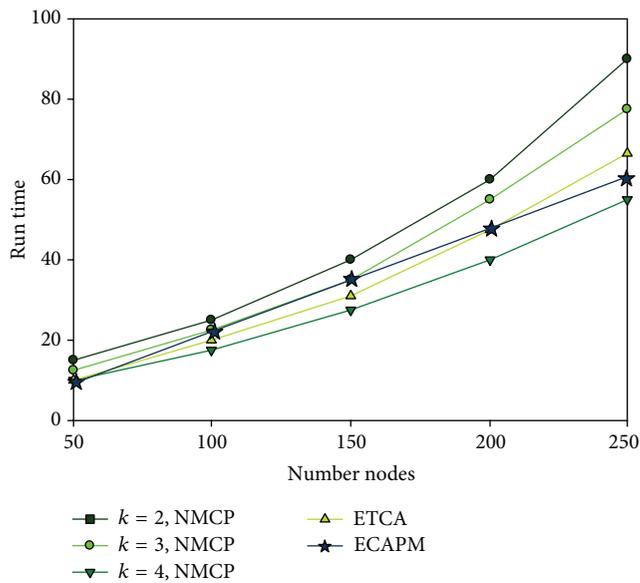


FIGURE 6: The run time comparison of the three algorithms.

requirements for covering the sensor node, which reduces the difficulty in the coverage problem. Although the EPDM algorithm also uses clustering technique, it uses centralized covering strategy in the process of switching energy between nodes by traversing all the sensor nodes in the node set before the optimal covering subset is determined.

To simulate the coverage rate, we carried out the comparison experiments between the algorithm in this paper and EPDM and ECAPM, with the monitored region id set to $200 \times 200 \text{ m}^2$. As shown in Figure 5, the coverage rate of the three algorithms increases along with the increase in the number of sensor nodes. When the coverage rate reaches 99.9%, the complete coverage over the target node is taken

on as finished. When the active nodes number is 50 and $k = 4$, the coverage rate of NMCP algorithm is 71%, while the active nodes numbers of the EPDM algorithm and ECAPM algorithm are 64% and 65%, respectively. When the coverage rate is 99.9%, the active nodes number of NMCP algorithm is 296, whereas the other two algorithms' coverage rates are 91% and 88%, respectively, when the active nodes number is 296. Therefore, on average, the NMCP algorithm in this paper can increase the coverage rate by 10.31% and 12.47% comparing to EPDM and ECAPM algorithm, respectively.

Experiment 1. Comparison experiments between the NMCP algorithm, ETCA algorithm, and LP_MLCEH protocol [36] are carried out about prolonging the network lifetime; the experimental data are the average of 200 times simulation data, as shown from Figures 8–10.

The second group of comparison experiments are carried out between NMCP algorithm, ETCA algorithm, and LP_MLCEH protocol in relation to the network lifetime in different monitored region. In the experiments, we give K different values and change network scale by changing the number of nodes randomly deployed in monitored region. For smaller monitored region, the number of the randomly deployed nodes is initiated at 20, which is also used as the unit to increase gradually. The simulation diagram shows that the lifetime of wireless sensor network rises in a linear upward trend with the increase of the number of sensor nodes. The main reason is that the members in the node set cover the target node in turn with nodes scheduling mechanisms; therefore the network life cycle is prolonged. In the same network environment, NMCP algorithm prolongs the network lifetime by 13.71% and 16.52% than ETCA algorithm and LP_MLCEH protocol on average; for a larger monitored network, the number of the randomly deployed nodes is initiated to 50, which is also used as the unit to

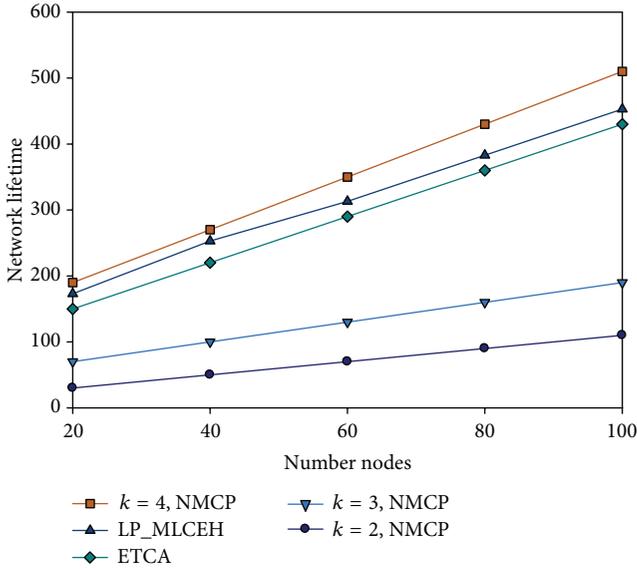


FIGURE 8: 100 * 100, the network lifetime curve.

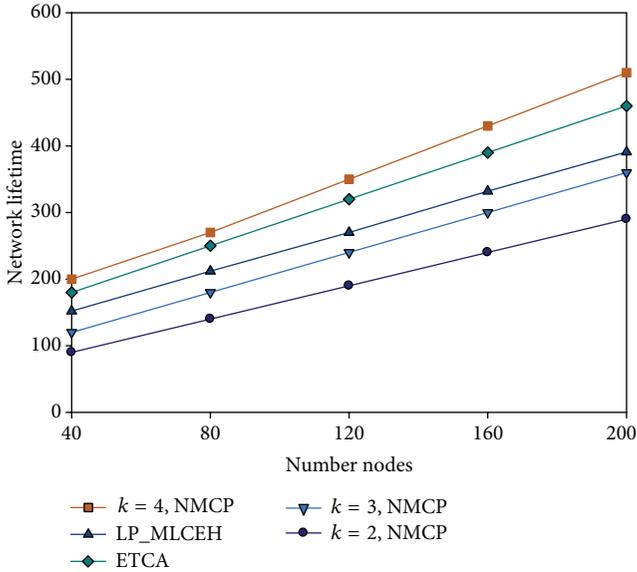


FIGURE 9: 200 * 200, the network lifetime curve.

increase gradually. The simulation diagram also shows that the lifetime of wireless sensor network rises with the increase of the number of sensor nodes. Furthermore, its rising trend exceeds that of smaller monitored region. Compared to ETCA algorithm and LP_MLCEH protocol, the network lifetime is increased by 15.13% and 17.27% on average.

Experiment 2. The comparison experiments about prolonging the network lifetime are carried out between the NMCP algorithm, EPDM algorithm [28], and OSCC protocol [11]. Taking the 200 * 200 as an example, the experimental data are the average of simulation data of 100 times, as shown from Figures 11–13.

In Figure 11, with the increase in the number of sensor nodes, the three algorithms demonstrate incremental change

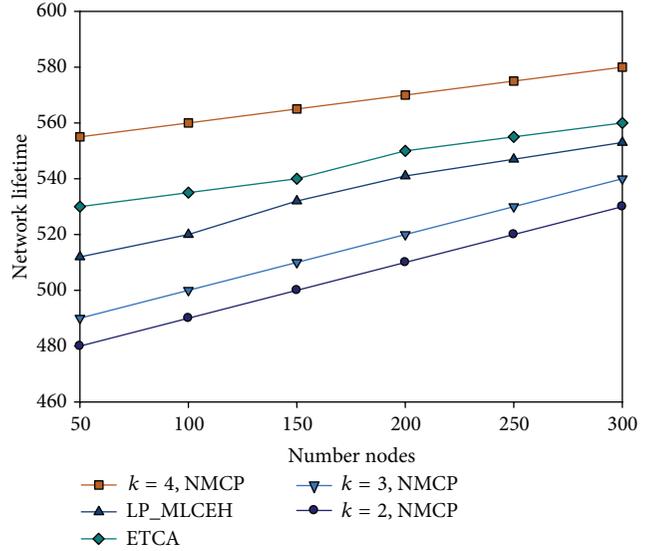


FIGURE 10: 300 * 300, the network lifetime curve.

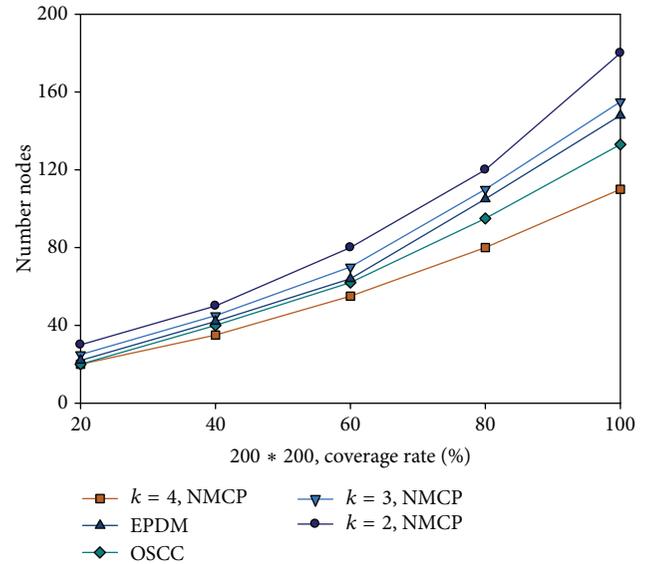


FIGURE 11: 200 * 200, network coverage curve.

in coverage rate. When the coverage rate is 99.9%, and $k = 2$, the number of sensor nodes is 180; when $k = 3$, the number of sensor nodes is 147; when $k = 4$, and the number of the sensor nodes is 107, this algorithm reaches 99.9%, which means that the k -degree coverage is completed, whereas EPDM algorithm and OSCC algorithm cannot reach 100%, which suggests that the NMCP algorithm in this paper has higher coverage rate than the EPDM algorithm and the OSCC algorithm, verifying the effectiveness of the algorithm presented in this paper. In Figure 12, at the beginning of the program execution, the two algorithms have almost the same coverage rate, but as time passes by, both the two contrasted algorithms' coverage rates decline. The main reason of that is the fact that in EPDM and OSCC algorithm the sensor nodes use uninterrupted covering method during network operation; namely, they cover the target nodes continuously in the monitored

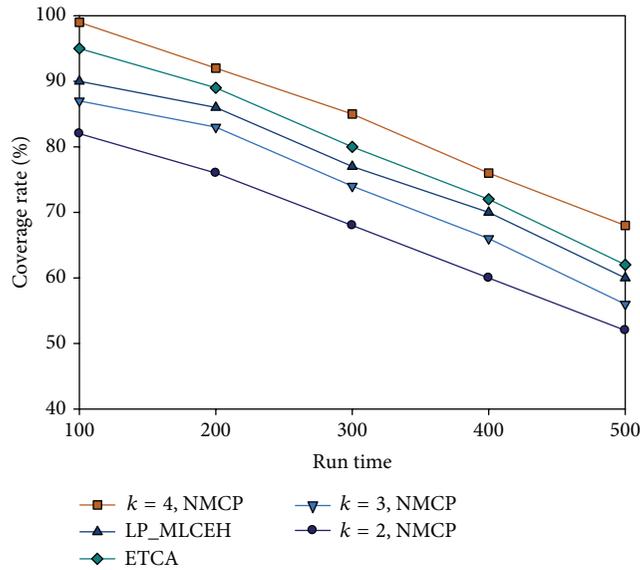


FIGURE 12: 200 * 200, the network running time curve.

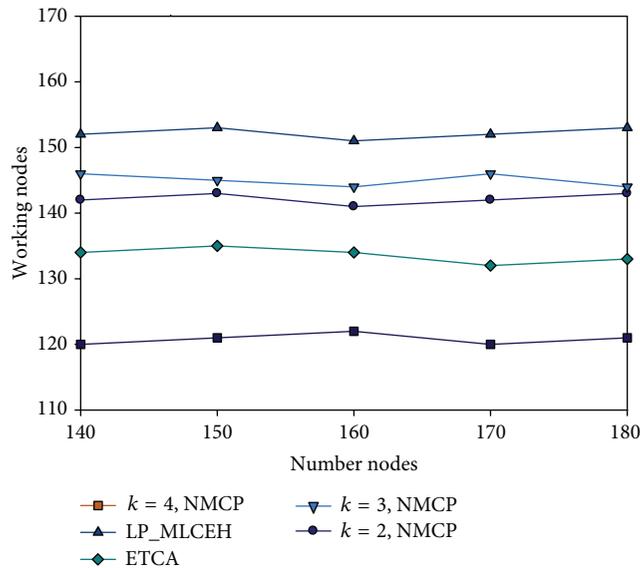


FIGURE 13: The comparison between working sensor nodes and sensor nodes.

region until the node energy is exhausted. When $t = 150$, the three algorithms' coverage rates drop quite obviously; its coverage is when $k = 2, 3, 4$, respectively, CPNMCP2 = 76.55%, CPNMCP3 = 85.91%, CPEPDM = 87.92%, CPOSCC = 94.24%, and CPNMCP4 = 98.01%. When $k = 4$, the coverage rate is higher than the average coverage rate of EPDM and OSCC algorithm, which shows that, with the same number of nodes, the coverage rate of NMCP algorithm is significantly higher than the other two algorithms, verifying the effectiveness of the algorithm proposed in this paper. Figure 13 shows the comparison curves of the working nodes number of the algorithm in this paper, the EPDM, and the OSCC algorithm on the premise of the same coverage rate. When the number of sensor nodes keeps between 140 and 180, the three

algorithms have almost steady number of sensor nodes; when $k = 2, 3, 4$, nodes number required in the algorithm in this paper generally keeps in 144, 141, and 122, while the EPDM and OSCC algorithm generally keep the number of working nodes between 132 and 150. The reason mainly lies in the fact that the algorithm in this paper finishes covering the monitored region by calculating the coverage expectation values of nodes to obtain the set of neighbour nodes in the perception radiuses of local nodes, whereas the other two algorithms finish covering the monitored region in a continuous covering manner, depending on the number of nodes. Therefore, on average, the algorithm in the paper needs less working sensor nodes than the other two algorithms by 3.49%.

6. Conclusions

First, the coverage problems and the deficiencies in the wireless sensor network were analysed and, on basis of that, this paper put forward a nonlinear multiobjective k -degree coverage preservation protocol. Second, the network model is established based on the above analysis, and the dependency relationship between the sensor node and the destination node is given; then the coverage rate and expectation value of the sensor node in monitored region are then calculated and verified; in the meanwhile the process of resolving the coverage rate for any node that is covered by multisensor nodes in the two-dimensional plane is dealt with. In terms of node energy, we have proved the relationship between the communication distance and the maximum distortion, as well as the implementation process of the NMCP protocol.

Finally, the effectiveness and feasibility of the NMCP protocol are verified by simulation experiments. Future work mainly focuses on how to achieve effective coverage on the boundary of monitored region and nonlinear coverage of irregular monitored region.

Competing Interests

The authors declare no competing interests.

Acknowledgments

The study is supported by Projects U1304603 and 61503174 supported by the National Natural Science Foundation of China; Projects 14B520099, 16A520063, and 17A520044 supported by Henan Province Education Department Natural Science Foundation; Projects 142102210471, 162102210113, and 162102410051 supported by Natural Science and Technology Research of Foundation Project of Henan Province Department of Science; Projects 1201430560 supported by Guangzhou Education Bureau Science Foundation; Projects 2016A030313540 supported by Guangzhou Education Bureau Science Foundation.

References

- [1] T. M. Chiwewe and G. P. Hancke, "A distributed topology control technique for low interference and energy efficiency in wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 8, no. 1, pp. 11–19, 2012.

- [2] Z. Y. Sun, H. Li, and H. Chen, "Optimization coverage of wireless sensor networks based on energy saving," *International Journal of Future Generation Communication and Networking*, vol. 7, no. 4, pp. 35–48, 2014.
- [3] B. Wang, K. C. Chua, V. Srinivasan, and W. Wang, "Information coverage in randomly deployed wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 6, no. 8, pp. 2994–3004, 2007.
- [4] H. M. Ammari and S. K. Das, "Critical density for coverage and connectivity in three-dimensional wireless sensor networks using continuum percolation," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 6, pp. 872–885, 2009.
- [5] Y. Yoon and Y.-H. Kim, "An efficient genetic algorithm for maximum coverage deployment in wireless sensor networks," *IEEE Transactions on Cybernetics*, vol. 43, no. 5, pp. 1473–1483, 2013.
- [6] L. Liu, X. Zhang, and H. Ma, "Percolation theory-based exposure-path prevention for wireless sensor networks coverage in internet of things," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3625–3636, 2013.
- [7] T. M. Chiwewe and G. P. Hancke, "A distributed topology control technique for low interference and energy efficiency in wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 8, no. 1, pp. 11–19, 2012.
- [8] K. Derr and M. Manic, "Wireless sensor network configuration-part II: adaptive coverage for decentralized algorithms," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 3, pp. 1728–1738, 2013.
- [9] C.-H. Tsai and Y.-C. Tseng, "A path-connected-cluster wireless sensor network and its formation, addressing, and routing protocols," *IEEE Sensors Journal*, vol. 12, no. 6, pp. 2135–2144, 2012.
- [10] X. Tang and J. Xu, "Optimizing lifetime for continuous data aggregation with precision guarantees in wireless sensor networks," *IEEE/ACM Transactions on Networking*, vol. 16, no. 4, pp. 904–917, 2008.
- [11] Z. Sun, W. Wu, H. Wang, H. Chen, and W. Wei, "An optimized strategy coverage control algorithm for WSN," *International Journal of Distributed Sensor Networks*, vol. 10, no. 7, Article ID 976307, 2014.
- [12] R. V. Sampangi and S. Sampalli, "Butterfly encryption scheme for resource-constrained wireless networks," *Sensors*, vol. 15, no. 9, pp. 23145–23167, 2015.
- [13] I. M. Santos, M. A. Dota, and C. E. Cugnasca, "Dynamic definition of the sampling rate of data in Wireless Sensor Network with Adaptive Automata," *IEEE Latin America Transactions*, vol. 9, no. 6, pp. 963–968, 2011.
- [14] L. Zhang, D. Li, H. Zhu, and L. Cui, "OPEN: an optimisation scheme of N-node coverage in wireless sensor networks," *IET Wireless Sensor Systems*, vol. 2, no. 1, pp. 40–51, 2012.
- [15] X. H. Xu, X. Y. Li, X. F. Mao, S. J. Tang, and S. G. Wang, "A delay-efficient algorithm for data aggregation in multihop wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 1, pp. 163–175, 2011.
- [16] Y. Xiao, H. Chen, K. Wu et al., "Coverage and detection of a randomized scheduling algorithm in wireless sensor networks," *IEEE Transactions on Computers*, vol. 59, no. 4, pp. 507–521, 2010.
- [17] P. K. Sahoo and W. X. Liao, "HORA: a distributed coverage hole repair algorithm for wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 14, no. 7, pp. 1397–1410, 2015.
- [18] A. Adulyasas, Z. Sun, and N. Wang, "Connected coverage optimization for sensor scheduling in wireless sensor networks," *IEEE Sensors Journal*, vol. 15, no. 7, pp. 3877–3892, 2015.
- [19] F. Z. Meng, H. Z. Wang, and H. He, "Connected coverage protocol using cooperative sensing model for wireless sensor network," *Acta Electronica Sinica*, vol. 29, no. 4, pp. 772–779, 2011.
- [20] J.-W. Lin and Y.-T. Chen, "Improving the coverage of randomized scheduling in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 12, pp. 4807–4812, 2008.
- [21] Y. S. Li, C. H. Vu, C. Y. Ai, G. T. Chen, and Y. Zhao, "Transforming complete coverage algorithms to partial coverage algorithms for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 4, pp. 695–703, 2011.
- [22] C.-J. Zhao, H.-R. Wu, Q. Liu, and L. Zhu, "Optimization strategy on coverage control in wireless sensor network based on Voronoi," *Journal on Communications*, vol. 34, no. 9, pp. 115–122, 2013.
- [23] S. Mini, S. K. Udgata, and S. L. Sabat, "Sensor deployment and scheduling for target coverage problem in wireless sensor networks," *IEEE Sensors Journal*, vol. 14, no. 3, pp. 636–644, 2014.
- [24] H. Mahboubi, K. Moezzi, A. G. Aghdam, K. Sayrafian-Pour, and V. Marbukh, "Distributed deployment algorithms for improved coverage in a network of wireless mobile sensors," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 1, pp. 163–175, 2014.
- [25] Y.-C. Tseng, P.-Y. Chen, and W.-T. Chen, "k-angle object coverage problem in a wireless sensor network," *IEEE Sensors Journal*, vol. 12, no. 12, pp. 3408–3416, 2012.
- [26] Z. B. Wang, J. L. Liao, Q. Cao, H. R. Qi, and Z. Wang, "Achieving k-barrier coverage in hybrid directional sensor networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 7, pp. 1443–1455, 2014.
- [27] X. F. Xing, G. J. Wang, and J. Li, "Polytype target coverage scheme for heterogeneous wireless sensor networks using linear programming," *Wireless Communications and Mobile Computing*, vol. 14, no. 14, pp. 1397–1408, 2014.
- [28] Z. Y. Sun, W. G. Wu, H. Z. Wang, H. Chen, and X. F. Xing, "A novel coverage algorithm based on event-probability-driven mechanism in wireless sensor network," *EURASIP Journal on Wireless Communications and Networking*, vol. 2014, article 58, pp. 1–17, 2014.
- [29] J. Zhu and B. Wang, "Sensor placement algorithms for confident information coverage in wireless sensor networks," in *Proceedings of the 23rd International Conference on Computer Communication and Networks (ICCCN '14)*, pp. 1–4, Shanghai, China, August 2014.
- [30] C. L. Yang and K.-W. Chin, "On complete targets coverage and connectivity in energy harvesting wireless sensor networks," in *Proceedings of the 22nd International Conference on Telecommunications (ICT '15)*, pp. 391–397, IEEE, Sydney, Australia, April 2015.
- [31] H. P. Gupta, S. V. Rao, and T. Venkatesh, "Sleep scheduling for partial coverage in heterogeneous wireless sensor networks," in *Proceedings of the 5th International Conference on Communication Systems and Networks (COMSNETS '13)*, pp. 1–10, Bangalore, India, January 2013.
- [32] T. M. Cheng and A. V. Savkin, "A distributed self-deployment algorithm for the coverage of mobile wireless sensor networks," *IEEE Communications Letters*, vol. 13, no. 11, pp. 877–879, 2009.
- [33] C. Yang and K.-W. Chin, "A novel distributed algorithm for complete targets coverage in energy harvesting wireless sensor

- networks,” in *Proceedings of the 1st IEEE International Conference on Communications (ICC '14)*, pp. 361–366, Sydney, Australia, June 2014.
- [34] Z. Y. Sun, H. Z. Wang, W. G. Wu, and X. F. Xing, “ECAPM: an enhanced coverage algorithm in wireless sensor network based on probability model,” *International Journal of Distributed Sensor Networks*, vol. 11, no. 6, Article ID 203502, pp. 1–11, 2015.
- [35] F. Yan, A. Vergne, P. Martins, and L. Deceusefond, “Homology-based distributed coverage hole detection in wireless sensor networks,” *IEEE/ACM Transactions on Networking*, vol. 23, no. 6, pp. 1705–1718, 2015.
- [36] M. Imran, N. Haider, and M. Alnuem, “Efficient movement control actor relocation for honing connected coverage in wireless sensor and actor networks,” in *Proceedings of the IEEE 37th Conference on Local Computer Networks Workshops (LCN Workshops '12)*, pp. 710–717, IEEE, Clearwater, Fla, USA, October 2012.
- [37] D. C. Harrison, K. G. Winston, and R. K. Rayudu, “Coverage preservation in energy harvesting wireless sensor networks for rare events,” in *Proceedings of the IEEE 40th Conference on Local Computer Networks (LCN '15)*, pp. 181–184, Clearwater Beach, Fla, USA, October 2015.
- [38] T. Shu and M. Krunz, “Coverage-time optimization for clustered wireless sensor networks: a power-balancing approach,” *IEEE/ACM Transactions on Networking*, vol. 18, no. 1, pp. 202–215, 2010.

Research Article

AR-RBFS: Aware-Routing Protocol Based on Recursive Best-First Search Algorithm for Wireless Sensor Networks

Farzad Kiani

Computer Engineering Department, Engineering and Natural Sciences Faculty, Istanbul Sabahattin Zaim University, 34303 Istanbul, Turkey

Correspondence should be addressed to Farzad Kiani; farzad.kiani@izu.edu.tr

Received 25 May 2016; Accepted 14 July 2016

Academic Editor: Fei Yu

Copyright © 2016 Farzad Kiani. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Energy issue is one of the most important problems in wireless sensor networks. They consist of low-power sensor nodes and a few base station nodes. They must be adaptive and efficient in data transmission to sink in various areas. This paper proposes an aware-routing protocol based on clustering and recursive search approaches. The paper focuses on the energy efficiency issue with various measures such as prolonging network lifetime along with reducing energy consumption in the sensor nodes and increasing the system reliability. Our proposed protocol consists of two phases. In the first phase (network development phase), the sensors are placed into virtual layers. The second phase (data transmission) is related to routes discovery and data transferring so it is based on virtual-based Classic-RBFS algorithm in the lake of energy problem environments but, in the nonchargeable environments, all nodes in each layer can be modeled as a random graph and then begin to be managed by the duty cycle method. Additionally, the protocol uses new topology control, data aggregation, and sleep/wake-up schemas for energy saving in the network. The simulation results show that the proposed protocol is optimal in the network lifetime and packet delivery parameters according to the present protocols.

1. Introduction

Wireless ad hoc networks are considered a great development in the autonomous systems technology. They are divided into two big general categories so one of them is wireless sensor networks (WSNs). These networks have played an important role in the development of intelligent systems because they are cheap, scalable, and flexible. These networks include large numbers of inexpensive, small-size sensor nodes and a few base stations (BS) or sinks so the sensor nodes have limited battery, throughput, and memory [1] and sensitive channel controls [2]. These nodes with low-powered sensing devices equipped for mobilization are deployed on animals, birds, plants, or humans to achieve better targeting and data fidelity. They form a wireless network by creating a communication system amongst themselves. Then, the sensor nodes sense and process a phenomenon and send their results to the BS or sink. WSNs can be used in different applications such as military applications, forests, monitoring systems, agriculture, and medicine. Despite the various applications of these

networks, they suffer from resource constraints as energy and memory. Therefore, researchers focus more on the constraints and balancing between resources and goals of system issues when they want to design any model for WSNs applications. One of the most important constraints is energy matter [3]. There are two types of energy consumption between sensor nodes. The first is energy consumption in communications and the second is consumption in computations. Obviously, communications consume more energy according to consumption computations. Therefore, minimizing communication costs is an important issue. Researchers propose different approaches to this goal such as energy efficiency by routing techniques, data aggregation, and duty cycle techniques. Sometimes, there are conflicts between some system targets such as reliability and energy saving. If the system designer wants high reliability performance, the sensor nodes will waste more energy. Therefore, designers must be careful about the balancing issue in the network [3].

The communication architecture and stack protocol of WSN have five layers and three planes [1, 4]. These layers are

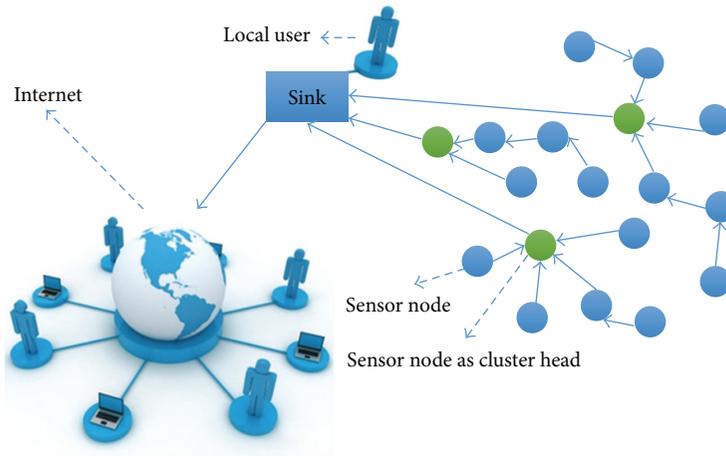


FIGURE 1: Data transmission view in WSN [4].

physical layer, data link layer, network layer, transport layer, and application layer. The planes are power management plane, mobility management plane, and task management plane. One important layer is the network layer. The network layer handles collected data from source node to destination node. Routing protocols in WSNs are different than traditional routing protocols in several respects. For example, they do not use ID-addresses or fix routes schemas in the routing processes. Therefore, the IP-based routing protocols cannot be used in the WSNs. A routing protocol should be attending to the limitations of network resources as energy, communication bandwidth, memory, and computational capabilities. Proper management of these limitations can increase the network lifetime. Additionally, a routing protocol can consider faulting tolerance, latency, data aggregation, energy efficiency, and providing internetworking with external networks-gateway principles [3, 6]. It should be noted that the data link layer handles how two nodes talk to each other and the network layer is responsible for deciding which node talks [4].

Many tasks of the above layers can be achieved by designing an aware-routing protocol and considering the importance of the balance issue between system goals and resources. In this paper, we proposed a new aware-routing protocol based on recursive searching method and implemented it for monitoring agriculture and university environments. One of the important goals in the routing algorithms is energy efficiency where the selective paths can increase network lifetime. In most applications, sensor nodes can aggregate data and send reached packets to the BS/sink. In the multihop networks, some of the sensor nodes are intermediate nodes for data transmission between two nodes. Figure 1 shows a sample of data forwarding in the cluster-based network. These collaborator nodes are called intermediate nodes. The method of finding optimized paths and selection of the intermediate nodes are the major tasks of routing protocols.

The rest of the paper is organized as follows. Section 2 describes related works in routing protocols on wireless sensor networks. Section 3 details the structure of the proposed protocol. In Section 4, we listed the simulation parameters

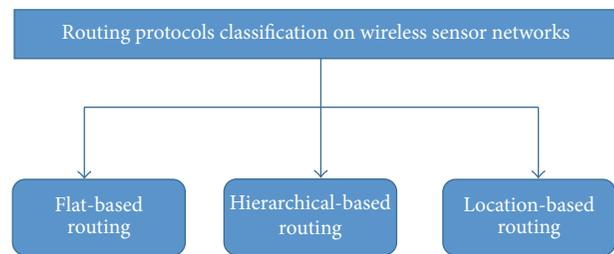


FIGURE 2: Routing protocols classification for WSNs [4].

and analysis of the results. Finally, conclusion is given in Section 5.

2. Relative Works

Many current algorithms and routing protocols can be classified into three groups as shown in Figure 2.

In the flat-based routing, the nodes forward self-data to the other nodes or BS/sink by single or multihop methods. Each sensor node has the same role in the network. As mentioned, ID is not used in the WSN structures because they consist of large numbers of nodes. Therefore, BS/sink will wait for receiving an answer from the sensor nodes when it broadcasts any query to all or selected regions of the network [8]. Accordingly, redundancy in the whole network is high and it causes more consumption of energy. This problem can be solved by data aggregation technique [1]. The flat-based routing study case is proposed in many protocols such as SPIN [9], Directed Diffusion (DD) [5], EAD [10], and GBR [11].

The flat-based routing protocols are most suitable for specific applications such as event detection. If this type of routing protocol is applied in the monitoring-based applications, then accuracy of the data is somewhat doubtful and it does not represent a real condition of the environment in transmission data packets. This problem or transmission delays in the large-scale networks are not acceptable. Hence, the flat-based routing protocols consume significant energy because a large number of nodes participate in the data transmission phase

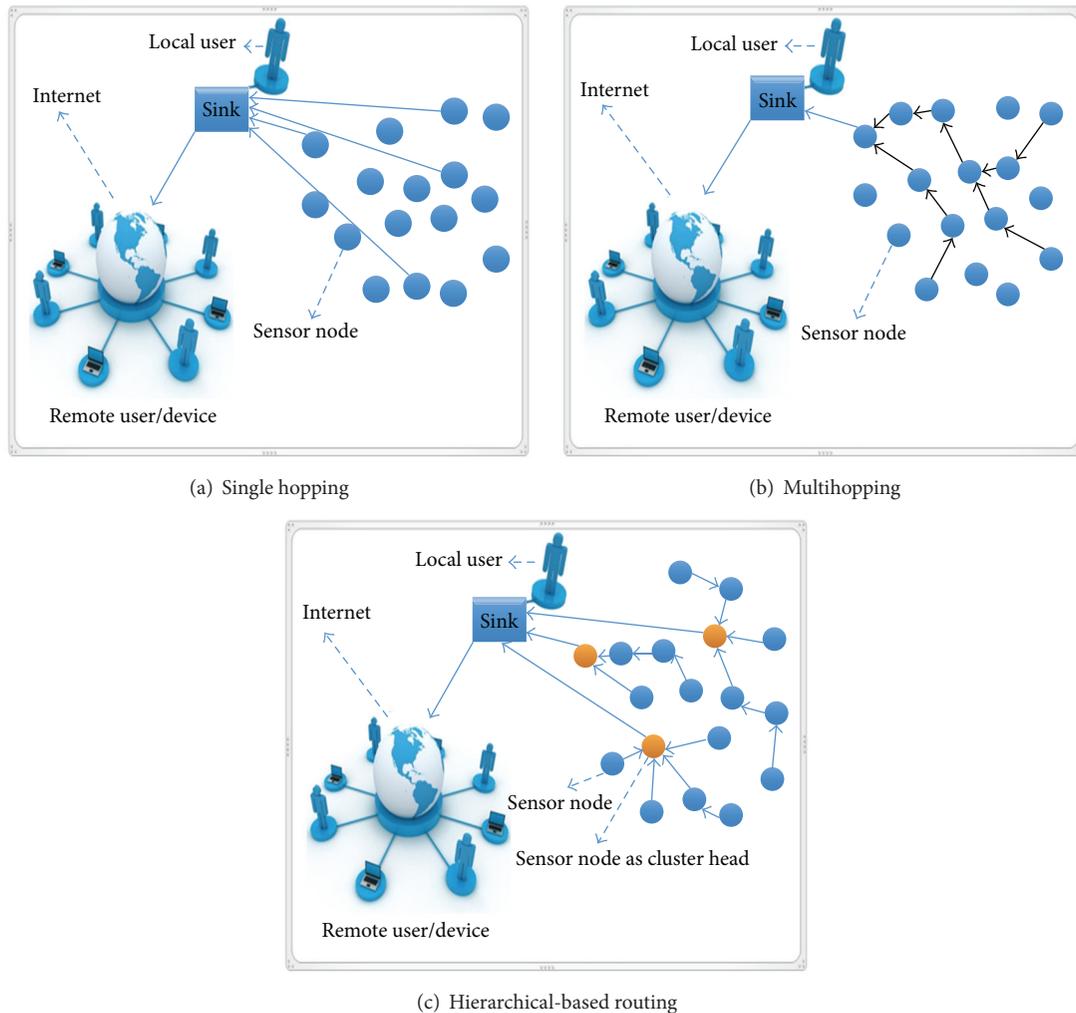


FIGURE 3: Models of routing and data transmission protocols [5].

and any node has the same role in the network. In Figure 3, we presented the three models of routing techniques. In model A, each node sends its sensed data to the sink directly without intermediate nodes. This position causes wasting energy in the whole network. Model B is the improvement of flat-based routing techniques that uses multihop method for sending data or responding to requested queries. This model reduces energy consumption significantly but, in the general case, it cannot reach energy efficiency yet. Researchers work on the energy efficiency factor in the hierarchically based routing protocols more than other protocols. They offered a new model for network configuration and named it hierarchical-based routing algorithms. This paper proposes an aware-routing protocol based on the hierarchical method. The basis of our approach is to cluster and use CH nodes as an interface between the clusters. CH nodes can communicate with other CHs or sink except for the nodes that are in the same cluster. Hence, sensor nodes are not involved in retention of routes between source nodes and sink. Generally, CHs use a CSMA MAC method and each node chooses a cluster to which it will belong and it is calculated based on the received signal

strength or its distance to the CH node. Under the same conditions, a node randomly selects a CH node and cluster. CH nodes compute a TDMA schedule for data transmission in clusters. After that, each node will know how and when it can send its data to other members. The schedule is broadcast to all nodes in the cluster except the CH node. The sensor nodes will send their data packets to CH nodes after formation clusters and allocation schedule mechanisms [6]. The network lifetime is increased and the routing protocols are converted to energy efficiency methods in the WSNs. Many protocols are proposed in the category such as HEED-NPF [12], Improved-LEACH [13], FTIEE [3], New-LEACH [14], EE-LEACH [15], and SALMA [16].

In the WSNs, almost every routing protocol needs the location information of sensor nodes. It is calculable from the distance between two special nodes. Coordinates of neighboring nodes were obtained using exchanges of some information between neighbors. If addressing scheme for a sensor network is not known, an energy efficient routing protocol can be accessible. Almost, the location-based routing protocols are proposed in the MANET [17]. However,

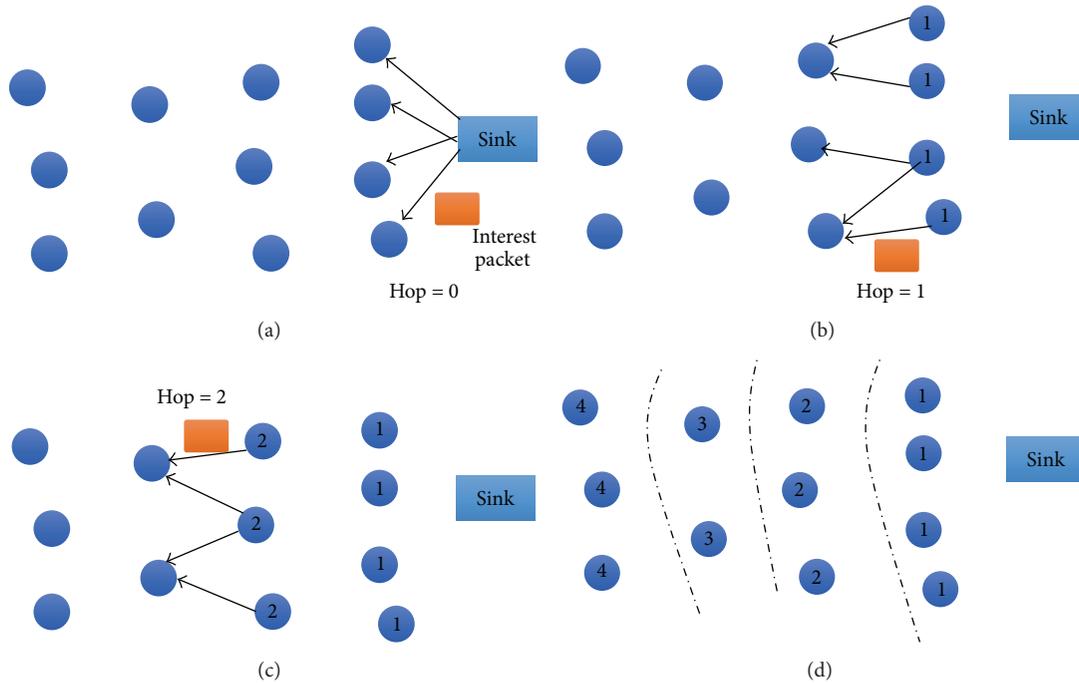


FIGURE 4: The network deployment.

they are also well applicable to WSNs where there is less or no mobility. The location of nodes can be reachable by communicating with a GPS or satellite directly but they are not inexpensive. More energy saving in the location-based protocols can be obtained by maintaining more nodes in sleep mode. The problem of scheduling of sleep period designing for each node in a localized manner was addressed in [6]. Many protocols are proposed in this category such as GAF [18], GEAR [19], and EEAR [20].

3. Designing Aware-Routing Protocol Based on Recursive Best-First Search Algorithm (AR-RBFS)

In the proposed protocol, data transmission is based on hybrid model and routes discovery is based on query model [6]. The paths which have been found by the protocol are related to destination nodes that are selected via the sink. Then, data can be collected by time-driven, query-based, or event-based methods. Additionally, a hybrid model is possible. For example, the time-driven methods in surveillance application, the event-based methods in target tracking in army applications, and the query-driven methods in habitat monitoring applications can be used. In the time-based approach, every node sends data packets periodically. In the event- and query-based approaches, if an event happens or a query is sent via the BS/sink to all sensor nodes, data transmission will be realized in the network. Data delivery is one of the important parameters in routing algorithms. The proposed protocol is implemented in two phases and discussed below.

3.1. Network Deployment Phase. Communications between sensor nodes must be clear in the network after completing the distribution of sensors in an environment. In the first phase, the sensor nodes will be deployed in the environment and they will be run in the whole network. In the second phase, condition-based environments may require the redeployment of nodes due to a high likelihood of continuous changes of network structures, topologies, and redeployment issue. The network structure is cluster-based and it will be shown as grid. Deployment of the network is done according to the following method. This method is valid and it is the same for both case studies of environments. Sink broadcasts interest message packet to the sensor nodes after deployment of the sensor nodes in the environment. This packet includes the interest hop field that has a default value of zero. The sensor nodes receive the packet and then each node adds one unit to interest hop value and saves this value as self-interest hop. Nodes that have the same interest hop value will be placed in the same layer. When the sink broadcasts the packet, it is only received by neighbors of the sink and then these neighbors broadcast it to their neighbors. This process is to be continued until all sensor nodes receive the packet. If the sensor nodes with interest hop value get any interest packet again, they remove the packet. Figure 4 shows the first phase of the proposed protocol. The nodes placement in the virtual layers is based on the closeness to the sink and number of hops. The first phase is finished in step d so all layers were created in the network. The pseudocode of network deployment is shown in Algorithm 1.

3.2. Data Transmission Phase. Our proposed protocol (AR-RBFS) uses data-centric routing schema to flow data packets

- (1) Sink broadcast interest-message to all nodes
- (2) The nodes receive the message
- (3) For all nodes
- (4) If message = not repeat
- (5) Interest hop = interest hop + 1
- (6) Else go to (7).
- (7) For all nodes
- (8) If interest hop's nodes are same
- (9) They are in a same layer
- (10) For all layers
- (11) While (duty-task-message \leq our limited number)
- (12) Send duty-task-message from any node to self-neighbors
- (13) If receive-answer-count = our limited number
- (14) While (Time is true)
- (15) Node is sleep mode
- (16) Go to (12).

ALGORITHM 1: Pseudocode of network deployment.

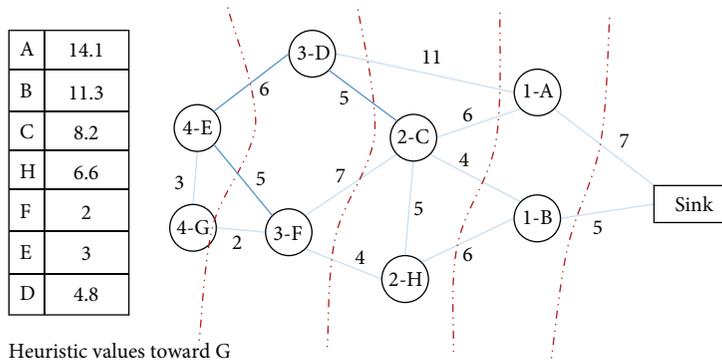


FIGURE 5: Routing and data transmission.

through multiple layers to the sink with route discovery. It is based on aware searching algorithm. Suppose we deployed our network and destination node is G as shown in Figure 5. This node is chosen via sink and is informed to network nodes based on a query. In this case, heuristic value (h_n) is calculated to all nodes and is saved for each node routing table as temporary. Each query message packet has certain lifetime that is assigned by the sink. This technique can avoid loops and energy and bandwidth wasting. Heuristic values are calculated based on direct distance costs per node to destination nodes.

This phase of the AR-RBFS has two different versions. One of them is applicable in chargeable environments. It is shown in (1). It creates a tree based on recursive search method for finding the best route between sink and destination node. It has similarity to deep search algorithms. The aim of the phase is to find the best neighbors and routes to destination nodes. If the application environment has electrical installations, we do not have an energy problem. In this case, our algorithm is run on first scenario as described in (1). In this scenario, the recursive algorithm is used in the protocol that allows the sensors to keep optimizing by using self-memory. Our algorithm selects a better route in each step

and also maintains the second best route (not all routes). A sample of all steps of the route discovery algorithm are shown in Figure 6. The steps are the same in the two versions and only the heuristic values of the calculations are different from each other. Calculation of the heuristic value for the second scenario is based on (2). Consider the following:

$$f(n_i) = h(n_i) + g(n_i), \quad (1)$$

where $h(n)$ is for heuristic costs and $g(n)$ is for path costs used. For example, in Figure 5, $g(n)$ is 6 between 1-B and 2-H and heuristic cost from B to destination node (G) is 11.3.

If the heuristic value is admissible, this proposed algorithm will be robust. However, it still has a problem in the over node regeneration because it has limited memory. Classic-RBFS [7] algorithm expands nodes in the best-first order even with a nonmonotonic cost function. The Classic-RBFS is a recursive algorithm that uses the heuristic and $g(n)$ values. $g(n)$ is the cost of path from root to "n." The Classic-RBFS is better than similar methods. Pseudocode is shown in Algorithm 2.

When the application environment does not have an energy problem, we can use the Classic-RBFS algorithm in

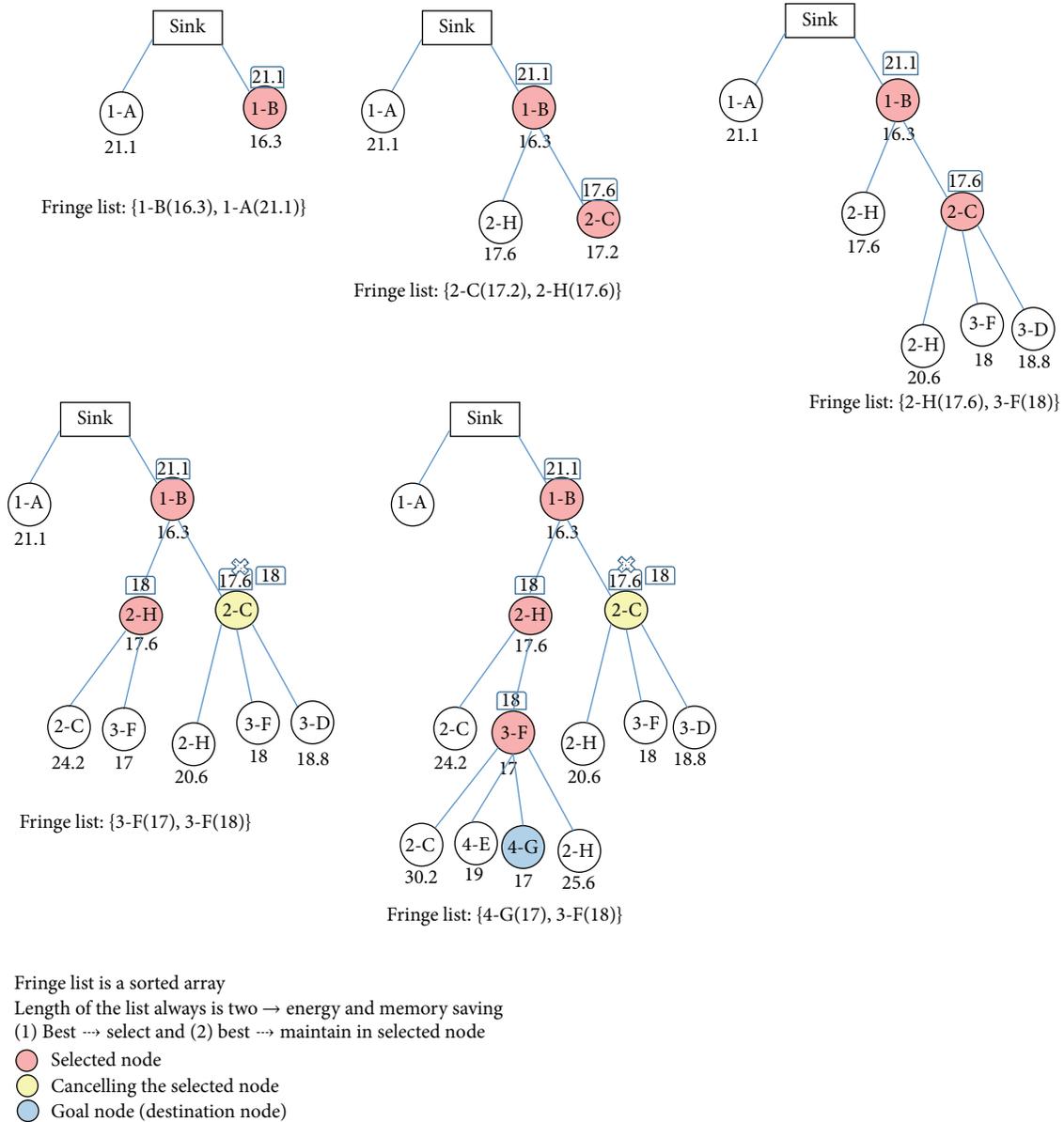


FIGURE 6: AR-RBFS algorithm steps.

routes discovery with some modification as described [7]. But it cannot be used in the environments that have energy problems. Therefore, we need another approach for routes discovery. In this case, our algorithm uses intermediate nodes by new f function given in (2). In this equation, we must consider the energy level of each sensor node ($E(n_i)$). Consider the following:

$$f(n_i) = \frac{[h(n_i) + g(n_i)]}{E(n_i)}. \quad (2)$$

Moreover, nodes have to be of a certain amount of energy to communicate. For example, if energy of any node is more than 1 nW, then the node can communicate with its neighbors based on (2). Otherwise, the nodes cannot collaborate in

the routes searching process. Therefore, the energy issue is important in the environments that are difficult to charge. Energy saving of the AR-RBFS protocol is based on duty cycle approaches. In this state, all nodes of each virtual layer can be modeled as a random graph [21]. This approach is based on duty cycle methods. The concept of the duty cycle methods is the maintenance of minimum active nodes for energy efficiency [22]. In fact, duty cycling methods focus on the networking subsystem. A good way for energy saving is to use the sleep (low-power) mode for idle sensor nodes. The proposed protocol creates a full connection topology for all active nodes in every layer. This protocol uses a virtual layers structure and it attempts to keep the network connections by maintaining enough number of sensor nodes in active mode in each layer as delegate nodes. These active nodes will have

```

RBFS( $n, B$ )
(1) if  $n$  is a goal
(2) solution  $\leftarrow n$ ; exit()
(3)  $C \leftarrow \text{expand}(n)$ 
(4) if  $C$  is empty, return  $\infty$ 
(5) for each child  $n_i$  in  $C$ 
(6) if  $f(n) < F(n)$  then  $F(n_i) \leftarrow \max(F(n), f(n_i))$ 
(7) else  $F(n_i) \leftarrow f(n_i)$ 
(8)  $(n_1, n_2) \leftarrow \text{best}_F(C)$ 
(9) while  $(F(n_1) \leq B$  and  $F(n_1) < \infty)$ 
(10)  $F(n_1) \leftarrow \text{RBFS}(n_1, \min(B, F(n_2)))$ 
(11)  $(n_1, n_2) \leftarrow \text{best}_F(C)$ 
(12) return  $F(n_1)$ 
    
```

ALGORITHM 2: Pseudocode of general RBFS algorithm [7].

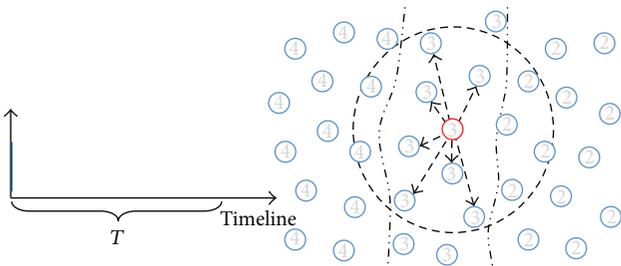


FIGURE 7: The selected node sends HELLO message to self-layer members.

communication with their sleep neighbor nodes in the same layer. In accordance with this purpose, the protocol uses two parameters. One of them is T that shows period times of duty cycling. Another variable is C and it defines the internal communications degree. Each node can go to sleep mode when it receives C numbers of task change messages from its active neighbors. The proposed approach in the paper is based on topology control technique and it uses some parameters for efficient data transmission.

Numbers of active nodes and communications in the network are increased with increasing the value of C parameter. In order to do so, each node spot considers time periods with duration T . Any node is waiting during t_v times and it is in sleep mode in this time. t_v is distributed uniformly and its value is in the range $[0, T)$. After this time, the node converts to active mode and sends HELLO message to self-neighbor. It goes into sleep mode again upon receiving the responses from the neighbors. The responses are based on C value and time is different to nodes. The C and T parameters guarantee connectivity of the network. Each active sensor node sends HELLO message packets to its sleep neighbors (Figure 7). Then, it listens to HELLO messages sent by other nodes. Assuming that the value of C parameter is three, we illustrate the operating style of the algorithm in Figure 8. The values of C and T are related to our environment conditions and parameters and also our system goals. In fact, a node will

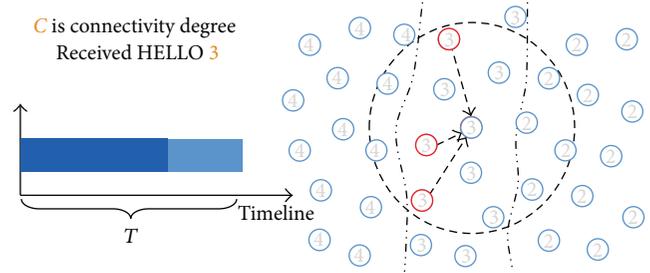


FIGURE 8: The received HELLO packets illustrate activation of other nodes (in this example, C is given the value 3).

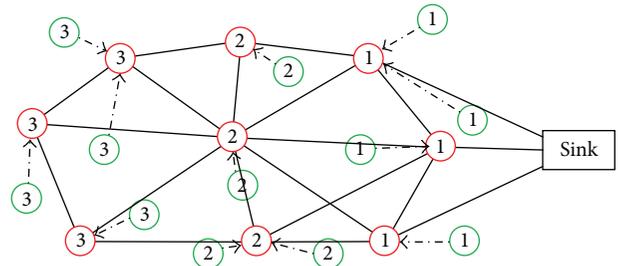


FIGURE 9: Packet routing in sleeping nodes.

be in the sleep mode after receiving an answer from the three neighboring nodes in the same layer.

Each node has waiting time (t_v) and period time (T). When it receives the activation HELLO message from its neighbors, it converts its mode to active. The active nodes will be in the activation mode for T time. The activation message numbers are reached from C parameter. For example, in Figure 8, value of C is “3.” Indeed, each node after publishing its activity sends its own HELLO packet and then goes to sleep mode after finishing its periods.

In this scenario, sleep nodes cannot be in the route discovery process by AR-RBFS algorithm but these nodes can send received packets to their neighbors active nodes when they become active. The received mode of sensor nodes is active any time even when the node is in the sleep mode. The scenario is shown in Figure 9.

4. Simulation

In the simulation of AR-RBFS protocol, AR-RBFS protocol results are compared with HEED-NF, EE-LEACH, and SALMA protocols. The output parameters are network lifetime and average packet delivery. Also, the input parameters are initial energy of each sensor node, radio and sensor energy consumption, transmit and receive/sense process costs, and buffer size (Table 1). In the simulation scenario, the sensor nodes are not mobile and they have similar architecture and design fundamental. The sensor nodes collect sensing phenomena and forward them toward BS/sink via intermediate nodes as multihopping method. A snapshot of AR-RBFS is shown in Figure 10. In this figure, the virtual layer

TABLE 1: Values of input parameters.

Initial (max) energy	0.7 J/bit	Receive buffer size	10000 bytes
Radio/sensor energy consumption	40 nJ/bit	Send buffer size	10000 bytes
Transmit process cost	40 nJ/bit	Deployment area size	(600 × 600) m
Receive/sense process cost	10 nJ/bit	Send/receive buffer counts	20
Data packet size	500 bytes	Sink position	(600 × 300) m
Sensing radius	7.5 m	Transmission radius	15 m

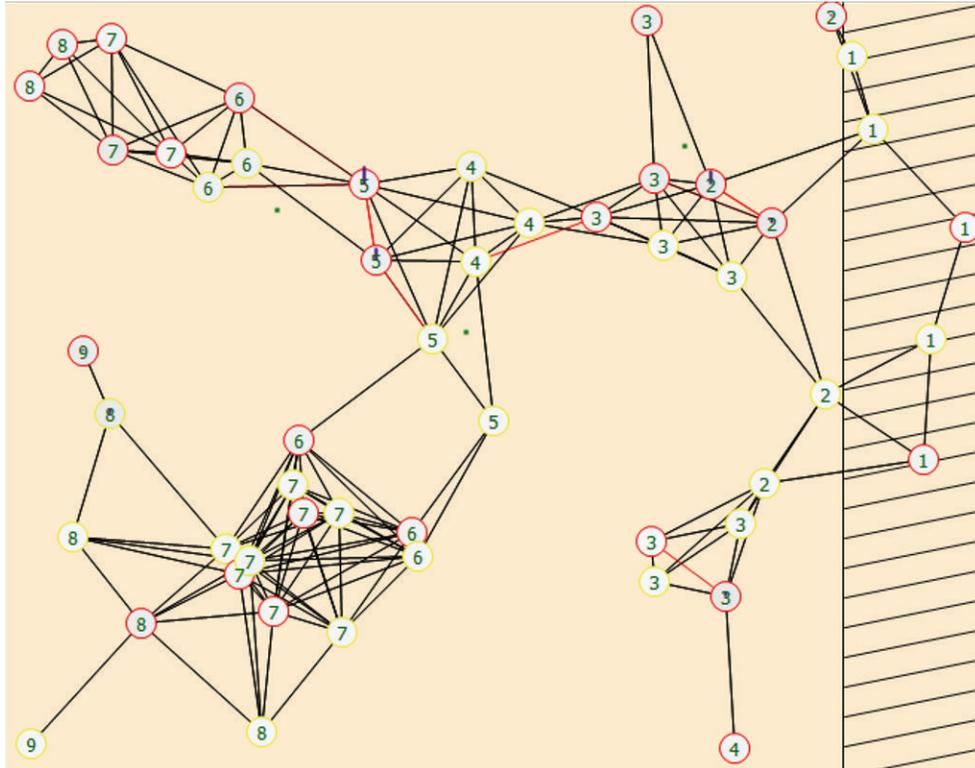


FIGURE 10: A snapshot of basic network topology in AR-RBFS protocol.

approach can appear. The proposed protocol can be available in areas such as border security.

The simulations are based on two different scenarios. The first scenario is developed for the nodes that have an unlimited energy source or easy-to-recharge batteries. They are charged by the environment energy source such as electrical installations. Another scenario is for low-power energy source environments.

The results show that AR-RBFS has a good performance in the network lifetime and average packet delivery rate. It can increase the energy saving factor using data aggregation, topology control, and sleep/wake-up methods. Network lifetime is directly related to the number of nodes. The network lifetime will be better when we use more sensor nodes. We can say that, with the increasing number of nodes, the number of received packets is increased but packet delivery rate is almost reduced because some of the factors such as increasing density of nodes, hop counts, and node failure probability are

effective. Figures 11 and 12 show simulation results on three protocols and proposed two scenario-based protocols.

5. Conclusion

This paper proposed the design of an AR-RBFS based routing protocol in two different scenarios on WSN. It is used to evaluate the power consumption and packet delivery rate of wireless sensor nodes. The algorithm computes an optimized path to route the packets from the sink to the destination node. The cluster-based structure and using the new duty cycle based energy saving technique help the network have a good performance in the output parameters (network lifetime and average packet delivery rate). Since the packets are routed through an optimized path, the energy required for transmission will be decreased; thus, the lifetime of the system is increased. Simulation results show that the proposed

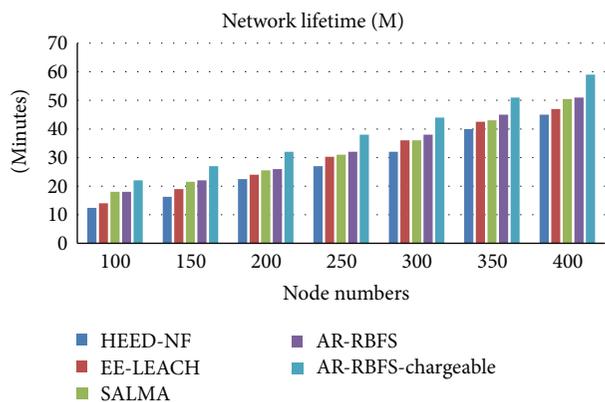


FIGURE 11: Network lifetimes in AR-RBFS (2 scenarios), HEED-NF, EE-LEACH, and SALMA.

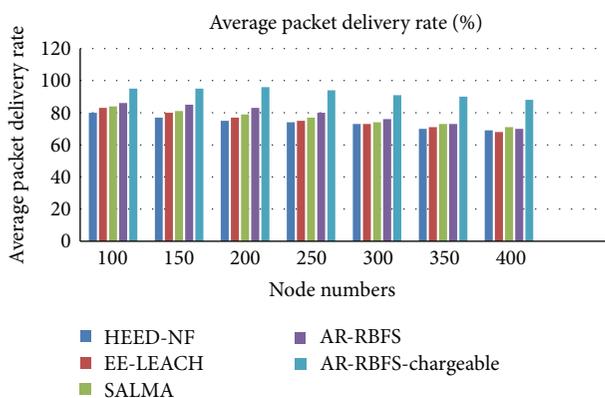


FIGURE 12: Average packet delivery rates in AR-RBFS (2 scenarios), HEED-NF, EE-LEACH, and SALMA.

AR-RBFS based approach for improving the energy saving in the WSN is better than the SALMA, EE-LEACH, and HEED-NF routing algorithms. Hence, the proposed algorithm is better than the existing algorithms. The proposed protocol for both environments can be implementable on various applications such as agriculture.

Competing Interests

The author declares that there are no competing interests.

References

- [1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.
- [2] F. Kiani, "A novel channel allocation method for time synchronization in wireless sensor networks," *International Journal of Numerical Modelling: Electronic Networks, Devices and Fields*, vol. 29, no. 5, pp. 805–816, 2016.
- [3] F. Kiani, E. Amiri, M. Zamani, T. Khodadadi, and A. Abdul Manaf, "Efficient intelligent energy routing protocol in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID 618072, 13 pages, 2015.
- [4] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–105, 2002.
- [5] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed-diffusion: a scalable and robust communication paradigm for sensor networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom '00)*, pp. 56–67, ACM, 2000.
- [6] F. Kiani, *Designing New Routing Algorithms Optimized for Wireless Sensor Network*, LAP LAMBERT Academic Publishing, Dusseldorf, Germany, 2014.
- [7] M. Hatem, S. Kiesel, and W. Rosel, "Recursive best-first search with bounded overhead," in *Proceedings of the 29th AAAI Conference on Artificial Intelligence*, vol. 29, pp. 1152–1157, 2015.
- [8] M. Maroti, "Directed flooding-routing for wireless sensor network," in *Proceedings of the ACM/IFIP/USENIX International Conference on Middleware*, vol. 2, pp. 99–114, 2004.
- [9] A. Martorosyan, A. Boukerche, and R. W. Pazzi, "A taxonomy of cluster-based routing protocols for wireless sensor networks," in *Proceedings of the International Symposium on Parallel Architectures, Algorithms, and Networks (i-span '08)*, pp. 247–253, Sydney, Australia, May 2008.
- [10] R. C. Shah and J. M. Rabaey, "Energy aware routing for low energy ad hoc sensor networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '02)*, pp. 350–355, Orlando, Fla, USA, March 2002.
- [11] L. Miao, K. Djouani, A. Kurien, and G. Noel, "A competing algorithm for gradient based routing protocol in wireless sensor networks," in *Proceedings of the International Conference on Wireless Information Networks and Systems (WINSYS '10)*, pp. 82–89, Athens, Greece, July 2010.
- [12] H. Taheri, P. Neamatollahi, M. Naghibzadeh, and M.-H. Yaghmaee, "Improving on HEED protocol of wireless sensor networks using non probabilistic approach and fuzzy logic (HEED-NPF)," in *Proceedings of the 5th International Symposium on Telecommunications (IST '10)*, vol. 2, pp. 193–198, Tehran, Iran, December 2010.
- [13] F. Xiangning and S. H. Yulin, "Improvement on LEACH protocol of wireless sensor network," in *Proceedings of the International Conference on Sensor Technologies and Applications (SENSORCOMM '07)*, pp. 260–264, Valencia, Spain, October 2007.
- [14] E. Arbab, V. Aghazarian, and A. Hedayati, "A LEACH-based clustering algorithm for optimizing energy consumption," in *Proceedings of the 2nd International Conference on Computer Science and Information Technology (ICCSIT '12)*, vol. 2, pp. 147–150, Singapore, April 2012.
- [15] N. Sharma and V. Verma, "Energy efficient LEACH protocol for wireless sensor network," *International Journal of Information and Network Security*, vol. 2, no. 4, pp. 333–338, 2013.
- [16] M. M. Umar, N. Alrajeh, and A. Mehmood, "SALMA: an efficient state-based hybrid routing protocol for mobile nodes in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2016, Article ID 2909618, 11 pages, 2016.
- [17] A. Kodole and P. Agarkar, "A survey of routing protocols in mobile ad hoc networks," *Multidisciplinary Journal of Research in Engineering and Technology*, vol. 2, no. 1, pp. 336–341, 2015.
- [18] S. Roychowdhury and C. Patra, "Geographic adaptive fidelity and geographic energy aware routing in Ad-Hoc routing," in *Proceedings of the International Conference (ACCTA '10)*, vol. 1, no. 2, pp. 309–313, August 2010.

- [19] B. Baranidharan and B. Shanthi, "A survey on energy efficient protocols for wireless sensor networks," *International Journal of Computer Applications*, vol. 11, pp. 35–40, 2010.
- [20] F. Kiani, A. Rad, M. Sis, A. Kut, and A. Alpkocak, "EEAR: an energy effective-accuracy routing algorithm for wireless sensor networks," *Life Science Journal*, vol. 10, no. 2, pp. 39–45, 2013.
- [21] S. D. Servetto and G. Barrenechea, "Constrained random walks on random graphs: routing algorithms for large scale wireless sensor networks," in *Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications*, vol. 11, pp. 12–21, September 2002.
- [22] G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella, "Energy conservation in wireless sensor networks: a survey," *Ad Hoc Networks*, vol. 7, no. 3, pp. 537–568, 2009.

Research Article

An Improved μ TESLA Protocol Based on Queuing Theory and Benaloh-Leichter SSS in WSNs

Haiping Huang,^{1,2} Tianhe Gong,^{1,2} Tao Chen,^{1,2} Mingliang Xiong,^{1,2}
Xinxing Pan,^{1,2} and Ting Dai³

¹College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

²Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, China

³Department of Computer Science, College of Engineering, North Carolina State University, Raleigh, NC 27695, USA

Correspondence should be addressed to Haiping Huang; hhp@njupt.edu.cn

Received 15 March 2016; Accepted 5 July 2016

Academic Editor: Iftikhar Ahmad

Copyright © 2016 Haiping Huang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Broadcast authentication is a fundamental security technology in wireless sensor networks (ab. WSNs). As an authentication protocol, the most widely used in WSN, μ TESLA protocol, its publication of key is based on a fixed time interval, which may lead to unsatisfactory performance under the unstable network traffic environment. Furthermore, the frequent network communication will cause the delay authentication for some broadcast packets while the infrequent one will increase the overhead of key computation. To solve these problems, this paper improves the traditional μ TESLA by determining the publication of broadcast key based on the network data flow rather than the fixed time interval. Meanwhile, aiming at the finite length of hash chain and the problem of exhaustion, a self-renewal hash chain based on Benaloh-Leichter secret sharing scheme (SRHC-BL SSS) is designed, which can prolong the lifetime of network. Moreover, by introducing the queue theory model, we demonstrate that our scheme has much lower key consumption than μ TESLA through simulation evaluations. Finally, we analyze and prove the security and efficiency of the proposed self-renewal hash chain, comparing with other typical schemes.

1. Introduction

We can imagine there will be thousands of sensors deployed in the future space, but how can we ensure the security of these sensors? Aside from confidential communications, authentication is one of the essential services in security protocols of wireless sensor networks (ab. WSNs) system [1]. If the authentication system stays defective or noneffective, attackers may launch threats to the whole network such as the wormhole attack, the man-in-the-middle attack, and the multiple identities attack. Data leakage may occur even in a military area, which can cause serious consequences. Therefore, the study of authentication system especially the broadcast authentication protocol for large-scale WSNs still remains challenging. However, restrained by the finite resources of WSNs, many previous protocols cannot be directly applied to the broadcast authentication of WSNs. For example, most protocols rely on asymmetric mechanism such

as the public key cryptography, but this mechanism has heavy communication, computation, and storage overhead, which are impractical for WSNs.

Therefore, designing a protocol that can guarantee the data integrity, confidentiality, and authentication in the broadcast has been a popular research topic in WSNs. One straightforward solution is to let the base station and all other nodes share a common broadcast authentication key, but the key will be disclosed if one of nodes is corrupt. Another solution is to use one-time key for each packet so that the leak of current key will not have a bad influence on the following packets, but the cost of frequently updating keys is unacceptable for WSNs. Perrig et al. proposed a classic broadcast authentication protocol μ TESLA [2], which has a great improvement over the original protocol TESLA [3, 4]. The contribution of μ TESLA protocol is to implement a broadcast authentication process based on the symmetric key mechanism instead of the asymmetric one, and it overcomes

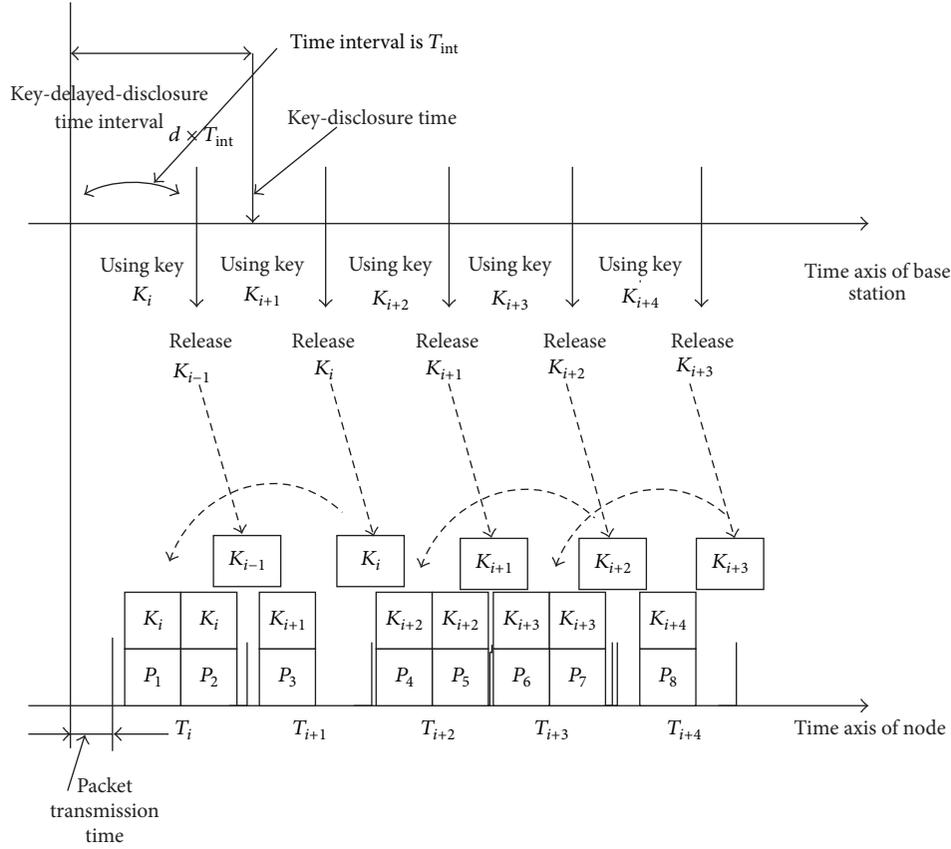


FIGURE 1: The broadcast authentication process of μ TESLA.

the problems in traditional protocols by delaying the publication of one-way hash function key. This protocol decreases the computational complexity for broadcast authentication and improves the authentication efficiency as well. In the following paragraph, we will give a brief overview of μ TESLA.

The main idea of μ TESLA is to broadcast a packet authenticated by the key K_{mac} at first and then publish K_{mac} so that there is no way to forge the broadcast packets before the publication of the key. In addition, the protocol achieves the secret sharing with the key generation algorithm shared by the entire network. The one-way hash function and the key chain mechanism can ensure the safety of keys and the tolerance of packet loss. Figure 1 illustrates the broadcast authentication process of μ TESLA.

μ TESLA protocol consists of three phases: (1) securely initializing the configuration of base station, (2) bootstrapping the new receivers, and (3) authenticating the broadcast packets. The base station generates a key pool ($K_{N-1}, K_{N-2}, \dots, K_1, K_0$) by one-way hash function in the first phase and determines the synchronization time interval T_{int} and the key-delayed-disclosure time interval $d \times T_{\text{int}}$. The synchronization time interval represents the lifetime of a broadcast key, which means the broadcast packets sent from the base station use the same key K_i in a synchronous period $[i \times T_{\text{int}}, (i + 1) \times T_{\text{int}}]$. The value of integer d should make $d \times T_{\text{int}}$ longer than the time of packet-switching between the base station and the farthest node so that all the nodes can

be ensured to have received the broadcast packet before the corresponding key is disclosed.

When the new node joins the network, μ TESLA distributes the key synchronized parameters and initialized related keys to the new node based on the SNEP protocol [3]. For example, Figure 1 shows the process of node A requesting to join the broadcast network during the time interval $[i \times T_{\text{int}}, (i + 1) \times T_{\text{int}}]$. Consider

$$\begin{aligned}
 A &\rightarrow S: (N_A \parallel D_{\text{req}}) \\
 S &\rightarrow A: (T_S \parallel K_i \parallel T_i \parallel T_{\text{int}} \parallel d), \\
 &\text{MAC}(K_{AS}, N_A \parallel T_S \parallel K_i \parallel T_i \parallel T_{\text{int}} \parallel d),
 \end{aligned} \tag{1}$$

where N_A is a nonce which is generated by A to achieve a strong freshness authentication; D_{req} is a request data packet; K_{AS} is an authentication key between A and S ; T_S is the current time; K_i is an initial key; T_i is the starting time of the current synchronization interval; T_{int} is the synchronization interval; and d is the disclosure delay. The key will be published after $d \times T_{\text{int}}$.

After receiving a broadcast packet from the base station, the receiver will judge the validity of authentication key based on the synchronization time. The node will further verify the key's validity by running the hash calculation on it. Finally, the node will use the key to authenticate the packets that have been stored in the buffer during the time interval.

In μ TESLA protocol, the publication of key is dependent on a specific time interval, which is fixed after initialization. However, we notice that the current network traffic is not stable in each time interval, and we divide this unstable traffic into two cases:

- (i) The base station broadcasts the packets frequently to the sensor nodes. In this case, the broadcast packets in one time interval will dramatically increase. If the key is still disclosed according to the original time interval, the excessive number of packets is unable to get a timely authentication and the storage space of the sensor nodes will be exhausted inevitably.
- (ii) The base station just broadcasts a few packets in a long time. In this case, it is possible that there are few packets during the fixed time interval. Consequently, the release of keys will lead to the increase of communication and computation overhead, which degrades the efficiency of key chain.

To decrease unnecessary consumption as well as to ensure security in the process of broadcast authentication, in this paper, we replace the fixed time interval with network traffic to determine the publication of broadcast key. In other words, the base station will not publish the authentication key unless it has broadcasted a certain number of packets. And our experiment has shown that some drawbacks of μ TESLA can be solved based on our mechanism.

Due to the one-way and lightweight characteristics, hash chains have been widely applied to various scenarios such as one-time password system [5], video stream security [6, 7], micropayment protocol [8], key distribution scheme [9], and broadcast authentication [10]. However, there is a trade-off between the length and the efficiency of hash chain. The exhaustion of the current hash chain will inevitably result in producing another new hash chain initialized with the public key cryptography. And this reinitialization will bring about the extra overhead of the network.

Aimed at overcoming the inadequacies of the above schemes, another concern of this paper is to design a novel self-renewal one-way hash chain scheme based on Benaloh-Leichter SSS (SRHC-BL). This scheme can effectively prolong the lifetime of network and increase the tolerance of key loss. Comparing with the typical self-renewal hash chain schemes, our approach has the benefit of higher security and less consumption of communication, computation, and storage.

Therefore, the main contribution of this paper can be summarized as follows:

- (1) A novel key distribution method based on data flow instead of fixed time interval is proposed in order to keep network stable in any situations. In addition, some special cases are discussed as the supplement.
- (2) A self-renewal one-way hash chain scheme based on Benaloh-Leichter SSS is adapted for both keeping extending life time of network and ensuring the tolerance of key loss.
- (3) Simulation experiments and theoretical analysis based on queue model are conducted to compare

the storage cost and calculation complex among our schemes and traditional μ TESLA protocol. Consequently, the result proves that our design achieves a better performance.

2. Preliminary Knowledge

2.1. Basic Concepts of Queue Theory. Queue theory, also known as random service system theory, is a theoretical basis for the queuing problem. It is one of the interdisciplinary theories of probability, statistics, and operational research. Queuing phenomenon is composed of two aspects: demand service and provide service. Here are four common queuing models as follows: M/D/1/ ∞ queuing model, M/M/1/ ∞ queuing model, M/G/1/ ∞ queuing model, and G/G/1/ ∞ queuing model.

Queuing system has the following six features, which can be applied to the broadcast authentication in WSNs:

- (i) Input process, which characterizes and describes the law of data packets coming to the random service system.
- (ii) Service time, namely, the time for the base station to authenticate the data packets.
- (iii) Waiter, namely, the base station.
- (iv) Size of line determined by the number of customers waiting to be served, which characterizes the number of valid data packets to be processed by the base station.
- (v) Customer source, which corresponds to the data packets.
- (vi) Queue rule, determined by the detail of queuing model.

2.2. Basic Concepts of Self-Renewal Hash Chain. In this section, we introduce some basic concepts of SSS and the definition of the Benaloh-Leichter SSS.

2.2.1. Concept of SSS. First, we formally define the necessary monotone access structure.

Definition 1. Given a set P , a monotone access structure on P is a family of subsets $Z \subseteq 2^P$ such that

$$\begin{aligned} A &\in Z, \\ A &\subseteq A' \subseteq P \\ &\downarrow \\ A' &\in Z. \end{aligned} \tag{2}$$

Let n be an integer, $n \geq 2$, let the set of participants be $P = \{p_1, p_2, \dots, p_n\}$, and let an access structure Z defined on P be comprised of a collection of subsets of P . Z is a monotone access structure whenever $A \in Z$ and $A \subseteq A' \subseteq P$.

Similarly, Z-SSS is a method of generating $(S, (I_1, \dots, I_n))$ such that,

- (1) for any $A \in Z$, finding the element S , given the set $\{I_i \mid i \in A\}$, is easy,
- (2) for any $A \in \bar{Z}$, finding the element S , given the set $\{I_i \mid i \in A\}$, is difficult.

The set Z is the authorized access structure or simply the access structure, S is the secret, and I_1, \dots, I_n are the shares (or the shadows) of S . The elements of the set Z are the authorized access sets of the scheme.

2.2.2. Benaloh-Leichter SSS

Definition 2. Let P be a set. The set V of variables indexed by P is the set $V = \{v_p \mid p \in P\}$.

Definition 3. Given a monotone function F on variables indexed by a set P , the access structure defined by F is the set of subsets of A of P for which F is true precisely when the variables indexed by A are set to be true.

It is clear that, for every monotone function F , the access structure defined by F is a monotone access structure.

Definition 4. For a given set P and a monotone access structure Z denoted by Z_{\min} on P , define $F(Z)$ to be the set of monotone function on $|P|$ variables such that, for every formula $F \in F(Z)$, the output of F is true if and only if the true variables in F correspond exactly to a set $A \in Z$.

Note that $F, F' \in F(Z)$ implies F and F' denote the same function. They may, however, use entirely different expressions to express this function.

The formula can be expressed using only \wedge operator and \vee operator, and it is sufficient to indicate how to “split” the secret with these operators.

Definition 5. One can recursively define the share of a secret S with respect to a formula F as follows:

$$F = \begin{cases} (S, i), & \text{if } F = v_i, 1 \leq i \leq n \\ \bigcup_{i=1}^n \text{Shares}(S, F_i); & \text{if } F = F_1 \vee F_2 \vee \dots \vee F_n \\ \bigcup_{i=1}^n \text{Shares}(s_i, F_i); & \text{if } F = F_1 \wedge F_2 \wedge \dots \wedge F_n, \end{cases} \quad (3)$$

where based on Definitions 1, 2, and 3, selecting the specific integer n and Z_{\min} , for the case $F = F_1 \wedge F_2 \wedge \dots \wedge F_n$, one can use a (k, n) -threshold secret sharing scheme for deriving some shares s_1, s_2, \dots, s_k corresponding to the secret S , and then every distinct share is assigned to each I_i . Thus one has $I_i = \{s_i \mid (s_i, i) \in \text{Shares}(S, F)\}$, for all $1 \leq i \leq n$, where F is an arbitrary formula in the set F_A .

2.2.3. Definition of Hash Chain

Definition 6. The secure hash function is a publicly known function $f_n : \{0, 1\}^* \rightarrow \{0, 1\}^k$, it takes s as an input, and the output is a bit string $f_n(s)$ of length n . In $f_n(s)$, s is generated randomly from a pseudo-random string generator. One-way hash chain can be visually expressed as follows:

$$s \xrightarrow{h(\cdot)} h(s) \xrightarrow{h(\cdot)} h^2(s) \dots \xrightarrow{h(\cdot)} h^n(s). \quad (4)$$

3. Our Scheme

3.1. The Key Distribution Algorithm Based on Data Flow. Compared with the traditional μ TESLA protocol which releases keys based on the fixed time interval, our approach releases keys according to the data flow based on the queue theory and the renewable hash chain.

3.1.1. Assumptions

(i) μ TESLA protocol is as follows:

- (1) the packet transmission time between the base station and the farthest node is T_{\max} ;
- (2) the base station releases the key every T_{int} by a fixed time interval;
- (3) the delay time of key publication is $\sigma \times T_{\text{int}}$, and it satisfies the condition that $\sigma \times T_{\text{int}} > T_{\max}$;
- (4) the verification condition is $\lfloor (T_c + \Delta - T_1) / T_{\text{int}} \rfloor < i + \sigma - 1$, where T_c is the current time, Δ is the maximum clock difference, T_1 is the start time, and i is the i th interval time.

(ii) The improved broadcast authentication protocol based on the queue theory and the renewable hash chain is as follows:

- (1) the maximum speed (or frequency) for the base station to send packets is $V_{s_{\max}}$;
- (2) the maximum transmission speed (or frequency) in WSNs is $V_{t_{\max}}$;
- (3) the communication radius of the base station is R_{bs} ;
- (4) the base station releases the authentication key every N_{int} packets based on data traffic;
- (5) the delay of data flow of key publication is $N_{\text{int}} + \theta$, and it satisfies the condition that $(N_{\text{int}} + \theta) / V_{s_{\max}} > R_{\text{bs}} / V_{t_{\max}}$;
- (6) the verification condition is $\lfloor (N_c - N_1) / N_{\text{int}} \rfloor < \lfloor i + \theta - 1 \rfloor$, where N_c is the identification number of packets that is currently received, N_1 is the ID number of first packet received, and i is the i th time interval of data flow.

3.1.2. The Process of Key Distribution Based on Data Flow. The process of broadcast authentication based on queue theory and renewable hash chain is shown in Figure 2. Comparing with Figure 1, we can see the difference between μ TESLA and

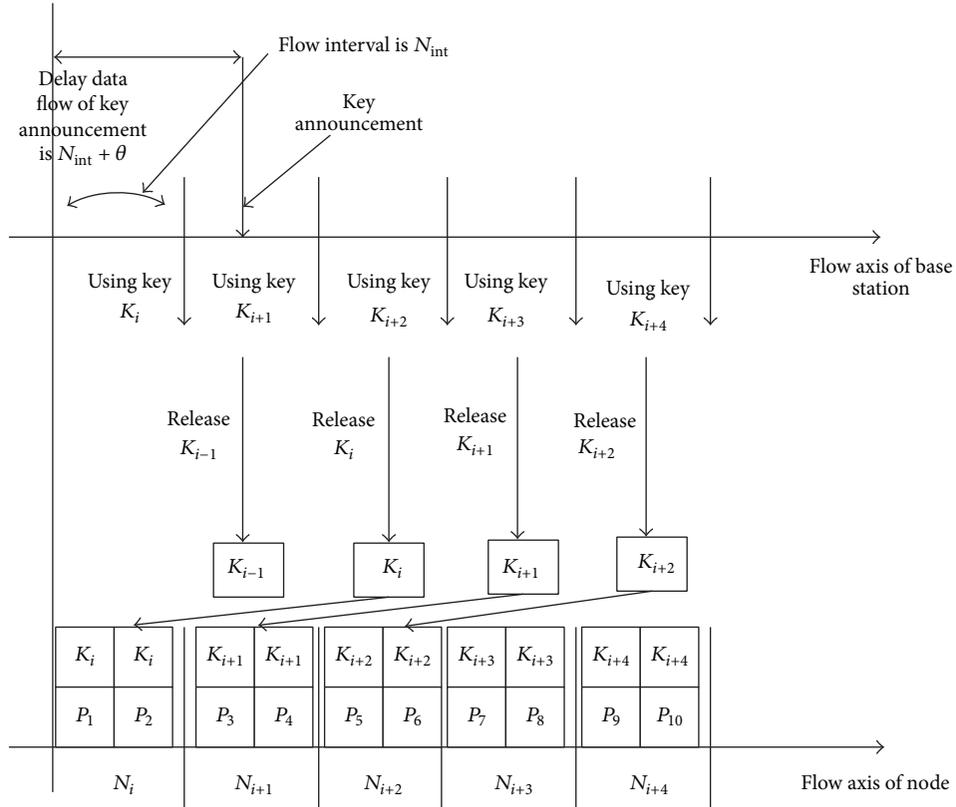


FIGURE 2: The process of broadcast authentication based on queue theory.

ours; μ TESLA maps the key distribution to the time domain, while ours maps the key distribution to the flow domain.

3.1.3. Several Cases to Discuss

Case 1. If the base station has not broadcasted a packet after a long period, and the number of packets broadcasted has not achieved a certain threshold, the base station will not release the key during this long period, which disables the node to authenticate the buffered packets. In this case, we can set a time threshold T (T is the upper bound of broadcast key lifetime). So after time T , the base station is required to release key no matter whether the condition is satisfied.

Case 2. It is very common to have packet loss in WSNs. Consider the following case: the base station will not send packets in a long period and thus the key for the next round will not be released either, but unfortunately, at this time, one node lost the current authentication key, which implies that this node cannot authenticate the remaining packets in the buffer any more. In terms of this case, we set the interval time $2T$ for the node to wait, where T is the upper bound of broadcast key lifetime. If the waiting time exceeds $2T$, the node can send the request message to the base station for the key of current round.

Case 3. Synchronization problem: how do we know which packet should be authenticated by which type of key? We use the counting mechanism to solve this problem. That is, the

broadcast packet sent by the base station is counted from 0 to N and authentication key is also numbered from 0 to N so that we can create the relations between the packet and the key by simply mapping.

3.2. A Self-Renewal Hash Chain Based on Benaloh-Leichter SSS. In this section, we propose a novel self-renewed hash chain based on Benaloh-Leichter SSS. This scheme has three phases: the hash chain initial phase, the hash chain usage phase, and the hash chain extension phase. Let C and R denote communication initiator and the recipient, respectively.

3.2.1. Initial Phase. In the initial phase, C and R are synchronized in time, and there is a maximum error time denoted as Δ ; R can reject the message which exceeds the time Δ plus the acceptable transmission delay.

- (1) The initiator C generates an initial random value s as the seed of the first hash chain, and then C uses the preloaded hash function to compute n hash value of the first hash chain. Consider

$$s \xrightarrow{h(\cdot)} h(s) \xrightarrow{h(\cdot)} h^2(s) \cdots \xrightarrow{h(\cdot)} h^n(s). \quad (5)$$

- (2) Then, C selects Z_{\min} based on Benaloh-Leichter SSS and a new random value s' to generate n hash value of the next hash chain. Consider

$$s' \xrightarrow{h(\cdot)} h(s') \xrightarrow{h(\cdot)} h^2(s') \cdots \xrightarrow{h(\cdot)} h^n(s'). \quad (6)$$

(3) Therefore, according to the Benaloh-Leichter SSS, C takes $h^n(s')$ as the secret S , divides it into n parts as the set V , and then defines the set $F(Z)$ as the set of formula on set V . Further, we select an arbitrary formula F in the set F_A . In this case, according to Z_{\min} we can obtain Shares (S, F) of the secret S . Thus, the shares corresponding to the secret S in the access structure Z are distributed as shadows I_1, I_2, \dots, I_n .

3.2.2. Usage Phase

- (1) Before the usage phase, C and R have confirmed the initial time T_0 , and meanwhile the value $h^n(s)$ and the hash function have been preloaded in R securely, as well as the message authentication code $MAC_0(h^{n-1}(s) \oplus I_1)$. During the usage phase, the hash value is used from $h^{n-1}(s)$ (firstly) to s (finally) corresponding to the time period $T_0 + i^* \Delta$ ($1 \leq i \leq n$).
- (2) In the time $T_0 + \Delta$, C releases the Msg_1 and its corresponding message authentication code MAC_1 to R , the formats of Msg_1 and MAC_1 are shown, respectively, as follows:

$$\begin{aligned} &Msg_1(T_0 + \Delta, h^{n-1}(s), I_1, MAC_1), \\ &MAC_1(h^{n-2}(s) \oplus I_2). \end{aligned} \quad (7)$$

So in the time $T_0 + i^* \Delta$ ($1 \leq i \leq n$), C will compute and release

$$\begin{aligned} &Msg_i(T_0 + i^* \Delta, h^{n-i}(s), I_i, MAC_i), \\ &MAC_i(h^{n-i-1}(s) \oplus I_{i+1}), \end{aligned} \quad (8)$$

where Msg_i is the content of current message and MAC_i is used to verify MAC_{i-1} .

- (3) For the i th authentication, after R receives the Msg_i and MAC_i , R will calculate the difference between the last time of receiving packets and the current time of receiving packets. If the difference has not exceeded Δ , R will carry out the following steps:
 - (a) Compute and verify whether $h(h^{n-i}(s))$ is equal to $h^{n-i+1}(s)$, where $h^{n-i+1}(s)$ is the valid hash value stored in the last process. If it is equal, R saves it.
 - (b) Compute and verify whether $I_i \oplus h^{n-i}(s)$ is equal to MAC_{i-1} . If it is, R saves MAC_i and I_i .

On the other hand, if the difference exceeds Δ ,

- (a) C drops $h^{n-i}(s)$ and I_i and saves MAC_i ; then it will wait until the next authentication process, which is assumed as the j th authentication where $i < j$;
- (b) compute and verify whether $h^{j-i+1}(h^{n-j}(s))$ is equal to $h^{n-i+1}(s)$, where $h^{n-i+1}(s)$ is the valid hash value stored in the last process; if it is equal, R saves it;

- (c) compute and verify whether $h^{n-j}(s) \oplus I_j$ is equal to MAC_{j-1} ; if all checks are valid, R verifies C successfully and then stores the shadow I_i .

The hash chain usage phase has a detailed description in μ TESLA. If the hash chain is exhausted, the protocol goes into the hash chain extension phase.

3.2.3. Extension Phase. When one hash chain has been exhausted, R has stored n shadows I_i . One thing we need to notice is that even though the number of shadows that R has stored is less than n (as long as the number is not less than k), we can still recover the final secret S . The detailed description is as follows.

- (1) Based on the shadows I_1, I_2, \dots, I_n , we can easily deduce Shares (S, F) corresponding to the secret S with the (k, n) -threshold secret sharing scheme.
- (2) With the Shares (S, F) , we can simply recover the secret S . In other words, we have obtained the tail of the next hash chain $h^n(s')$. Then, a new hash chain can be applied in the right way, and we can use the same protocol in the next hash chain in order to achieve the purpose of self-renewed one.

Therefore, this protocol provides an on-demand hash chain extension without exhaustion, so the hash chain is able to work smoothly and infinitely.

4. Performance Analysis

4.1. The Key Distribution Algorithm Based on Data Flow. (1) Our algorithm releases the keys based on the data flow instead of the original timeline and takes full account of the uneven distribution of arrival of the packets in the network.

(2) Valid packets simulation in the μ TESLA protocol: many simulation techniques in [11, 12] are introduced to wireless sensor networks to help researchers to understand the behavior of the network which is hard to capture in situ. In this paper, we use Matlab to simulate the four queuing models of $M/D/1/\infty$, $M/M/1/\infty$, $M/G/1/\infty$, and $GI/G/1/\infty$, respectively. We take the base station as the waiter and the broadcast packets as the customer source, so the service time obeys the distribution of the packets to be processed and broadcasted by the base station and customer source obeys the distribution of arrival of packets. By considering practical situations, we give an example of packets arriving intensively. The arrival of data packets of $M/D/1/\infty$, $M/M/1/\infty$, and $M/G/1/\infty$ obeys Poisson distribution with the randomly selected parameter $\lambda = 0.5$, while $GI/G/1/\infty$ obeys the general random distribution. We set a fixed time interval T_{int} as 60 s and the numbers of valid packets N_{str} in T_{int} as 20, and the simulation time was half an hour. If the number is over 20, we would consider it as invalid one. There are two reasons for that. First, overly late authentication would cause the large storage overhead caused by the accumulated packets in the node buffer. Second, the message is more likely to be vulnerable to chosen plaintext attacks. It can also be proved that the conclusions of simulation experiments will not change by altering the values of parameters such as λ and T_{int} .

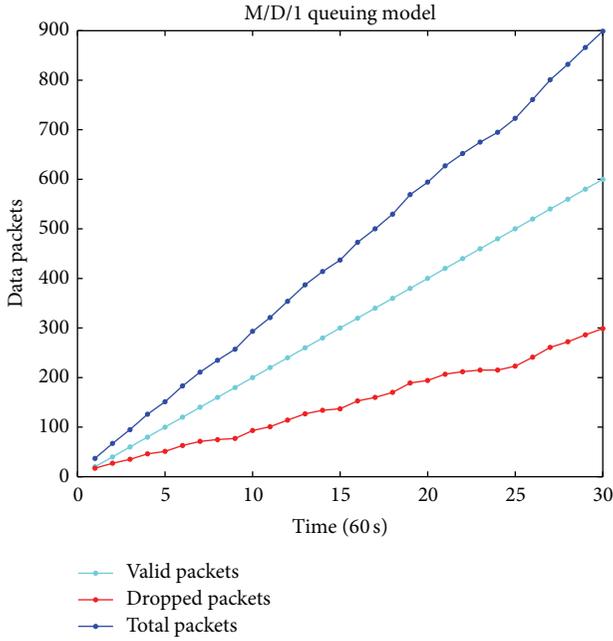


FIGURE 3: Packets of M/D/1.

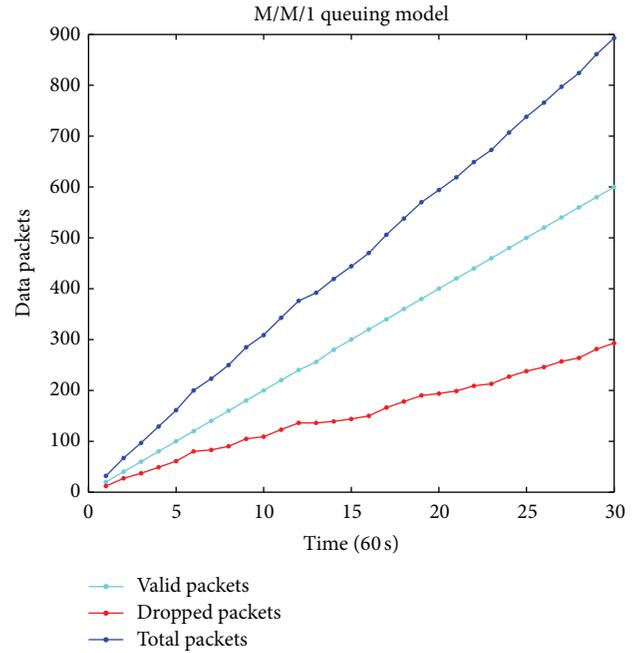


FIGURE 4: Packets of M/M/1.

(3) Simulation comparison of key packets consumed: we use Matlab to simulate the four queuing models of M/D/1/∞, M/M/1/∞, M/G/1/∞, and GI/G/1/∞, respectively, and we take the example of packets arriving sparsely. (a) The arrival of packets of M/D/1/∞ obeys the Poisson distribution with parameter $\lambda = 0.1$ and the service time obeys the uniform distribution with a fixed value $t = 1$ s. (b) The arrival of packets of M/M/1/∞ obeys the Poisson distribution with parameter $\lambda = 0.1$ and the service time obeys the Poisson distribution with parameter $\mu = 20$. (c) The arrival of packets of M/G/1/∞ obeys the Poisson distribution with parameter $\lambda = 0.1$ and the service time obeys the general random distribution. (d) The arrival of packets of GI/G/1/∞ and the service time obey the general random distribution. We set a fixed time interval $T_{\text{int}} = 60$ s, and the data flow interval is $N_{\text{int}} = 20$; the simulation time was ten hours.

- (i) In terms of the intensive rate of packets arrival, based on the fixed time interval, the simulation results of valid data packets, dropped packets, and total packets for 4 queuing models M/D/1/∞, M/M/1/∞, M/G/1/∞, and GI/G/1/∞ are shown in Figures 3–6, respectively.
- (ii) In terms of the sparse rate of packets arrival, we draw a comparison between μ TESLA (based on the fixed interval) and our protocol (based on the data flow). The simulation results of key consumption for 4 queuing models M/D/1/∞, M/M/1/∞, M/G/1/∞, and GI/G/1/∞ are shown in Figures 7–10, respectively.

From Figures 3–6, we notice that the intensive rate of broadcast packets will cause the packets to be cached in the nodes and unable to be authenticated timely, which eventually results in the loss of packets. Also, the probability of

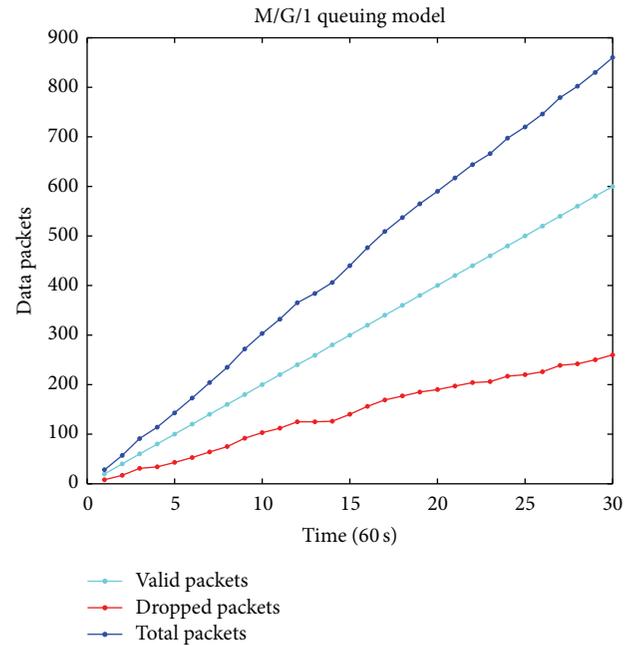


FIGURE 5: Packets of M/G/1.

choosing plaintext attack will become large if the number of packets exceeds the threshold N_{str} .

Furthermore, from Figures 7–10, the key consumption of our proposal is much lower than that of μ TESLA. Consequently, the life cycle of the key chain would be prolonged, and the network overhead would be reduced.

(4) The calculation complexity of the proposed algorithm is low. From Figures 1 and 2, we can find that there is no fallback process in both μ TESLA protocol and our algorithm.

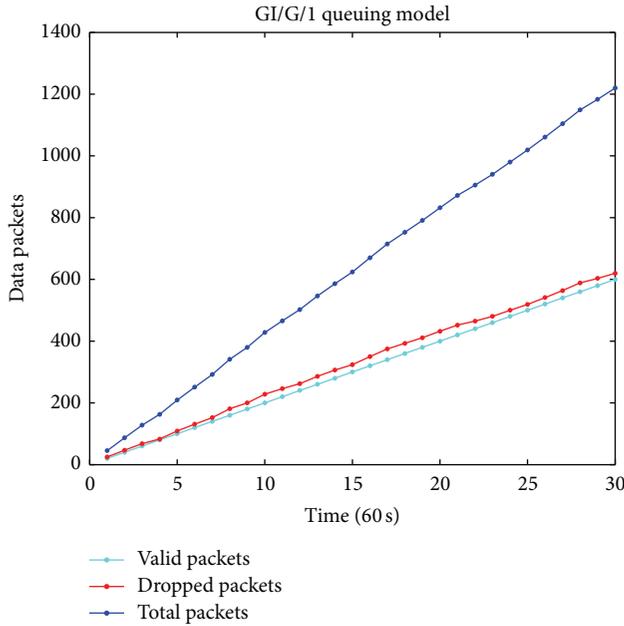


FIGURE 6: Packets of GI/G/1.

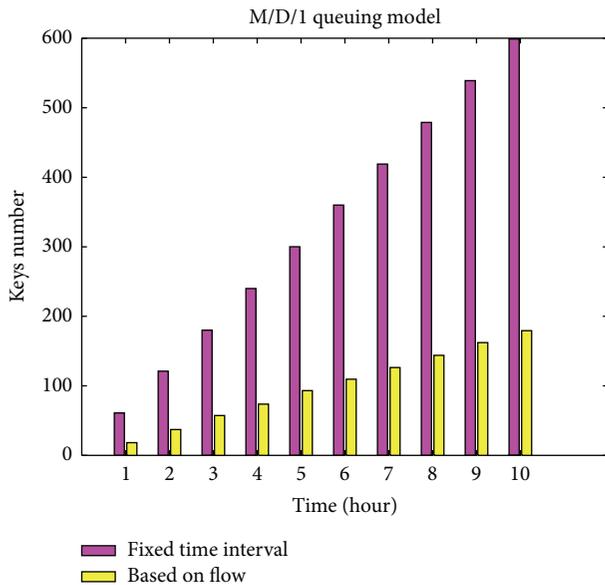


FIGURE 7: Keys consumption of M/D/1.

Although different network environments can contribute to different consumption of calculation, the proposed algorithm and μ TESLA both keep $O(n)$, where n is the number of hash calculations during authentication processes. However, in the protocol of multilevel μ TESLA [13], repeated hash operations are conducted to guarantee life time of keys at the expense of large amounts of calculations. For instance, m denotes the time of high-level calculation while n denotes that of low-level calculation in a 2-level μ TESLA process, which leads to $m \cdot n$ times of calculation. When $n = m$, the complexity achieves $O(n^2)$; the order of magnitudes increases sharply and

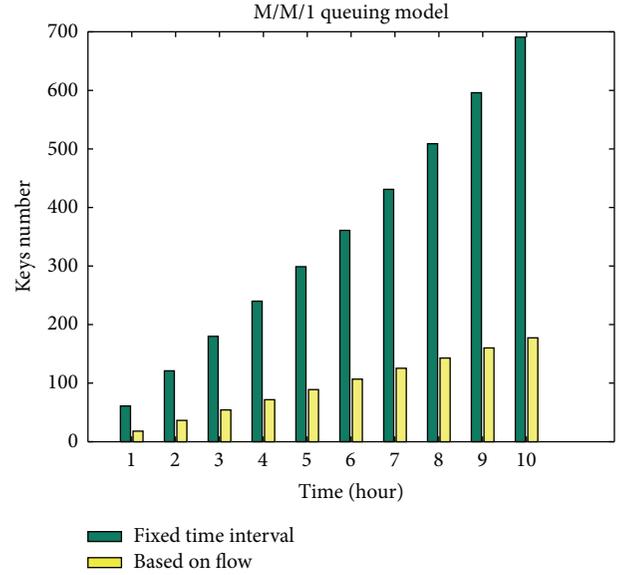


FIGURE 8: Keys consumption of M/M/1.

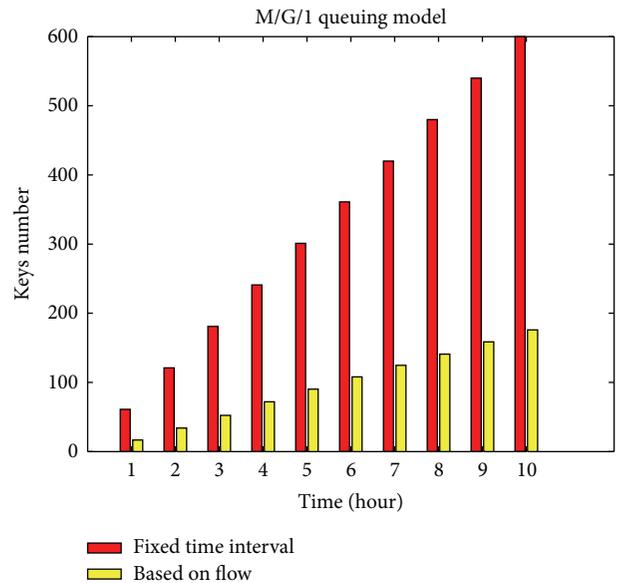


FIGURE 9: Keys consumption of M/G/1.

contributes to high calculation complexity if n becomes large. The variation tendency can be seen in Figure 11.

4.2. A Self-Renewal Hash Chain Based on Benaloh-Leichter SSS. In this section, we will present the security and performance analysis of the proposed hash chain in Section 3.

4.2.1. Security. The security of this scheme is based on one-way function and Benaloh-Leichter SSS. The purpose of XOR with hash value is to maintain the integrity and confidentiality of shadows. And the purpose of delaying key publication is to achieve nonrepudiation.

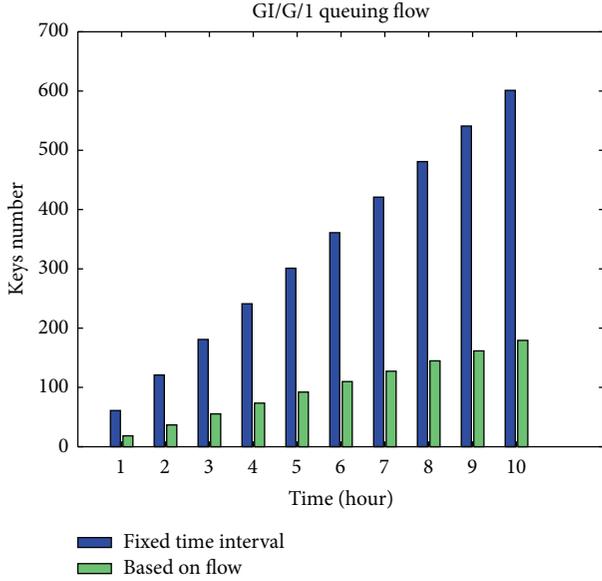


FIGURE 10: Keys consumption of GI/G/1.

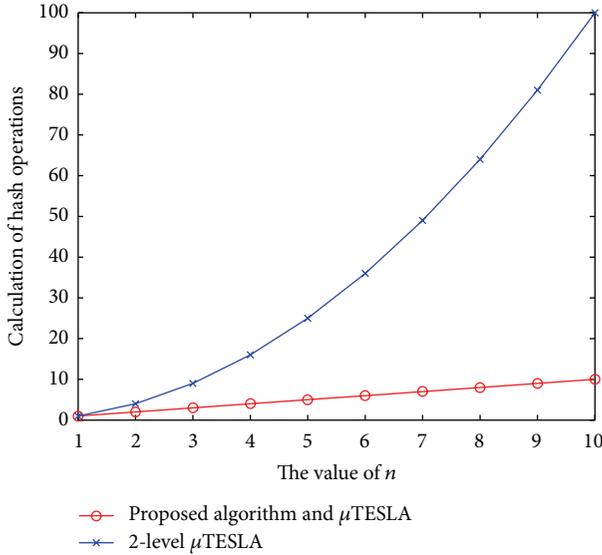


FIGURE 11: The calculation of three algorithms.

Meanwhile, Benaloh-Leichter SSS can efficiently generate a much richer family of access structures than the current schemes, and it is convenient to view an access structure as a function. Any monotone Boolean function over n variables can be computed by a monotone formula. Thus, every access structure can be realized by the scheme of Benaloh-Leichter SSS. On the other hand, for every set that does not belong to the access structure, the elements in the set do not have any information on s_i ; hence they will not reveal any information about secret S .

Also in the phase of authentication, the tolerance of packet loss or fault is embodied in our proposal. However, in Benaloh-Leichter SSS, even some s_i was dropped or lost; secret S can still be verified by other valid s_i as long as the number of shadows is not less than k .

Moreover, dual authentication in our scheme can strengthen the security and integrity. The first authentication is that whether $h^{n-i}(s)$ and I_i are received in a valid interval and they will not be stored unless both of them are verified correctly. And the second authentication is to judge whether $h^{n-i}(s)$ is valid according to $h^{n-i+1}(s)$ which has been stored in the first authentication and whether I_i is valid by the exclusive-OR function. The shadow I_i will be accepted only if the packet passes the dual authentication.

Finally, our self-renewal hash chain has satisfactory confidentiality. However, the shadow I_i exists in the packet with the form of plaintext and the attacker can obtain the key shadow information by snooping the packet. However, the attacker is unlikely to recover the secret S unless he or she can get more than k pieces of shadow, which obviously increases the difficulty. And even though the attacker can finally recover the secret S , he or she is still unable to produce the fake broadcast packets to play the role of the base station. The reason is that the secret S , namely, $h^n(s')$, is the tail of the next hash chain, which can only be used to authenticate the subsequent keys. And due to one-way feature of the hash function, the attacker cannot generate $h^{n-1}(s'), h^{n-2}(s'), \dots, s'$, so he or she is unable to fake the packet to deceive other sensor nodes. If the attacker does, these nodes can easily detect the validity of packets with $h^n(s')$.

4.2.2. Complexity. In this part, we will analyze the performance of our proposal. Before that, we first define some parameters which are mentioned as follows:

m : the output of hash function which is an m -bit string,

n : the length of hash chain,

i : the number of secret shadows in SRHC-BL,

M : the computation consumption of the hash function,

N : the computation consumption of the union operation,

$R, R_A, R_{A'}$: the computation consumptions of generating a random number in RHC, ERHC, and SUHC (or SRHC), respectively,

A, A' : the computation consumption of obtaining one bit from a random number by hard core predicate in SUHC and SRHC, respectively,

C, I, P : the computation consumption of obtaining Shares(S, F), computing the shadows I_i , and picking secret shadows s_i from I_i in SRHC-BL successively,

E : the computation consumption of XOR,

L_M : the communication or memory consumption of m (bit),

L_s : the communication or memory consumption of the seed of hash chain,

L_r : the communication or memory consumption of the generated random number,

L_I : the communication or memory consumption of shadows I_i in SRHC-BL,

L_e : the communication or memory consumption of the secret shadows s_i in SRHC-BL.

Then, we compare the computation, communication, and storage cost of our scheme SRHC-BL with the current schemes RHC, ERHC, SUHC, and SRHC. The comparison results are shown as follows.

RHC is as follows:

Computation:

$$\frac{1}{2}(m^2 + 9m)M + 2mR. \quad (9)$$

Communication:

$$2L_M + 3m \times L_r + 6m - 2. \quad (10)$$

Storage:

$$2L_s + 3L_r + (m + 6) \times L_M + m. \quad (11)$$

SUHC is as follows:

Computation:

$$\frac{1}{2}(m^2 + 12m - 2) \cdot M + mR_A + mA. \quad (12)$$

Communication:

$$(6m - 1) \cdot L_M + 2m \cdot L_r. \quad (13)$$

Storage:

$$2(L_s + L_r) + (m + 6)L_M + m. \quad (14)$$

ERHC is as follows:

Computation:

$$\frac{1}{2}(n^2 + 5n + 5m + 5[\log_2 m] + 5) \cdot M + 2(m + [\log_2 m] + 1) \cdot R + 2N. \quad (15)$$

Communication:

$$2(n + m + [\log_2 m] + 1) \cdot L_M + (m + [\log_2 m] + 1) \cdot L_r. \quad (16)$$

Storage:

$$(n + 3m + [\log_2 m] + 1) \cdot L_M + m \times (1 + 2L_r). \quad (17)$$

SRHC is as follows:

Computation:

$$\frac{1}{2}(m^2 + 11m - 2) \cdot M + m \cdot R_{A'} + mA'. \quad (18)$$

Communication:

$$4m \cdot L_M + 2m \cdot L_r. \quad (19)$$

Storage:

$$2L_s + 3L_r + (3 + m)L_M + m. \quad (20)$$

SRHC-BL is as follows:

Computation:

$$\frac{1}{2}(n^2 + 7n - 2)M + 2nE + n(I + P) + C. \quad (21)$$

Communication:

$$(4n - 2) \cdot L_M + 2n \cdot L_I. \quad (22)$$

Storage:

$$(n + 3) \cdot L_M + n \cdot L_I + i \cdot L_e + 2m. \quad (23)$$

For simplicity, we assumed that $m \approx n$, $R \approx R_A \approx R_{A'}$, $A \approx A'$, $M > N$, $M > C > I > P$, and $L_M \gg L_s \approx L_r \approx L_I > L_c$, so that it is easy to know the performance of our SRHC-BL relative to RHC, ERHC, SUHC, and SRHC. Through comparison, we can draw the following conclusion: the consumption of SRHC-BL in the initialization phase is much less than other schemes, while, in the phase of key distribution and authentication, SRHC-BL's consumptions of communication and storage are a little more than SRHC's but much less than RHC's, ERHC's, and SUHC's.

5. Related Work

5.1. Improved μ TESLA Protocol. Many hybrid broadcast authentication protocols have been proposed. Reference [14] proposed a broadcast authentication protocol with Bloom Filter compression to mainly reduce error rate of data broadcasting. Reference [15] introduced a multiuser broadcast authentication protocol to synchronously meet the requirements of multiuser. A lightweight secure authentication protocol was proposed in [16], which mainly focuses on the storage performance optimization. Reference [17] is a μ TESLA-like scheme based on symmetric keys, but the signature takes a large storage cost. A secure protocol named GPLD (Global Partition, Local Diffusion) was proposed in [18]; this scheme based on the symmetric encryption system and the geographical location information allows the different multicast group to exist in wireless sensor networks, and nodes can also act as the broadcast source and relay. On the basis of [18, 19] a broadcast authentication scheme based on users, which achieves the promising security, scalability, and performance, was proposed. Reference [13] proposes an enhanced broadcast authentication protocol based on multi-level μ TESLA, however, whose overhead has not achieved the satisfactory efficiency. Reference [20] put forward a broadcast authentication scheme with the Merkle tree; although it can

effectively resist the DoS attacks, the authentication delay seems to be inappropriate for most applications. Taking the tolerance of data loss into account, [21] presents a link-layer packet recovery algorithm which improves the reliability and minimizes the latency.

So we can see that μ TESLA protocol and its improved protocols are the mainstream of broadcast authentication protocol research in wireless sensor networks.

5.2. Reinitializable Hash Chain. Hash function has the characteristics of one-wayness and high computational efficiency. Therefore, the hash chain mechanism has been widely used into many encryption applications and services. Furthermore, the length of the hash chain is limited, which makes it difficult to meet the requirement of sustainability. And extending the length of the hash chain is difficult because a secure channel established through other encryption mechanisms is needed, and a large overhead is required.

To solve this contradiction, researchers have proposed some hash chain schemes. Goyal introduced the reinitializable hash chain (RHC) scheme with the idea that a fire-new RHC will be regenerated safely and undeniably when the old RHC is exhausted. On the basis of RHC, [22] put forward the elegant reinitializable hash chain (ERHC) scheme, which uses the one-way hash function to regenerate the hash chain safely and infinitely instead of using the public key mechanism. However, due to the publication part of S_U to authentication for the next seed of hash chain, it is likely to be susceptible to the chosen plaintext attack. Reference [23] proposed the self-updating hash chain (SUHC) scheme based on the hard core predicate algorithm. The solution of SUHC is that the sender distributes the first chain's every key value with one bit in the seed of second. In such a way, while the first one is exhausted, the receiver would receive all bits of second chain's seed. On the basis of [23, 24] the self-renewal hash chain (SRHC) scheme was proposed. The main difference between the above two schemes is the generation method of the random numbers. The security distributions of the seed of SUHC and SRHC rely on the security distribution of k random numbers, where k denotes the length of chain. Furthermore, these two schemes require all the received random numbers to satisfy integrity and inevitability. And then the seed of a new chain can be reconstructed. However, both of them have given up the original fault tolerance of hash chain. Based on SUHC, [25] put forward a novel self-updating hash chain (NSUHC) scheme; afterwards, according to NSUHC, [26] proposed a new self-updating hash chain based on erasure coding (SUHC-EC). In the former scheme, the seed of a new hash chain is transformed from k -dimensional to n -dimensional ($k < n$) and the latter one is transformed from one-dimensional to n -dimensional. Therefore, two schemes select one of the n random values to release without repeating. The new seed can be resumed after k times. These two schemes seem to realize the renewable hash chain, but actually there is no difference from the conventional hash chain. Reference [27] proposed a new self-updating hash chain based on

fair exchange idea (SRHC-FEI); this scheme uses one-time signature key to encrypt the first bit of the seed of a new hash chain in transmission when releasing the new hash value each time. It can enhance the security and fairness, but it inevitably increases the system time delay. After analysis, we can see that this scheme is also an enhanced scheme more than a strict hash chain renewable construction scheme.

From the analysis of the above typical schemes we can see that they all transform every bit of the new chain's seed into a random number and make the security of the new seed dependent on the security of distributed random numbers. Besides, they can successfully regenerate the new seed only when they receive all the random numbers correctly. As a result, they all weaken the security and increase the consumptions for reinitialization. On the other hand, NSUHC and SUHC-EC only expand the dimension of the seed of a new hash chain, but compared with RHC and ERHC and so forth, they increase the chance of encountering the man-in-the-middle attack. Above all, from a perspective of application of a hash chain, only RHC, ERHC, SUHC, and SRHC belong to the renewable construction scheme of hash chain.

6. Conclusion

This paper proposes a novel secret key release scheme based on the data flow, which addresses some problems of traditional key release schemes based on the fixed time interval, effectively improves the efficiency of the utilization of keys, prolongs the life cycle of hash chain, and reduces the network communication overhead and computational cost.

Moreover, we consider the scenario that when the number of packets using the same key to authenticate is greater than the threshold N_{str} , it may disable some packets to get a timely authentication and thus results in the loss of data. Also, the probability of chosen plaintext attack will be increased. To solve these problems, we introduce the flow threshold mechanism to prevent the attacks and enhance network security as well.

After that we put forward a new renewable hash chain based on Benaloh-Leichter SSS (SRHC-BL). The renewable process can be executed infinitely. And we have theoretically proved that SRHC-BL has better performance on integrity, confidentiality, and nonrepudiation by adopting the delay disclosure and one-wayness. In addition, our scheme can also tolerate message loss or fault due to the property of the shadows in Benaloh-Leichter SSS. Furthermore, the dual authentication and transformed secret shadows enable our scheme to have higher security than other schemes. Finally, the analysis of complexity has proved that SRHC-BL has less consumption than those typical schemes.

Competing Interests

The authors declare that there are no competing interests regarding the publication of this paper.

Acknowledgments

This work was supported in part by grants from the National Natural Science Foundation of China (nos. 61373138 and 61272422), the Key Research and Development Program of Jiangsu Province (Social Development Program, no. BE2015702), the Natural Science Foundation of Jiangsu Province (no. BK20151511), Postdoctoral Foundation (nos. 2015M570468 and 2016T90485), the Sixth Talent Peaks Project of Jiangsu Province (no. DZXX-017), the Fund of Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks (WSNLBZY201516), and Science and Technology Innovation Fund for Postgraduate Education of Jiangsu Province (no. KYLX15_0853).

References

- [1] L. Xu, M. Wen, and J. Li, "A bidirectional broadcasting authentication scheme for wireless sensor networks," in *Proceedings of the IEEE Conference on Collaboration and Internet Computing (CIC '15)*, pp. 200–204, Hangzhou, China, October 2015.
- [2] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: security protocols for sensor networks," *Wireless Networks*, vol. 8, no. 5, pp. 521–534, 2002.
- [3] A. Perrig, R. Canetti, D. Song, and J. D. Tygar, "Efficient and secure source authentication for multicast," in *Proceedings of the Network and Distributed System Security Symposium (NDSS '01)*, pp. 35–46, San Diego, Calif, USA, February 2001.
- [4] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in *Proceedings of the IEEE Symposium on Security and Privacy (S&P '00)*, pp. 56–73, Berkeley, Calif, USA, May 2000.
- [5] M. H. Eldefrawy, M. K. Khan, and K. Alghathbar, "One-time password system with infinite nested Hash chains," in *Security Technology, Disaster Recovery and Business Continuity*, pp. 161–170, Springer, Berlin, Germany, 2010.
- [6] S.-H. Ou, C.-H. Lee, V. S. Somayazulu, Y.-K. Chen, and S.-Y. Chien, "On-line multi-view video summarization for wireless video sensor network," *IEEE Journal on Selected Topics in Signal Processing*, vol. 9, no. 1, pp. 165–179, 2015.
- [7] G. Oligeri, S. Chessa, R. Di Pietro, and G. Giunta, "Robust and efficient authentication of video stream broadcasting," *ACM Transactions on Information and System Security*, vol. 14, no. 1, article 5, pp. 1–25, 2011.
- [8] A. Huszti, "Anonymous multi-vendor micropayment scheme based on bilinear maps," in *Proceedings of the International Conference on Information Society (i-Society '14)*, pp. 25–30, IEEE, London, UK, November 2014.
- [9] X. Zhang and J. Wang, "An efficient key management scheme in hierarchical wireless sensor networks," in *Proceedings of the International Conference on Computing, Communication and Security (ICCCS '15)*, pp. 1–7, Pamplemousses, Mauritius, December 2015.
- [10] D. Liu and P. Ning, "Multilevel μ TESLA," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 3, no. 4, pp. 800–836, 2004.
- [11] H. Jiang, J. Zhai, S. K. Wahba, B. Mazumder, and J. O. Hallstrom, "Fast distributed simulation of sensor networks using optimistic synchronization," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 11, pp. 2888–2898, 2014.
- [12] J. H. Lee, L. H. Kim, and T. Y. Kwon, "FlexiCast: energy-efficient software integrity checks to build secure industrial wireless active sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 1, pp. 6–14, 2016.
- [13] X. Li, N. Ruan, F. Wu, J. Li, and M. Li, "Efficient and enhanced broadcast authentication protocols based on multi-level μ TESLA," in *Proceedings of the 33rd IEEE International Performance Computing and Communications Conference (IPCCC '14)*, pp. 1–8, Austin, Tex, USA, December 2014.
- [14] Y.-S. Chen, I.-L. Lin, C.-L. Lei, and Y.-H. Liao, "Broadcast authentication in sensor networks using compressed bloom filters," in *Distributed Computing in Sensor Systems*, pp. 9–111, Springer, Berlin, Germany, 2008.
- [15] K. Ren, S. Yu, W. Lou, and Y. Zhang, "Multi-user broadcast authentication in wireless sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 8, pp. 4554–4564, 2009.
- [16] M. Sharifi, S. S. Kashi, and S. P. Ardakani, "LAP: a lightweight authentication protocol for smart dust wireless sensor networks," in *Proceedings of the International Symposium on Collaborative Technologies and Systems (CTS '09)*, pp. 258–265, Baltimore, Md, USA, May 2009.
- [17] C. Benzaid, S. Medjadba, A. Al-Nemrat, and N. Badache, "Accelerated verification of an ID-based signature scheme for broadcast authentication in wireless sensor networks," in *Proceedings of the IEEE 15th International Conference on Computational Science and Engineering (CSE '12)*, pp. 633–639, Nicosia, Cyprus, December 2012.
- [18] K. Ren, W. Lou, B. Zhu, and S. Jajodia, "Secure and efficient authentication in wireless sensor networks allowing ad hoc group formation," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 4, pp. 2018–2029, 2009.
- [19] X. Cao, W. Kou, L. Dang, and B. Zhao, "IMBAS: identity-based multi-user broadcast authentication in wireless sensor networks," *Computer Communications*, vol. 31, no. 4, pp. 659–667, 2008.
- [20] R. D. Pietro, F. Martinelli, and N. V. Verde, "Broadcast authentication for resource constrained devices: a major pitfall and some solutions," in *Proceedings of the 31st IEEE International Symposium on Reliable Distributed Systems (SRDS '12)*, pp. 213–218, Irvine, Calif, USA, October 2012.
- [21] C. Qiu, H. Shen, S. Soltani, K. Sapra, H. Jiang, and J. O. Hallstrom, "CEDAR: a low-latency and distributed strategy for packet recovery in wireless networks," *IEEE/ACM Transactions on Networking (TON)*, vol. 23, no. 5, pp. 1514–1527, 2015.
- [22] Y.-C. Zhao and D.-B. Li, "An elegant construction of re-initializable hash chains," *Journal of Electronics & Information Technology*, vol. 28, no. 9, pp. 1717–1720, 2006.
- [23] H. Zhang and Y. Zhu, "Self-updating hash chains and their implementations," in *Web Information Systems-WISE 2006*, pp. 387–397, Springer, Berlin, Germany, 2006.
- [24] H. Zhang, X. Li, and R. Ren, "A novel self-renewal hash chain and its implementation," in *Proceedings of the 5th IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC '08)*, pp. 144–149, Shanghai, China, December 2008.
- [25] M.-Q. Zhang, B. Dong, and X.-Y. Yang, "A new self-updating hash chain structure scheme," in *Proceedings of the International Conference on Computational Intelligence and Security (CIS '09)*, pp. 315–318, Beijing, China, December 2009.

- [26] Z. Wei, "Self-updating hash chains based on erasure coding," in *Proceedings of the International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE '10)*, pp. 173–175, Changchun, China, August 2010.
- [27] X.-Y. Yang, J.-J. Wang, J.-Y. Chen, and X.-Z. Pan, "A self-renewal hash chain scheme based on fair exchange idea(SRHC-FEI)," in *Proceedings of the 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT '10)*, pp. 152–156, Chengdu, China, July 2010.

Research Article

Disjoint Key Establishment Protocol for Wireless Sensor and Actor Networks

AtaUllah Ghafoor,^{1,2} Muhammad Sher,² Muhammad Imran,³ and Imran Baig⁴

¹Department of Computer Science, National University of Modern Languages, Islamabad 44000, Pakistan

²Department of Computer Science and Software Engineering, International Islamic University, Islamabad 44000, Pakistan

³College of Computer and Information Sciences, King Saud University, Riyadh 12372, Saudi Arabia

⁴Department of Electrical & Computer Engineering, College of Engineering, Dhofar University, 211 Salalah, Oman

Correspondence should be addressed to AtaUllah Ghafoor; ataullah4us@gmail.com

Received 25 March 2016; Accepted 5 May 2016

Academic Editor: Fanli Meng

Copyright © 2016 AtaUllah Ghafoor et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Key distribution is essential for providing secure communication between commercial and sensitive applications of wireless sensor and actor networks (WSANs). It becomes more challenging when any of the intermediate sensor nodes is compromised by the adversaries as the messages carrying secure keys will be exposed and links will be unreliable. This paper presents a Disjoint Key Establishment Protocol (DKEP) that does not require transmitting keys across the nodes. In DKEP, each node is preloaded with one row and one column from a matrix. After the deployment, indices for row and column are exchanged between the two nodes and values at intersection of row and column index will be used to calculate the key on each node. DKEP is verified by performing formal analysis using Rubin Logic and validated using simulations in NS-2. Simulation results demonstrate the effectiveness and efficiency of DKEP compared to contemporary schemes in terms of reducing storage and communication cost and improving resilience against node compromise attacks. Moreover, the proposed scheme is implemented in a group-based mobile application scenario for secure message exchange.

1. Introduction

Recent developments in sensing, actuation, computing, communication, and networking have led to the emergence of wireless sensor and actor networks (WSANs) [1–3] that allow autonomous and intelligent interaction with the environment. These networks employ number of miniaturized sensors with scarce resources (in terms of computation, communication, and energy) besides fewer powerful actor nodes. Sensors continuously monitor an event of interest and report it wirelessly to corresponding actors for coordinated action. Example applications include border protection, search and rescue, fire containment, and autonomous monitoring and maintenance of lifeline infrastructures [4]. Figure 1 depicts a typical WSAN environment. While most of these applications are critical, however, nodes are vulnerable to a number of attacks including node compromising, traffic capturing, and DOS attacks [5, 6]. Among others, secure key establishment

is one of the most prominent barriers in deploying WSAN for sensitive applications.

Key establishment is indispensable for secure communication between distant nodes because key is used for encryption and decryption [7, 8]. In many applications, matrix-based key distribution schemes are preferred because transmission of actual key is not required and nodes can independently calculate keys. Most of the existing matrix-based schemes either share randomly selected rows and columns values [9–11] from precalculated secret and public matrices or some values based on a pattern [12] from the matrices.

The main problem in these schemes is that a compromised node can reveal the rows and columns transmitted through it. At intermediate nodes, message is decrypted to plain text and then encrypted again using symmetric key of next node on the path. These messages cannot be encrypted because there is no prior end to end key between two distant nodes. The link is compromised before its establishment

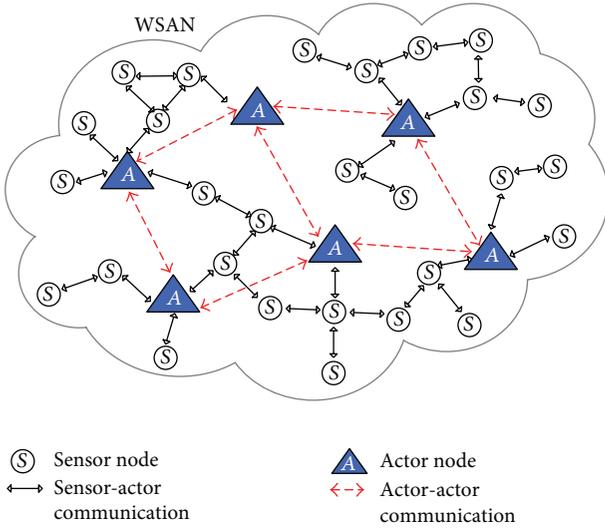


FIGURE 1: An autonomous WSN environment for sensitive applications.

and many schemes such as [8–12] suffer from key exposure problem. Moreover, most of the existing schemes only rely on nonformal (i.e., simulations) approaches for validation and hardly employ formal techniques for verifying the correctness.

Formal methods are advanced mathematical mechanism that are based on some computer tools for designing a system model and then apply the formal specifications. The use of formal specifications has evolved in past few years with the advent of new analyzing tools to verify the characteristics of network and security protocols. Informal methods cause a number of ambiguities during the implementation phase where bugs are produced due to misinterpretation of steps [13]. Different formal modeling techniques including BAN Logic [14], PCL [15], and Rubin Logic [16] are used for formalizing the security schemes for the verification of authentication, integrity protection, send, receive, formatting, and key freshness.

This paper presents a Disjoint Key Establishment Protocol (DKEP) for secure communication between nodes. In DKEP, only row and column indices are exchanged along with nonce and timestamp between sender and receiver instead of complete row and column values. After receiving these credentials, sender and receiver identify the common values at the intersection of rows and columns and then obtain the symmetric key taking XOR with exchanged credentials. Both the nodes simultaneously obtain keys in a disjoint manner. It increases the security level because adversary will not be able to reveal the key from the transmitted messages because actual key is never transmitted on the network. We use formal approach to verify the correctness and validate the performance of the proposed protocol. Rubin logic [16] is used for formal modeling of DKEP protocol for verifying and analyzing the operation. Moreover, performance of DKEP is validated using simulation in NS-2.35. Simulation results demonstrate the performance supremacy of DKEP over contemporary schemes in terms of resilience against malicious nodes, storage, and communication costs. The performance

results encourage using DKEP for many applications. We also implement DKEP to demonstrate its suitability for securing mobile applications.

The rest of the paper is organized as follows: Section 2 highlights some of the existing schemes related to this work. System model is described in Section 3. Section 4 describes the working of DKEP in various scenarios. Formal modeling and analysis of the proposed protocol using Rubin Logic are presented in Section 5. Simulation results and analysis are discussed in Section 6. Implementation of the proposed protocol on android based mobile phones is discussed in Section 7. Finally, the conclusion and future works are discussed in Section 8.

2. Related Work

Key management is mandatory for secure sharing of information among different nodes in the network by using encryption and decryption. Generally, key management schemes can broadly be categorized into asymmetric and symmetric, while the former provides higher degree of confidence to communicate securely over any open channel since it does not require transmitting private key for message decryption. However, it may not be suitable for resource-constrained sensor nodes as it requires high processing time (i.e., computationally slow) which reduces transmission speed. On the other hand, later is more appropriate for WSN as it uses same shared key for message encryption and decryption. However, secure key distribution over insecure channels is a challenging task especially in mission-critical application as some of the intermediate nodes might be compromised by the adversary. Few recent studies have investigated the challenges of key management in WSN [17, 18]. However, most of the existing key establishment schemes are proposed in the context of wireless sensor networks (WSNs) which may not be directly applicable to WSN because of various unique characteristics such as actor mobility. Unlike most existing schemes, we focus on devising a matrix-based key establishment scheme that does not require directly exchanging the key between the communicating nodes. Therefore, we limit our discussion on matrix-based symmetric key establishment schemes afterwards.

Blom's proposed a matrix-based symmetric key establishment scheme that contained a public matrix G with a size of $N \times (\lambda + 1)$, where N is network size and λ is level of security because Blom's scheme was λ -secure [9]. Secret matrix D of size $(\lambda + 1) \times (\lambda + 1)$ and matrix $A = (D \cdot G)^T$ of size $N \times (\lambda + 1)$ is generated where T is transpose. Sink node preloads a row from a matrix A and a column from matrix G in each sensor. During key K_{ik} establishment between sender S_i and receiver S_k , each node exchanges its column with neighbors in a plain text. Key is calculated by multiplying A 's row with G 's column as described in (1), where r and m are row and column indices. Due to symmetric matrix, keys calculated at both nodes are the same: that is, $K_{ik} = K_{ki}$:

$$K_{ik} = [A_{r,1}, A_{r,2}, \dots, A_{r,\lambda+1}] \begin{bmatrix} G_{1,m} \\ \vdots \\ G_{\lambda+1,m} \end{bmatrix}. \quad (1)$$

Blom's scheme is λ -secure and an adversary needs to compromise λ nodes to compromise rows of matrix A for calculating a number of keys between any two nodes in the network. Blom's scheme increases memory storage, communication, and computation overheads. However, our scheme only exchange single rows and column indices and hence reduces storage, communication, and computational overheads. Moreover, our scheme is not λ nodes resistant and adversary cannot access other keys by compromising even a large number of nodes. The author in [10] proposed a modified Blom's scheme (MBS) where Vandermonde matrix [19] was replaced by adjacency matrix. It was filled with 1's

$$\begin{array}{c}
 \left| \begin{array}{cccccc} 28 & 1 & 1 & 28 & 28 & 28 \\ 1 & 28 & 28 & 1 & 28 & 28 \\ 1 & 28 & 28 & 28 & 1 & 28 \\ 28 & 1 & 28 & 28 & 28 & 28 \\ 28 & 28 & 1 & 28 & 28 & 1 \\ 28 & 28 & 28 & 28 & 1 & 28 \end{array} \right| \\
 \text{Adjacency Matrix}
 \end{array}
 \left| \begin{array}{cccccc} 28 & 1 & 1 & 28 & 28 & 28 \\ 1 & 28 & 28 & 1 & 28 & 28 \\ 1 & 28 & 28 & 28 & 1 & 28 \\ 28 & 1 & 28 & 28 & 1 & 28 \\ 28 & 1 & 28 & 28 & 28 & 28 \end{array} \right| \\
 \text{Public Matrix } G
 \end{array}
 \left| \begin{array}{ccc} 3 & 5 & 2 & 7 \\ 5 & 6 & 9 & 1 \\ 2 & 9 & 3 & 5 \\ 7 & 1 & 5 & 4 \end{array} \right| \\
 \text{Secret Matrix } D
 \end{array}
 \left| \begin{array}{cccc} 26 & 9 & 5 & 24 \\ 3 & 20 & 24 & 5 \\ 18 & 18 & 14 & 26 \\ 22 & 20 & 28 & 14 \\ 16 & 26 & 16 & 22 \\ 12 & 8 & 10 & 12 \end{array} \right| \\
 A = (D \cdot G)^T \text{ mod } 29
 \end{array} \quad (2)$$

Sink node loads only a single row from matrix A where row id equals sensor id; that is, second row is loaded in sensor 2. In this scheme, column from adjacency matrix is not loaded in sensor because it can be calculated at node during key establishment. Sender S_i can set up a key by multiplying row R_i and column C_k whereas receiver S_k multiplies row R_k and column C_i where i and k are node ids and indices for rows and columns as well. It reduces storage overhead but the scheme is still λ -secure. Moreover, if an adversary captures a row of matrix A from some compromised node then key could be calculated by multiplying with column from identity matrix. Column id can be extracted from sender or receiver ID.

Khan et al. proposed a symmetric key establishment scheme [20] where a symmetric matrix is used along with a generator matrix having maximum rank distance (MRD) codes. A symmetric matrix D of size $k \times k$, where k represents number of symbols over a finite field. Sensors of count n are deployed in t groups where each group contains $(k - \lambda)$ nodes with $\lambda \geq 1$. It also prepares t number of generating matrix G with a size of $k \times N$ where N represents degree of finite field. First group will get a vector g_1 of N elements from this matrix and same is the case for other $(t - 1)$ groups. After that key spaces matrix $A_i = (DG_i)^T$ is generated for $i = 1, 2, 3, \dots, t$. Sensors of particular group are preloaded with a row from respective matrix A_i and a seed value from secret matrix G . After deployment, each sensor broadcasts its ID and a seed for the column from the matrix G . Each receiving sensor calculates the column from the provided seed value and then multiplies it with its own row preloaded from matrix A to calculate the key. Group formation improves the connectivity and reduces storage cost for matrix values and set up a link key between sender and receiver. It achieves node joining mechanism without changing existing values

and remaining 0's were replaced by $q - 1$ where q was a prime number. It supposed a network size of 6 nodes with $\lambda = 3$ and $q = 29$. An adjacency matrix of size $N \times N$ with $N = 6$ was generated and then matrix G was created by taking $N \times (\lambda + 1)$ means 6×4 submatrix from the adjacency matrix. A secret matrix D of size $(\lambda + 1) \times (\lambda + 1)$ means 4×4 is generated to calculate $A = (D \cdot G)^T$ of size $N \times (\lambda + 1)$ which means 6×4 where T is transpose as elucidated in (2) which is taken from scheme.

Modified Blom's scheme using adjacency matrix is as follows:

stored at nodes. Instead of seed, our scheme only transmits row and column indices to save communication cost. This scheme is limited for key establishment between the groups only and cross group or across the network communication will require calculating new matrices. Our scheme achieves cross WSN key establishment with very little storage cost. Chances of duplication are eliminated because in case of same timestamp, there is different nonce and cross sectional values that are used to generate a different key. Matrix of same values and size like $\alpha \times \alpha$ should be loaded in sensor located at different deployments of WSNs where value of α is fixed in all categories of networks.

The authors in [21] devised a naïve scheme for key distribution using unital design theory where a unital in geometry is represented as set consisting of $n^3 + 1$ points that are divided into subsets having a size of $n + 1$. It also imposes a condition that all pairs of distinct points of main set should be present in one subset. A unital is represented as $2 - (n^3 + 1, n + 1, 1)$ design where author used a $2 - (9, 3, 1)$ matrix with 9 points and 3 subsets with each pair of unique points existing in exactly one subset. The basic unital design and mapping to keying provide less probabilities in terms of key sharing; therefore, authors improved the unital design for achieving better network scalability and high key sharing probabilities. It achieves a better scalability and connectivity while providing secure key distribution and also reduces storage overhead. Our scheme reduces the risk of low percentage of finding common keys sharing among neighbors for establishing a secret key in larger networks. The proposed model also allows communication among different WSNs that are deployed nearby and rows and columns taken from a common matrix.

Parakh and Kak proposed a Symmetric Matrix-based Keying (SMK) scheme that preloads a sensor node with a row-column pair from X and Y matrices and $XY = K$, where K is an $N \times N$ symmetric matrix with N as network size [11]. The same row and column are loaded from two different matrices. For example, 5th row and column are loaded from X and Y matrices. For key establishment, nodes S_i and S_k exchange columns of Y and then calculate the key using (3) where Row_k is the row preloaded at S_k and Col_i is column received from S_i at S_k :

$$K_{ij} = Row_i \cdot Col_k = Row_k \cdot Col_i = K_{ji}. \quad (3)$$

Matrices X and Y are generated by taking Y as a square and nonsingular matrix and then calculate $X = K \cdot Y^{-1}$. Another approach is to calculate bivariate polynomials where size of X and Y matrices is less than K matrix as illustrated in (4) that is redrawn from scheme.

Calculation of X and Y matrices is as follows:

$$\begin{bmatrix} 1 & 3 & 1 \\ 3 & 4 & 1 \\ 9 & 9 & 1 \\ 4 & 6 & 1 \\ 5 & 1 & 1 \\ X \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 3 & 2 & 4 \\ 1 & 3 & 9 & 4 & 5 \\ Y \end{bmatrix} = \begin{bmatrix} 5 & 8 & 8 & 0 & 7 \\ 8 & 4 & 2 & 4 & 2 \\ 8 & 2 & 1 & 9 & 6 \\ 0 & 4 & 9 & 9 & 0 \\ 7 & 2 & 6 & 0 & 3 \\ K \end{bmatrix}. \quad (4)$$

Authors also proposed a new Commuting Matrix-based Keying (CMK) scheme to eliminate the use of symmetric matrix K and select matrices X and Y with a condition that $XY = YX$, where matrix Y is symmetric. Each node was preloaded with randomly selected r th row of X and r th column of matrix Y . For key establishment, nodes S_i and S_k exchange columns of matrix Y . S_i calculates key by taking hash of K_{ij} concatenated with K_{ji} as illustrated in

$$\begin{aligned} K &= H(K_{ij} \parallel K_{ji}), \\ K_{ij} &= Row_i(X) \cdot Col_k(Y), \\ K_{ji} &= Col'_k(Y) \cdot Col_i(X). \end{aligned} \quad (5)$$

Quorum based key Management Scheme (QKM) [12] requires preloading a subset of key matrix in each sensor. For key establishment, sender and receiver find a common key using preloaded subset of secret matrix as shown in Figure 2 taken from scheme.

After that both the nodes generate random number and then exchange it by encrypting with common key. Shared key is obtained by calculating XOR of common key along with random values using (6). Similarly sensor node y also obtains the shared key that is used for future secure message transmission:

$$SK_{x-y} = CK_{x-y} \oplus R_x \oplus R_y. \quad (6)$$

Dai and Xu provided a key distribution scheme using LU matrix [22] where two groups of polynomials are selected

Sensor 4						
$K_{1,1}$	$K_{1,2}$	$K_{1,3}$	$K_{1,4}$	$K_{1,5}$	$K_{1,6}$	$K_{1,7}$
$K_{2,1}$	$K_{2,2}$	$K_{2,3}$	$K_{2,4}$	$K_{2,5}$	$K_{2,6}$	$K_{2,7}$
$K_{3,1}$	$K_{3,2}$	$K_{3,3}$	$K_{3,4}$	$K_{3,5}$	$K_{3,6}$	$K_{3,7}$

Sensor 6						
$K_{1,1}$	$K_{1,2}$	$K_{1,3}$	$K_{1,4}$	$K_{1,5}$	$K_{1,6}$	$K_{1,7}$
$K_{2,1}$	$K_{2,2}$	$K_{2,3}$	$K_{2,4}$	$K_{2,5}$	$K_{2,6}$	$K_{2,7}$
$K_{3,1}$	$K_{3,2}$	$K_{3,3}$	$K_{3,4}$	$K_{3,5}$	$K_{3,6}$	$K_{3,7}$

FIGURE 2: Common key calculation.

from a pool to create lower and upper triangular matrices L and U , respectively. In case of a 3×3 matrix six polynomials are selected for each L and U matrices. It imposes a condition that the product of L and U should result in a symmetric matrix K . Each sensor is preloaded with one row of L and one column of U where row and column index number should be same like i th row of L and i th column of U . After deployment, any two sensors S_i and R_k initiate the key establishment process by exchanging their rows Row_i and Row_k with each other. After that, S_i obtains the key $K_{ji} = L_{Row_j} \times U_{Col_i}$ and R_k obtains the key $K_{ij} = L_{Row_i} \times U_{Col_j}$ by multiplying the row of other sensors with their own column. The row and column are from symmetric matrix; therefore, the same key will be generated at both nodes. Our scheme also loads one row and one column but we relax the restriction that row and column index should be the same. Sensors can have randomly selected row and column indices. Moreover, we do not exchange row or column values because it increases communication overhead; instead we share indices only. In this scheme, row and column values are directly used to calculate the secret keys and compromising a row through traffic analysis attack can expose the large amount of actual keys. In our scheme, row and column values are just used to get a common value and then nonce and time stamp are also used to generate a unique key which is not entirely dependent of row and column values.

In existing schemes, communication across the WSN is not supported due to confined set of key pools that support specific number of network size. After that, the chances of key duplication increases. Size of matrix increases for larger networks and hence becomes infeasible in terms of storage for ordinary sensor nodes. Our scheme will resolve it by using a matrix with a fix size and values like a WSN_1 with 2000 nodes and WSN_2 with 1400 nodes. The matrix size and values should remain the same across the network.

3. System Model

This section elaborates the possible key exchange scenarios. We consider WSN model in which actors are responsible for managing sensors in their cluster. Both sensors and actors are randomly deployed and they exchange security credentials once the network is set up. Sensors are stationary while

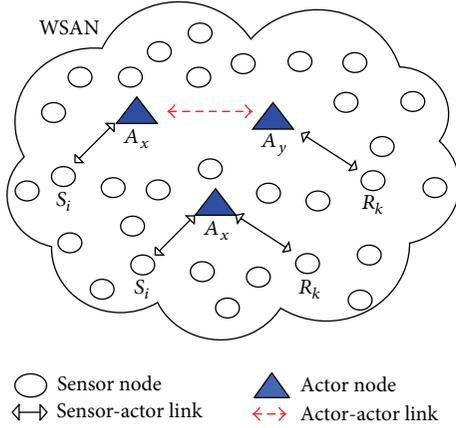


FIGURE 3: Intra- and intercluster communication scenarios.

actors can move on demand. Afterwards, any two nodes can distribute the key using DKEP procedure where an actor node is considered first priority to act as the intermediate node between sender and receiver. In other scenarios, ordinary sensor nodes or mixer of both is used as intermediaries between distant sender and receiver. We have considered scenarios where an actor is either stationary or mobile to collect desired data from sensor nodes. We assume that an actor contains the symmetric keys of all the sensor nodes in the network, and the sink node maintains a list of all actors and sensor nodes. It is also assumed that an intrusion detection system is available to detect the malicious nodes.

We consider four possible scenarios for message exchange between sender S_i and receiver R_k containing security parameters. In the first scenario, S_i and R_k can directly exchange messages when both are within direct communication range of each other. In second scenario, an actor A_x serves as an intermediary between S_i and R_k when they are not within range of each other as shown in Figure 3. In third scenario, both S_i and R_k belong to different clusters managed by the actors A_x and A_y , respectively, which require intercluster communication as illustrated in Figure 3.

In the fourth scenario we have considered that multiple WSNs are deployed in a region to perform activities for different categories of applications. Actors A_x and A_y are not in direct communication range and want to communicate for establishing secret key between distant nodes located in different WSN. In this scenario, an intermediate ordinary sensor node named gateway node (GN) which is located at common boundary of both WSN can exchange messages to a distant receiver R_k via A_y , as illustrated in Figure 4. The GN receives key messages from A_x and A_y and then proceeds with key establishment. It does not use an actor-actor link during such type of communication. Node S_i transmits encrypted message to A_x that decrypts the message and then reencrypts it with a key $E_{K_{A_x-GN}}$ established between A_x and the GN. Similarly, GN decrypts and reencrypts the message to forward towards actor A_y that further transmit to receiver R_k . After exchanging security parameters, both the nodes simultaneously perform XOR to obtain the keys.

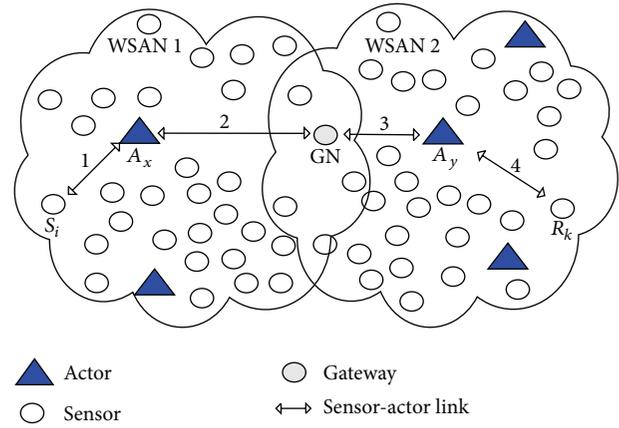


FIGURE 4: Inter-WSAN key establishment using gateway nodes.

This work is also applicable to mobile environments such as mobile ad hoc networks and vehicular ad hoc networks where same sized matrix can be preloaded on all devices. Most of the modern WSN applications such as [23] have to be integrated with other networks which may require establishing keys across the network. For example, the proposed DKEP can provide such ability to establish keys in these networks.

4. Disjoint Key Establishment Protocol (DKEP)

This section elaborates our proposed DKEP protocol. Key exchange between the communicating parties including sender, receiver, actor, and intermediaries is discussed in this protocol to ensure the secure transmission. Message structure for encryption and decryption procedure is elucidated in stepwise manner along with security parameters that are part of message. Role of message authentication code (MAC) is also highlighted to ensure integrity for each message. Finally key establishment procedure is explored. Moreover, the key establishment scenarios for sensor-sensor and actor-actor are illustrated briefly to show relevant steps of DKEP in those cases. A brief description for all notations used in proposed DKEP is provided in Notations.

In DKEP, security credentials are exchanged using intermediaries to obtain actual key at sender and receiver. We have used a matrix-based approach for key establishment scheme that securely distributes the key without transmitting the actual key on the network. Key distribution begins when rows and columns are taken from $\alpha \times \alpha$ matrix where α is selected as per security requirement and much less than cluster size. Before deployment, each node is preloaded with randomly selected rows and columns. After deployment, rows and column indices and security credentials can be exchanged between the sender and receiver. After receiving the parameters, both nodes decrypt the message, check message freshness by comparing timestamps, and check message integrity by using hash values. After that, common values are located at intersection of row and column indices. Finally the key is obtained simultaneously on both nodes

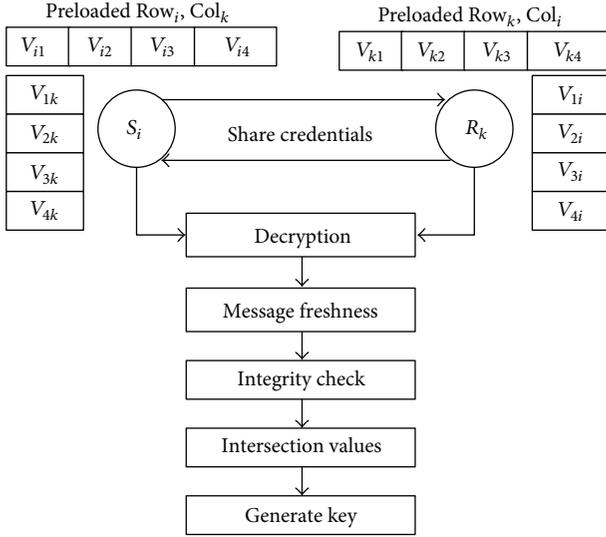


FIGURE 5: Matrix-based key establishment.

by taking XOR of parameters and the common values as illustrated in Figure 5 where S_i and R_k represent sender and receiver.

This section provides the detailed discussion on secure key distribution protocol for second scenario discussed earlier in Section 3. Key distribution process begins when sender node S_i encrypts message $(Row_i, Col_i, ts_i, rn_i, R_k, MAC(Row_i \parallel Col_i \parallel ts_i \parallel rn_i))$ using preestablished key $E_{K_{S_i-A_x}}$ between sender S_i and actor A_x as illustrated in (7). In the message, Row_i is row index, Col_i is column index, ts_i is timestamp, rn_i is the nonce from node S_i , and hash of values is also concatenated:

$$C_1 = E_{K_{S_i-A_x}} (Row_i, Col_i, ts_i, rn_i, R_k, MAC(Row_i \parallel Col_i \parallel ts_i \parallel rn_i)). \quad (7)$$

Sender node S_i sends the message (ID_{S_i}, C_1) to the actor node A_x . The message is decrypted by actor A_x to extract the values as illustrated in

$$(Row_i, Col_i, ts_i, rn_i, R_k, MAC(Row_i \parallel Col_i \parallel ts_i \parallel rn_i)) = D_{K_{S_i-A_x}} (ID_{S_i}, C_1). \quad (8)$$

Actor node A_x checks the message freshness by calculating difference of system's timestamp with ts_i and then comparing with threshold value. In case of successful result, actor A_x checks integrity of message by concatenating and then taking hash of values to compare it with hash value in the message. Finally the message is reencrypted using key $E_{K_{A_x-R_k}}$ preestablished between actor A_x and receiver R_k as shown in

$$C_2 = E_{K_{A_x-R_k}} (Row_i, Col_i, ts_i, rn_i, R_k, MAC(Row_i \parallel Col_i \parallel ts_i \parallel rn_i)). \quad (9)$$

Actor node A_x sends the message (ID_{A_x}, C_2) to the receiver R_k . The message is decrypted by receiver R_k to extract the values as illustrated in

$$(Row_i, Col_i, ts_i, rn_i, R_k, MAC(Row_i \parallel Col_i \parallel ts_i \parallel rn_i)) = D_{K_{A_x-R_k}} (ID_{A_x}, C_2). \quad (10)$$

Similarly receiver R_k validates the freshness and integrity of message. In case of success, R_k sends a message $(Row_k, Col_k, ts_k, rn_k, S_i, MAC(Row_k \parallel Col_k \parallel ts_k \parallel rn_k))$ after encrypting with key $E_{K_{R_k-A_x}}$ preestablished between sender R_k and actor A_x as illustrated in (11). In the message, Row_k is row index, Col_k is column index, ts_k is timestamp, rn_k is the nonce from node R_k , and hash of these values is also concatenated:

$$C_3 = E_{K_{R_k-A_x}} (Row_k, Col_k, ts_k, rn_k, S_i, MAC(Row_k \parallel Col_k \parallel ts_k \parallel rn_k)). \quad (11)$$

Receiver R_k responds to the actor A_x with a message (ID_{R_k}, C_3) for forwarding to node S_i . The message is further decrypted by the actor A_x to extract the values as illustrated in

$$(Row_k, Col_k, ts_k, rn_k, S_i, MAC(Row_k \parallel Col_k \parallel ts_k \parallel rn_k)) = D_{K_{R_k-A_x}} (ID_{R_k}, C_3). \quad (12)$$

Actor A_x checks freshness and integrity of the message. In case of success a message is sent towards S_i after encrypting it using key $E_{K_{A_x-S_i}}$ preestablished between actor A_x and S_i as shown in

$$C_4 = E_{K_{A_x-S_i}} (Row_k, Col_k, ts_k, rn_k, S_i, MAC(Row_k \parallel Col_k \parallel ts_k \parallel rn_k)). \quad (13)$$

Actor node A_x sends the message (ID_{A_x}, C_4) to the sender S_i . The message is decrypted by S_i to extract the values as illustrated in

$$(Row_k, Col_k, ts_k, rn_k, S_i, MAC(Row_k \parallel Col_k \parallel ts_k \parallel rn_k)) = D_{K_{A_x-S_i}} (ID_{A_x}, C_4). \quad (14)$$

Symmetric key can be obtained after exchanging row and column indices along with timestamp and nonce values. The sender S_i and receiver R_k simultaneously obtain keys by taking XOR of two nonce values (rn_i, rn_k) with time stamps (ts_i, ts_k) and the common value V_{RC} as illustrated in

$$K_{S_i-R_k} = rn_i \oplus ts_i \oplus V_{RC} \oplus ts_k \oplus rn_k. \quad (15)$$

In this equation, \oplus represents XOR and V_{RC} is the set of values at intersection of rows and columns of two nodes, for

example, row Row_i , column Col_k , and row Row_k , column Col_i as illustrated in

$$V_{RC} = V_{Row_i, Col_k} \oplus V_{Row_k, Col_i}. \quad (16)$$

For example, node S_i contains 5th row and 3rd column and node R_k contains 4th row and 1st column; then $V_{RC} = V_{Row_5, Col_1} \oplus V_{Row_4, Col_3}$. Both the nodes contain the row and column indices of each other; therefore, V_{RC} could be calculated using (16) on both nodes by identifying the values at intersection. Same values are selected at both sender S_i and receiver R_k . Moreover, same key value is obtained at both nodes and key is never transmitted on the network as illustrated in Figure 6. In case of sensor-sensor key distribution scenario, there is no end to end key and messages are not encrypted as illustrated in

$$\begin{aligned} S_i &\longrightarrow R_k : \{Row_i, Col_i, ts_i, rn_i, R_k, \\ &\quad MAC(Row_i \parallel Col_i \parallel ts_i \parallel rn_i)\} \\ R_k &\longrightarrow S_i : \{Row_k, Col_k, ts_k, rn_k, S_i, \\ &\quad MAC(Row_k \parallel Col_k \parallel ts_k \parallel rn_k)\} \\ K_{S_i-R_k} &= rn_i \oplus ts_i \oplus V_{RC} \oplus ts_k \oplus rn_k. \end{aligned} \quad (17)$$

In case of actor-actor key distribution scenario, actors are preloaded with three row and column pairs. During key establishment between A_x and A_y , one row and one column indices are randomly selected to exchange between them. After that, key is calculated using

$$\begin{aligned} A_x &\longrightarrow A_y : \{Row_x, Col_x, ts_x, rn_x, A_y, \\ &\quad MAC(Row_x \parallel Col_x \parallel ts_x \parallel rn_x)\} \\ A_y &\longrightarrow A_x : \{Row_y, Col_y, ts_y, rn_y, A_x, \\ &\quad MAC(Row_y \parallel Col_y \parallel ts_y \parallel rn_y)\} \\ K_{A_x-A_y} &= rn_x \oplus ts_x \oplus V_{RC} \oplus rn_y \oplus ts_y. \end{aligned} \quad (18)$$

In DKEP, the communication is not stopped even if the actor is compromised or damaged. Only the routing paths that were using the actor as intermediary node are affected and an alternate node can be selected for that path by establishing on demand symmetric keys. It also reduces the memory overhead as compared to the existing cluster based schemes because each node does not require $\gamma - 1$ nodes at the beginning. The number of keys stored in the memory grows according to the on demand contact with other nodes of the cluster. This contact can be done only to route the query to neighboring nodes and then route the required data towards the sink node. If a node is compromised and its rows and columns are exposed to the attacker then attacker is not able to get those keys that were established particularly using these rows and columns. These keys were calculated by using one value from matrix and taking its XOR with the two nonce values with timestamp which are not stored in the permanent memory. It means nothing is revealed by retrieving the rows

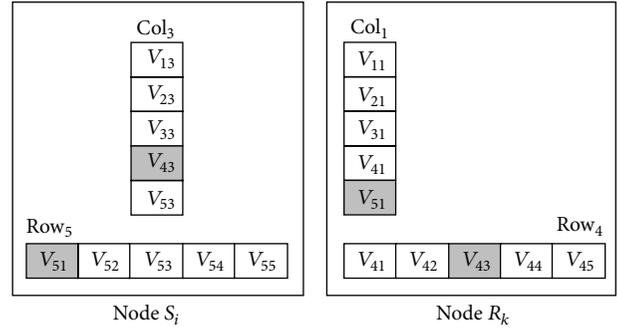


FIGURE 6: V_{RC} calculation at sender S_i and receiver R_k .

and columns. It also does not affect the keys in other nodes. It achieves much better resilience against node and traffic capturing attacks. In this way the key exposure problem at intermediate node is also resolved. It also ensures that any two distant nodes can establish keys securely and hence achieves much better connectivity. Moreover, the receiver transmits message using disjoint paths that confuse the traffic analysis attacker and strengthens the proposed scheme. If symmetric key is compromised from a node then intruder cannot recover any past keys established earlier or current keys between other nodes.

A possible variation in the scheme could be the use of lightweight public key cryptography like Elliptic Curve Cryptography (ECC) to secure only those key exchange messages that are shared between the ordinary nodes where actor nodes are not present nearby. In other scenarios discussed in system model, ordinary nodes encrypt the key exchange messages using preestablished secret keys between ordinary sensors and actor nodes.

5. DKEP Formal Specification

To verify correctness of DKEP, we use Rubin Logic [16] and performed stepwise formal modeling of the scheme. It verifies the proposed protocol for the standardized requirements of cryptographic functions including encryption, decryption, authentication, integrity protection, and freshness of message. Rubin Logic is equally applicable to verify the send, receive, and update operations performed during message exchange between distant nodes. This modeling technique includes the formalization steps that are similar to the flow of programming functions in real implementation of the scheme. A global set is maintained that contains information about entities, their roles, and global variables of protocol. The information saved in global set can be subdivided into observer, rule, secret, and principal sets. The schemes that provide stepwise discussion on formalization [24–26] of WSN security protocols are illustrated in the form of case studies.

A list of notations is provided earlier in Notations to elaborate the symbols used to describe DKEP protocol. In this section, additional notations are included in Notations to further elaborate the symbols used in local set during formal specification of DKEP.

TABLE I: Local set for DKEP.

(1) Sender (S_i)	(3) Receiver (R_k)
POSS(S_i) = {ID $_{S_i}$, $K_{S_i-A_x}$, RowVal $_i$, ColVal $_i$ }	POSS(R_k) = {ID $_{R_k}$, $K_{A_x-S_i}$, RowVal $_k$, ColVal $_k$ }
BEL(S_i) = {#(ID $_{S_i}$), #(K $_{S_i-A_x}$), #(RowVal $_i$), #(ColVal $_i$)}	BEL(R_k) = {#(ID $_{R_k}$), #(K $_{A_x-S_i}$), #(RowVal $_k$), #(ColVal $_k$)}
BL(S_i) = Hash($h(\cdot)$; Row $_i$, Col $_i$, rn $_i$, ts $_i$) \rightarrow H $_{S_{iRC}}$	BL(R_k) = Hash($h(\cdot)$; Row $_k$, Col $_k$, rn $_k$, ts $_k$) \rightarrow H $_{R_{kRC}}$
Concat(Row $_i$, Col $_i$, rn $_i$, ts $_i$, R $_k$, H $_{S_{iRC}}$) \rightarrow P $_{S_{iRC}}$	Concat(Row $_k$, Col $_k$, rn $_k$, ts $_k$, S $_i$, H $_{R_{kRC}}$) \rightarrow P $_{R_{kRC}}$
Encrypt({P $_{S_{iRC}}$ }K $_{S_i-A_x}$) \rightarrow C $_1$	Encrypt({P $_{R_{kRC}}$ }K $_{R_k-A_x}$) \rightarrow C $_2$
Send(A_x , Concat{ID $_{S_i}$, C $_1$ }) \rightarrow M $_1$	Send(A_x , Concat{ID $_{R_k}$, C $_2$ }) \rightarrow M $_2$
Update(rn $_i$, ts $_i$)	Update(rn $_k$, ts $_k$)
Receive(A_x , {ID $_{A_x}$, C $_4$ })	Receive(A_x , {ID $_{A_x}$, C $_3$ })
Split({ID $_{A_x}$, C $_4$ })	Split({ID $_{A_x}$, C $_3$ })
Decrypt({C $_4$ }K $_{A_x-S_i}$) \rightarrow P $_{R_{kRC}}$	Decrypt({C $_3$ }K $_{A_x-R_k}$) \rightarrow P $_{S_{iRC}}$
Split(P $_{R_{kRC}}$) \rightarrow (Row $_k$, Col $_k$, rn $_k$, ts $_k$, S $_i$, H $_{R_{kRC}}$)	Split(P $_{S_{iRC}}$) \rightarrow (Row $_i$, Col $_i$, rn $_i$, ts $_i$, R $_k$, H $_{S_{iRC}}$)
Freshness((ts $_i$ - ts $_k$) \geq Δt) \rightarrow Abort	Freshness((ts $_k$ - ts $_i$) \geq Δt) \rightarrow Abort
MAC(Concat(Row $_k$, Col $_k$, rn $_k$, ts $_k$)) \rightarrow H $^+$	MAC(Concat(Row $_i$, Col $_i$, rn $_i$, ts $_i$)) \rightarrow H A
Check(H $_{R_{kRC}}$, H $^+$) \rightarrow Abort	Check(H $_{S_{iRC}}$, H A)
XOR(V $_{Row_i, Col_i}$, V $_{Row_k, Col_k}$) \rightarrow V $_{RC}$	XOR(V $_{Row_i, Col_i}$, V $_{Row_k, Col_k}$) \rightarrow V $_{RC}$
XOR(rn $_i$, ts $_i$, V $_{RC}$, rn $_k$, ts $_k$) \rightarrow K $_{S_i-R_k}$	XOR(rn $_i$, ts $_i$, V $_{RC}$, rn $_k$, ts $_k$) \rightarrow K $_{S_i-R_k}$
Hash($h(\cdot)$; rn $_k$, KeySuccess) \rightarrow H $_{S_i}$	Hash($h(\cdot)$; rn $_i$, KeySuccess) \rightarrow H $_{R_k}$
Concat(rn $_k$, KeySuccess, H $_{S_i}$) \rightarrow P $_{S_i}$	Concat(rn $_i$, KeySuccess) \rightarrow P $_{R_k}$
Encrypt({P $_{S_i}$ }K $_{S_i-R_k}$) \rightarrow C $_6$	Encrypt({P $_{R_k}$ }K $_{S_i-R_k}$) \rightarrow C $_5$
Send(R_k , Concat{ID $_{S_i}$, C $_6$ }) \rightarrow M $_6$	Send(S_i , Concat{ID $_{R_k}$, C $_5$ }) \rightarrow M $_5$
Update(M $_{ID}$)	Update(M $_{ID}$)
Receive(R_k , {ID $_{R_k}$, C $_5$ })	Receive(S_i , {ID $_{S_i}$, C $_6$ })
Split({ID $_{R_k}$, C $_5$ })	Split({ID $_{S_i}$, C $_6$ })
Decrypt({C $_5$ }K $_{S_i-R_k}$) \rightarrow P $_{R_k}$	Decrypt({C $_6$ }K $_{S_i-R_k}$) \rightarrow P $_{S_i}$
Split(P $_{R_k}$) \rightarrow (rn $_k$, KeySuccess, H $_{R_k}$)	Split(P $_{S_i}$) \rightarrow (rn $_i$, KeySuccess, H $_{S_i}$)
Freshness((ts $_i$ - ts $_k$) \geq Δt) \rightarrow Abort	Freshness((ts $_k$ - ts $_i$) \geq Δt) \rightarrow Abort
Check(MAC(Concat(rn $_i$, KeySuccess)), H $_{R_k}$)	Check(MAC(Concat(rn $_k$, KeySuccess)), H $_{S_i}$)
Check(rn $_i$, KeySuccess) \rightarrow Update(K $_{S_i-R_k}$)	Check(rn $_k$, KeySuccess) \rightarrow Update(K $_{S_i-R_k}$)
(2) Actor (A_x)	
POSS(A_x) = {ID $_{A_x}$, $K_{A_x-S_i}$, $K_{A_x-R_k}$ }	Receive(R_k , {ID $_{R_k}$, C $_2$ })
BEL(A_x) = {#(ID $_{A_x}$), #(K $_{A_x-S_i}$), #(K $_{A_x-R_k}$)}	Split({ID $_{R_k}$, C $_2$ })
BL(A_x) = Receive(S_i , {ID $_{S_i}$, C $_1$ })	Decrypt({C $_2$ }K $_{A_x-R_k}$) \rightarrow P $_{R_{kRC}}$
Split({ID $_{S_i}$, C $_1$ })	Split(P $_{R_{kRC}}$) \rightarrow (Row $_k$, Col $_k$, rn $_k$, ts $_k$, S $_i$, H $_{R_{kRC}}$)
Decrypt({C $_1$ }K $_{A_x-S_i}$) \rightarrow P $_{S_{iRC}}$	Freshness((ts $_{A_x}$ - ts $_i$) \geq Δt) \rightarrow Abort
Split(P $_{S_{iRC}}$) \rightarrow (Row $_i$, Col $_i$, rn $_i$, ts $_i$, R $_k$, H $_{S_{iRC}}$)	MAC(Concat(Row $_k$, Col $_k$, rn $_k$, ts $_k$)) \rightarrow H $^-$
Freshness((ts $_{A_x}$ - ts $_i$) \geq Δt) \rightarrow Abort	Check(H $_{R_{kRC}}$, H $^-$) \rightarrow Abort
MAC(Concat(Row $_i$, Col $_i$, rn $_i$, ts $_i$)) \rightarrow H *	Encrypt({P $_{R_{kRC}}$ }K $_{A_x-S_i}$) \rightarrow C $_4$
Check(H $_{S_{iRC}}$, H *) \rightarrow Abort	Send(S_i , Concat{ID $_{A_x}$, C $_4$ }) \rightarrow M $_4$
Encrypt({P $_{S_{iRC}}$ }K $_{A_x-R_k}$) \rightarrow C $_3$	Update(M $_{ID}$)
Send(R_k , Concat{ID $_{A_x}$, C $_3$ }) \rightarrow M $_3$	
Update(M $_{ID}$)	

Each entity maintains a local set that is subdivided into possession set POSS(), belief set BEL(), seen set, and behavior List BL() where detailed discussion is provided in [16, 27]. Local set for DKEP scenario is illustrated in Table 1 that includes the procedural steps performed at sender, receiver, and the actor individually. In this scenario, POSS(S_i) and BEL(S_i) sets explore the storage requirements

during and after execution of protocol steps at sender node S_i . Computational and communication oriented details of the DKEP are enumerated in BL(S_i). All these steps are performed individually for each entity including S_i , R_k , and A_x . It also highlights the parameters and operations that are performed during protocol implementation of the scheme using C language for adding it in NS-2 protocols.

5.1. DKEP Analysis and Verification. In this section, DKEP is analyzed for intracluster key distribution scenario where both the distant sensor nodes are in communication range of one actor. In this scenario, initially sender S_i transmits message M_1 to actor node A_x . After the send operation, system calls the update procedure to refresh the rn_i, ts_i values in the observer list as shown below:

- (i) Hash($h(\cdot)$; Row $_i$, Col $_i$, rn $_i$, ts $_i$) $\rightarrow H_{S_{iRC}}$.
- (ii) Concat(Row $_i$, Col $_i$, rn $_i$, ts $_i$, R_k , $H_{S_{iRC}}$) $\rightarrow P_{S_{iRC}}$.
- (iii) Encrypt($\{P_{S_{iRC}}\}K_{S_i-A_x}$) $\rightarrow C_1$.
- (iv) Send(A_x , Concat{ID $_{S_i}$, C_1 }) $\rightarrow M_1$.
- (v) Update(rn $_i$, ts $_i$).

All the parameters including message M_1 , cipher text C_1 , hash $H_{S_{iRC}}$, concatenated string $P_{S_{iRC}}$, nonce and timestamp values rn $_i$, ts $_i$, and row and column indices Row $_i$, Col $_i$ are saved in possession set at S_i as illustrated below. Belief set also appends the message M_1 in the list:

$$\begin{aligned} \text{POSS}(S_i) &= \{\text{ID}_{S_i}, K_{S_i-A_x}, P_{S_{iRC}}, \text{Row}_i, \text{Col}_i, \text{rn}_i, \text{ts}_i, \\ &H_{S_{iRC}}, C_1, M_1, R_k\}. \\ \text{BEL}(S_i) &= \{\#(\text{ID}_{S_i}), \#(K_{S_i-A_x}), \#(M_1)\}. \end{aligned}$$

Similarly R_k also transmits the message containing row and column indices along with timestamp and nonce values:

- (i) Hash($h(\cdot)$; Row $_k$, Col $_k$, rn $_k$, ts $_k$) $\rightarrow H_{R_{kRC}}$.
- (ii) Concat(Row $_k$, Col $_k$, rn $_k$, ts $_k$, S_i , $H_{R_{kRC}}$) $\rightarrow P_{R_{kRC}}$.
- (iii) Encrypt($\{P_{R_{kRC}}\}K_{R_k-A_x}$) $\rightarrow C_2$.
- (iv) Send(A_x , Concat{ID $_{R_k}$, C_2 }) $\rightarrow M_2$.
- (v) Update(rn $_k$, ts $_k$).

Similarly the related parameters are saved in possession set at receiver node R_k as illustrated below:

$$\begin{aligned} \text{POSS}(S_i) &= \{\text{ID}_{S_i}, K_{S_i-A_x}, \text{Row}_k, \text{Col}_k, \text{rn}_k, \text{ts}_k, H_{R_{kRC}}, \\ &P_{R_{kRC}}, C_2, M_2, S_i\}. \\ \text{BEL}(S_i) &= \{\#(\text{ID}_{S_i}), \#(K_{S_i-A_x}), \#(M_2)\}. \end{aligned}$$

After the exchange of messages between sender and receiver, each sensor node splits the message to extract the cipher text. After that, it is decrypted using the shared key between actor and the sensor node S_i to retrieve concatenated string $P_{S_{iRC}}$ that is further split to extract Row $_i$, Col $_i$, rn $_i$, ts $_i$, R_k , $H_{S_{iRC}}$ values. For freshness evaluation of the message, initially timestamp ts_{A_x} is calculated at actor A_x and then received time stamp value ts_i is subtracted from it. A message can be aborted when timestamp difference is larger than the threshold time Δt . Otherwise, node R_k calculates the MAC of Row $_i$, Col $_i$, rn $_i$, ts $_i$ and compares it with hash $H_{S_{iRC}}$ to ensure integrity protection. Actor node proceeds with next steps by checking that both the hash values are equal otherwise message is discarded. Similar steps are followed by A_x to receive message M_2 from node R_k with different parameters:

$$\text{POSS}(A_x) = \{\text{ID}_{A_x}, K_{A_x-S_i}, K_{A_x-R_k}\}.$$

$$\begin{aligned} \text{BEL}(A_x) &= \{\#(\text{ID}_{A_x}), \#(K_{A_x-S_i}), \#(K_{A_x-R_k})\}. \\ \text{BL}(A_x) &= \end{aligned}$$

- (i) Receive(S_i , {ID $_{S_i}$, C_1 }),
- (ii) Split({ID $_{S_i}$, C_1 }),
- (iii) Decrypt($\{C_1\}K_{A_x-S_i}$) $\rightarrow P_{S_{iRC}}$,
- (iv) Split($P_{S_{iRC}}$) \rightarrow (Row $_i$, Col $_i$, rn $_i$, ts $_i$, R_k , $H_{S_{iRC}}$),
- (v) Freshness($(ts_{A_x} - ts_i) \geq \Delta t$) \rightarrow Abort,
- (vi) MAC(Concat(Row $_i$, Col $_i$, rn $_i$, ts $_i$)) $\rightarrow H^*$,
- (vii) Check($H_{S_{iRC}}$, H^*) \rightarrow Abort.

Actor node A_x further prepares message by encrypting received concatenated string $P_{S_{iRC}}$ using preestablished key $K_{A_x-R_k}$ between A_x and receiver node. The encrypted message is transmitted towards R_k and then temporary values ($P_{S_{iRC}}$, rn $_i$, ts $_i$, R_k , C_3 , M_3 , H^*) used during calculations are removed from memory using Forget procedure:

- (viii) Encrypt($\{P_{S_{iRC}}\}K_{A_x-R_k}$) $\rightarrow C_3$.
- (ix) Send(R_k , Concat{ID $_{A_x}$, C_3 }) $\rightarrow M_3$.
- (x) Update(M_{ID}).
- (xi) Forget($P_{S_{iRC}}$, rn $_i$, ts $_i$, R_k , C_3 , M_3 , H^*).

Actor node A_x maintains a list of variables and parameters in possession set to perform calculations during key establishment:

$$\begin{aligned} \text{POSS}(A_x) &= \{\text{ID}_{A_x}, K_{A_x-S_i}, K_{A_x-R_k}, P_{S_{iRC}}, R_k, \text{rn}_i, \text{ts}_i, \\ &C_3, M_3, H^*\}. \\ \text{BEL}(A_x) &= \{\#(\text{ID}_{A_x}), \#(K_{A_x-S_i}), \#(K_{A_x-R_k})\}. \end{aligned}$$

Actor node A_x performs the same operation for message received from R_k to forward towards sensor node S_i with different parameters. The receiver R_k receives the message from A_x and then splits the message to get C_3 which is decrypted to extract the concatenated string. It is further tokenized to get the security parameters including Row $_i$, Col $_i$, rn $_i$, ts $_i$, R_k , $H_{S_{iRC}}$. Freshness of message is checked and then comparison of the hash values is performed for integrity protection:

- (i) Receive(A_x , {ID $_{A_x}$, C_3 }).
- (ii) Split({ID $_{A_x}$, C_3 }).
- (iii) Decrypt($\{C_3\}K_{A_x-R_k}$) $\rightarrow P_{S_{iRC}}$.
- (iv) Split($P_{S_{iRC}}$) \rightarrow (Row $_i$, Col $_i$, rn $_i$, ts $_i$, R_k , $H_{S_{iRC}}$).
- (v) Freshness($(ts_{R_k} - ts_i) \geq \Delta t$) \rightarrow Abort MAC(Concat(Row $_i$, Col $_i$, rn $_i$, ts $_i$)) $\rightarrow H^\wedge$.
- (vi) Check($H_{S_{iRC}}$, H^\wedge).

Finally the symmetric key is obtained by calculating XOR of time stamps and nonce values exchanged between sender and receiver. It also includes the value V_{RC} which is obtained by taking XOR of common value at the intersection of rows and columns of sender and receiver as shown below. After that a key success message is exchanged between sender and receiver to confirm the secret key establishment as per the

following steps. At the end, Message ID is updated in the belief set and Forget operation is executed to remove the out of scope values from the memory of R_k :

- (vii) $\text{XOR}(V_{\text{Row}_i \text{Col}_k}, V_{\text{Row}_k \text{Col}_i}) \rightarrow V_{\text{RC}}$.
- (viii) $\text{XOR}(\text{rn}_i, \text{ts}_i, V_{\text{RC}}, \text{rn}_k, \text{ts}_k) \rightarrow K_{S_i-R_k}$.
- (ix) $\text{Hash}(h(\cdot); \text{rn}_i, \text{KeySuccess}) \rightarrow H_{R_k}$.
- (x) $\text{Concat}(\text{rn}_i, \text{KeySuccess}) \rightarrow P_{R_k}$.
- (xi) $\text{Encrypt}(\{P_{R_k}\}K_{S_i-R_k}) \rightarrow C_5$.
- (xii) $\text{Send}(S_i, \text{Concat}\{\text{ID}_{R_k}, C_5\}) \rightarrow M_5$.
- (xiii) $\text{Update}(M_{\text{ID}})$.
- (xiv) $\text{Forget}(\text{Row}_i, \text{Col}_i, \text{Row}_k, \text{Col}_k, H_{S_{\text{IRC}}}, P_{S_{\text{IRC}}}, \text{rn}_k, \text{ts}_k, C_3, M_3, H^\wedge, V_{\text{RC}}, H_{R_k}, P_{R_k}, C_5, M_5)$.

Possession set contains the variables and parameters used during calculations regarding key distribution and message extraction as shown below:

$$\begin{aligned} \text{POSS}(R_k) &= \{\text{ID}_{R_k}, K_{R_k-A_x}, \text{Row}_i, \text{Col}_i, \text{Row}_k, \text{Col}_k, \\ &H_{S_{\text{IRC}}}, P_{S_{\text{IRC}}}, \text{rn}_k, \text{ts}_k, C_3, M_3, H^\wedge, V_{\text{RC}}, H_{R_k}, P_{R_k}, C_5, \\ &M_5, K_{S_i-R_k}\}, \\ \text{BEL}(R_k) &= \#(\text{ID}_{R_k}), \#(K_{R_k-A_x}), \#(K_{S_i-R_k}). \end{aligned}$$

After execution of all steps illustrated above, the newly established key $K_{S_i-R_k}$ is stored in the belief set. Unnecessary and out of scope values are removed from the possession set and hence the memory of sender node S_i and receiver node R_k . For this purpose, it calls a function $\text{Forget}(\text{Row}_i, \text{Col}_i, \text{Row}_k, \text{Col}_k, H_{S_{\text{IRC}}}, P_{S_{\text{IRC}}}, \text{rn}_k, \text{ts}_k, C_3, M_3, H^\wedge, V_{\text{RC}}, H_{R_k}, P_{R_k}, C_5, M_5)$ after successful exchange of key success message between sender and receiver. The sender node S_i receives the cipher text C_5 for the key success message M_5 encrypted with currently established key $K_{S_i-R_k}$. Node S_i decrypts the cipher text C_5 to get $(\text{rn}_i, \text{KeySuccess})$ and verify the nonce value rn_i as shown in the following steps. Node S_i calls the Forget procedure to clear the out of scope variables from possession set and memory as well:

- (i) $\text{Receive}(R_k, \{\text{ID}_{R_k}, C_5\})$.
- (ii) $\text{Split}(\{\text{ID}_{R_k}, C_5\})$.
- (iii) $\text{Decrypt}(\{C_5\}K_{S_i-R_k}) \rightarrow P_{R_k}$.
- (iv) $\text{Split}(P_{R_k}) \rightarrow (\text{rn}_k, \text{KeySuccess}, H_{R_k})$.
- (v) $\text{Freshness}((\text{ts}_{S_i} - \text{ts}_k) \geq \Delta t) \rightarrow \text{Abort Check}(\text{MAC}(\text{Concat}(\text{rn}_i, \text{KeySuccess})), H_{R_k})$.
- (vi) $\text{Check}(\text{rn}_i, \text{KeySuccess}) \rightarrow \text{Update}(K_{S_i-R_k})$.
- (vii) $\text{Forget}(\text{rn}_k, \text{ts}_k, C_5, P_{R_k}, H_{R_k})$.

Similarly, the receiver node R_k also receives the cipher text C_6 for the key success message M_6 and performs all the steps illustrated above.

6. Results and Analysis

The proposed model is simulated for a clustered WSAAN using NS-2 where an actor is the cluster head. Running times for

TABLE 2: Simulation parameters.

Simulation setup	
Parameters	Values
Network field	1200 × 1200 meters
Initial energy at node	1000 J
Tx power at node	0.819 J
Receiving power	0.049 J
Queue type	Queue/DropTail/PriQue
Max packet in queue	50
Routing protocol	DSDV
Agent trace	ON
Router trace	ON
Cluster size	50–500 nodes
Network size	1000–10000
Neighbor count	5–25
Associations count	1–5
Intermediaries count	3,4,5
Captured gateway	1–4
Row column compromised	1 + 1

critical computations are calculated using C++ language with ns-2 and C# in visual studio 2013 as well. In WSAAN, nodes and actors are randomly deployed in a region of 1200 × 1200 meters where nodes were static and actors can move within the network field. Cluster sizes are varied from 50 to 500 nodes and 2 to 20 actors were deployed with an increase of one actor per 25 nodes. Queue type is assigned as Queue/DropTail/PriQue as shown in Table 2.

DKEP scheme is evaluated to measure the resilience, storage, and communication overhead during key establishment for intra- and intercluster scenarios.

6.1. Storage Overhead. Each sensor node is preloaded with matrix elements including row, column, or both. These elements are preloaded for future calculation for key establishment after deployment. In the following section, we have analyzed the storage required for preloading these matrix elements only. Figure 7(a) elucidates the storage per node in bytes for different cluster sizes and fixes network size of 1000 nodes. Different relevant existing schemes need to store key credentials like Blom's scheme [9] that requires $2(\lambda + 1)$ values of one row and column. If each value in matrix is S bytes which is considered 8 bytes in this scenario, then $2(\lambda + 1) \times S$ bytes whereas MBS [10] requires $(\lambda + 1) \times S$ bytes that is reduced due to the fact that one column is calculated from identity matrix.

QKM scheme [12] requires $(\gamma - 1) \times S$ bytes where γ represents cluster size and SMK scheme [11] reserves $3(\gamma) \times S$ bytes. Proposed DKEP scheme requires $2 \times \sqrt{\gamma} \times S$ bytes for storing row-column pair. Results prove the dominance of DKEP as compared to preliminaries. Figure 7(b) elucidates the storage per whole network in existing and proposed schemes for different network sizes with same cluster size equal to 100 nodes. Individual node requires needs to store $(\lambda + 1) \times S$ bytes for preloaded key material in MBS [10] and network wide storage cost is $(\lambda + 1) \times S \times N$ bytes, where N

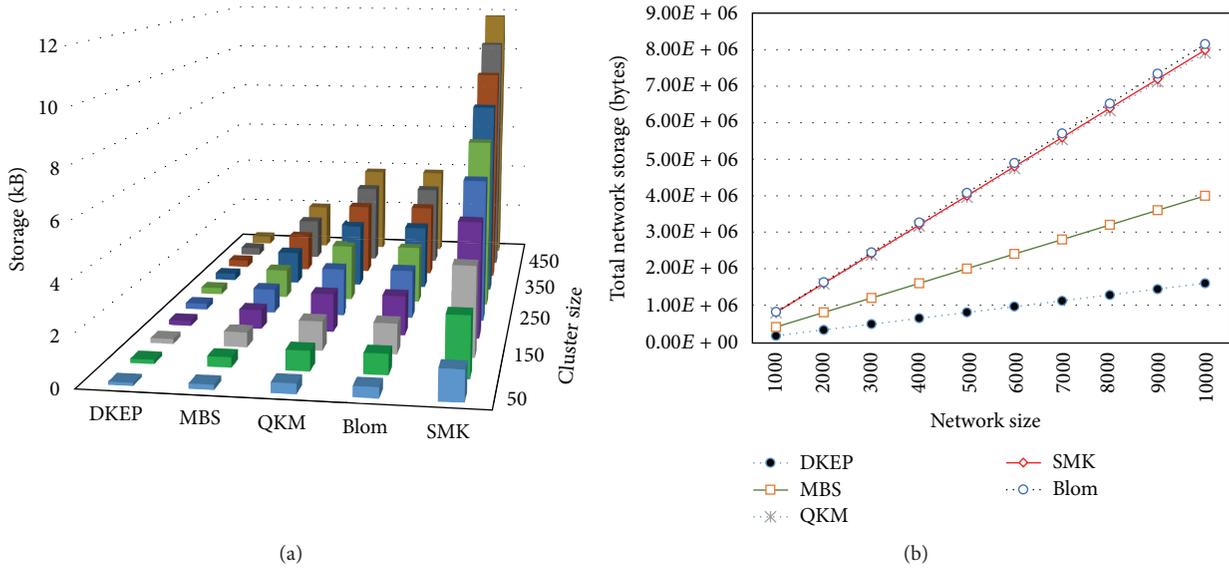


FIGURE 7: Storage per node is shown in (a) and network wide storage is shown in (b).

represents network size. Similarly the network wide cost of QKM scheme [12] is $(\gamma - 1) \times S \times N$ bytes, SMK scheme [11] reserves $2(\lambda + 1) \times S \times N$ bytes, and proposed DKEP scheme requires $2 \times \sqrt{\gamma} \times S \times N$ bytes. Results prove that proposed DKEP scheme is much more scalable and can be applied to large networks.

Gateway node stores two rows and columns in existing schemes whereas DKEP needs to load only one pair. DKEP requires to load row and column pair from same matrix in all clusters because key is not fully dependent on matrix values and cannot be calculated mathematically even intruder obtains all rows and columns. These stored matrix elements are also refreshed after regular interval to keep the network more resilient against node capturing attacks.

6.2. Communication Overhead. Source and destination nodes exchange messages during key establishment within the cluster. Figure 8(a) illustrates number of bytes transmitted during message exchange for keying between neighboring nodes. Cluster size is equal to 100 nodes and $\lambda = 50$ and number of neighbors are varied from 5 to 25. In QKM scheme [12], two nodes transmit two messages of size S for exchanging their IDs and two more messages of size T for exchanging random values that costs $((2 \times S) + (2 \times T))$ bits. SMK scheme [11] requires to transmit one column of matrix Y from each node that costs total $(2 \times \text{Col}_{\text{Size}} \times \text{EC}_{\text{size}})$ bits where EC_{size} is size of each element in column. MBS [10] requires transmitting one row and indices from each node that exchanges total $(2 \times \text{Row}_{\text{Size}} \times \text{ER}_{\text{size}}) + 4$ bits, where ER_{size} represents size of row elements. Blom's scheme [9] requires transmitting one row and one column that transmits $(2 \times (\text{Row}_{\text{size}} + \text{Col}_{\text{size}}) \times \text{EM}_{\text{size}})$ bits where EM_{size} represents size of matrix elements which is considered 8 bits per value.

DKEP requires $(2 \times P_{\text{size}})$ bits where P_{size} is sum of 16-bit node ID, 16-bit nonce, 16-bit timestamp, 8-bit row, and column index each. Communication cost increases rapidly

in SMK, MBS, and Blom's scheme with the increase in cluster size and hence number of neighboring nodes. QKM is suitable in terms of communication cost but it is not scalable due to storage overhead. Results ensure the applicability of DKEP for large cluster sizes and hence larger networks.

During intercluster path key establishment, messages are exchanged between sender S_i and receiver R_k across the cluster where actors A_x and A_y are also involved in this process along with gateway node GN. In this scenario, we have ignored the messages transmission cost between actors and considered the ordinary member nodes that transmit only 4 messages during S_i to A_x , GN to A_y , S_i back to A_y , and from node GN back to A_x transmission. Figure 8(b) elucidates message transmission cost for managing t associations across the cluster where t represents the number of path keys established with neighboring cluster. QKM scheme [12] requires $((4 \times S) + (4 \times T))$ bits, SMK scheme [11] requires $(4 \times \text{Col}_{\text{Size}} \times \text{EC}_{\text{size}})$ bits, MBS [10] requires $((4 \times \text{Row}_{\text{Size}} \times \text{ER}_{\text{size}}) + 4)$ bits, and proposed DKEP requires $(4 \times P_{\text{size}})$ bits for message exchange.

Figure 9 elucidates the cost for establishing the path key using intermediaries in the following communication scenarios including intracluster, intercluster, and inter-WSAN with gateway node. Communication cost $\text{Comm}_{\text{cost}}$ is calculated using (19) where message size Msg_{size} is calculated in such a way that Blom's scheme [9] requires $((\text{Row}_{\text{size}} + \text{Col}_{\text{size}}) \times \text{EM}_{\text{size}})$ bits, QKM scheme [12] requires $(S + T)$ bits, SMK scheme [11] requires $(\text{Col}_{\text{Size}} \times \text{EC}_{\text{size}})$ bits, MBS [10] requires $((\text{Row}_{\text{Size}} \times \text{ER}_{\text{size}}) + 4)$ bits, and DKEP requires P_{size} bits:

$$\text{Comm}_{\text{cost}} = \text{Interm}_{\text{count}} * \text{Msg}_{\text{size}} * \text{MsgCount}_{\text{node}}. \quad (19)$$

The number of intermediate nodes $\text{Interm}_{\text{count}}$ during path key is 3, 4, and 5 for intracluster, intercluster, and inter-WSAN with gateway node based communication scenarios. Each intermediate node sends total 2 messages that is represented as $\text{MsgCount}_{\text{node}}$.

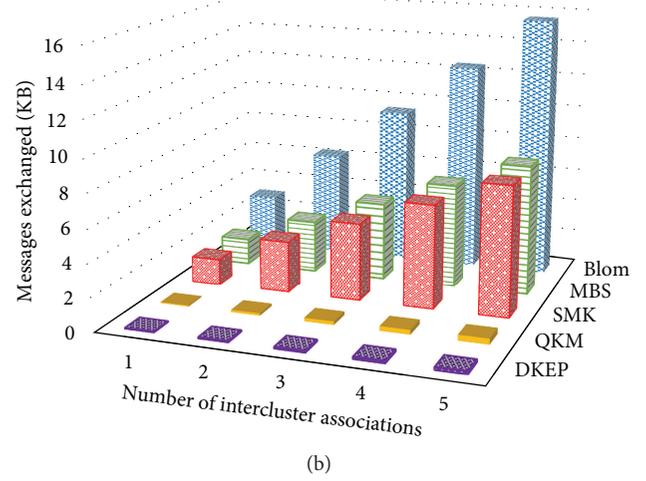
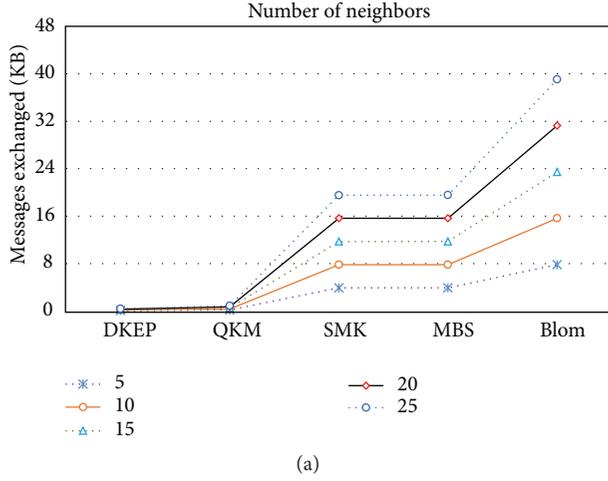


FIGURE 8: Communication cost for intracuster keying is shown in (a) and intercluster scenario is shown in (b).

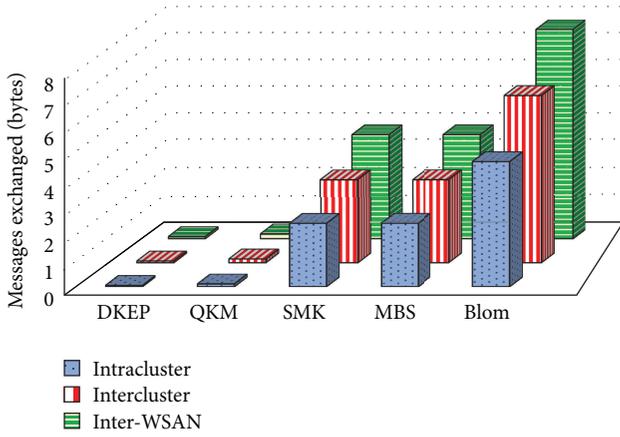


FIGURE 9: Communication cost for path key distribution.

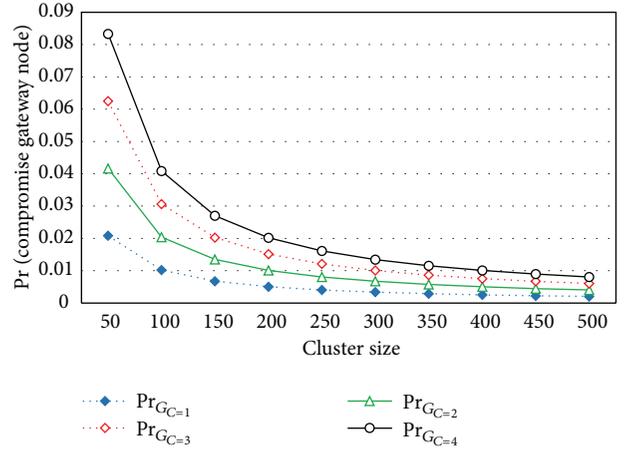


FIGURE 10: Probability of compromised gateway node.

6.3. *Resilience.* During inter-WSAN communication, two ordinary nodes from different regions communicate using two actors and gateway node. Probability $\Pr_{\text{Gateway_Node}}$ to calculate the existence of an uncompromised gateway node in the path can be calculated using (20) where γ is the cluster size and ψ is number of nodes captured by an attacker in the network:

$$\Pr_{\text{Gateway_Node}} = \frac{\binom{\gamma-3}{\psi}}{\binom{\gamma-2}{\psi}}. \quad (20)$$

Total uncompromised nodes $\gamma - 2$ represent that 2 ordinary nodes are excluded from compromised nodes in network whereas $\gamma - 3$ represents the further exclusion of one gateway node. The probability $\Pr_{\text{G_Compromised}}$ that a selected gateway node is captured at either sender or receiver side can be calculated using

$$\Pr_{\text{G_Compromised}} = 1 - \Pr_{\text{Gateway_Node}} = \frac{\psi}{\gamma - 2}. \quad (21)$$

Figure 10 elucidates the probability of compromising a gateway node during intercluster key establishment scenario for different cluster sizes. It considers scenario for calculating the probability $\Pr_{\text{GC}=1}$, $\Pr_{\text{GC}=2}$ up to 4 nodes compromised where cluster size varies from 100 nodes to 450 nodes. By compromising 3 nodes in a cluster size of 250 nodes, there is 1 percent chance that gateway node is compromised.

If an ordinary node is compromised then a single row and column pair are revealed to adversary. Probability that a particular row and column are compromised is calculated using (22) where ω rows and columns are compromised, respectively,

$$\Pr_{\text{RC_Compromised}} = 1 - \frac{\binom{M-1}{\omega-1}}{\binom{M}{\omega}} = \frac{\omega}{M}. \quad (22)$$

A column and row pair is loaded in a node; therefore, compromising an ordinary node reveals one row and column pair in Blom's scheme [9], QKM scheme [12], MBS [10], and proposed DKEP scheme. In case of SMK scheme [11],

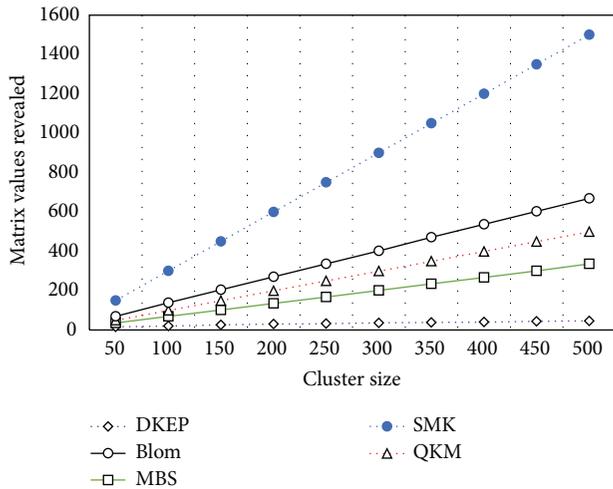


FIGURE 11: Matrix values revealed on node compromise.

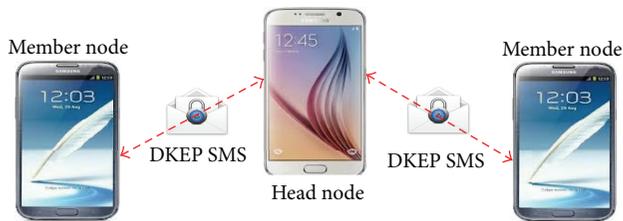


FIGURE 12: Client-server communication using DKEP.

one row and two columns are revealed. Figure 11 illustrates the exposure of number of matrix values when a node is compromised by an attacker. Network size is equal to 1000 nodes whereas cluster size varies from 100 to 500 and $\lambda = 60$. Results prove the strong resilience of DKEP as compared to existing schemes. It is much secure than these results because in existing schemes exposure of rows and columns results in key exposure as keys are calculated by multiplying row and column values. In DKEP scheme exposure of row and column does not expose the key because values at particular index of row and column are taken as one part of the key. Row and column values are also refreshed after regular intervals to further protect against node capture attacks.

7. DKEP Based Security in Mobile Applications

Proposed scheme is equally applicable in mobile applications for providing security in mobile ad hoc networks. Client and server applications are developed to operate in a peer to peer and cluster based scenario as illustrated in Figure 12. These applications are developed for the proof of the concept and verification of protocol steps in a practical scenario.

Client and server nodes are preloaded with one row and column from $\alpha \times \alpha$ matrix. Member nodes and server mobile exchange row and column indices along with timestamp and nonce values. Keys are established by taking XOR of these security credentials according to DKEP specifications.

Established keys and related details are saved in an XML file in flash memory of android mobile. It was tested by establishing keys with four mobiles and then sending encrypted SMS. Application at receiver side reads cipher message and decrypts it using preestablished key. It was also tested for chatting application between two android mobiles. Both client and server application are successfully performing the intended functionalities. DKEP is equally applicable in securing MANET based application scenarios.

7.1. Key Generation Phase. If two nodes do not contain a pre-established key then following steps are followed to establish a secret key between two mobiles. Established keys are saved in an XML and can be retrieved for encrypting or decrypting the SMS for secure communication between mobile nodes. Specifications of DKEP are adopted to establish keys.

Sender Side

- (1) Getting Mobile Number from User.
- (2) Checking the Mobile Number from XML File.
 - (a) If Mobile number already in File
"Continue Messaging".
 - (b) else
Call DKEP_KeyInit and DKEP_KeyGen functions.
 - (c) end if
- (3) Procedure DKEP_KeyInit(){
- (4) Randomly Generate Rows and Column Indices.
- (5) Concatenate Magic Word (MW), indices, time stamp and nonce.
- (6) Send SMS.
- (7) Saving values in XML File.
- (8) }
- (9) Procedure DKEP_KeyGen(){
- (10) Obtain Magic Word (MW), indices, time stamp and nonce from receiver
- (11) Take XOR of these values using DKEP to obtain Key
- (12) Save Key in XML file.
- (13) }

Receiver Side

- (1) Receive SMS.
- (2) If first 12 bits equals Magic Word then
- (3) Split the concatenated string
- (4) Save received values in XML File
- (5) Call DKEP_KeyInit function.
- (6) Call DKEP_KeyGen function.
- (7) else
- (8) Discard Message
- (9) end if

7.2. Secure Messaging between Cell Phones. A mobile user can communicate securely with mobile phones that are registered earlier through key generation phase. To validate steps of DKEP, user can select the secure option to transmit the message in a cipher text form. SMS is sent towards receiver by concatenating with a magic word where receiver first checks magic word to avoid unnecessary decryption efforts. Plain text message is displayed to user after successful decryption using preestablished key saved in XML file.

Sender Side

- (1) Getting Mobile Number and Message of Receiver.
- (2) If Mobile number not exist in XML file.
 - (a) Start Key Initialization and Generation Process
- (3) else
 - (a) Encrypt message using pre-established key.
 - (b) Converting them in to byte Array.
- (4) Concatenate the Magic Word “* * *DKEP* * *” with cipher text.
- (5) Send SMS

Receiver Side

- (1) Receive SMS and split the concatenated message.
- (2) If first 10 characters of Message equals “* * *DKEP* * *”.
 - (a) Decrypt the message
 - (b) Displaying Original Message.
- (3) else
 - (a) Displaying Original Message in list.

8. Conclusion

Secure key distribution is the essential requirement of industrial, medical, and military applications of WSN and WSN for providing secure messaging between sensor nodes. During key distribution between two nodes across the clusters, an intermediate gateway node that has established keys in both clusters across WSN plays a vital role for message exchange. A compromised gateway node can extract the key before the link establishment because sender and receiver have no prior end to end key to encrypt messages. In this scheme, indices for row and column are exchanged between the sender and receiver nodes and values at intersection of row and column index are used to calculate the key on both nodes. It can establish keys with neighboring nodes, actors, and sink and even across different WSN. Simulation results prove the dominance of DKEP as compared to existing schemes. DKEP reduces communication overhead as compared to existing schemes and achieves resilience against node compromising attacks because key is never transmitted across the nodes. The

proposed scheme is verified using Rubin Logic and results are validated with simulations using NS-2. DKEP is also tested for secure messaging between android mobiles in a group-based scenario.

Notations

Notations for DKEP

S_i :	Sender node
R_k :	Receiver node
$K_{S_i-R_k}$:	Symmetric key between sender and receiver
rn_i, rn_k :	Random nonce values from nodes S_i and R_k
ts_i, ts_k :	Time stamp from nodes S_i and R_k
Row_i :	Row sent by node S_i
Col_i :	Column sent by S_i
V_{RC} :	Values at intersection of row and column
V_{Row_i, Col_k} :	Values at intersection of row Row_i from node S_i and column Col_k from node R_k
V_{Col_k, Row_i} :	Values at intersection of row Row_k from node R_k and column Col_i from node S_i
A_x, A_y :	Actor nodes.

Notations of Local Set for DKEP

$RowVal_i, ColVal_i$	Row and column values stored at sender S_i and receiver R_k
$RowVal_k, ColVal_k$:	Concatenated string at sender S_i and receiver R_k
$P_{S_i} RC, P_{R_k} RC$:	Messages 1 to 6
M_1-M_6 :	Cipher texts of M_1 to M_6
C_1-C_6 :	Hash at S_i and R_k for nonce, time stamp, row, and column indices
$H_{S_i} RC, H_{R_k} RC$:	Hash calculated at actor A_x for messages received from S_i and R_k
H^*, H^\sim :	Hash of messages exchanged between S_i and R_k via actor A_x
H^+, H^\wedge :	Hash calculated at S_i and R_k for reply
H_{S_i}, H_{R_k} :	Concatenated value at S_i and R_k for reply.
P_{S_i}, P_{R_k} :	

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work is supported by the Deanship of Scientific Research at King Saud University through Research Group no. RG # 1435-051.

References

- [1] J. Yick, B. Mukherjee, and D. Ghosal, “Wireless sensor network survey,” *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

- [2] I. F. Akyildiz and I. H. Kasimoglu, "Wireless sensor and actor networks: research challenges," *Ad Hoc Networks*, vol. 2, no. 4, pp. 351–367, 2004.
- [3] H. Salarian, K.-W. Chin, and F. Naghdy, "Coordination in wireless sensor–actuator networks: a survey," *Journal of Parallel and Distributed Computing*, vol. 72, no. 7, pp. 856–867, 2012.
- [4] M. Imran, M. A. Alnuem, W. Alsali, and M. Younis, "A novel wireless sensor and actor network framework for autonomous monitoring and maintenance of lifeline infrastructures," in *Proceedings of the IEEE International Conference on Communications (ICC '12)*, pp. 6484–6488, Ottawa, Canada, June 2012.
- [5] J. Sen, "A survey on wireless sensor network security," *International Journal of Communication Networks and Information Security*, vol. 1, no. 2, pp. 59–78, 2009.
- [6] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 3, pp. 6–28, 2008.
- [7] P. Sundaram, M. Dharshini, and T. Gnanasekaran, "The unceasing detection of adjoining nodes, its connectivity, weakness impact on wireless sensor networks and actor networks," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 3, no. 1, pp. 1346–1362, 2014.
- [8] J. Du, E. Kranakis, and A. Nayak, "Distributed key establishment in disruption tolerant location based social wireless sensor and actor network," in *Proceedings of the 9th Annual Communication Networks and Services Research Conference (CNSR '11)*, pp. 109–116, IEEE, Ottawa, Canada, May 2011.
- [9] R. Blom, "An optimal class of symmetric key generation systems," in *Proceedings of the EUROCRYPT 84 Workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques*, pp. 335–338, 1985.
- [10] S. Sukumar, "Computational analysis of modified Blom's scheme," in *Proceedings of the Computing Research Repository (CoRR '13)*, 2013.
- [11] A. Parakh and S. Kak, "Matrix based key agreement algorithms for sensor networks," in *Proceedings of the 5th IEEE International Conference on Advanced Networks and Telecommunication Systems (ANTS '11)*, December 2011.
- [12] L.-C. Wu, C.-H. Hung, and C.-M. Chang, "Quorum-based key management scheme in wireless sensor networks," in *Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication (ICUIMC '12)*, February 2012.
- [13] J. Qadir and O. Hasan, "Applying formal methods to networking: theory, techniques, and applications," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 1, pp. 256–291, 2015.
- [14] M. Burrows, M. Abad, and M. Needham, "A logic of authentication," *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 426, no. 1871, pp. 233–271, 1989.
- [15] A. Datta, A. Derek, J. C. Mitchell, and A. Roy, "Protocol composition logic (PCL)," in *Electronic Notes in Theoretical Computer Science*, vol. 172, pp. 311–358, 2007.
- [16] A. Rubin and P. Honeyman, "Nonmonotonic cryptographic protocols," in *Proceedings of the Computer Security Foundations Workshop (CSFW '94)*, pp. 100–116, Franconia, NH, USA, 1994.
- [17] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," *Computer Communications*, vol. 30, no. 11–12, pp. 2314–2341, 2007.
- [18] M. A. Simplício Jr., P. S. L. M. Barreto, C. B. Margi, and T. C. M. B. Carvalho, "A survey on key management mechanisms for distributed Wireless Sensor Networks," *Computer Networks*, vol. 54, no. 15, pp. 2591–2612, 2010.
- [19] W. H. Press, B. Flannery, S. A. Teukolsky, and W. T. Vetterling, *Vandermonde Matrices and Toeplitz Matrices. 2.8 in Numerical Recipes in FORTRAN: The Art of Scientific Computing*, Cambridge University Press, Cambridge, UK, 1992.
- [20] E. Khan, E. Gabidulin, B. Honary, and H. Ahmed, "Matrix-based memory efficient symmetric key generation and pre-distribution scheme for wireless sensor networks," *IET Wireless Sensor Systems*, vol. 2, no. 2, pp. 108–114, 2012.
- [21] W. Bechkit, Y. Challal, A. Bouabdallah, and V. Tarokh, "A highly scalable key pre-distribution scheme for wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 2, pp. 948–959, 2013.
- [22] H. Dai and H. Xu, "Key predistribution approach in wireless sensor networks using LU matrix," *IEEE Sensors Journal*, vol. 10, no. 8, pp. 1399–1409, 2010.
- [23] J. Wan, J. Liu, Z. Shao, A. V. Vasilakos, M. Imran, and K. Zhou, "Mobile crowd sensing for traffic prediction in internet of vehicles," *Sensors*, vol. 16, no. 1, article 88, 2016.
- [24] A. Derhab, A. Bouras, M. R. Senouci, and M. Imran, "Fortifying intrusion detection systems in dynamic Ad Hoc and wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2014, Article ID 608162, 15 pages, 2014.
- [25] M. Imran and N. A. Zafar, "Formal specification and validation of a hybrid connectivity restoration algorithm for wireless sensor and actor networks," *Sensors*, vol. 12, no. 9, pp. 11754–11781, 2012.
- [26] A. Ghafoor, M. Sher, M. Imran, and A. Derhab, "Secure key distribution using fragmentation and assimilation in wireless sensor and actor networks," *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID 542856, 13 pages, 2015.
- [27] P. Kumar, A. J. Choudhury, M. Sain, S.-G. Lee, and H.-J. Lee, "RUASN: a robust user authentication framework for wireless sensor networks," *Sensors*, vol. 11, no. 5, pp. 5020–5046, 2011.

Research Article

System for Malicious Node Detection in IPv6-Based Wireless Sensor Networks

Kresimir Grgic, Drago Zagar, and Visnja Krizanovic Cik

Faculty of Electrical Engineering, Josip Juraj Strossmayer University of Osijek, Kneza Trpimira 2b, 31000 Osijek, Croatia

Correspondence should be addressed to Kresimir Grgic; kresimir.grgic@etfos.hr

Received 24 March 2016; Accepted 15 June 2016

Academic Editor: Fei Yu

Copyright © 2016 Kresimir Grgic et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The trend of implementing the IPv6 into wireless sensor networks (WSNs) has recently occurred as a consequence of a tendency of their integration with other types of IP-based networks. The paper deals with the security aspects of these IPv6-based WSNs. A brief analysis of security threats and attacks which are present in the IPv6-based WSN is given. The solution to an adaptive distributed system for malicious node detection in the IPv6-based WSN is proposed. The proposed intrusion detection system is based on distributed algorithms and a collective decision-making process. It introduces an innovative concept of probability estimation for malicious behaviour of sensor nodes. The proposed system is implemented and tested through several different scenarios in three different network topologies. Finally, the performed analysis showed that the proposed system is energy efficient and has a good capability to detect malicious nodes.

1. Introduction

Numerous intelligent sensors with basic computational and wireless communication capabilities are currently embedded into various devices and instruments worldwide. Since their number is growing rapidly, it could be expected that wireless sensor nodes will vastly outnumber conventional computers and other networked devices in the near future. Wireless sensor networks (WSNs) were the subject of intensive research and development during the last decade [1–3]. Due to strict resource constraints (both power and computational) the implementation of conventional Internet protocol architecture in WSNs used to be avoided at first, resulting in numerous noninteroperable solutions. Further development of WSNs naturally led to efforts to interconnect and integrate a WSN with conventional IP networks. These efforts resulted in certain frameworks and adaptation standards that enable the use of the IP in a WSN environment.

At the same time, a conventional IP network has also evolved and currently passes through the gradual implementation of the IPv6 (Internet Protocol version 6) that should replace the IPv4 in the future [4]. Current technologies of the WSN and IPv6 are highly complementary, and many efforts are currently focused on convergence of IPv6 and low power

multihop WSNs. The integration of sensor networks with IP networks will significantly diversify their array of applications. Certainly, it is possible to realize such integration efficiently and transparently for the end user, but there still remain some problems that require novel adequate solutions or optimization of existing solutions. Seamless integration of sensor networks with IP networks that satisfies demands on flexibility, scalability, and robustness represents the most important foundation for the Internet of Things (IoT) concept [5]. Thereby, the accent is on the implementation of the IPv6, since it provides huge address space and autoconfiguration mechanisms and extensibility (to support future innovations).

Very important aspects of the Internet of Things are security issues and their adequate solutions [6]. Solutions to security issues are an important precondition for wider acceptance and use of integrated sensor networks with IP networks. The implementation of the IPv6 into WSNs brings some specificities that hamper the use of existing security solutions known from IPv6 networks and conventional sensor networks. It is necessary to thoroughly adapt existing solutions and to invent novel solutions for the implementation in IPv6-based sensor networks. Node compromise and malicious behaviour make a quite possible scenario,

especially in networks with a large number of nodes, such as sensor networks.

The lack of quality, effective, and energy efficient intrusion detection system for IPv6-based WSN was the strongest motivation for the authors to focus the research efforts into this area. Existing proposals of intrusion detection systems for WSNs are focused on conventional WSNs, without taking care of certain specificities of IPv6-based WSNs. The fact that IPv6-based WSNs (being the basis of the Internet of Things) may possibly include a very large number of nodes motivated the authors to focus their research on distributed system based on cooperative algorithms and collective decision-making. Diversity of possible applications of IPv6-based WSNs was a motive to develop adaptive system suitable for different application requirements.

Therefore, this paper proposes a system for detecting malicious nodes in an IPv6-based WSN. The proposed system is designed for the IPv6 environment and it supports the IPv6 stack in a WSN. It is implemented into the sensor network that uses the IEEE 802.15.4 standard and the 6LoWPAN adaptation layer. For routing purposes, the RPL (routing protocol for low power and lossy networks) was implemented as the first routing protocol for sensor networks with full support for the IPv6. The UDP (user datagram protocol) is used as the transport layer protocol. The system for malicious node detection is implemented at the application layer. The proposed system uses cooperative algorithms and a collective decision-making procedure, so it is fully distributed and adaptive. Besides node characterization as malicious or legitimate, the system also estimates a probability of malicious behaviour for suspected nodes. The paper presents the implementation of the IPv6 stack into the WSN. Furthermore, the descriptions of the proposed intrusion detection system and its implementation are also given. The system is implemented in different characteristic scenarios, and the obtained results are analysed. Finally, some conclusions are drawn and some suggestions for future development are outlined.

2. IPv6 in Wireless Sensor Networks

The development of the IPv6 started in 1995, when it was obvious that some problems with the IPv4 will become more emphasised in the future (e.g., address space exhaustion, security issues, complex configuration, and routing table enlargement). Compared with IPv4, the IPv6 brings some significant improvements, such as 128-bit address space, a fixed-length simplified header, autoconfiguration mechanisms, and security improvements. Currently, the transition from IPv4 to the IPv6 is a long-lasting ongoing process [7].

Wireless sensor networks (WSNs) represent a special subgroup of mobile ad hoc networks (MANETs). However, strong computational and power limitations make them in some aspects significantly different from conventional MANETs. A WSN consists of a large number of inexpensive sensor nodes capable of sensing, basic data processing, and wireless communication with other nodes. WSN functions are based on communication between nodes and collaborative algorithms. Unfortunately, due to the above-mentioned limitations, most of existing technical and algorithmic solu-

tions known from MANETs cannot be directly applied to the WSN. Therefore, the WSN required adaptations of existing solutions and development of novel ones. Strict demands for low costs, small node dimensions, and energy efficiency noticeably influence the design of networking protocols and algorithms. They are designed with focus on consumption minimisation to prolong network lifetime. Since sensor nodes may be equipped with many different types of sensors, wireless sensor networks have a large variety of possible applications [8]. Sensor nodes with adequate sensors can be used for both continuous monitoring of the observed phenomenon and detection of certain events. In addition to detection, they can also identify the event that occurred and designate its location. Also, sensor nodes can be locally connected with different types of actuators. Today, WSNs are used for various military, environmental, health, home, and industrial applications.

In the beginning of WSN development, the implementation of the omnipresent and generally accepted IP stack into the WSN was considered impractical and inadequate. The IP was considered too demanding to operate properly with strongly limited resources. Therefore, the WSN usually used some alternative solutions (different protocols developed specially for WSNs) and avoided the IP. Unfortunately, a variety of protocols and the absence of a unique standard limited connectivity and interoperability of sensor networks with other types of networks. Consequently, during the last few years many efforts were focused on the implementation of the IP into the WSN, with necessary adaptations [9–11]. Since traditional IP networks are in transition from IPv4 to the IPv6, focus is on the implementation of the IPv6 into WSN.

The IETF working group 6LoWPAN (IPv6 over Low power Wireless Personal Area Network) defined the necessary adaptation layer that enables the implementation of the IPv6 into the WSN protocol stack. The adaptation is indispensable since the frame size used on the WSN physical layer is usually much smaller than that in conventional IP networks. The dominant standard for the physical layer in WSNs is currently IEEE 802.15.4. Therefore, the 6LoWPAN adaptation layer enables adaptation of an IPv6 packet for transmission within the IEEE 802.15.4 frame. The 6LoWPAN adaptation layer defines frame format, forming methods for link-local addresses and address autoconfiguration methods in networks based on IEEE 802.15.4. Additional specifications include methods for IPv6 header compression because of easier transfer over IEEE 802.15.4 links and resource savings. Although the IEEE 802.15.4 standard defines four types of frames (beacon frames, MAC command frames, acknowledgement frames, and data frames), IPv6 packets can be transferred only within data frames. Optionally, acknowledgements for received packets can be used.

A full IPv6 packet is too large for the IEEE 802.15.4 frame which has 127 bytes on the physical layer. Without any compression methods (maximal overhead) and with AES (advanced encryption standard) used on the data link layer, it would leave only 33 bytes available for the application layer data. Clearly, fragmentation would be necessary for larger data transfer. Since the fragmentation process consumes

additional resources, the 6LoWPAN adaptation layer focuses on header compression possibilities to get packets that could in most cases fit into the IEEE 802.15.4 frame. 6LoWPAN also defines compression of the UDP header and in the best case (local unicast communication) the UDP and IPv6 header can be compressed into 6 bytes.

The IETF working group ROLL (Routing Over Low power and Lossy networks) specified a new RPL (where wireless sensor networks also belong). The RPL is the first routing protocol with IPv6 support suitable for sensor networks. It was designed as a modular protocol, with a mandatory core part and optional application-dependent features. It was used as a routing protocol for an IPv6-based WSN in all analysed scenarios [12].

3. Security Aspects of Wireless Sensor Networks

Security issues in wireless networks are more challenging than in wired networks due to the open nature of the communication medium. Therefore, it is often more difficult to secure MANETs compared to conventional wired networks. Although WSNs are a special subset of MANETs, their strong resource limitations bring additional difficulties in their security aspects. Since most of wireless networks also use the TCP/IP stack, most of security threats known from wired networks persist in wireless networks [13, 14]. Further, a wireless environment brings some new security threats unknown in wired networks. There are some differences between the WSN and MANET that disable a direct implementation of known MANET security mechanisms into the WSN: the WSN may have a significantly larger number of nodes that are more densely deployed, sensor nodes are prone to failures (due to environmental effects and limited power supply) and have stronger resource limitations than a typical MANET node, and WSNs usually use a broadcast communication paradigm, while point-to-point communication still dominates in MANETs [15–19].

Specified differences make WSNs more vulnerable to denial-of-service attacks. Also, well-known public key cryptography methods are still practically inapplicable in WSNs because of their computational demands. Development of quality key management mechanisms, secure routing protocols, secure data aggregation mechanisms, and intrusion detection mechanisms still represents a great challenge in WSNs, especially in an IPv6-based WSN.

Providing physical security of every sensor node in the WSN would require significant costs, which would also be contrary to the WSN concept as a network of cheap network nodes. Therefore, in most cases WSNs are considered to be prone to physical attacks, and research is focused on different methods for detection and prevention of different possible attack types where the attacker does not have any physical contact with sensor nodes or the base station.

A large variety of possible attack types can be classified according to different criterions. The attacks on the WSN can be divided into outsider attacks (originated from nodes that do not belong to the targeted network) and insider attacks (former legitimate nodes are compromised and start

with malicious behaviour) [20]. Also, attacks can be passive (eavesdropping and tracking of transferred data) or active (include certain modifications of existing dataflows and creating of new data intentionally by the attacker). The attacks on the sensor network can be focused on confidentiality and authentication, network availability (denial-of-service attacks), or data and service integrity.

The attacks focused on the physical layer are jamming and tampering. The attacker can use their transmitter to cause interference intentionally on WSN operational frequencies. Advanced methods for interference avoidance (like FHSS communication) increase sensor node complexity and raise their cost and energy consumption. Since in most WSNs communication is limited to only one channel, they are usually very vulnerable to jamming attacks. Also, in most cases sensor nodes are not physically protected, so they are exposed to tampering. Therefore, all security mechanisms for WSNs have to predict possible compromise of certain nodes and to implement a mechanism for their exclusion from the network [21].

If two or more nodes try to transmit at the same frequency, the collision will occur, causing packet loss. The attacker may intentionally cause collisions, most frequently during transmissions of acknowledgements. It is not difficult to detect such attack type, but it is very difficult to protect against them. If collision occurs, nodes continuously try to retransmit the packets, which may result in resource exhaustion [22, 23]. Resource exhaustion by retransmission can be reduced by limiting the frequency of medium access (on the MAC layer) and by using time-division multiplexing.

Some attacks on sensor networks focus on a routing mechanism, where the attacker spoofs or modifies routing information. In this way, the intruder can intentionally create routing loops, attract or reject network traffic, change existing routes, increase latency, and generate false error messages [24]. Some of these problems can be reduced or avoided by using message authentication codes and timestamps. Most WSNs use the multihop communication principle, assuming that every sensor node will act as a router and forward packets toward their destination. The malicious node can intentionally drop some packets and disable their further propagation. The easiest case to detect is when the intruder drops all incoming packets and refuses to forward them to their neighbours (a “black hole” attack). It is more difficult to detect the case when the attacker forwards packets selectively (a selective forwarding attack). A possible countermeasure is the use of multiple routes. The attacker can also falsify routing data (e.g., advertising quality route to the base station) in order to attract all traffic from a certain network part (a sinkhole attack). A sinkhole attack can be prevented by using exact geographic location data in the routing procedure [25, 26].

The attacker frequently uses hardware that is much more powerful than the average sensor node (e.g., a notebook computer). In that case, the attacker can use several false identities at the same time, when they introduce themselves as several legitimate nodes (a Sybil attack). A Sybil attack may have a significant impact on the data aggregation process and other distributed networking mechanisms (e.g., distributed data storage or an intrusion detection system). Possible

measures to prevent Sybil attacks must include a node identity validation mechanism [27]. If the attacker has two notebook computers, they can create a low-latency fast link between two distant network parts that is invisible for legitimate nodes (a wormhole attack). Possible countermeasures include precise temporal or geographical marking of every packet (which assumes precise network time synchronisation and exact location data) [28].

Attacks targeted at transport layer protocols usually misuse the connection establishment mechanism. The attacker repeatedly sends requests to connect in order to exhaust resources required for connection establishment. In that case, legitimate connection requests will be ignored due to lack of required resources. Also, some security threats in WSNs target directly the application layer, when the attacker tries to excessively stimulate sensors causing intensive data transfer that exhaust network resources (an overwhelm attack). Negative impacts of such attacks can be reduced by limiting the frequency of sensor readings and by implementing of an effective data aggregation mechanism.

4. Intrusion Detection in Wireless Sensor Networks

Damage caused by unauthorized intrusions into computer systems and networks can be enormous with immense consequences. Consequently, intrusion detection and prevention systems are currently a very important security mechanism used in modern networks [29–31]. The spread of wireless networks has posed some new challenges and demands for IDS (intrusion detection system) development [32, 33]. Appearance and spread of WSNs requested development of IDS adjusted especially for the WSN. Development and implementation of intrusion detection systems designed for WSNs are still an intensive research area [34–38]. Due to constrained resources and other influencing factors, the implementation of IDS into a WSN represents a great challenge. Some of the important factors that affect the intrusion detection problem in WSNs are network topology, node mobility (mobile or stationary nodes), openness (allowed access for new nodes), current application, environment, routing algorithm, use of encryption, and interconnection with other networks.

Although there are some recent proposals of the intrusion detection systems for WSNs, generally they are intended for the conventional WSNs [39, 40]. There are also some attempts to improve routing mechanism in order to mitigate some types of attacks [41]. Therefore, there is still a lack of adequate IDS especially adapted for IPv6-based WSN with full IPv6 support implemented. The proposed IDS aspires to contribute to solution for this problem. In respect of detection methods and algorithms, the proposed system has certain similarities with some other intrusion detection systems proposed for conventional WSNs. It can be classified as a fully distributed and cooperative system that does not rely on any centralized network infrastructure. Consequently, it is most suitable for flat network infrastructures where each node cooperatively participates in all decisions and actions. There are some examples of the recently proposed distributed

systems for conventional WSNs [42, 43]. On the other hand, some recent proposals of the intrusion detection systems for conventional WSNs rely on a hierarchical (multilayer) or clustered network structure [44]. The proposed system implements specification based intrusion detection technique, as probably the best compromise with low false alarm rate and low energy and resource demands. There are some recently proposed IDS for conventional WSNs that also implement specification based detection [45], while some examples rely on the misuse based or anomaly based detection [46]. Some proposed solutions deal with mobility of network nodes [47]. Some authors introduce different possible detection methods (based on data mining, machine learning, game theory, or genetic algorithms) which require adaptation for implementation into the IPv6-based WSN [48, 49]. Most of the proposed solutions still focus on certain attack type and reside at particular network layer (usually the application layer) [50–52]. Certainly, in the future the research focus should be on cross-layer solutions integrated into the unique security framework with other security mechanisms.

An intrusion detection system developed for a wireless sensor network should satisfy the following requirements and characteristics: distributed architecture (both for data collection and for decision-making), minimal resource consumption (reducing communication as much as possible), finding a compromise between IDS effectiveness and monitoring area size, local data collection and analysis (without relying on central infrastructure), the fact that node compromise must not disrupt proper network function, the fact that neither node may be considered as absolutely secure and reliable, and the fact that the system should operate in real-time. The proposed distributed system for malicious node detection in the IPv6-based WSN tends to satisfy these requirements as much as possible.

Generally, there are two dominant types of WSN architecture: flat architecture (all sensor nodes are similar and use hop-by-hop communication) and hierarchical architecture (nodes are grouped into clusters, where a cluster head is responsible for routing operations). Network architecture has direct influence on positioning of IDS modules. There are a few typical positioning strategies of IDS modules: promiscuous monitoring (IDS module on every sensor node listening to all traffic inside the range of its receiver), IDS module on every node analysing only packets that it forwards, IDS module on the base station (full centralization), IDS modules on base station's neighbours, and IDS modules on cluster heads. There are some proposed solutions for intrusion detection in conventional WSNs, but most of them are focused on a single specific attack type and do not provide integral network security. Also, they mostly do not support the IPv6, so their implementation into the IPv6-based WSN would require proper adaptations and modifications. There is still a problem remaining and it refers to a lack of a quality and efficient intrusion detection system intended for IPv6-based wireless sensor networks and adapted for all specificities of such environment.

The implementation of several different independent security mechanisms into WSNs makes their maintenance more difficult. Therefore, they have to be integrated through

the unique cross-layer security framework [53]. The unique security framework should integrate different security mechanisms to provide basic security premises, that is, confidentiality, authentication, integrity, and availability. It should provide the possibility of data encryption (implying also the implementation of a secure key management mechanism), ensure secure data routing (supporting multiple and alternative routes), and include techniques for secure node localization and secure data aggregation [54–56]. One of the most important components of the quality security framework should be a system for detection of intrusions and malicious node behaviour.

The proposed distributed adaptive system for detection of intrusions and malicious node behaviour was implemented into the unique security framework for the IPv6-based WSN as its intrusion detection module (along with a cryptographic module, a secure routing module, and a secure data aggregation module).

5. Distributed Adaptive IDS for IPv6-Based WSN

Numerous security issues present in wireless sensor networks directly affect the design of security mechanisms, including the intrusion detection system. Some typical problems are as follows: resource limitation (which causes the need for reduced communication and disables the possibility of using the IPsec and public key cryptography), various possible security threats and attack types (denial-of-service, routing attacks, sinkhole, Sybil, wormhole, etc.), and key management problems.

The intrusion detection system for the IPv6-based WSN has to fulfil some general demands just like in the conventional WSN. It should provide an automated mechanism for attack source identification (a malicious network node), generate proper alert for the rest of the network, and take proper preventive measures. Every action targeted against data, communication, or computing resources can be considered as an attack. In order to properly detect an attack, IDS must be able to distinguish legitimate network activities from abnormal (malicious) ones. It could be a serious problem, since in larger networks possible legitimate activities can be vague and unpredictable. For distinguishing and classification of these activities we usually use one of the three following approaches: misuse detection, anomaly detection, and specification based detection.

The misuse detection technique compares current network activities with known attack signatures (behaviour patterns of known malicious activities). Therefore, it is often called signature-based detection. Its main disadvantage is possible detection of only previously known malicious activities for which the sensor node has a stored signature. The anomaly detection approach includes a learning phase, when the IDS learns the pattern of normal network behaviour. All statistical deviations from normal behaviour may in that case be categorized as malicious behaviour. The main disadvantage of this method is a relatively large number of false alarms. Specification based detection combines properties of these two methods, and it is chosen as the most appropriate

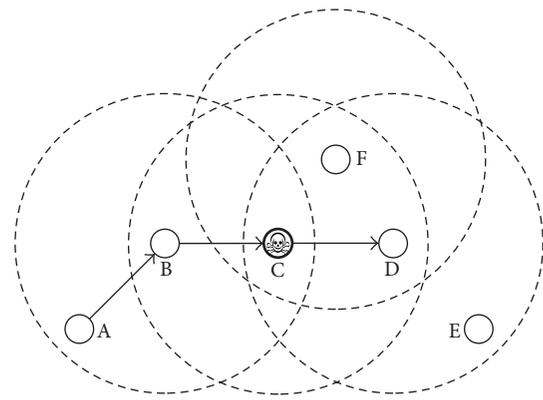


FIGURE 1: Watchdog technique: a possible error example.

method for the proposed IDS for the IPv6-based WSN. Like the anomaly detection technique, it also detects deviations from normal behaviour, but it has manually predefined specifications that describe normal network behaviour. Such approach is less resource demanding, and at the same time it also enables detection of novel attack types.

The proposed IDS is fully distributed and it relies on the cooperative decision-making procedure. Identical IDS modules are implemented on every wireless sensor node, executing cooperative algorithms and communicating with other modules. Since the system is fully distributed, every network node monitors network traffic. The watchdog technique is used for traffic monitoring purposes. It is assumed that every network node has several neighbouring nodes inside the range of its transceiver. Accordingly, all IDS modules listen to their neighbour's traffic and collect data that represent input parameters into collective decision-making process.

Figure 1 illustrates the situation when node A sends a packet to node D (route A-B-C-D). Node C is malicious, and it selectively drops packets addressed to node D. After sending the packet to node C, node B listens to whether node C forwards packet to node D (node B acts as a watchdog). If at the same time node A transmits to node B, due to collision, node B will not be able to determine if node C forwards packets or not. Also, it is possible that node B wrongly concludes that node C successfully forwarded the packet to node D. It will happen if node D or node E starts transmission at the same time. Therefore, it is clear that only one watchdog node is insufficient for successful detection of malicious behaviour. That is why IDS modules collect data from more surrounding watchdog nodes, where nodes cooperatively make final decisions.

At first sight, it seems that traffic monitoring by watchdog nodes will significantly increase power consumption. Fortunately, it is not true, since in most radio communication systems implemented in WSNs sensor nodes already receive packets broadcasted from their neighbours. Therefore, additional power is used only for additional data processing and for communication between IDS modules.

The intrusion detection problem (IDP) includes detection that a certain network node is attacked (compromised) as well

as identification of the attack source. Therefore, a solution (algorithm) to the IDP must satisfy the following properties:

- (i) If a legitimate node indicates possible malicious behaviour of another node, it will join the group of alerted nodes, and a potentially malicious node will be characterized as the attack source.
- (ii) If a malicious activity occurs, after a finite time interval all legitimate nodes from the group of alerted nodes will indicate possible malicious behaviour of the observed node.

The basic idea of cooperative intrusion detection is a mutual exchange of IDS agents (modules) output data. Modules exchange data about suspicious nodes, narrowing the group of possible malicious nodes. It is also possible that a malicious node falsely accuses its neighbours of malicious activities. There are two main conditions for solving the intrusion detection problem: intrusion detection condition (IDC) and neighbourhood conditions (NC). Intrusion detection condition is satisfied if neither network node has an identical alerted set as the malicious node. There are two neighbourhood conditions: all neighbours of the malicious node are alerted (first condition) and if two or more nodes are suspected by a majority of nodes, then all legitimate suspected nodes must have nonalerted neighbours (second condition). The intrusion detection problem (IDP) can be solved by a deterministic algorithm if (and only if) intrusion detection condition (IDC) or neighbourhood conditions (NC) are satisfied.

The Contiki operating system was used as a software platform for the implementation of a distributed adaptive intrusion detection system [57]. Contiki was one of the first operating systems for sensor networks that supports the IP. First, it was IPv4 support, and then after 6LoWPAN specification the IPv6 support was added. The implementation of IPv6 support was followed by support for the RPL. Support for IPv6 and RPL were the reasons for using the Contiki operating system. For testing and simulation purposes, we used the COOJA simulator, since it fully supports the Contiki OS at multiple levels, from machine code level to operating system level [58].

The system for malicious node detection in the IPv6-based WSN is a fully distributed system, based on collaborative algorithms without relying on central infrastructure. IDS modules (agents) are implemented on every node in the WSN. The main task of the IDS agent is to monitor neighbouring nodes (within transceiver range) and to participate in the collective decision process. The implemented algorithm operates independently of the primary sensor network application. The system is fully adapted for the protocol stack in the IPv6-based WSN (Figure 2).

The IDS agent core operates on the application layer. The UDP is used as the transport layer protocol, while the RPL is implemented as a routing protocol [59]. The 6LoWPAN adaptation layer is implemented for IPv6 header compression purposes, enabling the efficient transfer of IPv6 packets over the IEEE 802.15.4 physical layer [60]. Functionality of the IDS agent can be divided into the following three

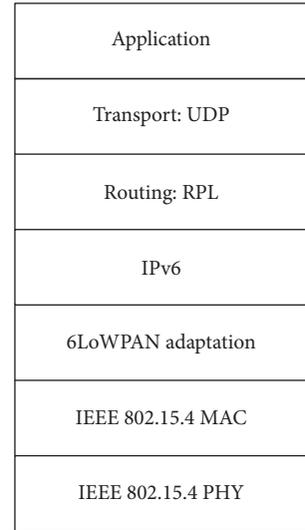


FIGURE 2: IPv6-based WSN protocol stack.

basic components: network monitoring (data gathering by monitoring neighbours' network traffic), decision-making (a collective process based on exchanged data through mutual communication and collaboration between IDS agents), and reaction (action in case malicious behaviour of a certain node has been detected). After sending the packet, every node monitors its neighbours in order to determine whether they forward packets further toward their final destination or not (a watchdog approach). Nonforwarded packets may indicate malicious behaviour, since in the WSN surroundings many other factors may also influence packet delivery success (e.g., collisions or node failures).

Therefore, the intrusion detection system defines a finite time interval in which the IDS module counts dropped packets on neighbouring nodes. The duration of this interval is a variable and adjustable parameter. Also, the threshold is defined that represents the maximal number of allowed packet drops. If dropped packets outnumber the threshold, the observed node is considered suspicious. This threshold is also a variable and configurable parameter that can be defined according to current application and network conditions. Due to a large variety of WSNs (regarding number and density of nodes, link capacity, and data amount) and their possible applications, it is impossible to set universal values of these parameters (monitoring interval and threshold) for all situations. Parameter values should be adjusted for every particular application. The proposed IDS uses a specification based detection approach, since other approaches (misuse detection or anomaly detection) would be more resource demanding. The structure of the IDS for the IPv6-based WSN is presented in Figure 3.

An intrusion detection agent consists of two main modules: a local detection module and a cooperative detection module. These modules are interconnected and together they participate in the process of detecting malicious sensor nodes. These two modules are also connected with a module for local traffic monitoring and with communication modules (for communication with other IDS agents and with the

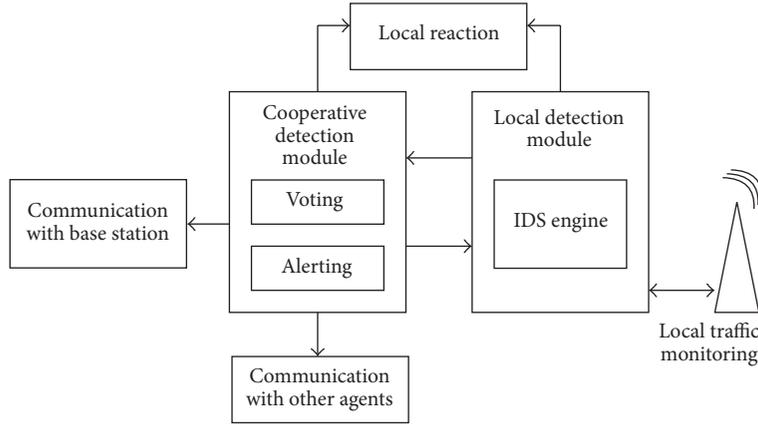


FIGURE 3: Intrusion detection system structure.

base station). Communication modules are indispensable for construction of the distributed system, since its proper functioning is based on cooperation of many IDS agents.

5.1. Local Detection Module. A local detection module is connected to a local traffic monitoring module that gathers data required for local decisions. This module analyses gathered data and creates a list of suspected neighbouring nodes (according to previously defined specifications). The local detection module alerts other neighbouring nodes about its suspect list. Every node creates a list of its suspected neighbours (neighbours whose behaviour can be characterized as possibly malicious). Also, the local detection module estimates the probability of malicious behaviour of its neighbours. This probability estimation is based on the number of forwarded and dropped packets during the observed time interval. Every node s estimates the probability of malicious behaviour of its neighbour i according to

$$p_m(i) = 1 - \frac{n_f(i)}{n_r(i)}, \quad \forall i \in N(s). \quad (1)$$

$p_m(i)$ is the estimated probability that neighbouring node i behaves maliciously, $n_r(i)$ is the number of packets that node i receives, $n_f(i)$ is the number of packets that node i forwards, and $N(s)$ is a set of neighbouring nodes of node s . If estimated probability $p_m(i)$ exceeds the predefined threshold value, node i will be added to the suspect set $D(s)$ of node s . Node s exchanges its list of suspected nodes (together with estimated probabilities) with other network nodes. After alert messages (which contain lists of suspected nodes and estimated malevolence probabilities) are exchanged, when all nodes gather messages from other nodes, the cooperative detection module is being activated. The cooperative detection module will make the final decision about suspected nodes. A trivial case is the situation when a certain sensor node has only one neighbouring node on its suspect list with the estimated malevolence probability equal to 1. In that case, the local detection module can directly activate local reaction and communication modules, without any need for

the cooperative decision procedure. Figure 4 represents the operating algorithm of the local detection module.

5.2. Cooperative Detection Module. The main task of the cooperative detection module is to make the final decision about behaviour character of suspected sensor nodes. The module makes this decision cooperatively with other nodes. The decision is made after executing the cooperative algorithm that implements a majority voting mechanism about node malevolence. Input data for the cooperative decision-making process are suspect node lists together with estimated malevolence probabilities. The final malevolence probability for every network node is calculated after execution of cooperative algorithms. If this value outnumbers the predefined threshold, the corresponding node will be finally declared as malicious. The final probability for every node is calculated by (2), where $p_M(s_i)$ is the final calculated malevolence probability for node s_i . Consider

$$p_M(s_i) = \frac{1}{n} \sum_{i=1}^n p_m(i), \quad \forall s_i \in S. \quad (2)$$

This probability is calculated as the average of all estimated probabilities $p_m(i)$ by all nodes that put node s_i into the suspected set. If probability $p_M(s_i)$ is above the predefined threshold value, the corresponding node will be considered malicious. In case more probabilities are above the threshold, the node with most votes will be classified as malicious. Node with the largest estimated malevolence probability $p_M(s_i)$ will be declared malicious if some nodes have an equal number of votes. In case behaviour of certain nodes is marked as malicious, the cooperative detection module activates communication modules in order to inform the base station and other network nodes. Malicious nodes will be excluded from the network by local reaction modules. Figure 5 presents the algorithm for the cooperative detection module.

5.3. Testing Scenarios. Behaviour of the proposed system for malicious node detection in the IPv6-based WSN was analysed and tested through different scenarios typical of sensor

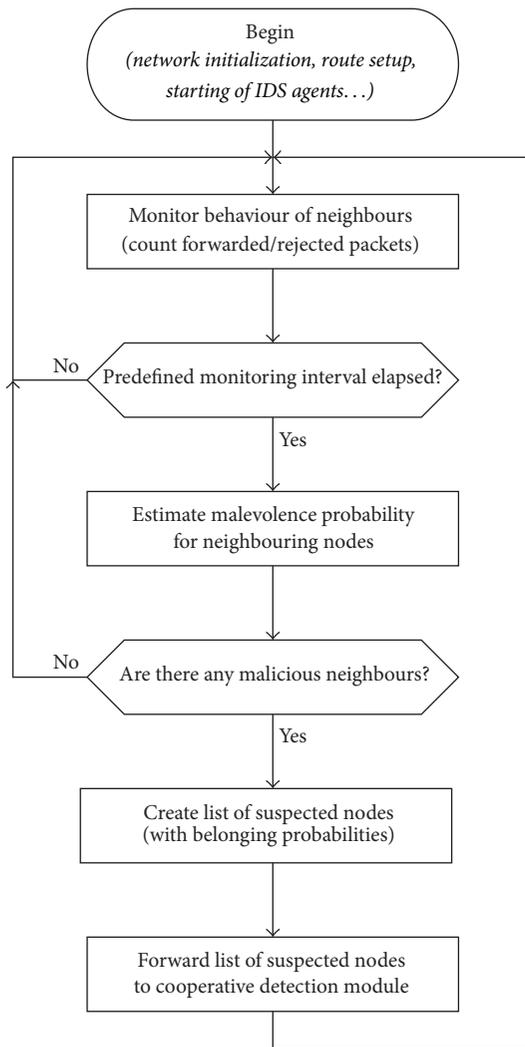


FIGURE 4: Local detection module algorithm.

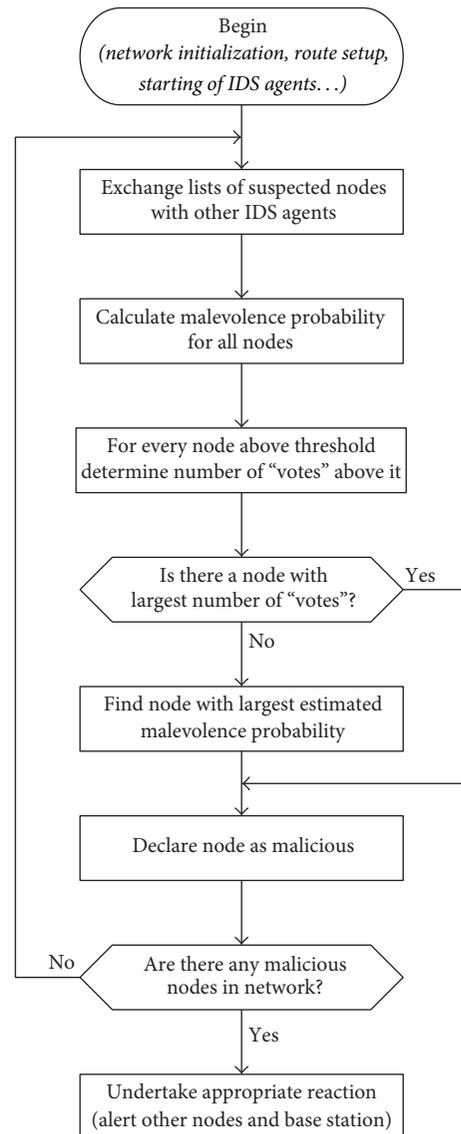


FIGURE 5: Cooperative detection module algorithm.

networks. The possibility of successful detection of nodes' malicious behaviour and the system influence on normal network functioning (primarily on power consumption and bandwidth occupation) were the focus of analyses and tests.

All tests were performed in three different networks. The first network consists of 6 nodes (5 sensor nodes and the base station), the second network consists of 10 nodes (9 sensor nodes and the base station), and the third network consists of 17 nodes (16 sensor nodes and the base station). These topologies were chosen because they reflect a large variety of practical sensor network applications. In all testing scenarios, the base station is located near the edge of the network area in order to enforce multihop communication. All network nodes have the same physical characteristics (a homogenous network) and the implemented IPv6 stack.

Three scenarios were analysed in every network (6, 10, and 17 nodes). The difference between these scenarios lies in the probability of successful sending and receiving of data packets. The first scenario represents a reference ideal case, where this probability equals 100%. However, the

packet loss in WSN is common due to interference, node failures, or collisions and sometimes malicious activities. It is very important to consider these situations, since packet losses and a need for retransmission directly affect network performance and resource consumption and also complicate (in extreme situations even prevent) detection of malicious activities. For that reason, beside ideal scenario two additional scenarios in all three networks are analysed. In the second scenario, in all networks Rx/Tx success ratio was 80%, and in the third scenario it was 60%.

Previous analysis of the WSN without intrusion detection system was performed for performance testing purposes (total of 9 scenarios, three scenarios in three different networks), in order to analyse normal network behaviour without any IDS influence on WSN performance. Thereby, sensor nodes collect data from their surroundings (temperature, humidity, and illumination) and send them to the base

station periodically (every minute). In all performed tests, the network was monitored during the one-hour interval. In every testing scenario, after network initialization and route establishment, the number of neighbours and the number of hops to the base station were recorded for every node. Since in observed scenarios all nodes were static, these values are generally related to network topology. Therefore, for the same network they did not significantly change depending on the analysed scenario (minor changes may occur if packet loss causes network reconfiguration and changes in some parts of the routes). The following parameters were observed and recorded for all testing scenarios: the number of received packets (for every node), the number of lost packets, ETX metrics (which shows the required number of retransmissions on individual links), an average radio duty cycle (for every network node), and power consumption (average for every network node). Total power consumption for every node includes the following four components: CPU consumption, consumption in low power mode (LPM), and radio transceiver consumption in listen and in transmit mode. The results obtained are used for comparison with identical scenarios, but with the proposed intrusion detection system implemented into the network (topology and all other parameters remained unchanged) in order to analyse the impact of the IDS on normal network operation. The goal was to investigate if the implemented IDS distorted network performances and whether it causes significant power consumption increment. Therefore, after IDS implementation, the analysis was repeated through all nine characteristic scenarios.

In addition to performance testing, the analysis of malicious behaviour detection capabilities of the proposed IDS was also performed. Detection capability analysis was also accomplished through the nine mentioned scenarios (three characteristic scenarios in three different networks), since detection capability is directly influenced by the total number of nodes and the number of networking nodes, as well as the number of unintentionally dropped packets. Every analysed scenario included one malicious node that selectively forwards packet, where it drops 80% of the packets. Two different situations were taken into consideration for every analysed scenario. In the first case, a malicious node selectively drops packets without accusing its neighbours of malicious behaviour. In the second case, a malicious node falsely accuses its neighbours of malicious behaviour, trying to disrupt IDS detection capabilities. IDS detection capabilities were analysed through all described scenarios, where the system also estimates malevolence probabilities of network nodes. The performed analyses resulted in certain conclusions about the influence of the number of nodes, the number of dropped packets, and malicious node behaviour on detection capabilities of the proposed IDS.

6. Result Analysis

6.1. IDS Performance Analysis. Performance analysis of the proposed IDS was performed through 9 different scenarios in three previously described different networks (6 nodes, 10 nodes, and 17 nodes). The first testing network includes

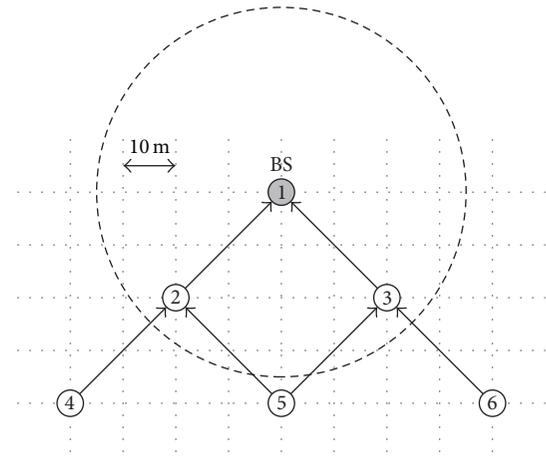


FIGURE 6: Six-node network topology.

6 nodes (5 sensor nodes and the base station), as shown in Figure 6.

Node 1 is the base station, while the others (2–6) are regular sensor nodes. Raster pattern size in the figure matches 10 m distance. A radio transceiver range is set to 30 meters (circular area), while the interference area radius equals 50 meters. These values directly influence network topology and the establishment of the routes to the base station, since the possibility of direct communication between nodes depends on their transceiver range. In a 6-node network, the base station is within the range of nodes 2 and 3. Neighbouring nodes are nodes that can directly communicate with each other. Therefore, a neighbouring node of node 4 is node 2, while a neighbouring node of node 6 is node 3. Neighbouring nodes of node 5 are nodes 2 and 3. Accordingly, nodes 2 and 3 have three neighbours, and node 5 has two neighbours, while nodes 4 and 6 have one neighbouring node. Consequently, routes from nodes 4, 5, and 6 to the base station include 2 hops, while nodes 2 and 3 can directly communicate with the base station.

After network initialization, every network node periodically (once a minute) sends its sensor readings to the base station (temperature, humidity, and illumination). Three scenarios with a different Rx/Tx success ratio were analysed. This ratio is 100%, 80%, and 60%, in the first, second, and third scenario, respectively. All tests were performed with and without the intrusion detection system implemented, in order to draw a conclusion about the IDS impact on network performance. Values of observed parameters (described in Section 5.3) are collected for all sensor nodes, and their summarized average values for 6-network nodes are given in Table 1.

In the first analysed scenario (which represents an ideal case, with no packet loss), the increased number of received packets can be noticed after the implementation of the IDS. It was expected since additional traffic is generated by the IDS agents. However, it is important to notice that there is no significant change in total energy consumption (since energy is the most limited resource in the WSN) after the IDS implementation. Some minimal deviations in recorded

TABLE 1: Performance analysis of 6-node network.

6 nodes	Received packets	Lost packets	Hops to BS	ETX	Energy consumption (mW)				Duty cycle (%)		
					CPU	LPM	Listen	Transmit	Total	Listen	Transmit
Scenario 1 (Rx/Tx = 100%)											
w/o IDS	59.200	0.000	1.600	1.008	0.065	0.162	0.391	0.033	0.650	0.651	0.062
w/ IDS	65.800	0.000	1.600	1.002	0.064	0.162	0.389	0.029	0.649	0.649	0.054
Scenario 2 (Rx/Tx = 80%)											
w/o IDS	58.400	0.600	1.600	2.256	0.083	0.161	0.419	0.146	0.808	0.699	0.274
w/ IDS	65.800	0.600	1.600	2.057	0.083	0.161	0.423	0.138	0.806	0.706	0.260
Scenario 3 (Rx/Tx = 60%)											
w/o IDS	50.600	7.000	1.629	5.991	0.135	0.159	0.514	0.484	1.292	0.857	0.912
w/ IDS	57.800	8.800	1.600	5.793	0.134	0.159	0.521	0.498	1.312	0.868	0.938

values can be explained by the application of stochastic algorithms and inability to measure real consumption very precisely. In the second scenario (with the Rx/Tx success ratio of 80%), smaller packet loss can be noticed in spite of acknowledgement and retransmission mechanisms used. An increment of the ETX compared to the first scenario shows that retransmission of some packets was necessary. A need for packet retransmission leads to an increased transceiver activity, which can be observed from their duty cycle. Since the radio transceiver is the most energy demanding part of the sensor node, its increased activity leads to an increase in energy consumption compared to the first scenario. However, the implementation of the IDS still does not bring any significant difference in energy consumption (compared to the same scenario without the IDS). The third scenario additionally increases the need for packet retransmission (the indicator is increased ETX), since the packet Rx/Tx success ratio is reduced to 60%, resulting in increased energy consumption. In spite of the retransmission mechanism, an increased number of lost packets were recorded. In the third scenario with the implemented IDS, a slight increase in energy consumption compared to the case without the IDS can be noticed.

The second testing network consists of 10 nodes (9 sensor nodes and the base station). The topology of second testing network is shown in Figure 7.

As in the first network (6 nodes), testing was performed through three scenarios, where the Rx/Tx success ratio was 100%, 80%, and 60%, respectively. In a 10-node network, nodes have from 2 to 5 neighbouring nodes (nodes 3, 7, and 9 have 2 neighbours; nodes 1, 6, and 8 have 3 neighbours; nodes 2 and 4 have 4 neighbours; and node 5 has 5 neighbours). Nodes 1, 2, 4, and 5 have one hop to the base station, nodes 3, 6, 7, and 8 have two hops, and node 9 has three hops. Average values of observed parameters in a 10-node network are summarized in Table 2.

The first analysed scenario in a 10-node network also represents the ideal case, without lost packets and any need for retransmission. The implementation of the IDS introduces a small amount of additional network traffic (generated by the IDS agents), without a significant influence on total energy consumption. Total average energy consumption of the first scenario in a 10-node network is comparable to an equivalent

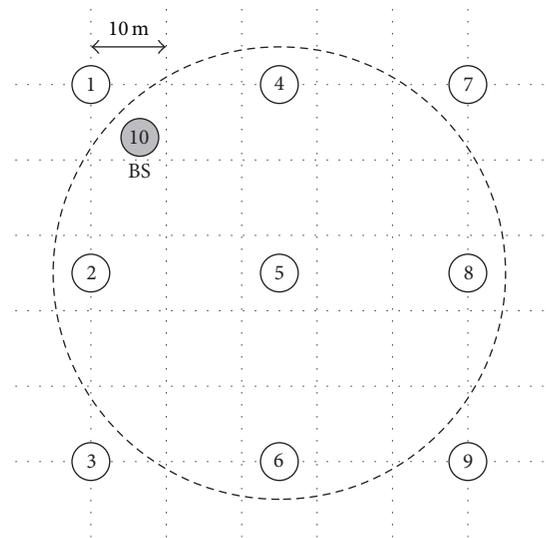


FIGURE 7: 10-node network topology.

scenario in a 6-node network. A decreased probability of successful packet transmissions in the second scenario causes packet loss and retransmissions. An increased transceiver activity increases energy consumption, which is comparable with consumption in an equivalent scenario in a 6-node network. The implementation of the IDS slightly increases energy consumption, but not to the extent of making the IDS implementation not justified. Further decrement of the Rx/Tx success ratio in the third scenario (to 60%) additionally increases the number of required retransmissions (the indicator is the ETX metrics) and energy consumption. Total consumption rises after the implementation of the IDS, but the increment is less than 10% and does not jeopardize validity of the IDS implementation.

Three different scenarios (with the Rx/Tx success ratio of 100%, 80%, and 60%) were also analysed in a 17-node network. The topology of the third testing network is shown in Figure 8 (nodes 1-16 are regular sensor nodes, and node 17 is the base station).

In a 17-node network, sensor nodes have 2 to 5 neighbours (nodes that are in a direct transceiver range). The minimal

TABLE 2: Performance analysis of 10-node network.

10 nodes	Received packets	Lost packets	Hops to BS	ETX	Energy consumption (mW)				Duty cycle (%)		
					CPU	LPM	Listen	Transmit	Total	Listen	Transmit
Scenario 1 (Rx/Tx = 100%)											
w/o IDS	62.222	0.000	1.667	1.000	0.064	0.162	0.392	0.029	0.647	0.654	0.055
w/ IDS	67.444	0.000	1.667	1.000	0.065	0.162	0.394	0.032	0.652	0.657	0.060
Scenario 2 (Rx/Tx = 80%)											
w/o IDS	58.667	1.222	1.690	1.766	0.081	0.161	0.431	0.133	0.806	0.718	0.250
w/ IDS	65.889	0.667	2.079	1.914	0.098	0.161	0.473	0.219	0.951	0.789	0.412
Scenario 3 (Rx/Tx = 60%)											
w/o IDS	51.889	7.333	1.692	5.148	0.122	0.160	0.527	0.409	1.218	0.878	0.770
w/ IDS	50.556	10.556	1.718	4.554	0.134	0.159	0.544	0.478	1.315	0.907	0.899

TABLE 3: Performance analysis of 17-node network.

17 nodes	Received packets	Lost packets	Hops to BS	ETX	Energy consumption (mW)				Duty cycle (%)		
					CPU	LPM	Listen	Transmit	Total	Listen	Transmit
Scenario 1 (Rx/Tx = 100%)											
w/o IDS	59.500	0.000	2.563	1.001	0.068	0.161	0.405	0.042	0.676	0.675	0.079
w/ IDS	66.625	0.000	2.563	1.000	0.069	0.161	0.407	0.043	0.680	0.678	0.081
Scenario 2 (Rx/Tx = 80%)											
w/o IDS	58.375	1.250	2.582	2.001	0.108	0.160	0.502	0.276	1.047	0.837	0.520
w/ IDS	64.563	1.750	2.648	2.029	0.110	0.508	0.847	0.289	1.068	0.847	0.545
Scenario 3 (Rx/Tx = 60%)											
w/o IDS	44.267	13.867	2.366	5.574	0.160	0.159	0.644	0.605	1.568	1.073	1.140
w/ IDS	44.125	13.313	2.538	5.714	0.168	0.158	0.657	0.666	1.649	1.095	1.255

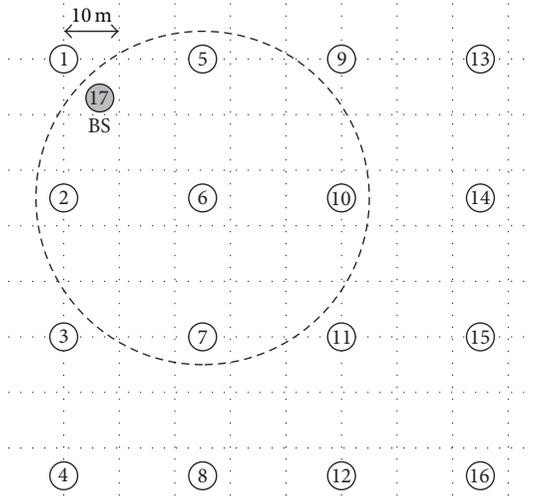


FIGURE 8: 17-node network topology.

distance from the base station is one hop (for nodes 1, 2, 5, and 6), while maximal distance is 5 hops (for node 16). Average values of observed parameters in a 17-node network are summarized in Table 3.

Similarly to 6-node and 10-node networks, the first scenario in a 17-node network is the ideal case without packet losses and retransmissions. Also, there is no significant

difference in power consumption for this scenario before and after the IDS implementation. In the second scenario, some packet losses appear, and packet retransmissions increase average energy consumption. Average energy consumption is slightly larger than in equivalent scenarios in 6-node and 10-node networks, but the implementation of the IDS in this scenario does not increase energy consumption significantly either. The third scenario in a 17-node network (the Rx/Tx success ratio is 60%) records the largest number of lost packets and retransmissions and consequently the smallest number of received packets. Moreover, in one case, due to excessive packet loss, the furthest node (node 16, i.e., 5 hops far from the base station) could not communicate with the base station. As expected, the third scenario in a 17-node network records the highest energy consumption. However, even in this scenario the implementation of the IDS does not significantly increase energy consumption.

The performed analyses show that the implementation of the proposed system for detection of malicious node behaviour in the IPv6-based WSN does not significantly degrade network performance. Also, it is a very important fact that the implementation of the proposed IDS does not lead to a significant increase in energy consumption as the most limited resource in the WSN. Moreover, in some analysed scenarios the difference in power consumption with and without the IDS is almost indistinguishable (because its magnitude is smaller than possible errors that can be

expected in the measurement process), while in other cases the difference does not exceed several percent.

Energy efficiency (e.g., very small additional energy demands) represents one of the two most important preconditions that the IDS must satisfy in order to consider its practical application and implementation into the WSN. Another important prerequisite is its capability for successful detection of malicious network nodes. Therefore, the following section analyses malicious node detection possibilities of the proposed IDS.

6.2. IDS Detection Capabilities Analysis. The analysis of malicious node behaviour detection capabilities for the proposed IDS was performed (similarly to its performance analysis) in three previously described networks with 6, 10, and 17 network nodes, respectively. In every network, detection capability was tested in all three characteristic scenarios (as in the case of performance testing) with the Rx/Tx success ratio of 100%, 80%, and 60%. It is important to test the IDS in such environment, where a malicious activity is not the only possible cause of packet dropping, but the packets can be lost during normal network operation (e.g., due to noise and collisions). A noisy and lossy environment makes malicious node detection more complicated.

In every analysed scenario, one malicious node was intentionally installed into the WSN. The malicious node selectively forwards packets such that it drops 80% of packets, while it forwards 20% of packets toward their destination. Two different cases were considered in every analysed scenario. In the first case, a malicious node just selectively forwards traffic in a described way (80% drops, 20% forwards). In the second case, besides selective forwarding, a malicious node falsely accuses its neighbouring nodes of the same malicious behaviour, and in this way it intentionally aggravates correct detection of the IDS.

A feature of the proposed IDS is its capability to estimate the malevolence probability besides characterization of a sensor node as malicious or legitimate. For testing purposes, the probability threshold is 50% (a node is considered malicious if the malevolence probability is greater than 50%). This threshold is adjustable and can be adapted to specific application requirements. In given tables, every row includes malevolence probabilities that every node estimates for its neighbouring nodes. The last row includes calculated final malevolence probabilities for every node. Some cells are empty since corresponding nodes are not neighbours, and therefore there is no estimated probability. The goal of the analysis is to determine the influence of different factors (e.g., the number of nodes, lost packets, and behaviour of the malicious node) on successful detection of a malicious node.

In a 6-node network (Figure 6), a malicious node is node 3. Table 4 contains estimated malevolence probabilities (in percent) for the first scenario (the Rx/Tx success ratio is 100%) in a 6-node network. The first number in each cell represents the estimated malevolence probability when a malicious node does not try to falsely accuse its neighbours (scenario 1a). The second number in each cell (printed in italics) represents the estimated malevolence probability when a malicious node additionally falsely accuses its neighbours

TABLE 4: Detection in 6-node network, scenario 1.

	2	<u>3</u>	4	5	6
2			0.0/0.0	0.0/0.0	
<u>3</u>				0.0/ <u>80.3</u>	0.0/ <u>80.3</u>
4	0.0/0.0				
5	0.0/0.0	80.3/80.3			
6		80.3/80.3			
p_M (%)	0.0/0.0	<u>80.3/80.3</u>	0.0/0.0	0.0/80.3	0.0/80.3

TABLE 5: Detection in 6-node network, scenario 2.

	2	<u>3</u>	4	5	6
2			0.0/0.0	1.5/1.5	
<u>3</u>				1.5/ <u>82.1</u>	3.0/ <u>83.3</u>
4	0.0/0.0				
5	0.0/0.0	79.1/79.1			
6		77.9/77.9			
p_M (%)	0.0/0.0	<u>78.5/78.5</u>	0.0/0.0	1.5/41.8	3.0/83.3

(scenario 1b). For example, the value “0.0/80.3” in the third row, the sixth column, means that in scenario 1a node 3 estimates the malevolence probability of 0.0% for node 6, and in scenario 1b node 3 estimates the malevolence probability of 80.3% for node 6 (it falsely accuses its neighbour).

In scenario 1a, the IDS easily draws a correct conclusion that node 3 is a malicious node (with estimated malevolence probability $p_M = 80.3\%$). In scenario 1b (where node 3 falsely accuses its neighbours), there are three nodes (nodes 3, 5, and 6) for which estimated malevolence probability p_M exceeds the threshold value of 50% ($p_M = 80.3\%$). Nevertheless, the IDS still makes a correct decision and designates node 3 as malicious since there are two estimates for node 3 that are above the threshold (by nodes 5 and 6), while nodes 5 and 6 have only one estimation above the threshold. However, it is obvious that false accusations (by malicious nodes) may significantly complicate the detection procedure and even cause incorrect conclusions.

Table 5 shows estimated malevolence probabilities for the second scenario in a 6-node network, where the Rx/Tx success ratio is 80%.

It is obvious that in scenario 2a detection of a malicious node was successful (the malevolence probability for node 3 equals 78.5%). But it is also apparent that additional packet losses present in this scenario cause the probability p_M to be somewhat lower than in the first scenario (which represents an ideal lossless case). For the same reason, some estimated malevolence probabilities for other nodes also appear. In scenario 2b (where node 3 falsely accuses its neighbours), there are two estimations above the threshold (for node 3 and node 6). A correct IDS decision was made since for node 3 there are two estimations above the threshold (while for node 6 there is only one).

Table 6 contains estimated malevolence probabilities for the third scenario in a 6-node network, where the Rx/Tx success ratio is 60%.

TABLE 6: Detection in 6-node network, scenario 3.

	2	3	4	5	6
2			22.4/22.4	21.5/21.5	
3				21.5/85.1	22.4/85.1
4	0.0/0.0				
5	0.0/0.0	63.2/63.2			
6		62.6/62.6			
p_M (%)	0.0/0.0	62.9/62.9	22.4/22.4	21.5/53.3	22.4/85.1

In scenario 3a, the IDS makes a correct decision and declares node 3 as malicious. However, it is noticeable that increased packet loss (Rx/Tx is lowered to 60%) reduces estimation quality (the malevolence probability is 62.9%), while at the same time malevolence probabilities for legitimate nodes increase but are still below the threshold. In scenario 3b, where a malicious node falsely accuses its neighbours, malevolence probabilities for three nodes (nodes 3, 5, and 6) exceed the threshold. The IDS also makes a correct decision in this case since for node 3 (a malicious node) there are two estimations above the threshold, while nodes 5 and 6 have one estimation above the threshold.

In a 10-node network (Figure 7), node 8 was deliberately made malicious for IDS detection testing purposes. Testing was performed for all three characteristic scenarios (similarly to a 6-node network). Table 7 represents results for the first scenario (Rx/Tx = 100%).

In the first case (scenario 1a), the IDS correctly recognizes node 8 as a malicious node with malevolence probability rating of 80.1%. In scenario 1b (where node 8 falsely accuses its neighbours), the IDS also draws a correct conclusion. It is noticeable that in scenario 1b some estimated malevolence probabilities emerged for other nodes (due to false accusations by node 8), but all are below the threshold value.

Table 8 presents testing results of the second scenario in a 10-node network (Rx/Tx = 80%).

Obviously, the IDS will correctly recognize a malicious activity of node 8, although in this scenario some malevolence estimations for other (legitimate) nodes occurred (due to certain packet loss). However, these probabilities by value are significantly below the threshold of 50%. Actually, these probabilities are even lower than estimated probabilities in the corresponding scenario of a 6-node network. This is because in the network with a larger number of nodes every node (on average) has more neighbours, making final estimations more accurate. Malicious node detection was also successful in scenario 2b, where a malicious node falsely accuses its neighbours. However, it is obvious that false accusations increase the probability of wrong malevolence estimations for legitimate nodes (which still remain below the threshold).

The results of the third testing scenario (Rx/Tx = 60%) in a 10-node network are presented in Table 9.

In scenario 3a, the IDS successfully detects a malicious node, but the quality of estimation (the value of final malevolence probability p_M) decreases. The final malevolence probability for a malicious node is lower than in previous scenarios

but still above the threshold ($p_M = 60.9\%$). At the same time, p_M values of incorrect estimations increase, so it happened that for node 9 the value of p_M also exceeds the threshold ($p_M = 52.75\%$) although it is the legitimate node. Further, it is visible that false accusation data that a malicious node puts into the network in scenario 3b significantly complicates a correct decision-making process. In this example, node 9 has the largest malevolence probability p_M ($p_M = 70.6\%$), which is actually legitimate node. Probability p_M also exceeds the threshold for node 8 ($p_M = 60.9\%$), which is in fact malicious. In this example, the IDS still drew a correct conclusion since there are two estimations above the threshold for node 8 (by nodes 5 and 7) and one estimation for node 9 (by node 8). Nevertheless, it should be noticed that the estimation for node 9 by node 6 was very close to the threshold (47.1%). Although it was an incorrect estimation (caused by packet losses that occurred), it could possibly happen that this estimation exceeds the threshold. In that case, the IDS would draw an incorrect conclusion that a malicious node is node 9. Furthermore, it is apparent that node 9 (again due to significant packet losses) made an incorrect estimation about node 8 (p_M was only 25.8%), which also aggravates the decision-making process.

In a 17-node network (Figure 8), for testing purposes, the malicious node was node 10. The results of the intrusion detection process for the first scenario (Rx/Tx = 100%) in a 17-node network are presented in Table 10.

In scenario 1a, in a 17-node network (an ideal case, with no packet losses), the IDS easily detects malicious activities of node 10. In scenario 1b, there are some malevolence estimations for legitimate nodes (caused by false accusations by node 10), but they are all below the threshold.

Table 11 shows testing results for the second scenario in a 17-node network (Rx/Tx = 80%).

In scenario 2a, in a 17-node network, malicious node detection was successful, but some malevolence estimations for legitimate nodes occur due to packet losses (all below the threshold). In scenario 2b (where node 10 falsely accuses its neighbours), detection is also successful, but the estimated malevolence probabilities for some legitimate nodes also increased due to false accusations by node 10 (they are still below the threshold).

Table 12 presents results of the third testing scenario in a 17-node network (Rx/Tx = 60%).

The results show that detection was successful in scenario 3a of a 17-node network, but it is obvious that increased packet loss causes the increment of wrong malevolence estimations for legitimate nodes (e.g., nodes 11 and 14 give estimations of 44.0% and 54.8% for the malevolence probability of malicious node 10, while at the same time for legitimate node 15 they give estimated malevolence probabilities of 53.2% and 66.1%). False accusations by node 10 (in scenario 3b) additionally increase incorrect estimations about malevolence of legitimate nodes. Fortunately, these estimations are still below the threshold, owing to correct estimations of a larger number of legitimate nodes that reduce a negative impact of false accusations by a malicious node.

Tests and analyses performed through more different characteristic scenarios showed that the system proposed for

TABLE 7: Detection in 10-node network, scenario 1.

	1	2	3	4	5	6	7	<u>8</u>	9
1		0.0/0.0		0.0/0.0					
2	0.0/0.0		0.0/0.0		0.0/0.0				
3		0.0/0.0				0.0/0.0			
4	0.0/0.0				0.0/0.0		0.0/0.0		
5		0.0/0.0		0.0/0.0		0.0/0.0		80.1/80.1	
6			0.0/0.0		0.0/0.0				0.0/0.0
7				0.0/0.0				80.1/80.1	
<u>8</u>					0.0/ <u>80.6</u>		0.0/ <u>80.6</u>		0.0/ <u>80.1</u>
9						0.0/0.0		80.1/80.1	
p_M (%)	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/20.2	0.0/0.0	0.0/40.1	80.1/80.1	0.0/40.1

TABLE 8: Detection in 10-node network, scenario 2.

	1	2	3	4	5	6	7	<u>8</u>	9
1		0.0/0.0		0.0/0.0					
2	0.0/0.0		1.5/1.5		0.0/0.0				
3		1.5/1.5				1.5/1.5			
4	0.0/0.0				0.0/0.0		0.0/0.0		
5		0.0/0.0		0.0/0.0		0.0/0.0		80.6/80.6	
6			1.5/1.5		0.0/0.0				4.5/4.5
7				0.0/0.0				80.6/80.6	
<u>8</u>					0.0/ <u>83.6</u>		0.0/ <u>83.6</u>		4.5/ <u>81.5</u>
9						4.5/4.5		79.8/79.8	
p_M (%)	0.0/0.0	0.5/0.5	1.5/1.5	0.0/0.0	0.0/20.9	2.0/2.0	0.0/41.8	80.3/80.3	4.5/43.0

TABLE 9: Detection in 10-node network, scenario 3.

	1	2	3	4	5	6	7	<u>8</u>	9
1		4.5/4.5		0.0/0.0					
2	4.5/4.5		23.1/23.1		0.0/0.0				
3		3.4/3.4				23.7/23.7			
4	0.0/0.0				0.0/0.0		9.2/9.2		
5		4.5/4.5		0.0/0.0		31.3/31.3		82.3/82.3	
6			16.6/16.6		0.0/0.0				47.1/47.1
7				0.0/0.0				74.7/74.7	
<u>8</u>					0.0/ <u>82.3</u>		7.8/ <u>89.2</u>		58.4/ <u>94.0</u>
9						9.8/9.8		25.8/25.8	
p_M (%)	2.3/2.3	4.1/4.1	19.9/19.9	0.0/0.0	0.0/20.6	21.6/21.6	8.5/49.2	60.9/60.9	52.75/70.6

malicious node detection in the IPv6-based WSN successfully detects presence of a malicious network node. Thereby, the proposed system satisfies an important prerequisite for the implementation into the IPv6-based WSN (in addition to necessary energy efficiency and a minimal influence on network performance and its proper operation). Unlike most other IDS known in conventional WSNs, the proposed system also gives the estimation of the node malevolence probability (while other systems usually just declare a node as malicious or legitimate). The performed tests showed the influence of different parameters on the decision-making process and the quality of estimation. Packet loss present in the network due to noise, collisions, or failures has a

negative impact on the quality of malevolence probability estimation. It is sometimes difficult to resolve the real reason for packet loss, that is, whether it is one of the aforementioned reasons or a malicious activity of the node that intentionally drops or selectively forwards packets. Furthermore, presence of packet loss may cause legitimate nodes to be considered malicious with some probability, which may, in extreme cases, exceed the threshold value (a situation where a malicious node is not detected or a legitimate node is incorrectly designated as malicious). A real sensor network represents an unstable environment in terms of communications (it is noise-sensitive and prone to failures). Therefore, the system should be tested before every implementation in the real

TABLE 10: Detection in 17-node network, scenario 1.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1		0.0/0.0			0.0/0.0											
2	0.0/0.0		0.0/0.0			0.0/0.0										
3	0.0/0.0	0.0/0.0		0.0/0.0			0.0/0.0									
4	0.0/0.0	0.0/0.0	0.0/0.0					0.0/0.0								
5	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0					0.0/0.0							
6	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0					80.3/80.3						
7	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0					0.0/0.0					
8	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0					0.0/0.0				
9	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0					0.0/0.0			
10	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/80.6	0.0/0.0	0.0/0.0	0.0/80.6	80.3/80.3	0.0/80.6	0.0/0.0	0.0/0.0	0.0/80.3		
11	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/80.6	0.0/0.0	0.0/0.0	0.0/80.6	80.3/80.3	0.0/0.0	0.0/0.0	0.0/0.0	0.0/80.3	0.0/0.0	0.0/0.0
12	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	80.3/80.3	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0
13	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	80.3/80.3	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0
14	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	80.3/80.3	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0
15	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	80.3/80.3	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0
16	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/20.2	0.0/0.0	0.0/0.0	0.0/26.9	<u>80.3/80.3</u>	0.0/20.2	0.0/0.0	0.0/0.0	0.0/26.8	0.0/0.0	0.0/0.0
P_M (%)	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/20.2	0.0/0.0	0.0/0.0	0.0/26.9	<u>80.3/80.3</u>	0.0/20.2	0.0/0.0	0.0/0.0	0.0/26.8	0.0/0.0	0.0/0.0

TABLE II: Detection in 17-node network, scenario 2.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1		0.0/0.0			0.0/0.0											
2	0.0/0.0		3.0/3.0			0.0/0.0										
3		0.0/0.0		5.9/5.9			1.5/1.5									
4			2.8/2.8					2.8/2.8								
5	0.0/0.0					0.0/0.0	1.5/1.5		1.5/1.5							
6		0.0/0.0			0.0/0.0		1.5/1.5	2.9/2.9		80.3/80.3						
7			2.9/2.9			0.0/0.0	1.5/1.5				1.5/1.5					
8				5.9/5.9								7.2/7.2				
9					0.0/0.0					79.1/79.1			6.0/6.0			
10						0.0/80.3	1.5/1.5	2.8/2.8	1.5/83.1	79.1/79.1	1.5/83.1	7.4/7.4		3.0/83.6	1.5/1.5	
11									1.4/1.4		1.4/1.4					
12																7.0/7.0
13													5.7/5.7		1.4/1.4	
14										75.4/75.4				2.9/2.9		7.5/7.5
15											1.5/1.5					
16												6.9/6.9				
P_M (%)	0.0/0.0	0.0/0.0	2.9/2.9	5.9/5.9	0.0/0.0	0.0/20.1	1.5/1.5	2.8/2.8	1.5/28.7	78.5/78.5	1.5/21.9	7.2/7.2	5.9/5.9	2.9/29.8	1.4/1.4	7.3/7.3

TABLE 12: Detection in 17-node network, scenario 3.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1		0.0/0.0			0.0/0.0											
2	3.1/3.1		12.1/12.1			0.0/0.0										
3		0.0/0.0		27.5/27.5			17.6/17.6									
4			8.3/8.3					24.7/24.7								
5	3.1/3.1					0.0/0.0			12.1/12.1							
6		0.0/0.0			0.0/0.0		20.0/20.0			80.3/80.3						
7			9.7/9.7			0.0/0.0		28.8/28.8			36.1/36.1					
8				20.1/20.1			12.0/12.0					48.0/48.0				
9					0.0/0.0					70.6/70.6			30.6/30.6			
10						0.0/80.3			9.0/83.3		33.5/90.3			23.6/86.4		
11							11.0/11.0			44.0/44.0		41.1/41.1			53.2/53.2	
12								9.0/9.0			11.3/11.3			20.7/20.7		24.2/24.2
13									7.9/7.9							
14										54.8/54.8			23.8/23.8		66.1/66.1	
15											1.4/1.4			1.0/1.0		0.0/0.0
16												2.3/2.3				
P_M (%)	3.1/3.1	0.0/0.0	10.0/10.0	23.8/23.8	0.0/0.0	0.0/20.1	15.2/15.2	20.8/20.8	9.7/34.4	62.4/62.4	20.6/34.8	30.5/30.5	27.2/27.2	15.1/36.0	39.8/39.8	12.1/12.1

network in order to adjust the probability threshold value to a particular application.

The number of neighbouring nodes is an important factor that influences the malevolence probability estimation process. Estimations of higher quality will be obtained in networks with a larger number of nodes, where malicious nodes have a larger number of legitimate neighbouring nodes. The estimations by legitimate nodes will in that case reduce a negative impact of false data inserted by a malicious node. Successful detection of malicious behaviour in a lossy environment (where the Rx/Tx success ratio is less than 100%) also depends on the chosen probability threshold value. A larger threshold value in a lossy environment lowers the detection efficacy since larger packet losses decrease the estimated malevolence probability for a malicious node and increase it for legitimate nodes. Also, if the threshold is too low, it is possible that a legitimate node will be characterized as malicious. The performed tests showed that many parameters influence the quality of estimation, for example, network topology (the number of nodes and their arrangement), the number of neighbours, packet loss (which is not caused by malicious behaviour), and a malicious node behaviour pattern. Therefore, it is not possible to define the universal probability threshold value that would be suitable for all networks.

7. Conclusions

In recent years, wireless sensor networks have been developing rapidly, and their application areas are extending continuously. Their strong resource limitations make them very specific and different from other types of wireless networks. Consequently, all usual networking mechanisms (e.g., routing or security mechanisms) required specific adaptations before their implementation into the WSN. Recently, there has been a strong tendency for interconnection of many different devices and integration of wireless sensor networks with other network types in the context of the Internet of Things paradigm. Protocol architecture of most current networks is based on the IP, and the transition to the new version of protocol (IPv6) is in progress. These parallel processes naturally led to the implementation of IPv6 into the WSN.

IPv6-based WSNs represent a novel trend in the area of sensor networks, and as such they raise certain problems and open issues that still require adequate solutions. Security aspects of IPv6-based WSNs are very important since good security solutions could guarantee their wider practical application. The paper gives an overview of security aspects of the IPv6-based WSN, focusing on existing security threats and different attack types. It also analyses some existing intrusion detection schemes that could be implemented into the IPv6-based WSN. The authors propose a solution for the distributed adaptive intrusion detection system intended especially for the IPv6-based WSN. Its distributed nature enables its execution on every sensor node in the network. Every node monitors the activity of its neighbours and estimates their malevolence probabilities. Final estimation of the malevolence probability for all nodes is calculated

after all IDS agents exchange their estimations. Calculation of the malevolence probability is also an advantage of the proposed intrusion detection system since most existing IDS just declare a certain node as malicious or legitimate, without estimation of the malevolence level.

The proposed system for malicious node detection fully supports the IPv6 in wireless sensor networks. As such, it is suitable for the IPv6-based WSN, while other intrusion detection solutions known from the conventional WSNs would require a proper adaptation (they cannot be directly applied into the IPv6-based WSN). Also, its advantage (compared to simple single-layer solutions) is possibility of integration into the unique cross-layer security framework along the other security mechanisms. Due to its distributed nature (where all network nodes contribute to decision-making process), the proposed system is tolerant on some node failures. The proposed system also estimates the malevolence probabilities for suspicious nodes, where most existing IDS do not estimate the malevolence level (they just declare node as a malicious or a legitimate one). Another advantage of the proposed system is adaptability for different application requirements achieved by the flexible (adjustable) malevolence threshold. At the same time, the proposed malicious node detection method proved to be energy efficient, which is very important in resource constrained environment of IPv6-based WSN. Finally, the proposed system showed very good detection capabilities despite lossy wireless environment and intentional aggravation of detection process by malicious nodes.

The proposed IDS solution was implemented in three different network topologies. In every network, detailed tests and analyses were performed through different characteristic scenarios. The goals of analysis were to examine performance and energy efficiency of the proposed IDS solution, its influence on normal network operation, and its capability of successful detection of malicious nodes in different situations. Successful detection is when the IDS correctly indicates a malicious node and extracts it from the set of legitimate nodes, giving thereby the malevolence probability estimation above the predefined threshold. The malicious node was deliberately inserted into the network for testing purposes. Therefore, it was surely possible to determine whether the IDS conclusion was correct or not. The tests performed also showed that the proposed IDS solution is energy efficient and with minor influence on normal network operation, while at the same time it has a very good capability of making correct decisions about malevolence of certain network nodes. In all testing scenarios, the IDS correctly indicated a malicious node, despite its attempts to falsely accuse its neighbours and to disable or at least aggravate the detection process. Future development of this IDS should include support for network node mobility that will additionally expand its possible application range.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

- [1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–105, 2002.
- [2] P. Baronti, P. Pillai, V. W. C. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: a survey on the state of the art and the 802.15.4 and ZigBee standards," *Computer Communications*, vol. 30, no. 7, pp. 1655–1695, 2007.
- [3] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, 2008.
- [4] RFC, "Internet protocol, version 6 (IPv6) specification," RFC 2460, 1998.
- [5] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.
- [6] J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the internet of things: a survey of existing protocols and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015.
- [7] M. Blanchet, *Migrating to IPv6: A Practical Guide to Implementing IPv6 in Mobile and Fixed Networks*, John Wiley & Sons, Chichester, UK, 2006.
- [8] K. Grgic and D. Zagar, "Wireless sensor networks-applications and development," in *Proceedings of the 2nd IFAC International Conference on Modelling and Design of Control Systems in Agriculture*, Osijek, Croatia, 2007.
- [9] J. Hui and P. Thubert, "Transmission of IPv6 packets over IEEE 802.15.4 networks," RFC 4944, IETF, 2007.
- [10] A. Dunkels and J. P. Vasseur, "IP for smart objects," IPSO Alliance (Internet Protocol for Smart Objects) Whitepaper 1, 2008.
- [11] J. Abeille, M. Durvy, J. Hui, and S. Dawson-Haggerty, "Lightweight IPv6 stacks for smart objects: the experience of three independent and interoperable implementations," IPSO Alliance (Internet Protocol for Smart Objects) Whitepaper 2, 2008.
- [12] K. Grgic, V. Krizanovic, and V. Mandric, "Security aspects of the RPL protocol implementation into IPv6-based wireless sensor networks," in *Proceedings of the 22nd International Conference on Software, Telecommunications and Computer Networks (SoftCOM '14)*, Split, Croatia, 2014.
- [13] D. Žagar and K. Grgić, "IPv6 security threats and possible solutions," in *Proceedings of the World Automation Congress (WAC '06)*, pp. 1–7, IEEE, Budapest, Hungary, June 2006.
- [14] D. Žagar, K. Grgić, and S. Rimac-Drlje, "Security aspects in IPv6 networks—implementation and testing," *Computers & Electrical Engineering*, vol. 33, no. 5–6, pp. 425–437, 2007.
- [15] E. Shi and A. Perrig, "Designing secure sensor networks," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 38–43, 2004.
- [16] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 8, no. 2, pp. 2–23, 2006.
- [17] M. Saxena, "Security in wireless sensor networks—a layer-based classification," CERIAS Tech Report 04-2007, 2007.
- [18] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," *IEEE Communications Surveys and Tutorials*, vol. 10, no. 3, pp. 6–28, 2008.
- [19] K. Stammberger, M. Semp, M. B. Anand, and D. Culler, "Introduction to security for smart object networks," IPSO Alliance (Internet Protocol for Smart Objects) Whitepaper 5, 2010.
- [20] C. Krauß, M. Schneider, and C. Eckert, "On handling insider attacks in wireless sensor networks," *Information Security Technical Report*, vol. 13, no. 3, pp. 165–172, 2008.
- [21] A. Hamid, M. Rashid, and C. S. Hong, "Defense against laptop class attacker in wireless sensor network," in *Proceedings of the 8th International Conference Advanced Communication Technology (ICACT '06)*, pp. 314–318, Phoenix Park, Republic of Korea, February 2006.
- [22] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.
- [23] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: attacks and defenses," *IEEE Pervasive Computing*, vol. 7, no. 1, pp. 74–81, 2008.
- [24] V. P. Singh, S. Jain, and J. Singhai, "Hello flood attack and its countermeasures in wireless sensor networks," *IJCSI International Journal of Computer Science Issues*, vol. 7, no. 11, pp. 23–27, 2010.
- [25] E. C. H. Ngai, J. Liu, and M. R. Lyu, "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks," *Computer Communications*, vol. 30, no. 11–12, pp. 2353–2364, 2007.
- [26] I. Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos, "Intrusion detection of sinkhole attacks in wireless sensor networks," in *Algorithmic Aspects of Wireless Sensor Networks*, M. Kutylowski, J. Cichoń, and P. Kubiak, Eds., vol. 4837 of *Lecture Notes in Computer Science*, pp. 150–161, 2008.
- [27] K.-F. Ssu, W.-T. Wang, and W.-C. Chang, "Detecting Sybil attacks in wireless sensor networks using neighboring information," *Computer Networks*, vol. 53, no. 18, pp. 3042–3056, 2009.
- [28] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *Proceedings of the 22nd Annual Joint Conference on the IEEE Computer and Communications Societies*, pp. 1976–1986, San Francisco, Calif, USA, April 2003.
- [29] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless Ad Hoc networks," *IEEE Wireless Communications*, vol. 11, no. 1, pp. 48–60, 2004.
- [30] T. S. Sobh, "Wired and wireless intrusion detection system: classifications, good characteristics and state-of-the-art," *Computer Standards & Interfaces*, vol. 28, no. 6, pp. 670–694, 2006.
- [31] F. Sabahi and A. Movaghar, "Intrusion detection: a survey," in *Proceedings of the 3rd International Conference on Systems and Networks Communications*, pp. 23–26, IEEE, Sliema, Malta, October 2008.
- [32] N. Marchang and R. Datta, "Collaborative techniques for intrusion detection in mobile ad-hoc networks," *Ad Hoc Networks*, vol. 6, no. 4, pp. 508–523, 2008.
- [33] B. Sun, L. Osborne, Y. Xiao, and S. Guizani, "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," *IEEE Wireless Communications*, vol. 14, no. 5, pp. 56–63, 2007.
- [34] A. P. Lauf, R. A. Peters, and W. H. Robinson, "A distributed intrusion detection system for resource-constrained devices in ad-hoc networks," *Ad Hoc Networks*, vol. 8, no. 3, pp. 253–266, 2010.
- [35] V. Bhuse and A. Gupta, "Anomaly intrusion detection in wireless sensor networks," *Journal of High Speed Networks*, vol. 15, no. 1, pp. 33–51, 2006.
- [36] I. Krontiris, Z. Benenson, T. Giannetsos, F. C. Freiling, and T. Dimitriou, "Cooperative intrusion detection in wireless sensor networks," in *Proceedings of the 6th European Conference on Wireless Sensor Networks (EWSN '09)*, pp. 263–278, Cork, Ireland, February 2009.

- [37] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in *Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '05)*, pp. 253–259, Montreal, Canada, August 2005.
- [38] Y. Wang, X. Wang, B. Xie, D. Wang, and D. P. Agrawal, "Intrusion detection in homogeneous and heterogeneous wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 7, no. 6, pp. 698–711, 2008.
- [39] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 1, pp. 266–282, 2014.
- [40] A. Abduvaliyev, A.-S. K. Pathan, J. Zhou, R. Roman, and W.-C. Wong, "On the vital areas of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 1223–1237, 2013.
- [41] T. Chen, H. Huang, Z. Chen, Y. Wu, and H. Jiang, "A secure routing mechanism against wormhole attack in IPv6-based wireless sensor networks," in *Proceedings of the 7th International Symposium on Parallel Architectures, Algorithms and Programming*, pp. 110–115, Nanjing, China, December 2015.
- [42] S. Lim and L. Huie, "Hop-by-Hop cooperative detection of selective forwarding attacks in energy harvesting wireless sensor networks," in *Proceedings of the International Conference on Computing, Networking and Communications (ICNC '15)*, pp. 315–319, Garden Grove, Calif, USA, February 2015.
- [43] A. R. Dhakne and P. Chatur, "Distributed trust based intrusion detection approach in wireless sensor network," in *Proceedings of the Communication, Control and Intelligent Systems (CCIS '15)*, pp. 96–101, IEEE, Mathura, India, November 2015.
- [44] Y. Maleh, A. Ezzati, Y. Qasmaoui, and M. Mbida, "A global hybrid intrusion detection system for wireless sensor networks," *Procedia Computer Science*, vol. 52, pp. 1047–1052, 2015.
- [45] C. B. Dutta and U. Biswas, "Specification based IDS for camouflaging wormhole attack in OLSR," in *Proceedings of the 23rd Mediterranean Conference on Control and Automation*, pp. 960–966, Torremolinos, Spain, June 2015.
- [46] Y. Mourabit, A. Bouriden, A. Toumanari, and N. Moussaid, "Intrusion detection techniques in wireless sensor network using data mining algorithms: comparative evaluation based on attacks detection," *International Journal of Advanced Computer Science and Applications*, vol. 6, no. 9, pp. 164–172, 2015.
- [47] J.-W. Ho, M. Wright, and S. K. Das, "Distributed detection of mobile malicious node attacks in wireless sensor networks," *Ad Hoc Networks*, vol. 10, no. 3, pp. 512–523, 2012.
- [48] H. Moosavi and F. M. Bui, "A game-theoretic framework for robust optimal intrusion detection in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 9, pp. 1367–1379, 2014.
- [49] G. Sandhya and A. Julian, "Intrusion detection in wireless sensor network using genetic K-means algorithm," in *Proceedings of the IEEE International Conference on Advanced Communication, Control and Computing Technologies (ICACCCT '14)*, pp. 1791–1794, Ramanathapuram, India, May 2014.
- [50] S. Sultana, G. Ghinita, E. Bertino, and M. Shehab, "A lightweight secure scheme for detecting provenance forgery and packet dropattacks in wireless sensor networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 3, pp. 256–269, 2015.
- [51] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 5, pp. 3718–3731, 2016.
- [52] C. Pu and S. Lim, "A light-weight countermeasure to forwarding misbehavior in wireless sensor networks: design, analysis, and evaluation," *IEEE Systems Journal*, 2016.
- [53] K. Grgic, D. Zagar, and V. Krizanovic, "Security in IPv6-based wireless sensor network—precision agriculture example," in *Proceedings of the 12th International Conference on Telecommunications*, pp. 79–86, Zagreb, Croatia, June 2013.
- [54] T. Zia and A. Zomaya, "A security framework for wireless sensor networks," in *Proceedings of the IEEE Sensors Applications Symposium*, pp. 49–53, Houston, Tex, USA, February 2006.
- [55] N. R. Prasad and M. Alam, "Security framework for wireless sensor networks," *Wireless Personal Communications*, vol. 37, no. 3-4, pp. 455–469, 2006.
- [56] K. Sharma and M. K. Ghose, "Cross layer security framework for wireless sensor networks," *International Journal of Security and Its Applications*, vol. 5, no. 1, pp. 39–52, 2011.
- [57] A. Dunkels, B. Grönvall, and T. Voigt, "Contiki—a lightweight and flexible operating system for tiny networked sensors," in *Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks*, pp. 455–462, Tampa, Fla, USA, November 2004.
- [58] F. Österlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, "Cross-level sensor network simulation with COOJA," in *Proceedings of the 1st IEEE Conference on Local Computer Networks*, pp. 641–648, IEEE, Tampa, Fla, USA, November 2006.
- [59] O. Gaddour and A. Koubâa, "RPL in a nutshell: a survey," *Computer Networks*, vol. 56, no. 14, pp. 3163–3178, 2012.
- [60] J. Hui, D. Culler, and S. Chakrabarti, "6LoWPAN: incorporating IEEE 802.15.4 into the IP architecture," IPSO Alliance (Internet Protocol for Smart Objects) Whitepaper 3, 2009.

Research Article

Adaptive Cross-Layer Multipath Routing Protocol for Mobile Ad Hoc Networks

Zeeshan Iqbal,¹ S. Khan,¹ Amjad Mehmood,¹ Jaime Lloret,² and Nabil Ali Alrajeh³

¹*Institute of Information Technology, Kohat University of Science and Technology (KUST), Kohat City 26000, Pakistan*

²*Integrated Management Coastal Research Institute, Universidad Politecnica de Valencia, Camino de Vera, 46022 Valencia, Spain*

³*Biomedical Technology Department, College of Applied Medical Sciences, King Saud University, Riyadh 11633, Saudi Arabia*

Correspondence should be addressed to Nabil Ali Alrajeh; nabil@ksu.edu.sa

Received 24 March 2016; Accepted 26 May 2016

Academic Editor: Jian Shu

Copyright © 2016 Zeeshan Iqbal et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Mobile ad hoc networks (MANETs) are generally created for temporary scenarios. In such scenarios, where nodes are in mobility, efficient routing is a challenging task. In this paper, we propose an adaptive and cross-layer multipath routing protocol for such changing scenarios. Our routing mechanisms operate keeping in view the type of applications. For simple applications, the proposed protocol is inspired from traditional on-demand routing protocols by searching shortest routes from source to destination using default parameters. In case of multimedia applications, the proposed mechanism considers such routes which are capable of providing more data rates having less packet loss ratio. For those applications which need security, the proposed mechanism searches such routes which are more secure in nature as compared to others. Cross-layer methodology is used in proposed routing scheme so as to exchange different parameters across the protocol stack for better decision-making at network layer. Our approach is efficient and fault tolerant in a variety of scenarios that we simulated and tested.

1. Introduction

Mobile ad hoc networks (MANETs) are composed of different nodes being operated in infrastructureless environment. These nodes work in a highly dynamic and random topology [1]. Nodes are distributed and mobile with the capability of self-organizing themselves. MANET nodes have resource constraints such as power, processing, and bandwidth. Comparing with the traditional network, MANET inherits the traditional problems of wired and wireless network. Its basic infrastructure less features imposes another burden on the standardization of network architecture. To compare with that of traditional networks, wireless network security must address two foundation aspects. One is key management, trust establishment, and membership control; the other one deals with network availability and routing security [2].

MANET aim is to think of network where each node is mobile one day without the limitation of nodes. Existing protocol also requires significant changes to cope with the challenges and aims of MANET.

Routing is needed whenever a packet is forwarded from source to destination through some intermediate nodes as in most cases the nodes are not directly connected with each other. Some sort of path finding mechanism is required by protocol, that is, the routing protocol. In case of MANET, routing is a serious research issue as the nodes are mobile in nature. These paths are not always connected; hence, some path maintenance is also an issue. Numerous protocols have been proposed considering the nature and diversity of application. Mostly the routing protocol for MANET falls into three categories, that is, proactive, reactive, and hybrid protocols.

Proactive or table driven routing protocol [3–8] established paths in their routing table before they are required. Nodes operating under proactive protocol continuously propagate routing related information to their neighbors to update their routing table. The exchange of information causes the neighbor nodes to propagate their routing information to compute their own routing tables. This process is

periodic in nature. Therefore, a source node before transmitting any data packet gets the full path in advance. In case of any link changes, respective nodes update their routing table by doing the same exchange of information process. The advantage of using proactive approach is quite straightforward; that is, the nodes get the full path in advance. The disadvantage is that nodes are always busy in computing their routing table and network overhead is large. Some of the popular proactive protocols are WRP (Wireless Routing Protocol), DSDV (Destination Sequence Distance Vector), FSR (Fisheye State Routing), and so forth.

Reactive or on-demand routing protocol [9–12] does not maintain routing information. Nodes try to find the routes whenever there is need for data transmission. These protocols do not work in advance. This approach might seem slow, but in reality it is somewhat better than proactive approach, considering the nature of MANET. The nodes are mobile so it is better to find the route at the time of transmission rather than in advance. The main advantage of using reactive protocol is that the overhead is small as no continuous route discovery process is running. However, the disadvantage is the delay because the reactive protocol is searching the path to destination before any transmission. Some of the major routing protocols that fall into the category are AODV (ad hoc on-demand distance vector) and DSR (Dynamic Source Routing), and so forth.

Hybrid routing protocols combine the features of both proactive and reactive routing. Hybrid protocols handle more frequently used paths in a proactive manner, while all other routes in reactive fashion. Some of the hybrid protocols are ZRP (Zone Routing Protocol) [13] and ZHLS (Zone based Hierarchical Link State Routing) [14].

Successful data transmission is a three-step process, that is, route discovery, data transmission, and route maintenance. Before sending any data, packet route request is broadcast to initiate route discovery process. In reply to that, route reply is received. In most of the cases, more than one route reply is received from different routes. Sender chooses one best path among all of them. Normally, this path is the shortest path. Other protocols propose some other way of choosing a single path.

Single path routing may result in congestion affecting the network in terms of bandwidth, throughput and delay. To overcome the problems of single path routing, we are planning to design multipath and cross-layered routing protocol for MANET.

The shortest path problem is that it is normally the central path of the network and normally always congested as every node tries to do data transmission via this central path [15]. Single path protocols are not fault tolerant and do not have the capability to distribute the load. To overcome the disadvantage of single path routing, researchers focus on the idea of multipath routing. It is borrowed from the traditional circuit switched network where call blockages are avoided by diverting call to some other route. Once all paths are known to sender, most important issues are about how to select among all available paths and how to distribute load among nodes.

To cope with the modern day challenges such as application diversity and dynamics changes, establishing path for

TABLE 1: Multipath routing advantages and disadvantages.

Advantages	Disadvantages
Fault tolerant 3	Longer paths
Load balancing	Special control messages
Bandwidth aggregation	Route request storm
Reduce delay	Inefficient route discover
	Duplicate packet processing

different application is quite cumbersome. MANET architecture also poses some important limitations, for example, limited bandwidth and energy saving. Researcher tries to find the best path among all available routes to satisfy the need. Evolving from single path to two paths which acts as a backup route in case that primary path fails proves better. This approach also adds the fault tolerant feature where one path breaks while the other one takes over. With the passage of time, these approaches were not sufficient for the user requirement and customer satisfaction. Multipath routing technique was used to achieve more efficiency and load distribution among paths. Multipath approaches are basically divided into two categories, that is, link disjoint and node disjoint multipaths. Shared medium always tends to be congested and also reduces the performance of the network due to packets loss and delay [16]. Multihop communication also needs the mutual cooperation required between physical, MAC, and routing layer. In addition, mobility also poses the need for establishment of new route again and again [17]. Shadowing environment feature RSS (Received Signal Strength) is used for stabilizing the link.

One of the major challenges is also on deciding that how many numbers of paths should be used. Using more paths also adds the excessive overload with very minor improvement in the throughput. Majority approaches used two or three paths for multipath scheme [18–20]. Some of the pros and cons of the multipath routing are provided in Table 1.

For simulation work, we use AODV (ad hoc on-demand distance vector) [9], DSR (Dynamic Source Routing) [10], OLSR (Optimized Link State Routing) [21], PLQBR (Predictive Location-Based QoS Routing in Ad Hoc Networks) [22], QAODV (Quality of Service for Ad Hoc On-Demand Distance Vector Routing) [23], CEDAR (Core Extraction Distributed Ad Hoc Routing) [24], SAODV (secure ad hoc on-demand distance vector) [25], and CSROR (Cross-Layer Secure and Resource-Aware On-Demand Routing) [26].

AODV [9] works on the philosophy of DSDV by improving the on-demand scheme. This helps in finding the up-to-date routes, also by reducing the route maintenance phase. Only the active nodes will exchange and maintain the control information. Destination sequence number is used by source node to avoid looping and freshness of the route. Like DSR, AODV broadcast RREQ to its neighbors, but unlike DSR source routing is not used. Here, source node and intermediate nodes will store the next hop routing information in its routing table and RREQ will be rebroadcasted. Once the RREQ reaches the final destination, it replies with the RREP

to the reverse path where entries are created at the intermediate nodes. In case intermediate nodes know the destination, they will only be allowed to send RREP if their sequence number is equal or greater to the sequence number mentioned in the RREQ. In case any error occurs, RERR (Route ERROR) will be generated and transmitted to both end nodes. RERR also causes the end nodes to remove the corresponding route entries. The main disadvantage of AODV is that if sequence number of source node is very small, then the number is used by intermediate nodes and can lead to stale route too causing the RERR frequently.

DSR [10] is well known to be classified as on-demand routing protocol by saving the bandwidth utilization and power consumption. It is different from others in a sense that it uses source routing by not relying on the routing table information. Source routing also helps in loop free, not requiring up-to-date information, thus saving time. DSR protocol works in two phases, that is, Route Discovery and Route Maintenance, simultaneously. One of the significant differences is no usage of HELLO message. Route discovery phase is carried out by flooding the RREQ (ROUTE REQUEST) in the network. The destination node however on receiving the RREQ replies with the RREP (Route Reply), which follows the same path as RREQ travelled through. Intermediate nodes will rebroadcast the RREQ if the path is not known to them; however, they can reply the source node if they have the fresh path to destination. Route cache is implemented to achieve source routing. In case the destination is not known to intermediate nodes, they will append their address in RREQ and rebroadcast to their neighbor. On the reverse with the help of RREP traversing back through them, intermediate nodes can also update their routing table accordingly too.

OLSR [21] is considered to be the table driven protocol. Nodes will exchange messages with the neighboring nodes in the network on regular time interval to update topological information about the network. MPR (Multipoint Relay) is used as a key role to reduce the flooding of the classical mechanism. HELLO messages will be transmitted by nodes to gain knowledge about their one hop neighbor. MPR are the subset of node among one hop neighbors which will be used to forward broadcast information rather than every node retransmitting message whenever it is received for the first time. Link state information is also generated by these MPR nodes only, thus also reducing the control messages flooding. MPR also helps nodes in finding the optimal routes and works well for large and dense network.

PLBQR [22] proposes a mechanism where nodes future physical location is predicted depending on its previous location updates, which in turn to predict the future routes. Stale routes are avoided by prediction the future location of nodes, thus increasing path reliability in terms of location. QoS routing used the update protocol, location, and delay prediction mechanisms. In update protocol, each node will broadcast its geographical update and resource information periodically and in case of major movement, respectively, called Type 1 update and Type 2 update messages. To start a communication source, node will predict the geographical information of both the destination and the intermediate nodes. This step

also is involved in predicting the delay as well. These predications are based on the result of update messages received from the destination and intermediate nodes. QoS routing is based on depth first search to find candidate routes satisfying the requirements. Geographically, shortest routes are being preferred. The disadvantage is that no resources are reserved on the path which in turn may lead to inaccurate delay prediction.

QAODV [23] specifies extensions which can be used to ensure maximum delay and minimum bandwidth along a route between a source and destination. Using the extensions in this document, AODV enables mobile nodes in an ad hoc network to specify, as part of a RREQ, Quality of Service requirements that a route to a destination must satisfy. In particular, a RREQ may include a QoS Object extension which includes bandwidth and delay parameters. In order to enable accumulated measurement for end-to-end delay, AODV also provides a Maximum Permissible Delay extension. If, after establishment of such a route, any node along the path detects that the requested Quality of Service parameters can no longer be maintained and that node must originate a ICMP QOS_LOST message back to the node which had originally requested the now unavailable parameters.

CEDAR [24] algorithm was basically designed for small and middle size network. CEDAR falls into reactive routing and core nodes are formed to perform the mechanism. These core nodes are selected by distributed algorithm and in a group of three hops where there is at least one core node. Transmission is done by these core nodes to their neighboring core node in the unicast manner. In the mobility of any core node, nodes attaching to it have to find another core node. CEDAR combines the support for QoS and routing. Subset of node is selected dynamically and distributed which maintains local topological information and route computation task. CEDAR protocol was defined to perform three-procedural task, that is, (1) self-organizing routing structure that is established and maintained for route computation, (2) unwavering higher bandwidth linking existing bandwidth information that is propagated to all core nodes whereas low bandwidth information of dynamic link is kept locally, and (3) QoS route computing using up-to-date local topology. The advantage of using CEDAR is that route discovery and maintenance tasks are limited to subset of nodes called core nodes which are easy to handle and low overhead is created. All the transmission lies on core nodes so it is the main disadvantage as well in case of core node movement or breakdown. This mobility affects the overall performance of the protocol.

SAODV [25] uses asymmetric cryptography to secure AODV routing messages. Route discovery mechanism is protected by using the security requirement features like data authentication, source authentication, importing authorization codes, and integrity. SAODV implies two mechanisms; that is, digital signatures are used to protect the nonmutable data in the RREQ and RREP messages and hash chains are used in SAODV to authenticate the hop count of the AODV routing messages (not only by the end points but by any node that receives one of those messages). A hash chain is formed by applying a one-way hash function repeatedly.

CSROR [26] uses different parameter from different layers employing the cross-layer information exchange mechanism. Destination node is responsible for selection of route on the basis of bandwidth, security, and energy. After the route request is initiated, these parameters are captured along the path for the resource aware and secure path establishment. Backup route is always maintained in case of any topological changes.

The rest of the paper is structured as follows. In Section 2, related works on different multipath routing protocol are summarized. In Section 3, proposed mechanism of adaptive cross-layer multimath routing protocol and its functionalities are given. Route discovery process details are explained in Section 4. Experimental results about simulation, parameters, and performance evaluation are presented in Section 5. Finally, conclusion and future work are given in Section 6.

2. Related Work

Some serious research has been carried out in MANET different aspects, ranging from routing, energy management, to security requirements, and so forth. MANET basic goal is to work in multihop fashion so that intermediate nodes forward packets to the destination. Therefore, intermediate nodes play an important role in MANET. Availability is the main focus in the overall performance of the network, which demands efficient routing mechanism for MANET. Large number of routing protocols have been developed, which can be broadly classified as table driven (proactive) and on-demand (reactive) schemes [27]. Another one combines the characteristics of both known as hybrid routing protocols. Proactive routing table searches for a path before anyone needs it. Reactive routing protocol searches for path whenever any node wants to send data to destination; however, both schemes have their own advantages and disadvantages. Our main focus of attention is reactive routing protocol. Reactive protocol works in two steps, that is, route discovery and route maintenance. In route discovery phase, whenever a source needs path to the destination, global flooding technique is used to detect all the possible paths to destination. Once all paths are discovered, source node selects one path to send the datagram packet to the destination. This single path selection is mostly done on the basis of shortest path. Shortest path generally follows the Bellman-Ford Algorithm, for example, OLSRBF [28]. The problem with the shortest path is that every node in the MANET will probably choose that path. This might become the center point of communication in most cases and more traffic passes through it. As a result more traffic yields more congestion and more delay [29]. This problem is solved by multipath routing.

Some or all paths can be utilized for sending data packet from source to the destination. Multipath protocols help in solving the congestion problem but add some complex questions as well. Once source gets all possible paths, there arises a need for mechanism for the selection of these paths; that is, how many paths are used? Some routing protocols make use of all paths available, while others tend to choose some of them based on certain criteria [30–33]. In efficient design of

a protocol, there is always a tradeoff between the following parameters, that is, reliability, energy, delay, overhead, and so forth. Some of the energy efficient protocols are in [34–36].

Some of the cross-layer approaches used by the research community are listed. Reference [37] uses transport layer protocol version to simulate the effective increase in efficiency in terms of performance. Using the routing information at the transport level protocol, better throughput and end to end are achieved. Load of the nodes and mobility increase the lost packet, which will be minimized with the better interaction between transport protocol and routing information.

Several routing protocols have been proposed for multimedia traffic. Increase in use of multimedia applications forces the researcher to focus on the development of multimedia routing protocol. Several protocols have been tested that show good result for multimedia communication in MANET. Reference [38] considers that, with the aim of improving the performance of multimedia services over ad hoc systems, the use of cross-layer techniques could be the trend to follow.

MANET ability to work depends on the intermediate nodes cooperation and trust worthiness. In addition to nodes, some applications also need secure environment. A variety of secure routing protocols [39] have been developed to provide security in terms of detecting corruption from the nodes as well as reliability of the path. Protocols like [40] add the trust management [41] feature to the secure protocols. Reference [42] also presented a secure routing protocol based on cross-layer design and energy harvesting methods. Parameters are exchanges between different layers to get the knowledge of the states of node for efficient utilization of energy.

The proposed routing is adaptive in nature, that is, keeping in view the nature of the application; it selects two or more routes from source to destination. There is one default path, while other paths are based on available data rates, end-to-end delay, and security. Cross-layered mechanisms are used to exchange parameters across different layers. The protocol is taking care of the following three scenarios:

- (i) Two or more than two default routes.
- (ii) Two or more than two routes for multimedia applications.
- (iii) Two or more than two secure routes for sensitive applications.

For better selection and optimization, cross-layer information is exchanged between different layers.

3. Proposed Mechanism

In MANET, there are many applications and may be a variety of scenarios. A single route selection mechanism may perform well in one scenario but may not in another. For example, AODV [9] routing protocol may perform well for simple applications but is not suitable for multimedia or such applications which need security. Similarly, CSROR [26] may work well to ensure some sort of security; however, it is not suitable for simple applications, which do not need security. Keeping in view wide range of applications and scenarios associated

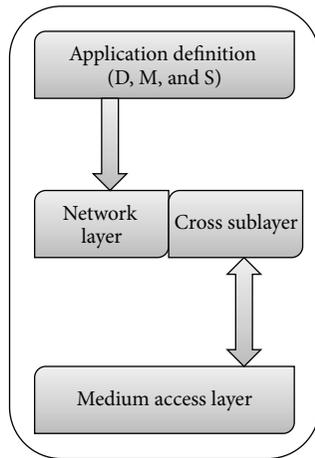


FIGURE 1: Proposed cross-layer architecture.

with MANETs, we propose an adaptive mechanism which decides multipath routes from source to destination by considering the type of application. The framework of the proposed scheme is given in Figure 1.

The proposed scheme defines the type of application at application layer, as D, M, and S, where

- (i) D represents default application;
- (ii) M represents multimedia application;
- (iii) S represents secure application.

The proposed protocol always selects two or more than two optimum routes depending on type of application. The route selection process is adaptive and closely matches the application requirements. Different types of applications have different requirements. An optimum route is always selected by default; however, various applications can convey their individual requirements to the proposed protocol using few parameters such as bandwidth, delay, and security.

The default route is used for those applications which are nonsensitive and do not need more bandwidth. Default route selects the shortest path from source to destination similar to AODV.

Multimedia applications need such routes which have more bandwidth and minimum end-to-end delay. For such application, the proposed routing protocol selects two or more than two routes which are bandwidth rich having minimum delay from source to destination.

Secure route is selected when some sort of sensitive application is sent from source to destination. The proposed routing protocol takes care of network layer related security attacks.

In the proposed routing protocol, some important features are as follows:

- (i) The type of application is defined by application layer.
- (ii) Security module is working at network layer.
- (iii) Bandwidth and end-to-end delay parameters are taken from medium access layer.

3.1. System Design

3.1.1. Basic Assumptions. We assume that, mostly, MANETs are established for three types of applications, that is, simple, multimedia, and applications having security concerned.

3.1.2. Basic Design. The proposed routing scheme uses two types of control packets for searching routes from source to destination:

- (i) A broadcast route request packet.
- (ii) A broadcast route reply packet.

The format of route request packet is given in Figure 2.

The route request packet consists of fields such as source ID, number of intermediate nodes, routing parameters, timer, and destination ID. The number of intermediate node fields increments itself with every intermediate node. Currently, we are using parameters up to $N3$, and the rest of subfields ($N4$, $N5$, and $N6$) are for future use. In case of a simple application which uses default routes, the parameters are assigned null values. The route request packet is discarded after expiry of the time value in timer field.

Route reply packet is similar to the route request packet.

3.1.3. Routing Table. The routing table consists of important information related to the path selection in accordance with the application. Typically, a routing table contains information such as destination address, hop count, and number of routes.

Routing table is shown in Table 2.

The routing table contains information of three paths from source to destination, so as to select at least two for sending data. As MANETs are mobile and dynamic networks, and routing paths are established and discarded regularly, the proposed scheme also discards routing table entries after expiry of timer.

3.1.4. Routing Parameters. The proposed scheme operates for three different types of scenarios having different parameters. Routing parameters are given in Table 3.

3.1.5. Cross-Layer Interface. A cross sublayer is defined which is used for exchanging cross-layer information as presented in Figure 1. Application layer defines the type of application, that is, default, secure, or multimedia, and the information is exchanged with the cross sublayer. Similarly, medium access layer provides information about available bandwidth and approximate delay. On the basis of the cross-layer information, the network layer selects multiple appropriate routes from source to destination.

4. Route Discovery Process

The adaptive route discovery process is discussed in this section.

TABLE 2: Routing table format.

Application type	Number of nodes	Parameter used	Source ID	Destination ID	Path 1	Path 2	Path 3	Timer
------------------	-----------------	----------------	-----------	----------------	--------	--------	--------	-------

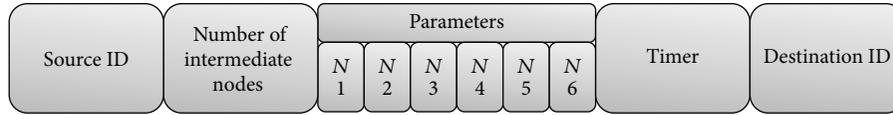


FIGURE 2: Packet format of route request.

TABLE 3: Application represented parameters.

Scenario/application	Parameter(s)
Default	Hop count
Security	Path reliability
Multimedia	Bandwidth and delay

4.1. Route Discovery Process (Default Route). Default route discovery process will be based on on-demand philosophy; that is, routes are discovered when needed. The route discovery process for default route is similar to AODV [9]. Two or more than two shortest routes from source to destination are selected among all available paths. Figure 3 demonstrates the flow of RREQ and RREP. Process will be started by source node initiation of the RREQ broadcast, also mentioning the number of paths desired by the application need. Intermediate nodes will broadcast the RREQ to their neighbors unless intermediate node is the destination node or knows a fresh path to the destination, in which case they are allowed to send the RREP. Destination node is allowed to reply according to the number of paths desired by the application. In case of N paths, destination node will reply to N RREQs. Destination will unicast the RREP to downstream neighbor which will further unicast till it reaches the source node. In case of any REER during transmission, new RREQ mechanism will be initiated by the source node. Flow chart of the mechanism is depicted in Figure 3.

4.2. Route Discovery Process (Multimedia Applications). Route discovery process for multimedia application will follow the procedure as mentioned in the default route but will take into account the parameter from different layer using the cross-layer mechanism, that is, bandwidth and delay. The destination node will here reply considering the maximum bandwidth and minimum delay. Flow chart is described in Figure 4.

4.3. Route Discovery Process (Secure). Route discovery process for secure application will follow the procedure as mentioned in the default route but will take into account the most secure path among all RREQ. Security algorithm will work on network layer. The destination node will reply to number of paths mentioned according to the preference mention in the security algorithm. Scenario of the flow of execution is given in Figure 5.

Combining algorithm of the mechanism is explained using pseudocode that is given in Algorithm 1. Route request module shows how the request will be generated after checking the sequence number. However, route reply will check the application and accordingly parameter will decide which path to choose.

4.4. Route Selection Process. Route selection process of the proposed scheme is discussed in detail in this section.

4.4.1. Default Route. Default routes will be searched if simple data needs to be transferred from source to destination; then two or more than two default routes are established between source and destination. These default routes will be the shortest routes among the available routes in terms of number of hops.

Path discovery for the default route is depicted in Figure 6. Source will send route request to its neighbor. Once all ROUTE-REQ are received by destination, the parameters are utilized in selecting the best path. In case of default route, shortest routes will be given preference. Destination will reply according to the set number of paths on shortest routes. Considering the shortest route according to number of hops, the destination node will reply to the two most suitable routes, that is,

Route 2 $\{n1, n7\}$,

Route 3 $\{n2, n7\}$.

4.4.2. Multimedia Application Route. Path discovery process for multimedia application is described in Figure 7, where route request is shown from source to destination. On receiving the route request, the destination will check the maximum bandwidth and less delay of all route requests.

Considering the high bandwidth and less delay, the three most suitable routes for multimedia application will be

(i) Route 7 $\{R3, R8, R14, R18\}$,

(ii) Route 8 $\{R3, R8, R13, R19\}$,

(iii) Route 9 $\{R3, R9, R12, R19\}$.

4.4.3. Secure Application Route. The proposed scheme uses multiple secure routes from source to destination. The mechanism prefers shortest paths. Our security approach is inspired from Confidant [43], which is capable of monitoring

```

Define App_Type, No_of _Paths;
Gen_RREQ()
{
If (no valid entry in route table for destination)
{RREQ is created with unknown Seq_No}
Else If (Have a valid destination in route table)
    {RREQ is created with last Seq_No}
SAVE [RREQ_ID]
Call Forward_RREQ()
}

Forward_RREQ()
{
If (Node listen a RREQ)
    {
    If (Same as forwarded previously)
        { Discard; }
    If (Node is destination) || (Node has route to destination)
        { Send_RREP;
          Discard RREQ; }
    Else { Forward_RREQ(); }
    }
}

Gen_RREP
{
    If (App_Type == "DEFAULT");
    {
    Create number of reply according to No_of _Paths;
    Destination will unicast reply to the shortest paths;
    }
    If (App_Type == "MULTIMEDIA");
    {
    Create number of reply according to No_of _Paths;
    Destination will unicast reply considering the maximum bandwidth and minimum delay;
    }
    If (App_Type == "SECURE");
    {
    Create number of reply according to No_of _Paths;
    Destination will unicast reply considering the most secure path preference wise;
    }
}

Data_Transmission()
{
Source node will start transmission after receiving RREP
    If (RERR occur)
    { Gen_RREQ(); }
}

```

ALGORITHM 1: Algorithm for generating route request and route reply.

and rating the nodes. When an anomalous node is detected, it is blacklisted and the proposed scheme avoids data forwarding through that particular node.

The architecture of the security module is given in Figure 8, where Reputation value (RV) is given to nodes describing the trust worthiness.

Secure route path discovery process is given in Figure 9. Route reply is based on the reputation value collected by route

request along the path. Blacklisted nodes are ignored by destination node while generating route reply.

Considering the security mechanism adaptive by secure route protocol, the most suitable routes for secure application will be

Route 1 {N1, N5, N9, N12},
Route 2 {N3, N7, N10, N13}.

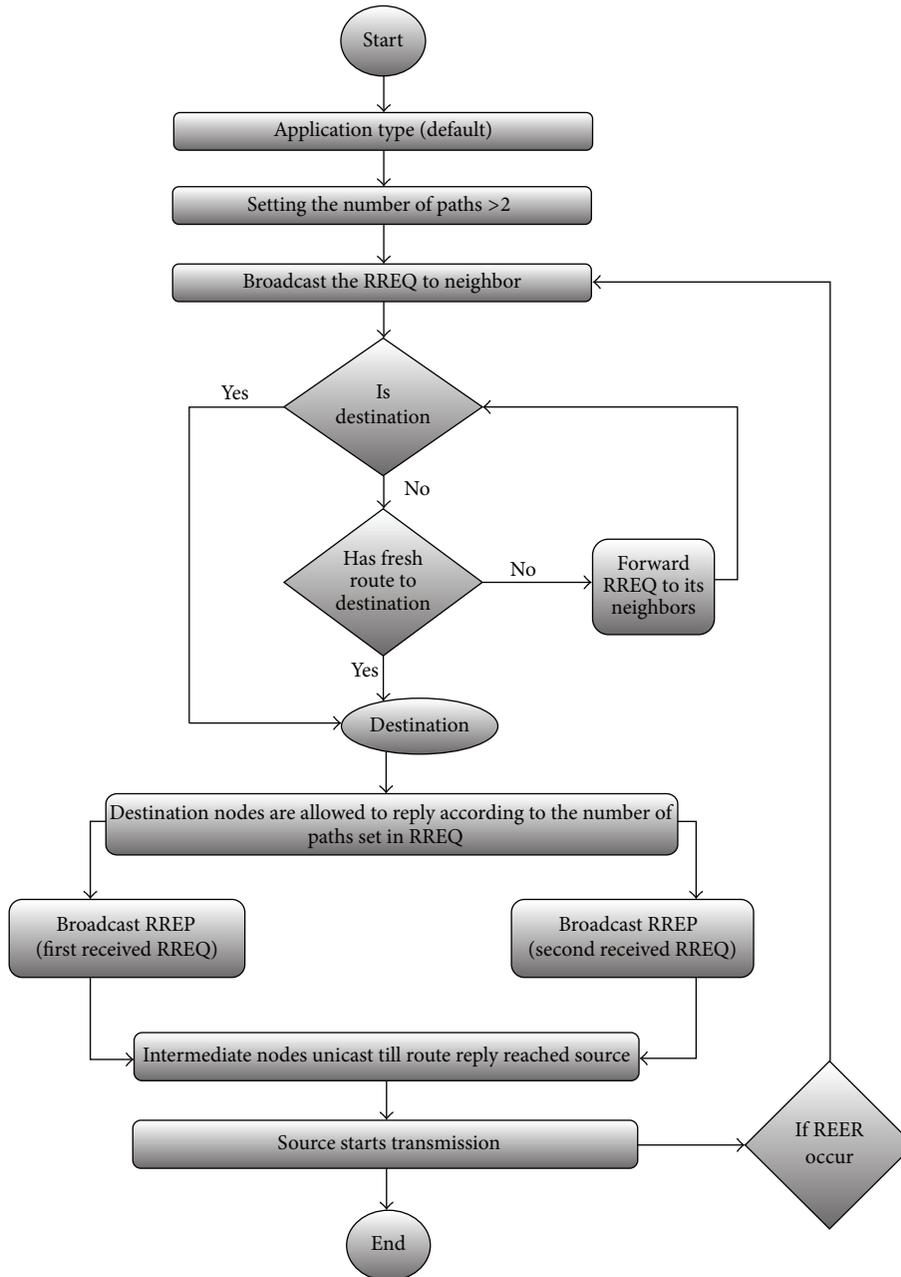


FIGURE 3: Flow of execution (default route).

5. Experimental Results

5.1. Simulation Parameters. In order to evaluate the performance of our proposed protocol, we conducted simulations in OPNET modeler 11.5. We used nodes based on 802.11 standards with different parameters given in Table 4.

5.2. Simulation Result of Comparing with Each Other. First of all, we compared the different variants, that is, default, multimedia, and secure proposed routing protocol.

Media access delay is given in Figure 10. In this case, the default variant outperforms the other two, by having below 0.001 sec media access delay in the presence of 100 nodes. The

TABLE 4: Simulation parameters.

Number of nodes	100, 200
Simulation time	3000 sec
Packet size	512 byte
Radio range	100 m
Maximum mobility	40 m/sec
Area	1500 · 500 m ²
Mobility model	Random waypoint

secure variant has the highest end-to-end delay of 0.006 sec. The reason is that secure variant first needs to search a secure

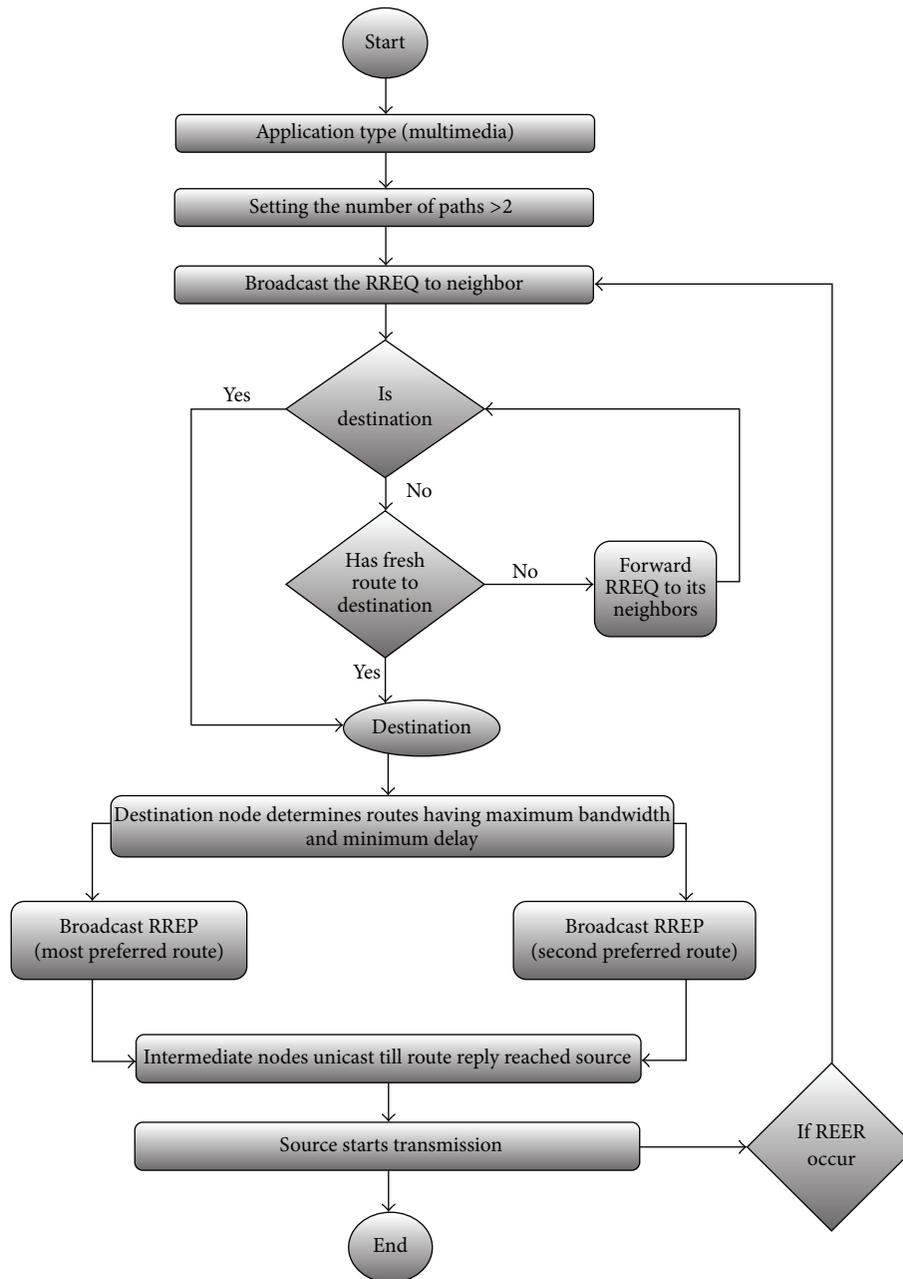


FIGURE 4: Flow of execution (multimedia applications route).

route from source to destination and then it will start packets transmission. On the other hand, multimedia variant has bandwidth parameters in its routing table, which enables it for immediate transmission from source to destination.

Route discovery efficiency of the three variants is given in Figure 11. In case of small numbers of intermediate nodes, all three variants have little difference in terms of searching routes from source to destination; however, as long as the number of nodes increases, the default variant becomes more stable as compared to the other two. The reason is that default variant searches the shorted paths from source to destination;

therefore, it takes less time. On the other hand, secure and multimedia variants have to take care of different parameters to search routes.

In any network, more data drop occurs if more nodes are added. It is clear that the data drop is less when the numbers of intermediate nodes are less as shown in Figure 12. Multimedia variant is showing less data drop as compared to the other two. The reason is that multimedia variant takes care of the data rates/bandwidth. A routing path having more bandwidth will have less data drop as compared to the others. Default route has more data drop as it searches the shortest

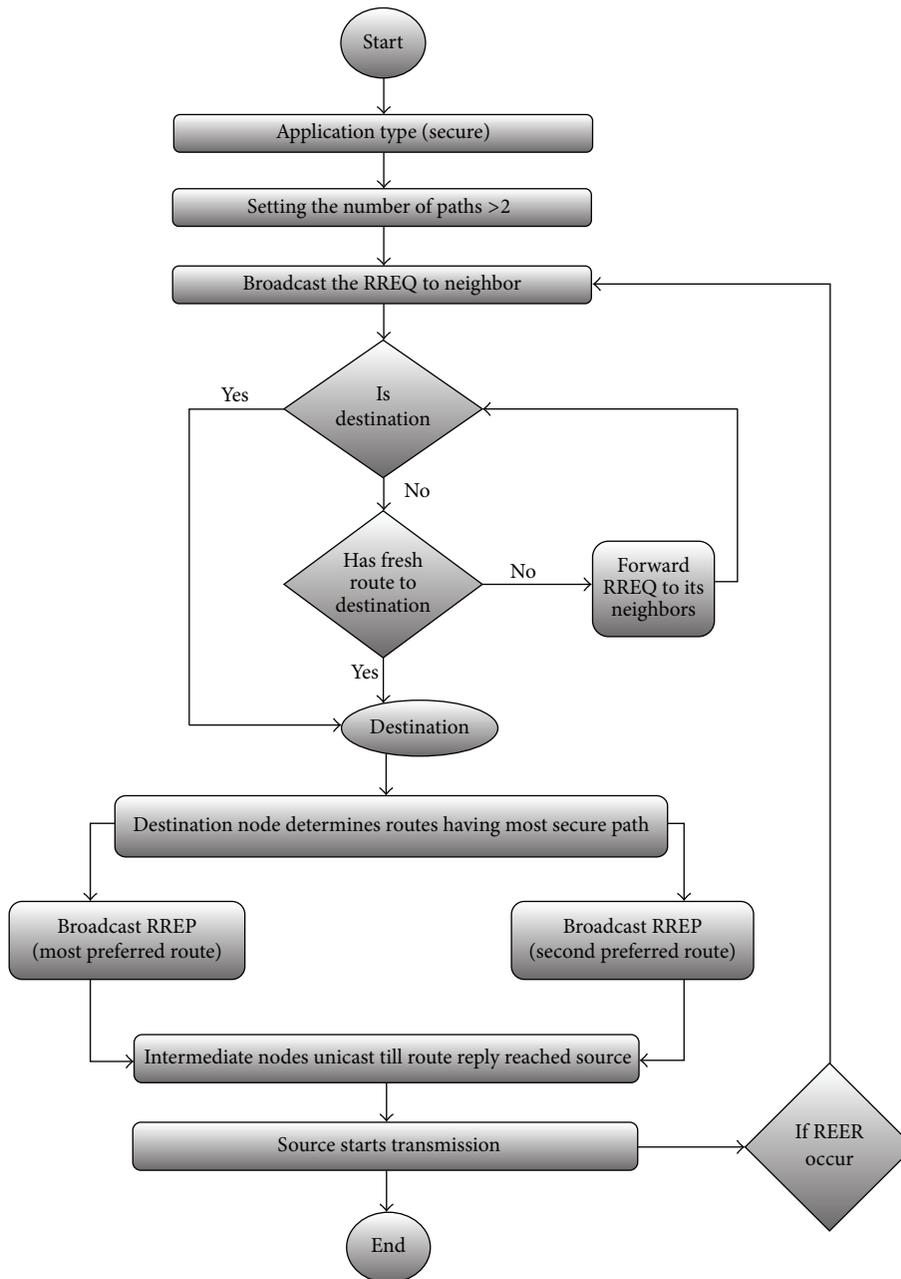


FIGURE 5: Flow of execution (secure route).

path from source to destination without considering available bandwidth and reliability of the selected routes. The shortest routes tend to be overloaded as well, hence dropping packets with higher ratio. Secure path shows average data drop as compared to the other two variants.

Routing overheads for a network of 100 nodes are given in Figure 13. These results show that the default variant has the smallest routing overheads as compared to the other two. The reason behind more routing overheads in multimedia and secure variants is that, both of them take care of additional parameters such as bandwidth and security for searching routes from source to destination. Such kind of searching

generates more control packets as compared to default variant, which selects the shortest route without considering additional parameters.

Network load is mentioned as shown in Figure 14. These results show that default network load is low and stable as compared to the other two variants. Multimedia has the highest network load as the paths have to communicate bandwidth parameter constantly before transmitting while the secure route has intermediate load as compared to the other two.

In Figure 15, it is clear that as the number of packet grows the multimedia variant outperforms the other two.

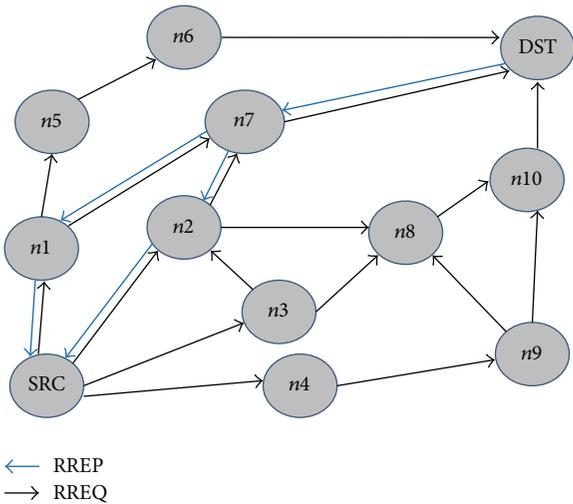


FIGURE 6: Path discovery process (default route).

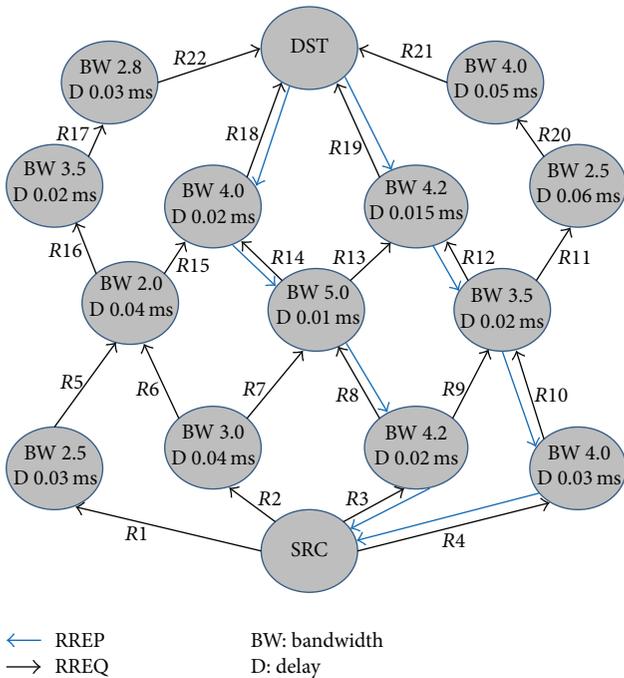


FIGURE 7: Path discovery process (multimedia application route).

The reason behind this is the bandwidth parameter taken by the multimedia application. The higher the bandwidth, the higher the number of packets transmitted. The default route just takes the shortest path into account which might not be useful for higher number of packets transmitted as the shortest paths are always congested, while the secure route is also considered the secure path not the fastest path.

5.3. Default Route Proposed Protocol Comparison with Different Protocol. Packet drop is shown in Figure 16 for 200 nodes. The comparison is made between DSR, AODV, OLSR, and proposed default routing protocol. It can be seen that DSR

and OLSR have higher packet drop than AODV, whereas proposed default route outperforms AODV as well.

Figure 17 shows the network load in case of 200 nodes. AODV and proposed default route have approximately same network load. Initially, as more nodes are involved in routing, more control packets are shared among the network. With the increase in time, the network load is stabilized. Default protocol also outperforms other opponent protocols.

Medium access delay of DSR, AODV, OLSR, and proposed default route is shown in Figure 18 for 200 nodes. It depicts that single path medium access delay is less as compared to our proposed default protocol. Medium access delay of default protocol is higher as compared to others because it searches for multiple optimal paths instead of relying on a single path. This delay increased to some extent in the case when the number of nodes increases, as many nodes will be involved in path establishment.

Figure 19 illustrates the routing overhead for 200 nodes. It is found that routing overhead is lesser in proposed default protocol as compared to existing opponents like DSR, AODV, and OLSR. In case of proposed default protocol, a small number of control messages are exchanged, hence lesser routing overhead.

Figure 20 represents the route discover time for 200 nodes. It depicts that OLSR and DSR have smaller route discovery time as compared to AODV and proposed default protocol. With the increase in number of nodes the route discovery time reduces gradually for default protocol. Default protocol tends to perform well as the saturation of nodes increases.

5.4. Multimedia Route Proposed Protocol Comparison with Different Protocol. Similar set of experiments have been carried out for multimedia data considering the PLQBR, QAODV, and CEDAR as opponents. Figure 21 compares the packet drop for 200 nodes. Main reason of packet drop is due to mobility; whenever intermediate route is not able to find a route, the packet is dropped. Packet is dropped by source node if, after some attempts, it is unable to find the route or buffer overflow occurs. Less packet drops are experienced due to rich bandwidth available path.

Network load of large network is shown in Figure 22 for 200 nodes. PLQBR, QAODV, and CEDAR seem to have higher load, while proposed multimedia route has smaller impact on the network traffic. Proposed multimedia route selects path on the basis of higher bandwidth and lower delay which accomplished the network to stay healthy.

Medium access delay is depicted in Figure 23 for 200 nodes. Here, it is also clear that our proposed multimedia protocol delay is larger than the others due to multipath nature of protocol. The protocol takes some time to search for rich bandwidth aware and less delay path.

Routing overhead is the number of control packets that every node sends in order to get the knowledge of the network and establish paths. Routing overhead for 200 nodes is shown in Figure 24. These results show that CEDAR has higher overhead, whereas PLQBR and QAODV show better performance than CEDAR. However, proposed multimedia route

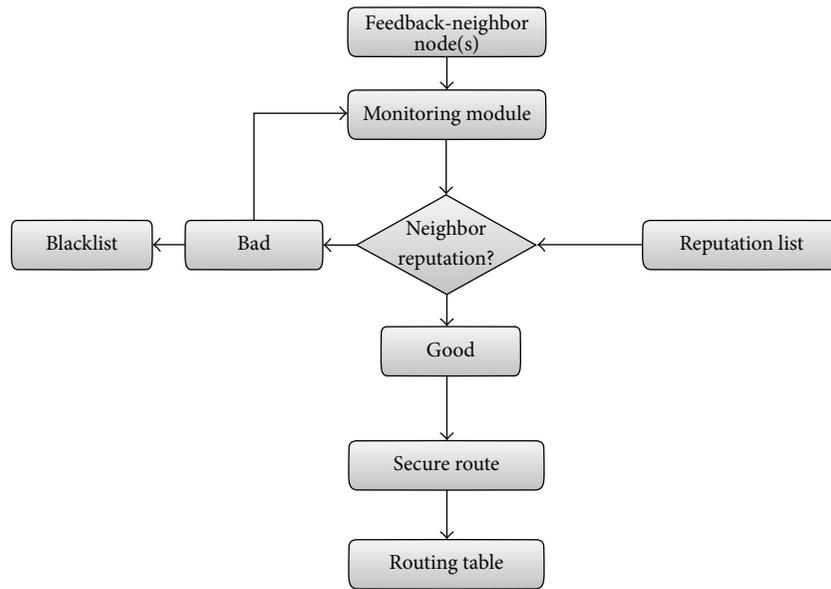
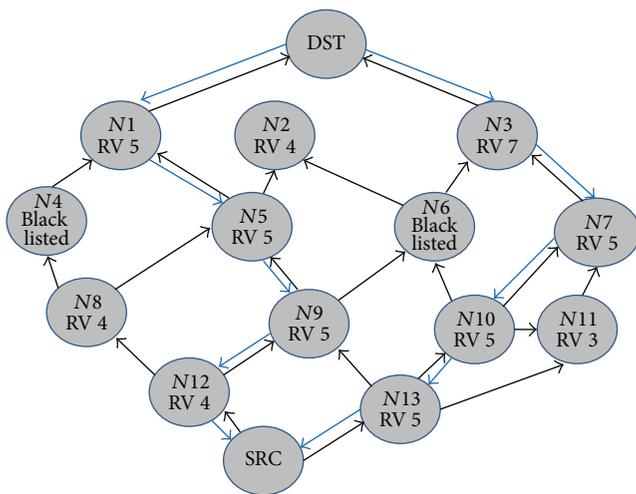


FIGURE 8: Architecture of the security module.



← RREP
 → RREQ
 RV: reputation value

FIGURE 9: Path discovery process (secure route).

shows excellent result in both scenarios outperforming the other variant.

Route discovery time of PLBQR, QAODV, CEDAR, and multimedia protocol is described in Figure 25 for 200 nodes. It can be observed from Figure 25 that CEDAR is fast enough to beat its opponent; however, as the saturation of nodes increases, proposed multimedia variant is good enough to bring its discovery time to best level among all of them.

5.5. Different Protocol Comparison with Security Route Proposed Protocol. Figure 26 shows the packet delivery ratio at

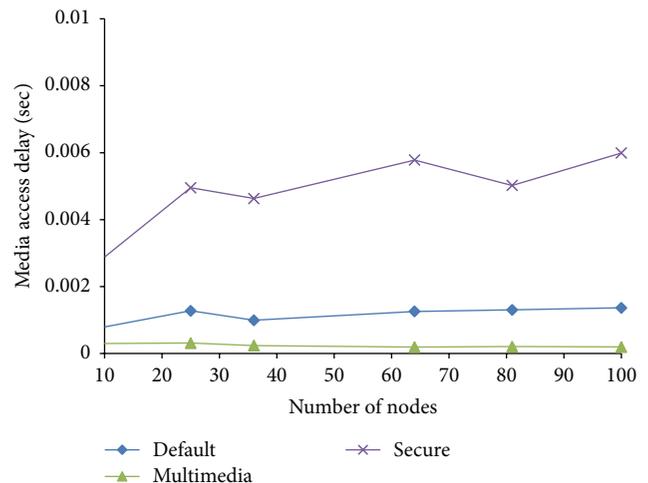


FIGURE 10: Media access delay for default, multimedia, and secure routes.

maximum speed between SAODV, CSROR, and proposed mechanism. SAODV delivery is decreased with the increase in speed. CSROR also shows the 77% delivery rate, whereas our proposed mechanism shows 88% delivery rate at all speeds.

Average delay at maximum speed is shown in Figure 27. Delay increases with the increase in mobility speed. SAODV has higher delay due to calculation of cryptographic algorithm, whereas CSROR performance is decreased with the increase in mobility. However, proposed secure routing protocol has 0.2 sec delay at maximum speed.

Routing overhead is mentioned in Figure 28 and shows that by increasing mobility the overhead will also be increased. However, proposed mechanism tends to show that

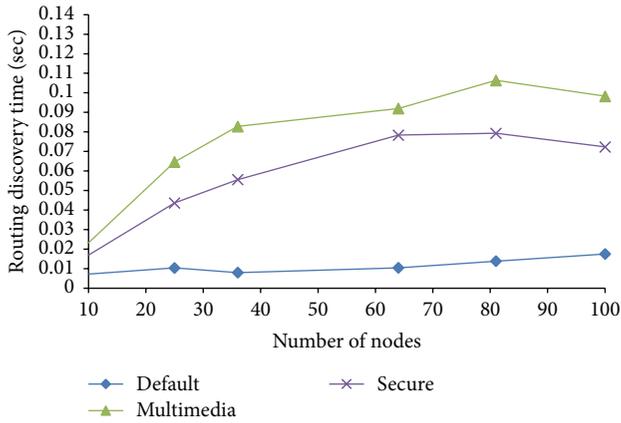


FIGURE 11: Route discovery time for default, multimedia, and secure routes.

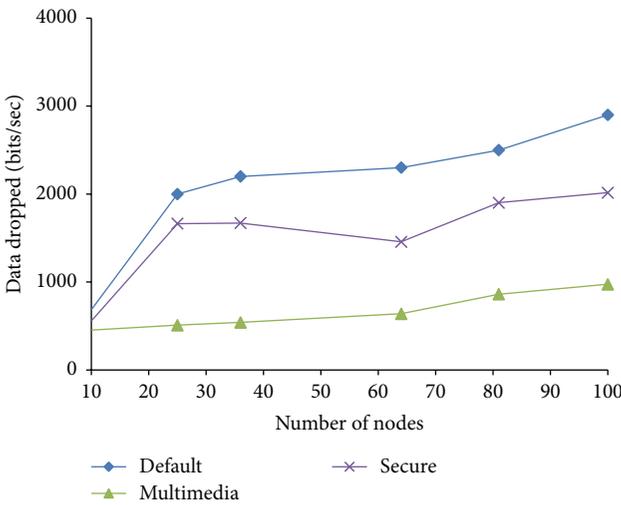


FIGURE 12: Data dropped in default, multimedia, and secure routes.

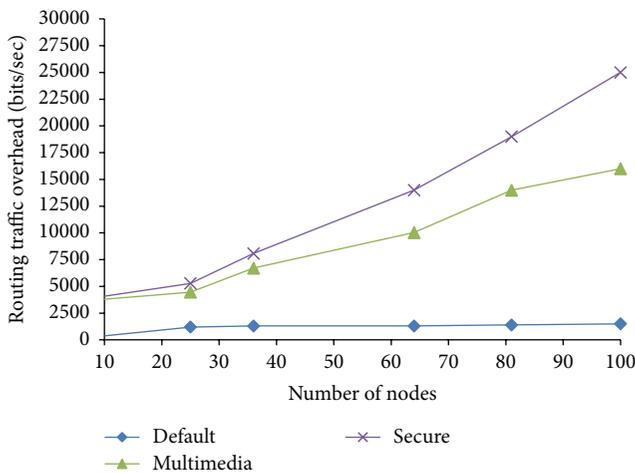


FIGURE 13: Routing traffic overhead time in default, multimedia, and secure routes.

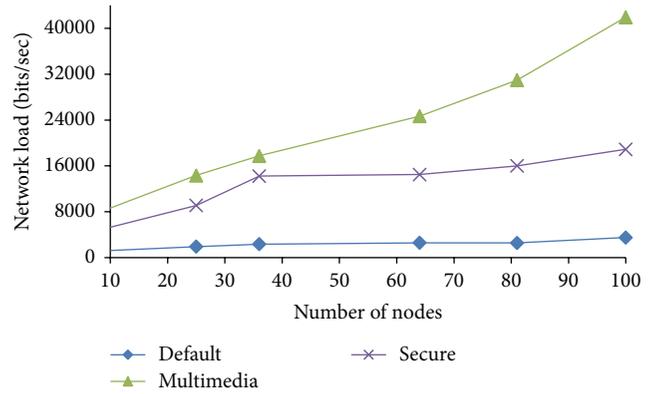


FIGURE 14: Network load in default, multimedia, and secure routes.

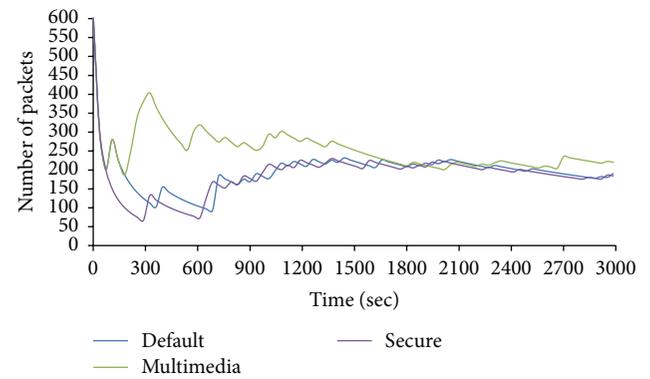


FIGURE 15: Number of packets sent in default, multimedia, and secure routes.

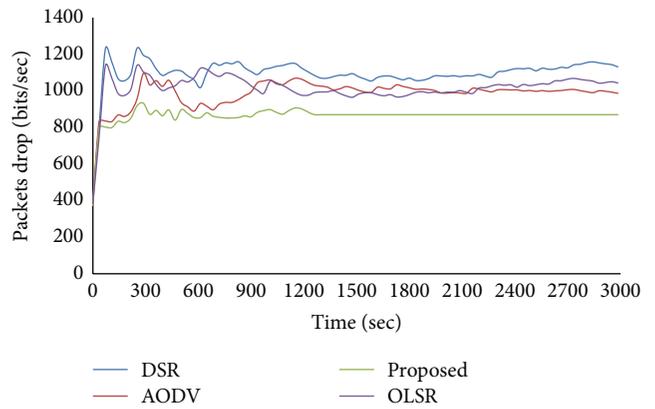


FIGURE 16: Packets drop (200 nodes).

overhead becomes stable after sometime showing no major variation.

The average end-to-end delay for a network in presence of malicious nodes is shown in Figure 29. Smallest end-to-end delay is observed in case of CSROR.SAODV that has slightly more end-to-end delay as compared to CSROR and proposed mechanism due to involvement of cryptographic operations in route discovery. In presence of malicious nodes, 0.5 sec delay is observed for proposed secure routing mechanism.

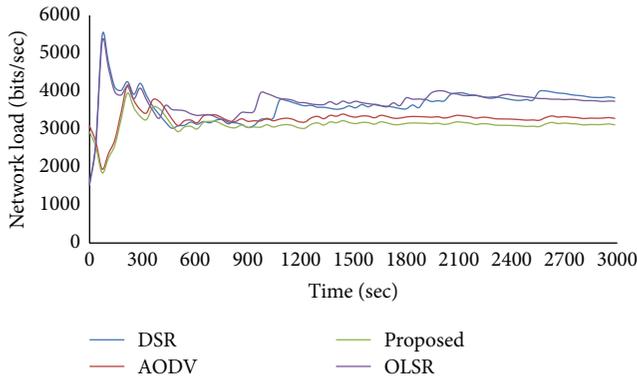


FIGURE 17: Network load performance (200 nodes).

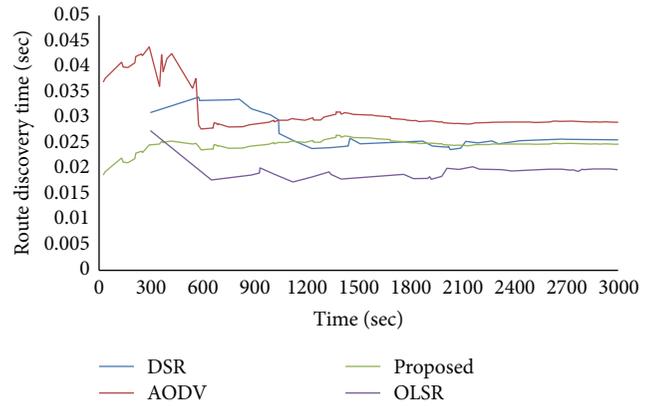


FIGURE 20: Route discovery time (200 nodes).

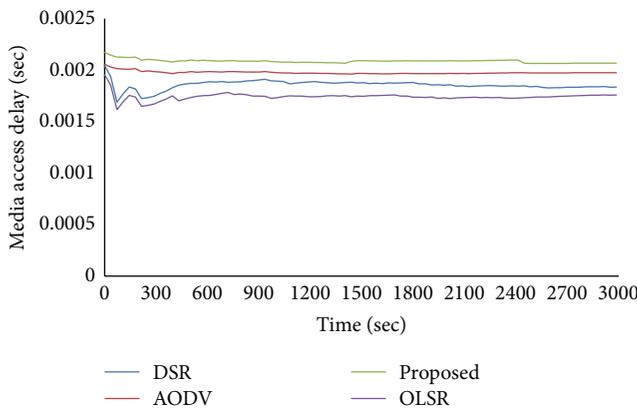


FIGURE 18: Media access delay (200 nodes).

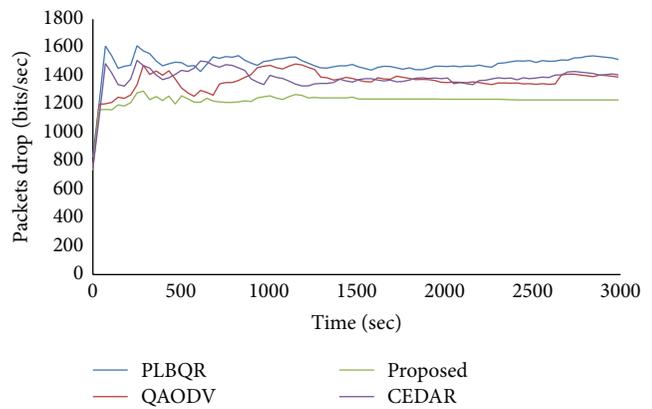


FIGURE 21: Packets drop (200 nodes).

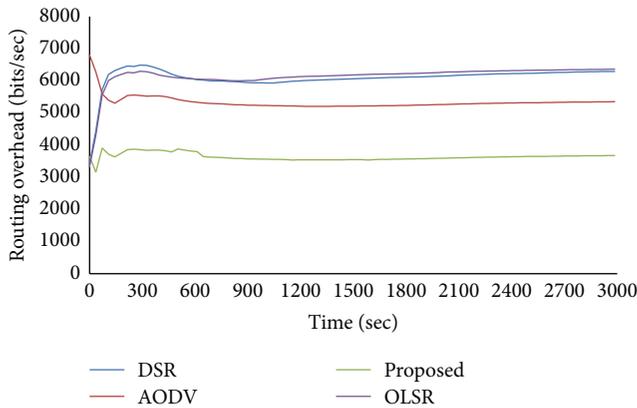


FIGURE 19: Routing overhead (200 nodes).

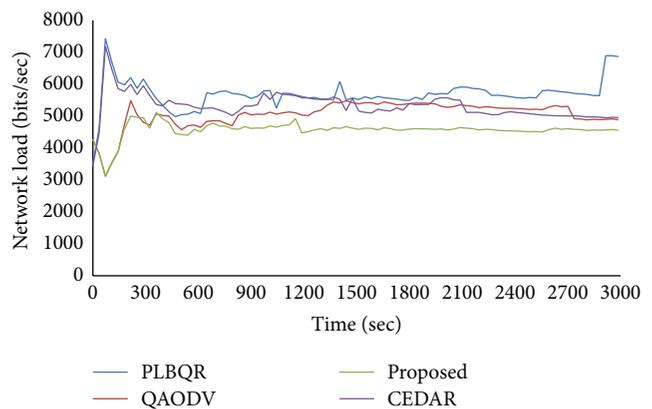


FIGURE 22: Network load performance (200 nodes).

In the presence of malicious nodes, average delay of proposed secure route, SAODV, and CSROR is mentioned in Figure 30, stating that CSROR performs well by providing less average delay than the other two opponents. Increasing pause time helps proposed mechanism in achieving less delay.

Packet delivery of secure proposed mechanism at maximum speed in presence of malicious nodes is also higher than CSROR and SAODV as shown in Figure 31. Packet delivery ratio is decreased to below 70% in SAODV and 80% in

CSROR, while in the proposed mechanism it is approximately 85%.

The packet delivery ratio of CSROR, SAODV, and proposed protocol with pause time in the presence of malicious nodes is given in Figure 32. The packet delivery ratio of proposed protocol is approximately 85% more than CSROR and SAODV because of neglecting the malicious nodes.

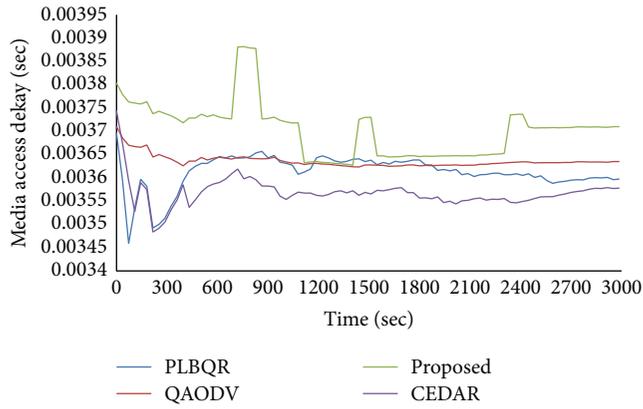


FIGURE 23: Media access delay (200 nodes).

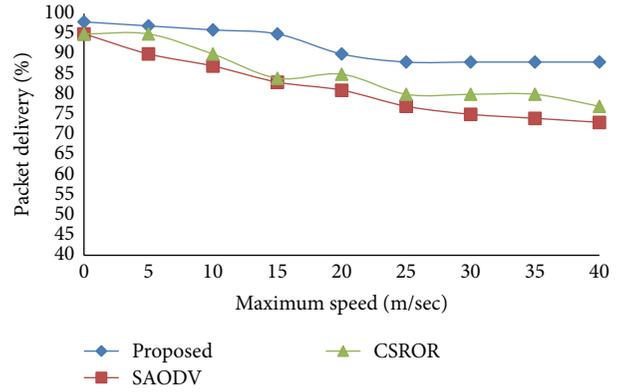


FIGURE 26: Packet delivery at maximum speed.

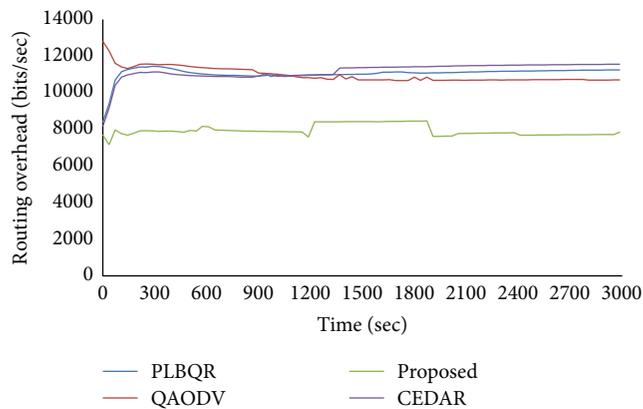


FIGURE 24: Routing overhead (200 nodes).

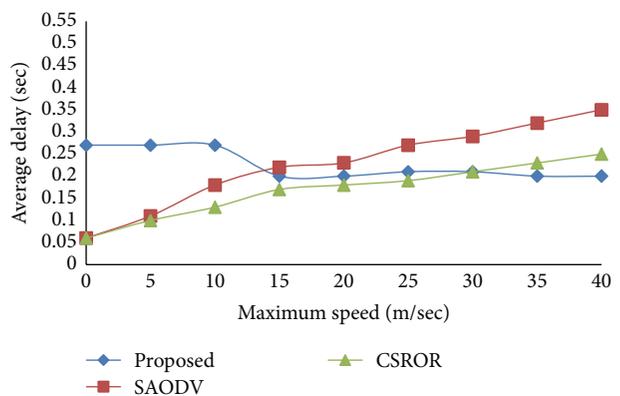


FIGURE 27: Average delay at maximum speed.

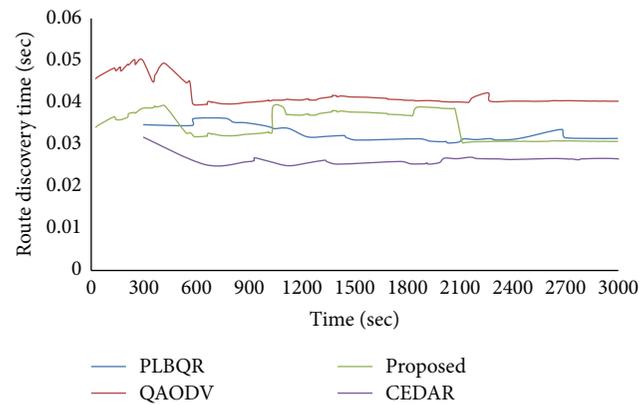


FIGURE 25: Route discovery time (200 nodes).

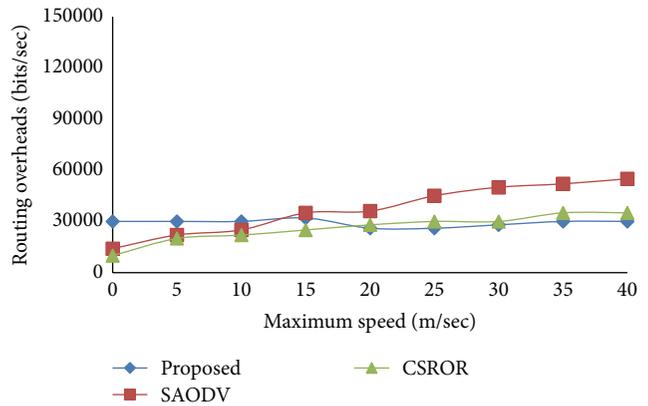


FIGURE 28: Routing overhead at maximum speed.

6. Conclusions and Future Work

In this paper, we presented cross-layer multipath routing protocol for MANET. The proposed protocol has two important features, that is, security and adaptive nature. These important features are achieved by multipath framework using cross-layer interface. Our proposed solution is capable of choosing multipaths by considering the type of application.

The proposed protocol is compared with many existing protocols such as DSR, AODV, OLSR, CEDAR, PLQBR, QAODV, SAODV, and CSROR to evaluate three important application environments, that is, default applications, multi-media applications, and applications requiring security. The comparison covers most of the scenarios such as the packet delivery ratio, average delay, and routing overheads with

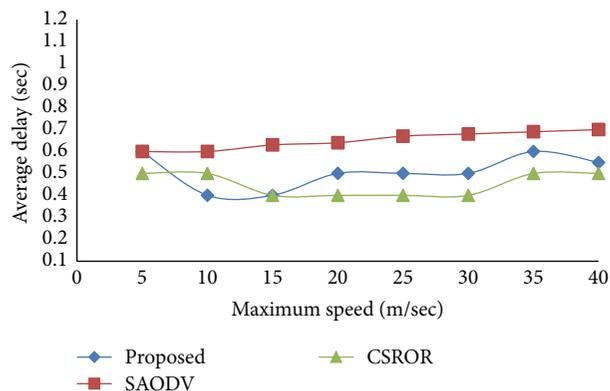


FIGURE 29: Average delay at maximum speed in presence of malicious nodes.

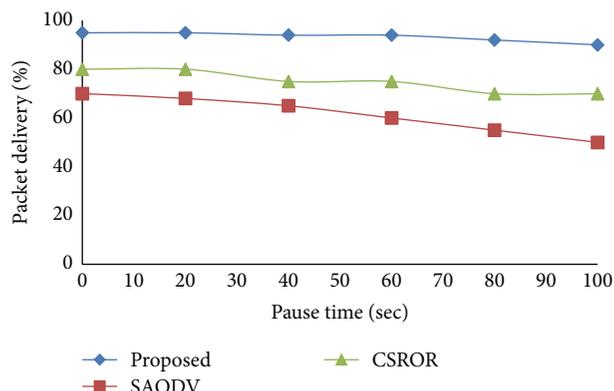


FIGURE 32: Packet delivery ratio with pause time in presence of malicious nodes.

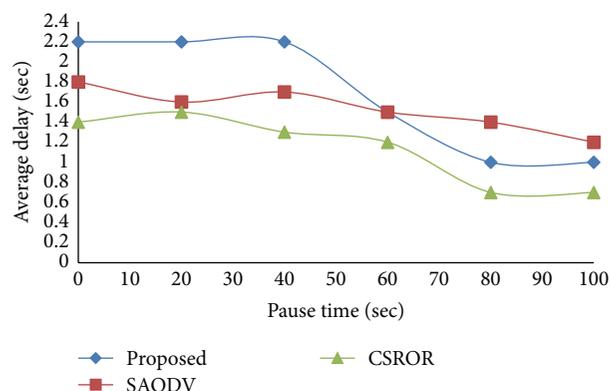


FIGURE 30: Average delay at pause time in presence of malicious nodes.

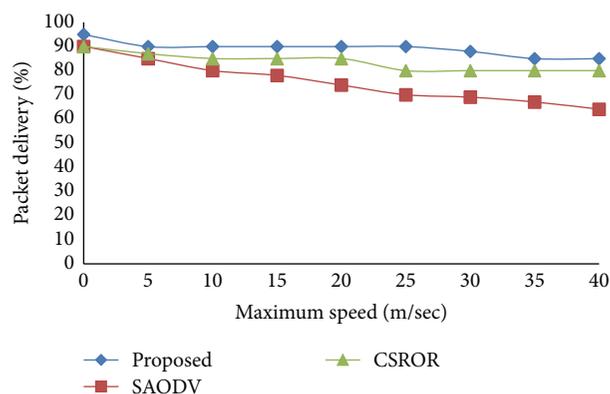


FIGURE 31: Packet delivery at maximum speed in presence of malicious nodes.

and without malicious nodes. The proposed protocol is very effective in most of the scenarios that we tested.

In future, we are planning to further strengthen the security of proposed routing scheme by introducing packet encryption and key exchange mechanism. Furthermore, we may consider to test and implement it in real scenarios.

Competing Interests

The authors declare that there are no competing interests regarding the publication of this paper.

Acknowledgments

The authors would like to extend their sincere appreciation to the Deanship of Scientific Research at King Saud University for funding this research group no. 037-1435-RG.

References

- [1] L. Abusalah, A. Khokhar, and M. Guizani, "A survey of secure mobile Ad hoc routing protocols," *IEEE Communications Surveys and Tutorials*, vol. 10, no. 4, pp. 78–93, 2008.
- [2] R. Lacuesta, M. Garcia, J. Lloret, and G. Palacios, "Study and performance of ad hoc routing protocols," in *Mobile Ad Hoc Networks: Current Status and Future Trends*, pp. 71–101, CRC Press, Taylor and Francis, 2011.
- [3] C. E. Perkins and P. Bhagwat, "Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers," in *Proceedings of the Conference on Communications Architectures, Protocols and Applications (SIGCOMM '94)*, pp. 234–244, London, UK, September 1994.
- [4] S. Murthy and J. Garcia-Luna-Aceves, "An efficient routing protocol for wireless networks," *Mobile Networks and Applications*, vol. 1, no. 2, pp. 183–197, 1996.
- [5] G. Pei, M. Gerla, and T.-W. Chen, "Fisheye State Routing: a routing scheme for ad hoc wireless networks," in *Proceedings of the IEEE International Conference on Communications (ICC '00)*, pp. 70–74, New Orleans, La, USA, June 2000.
- [6] J. J. Garcia-Luna-Aceves and M. Spohn, "Source-tree routing in wireless networks," in *Proceedings of the 7th International Conference on Network Protocols (ICNP '99)*, pp. 273–282, October–November 1999.
- [7] G. Malkin and M. Steenstrup, "Distance-vector routing," in *Routing in Communications Networks*, pp. 83–98, Prentice Hall, Englewood Cliffs, NJ, USA, 1995.
- [8] J. Moy, "Link-state routing," in *Link-State Routing, Routing in Communications Networks*, pp. 135–157, Prentice Hall, Englewood Cliffs, NY, USA, 1995.

- [9] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '99)*, pp. 90–100, New Orleans, La, USA, February 1999.
- [10] D. Johnson, D. Maltz, and J. Broch, "DSR: the dynamic source routing protocol for multi-hop wireless ad hoc networks," in *Ad Hoc Networking*, pp. 139–172, Addison-Wesley, 2001.
- [11] C.-K. Toh, "Associativity-Based routing for ad-hoc mobile networks," *Wireless Personal Communications*, vol. 4, no. 2, pp. 103–139, 1997.
- [12] V. D. Park and M. S. Corson, "Highly adaptive distributed routing algorithm for mobile wireless networks," in *Proceedings of the 16th IEEE Annual Conference on Computer Communications (INFOCOM '97)*, pp. 1405–1413, April 1997.
- [13] M. R. Pearlman and Z. J. Haas, "Determining the optimal configuration for the zone routing protocol," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, pp. 1395–1414, 1999.
- [14] T. Hamma, T. Katoh, B. B. Bista, and T. Takata, "An efficient ZHLS routing protocol for mobile ad HOC networks," in *Proceedings of the 17th International Conference on Database and Expert Systems Applications (DEXA '06)*, pp. 66–70, Krakow, Poland, September 2006.
- [15] A. Kumar, D. Manjunath, and J. Kuri, *Communication Networking: an Analytical Approach*, Morgan Kaufmann, Los Altos, Calif, USA, 2004.
- [16] S.-T. Chou, H.-T. Chern, C.-M. Shiao, and Z.-J. Lee, "Cross-layer design of AODV protocol for multi-hop flow in ad hoc network," *Ad-Hoc and Sensor Wireless Networks*, vol. 17, no. 3-4, pp. 233–252, 2013.
- [17] M. M. Zoulikha and B. Amal, "Cross-layer approach among physical, MAC and routing layer in a shadowing environment," *Ad-Hoc and Sensor Wireless Networks*, vol. 21, no. 1-2, pp. 101–119, 2014.
- [18] V. Carrascal, G. Delgado, and M. Igartua, "Multipath routing with layered coded video to provide QoS for video streaming applications over MANETs," in *Proceedings of the 14th IEEE International Conference on Communication Networks (ICON '06)*, pp. 1–6, Singapore, 2006.
- [19] V. Loscri, F. De Rango, and S. Marano, "Performance evaluation of on-demand multipath distance vector routing protocol over two MAC layers in mobile ad hoc networks," in *Proceedings of the 1st International Symposium on Wireless Communication Systems (ISWCS '04)*, pp. 413–417, September 2004.
- [20] Y. Zhen, M.-Q. Wu, D.-P. Wu, Q.-J. Zhang, and C.-X. Xu, "Toward path reliability by using adaptive multi-path routing mechanism for multimedia service in mobile Ad-hoc network," *Journal of China Universities of Posts and Telecommunications*, vol. 17, no. 1, pp. 93–100, 2010.
- [21] P. Jacquet and T. Clausen, *Optimized Link State Routing Protocol (OLSR)*, Internet Draft, IETF MANET Working Group, 2001.
- [22] S. H. Shah and K. Nahrstedt, "Predictive location-based QoS routing in mobile ad hoc networks," in *Proceedings of the International Conference on Communications (ICC '02)*, vol. 2, pp. 1022–1027, May 2002.
- [23] E. Royer and C. Perkins, "Quality of service for adhoc on-demand distance vector routing," IETF Internet Draft, July 2000.
- [24] R. Sivakumar, P. Sinha, and V. Bharghavan, "CEDAR: a core-extraction distributed ad hoc routing algorithm," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, pp. 1454–1465, 1999.
- [25] M. G. Zapata, "Secure ad hoc on-demand distance vector routing," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 6, no. 3, p. 106, 2002.
- [26] S. Khan and J. Loo, "Cross layer secure and resource-aware on-demand routing protocol for hybrid wireless mesh networks," *Wireless Personal Communications*, vol. 62, no. 1, pp. 201–214, 2012.
- [27] V. Sharma and B. Alam, "Unicast routing protocols in mobile ad hoc networks: a survey," *International Journal of Computer Applications*, vol. 51, no. 14, pp. 9–18, 2012.
- [28] D. Tepsic, M. Veinovic, D. Zivkovic, and N. Ilic, "A novel proactive routing protocol in mobile ad hoc networks," *Ad-Hoc and Sensor Wireless Networks*, vol. 27, no. 3-4, pp. 239–261, 2015.
- [29] M. Tarique, K. E. Tepe, S. Adibi, and S. Erfani, "Survey of multipath routing protocols for mobile ad hoc networks," *Journal of Network and Computer Applications*, vol. 32, no. 6, pp. 1125–1143, 2009.
- [30] A. Tsirigos, Z. Haas, and S. Tabrizi, "Multipath routing in mobile ad hoc networks or how to route in the presence of frequent topology changes," in *Proceedings of the Military Communications Conference*, pp. 878–883, Vienna, Va, USA, October 2001.
- [31] L. Wang, S. Jang, and T.-Y. Lee, "Redundant source routing for real-time services in ad hoc networks," in *Proceedings of the 2nd IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS '05)*, pp. 87–93, Washington, DC, USA, November 2005.
- [32] S. Mao, S. Lin, Y. Wang, S. S. Panwar, and Y. Li, "Multipath video transport over ad hoc networks," *IEEE Wireless Communications*, vol. 12, no. 4, pp. 42–49, 2005.
- [33] A. Nasipuri and S. Das, "On-demand multipath routing for mobile ad hoc networks," in *Proceedings of the 8th International Conference on Computer Communications and Networks*, pp. 64–70, IEEE, Boston, Mass, USA, 1999.
- [34] Z.-t. Li, Q. Chen, G.-m. Zhu, Y.-j. Choi, and H. Sekiya, "A low latency, energy efficient mac protocol for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID 946587, 9 pages, 2015.
- [35] Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and X. S. Shen, "Energy and memory efficient clone detection in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 15, no. 5, pp. 1130–1143, 2016.
- [36] M. Dong, K. Ota, A. Liu, and M. Guo, "Joint optimization of lifetime and transport delay under reliability constraint wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 1, pp. 225–236, 2016.
- [37] S. Hamrioui, P. Lorenz, J. Lloret, and M. Lalam, "A cross layer solution for better interactions between routing and transport protocols in MANET," *Journal of Computing and Information Technology*, vol. 21, no. 3, pp. 137–147, 2013.
- [38] R. Sanchez-Iborra and M. Cano, "An approach to a cross layer-based QoE improvement for MANET routing protocols," *Network Protocols and Algorithms*, vol. 6, no. 3, pp. 18–34, 2014.
- [39] L. Abusalah, A. Khokhar, and M. Guizani, "A survey of secure mobile ad hoc routing protocols," *IEEE Communications Surveys and Tutorials*, vol. 10, no. 4, pp. 78–93, 2008.
- [40] J. L. Tornos, J. L. Salazar, and J. J. Piles, "Secure trust management with source routing protocol for MANETs," *Network Protocols and Algorithms*, vol. 7, no. 2, pp. 42–59, 2015.
- [41] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys and Tutorials*, vol. 13, no. 4, pp. 562–583, 2011.

- [42] A. Nasipuri and S. Das, "On-demand multipath routing for mobile ad hoc networks," in *Proceedings of the 8th International Conference on Computer Communications and Networks (IC3N '99)*, pp. 64–70, Boston, Mass, USA, October 1999.
- [43] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the CONFIDANT protocol (cooperation of nodes—fairness in dynamic ad-hoc networks)," in *Proceedings of the 3rd Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '02)*, pp. 226–236, ACM Press, Lausanne, Switzerland, June 2002.

Research Article

Security Analysis and Improvements of Session Key Establishment for Clustered Sensor Networks

Jiye Kim, Jongho Moon, Jaewook Jung, and Dongho Won

College of Information and Communication Engineering, Sungkyunkwan University, Suwon-Si 16419, Republic of Korea

Correspondence should be addressed to Dongho Won; dhwon@security.re.kr

Received 2 February 2016; Revised 19 March 2016; Accepted 10 April 2016

Academic Editor: Fei Yu

Copyright © 2016 Jiye Kim et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

WSN (wireless sensor network) is one of the main technologies in IoT (Internet of Things) applications or services. To date, several schemes have been proposed to establish a pair-wise key between two nodes in WSN, and most of them are designed to establish long-term keys used throughout the network lifetime. However, in the near future, if WSN will be used for information infrastructures in various fields such as manufacturing, distribution, or public facilities management and its life cycle can be as long as that of other common networks, it will definitely be advantageous in terms of security to encrypt messages using session keys instead of long-term keys. In this paper, we propose a session key establishment scheme for clustered sensor networks that is based on elliptic curve Diffie-Hellman (ECDH) key exchange and hash chain. The proposed scheme eliminates vulnerabilities of existing schemes for WSN and has improved security. The proposed scheme is efficient in terms of energy costs compared to related schemes.

1. Introduction

A wireless sensor network (WSN) is composed of dozens to thousands of sensor nodes and more than one gateway and is employed with the objective of collecting data regarding the conditions or changes in the target area [1, 2]. WSN is one of the key technologies in IoT (Internet of Things) applications or services and is expected to be employed in various applications in fields such as military, healthcare, public facilities management, manufacturing, distribution, and agriculture in the near future [1, 3–5]. However, WSN is vulnerable to attacks such as node impersonation attacks, man-in-the-middle (MITM) attacks, and denial-of-service (DoS) attacks by eavesdropping or altering of the messages transmitted in wireless channels, as are other common wireless networks [6–8]. Therefore, WSN should employ security techniques to meet the security requirements of data confidentiality and integrity, availability of services, and node authentication [9].

The key establishment scheme is one of the most fundamental and feasible security techniques [10]. Lai et al.'s BROSK [11], Eschenauer and Gligor's random key pool-based scheme [12], and so forth provide the function of establishing a pair-wise key between sensor nodes [13]. Such schemes

are designed with the objective of establishing a long-term key to be used throughout the lifetime of WSN under the assumption that the life cycle of WSN is much shorter than the life cycle of other networks [14]. For example, if WSN is installed to monitor a hostile environment that is not easily accessible to people, such as a battlefield or a disaster area, its life cycle is shorter than the attack time needed to determine the cryptographic keys. In this case, it is more effective for the cryptographic keys not to be rekeyed after being established, except when adding new nodes or eliminating existing nodes. However, if WSN is used for information infrastructures in fields such as manufacturing, distribution, or public facilities management, its life cycle may be long. In this case, there is a need for a session key establishment scheme that continuously renews cryptographic keys according to a cycle or an event [14].

In an information and communication system, the message sender encrypts the confidential data and transmits it in the form of ciphertext to the message receiver. However, if an attacker obtains the decryption key by hacking, he/she can obtain the plaintext or additionally perform other serious attacks using the key. In order to decrease the damage caused by such key exposure, a cryptographic key known

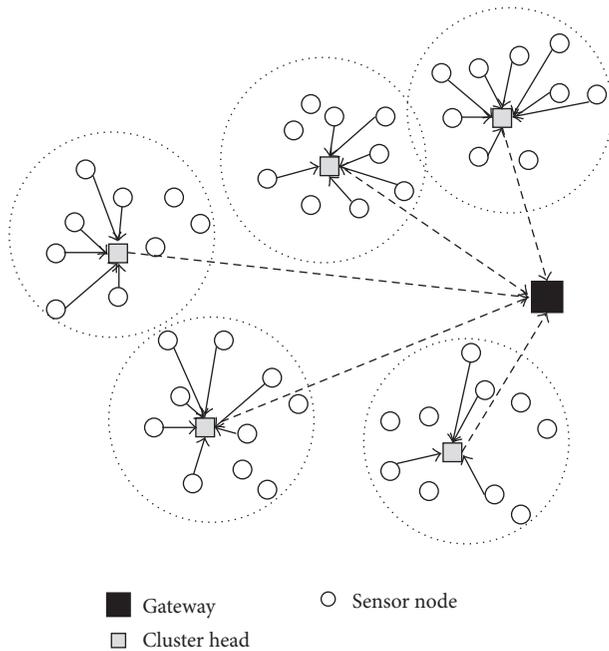


FIGURE 1: The flow of the sensed data in a clustered sensor network. In practice, the data is transmitted hop-by-hop between nonneighboring nodes.

as a session key is used only for a limited period of time. In communication protocols based on session keys, even if an attacker obtains one of the session keys, the number of ciphertexts he/she can decrypt with it is limited. Also, he/she needs more pairs of plaintext and ciphertext for cryptanalysis or needs to obtain more session keys for other attacks. Therefore, encryption of messages using session keys is definitely advantageous in terms of security [15].

In this paper, we focus on WSNs applied to applications such as healthcare, public facilities management, and industrial automation systems. Applying WSNs to such systems is more advantageous in terms of network performance and management costs compared to applying wired networks [18]. However, in such systems, WSNs should be operated for a long period of time and are security-critical. Moreover, for easy network management, such applications can employ clustered and hierarchical sensor networks, as shown in Figure 1 [19, 20]. When employing clustered sensor networks for such applications, the communication between the gateway and the cluster head requires stronger security than the communication between the cluster head and the sensor node; this is because the cluster head collects the data sensed by sensor nodes in its cluster and transmits it to the gateway [17]. Therefore, it is appropriate to apply the session key to the communication between the gateway and the cluster head in order to increase security. However, we found that existing session key establishment schemes for WSNs [16, 17] have several security flaws; they do not provide mutual authentication between two nodes and are vulnerable to node impersonation attacks and MITM attacks. In addition, neither scheme can guarantee secrecy of future

session keys if the long-term keying materials stored in the cluster head are exposed to an attacker.

In this paper, we propose a scheme to establish a session key between the gateway and the cluster head in order to enable the cluster head to transmit encrypted data to the gateway. Our proposed scheme should eliminate the weaknesses of existing schemes in order to achieve improved security. Moreover, not only the security but also the energy costs should be considered when designing the scheme because the nodes in WSNs are battery-powered. To meet these design requirements, the proposed scheme establishes session keys based on elliptic curve Diffie-Hellman (ECDH) key exchange [21, 22], an effective asymmetric key technique. Also, it employs hash chain [23–27] in order to provide mutual authentication between the gateway and the cluster head, verification of message integrity, and session key establishment, considering energy costs.

Our major contributions are as follows: first, the proposed scheme is secure against possible attacks in key establishment schemes for WSN, such as session key attacks, replay attacks, and node capture attacks. Also, it resists both node impersonation attacks and MITM attacks through mutual authentication of two communication parties and verification of message integrity. Second, compared to long-term key establishment between two nodes in WSN, and the studies are relatively more recent. Third, computation and communication costs incurred by a cluster head affect its energy consumption [28–30]. Therefore, the proposed scheme is designed to minimize the number of messages transmitted between two nodes for efficiency in terms of communication costs. Also, even though it employs asymmetric key techniques, it is more efficient in terms of computation costs compared to other schemes with similar design requirements and key establishment techniques.

The remainder of the paper is organized as follows. Section 2 reviews several key establishment schemes between nodes in WSN. Section 3 describes the assumptions, design requirements, and main ideas of our proposed scheme. Section 4 proposes the improved scheme and describes its phases in detail. Section 5 analyzes the security of the proposed scheme against possible attacks in key establishment schemes for WSN. Section 6 is devoted to analyzing its energy costs compared to other schemes with similar design requirements and key establishment techniques. Finally, Section 7 concludes this paper.

2. Review of Related Works

A few key establishment schemes have been proposed to establish a pair-wise key between sensor nodes and to provide the rekeying function in case of additions of new sensor nodes or revocation of existing sensor nodes [11, 12, 31–34]. In Lai et al.'s BROSKE [11], all sensor nodes share only one master key, and each sensor node establishes a pair-wise key with its neighboring nodes using that master key. This scheme is very efficient and simple, but the entire network can become vulnerable if even one sensor node in the network is compromised by an attacker. Eschenauer and

Gligor proposed a pair-wise key establishment scheme based on a random key pool [12]. In the predeployment phase of their scheme, keys are randomly chosen from one key pool and are preloaded in the sensor node. After deploying sensor nodes to the field, if a sensor node determines it has the same key as its neighboring node, it sets the same key to be the pair-wise key between two nodes. In this scheme, if an attacker compromises another sensor node that has the pair-wise key between two sensor nodes, he/she can decrypt the message transmitted between these two sensor nodes. Several modified schemes have been proposed in order to compensate for this weakness [32–34]. Based on Eschenauer and Gligor’s scheme, Chan et al. proposed a scheme where a pair-wise key can be established only when two sensor nodes share multiple keys instead of one key [32]. On the other hand, Du et al. proposed a scheme that combines the random key pool-based method with Blom’s method [33], which establishes a pair-wise key between two nodes using the symmetric matrix K in $K = A \cdot G$, where matrix G is the public information, and matrix A is private information in a finite field [35]. Also, Liu et al. proposed a scheme that combines Eschenauer and Gligor’s method with the polynomial-based method [34] that establishes a pair-wise key between two nodes using t -degree polynomial $f(x, y)$ that satisfies $f(i, j) = f(j, i)$ [36]. All of Chan et al., Du et al., and Liu et al.’s schemes are proposed to securely protect the links between uncompromised nodes unless a threshold number of nodes are compromised [32–34].

All of the schemes mentioned above have been proposed to establish a long-term key used throughout the life cycle of WSN [14]. Compared to such schemes, session key establishment schemes between nodes in WSN have been proposed more recently. References [14, 37, 38] proposed EBS-based rekeying schemes. Eltoweissy et al. proposed the exclusion basis system (EBS), which updates a group key for normal nodes when it evicts malicious nodes from a communication group [39]. An EBS-based scheme has a key pool of size $k + m$ ($1 < k, m < n$, where n is the number of nodes in a group). k administrative keys from the key pool are assigned to each node. When the scheme evicts some malicious nodes from the group, only m messages are needed to update a group key because the messages are encrypted using unknown keys to malicious ones. Chen and Lin proposed a session key establishment scheme for grid-based sensor networks [40]. This scheme is based on one-way hash function, mutual authentication between communication parties, and symmetric key encryption as follows: first, secret parameters (a_i, a_{i-1}) and (b_j, b_{j-1}) are preloaded to the sensor node S_i and the cluster head C_j , respectively. Then, the scheme encrypts the messages transmitted from S_i to C_j using the key $K_i = h(a_i \parallel a_{i-1})$ and the ones from C_j to the gateway using the key $K_j = h(b_j \parallel b_{j-1})$. After a period of time, K_i and K_j are replaced with $K'_i = h(K_i \parallel a_i \parallel RN_1)$ and $K'_j = h(K_j \parallel b_j \parallel RN_2)$, respectively, where both RN_1 and RN_2 are generated by the cluster head C_j . Eldefrawy et al. proposed a session key agreement scheme based on asymmetric key techniques [41]. In this scheme, the gateway receives random numbers from all sensor nodes in a cluster in order to compute

a session key for communication between member nodes in the cluster. The scheme encrypts the random numbers transmitted from sensor nodes to the gateway based on RSA [42] and the session keys from the gateway to sensor nodes based on elliptic curve cryptography [21]. Meanwhile, [43–45] proposed polynomial secret-sharing-based session key establishment schemes to address the node compromise problem.

Chen and Li’s scheme [16] and Lee and Kim’s scheme [17] employ different key establishment techniques to establish session keys between the gateway and the cluster head in clustered sensor networks. Chen and Li’s scheme establishes the $(i + 1)$ th session key by computing $sk_{i+1} = h(sk_i \parallel sk_{i-1})$, where sk_{i-1} and sk_i represent the $(i - 1)$ th and i th session keys, respectively [16]. However, if an attacker obtains sk_i and sk_{i-1} of CH_j , the future session keys to be generated in the i th and the following sessions can be computed. In other words, Chen and Li’s scheme does not guarantee the secrecy of future session keys. Lee and Kim applied a modified Diffie-Hellman key exchange (DHKE) technique [46] to their scheme in order to consider the efficiency in terms of computation costs of cluster heads [17]. However, because all cluster heads in this scheme share only one private key, which is a long-term key used throughout the life cycle of the WSN, it can also be compromised by an attacker. Therefore, this scheme cannot guarantee the secrecy of future session keys. Furthermore, we found that their scheme is vulnerable to node impersonation attacks or MITM attacks. In Appendices A through D, we review Chen and Li’s scheme and Lee and Kim’s scheme in detail and analyze their security.

3. Design Outline of the Proposed Scheme

We consider the applications of WSNs such as healthcare, public facilities management, and industrial automation systems. The WSNs utilized for such applications should be operated for a long period of time and are security-critical.

3.1. Network Model. Regarding the WSN that employs the proposed scheme, we assume the following:

- (i) The WSN is a clustered sensor network divided into several clusters; it consists of three types of nodes: sensor nodes, cluster heads, and a gateway. In a cluster, the sensor nodes sense the conditions or change regarding the target area and transmit the data to their cluster head. The cluster heads not only control the sensor nodes in respective clusters [13] but also collect the data sensed by the sensor nodes and transmit the data to the gateway [17].
- (ii) Sensor nodes have limited resources such as power, computation and communication capability, memory, and transmission range [1, 47–50], whereas the gateway has an abundance of these resources.
- (iii) Cluster heads are fixed and not selected from ordinary sensor nodes because resources of cluster heads are richer than those of ordinary sensor nodes. Nevertheless, our scheme can still be also applied to WSNs

that perform cluster head selection [51]. This will be discussed at greater length in Section 4.2.

- (iv) A sensor node or a cluster head communicates with a nonneighboring node in a hop-by-hop fashion. We assume that the intermediate nodes between the cluster head and the gateway are not required to read the message contents exchanged between two nodes. Therefore, though the cluster head transmits its message hop-by-hop to the nonneighboring gateway, the message is encrypted/decrypted only at the two nodes; that is, the message encryption/decryption is performed end-to-end.
- (v) In WSNs, sensor nodes or cluster heads are usually battery-powered. In this study, because the WSN nodes have a long life cycle, their batteries should be replaced or charged once every few years of system operation [18].
- (vi) Sensor nodes or cluster heads can be randomly scattered in a target area or deployed according to a defined network topology. We assume that their spatial distribution depends on the application.
- (vii) All nodes in the WSN, that is, sensor nodes, cluster heads, and the gateway, are static. That is, they are not mobile.

3.2. Adversary Capabilities. We assume that an attacker can eavesdrop on or modify transmitted messages. Sensor nodes and cluster heads are vulnerable to physical attacks because they are usually deployed without tamper-proof devices in unattended environments [30, 52–54]. Therefore, an attacker can perform node capture attacks, that is, the capture of a node in a WSN and the extraction of secret parameters for use in subsequent attacks. The gateway is a trusted node that is not compromised and is secure against privileged-insider attacks or stolen-verifier attacks.

3.3. Design Requirements. The goal of our proposed scheme is for the cluster head to securely transmit the data to the gateway. For this goal, the proposed scheme provides functions to establish a session key between the cluster head and the gateway and encrypt/decrypt the data using it. In addition, the security weaknesses of existing schemes described in Section 2 will be addressed in the proposed scheme. The design requirements of the proposed scheme are as follows:

- (i) Because the proposed scheme protects the data using a session key, the session key should not be exposed to an attacker attempting to eavesdrop on transmitted messages. Furthermore, although long-term parameters in the cluster head are exposed to an attacker, the attacker should be unable to compute future or past session keys.
- (ii) To achieve confidentiality and integrity of the data transmitted between the gateway and the cluster head, the proposed scheme should be designed such that it is secure against possible attacks on key establishment

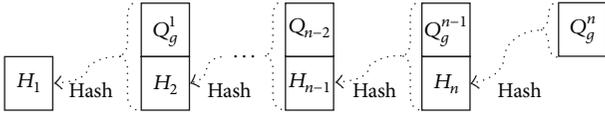
schemes such as node impersonation attacks, MITM attacks, and replay attacks.

- (iii) The security protocols alone cannot perfectly prevent node capture attacks; however, the proposed scheme should be designed to minimize the effects of such attacks [7]. That is, even if some sensor nodes are compromised by node capture attacks, it should have no effect on the communication with other normal nodes or the security of the entire network [9].
- (iv) Sensor nodes or cluster heads are battery-powered and their batteries should be replaced or charged once every few years of system operation [18]. This implies that the resources of cluster heads in our network model can be relatively richer than those of sensor nodes in other sensor networks; however, they are still limited. Therefore, the proposed scheme should be designed to consider the energy consumption and security. For this, the scheme will be designed to be efficient in terms of computation and communication costs.

3.4. Notations. Notations section shows the notations used in the remainder of the paper:

- (i) A pair of private and public keys for RSA signature [42] $(k_{g,pr}, k_{g,pub})$ is generated as follows: the scheme chooses two large primes p and q and computes $m = p \cdot q$. It chooses $e \in \{1, 2, \dots, \Phi(m) - 1\}$ which fulfills the notion that $gcd(e, \Phi(m)) = 1$, where $\Phi(m) = (p - 1)(q - 1)$. Then, it computes d which fulfills the notion that $d \cdot e \equiv 1 \pmod{\Phi(m)}$. Here, the public key $k_{g,pub}$ is m and e , and the private key $k_{g,pr}$ is d . In this paper, $SIG_{k_{g,pr}}(x)$ denotes the signing of a message x with the private key $k_{g,pr}$, and it means $x^d \pmod{\Phi(m)}$. $VER_{k_{g,pub}}(s, x)$ denotes the verifying of a message x and its signature s with the public key $k_{g,pub}$. It computes $x^* = s^e \pmod{\Phi(m)}$ and then compares x with x^* . If $x^* = x$, then the signature s is valid; otherwise, it is invalid.
- (ii) A pair of private and public keys for ECDH [21, 22] (d_j^i, Q_j^i) is generated as follows: the scheme chooses a large prime p and defines the elliptic curve E over Z_p ($p > 3$) which is the set of all pairs (x, y) which fulfills the notion that $y^2 \equiv x^3 + ax + b \pmod{p}$ and an imaginary point of infinity O , where $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$ ($a, b \in Z_p$). When P is a primitive element on the elliptic curve E and “ \times ” denotes an elliptic curve multiplication, the scheme chooses an integer d_j^i ($0 < d_j^i < n$, where n is the number of points on E) and computes $Q_j^i = d_j^i \times P$. Here, Q_j^i is another element on E .

3.5. Main Ideas. Symmetric key-based session key establishment schemes are efficient with regard to computation costs; however, one of their persisting issues is the sharing and updating of the symmetric key, that is, the session key



The gateway generates n public keys $Q_g^1, Q_g^2, \dots, Q_g^{n-1}, Q_g^n$

Then, it computes the following values in order:

$$\begin{aligned} H_n &= h(Q_g^n), \\ H_{n-1} &= h(Q_g^{n-1} \parallel H_n), \\ H_{n-2} &= h(Q_g^{n-2} \parallel H_{n-1}), \\ &\vdots \\ H_2 &= h(Q_g^2 \parallel H_3), \\ H_1 &= h(Q_g^1 \parallel H_2) \end{aligned}$$

FIGURE 2: Hash chain generation in the proposed scheme.

encryption key (KEK) by two nodes [15]. Moreover, if the KEK is a long-term key, it is futile to employ the session key because it can be exposed to an attacker. Meanwhile, another method to establish a session key is to generate the next session key using keying materials stored in the previous session, similar to Chen and Li's scheme [16]. However, in such schemes, if an attacker obtains keying materials in a session, the past or future session keys can be computed.

To meet the requirements described in Section 3.3, our proposed scheme is designed as follows:

- (i) The proposed scheme establishes a session key based on asymmetric key techniques in order to resist session key attacks and provide secrecy of past or future session keys. To take into account computation costs and energy consumption of cluster heads, the proposed scheme chooses an efficient key exchange technique, ECDH [21, 22], from asymmetric key techniques with the same security level.
- (ii) To resist node impersonation attacks, MITM attacks, and so forth, the proposed scheme should provide mutual authentication between the gateway and the cluster head and verify message integrity. To realize this, the proposed scheme is designed based on the hash chain containing the digests of public keys generated by the gateway, as shown in Figure 2. The gateway transmits one element of the hash chain to the cluster head for each session. Using the received hash chain element, the cluster head can authenticate the message sender and verify the integrity of the message. In our scheme, the cluster head can perform these processes efficiently in terms of computation and communication costs by computing only a single hash value.

4. Description of the Proposed Scheme

Our scheme is composed of the following three phases: predeployment phase, hash chain setup phase, and key establishment phase. The predeployment phase is performed before cluster heads are deployed in the field. After that, the

hash chain setup phase and the key establishment phase are performed. Each of these phases is described in detail from Section 4.1 to Section 4.3.

4.1. Predeployment Phase. Keying materials include information or algorithms required for key establishment. Not only in the proposed scheme but also in many secure protocols for WSN, keying materials are preloaded into nodes before they are deployed in the field [16, 17, 33, 55]. There are two reasons for preloading the keying materials. First, WSN is difficult to be equipped with secure channels such as mail compared to other common networks. Second, computation or communication costs can be reduced by skipping the initialization process after nodes are deployed in the target area. The predeployment phase of our scheme is as follows (steps (P-1) to (P-4)):

- (P-1) The scheme generates a pair of private and public keys for RSA signature [42] $(k_{g,pr}, k_{g,pub})$ as described in Section 3.4.
- (P-2) The two keys $(k_{g,pr}, k_{g,pub})$ are preloaded into GW. The private key $k_{g,pr}$ is stored only in GW and is not shared with other nodes. The public key $k_{g,pub}$ is preloaded into all cluster heads. In the hash chain setup phase described in Section 4.2, GW signs the first element of the hash chain using $k_{g,pr}$, and CH_j verifies the signature using $k_{g,pub}$.
- (P-3) The scheme generates a pair of private and public keys for ECDH [21, 22] (d_j^1, Q_j^1) as described in Section 3.4.
- (P-4) The two keys d_j^1 and Q_j^1 are preloaded into CH_j . d_j^1 is not shared with any cluster heads or sensor nodes other than CH_j . Q_j^1 are stored in the database of GW. In the hash chain setup phase described in Section 4.2, (d_j^1, Q_j^1) are used for CH_j to establish a session key based on ECDH [21, 22].

When this phase is completed, $(k_{g,pr}, k_{g,pub})$ and Q_j^1 are preloaded into GW. (d_j^1, Q_j^1) and $k_{g,pub}$ are preloaded into CH_j . The private key of GW, $k_{g,pr}$, and the private key of CH_j , d_j^1 , are secret parameters that cannot be shared with other nodes.

4.2. Hash Chain Setup Phase. In the hash chain setup phase, GW generates a hash chain to be used in the key establishment phase discussed in Section 4.3. If the number of elements in the hash chain is n , during n sessions, the hash chain setup phase is performed once only in the first session, and the key establishment phase is performed $(n-1)$ times in total, once in each session from the second to the n th session. In this phase, when GW transmits the first element of the hash chain, H_1 , with its signature to CH_j , CH_j verifies that H_1 is generated by GW and is not altered during the transmission using the signature. Figure 3 depicts the hash chain setup phase. The detailed process of this phase is as follows (steps (H-1) to (H-11)):

- (H-1) GW generates n private keys $(d_g^n, d_g^{n-1}, \dots, d_g^2, d_g^1)$ used for ECDH [21, 22] of n sessions. Then, GW

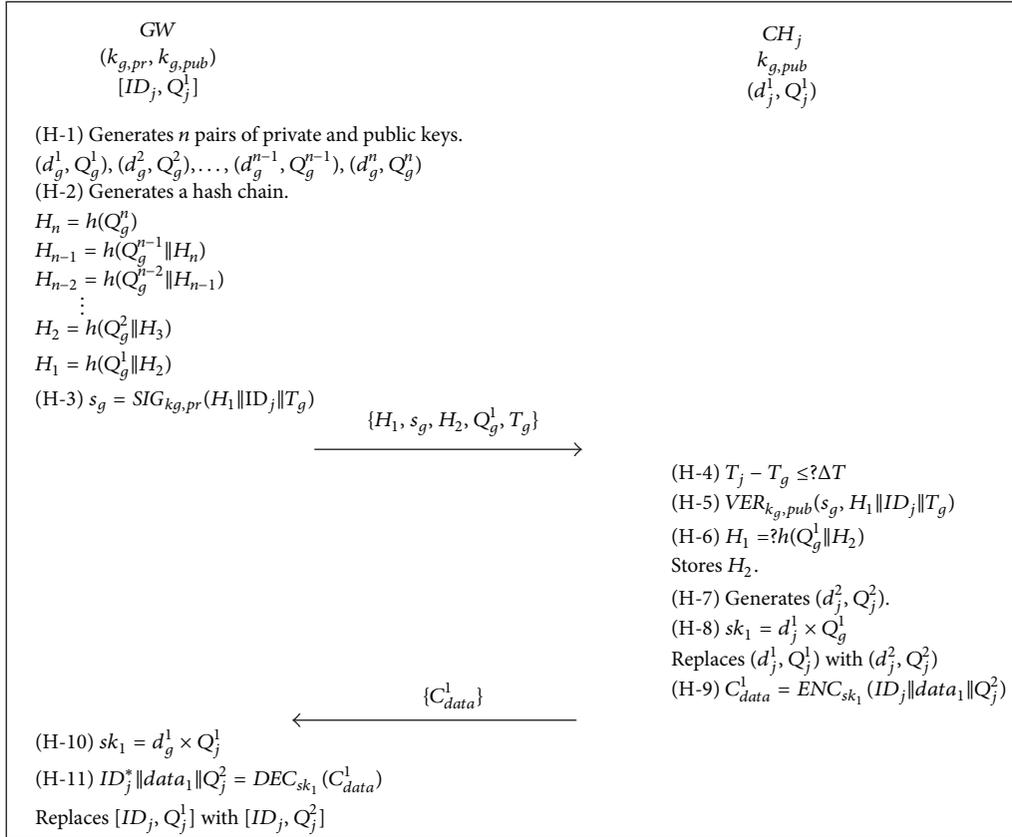


FIGURE 3: Hash chain setup phase of the proposed scheme.

computes n public keys $(Q_g^n, Q_g^{n-1}, \dots, Q_g^2, Q_g^1)$ corresponding to the private keys.

- (H-2) GW generates a single hash chain containing n elements, as shown in Figure 2, using the public keys $(Q_g^n, Q_g^{n-1}, \dots, Q_g^2, Q_g^1)$. First, GW computes the hashed value of Q_g^n ; that is, $H_n = h(Q_g^n)$, and it then computes the following values in order, $H_{n-1} = h(Q_g^{n-1} \| H_n)$, $H_{n-2} = h(Q_g^{n-2} \| H_{n-1})$, \dots , $H_2 = h(Q_g^2 \| H_3)$, $H_1 = h(Q_g^1 \| H_2)$:

$$\begin{aligned}
 H_n &= h(Q_g^n), \\
 H_{n-1} &= h(Q_g^{n-1} \| H_n), \\
 H_{n-2} &= h(Q_g^{n-2} \| H_{n-1}), \\
 &\vdots \\
 H_2 &= h(Q_g^2 \| H_3), \\
 H_1 &= h(Q_g^1 \| H_2).
 \end{aligned} \tag{1}$$

- (H-3) GW signs the first element of the hash chain (H_1) using its private key $k_{g,pr}$; that is, $s_g = SIG_{k_{g,pr}}(H_1 \|$

$ID_j \| T_g)$, where ID_j is the identity of CH_j , and T_g is the current timestamp of GW system. Then, GW transmits the message $\{H_1, s_g, H_2, Q_g^1, T_g\}$ to CH_j .

- (H-4) CH_j determines if $(T_j - T_g) \leq \Delta T$, where T_j is the current timestamp of CH_j system, and ΔT is the maximum permitted transmission delay time. If $(T_j - T_g) \leq \Delta T$, then the next step proceeds; otherwise, this phase is aborted.
- (H-5) CH_j verifies s_g using the preloaded public key $k_{g,pub}$; that is, CH_j performs $VER_{k_{g,pub}}(s_g, H_1 \| ID_j \| T_g)$. If the verification is successful, then the next step is performed.
- (H-6) CH_j compares the hashed value of Q_g^1 and H_2 with H_1 . In $H_1 = h(Q_g^1 \| H_2)$, it is very difficult to compute Q_g^1 or H_2 from H_1 because of the characteristics of the one-way hash function. Therefore, CH_j can verify that Q_g^1 and H_2 are generated by GW and not altered during the transmission by verifying $H_1 = h(Q_g^1 \| H_2)$. If the verification is obtained, then CH_j stores H_2 , and the next step will be performed.
- (H-7) CH_j generates a pair of private and public keys (d_j^2, Q_j^2) for ECDH [21, 22] in the next session.

- (H-8) CH_j computes the session key $sk_1 = d_j^1 \times Q_g^1$ for this first session. Then, CH_j replaces (d_j^1, Q_j^1) with (d_j^2, Q_j^2) .
- (H-9) CH_j encrypts $data_1$ and Q_j^2 using the session key sk_i ; that is, it performs $C_{data}^1 = ENC_{sk_1}(ID_j \parallel data_1 \parallel Q_j^2)$, where $data_1$ represents the data that CH_j wants to transmit to GW in this session. Then, CH_j transmits the message $\{C_{data}^1\}$ to GW .
- (H-10) Upon receiving the message from CH_j , GW finds $[ID_j, Q_j^1]$ from its database and then computes the session key $sk_1 = d_j^1 \times Q_g^1$.
- (H-11) GW decrypts C_{data}^1 using sk_1 . If the decryption is completed and the result values $(ID_j^* \parallel data_1 \parallel Q_j^2)$ are correct, it means that the message sender computed the same session key as sk_1 of GW . Therefore, GW can authenticate CH_j as the message sender and verify that the message is not altered during the transmission by checking the decryption result. GW will replace $[ID_j, Q_j^1]$ with $[ID_j, Q_j^2]$ in its database for the next session.

Our proposed scheme is more suitable for a network model wherein cluster heads are fixed and not selected from ordinary sensor nodes. In this case, the resources of cluster heads are usually richer than those of ordinary sensor nodes. Nevertheless, our scheme can still be applied to WSNs that perform random node deployment, clustering, or cluster head selection [51]. In the predeployment phase, our scheme preloads only three keys, that is, d_j^1 , Q_j^1 , and $k_{g,pub}$, to the cluster head CH_j . Even though nodes in WSNs have limited memory, they do not require additional memory to store these three keys. Therefore, when the cluster heads are replaced, the scheme preloads three keys to all cluster head candidates in the predeployment phase. Then, only the selected cluster heads perform the hash chain setup phase in the field.

4.3. Key Establishment Phase. After the hash chain setup phase generates a hash chain with n elements in the first session, the key establishment phase is performed for each session from the second session to the last, n th session. GW transmits a key establishment request message including one element of the hash chain to CH_j . Then, CH_j verifies the message, generates the session key based on ECDH [21, 22], encrypts the data using the key, and transmits it as the response message to GW . If all verifications in this phase are passed successfully, GW and CH_j can share the same session key and encrypt/decrypt the data using the key. Figure 4 shows the process of the key establishment phase as follows (steps (K-1) to (K-7)):

- (K-1) GW transmits the key establishment request message $\{Q_g^i, H_{i+1}\}$ to CH_j .
- (K-2) CH_j computes $h(Q_g^i \parallel H_{i+1})$ and verifies that $H_i = h(Q_g^i \parallel H_{i+1})$, where H_i is stored in the previous

session. If the verification is passed, then CH_j replaces H_i with H_{i+1} , and the next step is performed.

- (K-3) CH_j computes the session key $sk_i = d_j^i \times Q_g^i$.
- (K-4) CH_j generates its new private and public keys d_j^{i+1} and Q_j^{i+1} for the next $(i+1)$ th session and replaces (d_j^i, Q_j^i) with (d_j^{i+1}, Q_j^{i+1}) .
- (K-5) CH_j encrypts $data_i$ and Q_j^{i+1} using the session key sk_i ; that is, $C_{data}^i = ENC_{sk_i}(ID_j \parallel data_i \parallel Q_j^{i+1})$, where $data_i$ is the data that CH_j wants to transmit to GW in this session, and ID_j is the identity of CH_j . Then, it transmits the response message $\{C_{data}^i\}$ to GW .
- (K-6) When GW receives the message from CH_j , it finds $[ID_j, Q_j^i]$ from its database and computes the session key $sk_i = d_j^i \times Q_g^i$.
- (K-7) GW decrypts C_{data}^i using sk_i and determines whether or not the decryption result is correct. If the verification is passed successfully, GW can authenticate CH_j as the message sender and verify that the message was not altered during the transmission. GW replaces $[ID_j, Q_j^i]$ with $[ID_j, Q_j^{i+1}]$ in its database.

After GW exhausts the last element of the hash chain in the key establishment phase for the n th session, the scheme performs the hash chain setup phase for a set of n new sessions.

5. Security Analysis of the Proposed Scheme

The existing schemes are not able to protect past or future session keys if long-term keying materials are exposed to an attacker. The proposed scheme employs asymmetric key techniques to improve this problem, especially ECDH [21, 22], considering computation efficiency in cluster heads. Additionally, it employs the hash chain composed of digests of public keys generated by the gateway in order to resist MITM attacks or node impersonation attacks and to provide mutual authentication of two nodes and the verification of message integrity, considering computation and communication costs:

- (i) **Data Encryption Using a Session Key.** If the life cycle of WSN is much longer than the time required for an attacker to obtain cryptographic keys through cryptanalysis or hacking, it is better in terms of security to use the session key instead of a long-term key [15, 16, 56]. In the proposed scheme, CH_j or GW encrypts/decrypts the data using keys renewed in every session. Therefore, it is relatively more difficult for an attacker to guess cryptographic keys in our proposed scheme than in long-term key-based schemes because the information that he/she can obtain by eavesdropping messages is limited and valid in only one session. Furthermore, even when an attacker succeeds in guessing the cryptographic keys,

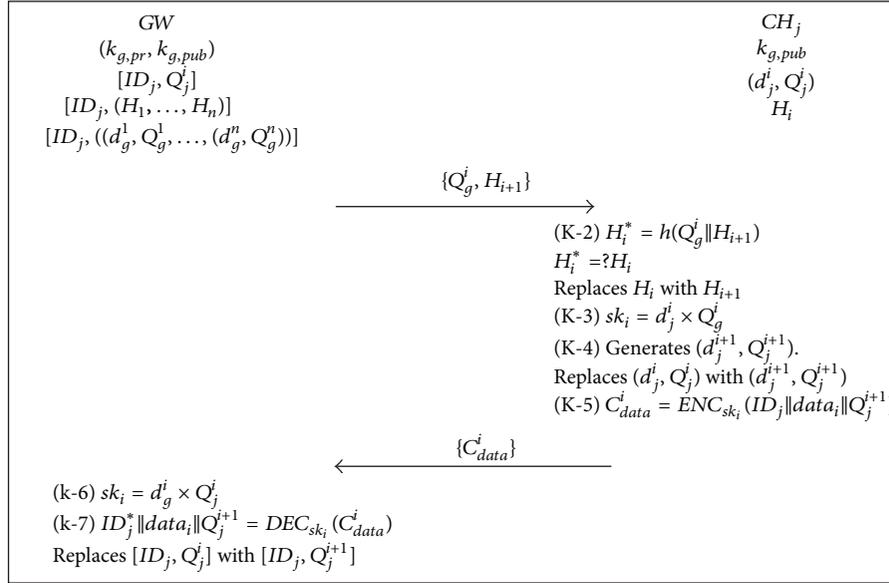


FIGURE 4: Key establishment phase of the proposed scheme.

the damage is significantly reduced because he/she can decrypt the data in only one session.

- (ii) *Session Key Attacks*. This attack is to obtain session keys by eavesdropping the messages exchanged between two nodes. In the key establishment phase of the proposed scheme, even if an attacker eavesdrops the key establishment request message $\{Q_g^i, H_{i+1}\}$ transmitted from GW to CH_j, he/she cannot compute the session key. Even if he/she can extract the public key of GW, $Q_g^i (= d_g^i \times P)$ from the message, it is very difficult to compute the private key of GW, d_g^i , because of the elliptic curved discrete logarithm problem (ECDLP) [21, 22]. Also, the private key of GW or CH_j, d_g^i or d_j^i , respectively, is not transmitted to other nodes in an insecure channel because it is a secure parameter. As a result, the attacker cannot decrypt or alter C_{data}^i because he/she cannot compute the session key $sk_i (= d_g^i \times Q_j^i = d_j^i \times Q_g^i = d_g^i \times d_j^i \times P)$ without knowing anything of the private keys of two nodes.
- (iii) *Mutual Authentication*. This means that one node should be authenticated as a legitimate node by another node with which it is in communication.

After GW generates a hash chain in the hash chain setup phase, it transmits the first element of the hash chain, H_1 , and its signature, s_g , to CH_j. CH_j verifies H_1 and s_g using the public key of GW, $k_{g,pub}$. If the verification is passed, CH_j can authenticate GW as the sender of H_1 . An attacker cannot impersonate GW because he/she cannot forge the signature s_g without knowing the private key of GW, $k_{g,pr}$.

Meanwhile, CH_j generates the public key Q_j^{i+1} for the $(i + 1)$ th session and transmits it to GW in the i th

session. Then, GW stores this Q_j^{i+1} in its database.

When GW receives the message $\{C_{data}^{i+1}\}$ from CH_j in the next $(i + 1)$ th session, it finds the public key of CH_j, Q_j^{i+1} , in its database and computes the session key $sk_{i+1} = d_g^{i+1} \times Q_j^{i+1}$. If GW can decrypt C_{data}^{i+1} using sk_{i+1} , that is, if the result value of decryption is a correct plaintext, then GW can authenticate CH_j as the sender of the message $\{C_{data}^{i+1}\}$. However, if GW fails to decrypt C_{data}^{i+1} or the result value of decryption is a meaningless random value, the session key sk_{i+1} is the wrong value. In this case, GW cannot be sure that the message sender is CH_j.

- (iv) *Node Impersonation Attacks*. Node impersonation attacks in WSN mean that an attacker communicates with a legitimate node by impersonating a gateway, a sensor node, or a cluster head. In the proposed scheme, if GW or CH_j receives a message, it performs the authentication process of the message sender. Therefore, an attacker cannot impersonate GW or CH_j.
- (v) *MITM Attacks*. This means that a malicious node decrypts or alters the messages transmitted between two legitimate nodes. The proposed scheme resists MITM attacks by the mutual authentication between GW and CH_j and the verification of the received messages integrity.

In the hash chain setup phase, when CH_j receives the message $\{H_1, s_g, H_2, Q_g^1, T_g\}$ from GW, it checks if H_1 is the first element of the hash chain generated by GW; that is, it verifies the signature of H_1 , s_g . If this verification is passed successfully, it means that the message sender is GW and that the value of H_1 is not altered during the transmission. Each element of

the hash chain, H_i , is the digest of Q_g^i and H_{i+1} , that is, $h(Q_g^i \parallel H_{i+1})$. Other nodes except GW are not able to compute Q_g^i or H_{i+1} from H_i because $h(\cdot)$ is a one-way hash function. Therefore, after CH_j completes one verification of H_1 and s_g , the following $(n-1)$ key establishment request messages can be successively verified using H_1 . That is, whenever CH_j receives the key establishment request message $\{Q_g^i \parallel H_{i+1}\}$, it compares H_i with the digest of Q_g^i and H_{i+1} to verify the message integrity. As a result, an attacker cannot alter the first element of the hash chain, H_1 , because he/she cannot forge the signature of GW , s_g . Also, he/she cannot alter the rest of the elements from H_2 to H_n because of the characteristics of the one-way hash function.

Meanwhile, the message $\{C_{data}^i\}$ transmitted from CH_j to GW is secure, unless the session key is exposed to the attacker because it is encrypted using the session key. Also, an attacker cannot alter this message without knowing the session key.

- (vi) *Secrecy of Past or Future Session Keys*. This means that an attacker should not be able to compute past or future session keys that were already used in the previous sessions or will be generated in the following sessions even when he/she obtains long-term keying materials. In the proposed scheme, GW and CH_j exchange their public keys, Q_g^i and Q_j^i , and generate the session key $sk_i (= d_g^i \times Q_j^i = d_j^i \times Q_g^i)$ based on ECDH [21, 22]. The parameters stored in CH_j are $k_{g,pub}$ and (d_j^i, Q_j^i) , where $k_{g,pub}$ is a long-term key, and (d_j^i, Q_j^i) are values renewed in each session. When they are exposed to an attacker, past or future session keys are protected as follows.

Even though an attacker obtains $k_{g,pub}$, he/she is not able to compute the private key $k_{g,pr}$ because of the integer factorization problem [42]. That is, because he/she cannot forge the signature of GW , s_g , he/she cannot alter Q_g^i transmitted from GW to CH_j .

d_j^i and Q_j^i are ephemeral keys renewed in each session. This means that CH_j replaces d_j^i and Q_j^i with d_j^{i+1} and Q_j^{i+1} , respectively, in the end of the i th session. Assume the worst scenario in which an attacker obtains the private key, d_j^{i+1} , between the i th and $(i+1)$ th sessions through some methods. Even in this case, the proposed scheme can protect the data securely transmitted before and after the $(i+1)$ th session. For example, if an attacker knows the private key of CH_j , d_j^{i+1} , and eavesdrops on the message of $\{Q_g^{i+1}, H_{i+2}\}$ transmitted from GW to CH_j in the $(i+1)$ th session, he/she can compute the session key $sk_{i+1} = d_j^{i+1} \times Q_g^{i+1}$ and decrypt the message C_{data}^{i+1} using sk_{i+1} . However, he/she cannot obtain any more information to restore the other session keys except

sk_{i+1} from the decryption result of C_{data}^{i+1} ($data_{i+1} \parallel Q_j^{i+2}$). As a result, the proposed scheme can assure the confidentiality of the data transmitted in all other sessions except the $(i+1)$ th session.

- (vii) *Replay Attacks*. This means an attacker stores messages transmitted on security protocols and transmits them again later. The proposed scheme resists replay attacks as follows:

In the proposed scheme, the message transmitted from GW to CH_j is the message $\{H_1, s_g, Q_g^1, H_2, T_g\}$ in the hash chain setup phase or the message $\{Q_g^i, H_{i+1}\}$ in the key establishment phase. The former contains the current timestamp of GW system, T_g , and is verified by the message receiver CH_j . The latter consists of the values that depend on the former because both are elements of a hash chain. Therefore, an attacker is not able to perform replay attacks using these messages.

The message $\{C_{data}^i\}$ is transmitted from CH_j to GW as a response to the hash chain setup request of GW or to the key establishment request of GW . Therefore, an attacker cannot use this message for replay attacks.

- (viii) *Node Capture Attacks*. This means that an attacker physically captures some nodes deployed in WSN and extracts secret parameters from them for other attacks. In the proposed scheme, each cluster head generates a unique session key. Therefore, the links between uncompromised nodes are still secure even when one cluster head is compromised by node capture attacks. For example, assume that an attacker captures CH_j and extracts d_j^i , Q_j^i , or $k_{g,pub}$ from it. The public key of GW , $k_{g,pub}$, is preloaded into not only CH_j but also all cluster heads. However, an attacker cannot use it for any other attacks because he/she is not able to compute the private key $k_{g,pr}$ from $k_{g,pub}$. Also, d_j^i and Q_j^i are not shared with other nodes except CH_j , so the attacker cannot obtain other session keys except a session key between CH_j and GW using these two values.

Table 1 shows the comparison of the security in the proposed scheme and that in other schemes that have design requirements similar to ours. Table 1 shows which scheme is secure against possible attacks in key establishment schemes or provides security functionalities. This table shows that the proposed scheme is clearly improved in terms of security. In Appendices A through D, we review and analyze the security of the schemes proposed by Chen and Li and Lee and Kim.

6. Energy Cost Analysis of the Proposed Scheme

In this section, we analyze the efficiency of the proposed scheme in terms of computation and communication costs. Computation costs refer to the number of times each operation is performed on a cluster head or a gateway system

TABLE 1: Security comparison of the proposed scheme.

Security attacks or features	Chen and Li's scheme [16]	Lee and Kim's scheme [17]	The proposed scheme
Data encryption using a session key	Partially	Partially	Yes
Session key attacks	Partially	Partially	Yes
Mutual authentication	No	No	Yes
Node impersonation attacks	Partially	No	Yes
MITM attacks	Partially	No	Yes
Secrecy of past session keys	Yes	Yes	Yes
Secrecy of future session keys	No	No	Yes
Replay attacks	Yes	No	Yes
Node capture attacks	Yes	No	Yes

Yes: the scheme resists the attacks or provides the functionality; No: the scheme does not resist the attacks or provide the functionality. Partially: "Yes" under the condition that the secret parameters stored in CH_j have not been exposed to an attacker.

TABLE 2: Computation cost analysis of the proposed scheme (during n sessions).

Phases	Nodes	Operations						
		1024-bit RSA		SHA1	64-bit AES		163-bit ECDH	
		Signing	Verification		Encryption	Decryption	Key generation	Key exchange
Hash chain setup (one time)	Gateway	1	0	n	0	1	n	1
	Cluster head	0	1	1	1	0	1	1
Key establishment ($n - 1$ times)	Gateway	0	0	0	0	$n - 1$	0	$n - 1$
	Cluster head	0	0	$n - 1$	$n - 1$	0	$n - 1$	$n - 1$

in a scheme. Communication costs refer to the number of messages exchanged between two nodes in a scheme. In a WSN, these two costs affect the energy consumption of nodes [28–30]. In addition, we compare the computation and communication costs of our scheme with those of existing schemes that are similar to ours in terms of design requirements or key establishment techniques.

We focus on the repeatedly performed phases, that is, the hash chain set up phase and the key establishment phase, and exclude the predeployment phase. The predeployment phase does not directly affect the efficiency because it is performed only prior to the deployment of sensor nodes and cluster heads in the field.

6.1. Computation Costs. Table 2 shows the kinds of operations and the number of times they are performed on a cluster head or gateway system in the proposed scheme during n sessions. In the proposed scheme, the hash chain setup phase is performed once, and the key establishment phase is performed ($n - 1$) times:

- (i) When the hash chain setup phase is performed once, the gateway performs one signing of RSA signature ((H-3) in Figure 3), data decryption ((H-11) in Figure 3), and ECDH key exchange ((H-10) in Figure 3) each. Moreover, the one-way hash operation ((H-2) in Figure 3) and ECDH key generation ((H-1) in Figure 3) are performed n times each.
- (ii) When the hash chain setup phase is performed once, the cluster head performs one verification of RSA signature ((H-5) in Figure 3), one-way hash operation

((H-6) in Figure 3), data encryption ((H-9) in Figure 3), ECDH key generation ((H-7) in Figure 3), and ECDH key exchange ((H-8) in Figure 3) each.

- (iii) When the key establishment phase is performed ($n - 1$) times, the gateway performs data decryption ((K-7) in Figure 4) and ECDH key exchange ((K-6) in Figure 4), ($n - 1$) times each.
- (iv) When the key establishment phase is performed ($n - 1$) times, the gateway performs one-way hash operation ((K-2) in Figure 4), data encryption ((K-5) in Figure 4), ECDH key exchange ((K-3) in Figure 4), and ECDH key generation ((K-4) in Figure 4) ($n - 1$) times each.

Table 3 also shows the types of operations and the number of times they are performed on a cluster head or gateway system in Lee and Kim's scheme [17] during n sessions. In terms of design requirements and key establishment techniques, our scheme is similar to that of Lee and Kim.

To analyze the energy costs of the proposed scheme, we define several notations as follows:

- (i) RSA_s : the energy cost of performing a signing of 1024-bit RSA signature.
- (ii) RSA_v : the energy cost of performing a verification of 1024-bit RSA signature.
- (iii) H : the energy cost of performing a SHA1.
- (iv) E : the energy cost of performing a 64-bit AES encryption.

TABLE 3: Computation cost analysis of Lee and Kim's scheme [17] (during n sessions).

Phases	Nodes	Operations				
		SHA1	64-bit AES		163-bit ECDH	
			Encryption	Decryption	Key generation	Key exchange
Procedure 2	Gateway	n	n	n	n	n
(n times)	Cluster head	0	n	n	0	n

TABLE 4: Energy costs comparison of the proposed scheme (during n sessions).

Schemes	Nodes	Total energy costs	Energy cost comparison* (mJ)
The proposed scheme	Gateway	$RSA_s + nH + nD + nEC_g + nEC_e$	$546.50 + 440.20n + 0.00121l$
	Cluster head	$RSA_v + nH + nE + nEC_g + nEC_e$	$15.97 + 440.20n + 0.00121l$
Lee and Kim's scheme [17]	Gateway	$nH + nE + nD + nDH_g + nDH_e$	$1922.46n + 0.00242l$
	Cluster head	$nE + nD + nDH_e$	$1046.50n + 0.00242l$

*Energy cost comparison based on the experimental results in [28]. We assume that the cluster head transmits the total of l byte data to the gateway during n sessions.

TABLE 5: Energy costs of cryptographic algorithms [28].

Cryptographic algorithms	Energy costs*
Signing of 1024-bit RSA signature	546.50 mJ
Verification of 1024-bit RSA signature	15.97 mJ
SHA1	0.76 μ J/byte
64-bit AES encryption	1.21 μ J/byte
64-bit AES decryption	1.21 μ J/byte
1024-bit DHKE key generation	875.96 mJ
1024-bit DHKE key exchange	1046.50 mJ
163-bit ECDH key generation	276.70 mJ
163-bit ECDH key exchange	163.50 mJ

*These values are the experimental results in [28], in which the cryptographic algorithms were developed on a Compaq iPAQ H3670 equipped with a 206 MHz Intel SA-1110 StrongARM processor and 64 MB RAM.

- (v) D : the energy cost of performing a 64-bit AES decryption.
- (vi) DH_g : the energy cost of performing a 1024-bit DHKE key generation.
- (vii) DH_e : the energy cost of performing a 1024-bit DHKE key exchange.
- (viii) EC_g : the energy cost of performing a 163-bit ECDH key generation.
- (ix) EC_e : the energy cost of performing a 163-bit ECDH key exchange.

Potlapally et al. described the energy consumption of well-known cryptographic algorithms and security protocols using the experimentation results in [28] (Table 5).

Table 4 shows the energy costs of our scheme and Lee and Kim's scheme based on computation cost analysis of the two schemes and Potlapally et al.'s experimentation results. Assume that the cluster head transmits the total of l byte data

to the gateway during n sessions. To perform the proposed scheme, the gateway uses about $546.50 + 440.20n + 0.00121l$ mJ ($= RSA_s + nH + nD + nEC_g + nEC_e$), and the cluster head uses about $15.97 + 440.20n + 0.00121l$ mJ ($= RSA_v + nH + nE + nEC_g + nEC_e$). Under the same conditions, to perform Lee and Kim's scheme, the gateway uses about $1922.46n + 0.00242l$ mJ ($= nH + nE + nD + nDH_g + nDH_e$), and the cluster head uses about $1046.50n + 0.00242l$ mJ ($= nE + nD + nDH_e$).

Given that the cluster heads are battery-powered, we have to focus more on the energy costs in the cluster head than in the gateway. Table 4 shows that the energy cost of the cluster head in our scheme is smaller than that in Lee and Kim's scheme ($15.97 + 440.20n + 0.00121l$ mJ $<$ $1046.50n + 0.00242l$ mJ). Therefore, in terms of energy consumption based on computation costs, the proposed scheme is more efficient than Lee and Kim's scheme. This can be attributed to the difference in the energy costs of the two key exchange algorithms, that is, 163-bit ECDH and 1024-bit DHKE; 163-bit ECDH and 1024-bit DHKE schemes have the same security level, but the energy consumption of the former is only one-quarter that of the latter ($276.70 + 163.50$ mJ $<$ $875.96 + 1046.5$ mJ in Table 5) [28]. Meanwhile, the verification of RSA signature in the proposed scheme does not significantly affect the total energy costs of CH_j , even though the scheme is an asymmetric key technique. This is because, for n sessions, the operation is performed only once in the hash chain setup phase and the verification is performed more efficiently than the signing in RSA signature (15.97 mJ $<$ 546.50 mJ in Table 5) [15, 28].

6.2. Communication Costs. Communication costs as well as computation costs affect the energy costs of cluster heads [29, 30]. In our scheme, the messages $\{H_1, s_g, H_2, Q_g^1, T_g\}$ and $\{C_{data}^1\}$ are exchanged between the cluster head and the gateway in the hash chain setup phase, while the messages $\{Q_g^i, H_{i+1}\}$ and $\{C_{data}^i\}$ are exchanged in the key establishment

phase. That is, in the proposed scheme, two message exchanges are needed between the two nodes during one session, which is same as the number of messages in Lee and Kim's scheme and less than the three messages in Chen and Li's scheme. The proposed scheme minimizes the number of messages, considering that it provides all functions of session key establishment, node authentication, and data encryption.

7. Conclusion

In this paper, we propose a session key establishment scheme for clustered sensor networks based on ECDH [21, 22] and hash chain [23–27]. Our proposed scheme is secure against the possible attacks in key establishment schemes of WSN such as session key attacks, node impersonation attacks, MITM attacks, replay attacks, and node capture attacks. The scheme eliminates vulnerabilities of existing session key establishment schemes for WSN and provides secrecy of past or future session keys. Additionally, the proposed scheme is designed to minimize the number of messages for efficiency in terms of communication costs. Also, it is more efficient in terms of computation costs compared to other schemes based on asymmetric key techniques. Because of the efficiency of the proposed scheme, the cluster head requires less energy to operate.

Appendix

A. Review of Chen and Li's Scheme

In Chen and Li's scheme [16], two secret parameters a_j and a_{j-1} are preloaded in CH_j before deploying nodes to the field. GW knows every secret parameter of cluster heads and sensor nodes in the network. After the nodes are deployed to the field, CH_j performs the following (CL-1) to (CL-10) in order to transmit the data to GW (in [16], Chen and Li's scheme is composed of two parts of data transmission from the sensor node to the cluster head and from the cluster head to the gateway. Section II reviews only the latter considering our topic). In the first session, all the steps of (CL-1) to (CL-10) are performed. After the second session, the steps except (CL-1) and (CL-3) are repeated in each session. Figure 5 shows session key establishment between the gateway and the cluster head in Chen and Li's scheme:

- (CL-1) CH_j computes $sk_1 = h(a_j \parallel a_{j-1})$ using its secret parameters a_j and a_{j-1} . CH_j will use the result value sk_1 as the session key to communicate with GW .
- (CL-2) CH_j transmits the message $\{C_1, ID_j\}$ to GW to request the keys to decrypt the data received from the sensor nodes. Here, $C_1 = ENC_{sk_1}(sensor_list \parallel ID_j \parallel RN_j)$, where $sensor_list$ is the list of sensor nodes that sent the data, ID_j is the identity of CH_j , and RN_j is a random number generated by CH_j .
- (CL-3) When GW receives the request message $\{C_1, ID_j\}$, it finds the secret parameters a_j and a_{j-1} of CH_j in its database and computes the session key sk_1 .
- (CL-4) GW decrypts C_1 using sk_1 ; that is, $sensor_list \parallel ID_j \parallel RN_j = DEC_{sk_1}(C_1)$.

- (CL-5) GW computes $C_g = ENC_{sk_1}(ID_g \parallel key_list \parallel RN_j \parallel RN_g)$, where ID_g is the identity of GW , key_list is the decryption key list in regard to $sensor_list$, and RN_g is a random number generated by GW . Then, it returns the response message $\{C_g, ID_g\}$ to CH_j .
- (CL-6) When CH_j receives the response message $\{C_g, ID_g\}$ from GW , it decrypts the messages using key sk_1 ; that is, $ID_g \parallel key_list \parallel RN_j^* \parallel RN_g = DEC_{sk_1}(C_g)$. Then, CH_j compares RN_j with RN_j^* , where RN_j is a random number generated in step (CL-2), and RN_j^* is a part of the decrypted results ($ID_g \parallel key_list \parallel RN_j^* \parallel RN_g$). If the verification is passed, the next step is performed.
- (CL-7) CH_j decrypts each data received from sensor nodes using the decryption keys in the key_list . Then, CH_j derives $data_1$ from the decrypted results to transmit them to GW .
- (CL-8) CH_j encrypts $data_1$ using session key sk_1 ; that is, $C_{data}^1 = ENC_{sk_1}(data_1 \parallel RN_g \parallel ID_j)$. Then, it transmits the message $\{C_{data}^1, ID_j\}$ to GW .
- (CL-9) GW decrypts C_{data}^1 using sk_1 when it receives the message $\{C_{data}^1, ID_j\}$; that is, $data_1 \parallel RN_g \parallel ID_j = DEC_{sk_1}(C_{data}^1)$. Then, GW compares RN_g^* with RN_g . If the verification is passed, GW can use $data_1$.
- (CL-10) CH_j and GW separately compute the next session key $sk_2 = h(sk_1 \parallel a_j)$ and replace secret parameters a_j and a_{j-1} with sk_1 and a_j .

B. Cryptanalysis of Chen and Li's Scheme

In the i th session of Chen and Li's scheme, CH_j or GW encrypts the message using the session key sk_i and then transmits it to the other node. Before the end of the session, two nodes separately compute the new session key $sk_{i+1} = h(sk_i \parallel sk_{i-1})$ for the next session and replace secret parameters sk_i and sk_{i-1} with sk_{i+1} and sk_i , respectively. The following analyzes the security of their scheme against possible attacks in key establishment schemes for WSN:

- (i) Session key attacks and MITM attacks: session key attacks mean that an attacker obtains session keys by eavesdropping the messages exchanged between two nodes. MITM attacks refer to attacks in which an attacker eavesdrops or alters the messages transmitted between two legitimate nodes. In Chen and Li's scheme, an attacker cannot compute the session key sk_{i+1} ($= h(sk_i \parallel sk_{i-1})$) using only the transmitted messages without knowing the secret parameters sk_i and sk_{i-1} , stored in CH_j .
- (ii) Node impersonation attacks: this attack means an attacker impersonates a gateway or a cluster head to communicate with legitimate nodes. Chen and Li's scheme does not provide any node authentication process. However, an attacker cannot impersonate GW or CH_j without knowing the secret parameters

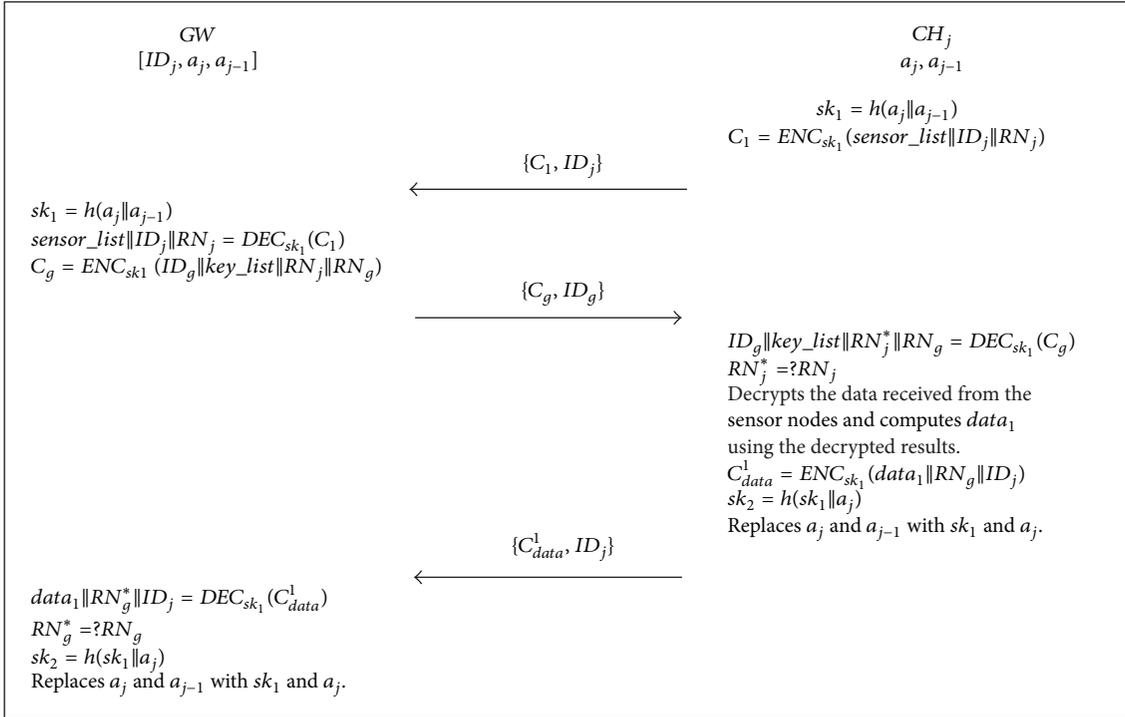


FIGURE 5: Session key establishment between the gateway and the cluster head in Chen and Li's scheme (redrawn from [16]).

such as (a_j, a_{j-1}) or (sk_i, sk_{i-1}) because the secret parameters are unique values for only CH_j and GW , and the two nodes encrypt/decrypt messages using the session keys derived from them.

- (iii) Secrecy of past session keys: this means that an attacker should be unable to compute the past session keys already used in the previous sessions even when the long-term keying materials are exposed to the attacker. In Chen and Li's scheme, even if an attacker obtains sk_i and sk_{i-1} from CH_j because of the characteristics of the one-way hash function, he/she cannot recover the past session keys used in the previous sessions, that is, from the first session to the $(i - 1)$ th session [16].
- (iv) Secrecy of future session key: this means that an attacker should be unable to compute the future session keys to be generated subsequent to the current session even when the long-term keying materials are exposed to the attacker. If an attacker obtains sk_i and sk_{i-1} of CH_j , he/she can compute the future session keys to be generated in the i th and the following sessions. That is, their scheme cannot assure the confidentiality or integrity of all messages transmitted, since the i th session until the GW system determines that the secret parameters of CH_j are compromised.
- (v) Node capture attacks: this means that an attacker captures sensor nodes or cluster heads deployed in the target field and uses secret parameters extracted from them for other attacks. Because sk_i and sk_{i-1} are derived from unique values a_j and a_{j-1} for CH_j ,

the link between uncompromised nodes is still secure even when an attacker captures CH_j and extracts the secret parameters sk_i and sk_{i-1} from it.

C. Review of Lee and Kim's Scheme

Lee and Kim proposed a session key establishment scheme based on Diffie-Hellman key exchange (DHKE) technique [46] for secure communication between the gateway and the cluster head [17]. Before nodes are deployed in the field, a large prime for modulus operations, m , and a primitive element, q ($q \in Z_m^*$), are stored in each cluster head and the gateway. After cluster heads are deployed in the field, procedure 1 is performed for the first session and procedure 2 is performed for the second and subsequent sessions. Figure 6 illustrates both procedures. In procedure 1, the following steps ((LK-1) to (LK-5)) are performed for key setup:

- (LK-1) The cluster head CH_j computes the hashed value of m , $k = h(m)$. Then, it generates a random number RN_j and encrypts RN_j and its identity ID_j using the key k ; that is, $C_j = ENC_k(ID_j \| RN_j)$. Then, CH_j transmits the key setup request message $\{C_j, ID_j\}$ to GW .
- (LK-2) Upon receiving the message from CH_j , GW computes the key $k = h(m)$ and then decrypts C_j using the key k ; that is, $ID_j \| RN_j = DEC_k(C_j)$. GW generates a random number RN_g and computes the session key $sk_1 = q^{RN_g \cdot RN_j} \text{ mod } m$.
- (LK-3) GW computes $k_j = q^{RN_g} \text{ mod } m$ and encrypts the result k_j and its identity ID_g using the key k ; that is,

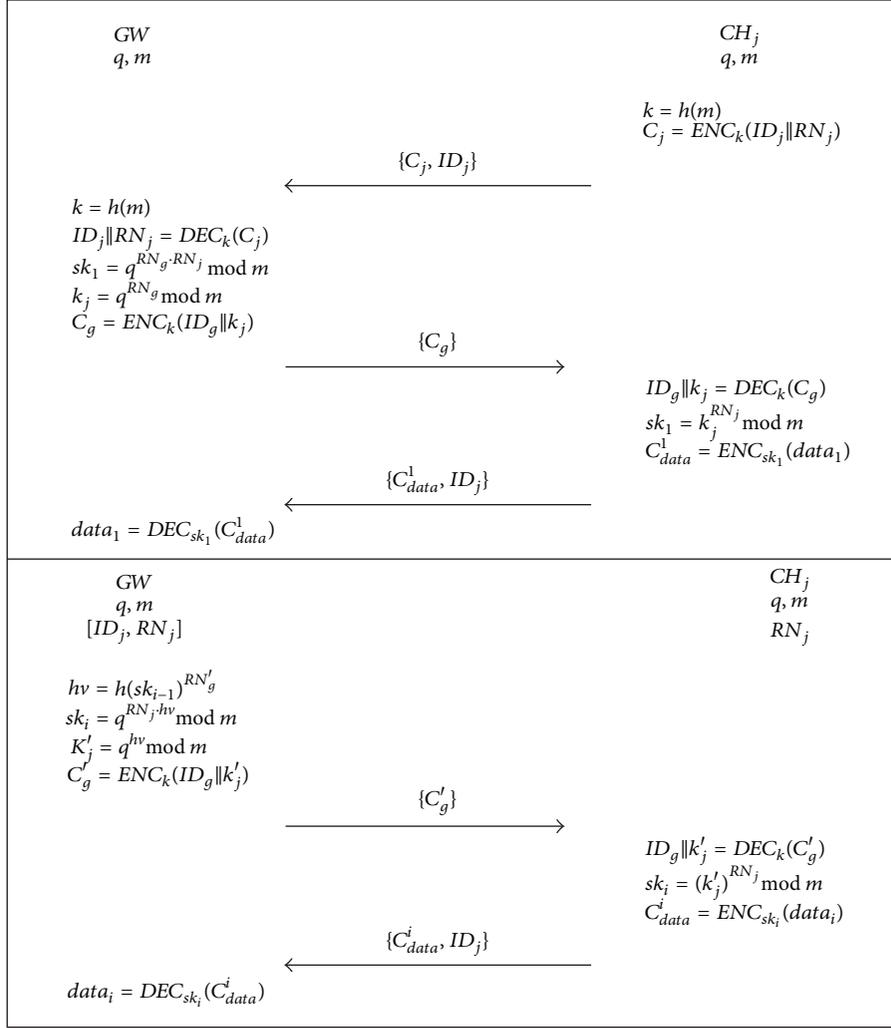


FIGURE 6: Procedures 1 and 2 in Lee and Kim's scheme (redrawn from [17]).

$C_g = ENC_k(ID_g \| k_j)$. Then, it returns the message $\{C_g\}$ to CH_j .

(LK-4) Upon receiving the message $\{C_g\}$ from GW , CH_j decrypts C_g using the key k . Then, CH_j computes $sk_1 = k_j^{RN_j} \bmod m$.

(LK-5) CH_j encrypts $data_1$ using the session key sk_1 and transmits the result to GW . Then, GW decrypts the message to obtain $data_1$.

Procedure 2 comprises the following steps ((LK-6) to (LK-10)) and is performed for CH_j to transmit data to GW for the second and subsequent sessions.

(LK-6) GW generates a new random number RN'_g and computes $hv = h(sk_{i-1})^{RN'_g}$, where sk_{i-1} is the previous session key shared with CH_j .

(LK-7) GW computes a new session key $sk_i = q^{RN_j \cdot hv} \bmod m$, where RN_j is the random number received from CH_j in procedure 1.

(LK-8) GW computes $k'_j = q^{hv} \bmod m$ and encrypts the result k'_j and ID_g using the key k ; that is, $C'_g = ENC_k(ID_g \| k'_j)$. Then, it sends the message $\{C'_g\}$ to CH_j .

(LK-9) Upon receiving the data request message $\{C'_g\}$ from GW , CH_j decrypts C'_g using the key k . Then, CH_j computes a new session key $sk_i = (k'_j)^{RN_j} \bmod m$.

(LK-10) CH_j encrypts $data_i$ using the session key sk_i and then transmits the result C_{data}^i to GW . Then, GW decrypts C_{data}^i using the key sk_i to obtain $data_i$.

D. Cryptanalysis of Lee and Kim's Scheme

In procedure 1 of Lee and Kim's scheme, CH_j and GW exchange their random numbers RN_j and RN_g in order to share the first session key $sk_1 (= q^{RN_g \cdot RN_j} \bmod m)$. In procedure 2, they compute the session key $sk_i = q^{hv \cdot RN_j} \bmod m$

for the second and subsequent sessions, where RN'_g is a new random number of GW , and $hv = h(sk_{i-1})^{RN'_g}$. However, q and m are likely to be exposed to attackers because they are shared by not only CH_j and GW but also all cluster heads in the network, and they are long-term parameters used throughout the lifetime of the network. If q and m are exposed to an attacker, this scheme can be vulnerable to node impersonation attacks and MITM attacks and cannot assure the secrecy of future session keys. The following analyzes the security of Lee and Kim's scheme against possible attacks in key establishment schemes for WSN:

- (i) Session key attacks: in this scheme, all the messages exchanged between GW and CH_j are encrypted with the key k . Therefore, an attacker cannot restore session keys using only these messages without knowing secret parameters q and m .
- (ii) Node impersonation attacks and MITM attacks: upon receiving a message, GW or CH_j only determines whether the message is encrypted using the key k without the message sender authentication process. Even if an attacker obtains the value of m from other cluster heads excluding CH_j , he/she can compute the key $k = h(m)$ and transmit data request messages to CH_j just like GW or can alter the messages.
- (iii) Secrecy of future session keys: RN_j stored in CH_j is a random number but is a long-term parameter that is not updated. If an attacker obtains RN_j after the i th session ended, he/she can compute future session keys between GW and CH_j in the following sessions. In this case, confidentiality and integrity of the data encrypted using these session keys cannot be guaranteed.
- (iv) Replay attacks: this means that an attacker resends the messages transmitted on security protocols. In their scheme, CH_j neither checks random numbers or timestamps nor authenticates GW in order to resist replay attacks using the data request messages from GW . Therefore, an attacker can repeatedly broadcast one of the data request messages to cluster heads to cause DoS attacks in WSN.
- (v) Node capture attacks: in their scheme, if an attacker extracts the values of q , m , and RN_j from a cluster head in the target area, he/she can compromise even links with other cluster heads. This vulnerability causes more serious problems when new cluster heads are added for expansion or changes in the network. When a new cluster head starts procedure 1 for key setup, GW and the new cluster head exchange their random numbers after encrypting them using the key k . If an attacker already knows the key k through node capture attacks against existing cluster heads, he/she can perform node impersonation attacks, MITM attacks, and so forth by eavesdropping the exchanged messages or altering the random numbers.

Notations

GW :	Gateway node
CH_j :	j th cluster head
ID_g :	Identity of GW
ID_j :	Identity of CH_j
$k_{g,pr}, k_{g,pub}$:	Private and public keys of GW for RSA signature scheme [42]
d_j^i, Q_j^i :	Private and public keys of CH_j for elliptic curve Diffie-Hellman key exchange (ECDH) [21, 22]
$SIG_k(x)$:	Signing of a message x with a key k in RSA signature scheme [42]
$VER_k(s, x)$:	Verification of a message x and its signature s with a key k in RSA signature scheme [42]
$ENC_k(m)$:	Encryption of a plaintext m using a symmetric key k
$DEC_k(c)$:	Decryption of a ciphertext m using a symmetric key k
$h(\cdot)$:	One-way hash function
RN_g or RN_j :	Random number generated by GW or CH_j
$data_i$:	Data that CH_j transmits to GW in the i th session
sk_i :	Session key for the i th session
\parallel :	Concatenation operation
$\leq?$ or $=?$:	Verification operation
T_g or T_j :	Current timestamp of GW or CH_j
Δt :	The maximum of transmission delay time permitted.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work was supported by Institute for Information & Communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (no. R0126-15-1111, The Development of Risk-based Authentication Access Control Platform and Compliance Technique for Cloud Security).

References

- [1] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, 2008.
- [2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, 2002.
- [3] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Pauthkey: a pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications," *International Journal of Distributed Sensor Networks*, vol. 2014, Article ID 357430, 14 pages, 2014.
- [4] M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks,'" *Sensors*, vol. 10, no. 3, pp. 2450–2459, 2010.

- [5] D. Nyang and M.-K. Lee, "Improvement of das's two-factor authentication protocol in wireless sensor networks," *IACR Cryptology ePrint Archive*, vol. 2009, p. 631, 2009.
- [6] J. Nam, M. Kim, J. Paik, Y. Lee, and D. Won, "A provably-secure ECC-based authentication scheme for wireless sensor networks," *Sensors*, vol. 14, no. 11, pp. 21023–21044, 2014.
- [7] J. Kim, D. Lee, W. Jeon, Y. Lee, and D. Won, "Security analysis and improvements of two-factor mutual authentication with key agreement in wireless sensor networks," *Sensors*, vol. 14, no. 4, pp. 6443–6462, 2014.
- [8] W. Jeon, J. Kim, J. Nam, Y. Lee, and D. Won, "An enhanced secure authentication scheme with anonymity for wireless environments," *IEICE Transactions on Communications*, vol. 95, no. 7, pp. 2505–2508, 2012.
- [9] S. A. Camtepe and B. Yener, "Key distribution mechanisms for wireless sensor networks: a survey," Tech. Rep., Rensselaer Polytechnic Institute, Troy, NY, USA, 2005.
- [10] Y. Lee, S. Kim, and D. Won, "Enhancement of two-factor authenticated key exchange protocols in public wireless LANs," *Computers & Electrical Engineering*, vol. 36, no. 1, pp. 213–223, 2010.
- [11] B. Lai, S. Kim, and I. Verbauwhede, "Scalable session key construction protocol for wireless sensor networks," in *Proceedings of the IEEE Workshop on Large Scale Real-Time and Embedded Systems (LARTES '02)*, p. 7, December 2002.
- [12] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pp. 41–47, Washington, DC, USA, November 2002.
- [13] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys and Tutorials*, vol. 8, no. 2, pp. 2–23, 2007.
- [14] M. Eltoweissy, M. Moharrum, and R. Mukkamala, "Dynamic key management in sensor networks," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 122–130, 2006.
- [15] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*, Springer Science & Business Media, 2009.
- [16] C.-L. Chen and C.-T. Li, "Dynamic session-key generation for wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2008, no. 1, Article ID 691571, 2008.
- [17] S. Lee and K. Kim, "Key renewal scheme with sensor authentication under clustered wireless sensor networks," *Electronics Letters*, vol. 51, no. 4, pp. 368–369, 2015.
- [18] G. Zhao, "Wireless sensor networks for industrial process monitoring and control: a survey," *Network Protocols and Algorithms*, vol. 3, no. 1, pp. 46–63, 2011.
- [19] O. K. Sahingoz, "Large scale wireless sensor networks with multi-level dynamic key management scheme," *Journal of Systems Architecture*, vol. 59, no. 9, pp. 801–807, 2013.
- [20] B. Premamayudu, K. V. Rao, and P. S. Varma, "A novel pairwise key establishment and management in hierarchical wireless sensor networks (HWSN) using matrix," in *ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India—Vol I*, pp. 425–432, Springer, 2014.
- [21] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.
- [22] V. S. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology—CRYPTO '85 Proceedings*, vol. 218 of *Lecture Notes in Computer Science*, pp. 417–426, Springer, 1986.
- [23] J. Deng, R. Han, and S. Mishra, "Secure code distribution in dynamically programmable wireless sensor networks," in *Proceedings of the 5th International Conference on Information Processing in Sensor Networks (IPSN '06)*, pp. 292–300, ACM, Nashville, Tenn, USA, April 2006.
- [24] P. K. Dutta, J. W. Hui, D. C. Chu, and D. E. Culler, "Securing the deluge network programming system," in *Proceedings of the 5th International Conference on Information Processing in Sensor Networks (IPSN '06)*, pp. 326–333, Nashville, Tenn, USA, April 2006.
- [25] S. Lee, H. Kim, and K. Chung, "Hash-based secure sensor network programming method without public key cryptography," in *Proceedings of the Workshop on World-Sensor-Web (WSW '06)*, Boulder, Colo, USA, 2006.
- [26] P. E. Lanigan, R. Gandhi, and P. Narasimhan, "Sluice: secure dissemination of code updates in sensor networks," in *Proceedings of the 26th IEEE International Conference on Distributed Computing Systems (ICDCS '06)*, 53 pages, IEEE, July 2006.
- [27] M. L. Das and A. Joshi, "Dynamic program update in wireless sensor networks using orthogonality principle," *IEEE Communications Letters*, vol. 12, no. 6, pp. 471–473, 2008.
- [28] N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," *IEEE Transactions on Mobile Computing*, vol. 5, no. 2, pp. 128–143, 2006.
- [29] W. Wang, S. Zhang, G. Duan, and H. Song, "Security in wireless sensor networks," in *Wireless Network Security*, pp. 129–177, Springer, Berlin, Germany, 2013.
- [30] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: a survey," in *Security in Distributed, Grid, Mobile, and Pervasive Computing*, Y. Xiao, Ed., vol. 1, p. 367, 2007.
- [31] G. Wang, S. Kim, D. Kang, D. Choi, and G. Cho, "Lightweight key renewals for clustered sensor networks," *Journal of Networks*, vol. 5, no. 3, pp. 300–312, 2010.
- [32] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proceedings of IEEE Symposium on Security and Privacy*, pp. 197–213, Berkeley, Calif, USA, May 2003.
- [33] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," *ACM Transactions on Information and System Security*, vol. 8, no. 2, pp. 228–258, 2005.
- [34] D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," *ACM Transactions on Information and System Security*, vol. 8, no. 1, pp. 41–77, 2005.
- [35] R. Blom, "An optimal class of symmetric key generation systems," in *Advances in Cryptology*, pp. 335–338, Springer, Berlin, Germany, 1985.
- [36] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," in *Advances in Cryptology—CRYPTO '92: 12th Annual International Cryptology Conference Santa Barbara, California, USA August 16–20, 1992 Proceedings*, vol. 740 of *Lecture Notes in Computer Science*, pp. 471–486, Springer, Berlin, Germany, 1993.
- [37] M. Eltoweissy, A. Wadaa, S. Olariu, and L. Wilson, "Group key management scheme for large-scale sensor networks," *Ad Hoc Networks*, vol. 3, no. 5, pp. 668–688, 2005.
- [38] M. F. Younis, K. Ghumman, and M. Eltoweissy, "Location-aware combinatorial key management scheme for clustered

- sensor networks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 17, no. 8, pp. 865–882, 2006.
- [39] M. Eltoweissy, M. H. Heydari, L. Morales, and I. H. Sudborough, “Combinatorial optimization of group key management,” *Journal of Network and Systems Management*, vol. 12, no. 1, pp. 33–50, 2004.
- [40] C.-L. Chen and I.-H. Lin, “Location-aware dynamic session-key management for grid-based wireless sensor networks,” *Sensors*, vol. 10, no. 8, pp. 7347–7370, 2010.
- [41] M. H. Eldefrawy, M. K. Khan, and K. Alghathbar, “A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography,” in *Proceedings of the International Conference on Anti-Counterfeiting, Security and Identification (ASID '10)*, pp. 1–6, IEEE, Chengdu, China, July 2010.
- [42] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
- [43] W. Zhang, S. Zhu, and G. Cao, “Predistribution and local collaboration-based group rekeying for wireless sensor networks,” *Ad Hoc Networks*, vol. 7, no. 6, pp. 1229–1242, 2009.
- [44] S. Guo and A.-N. Shen, “A compromise-resilient pair-wise rekeying protocol in hierarchical wireless sensor networks,” *Computer Systems Science and Engineering*, vol. 25, no. 6, pp. 397–405, 2010.
- [45] Y. Zhang, C. Wu, J. Cao, and X. Li, “A secret sharing-based key management in hierarchical wireless sensor network,” *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 406061, 7 pages, 2013.
- [46] W. Diffie and M. E. Hellman, “New directions in cryptography,” *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.
- [47] J. Nam, K.-K. R. Choo, S. Han, M. Kim, J. Paik, and D. Won, “Efficient and anonymous two-factor user authentication in wireless sensor networks: achieving user anonymity with lightweight sensor computation,” *PLoS ONE*, vol. 10, no. 4, Article ID e0116709, 2015.
- [48] M. L. Das, “Two-factor user authentication in wireless sensor networks,” *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1086–1090, 2009.
- [49] C.-T. Li, C.-Y. Weng, and C.-C. Lee, “An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks,” *Sensors*, vol. 13, no. 8, pp. 9589–9603, 2013.
- [50] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, and D. Won, “Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography,” *Sensors*, vol. 14, no. 6, pp. 10081–10106, 2014.
- [51] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy-efficient communication protocol for wireless microsensor networks,” in *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences (HICSS '33)*, p. 10, January 2000.
- [52] J. Rehana, “Security of wireless sensor network,” Tech. Rep. TKK-CSE-B5, Helsinki University of Technology, Helsinki, Finland, 2009.
- [53] J. Zhang and V. Varadharajan, “Wireless sensor network key management survey and taxonomy,” *Journal of Network and Computer Applications*, vol. 33, no. 2, pp. 63–75, 2010.
- [54] J. Sen, “A survey on wireless sensor network security,” *International Journal of Communication Networks and Information Security*, vol. 1, no. 2, 2010.
- [55] S. Lee and K. Kim, “Sensor authentication scheme for clustering routing protocols in wireless sensor networks,” in *Proceedings of the IEEE Sensors*, pp. 1819–1822, IEEE, November 2010.
- [56] M. Stamp, *Information Security: Principles and Practice*, John Wiley & Sons, 2011.

Research Article

RESH: A Secure Authentication Algorithm Based on Regeneration Encoding Self-Healing Technology in WSN

Wei Liang,¹ Zhiqiang Ruan,^{2,3} Yuntao Wang,⁴ and Xiaoyan Chen¹

¹Department of Software Engineering, Xiamen University of Technology, Xiamen, Fujian 361024, China

²Department of Computer Science, Minjiang University, Fuzhou 350108, China

³Fujian Provincial Key Laboratory of Information Processing and Intelligent Control, Fuzhou 350116, China

⁴Institute of Information Engineering Chinese Academy of Sciences, Beijing 100093, China

Correspondence should be addressed to Zhiqiang Ruan; rzq_911@163.com

Received 18 March 2016; Accepted 11 May 2016

Academic Editor: Fei Yu

Copyright © 2016 Wei Liang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In the real application environment of wireless sensor networks (WSNs), the uncertain factor of data storage makes the authentication information be easily forged and destroyed by illegal attackers. As a result, it is hard for secure managers to conduct forensics on transmitted information in WSN. This work considers the regeneration encoding self-healing and secret sharing techniques and proposes an effective scheme to authenticate data in WSN. The data is encoded by regeneration codes and then distributed to other redundant nodes in the form of fragments. When the network is attacked, the scheme has the ability against tampering attack or collusion attack. Furthermore, the damaged fragments can be restored as well. Parts of fragments, encoded by regeneration code, are required for secure authentication of the original distributed data. Experimental results show that the proposed scheme reduces hardware communication overhead by five percent in comparison. Additionally, the performance of local recovery achieves ninety percent.

1. Introduction

In recent years, wireless sensor network (WSN) is widely used to human life in various areas. The protection for individual privacy becomes increasingly prominent. In the area of medical care, various sensors are attached to human body in order to collect information of patients. The identity and signs data of patients are regarded as privacy and need protection [1]. WSN as a new way for information collection and processing is an interdisciplinary field of sensor technology, network communication, biological medicine, computer technology, and so forth. Nowadays, WSN becomes a hotspot in academia and industry [2]. Due to its features of small size, high flexibility, and low power, WSN is rapidly used in pervasive computing and system on chip, as shown in Figure 1. In WSNs it is used to cluster member nodes that take part in long distance data transmission to a base station (BS). However, the secure transmission and distribution of sensitive data in WSN require deep investigation in confidentiality and integrity of data transmission.

In previous transmission technologies, the fault-tolerant ability and resistance against node capturing are much lower. In communication, if the transmitted data is attacked, the security will be hardly ensured. Existing network recovery aims at single node: that is, the data in only one fault node can be restored each time. Multiple fault nodes are common in real application. Obviously, healing of single node will cause high communication bandwidth. Because encoded information of nodes is correlated and the correlation of fault nodes is not used in recovery of single node. Recently, many researchers have conducted work on healing technology for multiple fault nodes. The problems including key management, message authentication, secure time synchronization, and intrusion detection are considered in their research. Consequently, secure communication of data in WSN has been widely concerned [3].

In secure transmission of WSN, Benenson et al. proposed a secure authentication scheme in WSN based on asymmetric encryption [4]. Inner encryption of wireless network is

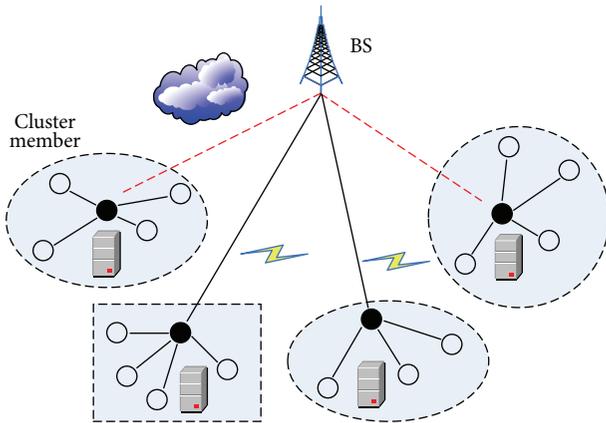


FIGURE 1: Clustering-based routing topology.

utilized for secure protection. After that, the scheme uses certificate authority for access control of the client. n neighbor nodes are selected as verifier. In this case, it is possible to verify the users by using (n, t) secret sharing method. Wang et al. [5] deployed a private wireless sensor network to monitor the whole vehicle network. The vehicle-mounted communication mode and the position of communication event are available. Besides, they have also conducted plenty of meaningful work in secure wireless vehicle network. Goyal et al. [6] proposed an access control strategy by allowing secret key to express any monotonous control tree. A user applies to a credibly authorized party for a secret key. The authorized party decides which characteristic combination in cryptograph can be decrypted by user. This strategy has added the expressive ability of KP-ABE, but the secret key of a user should be assigned in advance. Sahai and Waters [7] firstly presented a characteristic based encryption method and used it for access control. The encrypting party connects data with a series of characteristics. The secret key, assigned to user by the credible third party, is related to access structure of the characteristic set. The secret key reflects the privilege of user. The message is encrypted by using the characteristic. The key which satisfies the characteristic can only be used in decryption. However, this scheme cannot be popularized due to its lower expression of semantic. Bethencourt et al. [8] proposed another characteristic based encryption method. In this method, secret sharing is used in encryption stage to realize strict access control. The secret key is connected with related characteristic set. There is an access structure in the cryptograph. If the characteristic of secret key satisfies the access structure, it can be used in decryption. Otherwise, the decryption is rejected. The drawback of scheme in [9] is the requirement of polynomial interpolation to reconfigure the key. So, many complex operations of matching and exponentiation will be performed in decryption.

The authors in [9] have realized multiauthority attribute based encryption, which greatly reduced the computation overhead at stages of encryption and key generation. The security of encryption depends on hash function. Actually, no real random numbers are generated. In this case, the security of the proposed scheme is lower than that of SW

scheme. Cheung and Newport utilized random elements instead of secret sharing to realize strict access control [10]. In this scheme, the sizes of cryptograph and key increase linearly with the growth of the number of characteristics. So, this scheme has lower efficiency. Carbutar et al. [11] investigated privacy content in WSN by query and proposed a SPYC protocol. This protocol considers that previous query mechanisms in WSN are lack of protection for user privacy, which may cause privacy leaking in transmission. Sheng and Li [12] presented a distributed data storage and query scheme to protect data and query range from being known by base station. But it cannot cope with collusion attack of sensor nodes and storage nodes. Subramanian et al. [13] introduced anonymous medium nodes to hide the incredible data origin. It can protect privacy of data type and query when a few normal nodes, storage nodes, and anonymous nodes are captured at the same time. However, selection of medium nodes is random and unpredictable. If the medium node is far away from the original node and destination node, it will cause unnecessary communication overhead. Additionally, data type is limit and there is one-to-one mapping between data type and conversion type. Attackers could find the mapping relationship by capturing a number of nodes. Finally, invalidation of medium node will make the path of data transmission lose efficacy.

Recently, researchers focus on secure encoding scheme with self-recovery. In these schemes, sensor nodes can receive important privacy data even when the data is attacked. Pawar et al. [14] proposed a secure scheme by restoring nodes dynamically. In this work, the authors list a few security threats of distributed storage system based on network encoding. On this basis, an eavesdropper model against illegal attacks is proposed. The scheme has good ability to resist collusion attacks. The authors in [15] proposed a fault-tolerant encoding scheme, as shown in Figure 2. The scheme integrates (n, k) -RS encoding with simple XOR operation. It mainly aims at high efficient restoration of single node. Actually, the scheme has improved immunity of data transmission from interference by decreasing the data transmission rate. n ($n > k$) code words are generated by encoding k original data and distributed to n path for transmission. If there are multiple invalid paths, the destination node can restore k original data with the received m ($m > k$) code words.

The error correction coding has strong fault-tolerant ability and low data redundancy, which is suitable for secure data transmission. Kim et al. used linear block code to construct secure wireless data transmission [16]. Dulman et al. [17] developed an error correction coding (ECC) based data transmission scheme by making a balance between data reliability and communication overhead. Djukic and Valaee [18] proposed a secure protocol (DCDD) at transport layer in data collection oriented WSN. ECC is utilized in oriented diffused routing protocol, which improves reliability by ten percent and greatly reduces the delay. In [19], RDP coding mixed with redundancy is utilized to accelerate data restoration. Furthermore, diagonal redundancy based cross-recovery is used. A half is restored by using redundancy of counterdiagonal and the other is regarded as shared data. This scheme reduces overhead of restoring bandwidth in

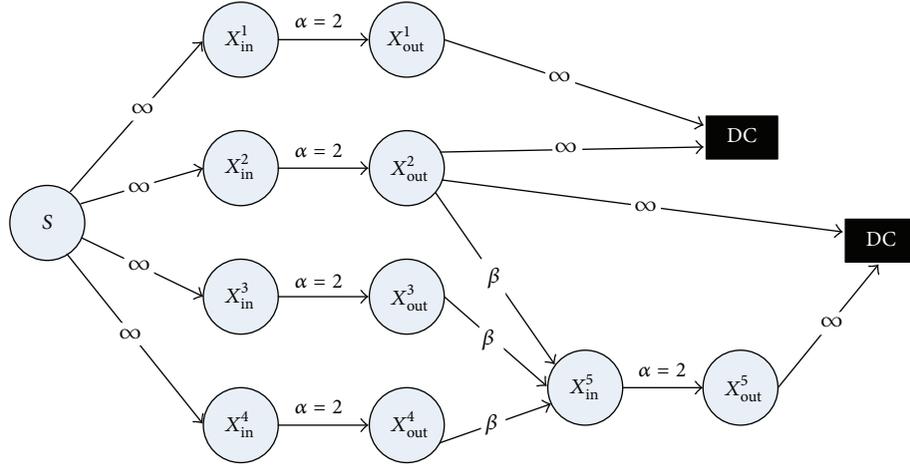


FIGURE 2: Multipath transmission based on error correction coding.

wireless nodes. The work of [20] proposed a method of combining scrambling technology with ECC to realize both confidentiality and reliability in wireless communication. The scheme overcomes burst error and has good security. But the communication overhead is large.

On the basis of the above studies, there are two issues on secure data transmission and data healing in WSN. On one hand, data storage in WSN is under security threat and can easily be attacked by dynamical tampering. Attackers could modify part of data content after capturing nodes. On the other hand, the usage rate of sensor nodes is limited. It may cause large performance overhead in transmission.

In this work, a secure fault-tolerant model in WSN is introduced. According to this model, the authors have designed an authentication scheme based on regeneration encoding self-healing technology. This scheme realizes secret dividing and content restoration of data on nodes in WSN. It can authenticate the integrality of data transmission without participation of original data. When wireless nodes suffered capture attack or tampering attack, the data can be restored with enough data fragments. After that, the secure authentication can be realized. The experimental results show that the proposed scheme has features of low complexity, high ability against capture attacks, and low overhead.

2. Preliminaries

In WSN, some nodes may lose efficacy if they are attacked. Thus, the invalid nodes will affect the reliability of data. In this work, we propose to solve data healing and security authentication by using regeneration code and secret sharing.

2.1. Regeneration Code. Regeneration code is a local encoding technology by combing (n, k) -RS code and simple XOR operation. It can restore arbitrary two missing data and has MDS feature to arbitrary n and k . By comparing with copying technology, regeneration code provides better efficiency of network storage and reliability of transmission. In traditional WSN, the operations of encoding and decoding are complex

because computation is on the basis of finite field. So, large bandwidth overhead is required for node restoration.

We assume the restoration degree of invalid data in invalid node to be d . As known from RS encoding, if a redundant data in WSN is invalid, other k data blocks are required in order to restore the invalid one. Meanwhile, it causes communication overhead of k times than that of the invalid block.

The increase of invalid data of nodes in WSN will enlarge overhead of data transmission and cause lots of instable security factors. To address the issues of communication overhead and security threat, Dimakis et al. proposed a scheme by using regeneration code [21]. The transmitted file is set to be S . It is separated into two parts: $S = [S(1), S(2)]$, $S(i) \in F^{1 \times k}$, $i \in \{1, 2\}$. F is finite field. $S(1)$ and $S(2)$ can, respectively, be encoded as a vector with the length of n by using (n, k) -RS code, $X = S(1) \cdot G$, and $Y = S(2) \cdot G$. Here, $G \in F^{k \times n}$ is a MDS matrix generated by (n, k) -RS code. With any k blocks encoded by regeneration code, a vector $C = X + Y$ is calculated through XOR operation. The value of C can be used to construct original data $S(1)$ and $S(2)$.

Firstly, the nodes in WSN should satisfy the (n, k) feature in encoding technology. In other words, encoded information is stored in n nodes and can tolerate $n-k$ faults. Generally, X regeneration code is required for distributed network storage. Regeneration code is an array to tolerate two faults. The simple structure is shown in Table 1. When one node (two nodes) is (are) invalid, the restoration can be realized through simple XOR operations. The decoding and update can achieve the optimal. So, it is called the optimal regeneration code because this regeneration code could correct a few faults in data transmission. The regeneration code combines multi-faults-tolerant RS code and X encoding technology. It realizes the features of (n, k) and simple restoration. RS code offers a restoration for $n-k$ faults. For single fault or double faults, the use of X encoding in RS code can achieve better performance in data healing.

X regeneration code is founded on polynomial, which has small local reparability [22]. Firstly, the generation rule based

Node 1	Node 2	Node 3	Node 4
x_1	x_2	x_3	x_4
y_2	y_3	y_4	y_1
z_3	z_4	z_1	z_2
$x_4 + y_4 + z_4$	$x_1 + y_1 + z_1$	$x_2 + y_2 + z_2$	$x_3 + y_3 + z_3$
$x_2 + y_4 + z_2$	$x_3 + y_1 + z_3$	$x_4 + y_2 + z_4$	$x_1 + y_3 + z_1$

Node 5	Node 6	Node 7	Node 8
x_5	x_6	x_7	x_8
y_6	y_7	y_8	y_5
z_7	z_8	z_5	z_6
$x_8 + y_8 + z_8$	$x_5 + y_5 + z_5$	$x_6 + y_6 + z_6$	$x_7 + y_7 + z_7$
$x_6 + y_8 + z_6$	$x_7 + y_5 + z_7$	$x_8 + y_6 + z_8$	$x_5 + y_7 + z_5$

FIGURE 3: The structure of X regeneration code when $n = 8$.

TABLE 1: The general structure of simple regeneration code.

Node 1	Node 2	...	Node $n-2$	Node $n-1$	Node n
x_1	x_2	...	x_{n-2}	x_{n-1}	x_n
y_2	y_3	...	y_{n-1}	y_n	y_1
s_3	s_4	...	s_n	s_1	s_2

on leading diagonal is utilized to divide redundant blocks at the first row. After that, the redundant blocks at the second row are divided by using counterdiagonal. We use 8 sensor nodes for illustration, as shown in Figure 3. For node 1, the redundant block is generated by performing xor operation on x_4, y_4, z_4 . The same operation is performed on x_3, y_5, z_2 to get the second block. The data at the diagonal are collected as a redundant group: for example, $\{x_1, y_1, z_1, x_1 + y_1 + z_1\}$. If a fault occurs in one node, the redundant group will be utilized to reconfigure the damaged data. For example, when a fault occurs in node 1, it is possible to restore x_1 by downloading y_1 from node 5, z_1 from node 4, and $x_1 + y_1 + z_1$ from node 3. It is the same case to damaged data in other nodes. For nodes from 1 to 8, the recovery only needs connecting several surviving nodes. In distributed storage system of wireless sensor nodes, the superiority of using X regeneration code will be more obvious if there are a large number of nodes.

2.2. Thought of Secret Sharing. Shamir [23] proposed a secret sharing method based on Lagrange interpolation formula.

It utilizes expressiveness of coplanar points to construct a reconfigurable polynomial function. The subkey and secret data are correlated into a class with the same attribute. The content of any item can be restored with other items. The scheme has strong security. But several conditions are satisfied in use of this scheme.

- (1) A large enough prime number q and positive integer s are selected, $q > s$.
- (2) $(m_i, m_j) = 1 (\forall i, j, i \neq j), \forall i, (q, m_i) = 1$: that is, m_i cannot be the integral multiple of q .
- (3) $N = \prod_{i=1}^k m_i > q \prod_{i=1}^k m_{n-i+1}$; N is the product of the top k numbers of m_i .
- (4) The condition in (1) shows the secret data s less than q . But in (3), if N/q is greater than the product of selected $k-1$ numbers of m_i , the random number is $A, 0 \leq A \leq [N/q] - 1$. The number of q and A can be made public.
- (5) Let calculation function for data distribution be $y = s + Aq$. Due to $0 \leq A \leq [N/q] - 1$, we have $Aq \leq N - q$. Besides, $q > s, s - q < 0$, we derive $y = s + Aq \leq s + N - q < N$. So, there must be a $y < N$ and y is a secret. The key can be calculated by solving the equation set $y_i \equiv y \pmod{m_i}, i = 1, \dots, n$.
- (6) When (m_i, y_i) is i th subkey, the set of $\{(m_i, y_i)\}_{i=1}^n$ could construct a (k, n) secret sharing scheme in

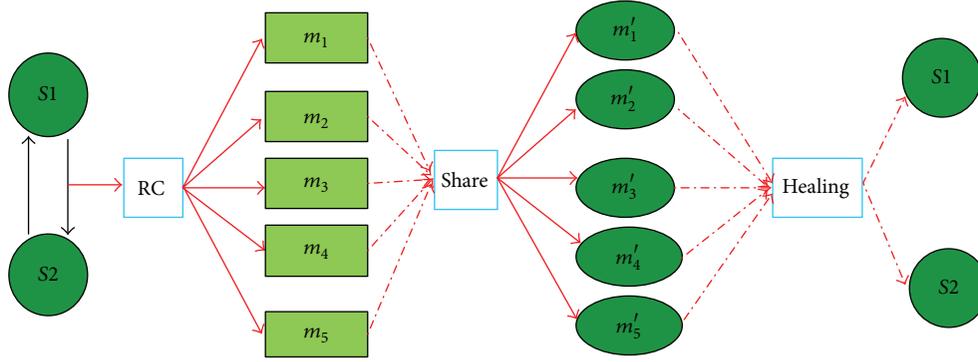


FIGURE 4: Secret sharing mechanism.

WSN. According to (5), $y \equiv y' \pmod{N'}$ is calculated. Here, we have $N' = \prod_{j=1}^k m_{i_j} \geq N$. y is the unique solution of congruence equation modulus N' , $N' \geq N$, $y < N$. So, $y = y'$ is unique. The secret data s is calculated through $s = y - Aq$.

Figure 4 illustrates the thought of secret sharing. The transmitted data $S(1)$ and $S(2)$ are encoded by regeneration code with the production of m_1, m_2, m_3, m_4 , and m_5 . The information is further shared into n fragments. In the receiving end, the reliability can be authenticated through several fragments. It mainly depends on regeneration code for data restoration. If several data blocks are damaged, it will be possible to restore the original $S(1)$ and $S(2)$.

3. Regeneration Code Based Authentication Scheme

In this section, we introduce the healing mechanism after encoding the transmitted data in WSN. This scheme is resilient to illegal attacks. In real WSN, nodes may face security threats in terms of storage and computation. The following attacks are assumed to be suffered. (1) Illegal attackers intercept information from the communication flow in WSN. (2) Illegal attackers can randomly capture a few nodes. After that, they will get the key in these nodes and crack information in other nodes. (3) After capturing some nodes, the attackers could remove, modify, or forge the collected data in real WSN. The data is damaged. In this case, it is unable to trace the attacks.

To illustrate the security and reliability of the authentication scheme, we define some parameters in WSN in Notations. Here, the security involves confidentiality and completeness of data. The reliability is that some invalid or captured nodes will not affect normal running of the system. Furthermore, the ability of fault-tolerance represents that the damaged data could be restored through X regeneration encoding when random faults occur or some data blocks are modified.

3.1. Structure of Regeneration Code. A WSN is deployed in area of πR^2 . The data is encoded by regeneration code. After that, the data in nodes is randomized. The regeneration

encoding technology is fully utilized to get the encoded data. The procedure is described as follows.

- (1) The information S in wireless sensor node is encoded into binary string and divided into groups. On the basis of regeneration encoding model, each group S_i is transformed into decimal number and fatherly encoded by (5, 3) RS code. In Galois Field $GF(24)$, the bit number of each information symbol is set as $m = 4$. (5, 3) RS code represents that five information symbols relate to two error correcting bits. In this case, three information symbols are a unit for RS encoding. S_i is transformed into binary string T with length of 12 (padding zero on left when the bits are insufficient).
- (2) For $S(x) = (S_1, S_2, \dots, S_i)$, each four bits are transformed into an element in Galois Field $GF(24)$. After that, a sequence G in $GF(24)$ is produced. Each row represents a sequence of elements for S_i in Galois Field.
- (3) The elements of each row in G are encoded and thus a matrix γ is produced. C_{ij} ($i = 1, 2, \dots, n; j = 1, 2, 3, 4$) denotes the data block before RS encoding and D_{ij} ($i = 1, 2, \dots, n; j = 1, 2$) is the error correction code of i th group of data after encoding. Each row in γ is a RS block BK_i ($i = 1, 2, \dots, n$). These blocks are randomly distributed and stored in nodes of wireless network.
- (4) The data in WSN is denoted by W , which is transformed into encoded sequence B with the length of λ after decoding. Let the length of a pseudorandom sequence P be λ . We perform XOR operation on both the sequences. Finally, the distributed data fragments $W = \{W_i \mid 0 \leq i < \lambda\}$ based on regeneration code are produced.

3.2. Implementation of Secret Sharing. The encoded data fragments M_i based on regeneration code are shared and then distributed. The threshold secret sharing [24] and regeneration encoding technology [25] are utilized in data encryption on nodes in WSN. The concrete implementation is described as follows.

We assume N nodes to form an undirected graph $G(V, E)$ in WSN. The collections of nodes and edges are, respectively, denoted by $V = \{v_1, v_2, \dots, v_N\}$ and $E = \{e_1, e_2, \dots, e_N\}$. Each node is denoted by v_i ($1 \leq i \leq N$), which has d_i neighbors. These nodes are organized as a collection NB_i . We produce a random session key k_s for v_i and compute hash value $H(D, K)$. After that, S_i and $H(D, K)$ are encoded by using k_s . Furthermore, the session key k_s is encrypted by public key Pk_u . Finally, two parts of data are produced, respectively, M_i and M_j . After that, v utilizes (m, n) secret sharing technology and regeneration code and divides M into n fragments, denoted by M_{ij} ($1 \leq i \leq n, 1 \leq j \leq n$). Meanwhile, E is divided into m parts in order to construct

$$M(x) = E_0 + E_1x + \dots + E_{m-1}x^{m-1}. \quad (1)$$

When v acquires n fragments S_j ($1 \leq j \leq n$), the equation $S_j = M(a^j)$ is satisfied. Here, $n \leq 2^p - 1$. Finally, v selects n neighbor nodes from NB_i and realizes secret sharing to each neighbor node. The shared secret keys are denoted by M'_i and M'_j .

3.3. Distribution of Regeneration Code. The data in original node S is encoded into M , which is fatherly shared into multiple blocks. We randomly select $n - 1$ ($n \leq N$) nodes as initial distribution nodes. For the $(j + 1)$ th distribution node, the shared key $k_{i,j+1}$ could be calculated by asymmetrical secret key pair ID_s/K_s and ID_{j+1} [26]. The reserved data fragment of original node is $S_{i,n-1}$. The encrypted data fragment S_{ij} is sent to the $(j + 1)$ th node, $1 \leq i \leq \lceil [T/m]/k \rceil$, $0 \leq j \leq n - 2$. The routing between original node and storage node cannot be determined in advance. When the $(j + 1)$ th node receives the response, the related key $k_{i,j+1}$ is calculated by ID_s/K_s and ID_{j+1} . Thus, $M'_{i,j+1}$ is produced. The above steps are repeated until all the data fragments are sent to the nodes.

3.4. Self-Healing Technology Based on Regeneration Code. When a part of data in wireless sensor node is attacked, the authentication data D is always damaged. In this section, we introduce a scheme to restore the damaged authentication data. Thus, the completeness of data in WSN can be ensured.

Let G be the generation matrix of regeneration code. If a receiving end receives k ($0 \leq k \leq n$) blocks without errors, it is able to restore the original data. We assume the blocks from the j th node. If there is no error, k blocks in i th group could be restored by solving the following equation:

$$\begin{bmatrix} u_{i_0}, u_{i_1}, \dots, u_{i_{(k-1)}} \end{bmatrix} \widehat{G} = \begin{bmatrix} c_{ij_0}, c_{ij_1}, \dots, c_{ij_{k-1}} \end{bmatrix}. \quad (2)$$

Here,

$$\widehat{G} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ a^{j_0} & a^{j_1} & \dots & a^{j_{k-1}} \\ (a^{j_0})^2 & (a^{j_1})^2 & & (a^{j_{k-1}})^2 \\ & & \vdots & \\ (a^{j_0})^{k-1} & (a^{j_1})^{k-1} & & (a^{j_{k-1}})^{k-1} \end{bmatrix} \quad (3)$$

\widehat{G} is established by element a in primitive field and index of c_{ij_ε} , $0 \leq \varepsilon \leq k - 1$.

The authentication of data in wireless sensor nodes is performed in stages. We assume there are l errors at l th stage. If decoding fails or the decoded data cannot pass verification of CRC, too many errors may occur. The regeneration code cannot correct all errors. Two redundant symbols are required to correct an error. So, $k + 2l$ symbols are required at l th stage. The procedure of recovery is described as follows.

(1) Let $i = k$, randomly select k wireless sensor nodes, and detect the encoded data $c_i = (c_{j_0}, c_{j_1}, \dots, c_{j_{(k-1)}})$. Set $r_i = c_i$.

(2) Calculate $u = r_i \widehat{G}^{-1}$ to produce the data blocks of i th group. If u passes verification of CRC, the CRC codes are removed to get original data u_0 . Otherwise, go to step (3).

(3) Set $i = i + 2$. Select two symbols c_{i_1} and c_{i_2} from the nodes s_1 and s_2 that have not been accessed. They are added behind the received symbols to get a new code, $c_i \leftarrow c_{i-2} \cup \{c_{i_1}, c_{i_2}\}$. k symbols are produced by decoding the new code. It repeats until a failure occurs or $i \leq n - 1$.

(4) $i \geq n - 1$ demonstrates too many errors and a failed decoding. In this case, it shows a message of failed decoding. Otherwise, it enters the next stage and performs step (2).

Recovery of data contents needs k subkeys at least. So, exposure of r ($r \leq k - 1$) subkeys will not leak the whole content. If the data of the nodes is lost or damaged, it can be successfully restored if there are k valid fragments. According to the sharing mechanism in Section 2.2, $\forall u \geq k$ number of m_{i_1}, \dots, m_{i_u} in m_1, m_2, \dots, m_n , we have $H(s \mid m_{i_1}, m_{i_2}, \dots, m_{i_u}) = 0$. If m_{i_1}, \dots, m_{i_u} are known, the uncertainty of S is zero; that is, the content of S can be completely determined.

(5) On the basis of the above steps, an authorized user could directly restore the authentication data $D(C)$ from S_j . After that, S is restored with S_j by using Lagrange interpolation. In other words, if m fragments of authentication data $D(C)$ are collected from n nodes, we will effectively restore original data S in transmission.

3.5. Authentication Based on Regeneration Code. The participants of RC based authentication involve data distributor, data owner, and verifier. The distributor is responsible for encoding and sharing the data into n independent redundant blocks. These blocks are distributed to n data owners. The verifier takes charge of verifying completeness of data. Nodes in WSN can participate in authentication with both the identities of data owner and verifier.

The encoded data fragments are denoted by D_1, D_2, \dots, D_n , $n \leq 2^p - 1$. Each fragment has k symbols, denoted by $\lambda_{i_1}, \lambda_{i_2}, \dots, \lambda_{i_k}$. The length of a symbol is p . All operations are performed in finite field $GF(2^p)$. Completeness verification for node S has the following steps.

- (1) $s_i \parallel h$ is encrypted by symmetric key K_{ij} , which is the shared key of d_i and d_j ($i \neq j$). After that, the encrypted $s_i \parallel h$ is sent to d_j .
- (2) After receiving all of $s_i \parallel h$ ($i \neq j$), d_j decodes them with K_{ij} ($i \neq j, i \in [1, n]$). The equation $h_i = g^{s_i}$

is verified. If not satisfied, there are some errors in data fragments from d_i . Otherwise, the recovery continues to use Lagrange interpolation $f(0) = D_i = \sum_{i=1}^k s_i \prod_{j=1, j \neq i}^k (j/(j-i)) \bmod p$ to restore d_i .

The regeneration code based authentication includes the following steps.

(1) *Generation of Validation Information.* Original node randomly selects u ($u \leq n$) elements $\beta_1, \beta_2, \dots, \beta_u$ in finite field $\text{GF}(2^p)$. n different odd-even check numbers P_1, P_2, \dots, P_u are produced, $P_j = \sum_{i=1}^n \beta_j^{i-1} S_i$, ($i \in [1, n]$, $j \in [1, u]$).

(2) *Distribution.* Original node v distributes u odd-even check numbers and n data fragments to n randomly selected neighbors in NB_i . For instance, original node selects P_j ($j \in [1, u]$) in u odd-even check numbers and S_i ($i \in [1, n]$) in n data fragments. After that, they are sent to a randomly selected neighboring node. Due to $u \leq n$, some nodes may only receive the data fragments other than odd-even check numbers. But some other nodes may receive both of them, which can be the verifiers. There are u verifiers among n nodes. The data is encrypted to avoid interception.

(3) *Inquiry.* Assume that the data owner of fragment $\{P_j, \beta_j\}$ wants to verify the data completeness. Firstly, an inquiry message $\{w_i, R_i, a, r\}$ is forecasted to all of data owners. r represents the number of required messages, $r \leq 2^p - 1$. a is a randomly selected element in $\text{GF}(2^p)$.

(4) *Response.* After receiving the inquiry message, the nodes with $\{R_i, S_i\}$ ($i \in [1, n]$) will calculate r messages $\Phi_{(a,r)}(S_i) = (\Phi_{a^1}(S_i), \dots, \Phi_{a^r}(S_i))$ and replies to w_i by broadcasting. The response message is encrypted to avoid interception.

(5) *First Verification.* With the returned $\Phi_{(a,r)}(S_i)$ ($i \in [1, n]$), node w_i verifies the equation $\Phi_{a^r}(P_j) = \Theta_j(\Phi_{a^1}(S_1), \dots, \Phi_{a^r}(S_n)) = \sum_{i=1}^n \beta_j^{i-1} (S_i)$, $t \in [1, r]$. There are r equations. Any unsatisfied equation shows that modification or errors occur.

(6) *Second Verification.* The node w needs to store the detected data during a period of time. Each node stores data packages from different origins or data fragments at various stages. Any node could perform the first verification to all data fragments from the same node at any time. At different periods, w produces data fragments S_i and S_i' . The verifier sends an inquiry message to verify both of the fragments. When the inquiry message at i th round is received, the message $\Phi_a(S_i \parallel S_i')$ is returned to the verifier. The odd-even check numbers for the verifier are, respectively, P_i and P_i' , $i \in [1, n]$. If all responses are received, the verifier calculates $\Phi_a(P_i \parallel P_i') = \Phi_a(P_i) + a^k \Phi_a(P_i')$ and performs verification. The proposed scheme could perform the second verification to the stored data during a period of time. No matter what the number of fragments is, the produced messages have the same size. It has effectively saved storage and communication overhead in procedure of authentication.

4. Performance Analysis

4.1. Overhead. In authentication of data in WSN, original node firstly calculates a hash value $h = g^{D_i} \bmod p$, n -order polynomial with degree of $k - 1$, and n hash values h_i . n data fragments are encrypted. Finally, the n hash values and data fragments are randomly sent to other nodes in network. The whole computation overhead in authentication is caused by decoding and hashing. In storage, each node stores n hash values. The communication cost is $n^* |S_i|$ because each authentication returns n data fragments. So, data distribution and verification at each round require n times of calculations. The overhead in communication is large.

Before generation of data fragments, original node needs to calculate a hash value H and perform two symmetrical encryptions, respectively, $H(D, K)$ and $\{k_s\}_{PK_u}$. The generation of data fragments requires calculating two polynomials. (m, n) RS code is utilized to encode $E = \{D_i, h(D_i, k_s)\}_{k_i}$ into n symbols. m is the number of data fragments and n is the number of selected neighbor nodes. Each data fragment is supposed to include c symbols. So, there are nc operations on polynomial. The original node utilizes (m, n) threshold secret sharing to get n symbols from $\{k_s\}_{PK_u}$. Finally, the check codes of all data fragments are produced. Let l be the length of data before encoding. The computation overhead of the original node includes hash of data with length of l , two symmetrical encryptions, $n(c + 1)$ operations on m -order polynomial, and t odd-even checks. The computation overhead for the owner of each fragment is one decryption.

The verification of data fragments is in the finite field $\text{GF}(2^p)$, $p = 8$. After generation of data fragments, the original node removes original data and sends n fragments of $\{ID_v \parallel R_i \parallel S_i \parallel \beta_i \parallel P_i\}_{K_{v,w_i}}$ to neighbor node i . Here, S_i contains k symbols. So, the communication overhead in distribution is almost $n(2k + 3)q$. Obviously, the storage overhead for each data owner is $(2k + 3)q$. After all of the fragments are received, the owner of each fragment performs verification of completeness. This procedure needs to calculate odd-even check and message with length of k . Suppose that data owner w conducts completeness verification. Firstly, an inquiry message $\{w_i, R_i, a, r\}$ is broadcasted to all of the owners. The communication overhead is $4p$. Each data owner calculates a digest and returns it to the verifier after receiving the inquiry message. The length of this digest is same to that of a symbol. A symbol with length of k is calculated. The response is $\Omega_a(S_i)$. So, the communication overhead is p .

4.2. Security. Illegal users make security attacks by deploying sensor nodes or capturing nodes in WSN. The deployed nodes pretend to be the real nodes in WSN, steal confidential information, or launch false data injection. Besides, if multiple nodes are captured, the attackers could send plenty of false data. In this case, the network resource, such as energy, bandwidth, computation ability, and storage space, will be exhausted rapidly.

When the data is attacked, we need to restore and authenticate the damaged data through the proposed scheme. In this section, the security of the proposed scheme against attacks of forging, tampering, or collusion is analyzed.

(1) *Ability against Forging Attacks.* The sender always sends data with his pseudonym to the receiver. Other nodes cannot counterfeit the pseudonym of u . Otherwise, it is unable to pass verification of authenticator. The difficulty to counterfeit identity of u equals that of attacking SHA-1 hash function.

(2) *Ability against Tampering.* On one hand, the key in encryption is generated by using regeneration code. The privilege of decoding is under control. So, it is unable for anyone, including the sender, to tamper the information. On the other hand, attackers know nothing about the key. So, they cannot counterfeit or tamper the contents. The key is generated in authentication for multiple nodes. A single node authentication cannot realize tampering.

(3) *Ability against Collusion Attacks.* WSN is self-organized. So, it is possible to realize collusion attack. The sensitive data is divided into k parts and authenticated in k nodes with high credibility. It reduces the dependency on the third party. To get the secret, attackers need to restore $k-1$ order polynomial $F(x)$. On the basis of Lagrange interpolation, a successful attack means enough interpolating points are required. In other words, k nodes conspired at least. But the conclusion of so many nodes is much difficult. On the other hand, it makes the proposed scheme have ability against noncooperation of $n-k$ nodes in procedure of recovery. So, the proposed scheme has high robustness in WSN.

4.3. *Anonymity.* Usually, it is unable to connect each authentication to real identity of the node. The data sent to authenticator is pseudonym. If no anonymity is stolen, attackers know nothing about real identity of authentication nodes. Of course, the real information in the nodes cannot be traced. Each authentication request utilizes multicast. So, attackers cannot destroy communication anonymity of medium nodes. Furthermore, authentication does not expose real identity of nodes. So, the attacked nodes cannot get other information. It offers good protection to sensitive information of wireless nodes.

4.4. *Traceability.* The data distribution system of nodes could trace behavior of attacks by using communication record. In other words, the nodes need to verify the key through cooperation of arbitration nodes before authentication. In this round of authentication, the arbitration nodes have sent the identity information to each node. The true identity is related to false identity. The relevance is kept all the time in authentication. Even if the attackers find resources in nonneighboring nodes through anonymous attack, the credentials could find the trace of attacks. In this case, the third institution can track out attackers on the basis of the information from the attacked nodes.

5. Experimental Result

5.1. *Stimulation.* The experiment is realized by C++ language and developed at visual C++ platform. In the secure network environment of this paper, the secret sharing mechanism is utilized to establish a secure recovery model based on

regeneration code. Here, the initial threshold value is set as 0.5. The number of nodes is set at 500 in Network Simulator-2 (NS-2). These nodes are deployed within an area of 500 m × 500 m. Each node has initial energy of 2 J. In experiment, the dead nodes will exit network immediately [26]. The nodes are set at the highest level of protection in simulation. Illegal attackers are unable to perform successful attack on the signed nodes. Only the common nodes in network may be attacked. In this section, we have considered several common attacks and compared the performance against these attacks.

5.2. Analysis of Experimental Results

5.2.1. *Security.* Assume that N wireless sensor nodes are deployed within the area of πR^2 . R denotes the transmission range. The positions of all nodes are supposed to obey two-dimensional Poisson distribution. So, when the communication radius of node s is denoted by r , the probability to include $n-1$ nodes within the area of h hops could be nearly calculated as follows:

$$\Pr[\chi(h) = n-1] = \frac{e^{-\theta}\theta^h}{h!}. \quad (4)$$

Here, $\theta = Nr^2/R^2$. h is regarded as a probability less than the expected value; that is, $\Pr[\chi(h) \geq n-1]$. The number of storage nodes is random, but the average value could be denoted by $\bar{n} = Nh^2r^2/R^2$. The probability of data hiding is calculated as the following formula:

$$P = 1 - \left(\frac{N'}{N}\right)^k \binom{\bar{n}}{k}. \quad (5)$$

Possibly, some common nodes in wireless network are selected as interception nodes. Illegal attackers attempt to intercept data package through decoding. In this experiment, the number of data packages is set as 500 at each time. Five illegal interception experiments are conducted for evaluation. Figure 5 shows the results. We observe the number of successful interception attacks in various schemes. The proposed RESH scheme has good ability against illegal interception by comparing to schemes in [27, 28].

5.2.2. *Overhead.* Figure 6 shows comparison of three schemes in overhead on storage and communication. The proposed scheme selects a few of key nodes for storage, which saves overhead on calculation and communication. The CADS scheme in [27] is based on discrete logarithm with complex calculation. Random walk in [28] has the highest communication cost because it utilizes broadcasting within the whole network. In the proposed scheme, the data in communication is compressed and has the ability of recovery due to the use of regeneration code. The results have verified effectiveness and availability in recovery. By analyzing, CADS scheme has higher detection rate, but the overhead on communication and calculation is much higher. For the proposed RESH scheme, it achieves higher detection rate, lower communication cost, and lower storage overhead.

We conduct experiments to evaluate time overhead. The downloading nodes and names of packages are randomly

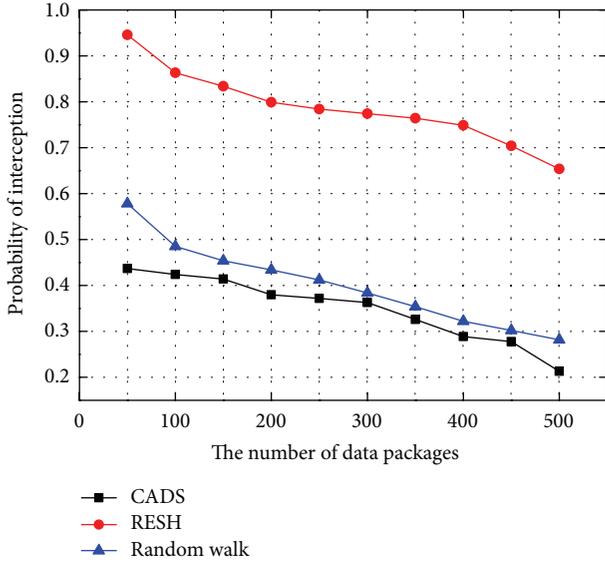


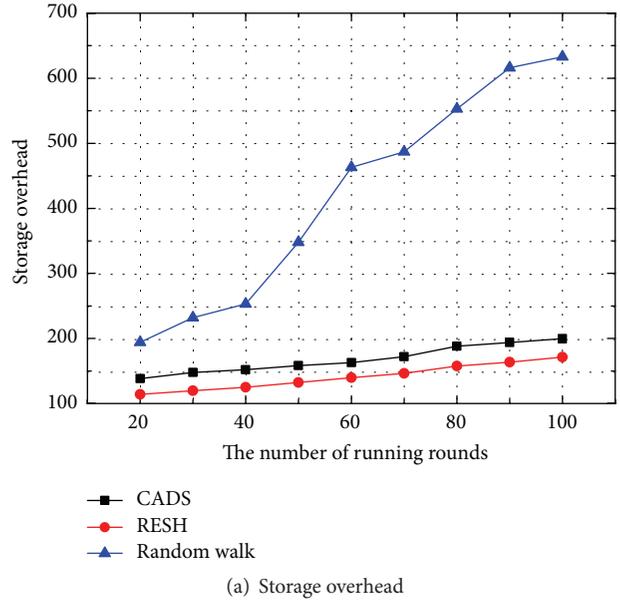
FIGURE 5: Comparison in probability of interception.

determined by system. The experiment considers the cases with different numbers of nodes. In Figure 7, we compare time cost of downloading data packages from nodes. The proposed scheme considers data communication based on regeneration code. It costs slightly more time by comparing to other schemes. But practically, it is valuable to exchange for privacy protection with less time cost.

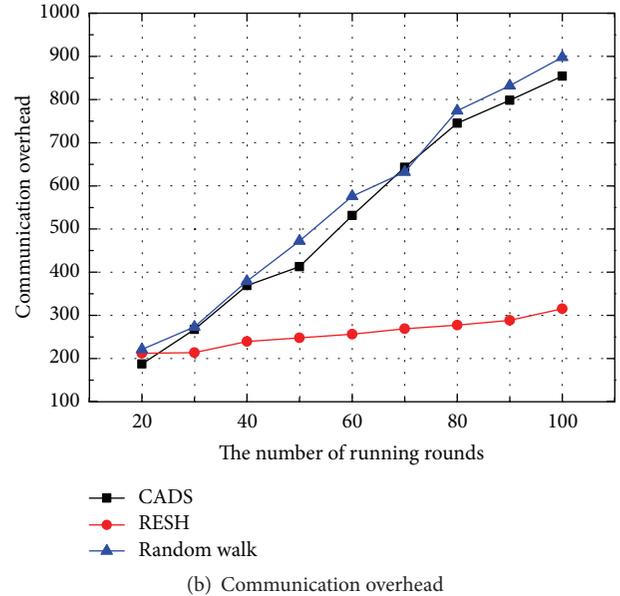
5.2.3. Recovery Ability. The performance of recovery in wireless communication is evaluated by the minimum Hamming distance d_{\min} of any two code words based on regeneration code. Odd-even check is utilized to restore the fault data. It enhances security in data transmission and storage. Due to the expandability of distributed cloud storage system, linear locally repairable codes (LRC) could restore encoded data through extended code and shortened code [29]. This method reduces the locality of restoring nodes by local and global redundancy. RS code is based on polynomial calculation and has lower locality of restoration. In Figure 8, we have compared the recovery ability of the proposed scheme to that of schemes based on RS encoding [30] and LRC encoding. The proposed scheme has good ability to restore fault nodes. The security and reliability of data transmission in wireless network are encouraging. The scheme based on regeneration code realizes real-time local healing when faults occur in nodes. If two nodes are fault at the same time, LRC based scheme [29, 31] needs to be transformed into RS encoding in restoration. It greatly decreases recovery ability of encoding algorithm. In our scheme, healing encoded information only requires connecting several local nodes. Once two nodes occurring faults, the recovery ability can also achieve 90 percent.

6. Conclusion and Prospect

This work considers secure transmission of data in WSN and proposes a model of completeness verification for WSN.



(a) Storage overhead



(b) Communication overhead

FIGURE 6: Overhead comparison for three schemes.

Before data authentication, the data is divided into data fragments and stored in various nodes. On this basis, a secure authentication scheme based on recovery technology and regeneration code is designed in WSN. The scheme can restore damaged data. Besides, it saves communication overhead and processing time. The main contributions are as follows. (1) Regeneration encoding and healing based on threshold scheme are combined to achieve good performance in self-healing. (2) The proposed scheme has good performance in local recovery. In future, we continue to study secure transmission of privacy data. The concentration is to find and protect contents that users are interested in. Fast and secure forensics of privacy data in WSN will be also investigated. Besides, we will focus on effective distribution

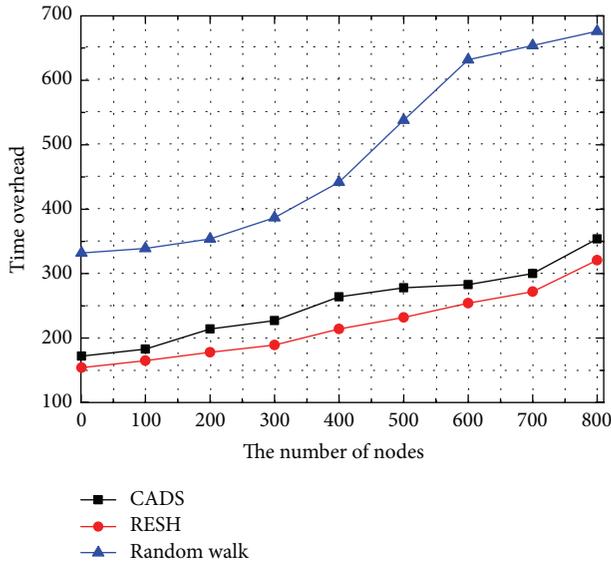


FIGURE 7: Comparison of time overhead.

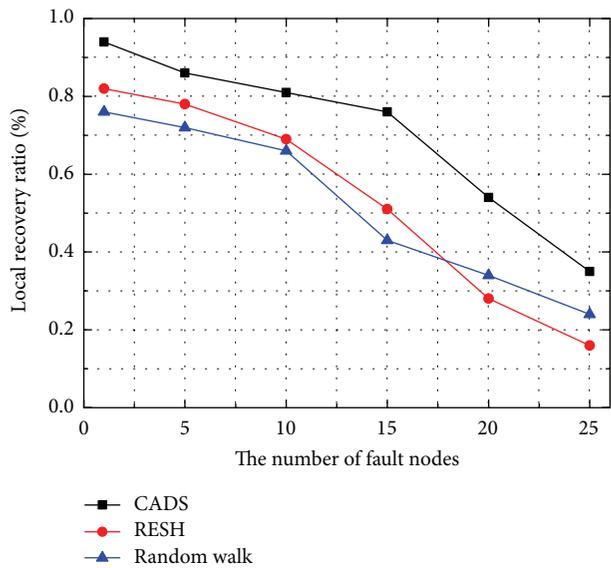


FIGURE 8: Comparison in local recovery ratio.

and secure communication of secret key in wireless network when the encoded content in network could be restored.

Notations

πR^2 :	Deployment area of wireless network
k_s :	Session key
B_i :	Encoded information
S :	Content of original node
D :	Authentication information
$E = \{e_1, e_2, \dots, e_y\}$:	Edge collection
P :	Secure hiding probability
C :	Power consumption in communication.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work is supported by the National Nature Science Foundation of China (Grant 61572188), the Natural Science Foundation of Fujian Province (Grant no. 2014J05079), the research project of Minjiang University (Grant no. MYZ14007), the research project of Fuzhou Science and Technology Office (Grant no. 2015-G-52), and the Research Project supported by Xiamen University of Technology (YKJ15019R).

References

- [1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–105, 2002.
- [2] Z. Chen, X. Li, B. Yang, and Q. Zhang, "A self-adaptive wireless sensor network coverage method for intrusion tolerance based on trust value," *Journal of Sensors*, vol. 2015, Article ID 430456, 10 pages, 2015.
- [3] S. R. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong, "TinyDB: an acquisitional query processing system for sensor networks," *ACM Transactions on Database Systems*, vol. 30, no. 1, pp. 122–173, 2005.
- [4] Z. Benenson, N. Gedicke, and O. Raivio, "Realizing robust user authentication in sensor networks," in *Proceedings of International Workshop on Realworld Wireless Sensor Networks (REALWSN '05)*, pp. 54–58, Stockholm, Sweden, 2005.
- [5] S. Wang, Q. Sun, H. Zou, and F. Yang, "Detecting SYN flooding attacks based on traffic prediction," *Security and Communication Networks*, vol. 5, no. 10, pp. 1131–1140, 2012.
- [6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)*, pp. 89–98, Alexandria, Va, USA, November 2006.
- [7] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology—EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22–26, 2005. Proceedings*, vol. 3494 of *Lecture Notes in Computer Science*, pp. 457–473, Springer, Berlin, Germany, 2005.
- [8] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the IEEE Symposium on Security and Privacy (SP '07)*, pp. 321–334, Berkeley, Calif, USA, May 2007.
- [9] M. Chase, "Multi-authority attribute based encryption," in *Proceedings of the 4th Theory of Cryptography Conference (TCC '07)*, pp. 515–534, Amsterdam, The Netherlands, 2007.
- [10] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proceedings of 14th International Conference on Computer and Communications Security (CCS '07)*, pp. 456–465, Alexandria, Va, USA, November 2007.
- [11] B. Carburnar, Y. Yu, L. Shi, M. Pearce, and V. Vasudevan, "Query privacy in wireless sensor networks," in *Proceedings of the 4th Annual IEEE Communications Society Conference on Sensor*,

- Mesh and Ad Hoc Communications and Networks*, pp. 203–212, IEEE, San Diego, Calif, USA, June 2007.
- [12] B. Sheng and Q. Li, “Verifiable privacy-preserving range query in two-tiered sensor networks,” in *Proceedings of the 27th IEEE Communications Society Conference on Computer Communications (INFOCOM '08)*, pp. 457–465, Phoenix, Ariz, USA, April 2008.
- [13] N. Subramanian, K. Yang, W. Zhang, and D. Qiao, “ElliPS: a privacy preserving scheme for sensor data storage and query,” in *Proceedings of the IEEE INFOCOM*, pp. 936–944, IEEE, Rio de Janeiro, Brazil, April 2009.
- [14] S. Pawar, S. El Rouayheb, and K. Ramchandran, “On secure distributed data storage under repair dynamics,” in *Proceedings of the IEEE International Symposium on Information Theory (ISIT '10)*, pp. 2543–2547, IEEE, Austin, Tex, USA, June 2010.
- [15] J. Luo, M. Shrestha, L. Xu, and J. S. Plank, “Efficient encoding schedules for XOR-based erasure codes,” *IEEE Transactions on Computers*, vol. 63, no. 9, pp. 2259–2272, 2014.
- [16] S. Kim, R. Fonseca, and D. Culler, “Reliable transfer on wireless sensor networks,” in *Proceedings of the 1st Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON '04)*, pp. 449–459, Santa Clara, Calif, USA, October 2004.
- [17] S. Dulman, T. Nieberg, J. Wu, and P. Havinga, “Trade-off between traffic overhead and reliability in multipath routing for wireless sensor networks,” in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '03)*, pp. 1918–1922, New Orleans, La, USA, March 2003.
- [18] P. Djukic and S. Valaee, “Reliable and energy efficient transport layer for sensor networks,” in *Proceedings of 49th IEEE Global Telecommunication Conference (GLOBECOM '06)*, San Francisco, Calif, USA, December 2006.
- [19] G. Wang, X. Liu, S. Lin, G. Xie, and J. Liu, “Generalizing RDP codes using the combinatorial method,” in *Proceedings of the 7th IEEE International Symposium on Networking Computing and Applications (NCA '08)*, pp. 93–100, July 2008.
- [20] M. Zhang, Z. Wang, and M. Guo, “A method of combining scrambling technology with error control coding to realize both confidentiality and reliability in wireless M2M communication,” *KSII Transactions on Internet and Information Systems*, vol. 6, no. 1, pp. 162–177, 2012.
- [21] A. G. Dimakis, P. B. Godfrey, M. J. Wainwright, and K. Ramchandran, “Network coding for distributed storage systems,” in *Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM '07)*, pp. 2000–2008, IEEE, Anchorage, Alaska, USA, May 2007.
- [22] V. R. Cadambe and A. Mazumdar, “Bounds on the size of locally recoverable codes,” *IEEE Transactions on Information Theory*, vol. 61, no. 11, pp. 5787–5794, 2015.
- [23] A. Shamir, “How to share a secret,” *Communications of the Association for Computing Machinery*, vol. 22, no. 11, pp. 612–613, 1979.
- [24] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, “A dynamic password-based user authentication scheme for hierarchical wireless sensor networks,” *Journal of Network and Computer Applications*, vol. 35, no. 5, pp. 1646–1656, 2012.
- [25] A. Mazumdar, V. Chandar, and G. W. Wornell, “Update-efficiency and local repairability limits for capacity approaching codes,” *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 5, pp. 976–998, 2014.
- [26] I. S. Reed and G. Solomon, “Polynomial codes over certain finite fields,” *Journal of the Society for Industrial and Applied Mathematics*, vol. 8, no. 2, pp. 300–304, 1960.
- [27] Z. Ruan, X. Sun, W. Liang, D. Sun, and Z. Xia, “CADS: co-operative anti-fraud data storage scheme for unattended wireless sensor networks,” *Information Technology Journal*, vol. 9, no. 7, pp. 1361–1368, 2010.
- [28] Y. Lin, B. Liang, and B. Li, “Data persistence in large-scale sensor networks with decentralized fountain codes,” in *Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM '07)*, pp. 1658–1666, IEEE, Anchorage, Alaska, USA, May 2007.
- [29] G. M. Kamath, N. Prakash, V. Lalitha, and P. V. Kumar, “Codes with local regeneration,” in *Proceedings of the IEEE International Symposium on Information Theory Proceedings (ISIT '13)*, pp. 1606–1610, IEEE, Istanbul, Turkey, July 2013.
- [30] T. Ernvall, T. Westerback, R. Freij-Hollanti, and C. Hollanti, “Constructions and properties of linear locally repairable codes,” *IEEE Transaction on Information Theory*, vol. 62, no. 3, pp. 1129–1143, 2016.
- [31] Z. Ruan, H. Luo, and Z. Chen, “Improving reliability of erasure codes-based storage paradigm under correlated failures for wireless sensor networks,” *International Journal of Communication Systems*, vol. 29, no. 5, pp. 992–1011, 2016.

Research Article

Multilevel Modeling of Distributed Denial of Service Attacks in Wireless Sensor Networks

Katarzyna Mazur,¹ Bogdan Ksiezopolski,¹ and Radoslaw Nielek²

¹*Institute of Computer Science, Maria Curie-Skłodowska University, Pl. M. Curie-Skłodowskiej 5, 20-031 Lublin, Poland*

²*Polish-Japanese Academy of Information Technology, Koszykowa 86, 02-008 Warsaw, Poland*

Correspondence should be addressed to Katarzyna Mazur; katarzyna.mazur@umcs.pl

Received 24 March 2016; Accepted 29 May 2016

Academic Editor: Fei Yu

Copyright © 2016 Katarzyna Mazur et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The growing popularity of wireless sensor networks increases the risk of security attacks. One of the most common and dangerous types of attack that takes place these days in any electronic society is a distributed denial of service attack. Due to the resource constraint nature of mobile sensors, DDoS attacks have become a major threat to its stability. In this paper, we established a model of a structural health monitoring network, being disturbed by one of the most common types of DDoS attacks, the flooding attack. Through a set of simulations, we explore the scope of flood-based DDoS attack problem, assessing the performance and the lifetime of the network under the attack condition. To conduct our research, we utilized the Quality of Protection Modeling Language. With the proposed approach, it was possible to examine numerous network configurations, parameters, attack options, and scenarios. The results of the carefully performed multilevel analysis allowed us to identify a new kind of DDoS attack, the delayed distributed denial of service, by the authors, referred to as DDDoS attack. Multilevel approach to DDoS attack analysis confirmed that, examining endangered environments, it is significant to take into account many characteristics at once, just to not overlook any important aspect.

1. Introduction

Wireless sensor networks (WSNs) are becoming an increasingly growing topic of conversation both in the scientific world and outside of it. As WSN continues to expand, it opens the door to a lot of opportunities, but also to many challenges. Security concerns are the issues being often times brought up: besides the security threats, we have the issue of privacy and data sharing. Unfortunately, the rapid growth of WSN is not always accompanied by a rapid improvement of efficient security solutions, giving criminals new opportunities to explore this technology as new attack vectors. One of the most common and dangerous types of attack that takes place these days is a distributed denial of service (DDoS). Distributed denial of service attacks are defined as attacks launched from multiple ends of a wireless sensor network, towards a set of legitimate nodes, with the intent of exhausting their limited resources. DDoS attacks can take on many forms, depending upon the target system and objectives of the attacker, but they all have the same goal: these attacks

significantly affect the performance of the network and eventually lead to complete paralysis of network operation. As network devices proliferate, vulnerabilities could enable attackers to assemble a large number of nodes to use in such attacks. If the attack is powerful enough, sensors will fail in serving their functions normally, becoming unreachable, so even legitimate users cannot use them. While this intense strain is taking over devices, hacker can try to slip into the back door unnoticed. That is the reason why security needs to be backed into wireless sensor networks from the initial design phase; it needs to be built in as the foundation of WSN environments, with rigorous validity checks, authentication, and data verification, and all communication needs to be encrypted. In light of the importance of what sensors have access to, it is essential to understand their security risks.

However, practical experiments with distributed denial of service attacks are difficult, because the scope of attack sources spreads in a wide geographical area and experiments in the local network can be insufficient to illustrate the real situation. Moreover, DDoS attacks require plenty of

controlled devices and therefore make difficulties in getting a sufficient amount of infected and ready to attack machines under the laboratory conditions. Instead of performing the real execution of distributed DoS attacks, their examination can be done using different modeling methods and tools. Modeling allows making the estimation of the influence of different attack properties with less time and resource supplies. It provides a test-bed to evaluate the costs and consequences imposed by various attack scenarios and defenses.

As WSN is especially vulnerable against external and internal attacks due to its peculiar characteristics, it should comply with certain security requirements, such as confidentiality, integrity, and authentication, derived from the application context. However, deploying security in WSN is a complex and time-consuming process, which seeks to accommodate frequently competing factors, such as functionality, scalability, or simplicity. In such case, the multilevel analysis is essential: it provides a better understanding of the security threats problem and allows for examining it from miscellaneous points of view.

In this paper, we contribute to solving the problem of the analysis of wireless sensor network environments, which struggle with flood-based distributed denial of service attack. The main contributions of this paper are summarized as follows:

- (1) We performed a multilevel analysis, in which we examined the influence of the number of compromised sensors on sink's performance. To conduct our research, we prepared and implemented distributed denial of service model in Quality of Protection Modeling Language (QoP-ML) [1], to be able to analyze how different properties of the attack influence its success probability.
- (2) An approach proposed in this paper was utilized in a case study of structural health monitoring of historical buildings, which represents critical systems, which need constant and careful monitoring. Through a set of performed simulations, we determined the energy consumption of wireless sensors deployed in critical points of the building structure, disturbed by a DDoS attack. Further, we estimated the lifetime of a base station, identifying another aspect of the multilevel analysis: the influence of DDoS attack on energy resource exhaustion, defining a new kind of DDoS attack, *DDDoS*, defined by the authors as the *delayed distributed denial of service attack*.
- (3) Another contribution of this paper is the QoP-ML model of WSN under the DDoS attack, prepared for our case study. This model can be used for testing how well existing mitigation methodologies perform and how they can be improved to prevent DDoS occurrence. With the proposed approach, we can systematically investigate and characterize how to provide denial of service defenses at the lowest (performance, energy, and finance) cost, satisfying the availability of network connections during the attack and assuring defined security objectives at the same time.

The multilevel analysis utilized in this paper is an innovative and unique evaluation method, which allows for taking into account not only sink's performance, but also the energy consumption. Using Quality of Protection Modeling Language, we are able to build a single model and consider it in many terms, such as the quality of protection, effect on the environment, or the influence on financial and economic performance. In this paper, we focus on time and energy consumption analyses.

The remainder of this paper is divided into six sections. In Section 2, we include the related work about distributed denial of service modeling. We try to compare our approach to those available in the literature, briefly discussing Quality of Protection Modeling Language. Moving on to Section 3, we examine an example network architecture and its components and dynamics, together with describing the most essential elements of analyzed environment. Turning on to Sections 4 and 5, we focus on modeling, simulation, and analysis of gathered results and conclude with Section 6, in which we summarize our work.

2. Related Work

The problem of distributed denial of service attacks is not new to the literature. However, every published view of this type of attack is somewhat different. Some authors examine the denial of service attacks from the OSI or TCP/IP reference models point of view [2–4] providing a comprehensive taxonomy of DDoS attacks [5–7]. Others try to use miscellaneous modeling tools to analyze distributed denial of service [8–11], while some focus on detection and mitigation techniques [12–15].

Although the literature on DDoS is more than rich, only a few authors consider formal modeling of DDoS attacks in wireless sensor networks [15–19]. To compare and organize all the existing approaches to denial of service formal modeling, we prepared a set of requirements which, if met, allow for an in-depth and detailed analysis of proposed methods in terms of their usefulness and efficiency. The modeling approach, to be considered a valuable, functional, and effective framework, should possess defined set of qualities. In Table 1 we investigated different approaches available in the literature and assessed them taking into account selected attributes. A proposed set of modeling qualities along with their explanations are presented below:

- (i) *Analytical Representation (AR)* refers to the mathematical representation of the model, defines if the model is represented in mathematical and analytical ideas (providing logical relationships and formulas), and moreover specifies the capability of being executed and support of automated tools being able to execute the model.
- (ii) *Universality (U)* determines if the given approach is a general purpose approach (can be utilized for building and analyzing models not only of wireless sensor networks).
- (iii) *Performance Evaluation (PE)* gives the possibility of performance evaluation of the analyzed system.

TABLE 1: Comparison of existing DDoS modeling approaches.

Approach	Characteristic							
	AR	S	PE	F	MA	C	SCL	EE
Dines Kumar and Navaneethan [15]	✓	—	✓	✓	—	✓	✓	✓
Chen et al. [16]	✓	✓	✓	—	—	✓	✓	—
Eian and Mjølunes [17]	✓	✓	✓	—	—	✓	✓	—
Dini and Tiloca [18]	✓	—	✓	✓	—	✓	✓	—
Zhang et al. [19]	✓	—	✓	—	—	✓	—	✓
QoP-MLs approach	✓	✓	✓	✓	✓	✓	✓	✓

- (iv) *Flexibility (F)* concerns the ease of adaptation to introduced changes; modeling approach is considered *flexible* if changes in real environment can be easily applied to existing models.
- (v) *Multilevel Analysis (MA)* allows taking into account lots of different attributes, components, and aspects of the considered system during the modeling process.
- (vi) *Consistency (C)* stands for the ability to model the system maintaining its states and communication steps consistency.
- (vii) *Scalability (SCL)* is the capability of an approach to handle a growing amount of model components, or its potential to be enlarged in order to accommodate that growth. The approach is *scalable* if it allows analyzing architectures of any size.
- (viii) *Energy Evaluation (EE)* allows for evaluation of the of energy efficiency of the analyzed system.

In [15] authors proposed an algorithm for *incorporated cryptographic mechanism and clustering method for preventing DoS attacks*. Due to the fact that the mechanism is described in a form of organized steps, it satisfies the *Analytical Representation* criteria. In the paper, researchers do not mention if it is possible to use proposed mechanism in different environments (hence, it does not pose the *Universality* requirement). In their work, scientists present performance results (*Performance Evaluation*), mentioning the *Energy Evaluation* as well. Their approach is *flexible*, *scalable*, and *consistent*, but it is not entirely *Multidimensional* (for instance, it does not take into account economic or ecological point of view and considers only a limited set of network characteristics).

Building a DDoS attack cost model based on mathematical equations, authors in [16] answered questions about *Analytical Representation* and *Consistency*. Presenting simulation results, they discuss *Performance Evaluation*; however, they do not say a word about *Energy Evaluation*. Proposed approach can act as a general purpose approach (can be implemented in any type of network), since it relies on numerical results (*Universality*). However, due to the fact that the model requires much computation, it is quite *inflexible*. When it comes to *Multilevel Analysis*, research introduced in [16] considers only defined group of examined variables. Numerical representation of the model makes it *scalable*.

When it comes to formal DDoS modeling methods, in [17] scientists proposed a formal method for modeling semantic DoS attacks against wireless networks and showed

how the model can be used to discover protocol vulnerabilities. Their approach relies on formal description and analysis (*Analytical Representation*). The method is *scalable*; however, it is quite *inflexible* (due to its formalism and accuracy). The authors consider *Performance Evaluation* and introduce the cost model but do not mention *Energy Evaluation*. Same as in the case of previously discussed works, *Multilevel Analysis* is also not satisfied.

Since an approach introduced in [18] provides an attack specification language, compiler, and simulator, it automatically satisfies the *Analytical Representation* criteria. (Because the model is defined as a set of logical rules (algorithms), it can be considered as *Analytically Represented*.) However, the solution presented in [18] does not pose the *Universality* characteristic, because it is designed only for wireless sensor networks. It is noteworthy that using *ASF* it is quite straightforward to make changes in the existing model (*Flexibility*), as well as handling its growth (*Scalability*). Regarding *Multilevel Analysis*, [18] does better than remaining approaches; however, it does not cover all the demands that a real deployment environment would require.

Another approach which makes use of algorithms is presented in [19] (*Analytical Representation*). Here, the authors proposed a novel Message Observation Mechanism (MoM) for preventing DoS attacks. This mechanism utilizes a similarity function which is based on spatiotemporal correlation for identifying the frequency attacks and content attacks. Nevertheless, in the article, researchers do not give all mechanisms of reroute and rekeys, making the approach *unscalable* and *inflexible*. Although the authors mention *Energy Evaluation* (and *Performance Evaluation*), they do not refer to other analysis dimensions (*Multilevel Analysis*). Because proposed mechanism is designed for wireless sensor networks, it does not meet the *Universality* requirement.

Although different approaches to distributed denial of service attack exist, there still is a lack of composite denial of service attack model that combines various types of resource exhaustion for a more realistic representation of an attack. Systematic, standardized, and organized methodologies should be appointed to detect, defend, and mitigate against denial of service attacks. A multidimensional, profound analysis, which allows examining miscellaneous aspects of an attack using logical formulas, is the most reliable approach to deal with DDoS. To the best of the author's knowledge, Quality of Protection Modeling Language (QoP-ML), introduced in [20], is the only existing modeling

language which satisfies all these requirements simultaneously. It allows for balancing security against the system efficiency, performing multicriteria analysis and extending the possibility of describing the state of the environment in detail (*Analytical Representation*). Quality of Protection Modeling Language permits determining the required quality of protection (QoP) and adjust some of the security measures to these requirements, together with ensuring efficient system performance (*Performance Evaluation*). This type of profound analysis can be accomplished by the help of the Automated Quality of Protection Analysis tool [1] (*Flexibility, Scalability*), which allows for the evaluation of the impact of every single operation defined in the prepared security model in terms of the overall system security. Additionally, in previous works, there were proposed and examined approaches which were successful also in assessing time, energy (*Energy Evaluation*), quality of protection, financial expenditures, and impact on the environment of the analyzed IT environments at the same time. Building a network model in Quality of Protection Modeling Language, one is able to take into account type of the device (thanks to the possibility of using real hardware performance metrics, one can actually use any type of device), communication medium type and its characteristics, network topology, packet flow (routing) (*Multilevel Analysis*) and examine how all these components combined together in different configurations can influence DDoS success probability.

For additional information about QoP-ML itself, its syntax, semantics, algorithms, and capabilities, please refer to [20, 21].

3. Flood-Based Denial of Service Attack Analysis

In this section, we describe a conventional DDoS attack tactic, in which an attacker floods targeted resource with packets. We propose an example network architecture along with scenarios, where we launch a DDoS attack, a type of malicious activity aimed at disrupting the availability of a sink so it can no longer deliver its functionality.

Further, we present and discuss prepared environment in detail, providing more concise representation of utilized devices, routing, medium, network architecture, and topology.

Distributed denial of service flooding attacks are one of the biggest concerns for security professional. They are typically explicit attempts to disrupt legitimate nodes' access to a sink node. The attackers usually gain access to a large number of sensor devices, by exploiting their vulnerabilities to set up attack armies. Once an attacking army has been set up, an attacker can invoke a coordinated, large-scale attack against one or more gateways. A flooding-based distributed denial of service attack sends a large amount of unwanted traffic to a victim sink. This results in consuming large amounts of its resources in order to maintain a very large list of connections, eventually leading to the device running out of resources and becoming unable to provide normal services. In the case of flood-based DDoS attack, the attacker must be in control of

a large number of nodes which can be instructed to execute specific requests to the target sink, in a synchronized manner and for a specific period of time. The so-called "bots" are compromised sensors, used by the attacker. Once a trigger is sent from the attacking node, the bots will execute the designated requests and the attacker will rely on the sheer number of requests/second to bring the sink's processing power to its knees, causing it to cease responding to legitimate sensors. The existence of a vulnerability is not a precondition of this type of attack, in the sense that the attack does not rely on vulnerabilities to execute. However, controlling a large "army" of bots usually implies exploiting vulnerabilities.

For a more concise representation of our approach to DDoS attack analysis, we proposed expressing it through a set of key points, on which we elaborate in the following sections.

3.1. Utilized Protocols. The network deployed in [22] is an example of an insecure network, as it does not ensure any security attributes; packets traversing the network are unencrypted. In our case study, we intend to evaluate the influence of security attributes on the performance of the network, from the time and energy point of view. We introduced two protocols, which guarantee two different levels of security: *no security* (with no encryption) and *security* (where we use AES to encrypt the data).

In the *no security* level protocol, sensors start measurement and send the acceleration data (the result of the measurement) to the sink node for further processing. In this protocol level, no security attributes are guaranteed.

The *security* level protocol introduces confidentiality of accelerated data. After measurement, sensors encrypt the data with a predeployed network key. In this protocol, the AES algorithm is chosen for the encryption in the CTR (CTR stands for *counter* and represents a mode of operation, which uses a block cipher to encrypt messages of arbitrary length in a way that provides confidentiality or authenticity) mode and with the key size equal to 128 bytes.

3.2. Network Architecture and Topology. For example, hypothetical deployment of wireless sensors inside a heritage building, which we examine in this paper, is pictured in Figure 1. Our example network is based on the one presented in [22]. Here, wireless sensors, located in critical points of the building structure, measure required physical quantities (such as vibrations, temperature, or humidity). Data collected by nodes flow into the base station where further data compression and analysis are performed. In such a network architecture, the sink node is a bottleneck and a single point of failure. Proper operation of the base station is crucial for the entire network. Once the sink node fails, the whole network will be paralyzed. In our simulation scenarios, we distinguished 3 types of sensor nodes: compromised sensors, sink node (also known as the gateway or base station), and attacker node. Because the function of legitimate sensors is to take the measurements and send the data to the base station several times during an hour, their operation does not influence much DDoS attacks which last for a few minutes. Due to the fact that the traffic they generate is quite

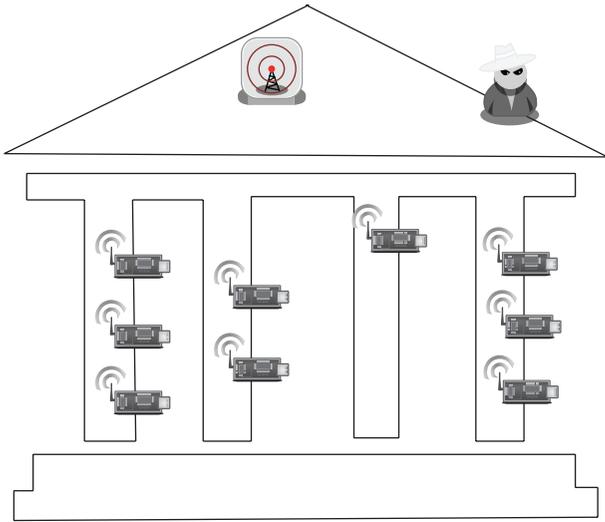


FIGURE 1: Example network considered for a distributed denial of service attack model.

imperceptible from DDoS attack point of view, we decided to focus only on compromised nodes, the sink node, and the attacker node preparing our model. In order to obtain realistic results, we assumed that all the utilized sensors (compromised sensors, sink node, and the attacker) are TelosB devices, equipped in two AA batteries with 1200 mAh capacity [23]. Because of the flexibility of the QoP-ML, we managed to use the real hardware performance metrics and physical attributes of TelosB nodes and even model its power consumption characteristics.

3.3. Data Flows and Routing. While the primary purpose of a sensor node is data sensing and gathering toward a base station through wireless communication, each of them also has limited processing capabilities that may be exploited, as in the case of an attack. During a normal network operation, sensors continuously monitor the environment, gather relevant data, and send it to the gateway. Data collected from all sensor nodes is uploaded to a sink node and further processed. Considering the attack scenario, network traffic and packet flows increase: attacker takes control of the available sensors (legitimate sensors then become compromised ones) and uses them to generate flooding traffic in order to exhaust sink resources and consequently disturb the whole network. The aggressor knows that if the sink node fails, the entire network will be paralyzed. In our model, we assumed that the attacker communicates with compromised sensors and after every 10 seconds broadcasts a flood message to the devices which he controls. Nodes controlled by the attacker in an infinite loop listen for incoming requests (the flood orders) and flood sink with useless messages. Although there is only one packet in each flood wave, attack's power is hidden in the number of compromised sensor devices. It is considered that structural health monitoring network consists of 200 devices. In our simulations, the attacker takes control of 150 (scenarios 1 and 2), 100 (scenarios 3 and 4), 75 (scenarios 5 and 6), and 50 (scenarios 7 and 8)

sensors. During the first flood wave, each sensor sends a single packet to the base station (which results in 150, 100, 75, and 50 packets in total). When the attack escalates, the number of send packets increases, respectively, (resulting in $\text{flood wave number} \times \text{number of compromised sensors}$ packets). The more devices attacker has under his control, the more powerful attack is generated.

As for routing information, considered network is a single-hop wireless network in which each station can transmit or communicate directly with the sink node.

3.4. OSI Layers and Protocols. Network and transport layer DDoS attacks can be carried out on a wired or wireless network. The majority of DDoS attacks target the network and transport layers. Such attacks occur when the amount of data packets and other traffic overloads a network or server and consumes all of its available resources. For this reason, during analysis, we focus on layer 3 and layer 4 DDoS attacks, because they are types of volumetric DDoS attacks on a network infrastructure. Layer 3 DDoS (network layer) and layer 4 DDoS (transport layer) attacks rely on extremely high volumes (floods) of data to slow down sink performance, consume bandwidth, and eventually degrade access for legitimate sensors. Our DDoS attack analysis does not refer to a specific protocol but can be applied to all protocols running on the network and transport OSI layers.

3.5. Communication. As mentioned before, the network presented in Figure 1 is a wireless network. Here, all the existing sensor devices use same communication channels to communicate, and the message broadcasted by one of the nodes on the common channel is simultaneously heard by all other nodes. In our environment, we consider two air channels: one of them is used by the attacker and compromised nodes, while the other one is responsible for the communication of compromised nodes and a sink node. As the sink node must have some mechanisms to store and forward arriving requests, we assumed that it is equipped with a communication buffer, which is capable of storing a defined number of packets. Sink uses available communication channels to continuously wait for incoming data packets. These packets can be send as a plain text or can be encrypted. When the buffer on the specific channel is full, and there are still requests to handle, they are simply dropped. Under certain conditions, overflow of sink's buffer indicates that the denial of service occurred.

4. DDoS Attack Model in Quality of Protection Modeling Language

Examining a DDoS attack in Quality of Protection Modeling Language, we prepared the model of wireless sensor network discussed above, gathered and utilized real hardware security metrics, and developed different versions of the proposed scenario (Table 2). Modeling DDoS attack, we defined QoP-ML's functions, equations, channels, processes, subprocesses, and hosts. Prepared scenarios (and thus the QoP-ML's security model designed and used in our case

TABLE 2: Scenarios prepared for DDoS detection and analysis. Considered WSN consists of 200 nodes in total.

Scenario number	Sink type	Buffer size	Number of compromised sensors	Communication type
1	TelosB	192	150	Encryption: AES-CTR 128-bit key
2	TelosB	192	150	No encryption
3	TelosB	192	100	Encryption: AES-CTR 128-bit key
4	TelosB	192	100	No encryption
5	TelosB	192	75	Encryption: AES-CTR 128-bit key
6	TelosB	192	75	No encryption
7	TelosB	192	50	Encryption: AES-CTR 128-bit key
8	TelosB	192	50	No encryption

study) can be downloaded from QoP-MLs project web page [1].

After a brief introduction of the network components and existing traffic flows presented in the previous section, let us now move on to the utilization of our modeling framework, where we discuss abstracted environment in more detail.

4.1. Network Architecture and Topology. Modeling considered network architecture in QoP-ML, we distinguished 3 types of `host` structures, namely, `sink`, `attacker`, and `compromised sensor`. Using one of the QoP-MLs features, known as security metrics, we were able to determine how hardware specifications influence system performance in the case of DDoS attack. We assumed that all sensor nodes (`sink`, `attacker`, and `compromised sensors`) have exact hardware characteristics, taken from TelosB datasheet [23] and previous experiments [24]. Using the `communication` module introduced in [25], we were able to translate existing network topology to QoP-ML as well.

When legitimate sensor becomes an intruder (Listing 1), its main role is to continuously wait for flood orders from the attacker (line (9)). When compromised sensors receive a flood command from an attacker (line (13)), they prepare data (lines (15)-(16)) and depending on the command type included in the message (lines (26)-(34)) generate useless messages (lines (23)-(24)) to flood sink (lines (27) and (33)). Special command type send by the attacker indicates that sensors should stop communicating with sink (lines (36)-(37)). Compromised sensors are also able to encrypt data before transmission (lines (18)-(21)). Such a solution allows determining how this cryptographic process influences attack success probability and assesses how well utilized security mechanisms perform.

Attacking node, modeled in QoP-ML, is presented in Listing 2. It is a special type of device, which, by means of the `mgmt` channel, communicates with compromised nodes. The role of the attacker is to generate a flood command (lines (9)-(21)) and send it through the `mgmt` channel to the compromised mote (lines (11) and (20)). After receiving a flood order from the attacker, compromised sensors start to flood the network with useless traffic. When the attack is

```

(1) host CompromisedSensor(rr)(*)
(2) {
(3)
(4) #MY_ID = id();
(5) #Attacker_ID = id(Attacker);
(6) #SINK_ID = id(Sink);
(7) #KEY = nonce();
(8)
(9) process MainProcess(*)
(10) {
(11) while(true)
(12) {
(13) in(ch_MGMT: MESSAGE: |*,*|);
(14)
(15) DATA = collected_data() [UPDATED];
(16) save_collected_data(DATA) [UPDATED];
(17)
(18) subprocess EncCollectedData(*) {
(19)   DATA = (DATA, nonce());
(20)   DATA = s_enc(DATA, KEY) [AES-CTR,128];
(21) }
(22)
(23) DATA_MSG = (MY_ID, SINK_ID, data_msg(),
(24)   non_legit(), DATA);
(25)
(26) if(MESSAGE[2] == msg_flood1()){
(27)   out(ch_WSN: DATA_MSG);
(28) }
(29)
(30) %...
(31)
(32) if(MESSAGE[2] == msg_flood6()){
(33)   out(ch_WSN: DATA_MSG);
(34) }
(35)
(36) if(MESSAGE[2] == msg_stop()){
(37)   break;
(38) }
(39) }
(40) }
(41) }

```

LISTING 1: Compromised sensor node modeled in QoP-ML.

```

(1) host Attacker(rr)(*)
(2) {
(3)   #MY_ID = id();
(4)   #SENSOR_ID = id(CompromisedSensor);
(5)   #KEY = nonce();
(6)
(7)   process MainProcess(*)
(8)   {
(9)     subprocess FirstFloodWave(*){
(10)      FLOOD_MSG = (MY_ID, SENSOR_ID, msg_flood1());
(11)      out(ch_MGMT: FLOOD_MSG);
(12)      wait()[UPDATED];
(13)    }
(14)
(15)    %...
(16)
(17)    subprocess SixthFloodWave(*){
(18)      FLOOD_MSG = (MY_ID, SENSOR_ID, msg_flood6());
(19)      out(ch_MGMT: FLOOD_MSG);
(20)      wait()[UPDATED];
(21)    }
(22)
(23)    STOP_MSG = (MY_ID, SENSOR_ID, msg_stop());
(24)    out(ch_MGMT: STOP_MSG);
(25)  }
(26) }

```

LISTING 2: Attacker node modeled in QoP-ML.

over, attacker informs compromised nodes that they can stop sending messages (lines (23)-(24)).

Sensor, which is subject to a DDoS attack, is modeled in Listing 3. Its function is to handle incoming requests (line (10)), preserve (lines (12)-(13)), and finally process them (line (20)). When the data coming to sink both from compromised nodes is encrypted, before processing, sink decrypts data packets (lines (15)-(18)).

Further information about the definition of hosts, processes, and subprocesses structures can be found in [20].

Security metrics utilized in our scenarios concern communication (electric currents in one of the possible node states: listening, sending, and receiving), cryptographic primitives (symmetric and asymmetric encryption), and CPU type. With QoP-ML's metrics it is possible to take into account different hardware characteristics during the simulation process. Such a feature lets one to examine how they influence network performance under an attack. Metrics used by our model are presented in Listing 4. Here we specify the encryption/decryption algorithm, its key characteristics (lines (6)-(10)), and the current of the utilized CPU (lines (12)-(13)). Additional details on security metrics can be found in [20].

Besides defining hardware characteristics, QoP-ML allows for expressing topology of the considered network

```

(1) host Sink(rr)(*)
(2) {
(3)   #MY_ID = id();
(4)   #KEY = nonce();
(5)
(6)   process MainProcess(*)
(7)   {
(8)     while(true)
(9)     {
(10)      in(ch_WSN: DATA_MSG: |*, *, data_msg());
(11)
(12)      DATA = DATA_MSG[4];
(13)      save_collected_data(DATA)[UPDATED];
(14)
(15)      subprocess DecCollectedData(*) {
(16)        DATA = s_dec(DATA, KEY)[AES-CTR,128];
(17)        DATA = DATA[0];
(18)      }
(19)
(20)      process_data(DATA)[UPDATED];
(21)    }
(22)  }
(23) }
(24) }

```

LISTING 3: Sink node modeled in QoP-ML.

```

(1) metrics {
(2)   conf (TelosB) {
(3)     CPU = 16-bit 8MHz TI MSP430;
(4)   }
(5)   data(TelosB) {
(6)     primhead[function] [alg] [key_size] [time:block(ms,B)]
(7)       [size:ratio];
(8)     primitive[s_enc] [AES-CTR] [128] [1:34:16] [1:1];
(9)     #
(10)    primhead[function] [alg] [key_size] [time:block(ms,B)]
(11)      [size:nested];
(12)    primitive[s_dec] [AES-CTR] [128] [1:34:16] [1:1];
(13)    #
(14)    primhead[function] [current:exact(mA)];
(15)    primitive[cpu] [2.4];
(16)    % ...
(17)  }
(18) }

```

LISTING 4: Security metrics related to cryptographic primitives (symmetric and asymmetric encryption), obtained for TelosB.

```

(1) communication {
(2)   medium[wsn] {
(3)     % ...
(4)     topology {
(5)       Sink <- CompromisedSensor;
(6)     }
(7)   }
(8) }

```

LISTING 5: Topology for WSN communication channel.

```

(1) communication {
(2)   medium[mgmt] {
(3)     % ...
(4)     topology {
(5)       Attacker -> CompromisedSensor;
(6)     }
(7)   }
(8) }

```

LISTING 6: Topology for MGMT communication channel.

for the specific medium (Listing 5). From Listing 5 one can easily deduce that the sink node communicates with both compromised nodes (Listing 5, lines (4)–(6)), and attacker exchanges information with compromised devices too (Listing 6, lines (4)–(6)). Article [25] provides a detailed view of the topology structure.

4.2. Data Flows and Routing. By specifying the communication structure (Listings 5 and 6), it is possible to translate

not only the topology of the network, but also packet flows. Defining direction of the arrowheads in the topology structure, one is able to map the existing packet flows onto an abstract model and precisely specify the movement of the network traffic. Topology represented in Listing 5 indicates that on a wsn channel packets can be sent from the sink node to compromised nodes. Concerning mgmt communication channel, it is used only by the attacker and compromised nodes (Listing 6). With the help of this channel attacker instructs compromised nodes to flood the base station. Details about the communication structure are available in [25].

4.3. OSI Layers and Protocols. Protocol implemented and tested in our scenarios refers to network and transport OSI layers. Designed protocol consists of only one communication step. Its operation is quite simple: compromised nodes, instructed by the attacker, send data messages to sink in order to flood it with useless packets.

4.4. Communication. In listing 7 one can find a definition of the communication structure for one of the communication channels used by the modeled network. Here one can specify a set of parameters, like the quality of the channel (line (4)), default transmission time (line (5)), calculated by the algorithm presented on Listing 9, together with default listening (line (6)), and sending (line (7)) and receiving (line (8)) current values. Details about the algorithm from Listing 9 can be found in [25].

The communication between interconnected devices is modeled by means of channels: sink's ability to store specified number of incoming packets was translated to the size of the buffer given for the specific communication channel (Listing 8). Any type of data can be passed through these channels. Due to the fact that ch.MGMT(*) is used only by the attacker to control zombie armies, it acts as the management channel;

```

(1) communication {
(2)
(3)   medium[wsn] {
(4)     default_q = 1;
(5)     default_time = wsn_time [ms];
(6)     default_listening_current = 0.02 mA;
(7)     default_sending_current = 17.4 mA;
(8)     default_receiving_current = 19.7 mA;
(9)
(10)    % ...
(11) }

```

LISTING 7: TelosB electric characteristics.

```

(1) channels
(2) {
(3)   channel ch_WSN(192) [wsn];
(4)   channel ch_MGMT(*) [mgmt];
(5) }

```

LISTING 8: Utilized communication channels.

there is no limit for message passing by this channel (line (4)). Since in our analysis we focus on volumetric DDoS attacks, which are simply about causing congestion, we needed to model the other channel as a medium with fixed buffer size, to examine its potential overflow. From TelosB datasheet [23] we know that this device is equipped with 48 K bytes of program flash memory, 1024 K bytes of measurement serial flash, and 10 K bytes of RAM. In order to perform our simulations in timely and effective manner, we reduced the message buffer accordingly, in a way that it is capable of storing the maximum of 192 messages and provides asynchronous communication (line (3)). When 192 packets on `ch_WSN` channel are waiting to be processed, its buffer is considered to be full. It means that additional, incoming requests cannot be handled and are, as a result, dropped.

Article [20] contains more information about message passing and the logic of channel's buffer.

5. Multilevel Attack Assessment: Simulation, Results Analysis, and Algorithms

In this section, we describe our simulation environment, mention utilized software, and present detailed results for each of the defined scenarios. In short, the multilevel analysis performed here focuses on many various aspects of the examined problem at once. This means that, during a single analysis, we are able to take into account many different factors at the same time (network architecture and topology, data flows and routing, utilized protocols, and communication and security mechanisms) and examine results in terms of time, energy consumption, financial expenditures, or environmental impact. The metrics utilized here refer to time

and energy consumed during the accident, incurred costs (related to the time when the infrastructure could not deliver its services), and the influence on environment.

To examine network performance with different number of compromised, attacking nodes, we implemented 8 scenarios, which are known as *versions* in QoP-ML's nomenclature. Our tests were taken with fully automated tool, designed for the analysis of cryptographic protocols (AQoPA). The selection of the utilized tool was dictated by previous works. In [24, 26, 27], credibility and reliability of the results gathered for internet protocols (TLS, Kerberos) and WSN protocols, modeled with QoP-ML, were carefully inspected and finally verified. Both the model and the AQoPA tool can be downloaded from the web page of the QoP-ML project [1].

5.1. DDoS Attack Evaluation. During analyses performed in this paper, we focused on the percentage of dropped packets in each flood wave and the time taken by the sink to handle incoming packets. Detailed simulation results are presented in Tables 3 and 4.

Gathered results indicate that utilized security mechanisms significantly affect sink's performance. Considering the results obtained for scenarios with packet encryption (scenarios 1, 3, 5, and 7), it is clear that the number of compromised devices has a meaningful impact on DDoS success probability. This relationship is the result of the percentage of dropped packets in each flood wave. As it can be seen from Tables 3 and 4, the more devices the attacker has under his control, the faster the DDoS occurrence. Consider, for instance, scenarios 7 and 8. Here, 50 compromised sensors flood sink with useless messages. With unencrypted traffic, there are any dropped packets (scenario 8). However, when the traffic is encrypted (scenario 7), sink starts dropping packets in 5th flood wave. With 75 compromised sensors, normal network operation is possible until the 5th flood wave for unencrypted traffic and 2nd flood wave for encrypted traffic. When the number of controlled motes increases to 100, distributed denial of service can be observed in 3rd and 2nd flood waves (for unencrypted and encrypted traffic, resp.). The attacker, who has the greatest number of motes (150) under his control, has the most powerful weapon to bring down the whole network; it can cause denial of service generating only 2 flood waves (Figures 2 and 3).

Sink's service time increases with the number of compromised devices as well. Comparing data only for first flood waves in each scenario, one can observe that the time needed by the sink to handle incoming requests extends with the number of motes controlled by the attacker, for both encrypted and unencrypted traffic.

5.2. Multilevel Analysis of DDoS Attack. Besides the performance, we also considered the energy consumed by the sink and estimated its lifetime under the DDoS attack. An interesting conclusion can be drawn from the results of the consumed energy. As it can be seen from Tables 3 and 4, when sink deals with encrypted traffic, it consumes more energy than handling unencrypted packets. It is worth noticing that the number of the flood wave has an impact on the percentage of dropped packets when considering encrypted traffic but

```

(1) algorithms {
(2)   alg wsn_time(msg) {
(3)     msg_size = size(msg[3]);
(4)     xtime = 0;
(5)     while (msg_size > 0) {
(6)       sending = 18;
(7)       one_size = 110;
(8)       if (msg_size < one_size) {
(9)         one_size = msg_size;
(10)      }
(11)      transmitting = one_size * 0.12;
(12)      xtime = xtime + sending + transmitting;
(13)      msg_size = msg_size - 110;
(14)    }
(15)    return xtime;
(16)  }
(17) }

```

LISTING 9: Algorithm used for calculating the packet transmission time in utilized air channels.

TABLE 3: Detailed simulation results for scenarios 1–4.

Scenario number	Flood wave number	Dropped packets [%]	Time taken by sink to handle incoming packets [s]	Energy consumed by sink [J]	Sink's lifetime [days]
1	1	0	371.45	604.76	21.42
1	2	34	486.79	607.01	21.35
1	3	55	496.61	607.18	21.34
1	4	66	506.43	607.35	21.33
1	5	72	516.24	607.53	21.33
1	6	76	526.06	607.68	21.32
2	1	0	37.68	481.52	26.91
2	2	22	58.15	505.17	25.65
2	3	39	68.14	507.19	25.55
2	4	47	78.13	508.69	25.47
2	5	52	88.13	509.79	25.42
2	6	56	98.12	510.72	25.37
3	1	0	248.74	600.91	21.56
3	2	2	486.79	607.01	21.35
3	3	33	496.61	607.18	21.34
3	4	49	506.43	607.35	21.33
3	5	58	516.24	607.53	21.33
3	6	65	526.06	607.68	21.32
4	1	0	25.49	474.53	27.31
4	2	0	49.86	502.52	25.78
4	3	8	68.14	507.19	25.55
4	4	21	78.13	508.69	25.47
4	5	29	88.13	509.79	25.42
4	6	34	98.12	510.72	25.37

TABLE 4: Detailed simulation results for scenarios 5–8.

Scenario number	Flood wave number	Dropped packets [%]	Time taken by sink to handle incoming packets [s]	Energy consumed by sink [J]	Sink's lifetime [days]
5	1	0	187.39	599.39	21.62
5	2	0	371.45	604.76	21.42
5	3	11	496.61	607.18	21.34
5	4	32	506.43	607.35	21.33
5	5	44	516.24	607.53	21.33
5	6	53	526.06	607.68	21.32
6	1	0	19.4	445.36	29.1
6	2	0	37.68	481.52	26.91
6	3	0	55.95	494.15	26.22
6	4	0	74.23	500.49	25.89
6	5	5	88.13	509.79	25.42
6	6	12	98.12	510.72	25.37
7	1	0	126.03	589.57	21.98
7	2	0	248.74	600.91	21.56
7	3	0	371.45	604.76	21.42
7	4	0	494.16	606.70	21.36
7	5	16	516.24	607.53	21.33
7	6	29	526.06	607.68	21.32
8	1	0	13.3	454.73	28.5
8	2	0	25.49	474.53	27.31
8	3	0	37.68	481.52	26.91
8	4	0	49.86	502.52	25.78
8	5	0	62.05	501.27	25.85
8	6	0	74.23	500.49	25.89

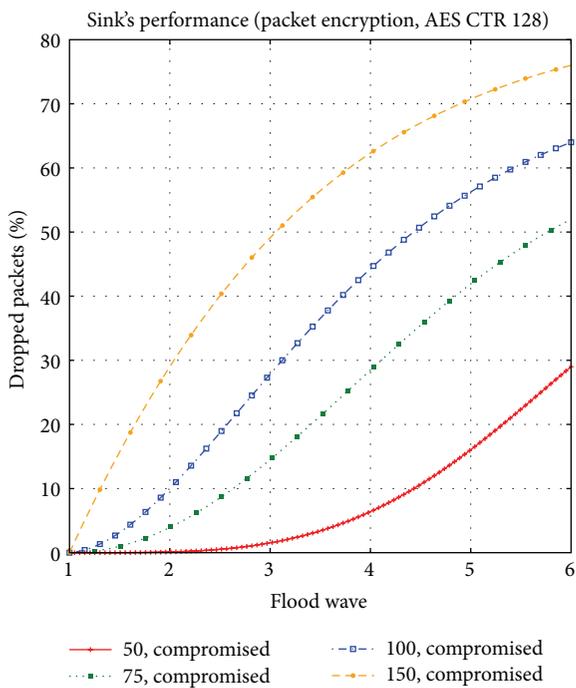


FIGURE 2: Percentage of dropped packets in each flood wave. Data is encrypted with AES in CTR mode with 128-bit key.

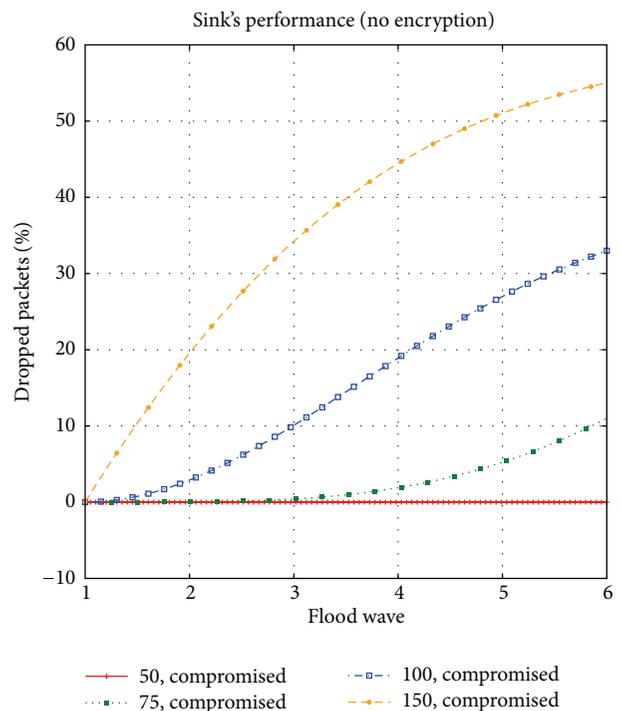


FIGURE 3: Percentage of dropped packets in each flood wave. Data is unencrypted.

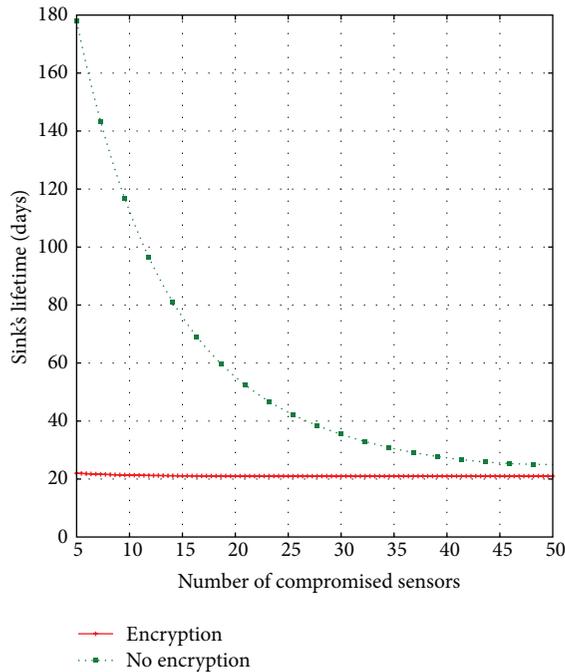


FIGURE 4: Sink's lifetime for encrypted and unencrypted traffic.

does not affect much the consumed energy. The difference in joules between flood waves in encrypted communication (scenarios 1, 3, 5, and 7) is quite small. Regarding scenarios with nonencrypted data (2, 4, 6, and 8), we presume that it is still possible to bring down the sink, exploiting another aspect of the network, namely, energy resources. Although the gateway copes better with plain packets than encrypted ones when it comes to the number of dropped messages, it fails to resist the attack on energy resources. Obtained results indicate that when compromised sensors continuously flood sink with unencrypted packets, the attack can be undetected by defense mechanisms (because there is no dropped packets) but still can be dangerous, as it reduces the sink's lifetime severely. Consider, for instance, scenario 6, where dropped packets can be observed in 5th flood wave, but the actual attack on energy resources should be noticed and prevented after the first flood wave to stop undesirable resource consumption. To confirm our assumptions, we performed another set of simulations, with less than 50 compromised devices, namely, 5, 10, 15, 20, 25, 30, 35, 40, and 45. We examined the lifetime of the sink node being flooded with useless messages by the mentioned number of sensors with different security mechanisms applied. The influence of DDoS attack on the energy consumed by the sink, which can be further considered as the lifetime prediction, can be observed in Figure 4.

Results available in Figure 4 clearly state that even with unencrypted traffic it is possible to induce a DDoS attack. This special type of DDoS attack is defined by the authors as the DDDoS attack (delayed distributed denial of service). With 5, 10, ..., 50 compromised sensors, for the considered network consisting of 200 devices in total, traditional DDoS defense mechanisms, which relies on the number of dropped

packets or the traffic volume, will fail. As it can be seen in Figure 4, if the sink node will be continuously flooded by 5 compromised sensors for 24 hours (by using only the sixth flood wave), its lifetime will be equal to about 21 and 180 days (for encrypted and nonencrypted traffic, resp.). However, when we increase the number of compromised devices to, for instance, 20 sensors, the lifetime of the sink will decrease to about 20 and 55 days (encrypted, nonencrypted). Introduced attack is a nasty kind of distributed denial of service attack, as it can decrease the lifetime of the sink node by slowly and imperceptibly consuming its valuable power, leading to total exhaustion of energy resources. The DDDoS attack is especially dangerous for WSNs, where the energy is one of the constrained resources. In most cases, due to the deployment in remote and hard to access locations, it is very difficult (costly and time-consuming) or even impossible to change the batteries for the sensor nodes. Eliminating the source of an attack is sometimes not enough: when the energy of a sensor reaches a certain threshold, the sensor will become faulty and will not be able to function properly, which will have a major impact on the network performance.

6. Conclusions

In the paper we presented the multilevel analysis of the DDoS attack problem. We defined 8 scenarios with two security levels (encryption/no encryption) and different number of compromised devices (50, 75, 100, and 150). Performing a set of simulations, we investigated the sink's performance and energy consumption under the DDoS attack. By examining the results gathered for prepared simulations, we identified a new kind of distributed denial of service attack, the DDDoS attack. Our analysis showed that although the packets traversing the network are not encrypted (meaning should be less harmful for the sink node in terms of its performance), they still can be dangerous and quietly imperceptibly bring down the whole network, exhausting valuable energy resources.

Another interesting conclusion can be drawn from the above analysis: depending on the type of the DDoS attack, it is possible to adjust the security level in order to prevent different types of attacks. Our simulations showed that, in certain conditions, by lowering security level, it was possible to avoid DDoS or delay its occurrence.

Using the multifaceted analysis approach supported by the Quality of Protection Modeling Language, it was possible to examine the performance of miscellaneous devices, by changing utilized security metrics, and consider gathered results on multiple levels, starting with time and energy consumption, through ecology and finance, ending at quality of protection. Existing frameworks focus on one aspect of an attack at once, while proposed approach is multilevel, thus being capable of examining different characteristics at the same time. The presented DDoS attack model can be further used for testing different attack mitigation methodologies.

Our future work is to focus on DDoS and DDDoS attacks and examine them in detail. We would like to build a scenario, in which we analyze a complex Internet of Things (IoT) network architecture and analyze its performance during the DDoS (and DDDoS) attacks.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

- [1] B. Ksiezopolski, "The official web page of the qop-ml project, 2012".
- [2] M. Dhar and R. Singh, "A review of security issues and denial of service attacks in wireless sensor networks," *International Journal of Computer Science and Information Technology Research*, vol. 3, no. 1, pp. 27–33, 2015.
- [3] G. Kumar, "Understanding denial of service (dos) attacks using osi reference model," *International Journal of Education and Science Research*, vol. 1, no. 5, 2014.
- [4] Isha, A. Malik, and G. Raj, "Dos attacks on tcp/ip layers in wsn," *International Journal of Computer Networks and Communications Security*, vol. 1, no. 2, pp. 40–45, 2013.
- [5] A. D. Wood and J. A. Stankovic, "A taxonomy for denial-of-service attacks in wireless sensor networks," in *Handbook of Sensor Networks Compact Wireless and Wired Sensing Systems*, M. Ilyas and I. Mahgoub, Eds., CRC Press, New York, NY, USA, 2004.
- [6] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39–53, 2004.
- [7] A. Asosheh and N. Ramezani, "A comprehensive taxonomy of DDoS attacks and defense mechanism applying in a smart classification," *WSEAS Transactions on Computers*, vol. 7, no. 4, pp. 281–290, 2008.
- [8] D. K. Chaitanya and G. Arindam, "Analysis of denial-of-service attacks on wireless sensor networks using simulation," in *Proceedings of the IT Security for the Next Generation—European Cup*, University of Applied Sciences, Erfurt, Germany, January 2011.
- [9] Q. Huang, H. Kobayashi, and B. Liu, "Modeling of distributed denial of service attacks in wireless networks," in *Proceedings of the IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*, pp. 41–44, Victoria, Canada, August 2003.
- [10] L. Pei, C. Li, R. Hou, Y. Zhang, and H. Ou, "Computer simulation of denial of service attack in military information network using opnet," in *Proceedings of the 3rd International Conference on Multimedia Technology (ICMT '13)*, 2013.
- [11] I. Mukhopadhyay, S. Polle, and P. Naskar, "Analysis of denial-of-service attacks on wireless sensor networks using simulation," *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 16, 2014.
- [12] R. Bhatnagar, "The proposal of hybrid intrusion detection for defence of sync flood attack in wireless sensor network," *International Journal of Computer Science & Engineering Survey*, vol. 3, no. 2, pp. 31–38, 2012.
- [13] S. Tripathy and S. Nandi, "Defense against outside attacks in wireless sensor networks," *Computer Communications*, vol. 31, no. 4, pp. 818–826, 2008.
- [14] J.-H. Son, H. Luo, and S.-W. Seo, "Denial of service attack-resistant flooding authentication in wireless sensor networks," *Computer Communications*, vol. 33, no. 13, pp. 1531–1542, 2010.
- [15] V. S. Dines Kumar and C. Navaneethan, "Protection against denial of service (dos) attacks in wireless sensor networks," *International Journal of Advanced Research in Computer Science & Technology*, vol. 2, no. 1, pp. 439–443, 2014.
- [16] L.-C. Chen, T. A. Longstaff, and K. M. Carley, "Characterization of defense mechanisms against distributed denial of service attacks," *Computers and Security*, vol. 23, no. 8, pp. 665–678, 2004.
- [17] M. Eian and S. F. Mjølunes, "The modeling and comparison of wireless network denial of service attacks," in *Proceedings of the 3rd ACM SOSP Workshop on Networking, Systems, and Applications on Mobile Handhelds (MobiHeld '11)*, October 2011.
- [18] G. Dini and M. Tiloca, "ASF: an attack simulation framework for wireless sensor networks," in *Proceedings of the IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '12)*, pp. 203–210, Barcelona, Spain, October 2012.
- [19] Y.-Y. Zhang, X.-Z. Li, and Y.-A. Liu, "The detection and defence of DoS attack for wireless sensor network," *The Journal of China Universities of Posts and Telecommunications*, vol. 19, no. 2, pp. 52–56, 2012.
- [20] B. Ksiezopolski, "QoP-ML: quality of protection modelling language for cryptographic protocols," *Computers & Security*, vol. 31, no. 4, pp. 569–596, 2012.
- [21] B. Ksiezopolski, *Multilevel Modeling of Secure Systems in QoP-ML*, CRC Press/Taylor & Francis, New York, NY, USA, 2015.
- [22] G. Anastasi, G. Lo Re, and M. Ortolani, "WSNs for structural health monitoring of historical buildings," in *Proceedings of the 2nd Conference on Human System Interactions (HSI '09)*, pp. 574–579, IEEE, Catania, Italy, May 2009.
- [23] Crossbow Technology, "TelosB mote platform datasheet," Document Part Number 6020-0094-01, rev B, 2004, <http://www.willow.co.uk/TelosB Datasheet.pdf>.
- [24] I. Mansour, D. Rusinek, G. Chalhoub, P. Lafourcade, and B. Ksiezopolski, "Multihop node authentication mechanisms for wireless sensor networks," in *Ad-Hoc, Mobile, and Wireless Networks: 13th International Conference, ADHOC-NOW 2014, Benidorm, Spain, June 22–27, 2014 Proceedings*, vol. 8487 of *Lecture Notes in Computer Science*, pp. 402–418, Springer, Berlin, Germany, 2014.
- [25] D. Rusinek, B. Ksiezopolski, and A. Wierzbicki, "Security trade-off and energy efficiency analysis in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID 943475, 17 pages, 2015.
- [26] B. Ksiezopolski, D. Rusinek, and A. Wierzbicki, "On the modelling of kerberos protocol in the quality of protection modelling language (QoP-ML)," *Annales UMCS, Informatica*, vol. 12, no. 4, pp. 69–81, 2012.
- [27] P. Szalachowski, B. Ksiezopolski, and Z. Kotulski, "Optimization of the TLS security protocol," *Annales UMCS: Informatica*, vol. 9, pp. 59–75, 2009.

Research Article

Study of Wireless Authentication Center with Mixed Encryption in WSN

Yiqin Lu, Jing Zhai, Ronghuan Zhu, and Jiancheng Qin

School of Electronic and Information Engineering, South China University of Technology, Guangzhou 510000, China

Correspondence should be addressed to Jing Zhai; 1320503196@qq.com

Received 25 March 2016; Accepted 29 May 2016

Academic Editor: Iftikhar Ahmad

Copyright © 2016 Yiqin Lu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

WSN (wireless sensor network) has been used in a wide range of applications nowadays. Sensor networks may often relay critical data; thus, security must be a high priority. However, due to their limited computational, energy, and storage resources, sensor nodes are vulnerable to attack. So how to protect sensor nodes from attacks without raising computational capability and energy consumption is a worthwhile issue. A WAC (wireless authentication center) with mixed encryption named “MEWAC” is proposed. MEWAC is based on MCU (Microcontroller Unit) and WiFi (Wireless Fidelity) module and uses RSA, AES (Advanced Encryption Standard), and SHA-1 (Secure Hash Algorithm 1) to provide high performance authentication and data encryption services for sensor nodes. The experimental results show that MEWAC has the advantages of low cost, low power consumption, good performance, and stability; moreover, the authentication protocol improves the security of WSN and reduces the overhead in node authentication.

1. Introduction

The WSN has recently attracted a lot of interest due to the range of applications it enables [1]. It can be used in many applications such as battlefield, environmental surveillance, and smart home [2]. Security is the prerequisite for the application to be implemented. In order to protect the information security of WSN, it is necessary to identify nodes. But it is a challenge for the nodes to run encryption algorithms and store data due to the limited computational capability and resources.

In recent years, the research on sensor node authentication has achieved some results. User entity authentication of public key system [3] in WSN is proposed for the first time, but it brings a large amount of computation. Reference [4] proposes symmetric key encryption algorithm with low-energy consumption is required to the applicable sensor networks, but AES algorithms have difficulty managing their own keys. So the security of this protocol is yet to be further improved. Some authors propose a distributed authentication scheme [5, 6]. However, a lot of nodes are involved. The computation and communication overhead will increase with authentication requests times increasing.

As a result, the energy consumption is relatively large. Reference [7] proposes authentication schemes that leverage sensor cooperation to achieve data authentication in an unattended wireless sensor network. But this scheme assumes that each node and sink node share a pair of keys, which easily cause single point failure. According to mobility of sensor node in WSN, an efficient node authentication and key exchange protocol are introduced in [8]. The protocol reduces the overhead in node reauthentication and also provides untraceability of mobile nodes.

We propose a wireless authentication center with mixed encryption named “MEWAC” according to shortcomings of the current schemes. MEWAC has the advantages of low cost, low power consumption, good performance, and stability; moreover, the authentication protocol improves the security of sensor nodes and reduces the overhead in node authentication.

The scope of this paper covers the following: Section 2 introduces the MEWAC-based WSN topology. Section 3 describes the design of MEWAC. Section 4 shows MEWAC workflow. Section 5 presents the experimental results. Conclusions and future work are given in Section 6.

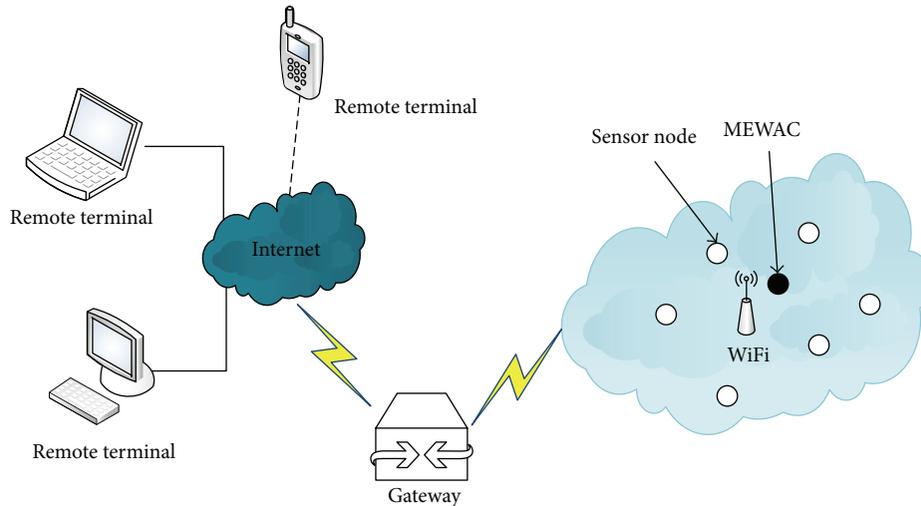


FIGURE 1: The MEWAC-based smart home topology.

2. MEWAC-Based WSN Topology

A WSN mainly consists of autonomous sensors used to collect information and to cooperatively pass their data through the network to a main location [9]. In order to simplify the application environment, we use MEWAC in smart home. Compared with the general sensor network, the number of sensor nodes in smart home is relatively small, and the smart home topology is relatively stable. So just one MEWAC can meet the actual demand. The smart home topology which is based on MEWAC is shown in Figure 1.

The topology is formed by the home gateway, sensor nodes, MEWAC, and remote terminals. The sensor nodes can send authentication requests and data requests to MEWAC. MEWAC provides authorization and data encryption storage services for sensor nodes. If the sensor node cannot be certified by MEWAC or read correct data from MEWAC, it cannot access the WSN.

3. Design of MEWAC

3.1. Overall Structure. Figure 2 shows the overall structure of MEWAC, which is the encryption product composed of hardware and software. The following sections will introduce hardware modules and software modules in detail.

3.2. Hardware Design. MEWAC is divided into three parts in the hardware framework: WiFi module, MCU module, and configuration module, which are shown in Figure 3. The WiFi module is used to connect to the Internet, which communicates with the MCU module via SDIO bus. The MCU module runs various algorithms and stores data needed for sensor nodes. Configuration module provides modification functions, such as ID number and keys.

In order to avoid the wireless communication link being cracked, the performance of the WiFi module must be able to meet the actual requirements. Through analysis and comparison, we select WM631-M as WiFi module. This module

supports IEEE 802.11b+g standard [10]; the transmission speed can reach 54 Mbps.

In order to achieve low power consumption and low cost and maintain good function, the STM32 MCU is chosen as hardware platform. It offers a 32-bit product range that combines very high performance, real-time capabilities, digital signal processing, and low-power, low-voltage operation, while maintaining full integration and ease of development. Finally, the MCU we choose is STM32F405RGT6, which offers the full performance of the Cortex™-M4 core (with floating point unit) running at 168 MHz. This chip has not only 1 MB of FLASH and 192 KB of SRAM, but also rich peripherals.

We use UART port as configuration port, through which we can change the data stored in MCU flexibly. UART is a universal serial data bus for asynchronous communication and usually used as peripheral devices integrated in a micro-processor.

3.3. Software Design. It is vital to realize the function of MEWAC based on the above hardware platform. The software framework of MEWAC is shown in Figure 4, which consists of five parts: (1) MCU logic processing module; (2) WiFi module driver; (3) WiFi protocol stack; (4) security module; (5) TCP/IP protocol stack.

TCP/IP protocol stack is based on uIP 1.0 [11]. The uIP protocol stack is a very small TCP/IP protocol stack, which can be used in the embedded system built by the microprocessor. The security module is the core of MEWAC. It stores the application program and processes the authentication request and data request sent by sensor nodes. The WiFi module driver and WiFi protocol stack are based on the Linux platform source since the MCU platform is too weak to run Linux operation system.

3.4. Extendibility. In the hardware design of MEWAC, we set aside a large amount of storage space. Furthermore, configuration module is added, which makes it easy to change

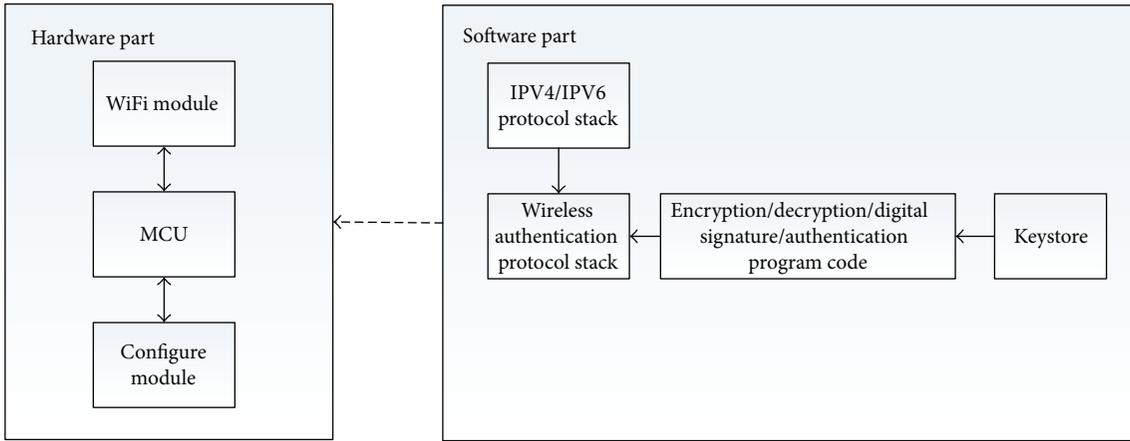


FIGURE 2: The overall structure of MEWAC.

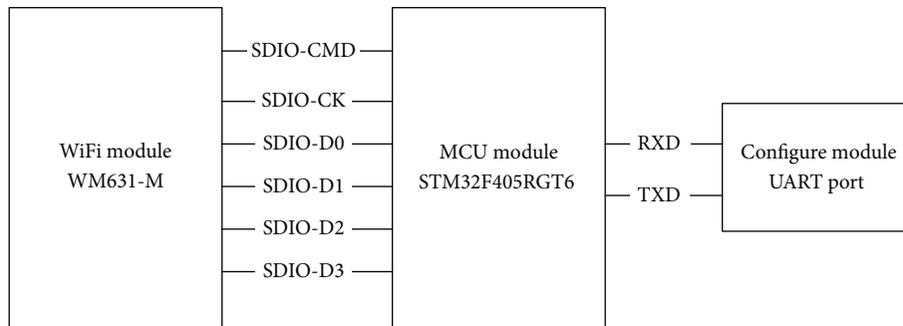


FIGURE 3: Hardware framework of MEWAC.

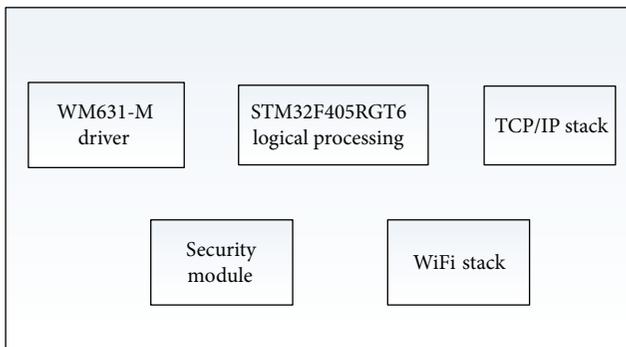


FIGURE 4: Software framework of MEWAC.

the data stored in MCU; in terms of program design, 8-bit space in data packet is reserved. These provide convenience for the further escalation of MEWAC.

4. MEWAC Workflow

4.1. The Basic Working Process. When users start up intelligent controller to monitor the equipment in the smart home, sensors will send authentication requests to MEWAC. After being certified by MEWAC, sensors will begin to detect the temperature, humidity, and so forth. After finishing

the authentication, if the sensor nodes want to communicate with each other, sensors can send key requests to MEWAC to negotiate another AES session key, which is used to encrypt the data for communication between nodes. In addition to the key requests, the sensor can also send other data requests. It depends on the specific circumstances.

The workflow of MEWAC is shown in Figure 5. After MEWAC is powered on, it begins the initialization process immediately and reads the configuration information to access the wireless network. After that, MEWAC receives and analyzes the incoming network packets. If the incoming packet is authentication request, MEWAC will start the authentication process. If the node passes the certification successfully, it will be added to the trust list by MEWAC. MEWAC will return the AES key to the node, and the node will access the WSN. If the incoming packet is data request, MEWAC will check whether the node is in the trust list. If not, the packet will be dropped. Otherwise the packet will be decrypted, and the data required by the node will be encrypted and returned to the node.

4.2. Wireless Authentication Protocol. In the process of data communication, we select RSA, AES, and SHA-1 to encrypt data. RSA with asymmetric keys and AES with symmetric key are state-of-the-art cryptographic algorithms [12]. SHA-1 is used to compute a message digest for a message or data file that is provided as input [13]. The SHA-1 is computationally

TABLE 1: Authentication packet of sensor node.

Product ID number	Serial number	Hash value	Reserved bits	Client ID number
152 b	192 b	160 b	8 b	8 b
	512 b (cipher text)	520 b		8 b (plain text)

TABLE 2: Authentication packet of MEWAC.

ID number	License	Random number	Hash value	Reserved bits
88 b	240 b	16 b	160 b	8 b
		512 b (plain text)		
		512 b (cipher text)		

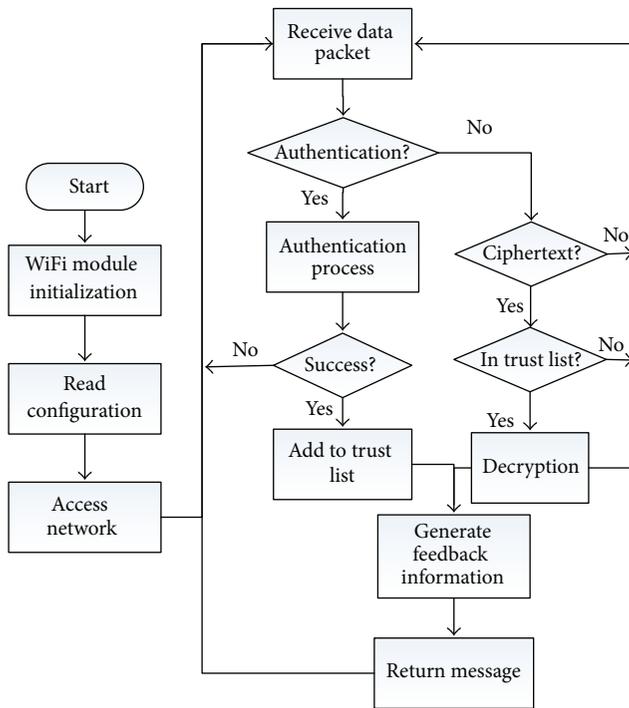


FIGURE 5: Workflow of MEWAC.

infeasible to find a message which corresponds to a given message digest. And any change to a message in transit will, with very high probability, result in a different message digest, so the signature will fail to be verified.

MEWAC and each node have their own information, including the ID number, public and private key. To be able to identify and communicate with each other, MEWAC stores ID number and the public key of each node which is within MEWAC's jurisdiction, and each node stores ID number and the public key of MEWAC. All of the information stored in memory is read-only. The public key of each device is unique. If it is fake, which device it is can be known from the public key, so as to realize the purpose of tracking the system.

As shown in Table 1, the authentication packet sent by sensor node includes its own product ID number, client ID number, serial number, and hash value. The sensor nodes

within the jurisdiction of MEWAC have the same product ID number. To distinguish between various sensor nodes, each node is assigned to a client ID number. The serial numbers mainly composed of random numbers can prevent the message from becoming intercepted and retransmitted. The hash value is calculated by the product ID number and the serial numbers, which can effectively prevent the message from being tampered with during the process of transmission. We use the public key of MEWAC to encrypt the 512-bit plain text. The data encrypted by public key can only be decrypted by the corresponding private key, which is saved locally to ensure that the message cannot be decrypted by others.

The structure of the authentication packet sent by MEWAC is shown in Table 2. The license is calculated according to the serial number of node. We use the public key which corresponds to the sensor node's ID number to encrypt the packet. Just like the authentication packet of sensor node, the authentication packet of MEWAC also has the effect of antiretransmission, antitampering, and anticrack.

Authentication process is shown in Figure 6. The authentication between sensor node and MEWAC is bidirectional. In order to prevent DoS (Denial of Service) attacks, we limit how many times the sensor node can visit MEWAC in a unit of time.

4.3. Encrypted Communication. RSA algorithms easily manage their own keys. However, their computing quantity is large and computing time is relatively long. AES algorithms are just the opposite. The combination of both has the salient features of Symmetric Cryptography, having fast speed and being easy to process, and features of Asymmetric Cryptography such as being secured, avoiding key transportation, and providing the power to the users to generate their own keys of variable length [13]. As a result, during the authentication process, MEWAC and the node make agreement to use part of the returned message as the first communication AES key. The license and random number are used as the AES-256-bit key. After finishing the authentication process, sensor nodes can send data requests encrypted by the AES-256-bit key to WDongle.

4.4. Performance Analysis of Mixed Encryption. Compared to the traditional method of using AES encryption for sensor

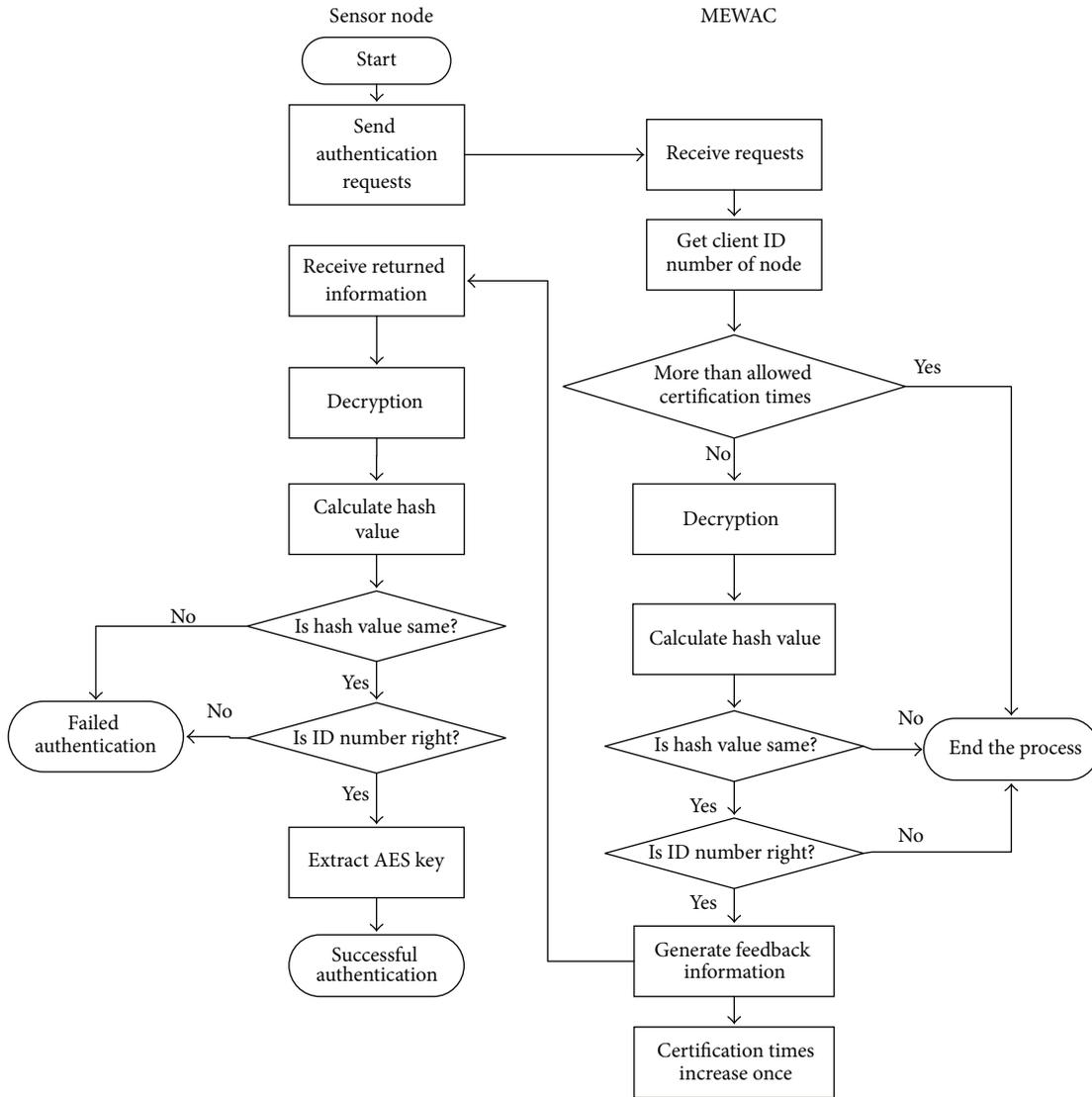


FIGURE 6: Authentication process of MEWAC.

nodes authentication [4], the mixed encryption method has a higher security. Firstly, SHA-1 encryption algorithm can ensure the integrity of the data; then RSA encryption packet is used to pass a AES-256 b session key, which avoids the insecurity of key transportation. Although the energy consumption of mixed encryption is relatively larger than that of AES encryption, the increase in energy consumption is not large, which is in acceptable range of the nodes and MEWAC. On the one hand, the shorter the key length is, the less the energy consumption is [14]. So we choose RSA-512 b which is relatively shorter; on the other, RSA encryption packet which also is the authentication package is not only used to transfer the AES key, but also used for identity authentication. So there is no extra information for the transmission of the AES key.

Calculation and energy consumption of mixed encryption are smaller compared to the RSA encryption for nodes authentication, and the node security can also be guaranteed.

TABLE 3: Hardware parameters and costs.

MCU	STM32F405RGT6
Storage	1 MB
Voltage	5 V
Frequency	168 MHz
NIC	WM631-M
Memory	192 KB
Power	1.4 W
Price	6.4\$

5. Experiments

According to MEWAC's design principle, we implement this WAC based on MCU and WiFi module, which is used as our experimental platform. To test and approach the pure

TABLE 4: Algorithms running time.

Encryption model	RSA			AES		SHA-1
Key length	512 b	768 b	1024 b	128 b	256 b	
Time	602 ms	2.01 s	4.89 s	185 μ s	610 μ s	227.9 μ s

TABLE 5: Average response time.

	Authentication process	Data request process
Time	1.544 s	13.1 ms

performance of MEWAC, we use 9 clients on the personal computer instead of 9 sensor nodes. The hardware parameters and costs are shown in Table 3. We can see it complies with the requirements of low power and low cost. According to the results, the entire design occupies about 49 KB memory including 14 KB used by memory management and occupies about 211 KB storage volume. Therefore, the MEWAC also has the possibility of further escalation.

Different encryption methods directly affect the performance of WEWAC and nodes, such as security level and power consumption. On the one hand, a longer key consumes more power and results in more heat dissipation [14]; on the other, the security of any type of cryptography depends on number of bits used in a key and the amount of computation required to break the cipher [15]. According to the test result and the comparison of encryption algorithms, we chose RSA-512 b, AES-256 b, and SHA-1. The running time which is taken by these algorithms to encrypt the same 512-bit packets in our platform is shown in Table 4.

We stipulate the whole times a sensor node can send authentication request to MEWAC in 15 minutes are not more than 12. In fact, times the sensor node can visit MEWAC in a unit of time can be artificially set according to the actual situation. During the experiment, the sensor can only operate in a limited range. If out of WiFi coverage, the sensor cannot access wireless network to communicate with MEWAC.

In order to know the average response time of authentication and data requests process in our platform, we do some tests and the experimental results are shown in Table 5. Authentication process is the whole process shown in Figure 6. Data requests process includes mainly data request transmission, reception of MEWAC's feedback packet, and correct reading of packet.

In order to know the stability of MEWAC, a stress test is carried out. The sensor node sends 500 times of data read request to the WAC with AES session key. The success rate of this test is 100%. Figure 7 shows the response time for each data request processing, which indicates that the WAC has sufficient performance and stability.

6. Conclusions and Future Work

The authentication for resource-constrained sensor node identity can effectively protect sensor node from attacks. This paper proposes a mixed encryption wireless authentication center named MEWAC according to shortcomings of

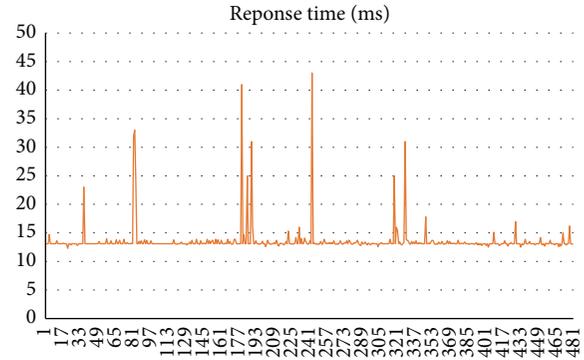


FIGURE 7: Stress test.

the existing schemes. MEWAC can reduce the overhead and prevent retransmission, tampering, and DoS attacks. Furthermore, we can use the unique public key of each device to track the system, and the sensor nodes can only work in a limited range which the WiFi of MEWAC can cover. The experimental results show that MEWAC not only has the advantages of low power consumption, low cost, and good performance, but also provides advanced protection for sensor nodes.

MEWAC is extensible, which provides convenience for the further upgrading. In future work, we can consider using Bluetooth instead of WiFi, which can reduce the cost and power consumption of MEWAC ulteriorly [16]. We also can use steganography [12, 17, 18] to provide more advanced security protection for sensor nodes.

MEWAC can be generalized to common WSN. Multiple MEWACs collaborate to complete the node certification, which forms a distributed authentication scheme. Except for being used in WSN, the MEWAC can protect the copyright of software.

Competing Interests

The authors declare that there are no competing interests regarding the publication of this paper.

References

- [1] E. Sabbah, A. Majeed, K.-D. Kang, K. Liu, and N. Abu-Ghazaleh, "An application-driven perspective on wireless sensor network security," in *Proceedings of the 2nd ACM International Workshop on Quality of Service & Security for Wireless and Mobile Networks (Q2SWinet '06)*, pp. 1-8, ACM, October 2006.
- [2] X.-Y. Yang, Q. Zhang, and L.-X. Wei, "A robust entity authentication in wireless sensor networks," in *Proceedings of the International Conference on Information Engineering and Computer Science*, pp. 1-4, IEEE, Wuhan, China, December 2009.

- [3] R. Watro, D. Kong, S.-F. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "TinyPK: securing sensor networks with public key technology," in *Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04)*, pp. 59–64, ACM Press, Washington, DC, USA, October 2004.
- [4] H. Lee, K. Lee, and Y. Shin, "Implementation and performance analysis of AES-128 CBC algorithm in WSNs," in *Proceedings of the 12th International Conference on Advanced Communication Technology (ICACT '10)*, pp. 243–248, IEEE Press, 2010.
- [5] K. Bauer and H. Lee, "A distributed authentication scheme for a wireless sensing system," *ACM Transactions on Information and System Security*, vol. 11, no. 3, pp. 1–35, 2008.
- [6] R. Bellazreg, N. Boudriga, and M. Hamdi, "A dynamic distributed key tunneling protocol for heterogeneous wireless sensor networks," in *Proceedings of the 11th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 1077–1082, IEEE, Liverpool, UK, June 2012.
- [7] R. D. Pietro, C. Soriente, A. Spognardi, and G. Tsudik, "Collaborative authentication in unattended WSNs," in *Proceedings of the 2nd ACM Conference on Wireless Network Security (WiSec '09)*, pp. 237–244, Zurich, Switzerland, March 2009.
- [8] K. Han, K. Kim, and T. Shon, "Untraceable mobile node authentication in WSN," *Sensors*, vol. 10, no. 5, pp. 4410–4429, 2010.
- [9] A. Q. Zhao, Y. N. Weng, Y. Lu, and C. Y. Liu, "Research on dynamic routing mechanisms in wireless sensor networks," *The Scientific World Journal*, vol. 2014, Article ID 165694, 7 pages, 2014.
- [10] Y.-Q. Lu, D.-W. Wu, and J.-C. Qin, "Wireless authentication center based on embedded Wi-Fi technology," *WIT Transactions on Information and Communication Technologies*, vol. 59, pp. 387–394, 2014.
- [11] Y.-Q. Lu, D.-W. Wu, and J.-C. Qin, "Design of embedded web server based on MCU and IPv6," *International Journal of Advancements in Computing Technology*, vol. 5, no. 5, pp. 1232–1240, 2013.
- [12] S. F. Mare, M. Vladutiu, and L. Prodan, "Secret data communication system using steganography, AES and RSA," in *Proceedings of the IEEE 17th International Symposium for Design and Technology of Electronics Packages (SIITME '11)*, pp. 339–344, October 2011.
- [13] D. Eastlake III and P. Jones, *US Secure Hash Algorithm 1 (SHA1)*, RFC Editor, 2001.
- [14] A. Kakkar, M. L. Singh, and P. K. Bansal, "Comparison of various encryption algorithms and techniques for secured data communication in multinode network," *International Journal of Engineering and Technology*, vol. 2, no. 1, pp. 87–92, 2012.
- [15] W. Heng-Qing and S. Ru-Min, "The security of public key cryptosystem depends on the length of the key," *Scientific and Technological Information: Academic Research*, vol. 34, 2008.
- [16] C. You-ping, "Study on the coexistence of bluetooth and Wi-Fi," *Science and Technology Wind*, no. 8, p. 99, 2009.
- [17] N. Hopper, L. von Ahn, and J. Langford, "Provably secure steganography," *IEEE Transactions on Computers*, vol. 58, no. 5, pp. 662–676, 2009.
- [18] J. Daemen and V. Rijmen, "The first 10 years of advanced encryption," *IEEE Security & Privacy*, vol. 8, no. 6, pp. 72–74, 2010.

Research Article

Enhancing Energy Efficiency of Wireless Sensor Network through the Design of Energy Efficient Routing Protocol

Noor Zaman,¹ Low Tang Jung,² and Muhammad Mehboob Yasin¹

¹College of Computer Sciences & IT, King Faisal University, Al Ahsa 31982, Saudi Arabia

²Department of Computer & Information Sciences, Universiti Teknologi PETRONAS, 32610 Seri Iskandar, Perak, Malaysia

Correspondence should be addressed to Noor Zaman; nzaman@kfu.edu.sa

Received 25 March 2016; Revised 22 May 2016; Accepted 29 May 2016

Academic Editor: Fei Yu

Copyright © 2016 Noor Zaman et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Wireless Sensor Network (WSN) is known to be a highly resource constrained class of network where energy consumption is one of the prime concerns. In this research, a cross layer design methodology was adopted to design an energy efficient routing protocol entitled “Position Responsive Routing Protocol” (PRRP). PRRP is designed to minimize energy consumed in each node by (1) reducing the amount of time in which a sensor node is in an idle listening state and (2) reducing the average communication distance over the network. The performance of the proposed PRRP was critically evaluated in the context of network lifetime, throughput, and energy consumption of the network per individual basis and per data packet basis. The research results were analyzed and benchmarked against the well-known LEACH and CELRP protocols. The outcomes show a significant improvement in the WSN in terms of energy efficiency and the overall performance of WSN.

1. Introduction

Wireless sensor technology is playing a vital role in many of the commercialized industrial automation processes and various other real life applications [1–4]. It is particularly suitable for harsh environment applications where deploying of other network infrastructure is difficult and/or almost impossible such as in battlefield, in hazardous chemical plant, and in high thermal environment. It is not uncommon to see that most of the crucial surveillance and security applications also rely on sensor based applications. Sensors which are tiny in size and cheap in cost have the capabilities to be deployed in a range of applications as explained in [5–9]. Essentially all sensor networks comprise some forms of sensing mechanism to collect data from an intended physical environment either by a time driven approach or by event triggering approach. By these approaches a sensor will convey the sensed data to a destination or sink (multiple destinations/sinks are also possible) via some kinds of routing algorithm such as Minimum Cost Forwarding Algorithm (MCFA), Directed Diffusion Routing Protocol (DDRP), or one of the cluster-based routing protocols. Being very small in size, sensor

nodes are built with limited computational capacity, small storage memory, and finite battery power capacity [10].

The structure of a typical WSN node [11] consists of four main components: a sensing element, normally used for sensing a physically measurable parameter; an Analog-to-Digital Converter (ADC), used for converting analog signals to some digital formats; a processing unit, providing simple/basic data processing and computation capabilities; and a power unit, responsible for sensor node's operation life span. It is a known fact that WSN is a resource constrained network in which energy efficiency is always the main issue since the operation of WSN depends heavily on the life span of the sensor nodes' battery [12]. The most energy consuming operation in WSN is the data packet routing activity. The characteristics of the WSN are different from the conventional networks [13, 14]. These unique characteristics are often taken into account for addressing the issues and challenges related to network coverage, runtime topologies management, node distribution, node administration, node mobility energy efficiency/consumption, network deployment, application areas/environment, and so forth [15–17].

Nodes in a WSN are generally energy, computation, and memory constrained. Consequently, there is a need for research and development into low-computation resource-aware algorithms for WSNs, targeting at small, highly resource constrained embedded sensor nodes. Energy consumption is of prime importance in WSNs and thus some algorithms [18–24] and hardware were designed with energy efficiency or energy awareness as a central focal point of interest. Enhancing energy efficiency of WSN with respect to the communication routing protocol is the primary concern of this research. We propose a new routing protocol entitled “Position Responsive Routing Protocol (PRRP)” and compare its performance with the well-known LEACH and CELRP protocols. The simulation results show a significant improvement over the aforementioned protocols in terms of energy efficiency and the overall performance of the WSN.

2. Literature Review

The main operational sustainability concern in WSN is its energy resource constraint. This brings along in recent years that a great number of energy efficient routing protocols have been proposed for WSNs based on the network organization and the routing protocol operations. Some of these focused on minimizing the communication distance to reduce the energy consumption and a handful of them focused on fair energy distribution to avoid the routing hole (hot spot) problems [25, 26]. The routing hole issue was described and addressed in [25–28] by utilizing mobility based energy efficient routing protocols. These protocols are suitable in certain situations; however they may not be applicable in cases where mobility is not feasible such as earthquake, forest fire, and disaster management [29]. Mobility techniques do have other challenges like increased energy overhead owing to frequent network topology changes and data packet drops due to high latency [30, 31]. Various other research papers focusing on energy efficiency routing protocols can be found in [32–37]. Many researchers pay attention to the WSN energy issue by designing different routing techniques and MAC-layer protocols to raise the energy level in WSN. Our literature review reveals that a range of different energy efficient routing protocols in the recent past were designed mostly based on the network structure such as hierarchical routing, location routing, and flat based routing. Our extensive literature review also reveals that the existing routing protocols are still facing energy efficiency limitation issues. Critical analyses of some of the popular existing energy efficient routing protocols are presented in this section.

Hierarchical routing protocols are considered more energy efficient when compared with flat and location based routing protocols. A number of hierarchical based energy efficient routing protocols have been referred to in the literature review such as LEACH [38], TEEN and APTEEN [39, 40], PEGASIS [41], MECN and SMECN [35, 42], SOP [43], HPAR [44], VGA [45], Sensor Aggregate [46], TTDD [47], Energy Efficient Self-Healing [48], Energy Efficient Position Based [49], and CELRP [50]. The literature review refers to the fact that the main advantage of hierarchical approach is to control the data duplication and is best suited for data aggregation.

With this format, nodes are not allowed to communicate with the sink directly that they must go through a cluster head for communication purposes, while the cluster head collects the data from different nodes within a specific cluster area, and then it sends the collected data either to another cluster head or directly to the sink. This approach is more balanced and energy efficient comparable to flat and location based routing protocols [51–57]. However, the disadvantage of this approach is that it results in quick energy drain of the cluster head nodes as most of the time they are involved in sending and receiving the data packets. Rotation of cluster heads is possible but it also brings along an issue related to the loss of the energy resource.

A number of different protocols have been proposed for WSN node localization or location based routing. These include GAF [58], GEAR [59], SPAN [60], MFR, GEDIR [61], and GOAFR [62]. These literatures referred to the fact that the main advantage of these protocols is the ability to identify the correct location of the sensor node within the sensor network. Node localization is directly linked to energy efficiency of WSN. It saves energy resources of WSN. However in most cases these protocols resulted in energy loss due to its geographical topology and node distribution in the WSN. There is thus still a gap in energy efficient routing protocol design and solutions for this class of routing.

A good number of flat based routing protocols have been studied such as SPIN [63], Directed Diffusion [64–66], Rumor Routing [67], GBR [68, 69], MCFA [70], COUGAR [71], CADR [72], ACQUIRE [73], and EAR [74]. The literature review referred to the fact that the main advantage of flat based routing protocol is its simplicity in operation and it had a direct communication mechanism with the base station in which all nodes are allowed to participate during the routing operation. For its simplicity, the nodes only need information about their closest neighbors. However, the major disadvantage is that nodes spread out in a flat manner and all nodes are attempting to participate equally thus causing the nodes closer to the sink to deplete their power sooner than those located further away from the sink. This is mainly due to the heavy data transmission load. This is badly affecting the nodes closer to the sink for keeping them alive longer. Therefore the nodes further away may be unable to communicate with the base station after some time due to network isolated segmentation problem in the WSN. Consequently many of the nodes are not able to participate in routing thus not utilizing their entire energy effectively. More research works are deemed necessary to address the WSN energy efficiency in this aspect. In addition, flat routing is still having issues in data collision overhead, links formed on the fly without synchronization, energy dissipation depending on traffic patterns, and fairness being not guaranteed.

3. PRRP Research Methodology

This research is aimed to design a new energy efficient routing protocol, namely, Position Responsive Routing Protocol (PRRP), to address the energy issues in WSN and specifically to enhance the energy efficiency in WSN. The main contribution of PRRP is the novel way of selecting the

cluster head (CH) in WSN. In comparing to the existing protocols such as LEACH and CELRP whereby the CHs are chosen randomly among all nodes based on their respective residual energy, in PRRP we considered different parameters such as distance from the sink, energy level, and the average distance of neighboring nodes from the candidate CH node.

3.1. Basic Assumptions. PRRP differs from existing protocols such as LEACH and CELRP in many ways. This research assumes that nodes are aware of their geographical locations in WSNs using GPS or some other cost effective location surveys [50, 75–79]. Each node is able to use different frequencies for transmitting and receiving as it is assumed that sensor node has a multichannel transceiver. It is assumed that each node can transmit its data to the sink as node has ability to transmit for longer distance. All nodes have homogeneous energy level at initial stage and this assumption is widely used in literature [80]. Sensor nodes are distributed in the grid format with a uniform random fashion and the sink is placed in the center of sensor network. This assumption is particularly relevant for forest fire surveillance systems and disaster management systems.

3.2. Network Model. The conceptual network model for PRRP implementation has the layout as shown in Figure 1. It is considered a randomly uniform distributed WSN where nodes are distributed randomly in a sensor field based on a grid format. The static sink is located in the center of the network. The sensor nodes in the network are divided into different groups of clusters on both side of the sink. Normally, the tiers are defined in radii around the sink ranging within tier D_0 , tier D_1 , and so forth, depending on the network size. Each tier covers more than one grid (partially or fully) and has a logical range in which the number of nodes lies, which is depending on the distribution of the nodes. Initially, a signal with energy level E_0 is transmitted from the sink into the network. The signal with energy E_0 shall be received only by those nodes placed near the sink. After listening to the signal, these nodes will respond to the sink and they will be registered as tier D_0 nodes. Next, the sink will advertise signal with transmission energy of E_1 , where $E_1 > E_0$. The nodes, other than D_0 , shall respond to this signal, forming tier D_1 nodes. This process will be repeated until a preset number of tiers are formed.

3.3. Energy Model. The power control model used in this research work is based on the concept that energy consumption is directly proportional to the transmission distance. Equation (1) below shows the node energy consumption for transmitting k bits of data for a distance of d meters. The energy consumed for receiving of k bits is given by (2) [81]:

$$E_{Tx} = kE_{elec} + kE_{amp}d^2, \quad (1)$$

$$E_{Rx} = kE_{elec}, \quad (2)$$

where E_{elec} is the electronics energy in transceiver and E_{amp} is the amplifier energy.

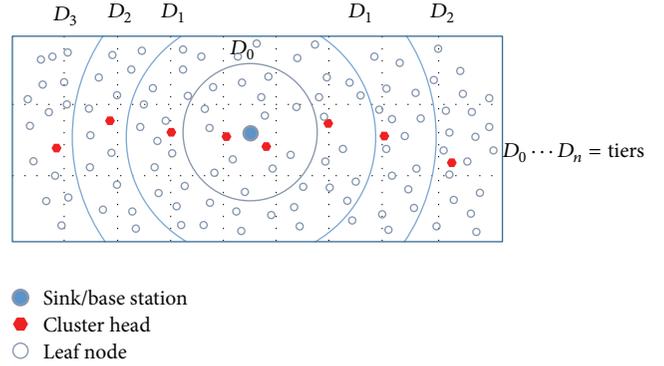


FIGURE 1: PRRP network model.

The minimum energy for a node to be able to participate in the coming round of routing (or it is the minimum energy to participate in next round) is given in (3) as $E_{\text{thresholdmin}}$:

$$E_{\text{thresholdmin}} = kE_{elec} + kE_{amp}d^2 + 8kE_{elec}. \quad (3)$$

3.4. Analysis of PRRP. This section presents a brief analysis of the energy utilization in terms of energy consumed by cluster head nodes and the leaf nodes that can be linked to the life span of the CH node. Consider a WSN comprising of N wireless sensor nodes that are uniformly distributed within a grid of size $m \times m$, and within each grid cell one of the nodes acts as the cluster head (CH).

CH spends its life in three modes, namely, receiving data samples from member nodes, transmitting its own data (and/or member nodes' data), and sleep mode. Let E_{in} , E_{th} , E_r , and E_t , respectively, denote the initial energy, threshold energy, energy consumed during reception, and energy consumed during transmission of one data sample. Further, we assume that each data sample has a fixed size; therefore the transmitting time and the receiving time for each data sample are the same, namely, T_s . During each sampling interval, a CH, with k member nodes, spends T_t time for transmission, kT_t time for receiving samples, and remaining $T_s - (k+1)T_t$ time in sleep mode. The CH is assumed to have died when its residual energy falls below the threshold (E_{th}) necessary for a node to function. Therefore, the life of the CH can be calculated in terms of the number of sampling intervals, N_s , as

$$N_s = \frac{E_{in} - E_{th}}{E_t + kE_r + (T_s - (k+1)T_t)P_s}. \quad (4)$$

3.5. Proposed Routing Protocol PRRP Description. After system modeling, suitable gateways are identified from each cluster as all nodes are aware of their respective location and the distance from the sink and from their neighboring nodes. The selection of the gateway is based on parameters such as the node distance, number of nodes close to a particular node, and the energy threshold level. The energy threshold level is more significant than others. On this note, PRRP is therefore aimed to minimize the distance between the nodes and the gateway to save energy during data transmission.

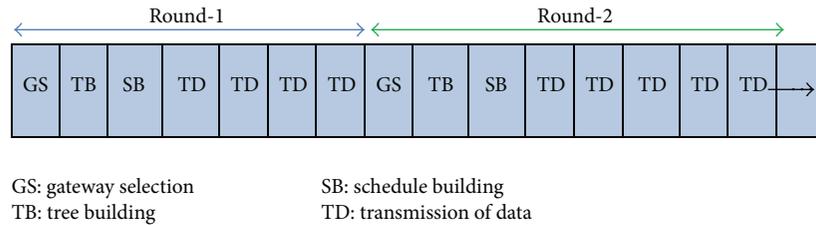


FIGURE 2: PRRP phases.

PRRP assumes that node's data acquisition is event driven. That is, the majority of nodes will remain in sleep mode to save energy. It is assumed that type of all the sensed data within one grid is the same, so data aggregation can be applied and nodes will transfer their sensed data on a fixed schedule based on TDMA principle. Each node in PRRP will transmit its data to its closest neighbor. This is to ensure its transmission distance is shortest and therefore less energy is consumed for data transmission. It is noted that tree routing is an energy efficient routing mechanism; thus this mechanism is adopted in the proposed PRRP. A tree is built starting from the leaf nodes to the sink. The sink is placed in the center of the network instead of on the one end as in LEACH and CELRP. It should be mentioned here that, in PRRP, any node on the network can be a gateway but selection of a gateway is based on three parameters as mentioned earlier. Under the PRRP scheme, a node can only be allowed to join a tree if its energy is sufficient to survive for a complete round.

An efficient distributed TDMA scheduling is used in the proposed PRRP. In this scheduling the radio module of the nonleaf node will be turned ON only for the assigned time slots instead of being ON for all times such as in LEACH protocol. In PRRP the number of leaf nodes and the distance from the nonleaf node is less as compared to LEACH and CELRP. Consequently energy conservation can be optimized based on stated technique. The distributed TDMA scheduling in PRRP strongly supports energy efficiency and good data throughput in the proposed PRRP.

3.5.1. The Proposed PRRP Algorithm. In PRRP, each round of processing time consists of four phases: (1) gateway selection (GS), (2) tree building (TB), (3) schedule building (SB), and (4) transmission of data (TD) as shown in Figure 2. Processing rounds will continue till the routing tree is broken due to the energy level of the gateway dropping below the threshold level.

In the first phase, GS process is completed on the basis of its position, its residual energy level, and the number of neighboring nodes around it. This gateway will be responsible for transferring the aggregated/collected data from the neighboring nodes to the sink. This phase starts with the message initiated from the sink with energy threshold level of E_0 . In the second phase (TB), a routing tree rooted at the sink is built. The newly formed tree will be based on two types of the sensor node such as nonleaf nodes and leaf nodes. Leaf node transmits sensed data from the monitored area to its parent. The nonleaf nodes act as the intermediate nodes to

transmit data from lower to upper level of the tree. Based on this tree, a Time Division Multiple Access (TDMA) schedule subsequently is built in phase-3 (SB) in a distributed manner. In the final phase (TD), the data are transmitted from nodes to the sink based on the schedule prepared in phase-3, that is, the distributed TDMA scheduling.

The time required to forward all data packets in a single round is denoted as one data transmission period. That is, a data transmission period may consist of multiple TDs. The TDs may be repeated numerous times in a single round, depending on the energy level of the gateways as illustrated in Figure 2. For instance, in the second round, it has more TDs than in the 1st round. On another note, the number of data transmission periods in a single round shall depend on the application and the periodic events of the sensor network data collection. The PRRP process flow is depicted in Figure 3. Always in case of tree rebuilt, different sensor nodes will take part in that process, which will become source of equal energy distribution in the network. The energy consumption for overall network will be distributed fairly among all nodes. The following sections describe all the phases.

3.5.2. Gateway Selection. In the first phase a few nodes will be selected as gateways in such a manner as to minimize overall energy consumption in the WSN. The network is assumed to be divided into different grid cells and the cells are further divided into a number of tiers, say n , on both sides of the sink. Initially the nodes in tier D_0 will be considered as the potential gateway candidates based on their energy level e , the distance from the sink d , and the number of neighboring nodes n . Some of these nodes are allowed to advertise themselves as gateways. However priority will be based on the residual energy in a node. A potential gateway will act as a gateway until its residual energy drops below a threshold value E_{th} . Following this, new gateways will be selected from the nodes of tier D_1 . Again, the new selected nodes will act as gateways until their residual energy drop below E_{th} , and so on. When all tiers are considered and no more nodes can be selected as gateways based on the current E_{th} , a new round will start with a new lower E_{th} . The flow chart for gateway selection is given in Figure 4.

This mechanism will continue until the last tier (D_n) and with the second cycle the same process will be continued. However, in this time E_{th} by the sink will be little reduced by factor (e). The same mechanism will be continued for all tiers and all cycles until the end. The sink and sensor nodes will exchange messages using the CSMA mechanism.

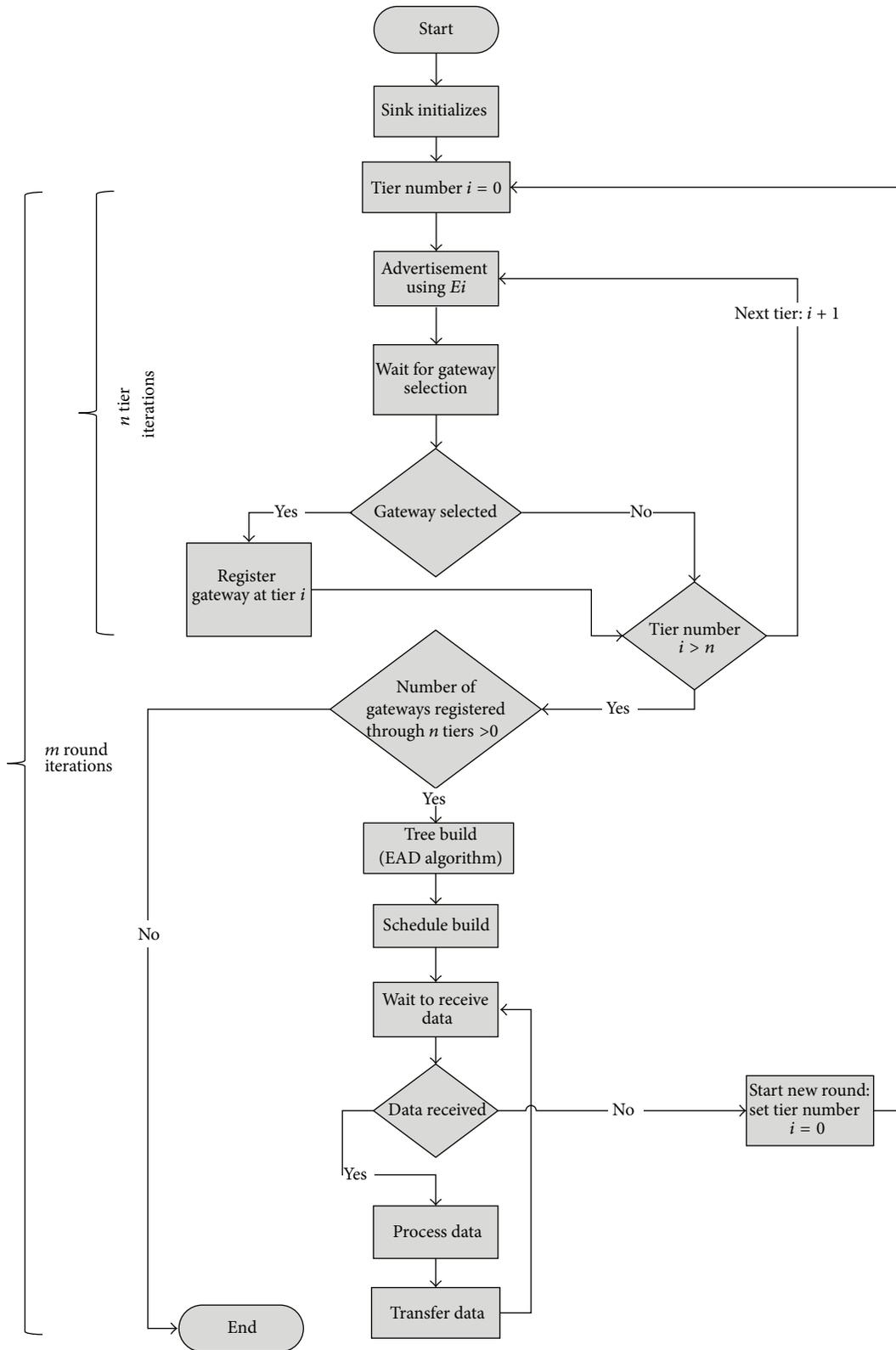


FIGURE 3: PRRP process flow.

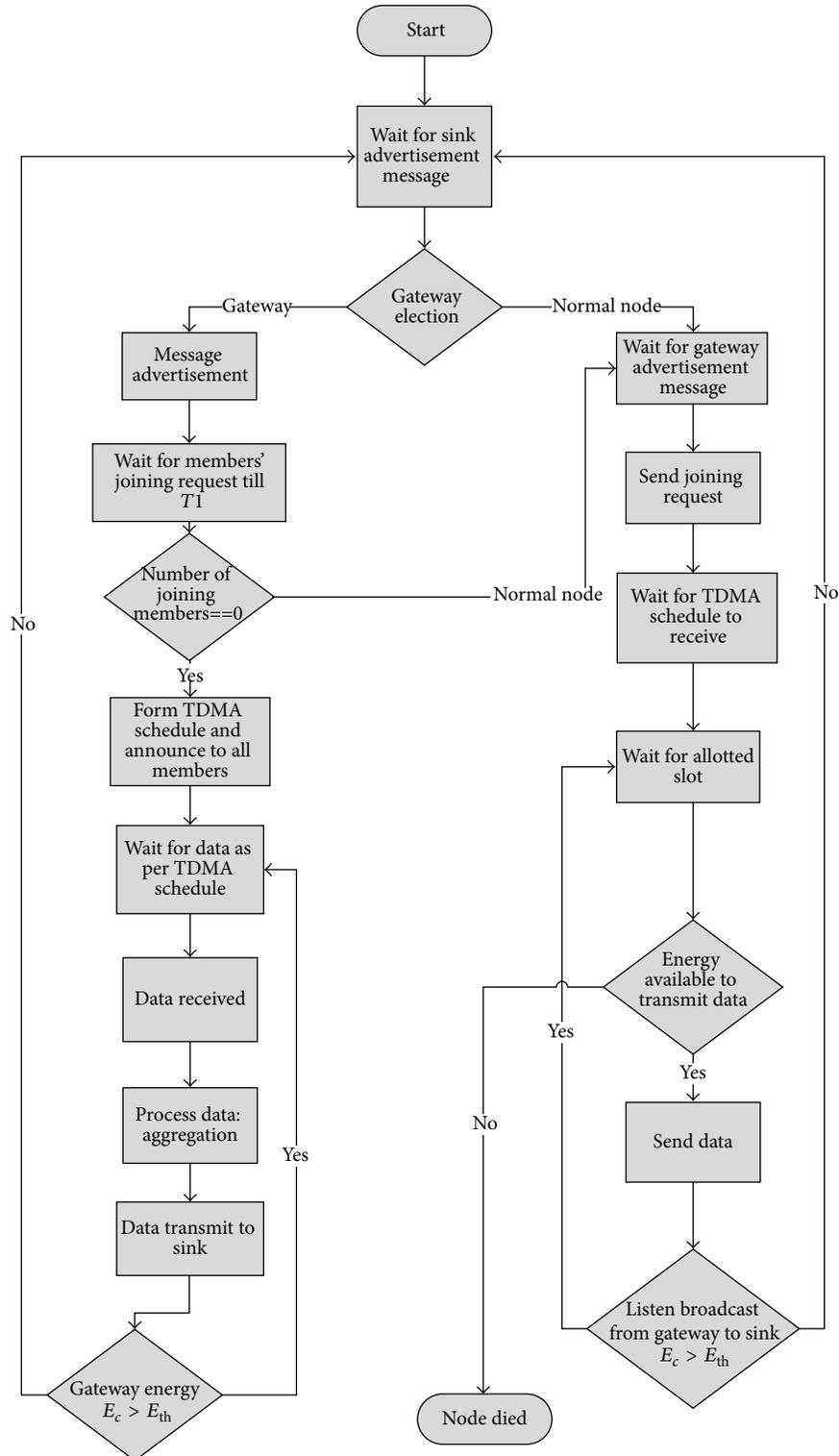


FIGURE 4: Gateway selection flowchart.

The node will remain ON until it receives the ADV message from the sink and then it sends the JOIN message. Since the node does not need a confirmation from the sink, it will go to sleep immediately after sending the JOIN message. The

gateway selection is based on three different parameters such as energy level, number of neighboring nodes, and position from the sink. After selecting the gateways, the next phase will start to build the tree. The gateway nodes will initiate

```

Step A:
Wait for sink advertisement message
IF (gateway Election → Gateway)
    Message advertise
    Wait for members' joining request till T1
    IF (number of joining members == 0)
        Go to Step C
    Form TDMA schedule and announce to all members
Step B:
Wait for data as per TDMA schedule
Data received
Process data: aggregation
Data transmit to sink
While (Gateway Energy  $E_c > E_{th}$ )
    Repeat from Step B
Repeat from Step A
ELSE (gateway Election → Normal node)
Step C:
Wait for gateway advertisement message
Send joining request
Wait for TDMA schedule to receive
Step D:
Wait for allotted slot
IF Energy available to transmit data
    Send data
    While (Gateway Energy  $E_c > E_{th}$ )
        Listen Broadcast from sink to gateway
    Repeat from Step D
Repeat from Step A
ELSE
    Node died
END IF

```

ALGORITHM 1: Gateway selection algorithm.

the process of building the tree. For further clarification for the mechanism of gateway selection, the algorithm in pseudocode is given in Algorithm 1.

3.5.3. Tree Building. Upon completing the gateway selection the tree building phase is initiated. A tree rooted at the sink is built by using a modified version of the algorithm proposed in [82]. A tree is built by the sink broadcasting a control message containing six fields, namely, *sender, position, type, level, parent, and energy*. For a sender node v , $type_v$ represents its status in which 0 is for undefined status, 1 is for leaf node, and 2 is for nonleaf node. $Level_v$ refers to the number of hops from v to the sink. $Parent_v$ is the next hop of v in the path to the sink, $energy_v$ is the residual energy E_v , and P_v denotes the position of the node from the sink.

Initially each node has status 0, while sink always have status 2, implying that sink is a nonleaf node. The sink broadcasts the message $(s, 2, 0, NULL, \infty, P_s)$, where s is the identifier of sink, 2 is the status of the sink, $NULL$ indicates that there is no parent of the sink, ∞ indicates that the sink is connected to a power source, and P_s is the position of the sink. When a node v receives a message $(u, 2, level_u, parent_u, E_u, P_u)$ from node u , it becomes a leaf node, senses the channel until the channel is idle, and then waits for T^v_2

time duration. If the channel is still idle, v will broadcast message $(v, 1, level_u + 1, u, E_v, P_v)$. If v receives message $(u, 1, level_u, parent_u, E_u, P_u)$ from u , it will sense the channel until it is idle, and it waits for T^v_1 time duration. If the channel is still idle, v broadcasts message $(v, 2, level_v, parent_v, E_v, P_v)$. Then, it becomes nonleaf node. If node v receives more than one message from different nodes before broadcasting its message, it will select the node with larger energy and with the nearest distance to it as its parent. If multiple nodes have the same energy and distance, v will select one of them randomly. If there is another node occupying the common channel before its time is out, the waiting node will go back to sensing state. If a node v receives message $(w, 2, level_w, v, E_w, P_w)$ from node w indicating that v is its parent, v will broadcast message $(v, 2, level_v, parent_v, E_v, P_v)$ immediately after the channel is idle {explain why}. By this process, eventually all gateways will be able to build a routing tree from nodes to the sink as shown in Figure 5.

3.5.4. Schedule Building. The schedule building is the third phase for building an effective distributed scheduling scheme using TDMA principle for data transmission. The schedule is built on the assumption that all the nodes which are connected with the same gateway will transfer their

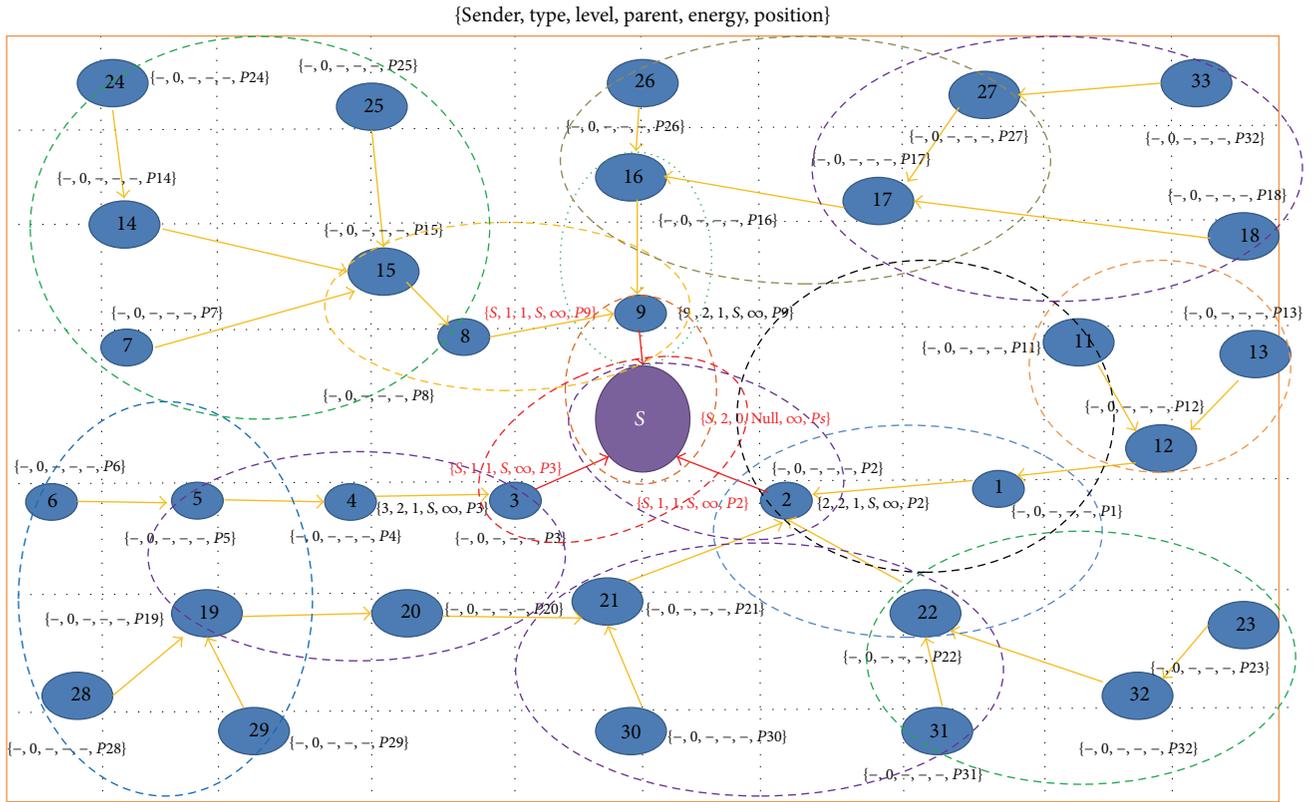


FIGURE 5: Showing final routing trees built among the different regions.

data using same frequency. This assumption implies that nodes connecting to different gateways are using different frequencies for data transmission therefore simultaneous data transmission is allowed among the different trees. We have identified two time constants: Time Ready to Receive (TRR) and Time Ready to Transmit (TRT). TRR_v and TRT_v represent two different time slots: TRR_v , indicates when a node v is ready to receive from its children nodes and TRT_v shows when a node v can transmit to its parent towards the sink. The node wakeup time, during which its transceiver will stay in the *ON* state, can be calculated using the values of TRT_v and TRR_v . For the leaf node, transmission time TRT_v is equal to the width of one time slot denoted as t_0 , while reception time TRR_v is zero since it does not have any children.

On the other hand, for nonleaf node v ,

$$\begin{aligned} TRR_v &= \max(TRT_i), \quad \text{where } i = 1, 2, 3, \dots, n_v^c, \\ TRT_v &= TRR_v + n_v^c T_t. \end{aligned} \quad (5)$$

In the above equation i show an index for the children of v node, n_v^c represents the count of v 's children which represents one data packet transmit time. As we select max function, the parent node will stay in the *ON* state only when all of its children are ready to transmit, which is better than switching its state repeatedly from *OFF* to *ON* and back. Once the received data from children are aggregated then the parent can transfer the data to the next node. Initially, each leaf node

will transmit its TRT value to its parent. After receiving TRT values from all of its children, the parent will calculate its TRT and TRR using above equation and then build a schedule for its children as shown in Figure 6.

The flow chart for building the schedule as explained above is given in Figure 7.

3.5.5. Transmission of Data. The data transmission phase can be repeated many times for a same round of schedule but node will require energy to be alive. Nonleaf node will remain *ON* for more slots for having responsibility to collect the data from its child and then transfer it to its parent, while the leaf nodes will be *ON* only for one slot, just to transfer the data to its parent. For each node, a time slot labeled by T represents a time slot at which a node transmits data and a time slot labeled by R represents time slot at which a node receives data as shown in Figure 8.

As a summary, in PRRP the WSN is divided into grid and cells and then into different tiers. Meanwhile, sink is assumed to be placed in the center of the topology. The nodes are distributed in random fashion with an assumption that they are aware of their position/location through Global Positioning System (GPS) or any other local means. The gateways are the nodes that are close to the sink, normally with tier₀. Furthermore, the gateways are selected with other tiers on the basis of node energy level, its position from the sink, and the number of nodes in its neighbor. PRRP operates in different phases starting from the gateway selection up to

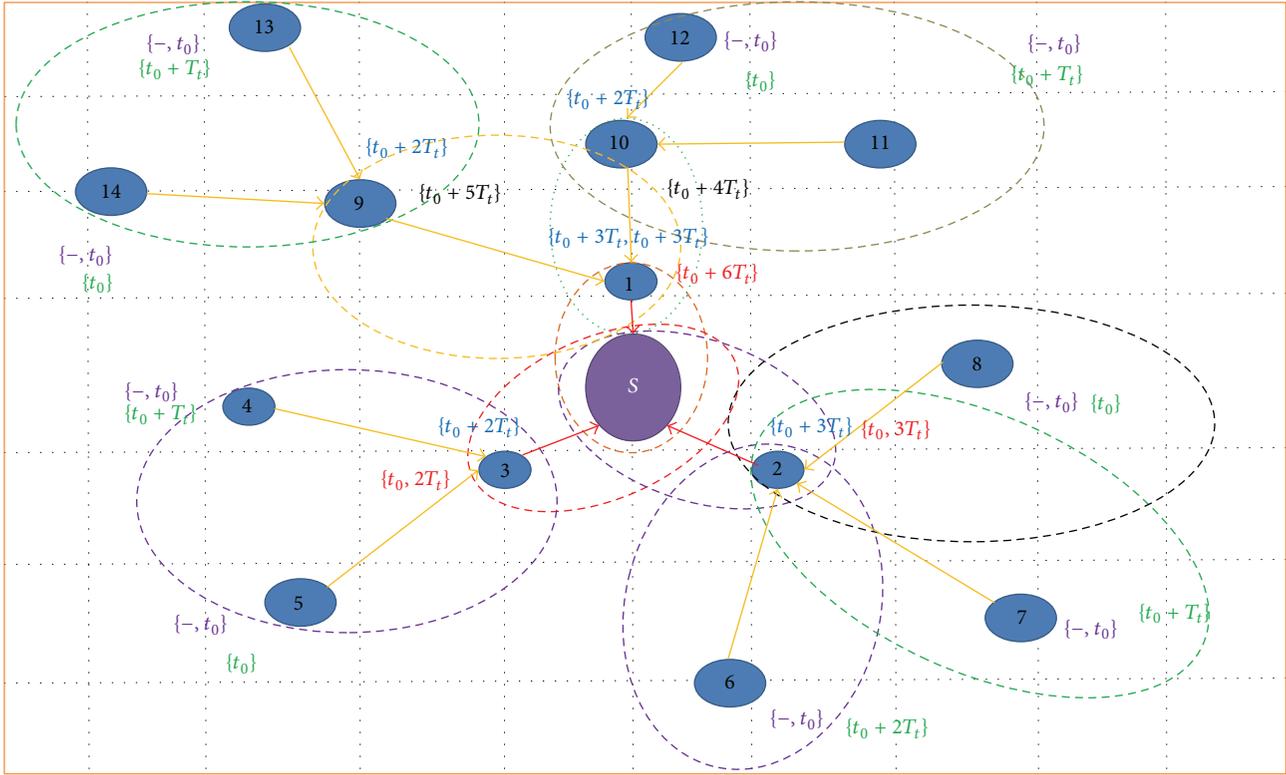


FIGURE 6: Building TRT and TRR scheduling time.

the data transfer. A tree rooted at the sink is formed and then data is collected using a TDMA scheduling technique. PRRP assumes that node can only join its neighbor which is available within the same tier. In such case, the minimum distance is ensured and so energy can be saved during data transfer, whereby each node will select a parent among its closest neighbors to avoid a long distance data transfer. Consequently, the transmission range for nodes is always short. Each node can listen to the transmission of the nodes close to it or available within the same tier. This technique guarantees the distance among communicating nodes is minimum for data transfer hence saving energy.

4. Performance Evaluations

4.1. Simulation Parameters. Simulation parameters are shown in Table 1, while few assumptions were made on the basis widely available in literature review such as the fact that there will be no message loss as the physical channel will be reliable. The coverage of the radio is in circular direction and antenna is in omnidirection; nodes are distributed in open area [81, 82].

4.2. Comparative Analysis between PRRP and LEACH. In this section, it is attempted to compare PRRP protocol with LEACH. Principally, PRRP is similar to LEACH protocol in which any node can communicate with the sink and the data collection or transmission mechanism is the time based schedule. The differences between them lie on several factors.

Firstly, in LEACH the clusters and cluster heads are formed within each cluster for the data transmission. Those cluster heads normally are responsible for collecting the data from their related clusters and then transfer it to the sink. On the other hand, a tree in PRRP is constructed rooted to the sink and the gateways are responsible for transferring the data to the sink. Finally, the number of children is less in PRRP compared with LEACH. On comparing the performance evaluation among LEACH and PRRP on different aspects such as energy efficiency, number of live nodes, network throughput/goodput, and average consumed energy per packet for different data transmission periods, it is observed that, in LEACH, there are two types of sensor nodes such as nonhead node and cluster head while in PRRP there are three types of the sensor nodes such as gateway nodes, leaf nodes, and nonleaf nodes. Energy can be consumed in both protocols during transmitting, receiving, and idle listening state.

While comparing both protocols after several periods of data transmission, PRRP showed significant improvement as illustrated in Figure 9, collectively for all rounds together including 1, 5, and 10 rounds altogether. Simulation results illustrate that with PRRP nodes can stay longer and utilize their maximum possible energy for longer time period. For example, after a 10-round test run, the figure shows that the last node of the LEACH protocol dies after 275 seconds while PRRP nodes start dying after 350 seconds.

4.2.1. Comparative Analysis: Total Energy Consumed. In PRRP, during tree formation phase nodes can transmit signals

TABLE 1: Simulation parameters.

Parameter	Value
Network area	200 m × 200 m or 400 m × 400 m
Number of sensors	200 or 400
Sensor distribution	Uniform random
Location of the sink	Center of the area
Radio range	50 m
MAC layer	IEEE 802.11
Unusual event sources	4
Routine data source probability	P
Failure rate	F
Time-out constant	$1/r$
Delay for retransmission M	0.02 s
Maximum communication distance between two nodes (d)	$\sqrt{2} \times 5$ m
Electronics energy (E_{elec})	50 nJ/bit
Amplifier energy (E_{amp})	100 pJ/bit/m ²
Initial energy in each node	2 J
Control packet size	48 bytes
Data packet size	100 bytes
$E_{\text{threshold}}$ (single data transmission period)	4×10^{-4} J
E_{th} (initial)	1 J
e	0.5

with minimum energy level as closer node can be selected by the parent which saves the node energy by reducing distance. In PRRP, parent can be any node and can select the closer nodes to save its energy level. However, LEACH does not consider the location or the distance among nodes with an assumption that each node can hear all other nodes in the network. The transmission distance is shorter in PRRP. In LEACH, the main reasons for energy consumption are, for example, longer distance among the nodes and cluster head and that nodes randomly advertise themselves as cluster heads based on the energy level of the nodes. In LEACH, with most of the cases nominated cluster heads are at longer distance from the normal nodes which becomes one more reason for energy loss compared to PRRP. Furthermore, by comparing nonleaf node and the cluster head node of LEACH, it can be seen that nonleaf nodes in PRRP consume little energy due to the idle listening state while they wait to receive and transmit data at the specific time slots only, while LEACH has different approach completely. In addition each cluster head has more number of children compared to PRRP and cluster head requires more time to be in ON state which becomes one more reason for comparatively more energy loss than PRRP.

Figure 10 shows an illustration for different rounds among LEACH and PRRP; if compared with 10 data transmission periods at ($t = 150$) seconds, total consumed energy is around 220 J in LEACH and 120 J in PRRP. The consumed energy is dropped which is quite significant, though PRRP shows significant improvement for overall energy consumed compared till the end of the network lifetime and higher throughput for the same initial energy level.

4.2.2. Comparative Analysis on per Packet Average Consumed Energy. When comparing PRRP with LEACH on the basis of average energy consumed per packet, it is found that PRRP consumes less energy as shown in Figure 11. The observations show that, in PRRP with the initial data transmission periods, the average consumed energy is higher. On the other hand, when comparing PRRP and LEACH with more rounds of data transfer, it is found that PRRP is more efficient than LEACH. The reason for more average energy consumed in the initial round in PRRP protocol with single data transmission phase is that the initial setup cost is little higher and energy consumed in initial phases is considered to be overhead energy. However, PRRP outperforms LEACH for average per packet energy use after completing its entire round.

4.2.3. Comparative Analysis on the Basis of Throughput. Table 2 describes the network throughput comparison between LEACH and PRRP in terms of the data packets delivery to the sink. Simulation results show significant improvement of network throughput for all rounds including 01, 05, and 10. PRRP saves a great amount of energy during data transmission phase for multiple periods. Overall significant performance improvement is seen based on several factors such as enhancement in the network life time, energy efficiency, and utilizing maximum possible energy of each individual sensor network node; with the increase in rounds, the network throughput even increases more.

4.3. Comparative Analysis between PRRP and CELRP. This section is aimed at comparing PRRP and CELRP based on

TABLE 2: A comparison between PRRP and LEACH in terms of throughput.

Periods	PRRP	LEACH	Improvement with PRRP in %
1 data transmission period	15834	3607	4.38 times
5 data transmission periods	53950	13045	4.13 times
10 data transmission periods	64100	25640	2.50 times

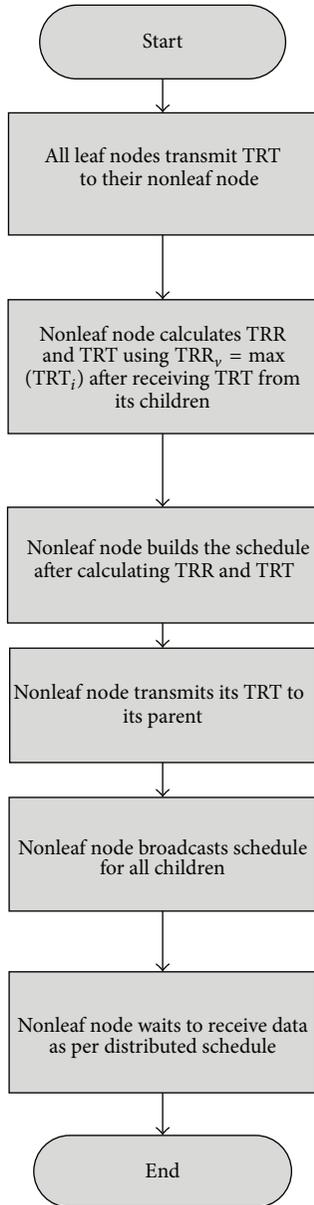


FIGURE 7: Flow chart for building time schedule.

their operation and node types, as described earlier that in PRRP there are three types of the nodes including nonleaf node, leaf node, and gateway nodes, while in CELRP the situation is different where nodes are either cluster head or nonhead nodes while cluster head leader (CHL) can be chosen from available cluster heads. The sink in CELRP is

placed outside of the network which increased the distance from among the cluster heads, cluster head leaders, and the sink, while the situation is different with PRRP where the sink is placed in the center of the network and all nodes are fairly distributed around it which becomes one of the main reasons for lower distance among the nodes and the sink. Figure 12 shows a great difference among PRRP and CELRP for different periods such as 01, 05, and 10. PRRP outperforms CELRP with the increase of periods as it can be observed. PRRP allows any node to become gateway provided on its energy level, if it distributes fairly energy consumption for the entire network, while the situation is the different in CELRP.

4.3.1. Comparative Analysis: Total Energy Consumed. Tree building, effective TDMA scheduling, and data transmission phases are the strength of PRRP; each phase has an edge over CELRP. In PRRP, during tree building nodes normally transmit signals with minimum energy level as closer nodes can be selected by the parents. This technique is ensuring to reduce the distance among the parent and child node as energy can be saved during data transmission. In addition with PRRP the sink is also placed in the center of the network to reduce the overall distance for each sensor node including leaf node, nonleaf node, and gateways. PRRP also has consideration for location of neighboring nodes in order to reduce the data transmitting distance. The situation is different with CELRP where nodes can act as normal nodes, cluster heads, and cluster head leaders while sink is placed outside the distance. Hence longer data transmission distances become one of the major reasons for more energy loss compared with PRRP. Figure 13 shows significant difference among results for total consumed energy for different rounds such as 01, 05, and 10, respectively. In PRRP an effective TDMA schedule is also implemented for transmitting data on their respective times and in addition to keep nodes ON only for required time slots which has great effects on overall energy efficiency of sensor network and can be observed through Figure 13.

As an illustration, we can compare results of PRRP and CELRP at any stage in Figure 13; consider for 10 data transmission periods at $(t = 150)$ seconds consumed energy is 230 J in CELRP and 140 J in PRRP. The consumed energy is dropped which is quite significant. Overall performance of PRRP over CELRP is significant as can be noticed from Figure 13.

4.3.2. Comparative Analysis: Per Packet Average Consumed Energy. In this analysis, PRRP and CELRP protocol are compared on the basis of the average consumed energy per packet as shown in Figure 14. It is found from our observations that CELRP initially shows good performance for average energy per packet compared to PRRP. However, after a short span

Node 14	T						
Node 13		T					
Node 12	T						
Node 11		T					
Node 10	R	R		T			
Node 9	R	R			T		
Node 1				R	R	R	T
Sink			R	R			R
Node 3	R	R	T				
Node 2	R	R	R	T			
Node 4		T					
Node 7		T					
Node 5	T						
Node 6			T				
Node 8	T						
Time slot	t_0	$t_0 + T_t$	$t_0 + 2T_t$	$t_0 + 3T_t$	$t_0 + 4T_t$	$t_0 + 5T_t$	$t_0 + 6T_t$

FIGURE 8: Data transmission scheduling.

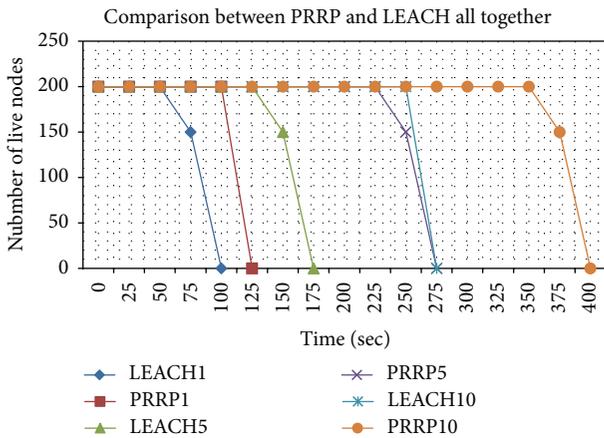


FIGURE 9: Number of live nodes versus time (collectively for 1, 5, and 10 rounds).

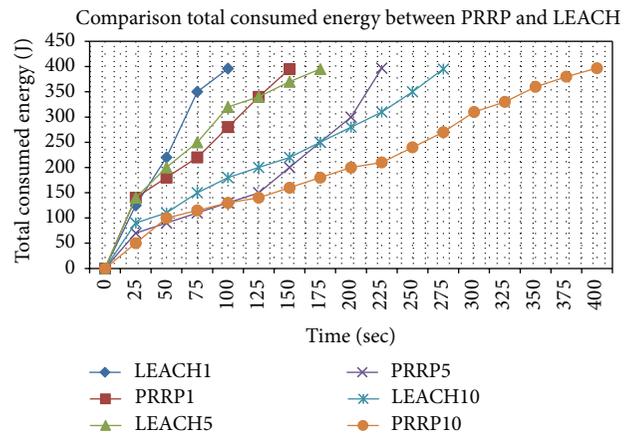


FIGURE 10: Total consumed energy versus time (LEACH and PRRP).

of time PRRP shows a significant improvement in it with the increased number of data periods.

On the other hand, when comparing PRRP and CELRP with more rounds of data transfer, it is found that PRRP is more efficient than CELRP. In PRRP, the reason for more average energy consumed at the initial round is that the three initial phases are for setup and there is no data transmission during this. So, the energy consumed in these initial phases is considered to be overhead energy, which is more than the energy saved in data transmission phase for first period. PRRP stands for high performance for average per packet energy use after completing its entire round and especially after continuing its several transmission periods with its initial build tree.

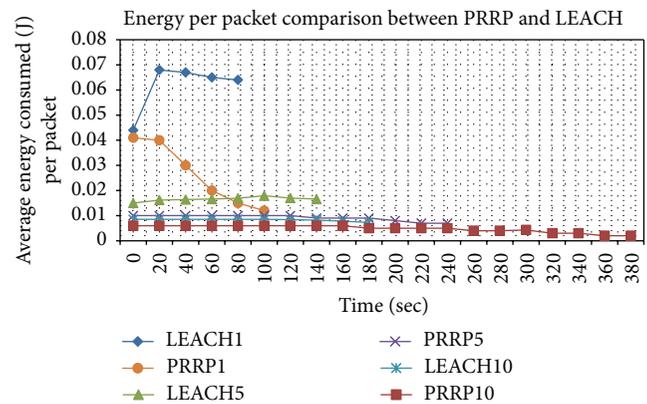


FIGURE 11: Average consumed energy per packet (PRRP and LEACH).

TABLE 3: A comparison between PRRP and CELRP in terms of throughput.

Periods	PRRP	CELRP	Improvement with PRRP%
1 data transmission period	16733	5950	2.81 times
5 data transmission periods	54555	19985	2.72 times
10 data transmission periods	65305	35710	1.82 times

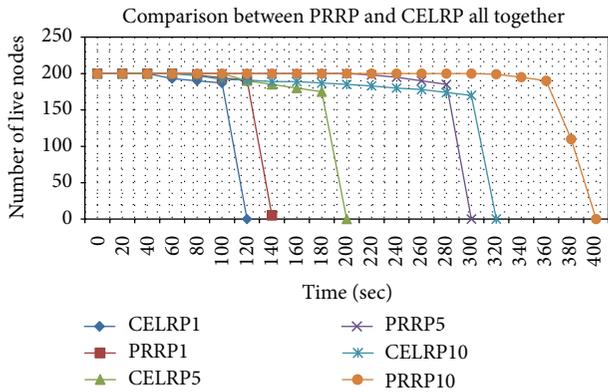


FIGURE 12: Number of live nodes versus time (PRRP and LEACH collectively).

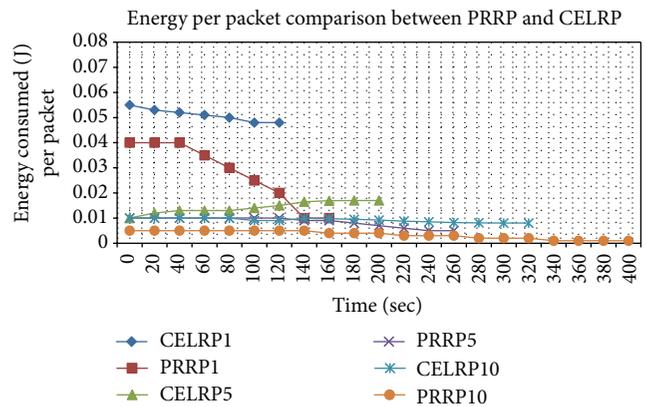


FIGURE 14: Average consumed energy per packet (PRRP and CELRP).

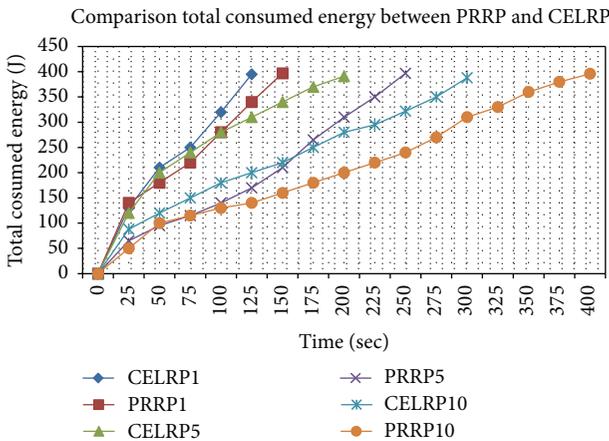


FIGURE 13: Total consumed energy versus time (CELRP and PRRP).

4.3.3. *Comparative Analysis on the Basis of Throughput.* Following Table 3 describes the network throughput comparison between PRRP and CELRP in term of the data packets delivery to the sink. Simulation results show significant improvement of network throughput for all rounds including 01, 05, and 10. PRRP saves a great amount of energy during data transmission phase for multiple periods. Overall significant performance improvement is seen based on several factors such as enhancement in the network life time, energy efficiency, and utilizing maximum possible energy of each individual sensor network node; with the increase in rounds, the network throughput even increases more.

5. Conclusion

The performance of PRRP is evaluated on the basis of energy lifetime, average energy consumption of the network both individually and per packet basis, and the network throughput. The theme is to discuss the results of PRRP and its performance as compared to the existing routing protocols such as LEACH and CELRP. PRRP shows better results when compared with LEACH, where PRRP shows an impressive performance in the form of improving the network lifetime (by reducing the energy consumption) and the network throughput. The throughput is increased by 2.5 times and network lifetime is improved by more than 50% while the energy consumption per packet is reduced to less than 50%. The comparative analysis of PRRP against CELRP shows that PRRP increased the throughput of the network by 1.82 times, network lifetime is improved more than 35%, and the energy consumption is reduced by more than 35%.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

- [1] E. A. Basha, S. Ravela, and D. Rus, "Model-based monitoring for early warning flood detection," in *Proceedings of the 6th ACM Conference on Embedded Networked Sensor Systems (SenSys '08)*, pp. 295–308, New York, NY, USA, November 2008.
- [2] A. Ellaboudy, K. Pister, and EECS Department UC Berkeley, "Outlet power monitoring using wireless sensor networks,"

- Tech. Rep. UCB/EECS-2012-152, Electrical Engineering & Computer Sciences Department, Fremont, Calif, USA, 2012, <http://www.eecs.berkeley.edu/Pubs/TechRpts/2012/EECS-2012-152.html>.
- [3] G. Zhao, "Wireless sensor networks for industrial process monitoring and control: a survey," *Network Protocols and Algorithms*, vol. 3, no. 1, pp. 47–63, 2011.
 - [4] M. Paavola, "Wireless technologies in process automation—a review and an application example," Report A 33, Control Engineering Laboratory, University of Oulu, Oulu, Finland, 2007.
 - [5] K. Maraiya, K. Kant, and N. Gupta, "Application based Study on Wireless Sensor Network," *International Journal of Computer Applications*, vol. 21, no. 8, pp. 9–15, 2011.
 - [6] M. Erol-Kantarci and H. T. Mouftah, "Wireless multimedia sensor and actor networks for the next generation power grid," *Ad Hoc Networks*, vol. 9, no. 4, pp. 542–551, 2011.
 - [7] B. Lu and V. C. Gungor, "Online and remote motor energy monitoring and fault diagnostics using wireless sensor networks," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 11, pp. 4651–4659, 2009.
 - [8] V. C. Gungor and F. C. Lambert, "A survey on communication networks for electric system automation," *Computer Networks*, vol. 50, no. 7, pp. 877–897, 2006.
 - [9] J. Buckley, K. Aherne, B. O'Flynn, J. Barton, A. Murphy, and C. O'Mathuna, "Antenna performance measurements using wireless sensor networks," in *Proceedings of the IEEE 56th Electronic Components and Technology Conference*, pp. 1652–1657, San Diego, Calif, USA, May 2006.
 - [10] S.-H. Yang, "Principals of wireless sensor networks," in *Wireless Sensor Networks Principles, Design and Applications*, Signals and Communication Technology, pp. 7–47, Springer, London, UK, 2014.
 - [11] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: a survey," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 6–27, 2004.
 - [12] K. Kaur and B. Singh, "Wireless sensor network based: design principles & measuring performance of IDS," *International Journal of Computer Applications*, vol. 1, no. 28, pp. 94–99, 2010.
 - [13] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–105, 2002.
 - [14] M. Chu, H. Haussecker, and F. Zhao, "Scalable information-driven sensor querying and routing for ad hoc heterogeneous sensor networks," *International Journal of High Performance Computing Applications*, vol. 16, no. 3, pp. 293–313, 2002.
 - [15] S. K. Singh, M. Singh, and D. K. Singh, "Routing protocols in wireless sensor networks—a survey," *International Journal of Computer Science & Engineering Survey*, vol. 1, no. 2, pp. 63–83, 2010.
 - [16] G. Kalpana and T. Bhuvaneshwari, "A survey on energy efficient routing protocols for wireless sensor networks," *International Journal of Computer Applications*, vol. 86, no. 12, pp. 12–18, 2011.
 - [17] Q. Cao, T. Abdelzaher, T. He, and R. Kravets, "Cluster-based forwarding for reliable end-to-end delivery in wireless sensor networks," in *Proceedings of the 26th IEEE International Conference on Computer Communications (IEEE INFOCOM '07)*, pp. 1928–1936, Anchorage, Alaska, USA, May 2007.
 - [18] R. Singh and G. Mittal, "Lifetime enhancement of cluster head selection for MIMO routing algorithm based on weighted sum method for WSN," *International Journal of Engineering Research and Applications*, vol. 3, no. 5, pp. 1894–1898, 2013.
 - [19] S. Manda, N. Archana, and N. Umarani, "Maximizing the lifetime of wireless sensor networks using CRT based packet splitting algorithm," *International Journal of Advancements in Research & Technology*, vol. 2, no. 4, pp. 48–58, 2013.
 - [20] A. E. A. A. Abdulla, H. Nishiyama, and N. Kato, "Extending the lifetime of wireless sensor networks: a hybrid routing algorithm," *Computer Communications Journal*, vol. 35, no. 9, pp. 1056–1063, 2012.
 - [21] J. Bahi, M. Haddad, M. Hakem, and H. Kheddouci, "Efficient distributed lifetime optimization algorithm for sensor networks," *Ad Hoc Networks*, vol. 16, pp. 1–12, 2014.
 - [22] D. Ebrahimi and C. Assi, "Compressive data gathering using random projection for energy efficient wireless sensor networks," *Ad Hoc Networks*, vol. 16, no. 1, pp. 105–119, Feb 2014.
 - [23] J.-Y. Chang and P.-H. Ju, "An energy-saving routing architecture with a uniform clustering algorithm for wireless body sensor networks," *Future Generation Computer Systems*, vol. 35, pp. 128–140, 2014.
 - [24] R. S. Bhadoria and D. G. Chandra, "Routing protocol in Wireless Sensor Networks," in *Proceedings of the 2nd IEEE Conference on Parallel Distributed and Grid Computing*, vol. 35, no. 1, pp. 128–140, February 2012.
 - [25] N. Gautam, W.-I. Lee, and J.-Y. Pyun, "Track-sector clustering for energy efficient routing in wireless sensor networks," in *Proceedings of the IEEE 9th International Conference on Computer and Information Technology (CIT '09)*, pp. 116–121, IEEE, Xiamen, China, October 2009.
 - [26] M. T. Nguyen, "Minimizing energy consumption in random walk routing for wireless sensor networks utilizing compressed sensing," in *Proceedings of the 8th International Conference on System of Systems Engineering (SoSE '13)*, pp. 297–301, IEEE, Maui, Hawaii, USA, June 2013.
 - [27] B. Nazir and H. Hasbullah, "Energy efficient and QoS aware routing protocol for Clustered Wireless Sensor Network," *Computers and Electrical Engineering*, vol. 39, no. 8, pp. 2425–2441, 2013.
 - [28] B. Nazir and H. Hasbullah, "Mobile Sink based Routing Protocol (MSRP) for prolonging network lifetime in clustered wireless sensor network," in *Proceedings of the International Conference on Computer Applications and Industrial Electronics (ICCAIE '10)*, pp. 624–629, Kuala Lumpur, Malaysia, December 2010.
 - [29] W. M. Aioffi, G. R. Mateus, and F. P. Quintao, "Optimization issues and algorithms for wireless sensor networks with mobile sink," in *Proceedings of the International Network Optimization Conference Spa*, pp. 1–6, Spa, Belgium, April 2007.
 - [30] A. Waheed Khan, A. H. Abdullah, M. H. Anisi, and J. Iqbal Bangash, "A comprehensive study of data collection schemes using mobile sinks in wireless sensor networks," *Sensors*, vol. 14, no. 2, pp. 2510–2548, 2014.
 - [31] M. Di Francesco and S. K. Das, "Data collection in wireless sensor networks with mobile elements: a survey," *ACM Transactions on Sensor Networks (TOSN)*, vol. 8, no. 1, article 7, 2011.
 - [32] M. T. Nguyen and N. Rahnavard, "Cluster-based energy-efficient data collection in wireless sensor networks utilizing compressive sensing," in *Proceedings of the IEEE Military Communications Conference (MILCOM '13)*, pp. 1708–1713, November 2013.
 - [33] H. Lee and K. Lee, "Energy minimization for flat routing and hierarchical routing for wireless sensor networks," in *Proceedings of the 2nd International Conference on Sensor*

- Technologies and Applications (SENSORCOMM '08)*, pp. 735–742, Cap Esterel, France, August 2008.
- [34] B. He and H. Zhang, “An energy optimization method for wireless sensor network,” in *Proceedings of the Automatic International Conference on Control and Artificial Intelligence (ACAI '12)*, pp. 402–406, IEEE, Xiamen, China, March 2012.
- [35] V. Rodoplu and T. H. Meng, “Minimum energy mobile wireless networks,” *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, pp. 1333–1344, 1999.
- [36] W.-Y. Zhang, Z.-Z. Liang, Z.-G. Hou, and M. Tan, “A power efficient routing protocol for wireless sensor network,” in *Proceedings of the IEEE International Conference on Networking, Sensing and Control (ICNSC '07)*, pp. 20–25, IEEE, London, UK, April 2007.
- [37] T. Liu and F. Li, “Power-efficient clustering routing protocol based on applications in wireless sensor network,” in *Proceedings of the 5th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '09)*, pp. 1–6, Beijing, China, September 2009.
- [38] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy-efficient communication protocol for wireless micro-sensor networks,” in *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences (HICSS '00)*, vol. 8, p. 8020, Maui, Hawaii, USA, January 2000.
- [39] A. Manjeshwar and D. P. Agrawal, “TEEN: a protocol for enhanced efficiency in wireless sensor networks,” in *Proceedings of the 15th International Parallel and Distributed Processing Symposium*, pp. 305–312, IEEE, San Francisco, Calif, USA, April 2000.
- [40] A. Manjeshwar and D. P. Agrawal, “APTEEN: a hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks,” in *Proceedings of the 2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing*, pp. 215–221, Ft. Lauderdale, Fla, USA, April 2002.
- [41] S. Lindsey and C. S. Raghavendra, “PEGASIS: power-efficient gathering in sensor information systems,” in *Proceedings of the Aerospace Conference*, pp. 1125–1130, IEEE, March 2002.
- [42] L. Li and J. Y. Halpern, “Minimum energy mobile wireless networks revisited,” in *Proceedings of the IEEE International Conference on Communications (ICC '01)*, pp. 93–100, Helsinki, Finland, June 2001.
- [43] L. Subramanian and R. H. Katz, “An architecture for building self-configurable systems,” in *Proceedings of the 1st Annual Workshop on Mobile and Ad Hoc Networking and Computing (MobiHOC '00)*, pp. 63–73, Boston, Mass, USA, August 2000.
- [44] Q. Li, J. Aslam, and D. Rus, “Hierarchical power-aware routing in sensor networks,” in *Proceedings of the DIMACS Workshop on Pervasive Networking*, pp. 47–52, May 2001.
- [45] J. N. Al-Karaki, R. Ul-Mustafa, and A. E. Kamal, “Data aggregation in wireless sensor networks—exact and approximate algorithms,” in *Proceedings of the Workshop on High Performance Switching and Routing (HPSR '04)*, pp. 241–245, Phoenix, Ariz, USA, April 2004.
- [46] Q. Fang, F. Zhao, and L. Guibas, “Lightweight sensing and communication protocols for target enumeration and aggregation,” in *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC '03)*, pp. 165–176, Annapolis, Md, USA, June 2003.
- [47] F. Ye, H. Luo, J. Cheng, S. Lu, and L. Zhang, “A two-tier data dissemination model for large-scale wireless sensor networks,” in *Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MOBICOM '02)*, pp. 148–159, ACM/IEEE Press, Atlanta, Ga, USA, September 2002.
- [48] N. Zaman, L. T. Jung, and V. Ponnusamy, “Application of self-healing in wireless sensor network: a survey,” in *Biologically-Inspired Energy Harvesting through Wireless Sensor Technologies*, pp. 217–218, IGI Global, 2016.
- [49] N. Zaman, T. J. Low, and T. Alghamdi, “Enhancing routing energy efficiency of wireless sensor networks,” in *Proceedings of the 17th IEEE International Conference on Advanced Communications Technology (ICACT '15)*, vol. 4, no 2, pp. 587–595, GiRI (Global IT Research Institute), Seoul, Republic of Korea, July 2015.
- [50] Nurhayati, S. H. Choi, and K. O. Lee, “A cluster based energy efficient location routing protocol in wireless sensor network,” *International Journal of Computers and Communications*, vol. 5, no. 2, pp. 67–74, 2011.
- [51] N. Zaman and A. Abdullah, “Energy efficient routing in wireless sensor network: research issues and challenges,” in *Proceedings of the IEEE International Conference on Intelligence and Information Technology (ICIIT '10)*, pp. 239–243, 2010.
- [52] N. Zaman, L. Tang Jung, F. Alsaade, and T. Alghamdi, “Wireless Sensor Network (WSN): routing security, reliability and energy efficiency,” *Journal of Applied Sciences*, vol. 12, no. 6, pp. 593–597, 2012.
- [53] A. Noor Zaman and A. Abdullah, “Different techniques towards enhancing Wireless Sensor Network (WSN) routing energy efficiency and Quality of Service (QoS),” *World Applied Science Journal (WASJ)*, vol. 13, no. 4, pp. 798–805, 2011.
- [54] N. Zaman, A. B. Abdullah, and L. T. Jung, “Optimization of energy usage in Wireless Sensor Network using Position Responsive Routing Protocol (PRRP),” in *Proceedings of the IEEE Symposium on Computers & Informatics (ISCI '11)*, pp. 51–55, Kuala Lumpur, Malaysia, March 2011.
- [55] N. Zaman and A. B. Abdullah, “Position Responsive Routing Protocol (PRRP),” in *Proceedings of the 13th International Conference on Advanced Communication Technology: Smart Service Innovation through Mobile Interactivity (ICACT '11)*, pp. 644–648, Seoul, Republic of Korea, February 2011.
- [56] N. Zaman, “Energy Optimization through Position Responsive Routing Protocol (PRRP) in wireless sensor network,” *International Journal of Information and Electronics Engineering*, vol. 2, no. 5, pp. 748–751, 2012.
- [57] N. Zaman, T. J. Low, and T. Alghamdi, “Energy efficient routing protocol for wireless sensor network,” in *Proceedings of the 16th International Conference on Advanced Communication Technology (ICACT '14)*, pp. 808–814, IEEE, Pyeongchang, South Korea, February 2014.
- [58] Y. Xu, J. Heidemann, and D. Estrin, “Geography-informed energy conservation for ad hoc routing,” in *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (MobiCom '01)*, pp. 215–222, Rome, Italy, July 2001.
- [59] Y. Yu, D. Estrin, and R. Govindan, “Geographical and energy aware routing: a recursive data dissemination protocol for wireless sensor networks,” Tech. Rep. UCLA/CSD-TR-01-0023, UCLA Computer Science Department, Los Angeles, Calif, USA, 2001.
- [60] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, “Span: an energy-efficient coordination algorithm for topology maintenance in Ad Hoc wireless networks,” in *Proceedings of the 7th ACM International Conference on Mobile Computing and Networking*, pp. 315–322, July 2001.

- [61] I. Stojmenovic and X. Lin, "GEDIR: loop-free location based routing in wireless networks," in *Proceedings of the International Conference on Parallel and Distributed Computing and Systems*, pp. 109–115, Boston, Mass, USA, November 1999.
- [62] F. Kuhn, R. Wattenhofer, and A. Zollinger, "Worst-case optimal and average-case efficient geometric ad-hoc routing," in *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC '03)*, pp. 267–278, Annapolis, Md, USA, June 2003.
- [63] J. Kulik, W. Heinzelman, and H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks," *Wireless Networks*, vol. 8, no. 2, pp. 169–185, 2002.
- [64] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," in *Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '00)*, pp. 93–99, Boston, Mass, USA, August 2000.
- [65] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, "Directed diffusion for wireless sensor networking," *IEEE/ACM Transactions on Networking*, vol. 11, no. 1, pp. 2–16, 2003.
- [66] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next century challenges: scalable coordination in sensor networks," in *Proceeding of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '99)*, pp. 263–270, Seattle, Wash, USA, August 1999.
- [67] D. Braginsky and D. Estrin, "Rumor routing algorithm for sensor networks," in *Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications (ACM WSNA '02)*, pp. 22–31, Atlanta, Ga, USA, October 2002.
- [68] C. Schurgers and M. B. Srivastava, "Energy efficient routing in wireless sensor networks," in *Proceedings of the Communications for Network-Centric Operations: Creating the Information Force (MILCOM '01)*, pp. 155–161, McLean, Va, USA, 2001.
- [69] S. M. Hedetniemi, S. T. Hedetniemi, and A. L. Liestman, "A survey of gossiping and broadcasting in communication networks," *Networks*, vol. 18, no. 4, pp. 319–349, 1988.
- [70] F. Ye, A. Chen, S. Lu, and L. Zhang, "A scalable solution to minimum cost forwarding in large sensor networks," in *Proceedings of the 10th International Conference on Computer Communications and Networks (ICCCN '01)*, pp. 304–309, Scottsdale, Ariz, USA, October 2001.
- [71] Y. Yao and J. Gehrke, "The cougar approach to in-network query processing in sensor networks," *SIGMOD Record*, vol. 31, no. 3, pp. 9–18, 2002.
- [72] M. Chu, H. Haussecker, and F. Zhao, "Scalable information-driven sensor querying and routing for ad hoc heterogeneous sensor networks," *The International Journal of High Performance Computing Applications*, vol. 16, no. 3, pp. 293–313, 2002.
- [73] N. Sadagopan, B. Krishnamachari, and A. Helmy, "The ACQUIRE mechanism for efficient querying in sensor networks," in *Proceedings of the 1st International Workshop on Sensor Network Protocol and Application (SNPA '03)*, pp. 149–155, Anchorage, Alaska, USA, May 2003.
- [74] R. C. Shah and J. M. Rabaey, "Energy aware routing for low energy ad hoc sensor networks," in *Proceedings of the Wireless Communications and Networking Conference (WCNC '02)*, pp. 350–355, IEEE, March 2002.
- [75] A. Savvides, C.-C. Han, and M. B. Srivastava, "Dynamic fine-grained localization in ad-hoc networks of sensors," in *Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '01)*, pp. 166–179, Rome, Italy, July 2001.
- [76] D. Niculescu and B. Nath, "DV based positioning in Ad Hoc networks," *Telecommunication Systems*, vol. 22, no. 1–4, pp. 267–280, 2003.
- [77] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less low-cost outdoor localization for very small devices," *IEEE Communications Magazine*, vol. 7, no. 5, pp. 28–34, 2000.
- [78] S. Mishra and A. Nasipuri, "An adaptive low power reservation based MAC protocol for wireless sensor networks," in *Proceedings of the 23rd IEEE International Performance, Computing, and Communications Conference, Conference Proceedings (IPCCC '04)*, pp. 731–736, April 2004.
- [79] N. Bulusu, D. Estrin, L. Girod, and J. Heidemann, "Scalable coordination for wireless sensor networks: self-configuring localization system," in *Proceedings of the 6th International Symposium on Communication Theory and Application (ISCTA '01)*, pp. 75–82, Ambleside, UK, July 2001.
- [80] E. Amiri, H. Keshavarz, M. Alizadeh, M. Zamani, and T. Khodadadi, "Energy efficient routing in wireless sensor networks based on fuzzy ant colony optimization," *International Journal of Distributed Sensor Networks*, vol. 2014, Article ID 768936, 17 pages, 2014.
- [81] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660–670, 2002.
- [82] A. Boukerche, X. Cheng, and J. Linus, "A performance evaluation of a novel energy-aware data-centric routing algorithm in wireless sensor networks," *Wireless Networks*, vol. 11, no. 5, pp. 619–635, 2005.

Review Article

Information Security of PHY Layer in Wireless Networks

Weidong Fang,^{1,2} Fengrong Li,² Yanzan Sun,¹ Lianhai Shan,^{3,4} Shanji Chen,⁵
Chao Chen,⁵ and Meiju Li⁵

¹Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Shanghai University, Shanghai 200444, China

²Key Laboratory of Wireless Sensor Network & Communication, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 201899, China

³Shanghai Internet of Things Co., Ltd., Shanghai 201899, China

⁴Shanghai Research Center for Wireless Communications, Shanghai 200335, China

⁵College of Physics and Electronic Information Engineering, Qinghai University for Nationalities, Xining, Qinghai 810000, China

Correspondence should be addressed to Fengrong Li; lifengrongsim@mail.sim.ac.cn

Received 2 December 2015; Accepted 16 February 2016

Academic Editor: Fei Yu

Copyright © 2016 Weidong Fang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Since the characteristics of wireless channel are open and broadcasting, wireless networks are very vulnerable to be attacked via eavesdropping, jamming, and interference. As traditional secure technologies are not suitable for PHY layer of wireless networks, physical-layer security issues become a focus of attention. In this paper, we firstly identify and summarize the threats and vulnerabilities in PHY layer of wireless networks. Then, we give a holistic overview of PHY layer secure schemes, which are divided into three categories: spatial domain-based, time domain-based, and frequency domain-based. Along the way, we analyze the pros and cons of current secure technologies in each category. In addition, we also conclude the techniques and methods used in these categories and point out the open research issues and directions in this area.

1. Introduction

With the development of information technology, wireless networks have evolved from initial single networks into multimode, multistandard networks (3G, 4G, wireless sensor networks, ad hoc networks, etc.), which made mobile users convenient to access. However, because of broadcast nature of wireless communication, dynamic topology, mobility, signal channel instability, and so forth [1], they are also vulnerable to various security threats and attacks such as DoS (Denial of Service), counterfeiting, tampering, leakage, interference, network flooding, eavesdropping, and traffic analysis [2]. Particularly, with the popularity of intelligent terminals, some bad information, such as obscenity information, viruses, and Trojans, becomes more and more widespread [3]. This bad information not only occupies lots of user's traffic, but also endangers the privacy of users. Therefore, the issue of information security has become a key challenge to the development of wireless networks.

To solve the issues of information security threats and attacks in wireless networks, the traditional technologies mainly focus on encryption/decryption [4], trust management [5, 6], authentication [7], and so forth. However, for complex structure of wireless networks, only depending on encryption/decryption method is not enough to ensure the information security of wireless networks. For example, it cannot eliminate the issues of eavesdropping and interference in PHY layer. Fortunately, with the emergence of new technologies, some novel security technologies can overcome the above drawbacks in PHY layer, such as cooperative techniques [8, 9] and structured signaling schemes [10]. For one thing, these technologies can make full use of the characteristics of the wireless channel for information transmission without high computational complexity. For another thing, they can also eliminate or mitigate the risks of intentional or unintentional security attacks and interferences by means of spread spectrum, random parameter, and so on.

Although Shannon had put forward the Communication Theory of Secrecy Systems in 1948, security technologies of PHY layer were seldom paid attention to by researchers in recent years. In this paper, the threats and vulnerabilities in PHY layer of wireless networks are identified first. The rest of this paper is organized as follows: attack technologies in PHY layer are described and summarized in Section 2. Section 3 illustrates classification of the existing secure schemes. Various secure schemes are analyzed in Section 4. Finally, conclusions are made in Section 5.

2. Attacks to PHY Layer

PHY layer of wireless networks is at the bottom of the network, which is mainly responsible for frequency selection, carrier frequency generation, and signal detection and modulation. Meanwhile, it receives wireless signals from the air interface and transmits the demodulated data stream to the upper layer. Because of PHY layer transmission characteristics, major types of physical attacks include interference, jamming, eavesdropping, and traffic analysis. In general, these attacks fall into two categories: active attacks and passive attacks.

2.1. Active Attacks. Active attacks mainly include interference and jamming. These two kinds of active attacks are implemented similarly in principle by broadcasting interference signals on some specific frequency bands. The differences between them are the different objectives they attack. Jamming attacks by means of continuing occupying the channel cause the transmitter failure. Interference attacks by deteriorating the legal signal result in the receiver failure. Most of the jamming attacks are malicious attacks, and interference suffers not only from hostile attackers, but also from other users around the signal over the same channel or environmental effects. For example, a large number of sensor nodes are randomly distributed in wireless sensor networks (WSNs), and through multihop transmission for communication, signal interferences of transmission to other nodes are very easy.

According to the difference of jamming attack technologies, the common jamming can be divided into spot jamming, sweep jamming, barrage jamming, and deceptive jamming [11]:

- (1) *Spot Jamming.* It mainly focuses on single frequency jamming, by transmitting high enough power to cover the original signal. It is simple and widely applied.
- (2) *Sweep Jamming.* The attacker frequently hops from one frequency to another. The advantage is that it can cover a wide range of frequencies and be an effective attack to frequency hopping technology. However, it cannot cover multiple frequencies at the same time.
- (3) *Barrage Jamming.* It can attack a large range of frequencies at the same time and cause great impact on the user communication under its coverage. Due to limitations of transmission power, the wider the frequency it attacks, the weaker its jamming ability is.

- (4) *Deceptive Jamming.* The attackers transmit forged data packets in the network and make the user receive them as normal data packets. This kind of jamming is not easy to be detected and is very destructive.

The attacker also has two types of interference methods: active interference and passive interference [12]. Active jamming can be further divided into sustained interference, random interference, and on-demand interference [13]:

- (1) *Sustained Interference.* It refers to the attacker continuously sending interference signal, thus affecting user normal communication. Its purpose is long-term occupation of the user channel so that the channel could keep busy. Meanwhile, it interferes with the ongoing data transmission and also destroys the transmitting message.
- (2) *Random Interference.* It refers to the attacker randomly interfering with the user. The interference time and cycle are uncertain. Compared with the sustained interference, it can effectively save the attacker's energy consumption and lead to a great impact on the multihop WSNs.
- (3) *On-Demand Interference.* It is to maintain idle state if the channel is idle. Otherwise, the signal interfered with will be transmitted to interrupt ongoing transmission and information hiding technique is implemented. Direct Sequence Spread Spectrum (DSSS) has low power spectrum density of transmitted signal. Its signal spectrum is similar to noise signal so that it could effectively enhance the information hiding.

The signal bandwidth of interference attacks and jamming attacks can also be classified as narrowband and wideband. The frequency range interfered with is usually narrow in narrowband attack. However, with the development of 3G and 4G technology, the bandwidth of interference and jamming could be up to several megahertz.

2.2. Passive Attacks. Passive attacks are mainly divided into two categories: eavesdropping and traffic analysis. The two attacks are caused by the fundamental characteristic of wireless medium, namely, broadcast. The broadcast nature of wireless communication makes it difficult to shield transmitted signals from unintended recipients, while these legal or illegal users within the transmission range analyze and utilize wireless broadcast signals.

Eavesdropping on the communication information of other users leads to information disclosure problems and can be easily achieved due to open access of wireless channels. Traffic analysis refers to an attacker according to changes in the flow of information in the network, some attacks prompted through extracting information from ongoing transmission. For example, an attacker can judge the base station position according to the changes of network traffic in wireless sensor networks. In a word, the attacker interferes with or captures the base station, which leads to paralysis of the entire wireless sensor networks.

3. Results and Discussion

The theoretical basis behind the concept of information security in PHY layer security transmission, which builds on Shannon's notion of perfect secrecy in 1949 [13], was laid by Wyner [14] and then expanded by Csiszár and Korner [15]. In [16], Shannon proved that there exist channel codes guaranteeing the security of the information if secret key length is longer than or equal to the transmission of information. Wyner proved that source and destination can securely transmit information when the legitimate user's channel condition is superior to the eavesdropper.

Nowadays, with emergence of a variety of novel technologies, many security technology methods in PHY layer are put forward for SIMO (single-input multiple-output), MIMO (multiple-input multiple-output), and relay channel. These schemes have possibly increased the potential secrecy capacity and enhanced PHY layer security using these technologies, which to a certain extent can increase the channel capacity of the networks [17]. Subsequently, the system can enhance the PHY layer security by combining with some other PHY layer security technologies. In [18], Barcelo-Llado et al. proposed the amplify-and-forward compressed sensing (AF-CS) framework to assess the physical-layer secrecy performance when malicious eavesdropping nodes are listening. According to the different types of technology, this section will introduce some common and novel PHY layer security methods from the view of the spatial domain, frequency domain, and time domain [19] and finally conclude security technologies from the point of PHY layer attacks.

3.1. Spatial Domain Technologies. Spatial domain technologies consist of directional antenna, beamforming, and some improved technologies based on beamforming. Through suitable antenna technology of avoiding signal interference or realization of the randomization of the channel parameters, the system can achieve anti-interference and antijamming and resist wiretap.

3.1.1. Directional Antenna and Beamforming Technology. Directional antenna has high transmission power in one or more specific directions with the characteristics of long transmission distance and wide geographical coverage. When the signals were received, the directional antenna made the main beam align with the direction of useful information and the nulling align with the interfering signals. Thereby, the directional antenna could reduce or eliminate the interference signal and achieve the purpose of interference and jamming. At the same time, it avoids or degrades the interference and achieves anti-interference and antijamming goal [19]. Compared to unidirectional antenna, directional antenna can significantly enhance the antijamming performance [20]. It has smaller energy consumption than unidirectional antenna. Meanwhile, in the case of lower transmit power and equal equivalent isotropically radiated power in receiver, the directional antenna can effectively reduce the probability of being detected. Hence, the directional antenna has more invisibility in an adverse environment [21]. With directional antenna miniaturization and gain performance

improvement, it has also been widely used in various wireless mesh networks, ad hoc networks to enhance its performance [22]. The directional antennas can be a good solution to network interference and connectivity issues; it has higher spatial multiplexing and farther transmission distance. However, the cost of directional antenna is relatively higher. Furthermore, the breakthrough of antenna polarization and gain are to exploit the characteristic of complex wireless channel, such as fading or noise.

Beamforming also is a specific alterable directional antenna, named smart antenna, which is composed of a multiantenna array. It can realize the transformation of the antenna beam direction through configuration of number of the antennas, element spacing, and geometry. The antenna radiation direction towards the legitimate receiver could avoid interference [23]. Moreover, because transmitting signal is intense and concentrated, it enhances the ability to resist the eavesdropping [24], jamming, and cross talk among multiple users. However, it cannot apply to some energy limited networks because its power consumption is far higher than the directional antenna using multiantennas. Reference [25] designs joint information beamforming and jamming beamforming to protect both transmit security and receive security for a full-duplex base station. Chen et al. proposed multiantenna secure relaying technologies to aid wireless physical-layer security [26]. The proposed large-scale multiple-input multiple-output (LS-MIMO) relaying technology can solve the problem with short-distance interception under adverse conditions.

At present, smart antenna has been widely applied in 3G and 4G. It also makes the communication rate improve while effectively solving multiuser communication interference issue. Besides, beamforming not only uses multiple antenna arrays, but also uses the cooperative relay for some multinode cooperative relay networks [27].

3.1.2. Random Parameters and Random Antenna Technology. Random parameter is developed based on the beamforming. Random transmission antenna weight causes randomization of received eavesdropper's signals and the trained legitimate users are not affected through channel preestimation. It exploits the redundancy of transmit antenna arrays for deliberate signal randomization. The multiplication of channel parameters and default random coefficient is fixed value, and demodulation is not affected [28]. This randomized array transmission scheme guarantees wireless transmissions with inherent low probability of interception (LPI) via proving the indeterminacy of the eavesdropper's blind deconvolution.

The random antenna is similar to the random parameter. The difference between random antenna and random parameter is that the random antenna can achieve the randomness of the receiver signal, while the random parameter is realized by the random weighting coefficient. The random antenna method is most used in multiple-input and multiple-output systems. In the process of signal transmission, the transmitter transforms the transmitting antenna continuously and randomly, so as to realize the channel randomization between the transmitter and the legal or illegal users [29]. Hong et al. presented a secure multiple-input single-output (MISO)

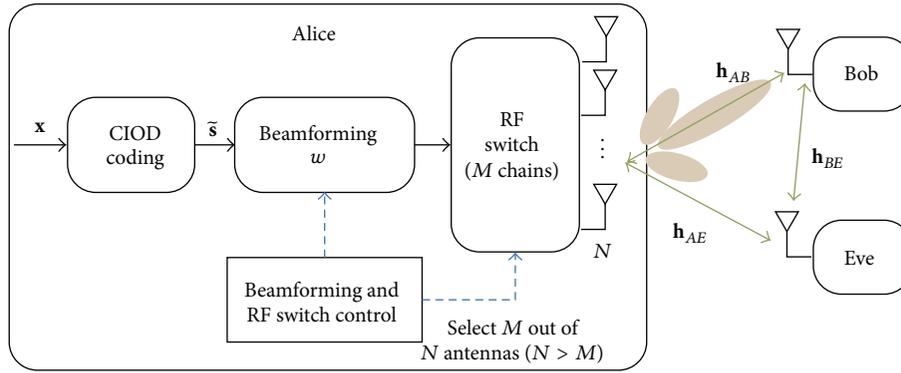


FIGURE 1: System model of ASM with CIOD.

wireless transmission scheme based on a combination of the random Antenna Subset Modulation (ASM) scheme and Coordinate Interleaved Orthogonal Designs (CIOD) [30]. The proposed scheme enjoyed both diversity and array gains to guarantee against potential eavesdropping. The system model was shown in Figure 1. Valliappan et al. proposed ASM scheme to take advantage of massive antenna arrays at mm-wave frequencies [31]. In ASM, the radiation pattern of the array was modulated at the symbol rate to achieve direction dependent data transmission. ASM provided security by introducing additional points in the constellation that appear to be effectively random to an undesired receiver. Similar to the random parameters, the legitimate user after training channel can smoothly demodulate the signal, but the received signal of eavesdropper has confusing superposition. In addition, the allocation of the antennas number can also enhance performance [17]. However, low signal utilization is the inherent weakness of this technology due to its use of multiple transmit antennas.

3.1.3. Artificial Noise Technology. Artificial noise acquires higher secrecy capacity of legitimate channel than that of the eavesdropping channel when the Channel State Information (CSI) of the legitimate channel is better than the eavesdropping channel [14] or deteriorates the eavesdropping channel or optimizes the legitimate channel. The transmitter utilizes some of the available power to produce artificial noise, such that only the eavesdropper's channel is degraded. At present, the common method used is artificial noise aided beamforming.

The initial research of artificial noise assisted beamforming method was proposed by Goel and Negi [32], which used multiantenna array to develop a "zero space." Then, it introduced noise signal into zero space of the legitimate channel, which made the legitimate receiver extract the information via noise filtering, but the illegal users are impacted by these introduced noise signals. In recent years, the researchers have carried out many subsequent studies and optimization based on this method [33, 34]. For example, ensuring the quality of service, [35] used the limited indicator signal to interference plus noise ratio (SINR) to assist artificial noise, and to achieve energy saving and secrecy capacity improvement, [36] extended the artificial noise from the null

space to signal space and achieved better performance. Deng et al. presented analog network coding systems based on artificial noise to enhance physical-layer security [37]. In this scheme, the relay node selected part of antennas from its total antennas as the received reference signal in broadcast phase and then derived the beamforming matrix and artificial noise vector from the equivalent channel fading matrix. The simulated results showed that the proposed scheme outperforms classical beamforming scheme. Cephehi and Kurt extended the existing artificial noise techniques to MIMO-OFDM (Orthogonal Frequency Division Multiplexing) and proposed a spatiotemporal selective artificial noise approach to cause extensive channel estimation error for eavesdroppers [38]. However, comprehensive technology is still high in practical applications, and there are still many issues to be solved.

3.2. Frequency Domain Technologies. Frequency domain technology especially spread spectrum is the most applied PHY defense technology. It usually reduces or avoids the interference of the carrier frequency band by using the wide range and variability of carrier frequency. The concept of spread spectrum was first introduced by Nicola Tesla, and then spread spectrum was real studied in the U.S. Military. Because of its good antijamming property, it has been applied in the military field and gradually applied to civil area until the beginning of the last century in the 1980s [39].

The principle of spread spectrum is to modulate the transmitted signal with a pseudorandom sequence, while the receiver then demodulates the signal using the same sequence to get the original signal. In this process, the signal noise ratio (SNR) is increased, and the influence of the interference is also reduced.

According to the method of extending narrowband signal, spread spectrum can be divided into the following categories: FHSS (Frequency Hopping Spread Spectrum), DSSS, THSS (Time Hopping Spread Spectrum), CSS (Chirp Spread Spectrum), and the combination of these techniques. We majorly study FHSS and DSSS, which have better anti-jamming performance than others.

The principle of DSSS modulation is that the sender modulates signal with a pseudo noise sequence on a broad band. The modulated signal spectrum is similar to the noise sequence, which decreases the interference effects

and enhances the concealment of the signal. The receiver demodulates the spread signal by the same sequence. Then, the spectrum density of the useful signal is increased and the spectrum density of the interference noise is very small. It finally gets the original signal by filtering most of the noise. In this process, the impact of narrowband interference will be very limited because of its wide bandwidth. There also are many hybrid DS/FH DSSS technologies, which can get better performance in the face of jamming, multiuser interference, and channel fading [40, 41].

The FHSS mentions that the sender uses a set of pseudorandom code sequences to realize the carrier frequency hopping fast in different frequency and the sequence of hopping frequency (i.e., code sequence) only known between the sender and receiver. The recipients can use the sequence to despread the received signal [42]. On the one hand, the security of FHSS depends on the complexity of frequency hop pattern. Leukhin et al. presented a new method for constructing CDMA sequence sets with the linear complexity of the Legendre sequences and formed new frequency hop patterns [43]. However, the freshness of the hopping sequences and terminals synchronization were difficult to obtain [44]. On the other hand, the FHSS can hop in a wide range so that it has stronger ability to resist interference of the narrowband signal. Otherwise, it increases the hop rate for the more intelligent tracking jamming to improve the anti-interference ability [45]. The higher the frequency jumps, the stronger the antijamming performance of tracking. The jump of the carrier frequency can affect the attacker's monitoring of the signal flow and can better resist the traffic analysis attack. However, with FHSS of different frequency fast hopping, the sender and receiver strictly need synchronization requirements. Based on the OFDM framework and the secure sub-carrier assignment algorithm, Hao et al. introduced collision-free frequency hopping (CFFH) to achieve high information capacity through collision-free multiple access [46]. The proposed CFFH could resolve the strict synchronization limitation and ensure that each user still transmitted through a pseudorandom frequency hopping scheme. CFFH could maintain the inherent antijamming and anti-interception security features of the conventional FH system.

In addition, except for the good performance of the fast frequency hopping (FFH), adaptive frequency hopping technology can effectively resist the intelligence and sweep frequency jamming via adaptive carrier frequency, power [47, 48]. In [49], the authors put forward a new algorithm with blacklisting which can generate frequency hopping sequences (FHSs) in the presence of interference without regeneration overhead and maintains optimal/near-optimal properties with different channel number from one original sequence. A random spread spectrum based wireless communication called Frequency Quorum Rendezvous (FQR) is described in [50]. FQR coordinates two random hopping sequences to prevent eavesdropping and active attacks and exploits a quorum system that is a tool for increasing the availability and efficiency of replicated services in distributed computing. Chen et al. introduced a differential jamming rejection (DJR) receiver in FFH M-ary Frequency Shift Keying (MFSK) systems with worst-case band multitone jamming (MTJ)

[51]. Based on detecting frequency spectrum difference in forward-backward time slot while the FFH/MFSK signal arrives at receiver, the proposed receiver implemented differential suppression of worst-case band multitone jamming without any side information. The FHSS has better antijamming performance and lower bit error rate (BER). Because hardware requirements of FHSS are lower than DSSS, FHSS can be applied to many low hardware networks, and the data transmission rate is as high as DSSS.

3.3. Time Domain Technologies. Time domain is the main technique of channel coding, which was firstly studied by Shannon [16]. Shannon in his channel model proved that encoded information can be in the presence of noise which can realize the secure transmission by the channel capacity of arbitrary rate below. In addition, channel coding can play an essential role in correcting the transmission of information using addition of some check code. The receiver can utilize these symbols to check whether transmission information has error or not and correct error timely to reduce the influence of jamming attacks. Nowadays, there are many channels coding schemes such as convolution codes [52], BCH (Bose, Ray-Chaudhuri) [53], Turbo [54], LDPC (Low-Density Parity Check) code [55, 56], and soft decode-compress-forward scheme [57].

In addition, Kwak et al. introduced a binary numeral system called Yarg code [58], which can be used as a QAM (Quadrature Amplitude Modulation) symbol mapping scheme to map a sequence of multiple binary bits to the symbols of QAM constellation. The characteristic of this Yarg code was different from the QAM symbol mapping scheme Gray code. That was due to the fact that the objective of Gray code [59] was to minimize the required SNR that achieves the target BER, but the objective of Yarg code was to minimize the security gap. Through researching the usage of nonsystematic codes based on scrambling matrices, Baldi et al. estimated the security gap over the AWGN (Additive White Gaussian Noise) wiretap channel as a measure of the effectiveness of several transmission schemes [60]. This scheme used puncturing techniques to reduce the security gap between the authorized and unauthorized channels. Hence, the proposed security gap could be further reduced by using nonsystematic codes and scramble information bits within the transmitted codeword.

Among them, LDPC is a hot research channel code after Turbo and has been widely used in military, civil, commercial, and other fields due to its good error correction. Besides single encoding, the joint coding is also used. For example, the downlink and uplink of the communication use different coding or joint source channel coding. The video transmission and some high-speed network have achieved good results. Taieb and Chouinard proposed a physical-layer coding scheme based on nonsystematic Rate Compatible Low-Density Parity Check (RC-LDPC) codes to secure communications over the Gaussian wiretap channel [61]. In the coding scheme, a finer granularity rate compatible code was used to increase the eavesdropper decoding failure rate; meanwhile, a rate estimator based on the wiretap channel capacity was used to reduce decoding delays. The proposed

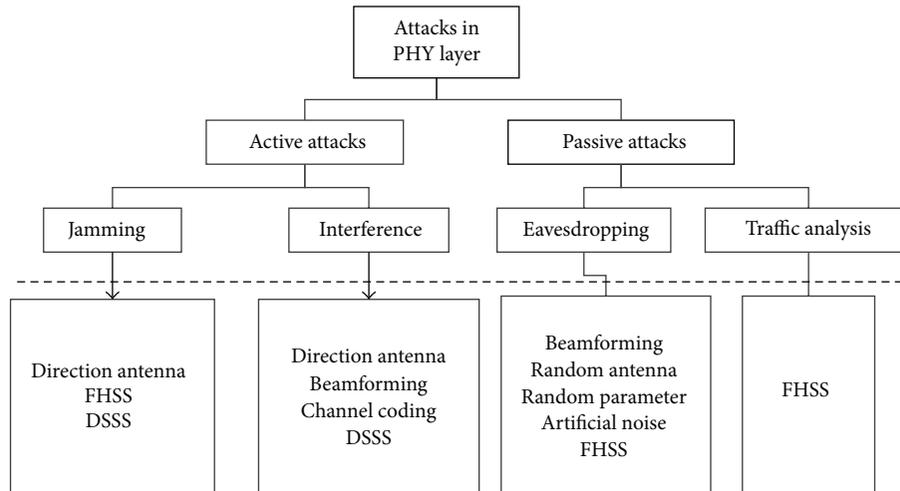


FIGURE 2: Attacks and defense in PHY layer.

coding scheme could improve security of PHY layer in terms of error amplification, and negative security gaps could also be achieved at the PHY layer. Yang et al. proposed a scheme where LDPC code and artificial noise were combined in wiretap channel to enhance the security in physical layer [62]. In the scheme, artificial noise was designed such that it spans a null space at the legitimate receiver but acts as random interference at the eavesdropper receiver and is added at the transmitter using precoding. A scrambling matrix was designed and used in LDPC code to reduce the outage probability of the wiretap channel deduced. Baldi et al. researched the reliability and secrecy performance achievable by practical LDPC codes and proposed a code optimization algorithm to design irregular LDPC codes, which was able to approach the ultimate performance limits [63]. Zhang et al. proposed a concatenated coding scheme based on polar codes and LDPC codes for the AWGN wiretap channel. They analyzed the BER performance of the proposed coding scheme through the density evolution (DE) and then investigated the security gap that the proposed coding scheme could achieve. Finally, a transmission scheme using rate compatible Polar-LDPC codes was presented to adapt to the dynamic environments [64]. However, the computational complexity of the channel code is a critical problem. In the practical application, the channel coding can also be considered as the flexible optimized coding rate and algorithm, which makes the channel coding powerful.

This section mainly concludes a number of common PHY security technology and development applications in the perspective of the security defense. The category of PHY attack is listed in Figure 2.

4. Analysis of Security Technology and Future Issues in PHY Layer

In this section, the security technology in PHY layer is analyzed and compared, and then some very innovative trends for future research are identified.

As mentioned above, the secure techniques of PHY layer could effectively defend against the interference, jamming, and eavesdropping attack. In this section, we analyze, compare, and summarize the previous secure techniques of PHY layer in wireless networks, through the research of the factors affecting the technical characteristics, ability to defend against attacks, and complexity which is illustrated in Table 1, with (—) signifying no consideration or weakness.

From Table 1 secure techniques are divided into three categories: spatial domain-based, time domain-based, and frequency domain-based. Strictly speaking, random parametric technique does not act as defense against eavesdropping attacks from space but relies on randomization of weighting coefficients to achieve the eavesdropper's received signal randomization. However, because there are the same beamforming technology-based and many similarities of representation formula, we compare the random parameter with random antenna in Section 3.

Research field of physical security, especially in mobile devices, becomes increasingly widespread in recent years. Much effort has been (and is being) made worldwide for providing secrecy in the absence of complete or perfect channel knowledge of the parties. As shown in Table 1, we could claim that secure techniques defending against eavesdropping attacks have mainly three types:

- (i) *Directional Transmission Technology (Beamforming and Directional Antenna)*. It can only enhance the resilience of the eavesdropping attack to some extent but is not able to effectively eliminate the threat from eavesdropping attacks. However, with the development of antenna technology, defensive performance could gradually be improved.
- (ii) *Random Parameters, Random Antennas, and FHSS*. Through randomization of weighting coefficients, channel parameters, and carrier frequency, an eavesdropper cannot effectively demodulate the correct information. These secure techniques have a high ability to resist eavesdropping.

TABLE 1: Comparison of PHY layer's security technique in wireless networks.

Secure technique	Type	Technical characteristics	Ability to defend against eavesdropping attacks	Ability to defend against jamming attacks	Ability to defend against interference attacks	Complexity
Directional antenna		Increased receive gain in particular direction of space	Low	Medium	Low	Low
Beamforming	Spatial domain	Superimposed multiantenna signal	Medium	—	Low	High
Random antennas		Increased channel randomness	Higher	—	—	High
Artificial noise		Increased channel diversity	High	—	—	High
Random parameters	—	Increased signal randomness	Higher	—	—	High
FHSS	Frequency domain	Fast hopping of carrier frequency	Higher	High	—	Medium
DSSS		Increased bandwidth	—	Higher	Medium	Medium
Channel coding	Time domain	Powerful error correction capability	—	—	High	Low

(iii) *Artificial Noise*. It relies on adding artificial noise to increase channel diversity in the channel, make eavesdropping channel quality far worse than legitimate channel quality, impact eavesdropper's information demodulation.

In general, the latter two technologies rely on the unknown of legitimate channel's CSI information for eavesdroppers. Thereby, the eavesdroppers could not correctly demodulate the signal information. Artificial noise and random parameters are developed based on the beamforming, which enables users to track multiple directions. Therefore, accurately tracking user location and selecting the best transmission channel are an important research direction of the beamforming technology. At the same time, large-scale application of smart antenna technology is required to have low cost and complexity and new development of beamforming technology is another research direction. The application implementation of random parameters and artificial noise is a difficult issue in the research. Random antenna technology achieves data confidentiality of the eavesdropper by array antenna redundancy. However, this technology caused low signal utilization and it cannot guarantee the security of the information if the number of antennas of the eavesdropper is larger than those of itself. How to improve the signal utilization and enhance the signal confidentiality is the promising issue, which can make it have a wide range of applications. Spread frequency and directional antenna are mainly technologies that defend against jamming attack. DSSS and FHSS have similar characteristics. Their frequency ranges are wide. To defend against jamming attack, the former depends on the extension of spectrum, while the latter relies on the carrier frequency hopping. The former has a higher transmission rate, and complexity of its hardware implementation is also

higher. The directional antenna with high antenna gain is suitable for long distance signal transmission, and it is the jamming avoidance in space. Therefore, the high-gain directional antenna is one of the important research directions for defending against jamming attack.

For jamming attack, directional antenna and beamforming mainly depend on the orientation of their transmission signals to reduce interference. Then, the DSSS signal is dispersed by the spread signal to achieve the low noise density spectrum, so that it has a strong attack on the interference resilience. Nevertheless, the channel coding and the former are not the same type of technology. It corrects the interference receiving code word based on powerful error correction capability. In a communications system, there are a wide variety of conflicting design tradeoffs. If channel coding technology is used to enhance the physical-layer security in the WSN and ad hoc networks, it will provide guidelines for engineers to balance between complexity and security. Nowadays, the research demonstrates that optimization of H matrix in LDPC can effectively reduce the computational complexity, which seems to be the relevant tradeoff. In general, the directional antenna and the beamforming strongly depend on the hardware; moreover, the channel coding relies on complex calculations to achieve the error correction. Since the channel coding's ability is better than the directional antenna and the beamforming ability in defending against the interference attack, it is widely used in a variety of information transmissions.

5. Conclusions

We notice that a few researchers focus on the information security of PHY layer in wireless networks. In this paper, we firstly research the attacks of PHY layer in wireless networks.

From three aspects of the spatial domain, frequency domain, and time domain, previous secure techniques are described. However, the secure techniques of spatial domain have to face the implementation complexity and energy consumption. Otherwise, the implementation of PHY layer's information security requires larger storage spaces and more powerful computing capabilities and even requires additional hardware units.

In the current field of wireless communication, major secure techniques could be applied to defend against interference and jamming attacks. Defense against eavesdropping attack mainly depends on data encryption technology of upper level. Mostly novel security techniques of PHY layer are still in theoretical research stage; how theoretical research results in practical applications is one of the hotspots for future research.

Competing Interests

The authors declare no conflict of interests.

Acknowledgments

This work is partially supported by the National Natural Science Foundation of China (61302113, 61501289), the Shanghai Natural Science Foundation (13ZR1440800), the Shanghai Rising-Star Program (14QB1404400), Shanghai Key Laboratory of Specialty Fiber Optics and Optical Access Networks (SKLSFO 2014-03), the Science and Technology Innovation Program of Shanghai (14511101303), Shanghai Sailing Program (15YF1414500, 14YF1408900), the International Science & Technology Cooperation Project of Qinghai (2014-HZ-821), and the Application Foundation Research Project of Qinghai (2015-ZJ-721).

References

- [1] T. Jiang, T. Li, and J. Ren, "Toward secure cognitive communications in wireless networks," *IEEE Wireless Communications*, vol. 19, no. 4, pp. 82–88, 2012.
- [2] F. Yu, C.-C. Chang, J. Shu, I. Ahmad, J. Zhang, and J. M. de Fuentes, "Recent advances in security and privacy for wireless sensor networks," *Journal of Sensors*, vol. 2015, Article ID 169305, 2 pages, 2015.
- [3] W. Zhang, Y. Zhang, and T.-H. Kim, "Detecting bad information in mobile wireless networks based on the wireless application protocol," *Computing*, vol. 96, no. 9, pp. 855–874, 2014.
- [4] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: a survey," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.
- [5] Z. Chen, M. He, W. Liang, and K. Chen, "Trust-aware and low energy consumption security topology protocol of wireless sensor network," *Journal of Sensors*, vol. 2015, Article ID 716468, 10 pages, 2015.
- [6] F. Ishmanov, A. S. Malik, S. W. Kim, and B. Begalov, "Trust management system in wireless sensor networks: design considerations and research challenges," *Transactions on Emerging Telecommunications Technologies*, vol. 26, no. 2, pp. 107–130, 2015.
- [7] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: the road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.
- [8] R. Bassily, E. Ekrem, X. He et al., "Cooperative security at the physical layer: a summary of recent advances," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 16–28, 2013.
- [9] H. M. Wang and X. G. Xia, "Enhancing wireless secrecy via cooperation: signal design and optimization," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 47–53, 2015.
- [10] A. Yener and S. Ulukus, "Wireless physical-layer security: lessons learned from information theory," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1814–1825, 2015.
- [11] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 4, pp. 42–56, 2009.
- [12] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66–74, 2011.
- [13] W. Xu, W. Trapper, Y. Zhang, and T. Wood, "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 (MobiHoc '05)*, pp. 46–57, Chicago, Ill, USA, May 2005.
- [14] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [15] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.
- [16] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.
- [17] Y. Zou, J. Zhu, and B. Zheng, "Defending against eavesdropping attack leveraging multiple antennas in wireless networks," in *Proceedings of the 8th International ICST Conference on Communications and Networking in China (CHINACOM '13)*, pp. 699–703, Guilin, China, August 2013.
- [18] J. E. Barcelo-Llado, A. Morell, and G. Seco-Granados, "Amplify-and-forward compressed sensing as a physical-layer secrecy solution in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 839–850, 2014.
- [19] P. H. Yang, *Tactical communication network node immunity of the antenna based on OPNET [M.S. thesis]*, Xidian University, Xi'an, China, 2011.
- [20] G. Noubir, "On connectivity in ad hoc networks under jamming using directional antennas and mobility," in *Wired/Wireless Internet Communications*, pp. 186–200, Springer, Berlin, Germany, 2014.
- [21] X. Lu, F. D. Wicker, D. Towsley, Z. Xiong, and P. Lio, "Detection probability estimation of directional antennas and omnidirectional antennas," *Wireless Personal Communications*, vol. 55, no. 1, pp. 51–63, 2010.
- [22] Y. Li, P. Michal, and L. Björn, "Fair flow rate optimization by effective placement of directional antennas in wireless mesh networks," *Performance Evaluation*, vol. 87, pp. 92–106, 2015.
- [23] O. Bazan and M. Jaseemuddin, "A survey on MAC protocols for wireless adhoc networks with beamforming antennas," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 2, pp. 216–239, 2012.

- [24] C. Walsh, D. Hakkarinen, and T. Camp, "Distributed decode and forward beamforming," in *Proceedings of the 37th Annual IEEE Conference on Local Computer Networks (LCN '12)*, pp. 436–444, IEEE, Clearwater, Fla, USA, October 2012.
- [25] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information- and jamming-beamforming for physical layer security with full duplex base station," *IEEE Transactions on Signal Processing*, vol. 62, no. 24, pp. 6391–6401, 2014.
- [26] X. Chen, C. Zhong, C. Yuen, and H. Chen, "Multi-antenna relay aided wireless physical layer security," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 40–46, 2015.
- [27] Z. Liu, C. Chen, L. Bai, H. Xiang, and J. Choi, "Transmit power minimization beamforming via amplify-and-forward relays in wireless networks with multiple eavesdroppers," in *Proceedings of the IEEE International Conference on Communications (ICC '14)*, pp. 4698–4703, Sydney, Australia, June 2014.
- [28] X. Li, J. Hwu, and E. P. Ratazzi, "Using antenna array redundancy and channel diversity for secure wireless transmissions," *Journal of Communications*, vol. 2, no. 3, pp. 24–32, 2007.
- [29] G. Y. Zhao, "Secure transmission in PHY layer of wireless communications based on random antenna array," *China CIO News*, vol. 5, p. 96, 2013.
- [30] Y. Hong, S. Im, and J. Ha, "Secure antenna subset modulation with coordinate interleaved orthogonal designs," in *Proceedings of the 5th International Conference on Information and Communication Technology Convergence (ICTC '14)*, pp. 97–98, Busan, South Korea, October 2014.
- [31] N. Valliappan, A. Lozano, and R. W. Heath Jr., "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Transactions on Communications*, vol. 61, no. 8, pp. 3231–3245, 2013.
- [32] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.
- [33] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, "PHY layer security based on protected zone and artificial noise," *IEEE Signal Processing Letters*, vol. 20, no. 5, pp. 487–490, 2013.
- [34] S. H. Chae, W. Choi, J. H. Lee, and T. Q. S. Quek, "Enhanced secrecy in stochastic wireless networks: artificial noise with secrecy protected zone," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 10, pp. 1617–1628, 2014.
- [35] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: an optimized artificial-noise-aided approach," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1202–1216, 2011.
- [36] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1728–1740, 2013.
- [37] D. Deng, Z.-L. Yang, and M. Zhao, "PHY security enhancement in analog network coding based on artificial noise," in *Proceedings of the 6th International Conference on Wireless Communications and Signal Processing (WCSP '14)*, pp. 1–6, Hefei, China, October 2014.
- [38] O. Cepheli and G. K. Kurt, "Efficient PHY layer security in MIMO-OFDM: spatiotemporal selective artificial noise," in *Proceedings of the IEEE 14th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM '13)*, pp. 1–6, Madrid, Spain, June 2013.
- [39] W. Xu, "Jamming attack defense," in *Encyclopedia of Cryptography and Security*, pp. 655–661, Springer, New York, NY, USA, 2011.
- [40] M. Olama, S. Smith, T. Kuruganti, and X. Ma, "Performance study of hybrid DS/FFH spread-spectrum systems in the presence of frequency-selective fading and multiple-access interference," in *Proceedings of the IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR '12)*, pp. 1–5, San Diego, Calif, USA, May 2012.
- [41] M. M. Olama, X. Ma, T. P. Kuruganti, S. F. Smith, and S. M. Djouadi, "Hybrid DS/FFH spread-spectrum: a robust, secure transmission technique for communication in harsh environments," in *Proceedings of the IEEE Military Communications Conference (MILCOM '11)*, pp. 2136–2141, IEEE, Baltimore, Md, USA, November 2011.
- [42] M. Darnell and H. M. Yung, "Security considerations in frequency hopping radio systems," in *Proceedings of the IEEE Colloquium on Security and Cryptography Applications to Radio Systems*, pp. 11/1–11/3, London, UK, 1994.
- [43] A. Leukhin, O. Moreno, and A. Tirkel, "Secure CDMA and frequency hop sequences," in *Proceedings of the 10th International Symposium on Wireless Communication Systems (ISWCS '13)*, pp. 1–5, VDE, Ilmenau, Germany, August 2013.
- [44] F. Meucci, S. A. Wardana, and N. R. Prasad, "Secure physical layer using dynamic permutations in cognitive OFDMA systems," in *Proceedings of the IEEE 69th Vehicular Technology Conference (VTC '09)*, pp. 1–5, Barcelona, Spain, April 2009.
- [45] P. P. Pan and D. M. Zhang, "Research on anti-hopping communication system," *Neijiang Technology*, vol. 6, pp. 103–115, 2014.
- [46] L. Hao, T. Li, and Q. Ling, "A highly efficient secure communication interface: collision-free frequency hopping (CFFH)," in *Proceedings of the IEEE Workshop on Signal Processing Applications for Public Security and Forensics (SAFE '07)*, vol. 4, pp. 1–4, Washington, DC, USA, April 2007.
- [47] M. Putzke and C. Wietfeld, "Self-organizing fractional frequency reuse for femtocells using adaptive frequency hopping," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '13)*, pp. 434–439, IEEE, Shanghai, China, April 2013.
- [48] M. K. Hanawal, M. J. Abdel-Rahman, and M. Krunz, "Game theoretic anti-jamming dynamic frequency hopping and rate adaptation in wireless systems," in *Proceedings of the 12th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt '14)*, pp. 247–254, Hammamet, Tunisia, May 2014.
- [49] C.-F. Shih, A. E. Khafa, and J. Zhou, "Practical frequency hopping sequence design for interference avoidance in 802.15.4e TSCH networks," in *Proceedings of the IEEE International Conference on Communications (ICC '15)*, pp. 6494–6499, IEEE, London, UK, June 2015.
- [50] E.-K. Lee, M. Gerla, and S. Y. Oh, "Physical layer security in wireless smart grid," *IEEE Communications Magazine*, vol. 50, no. 8, pp. 46–52, 2012.
- [51] Y. Chen, G. Li, S. Li, and Y. Cheng, "A new anti-jam receiver for MFSK/FFH system with multitone jamming," in *Proceedings of the 11th IEEE Singapore International Conference on Communication Systems (ICCS '08)*, pp. 451–455, Guangzhou, China, November 2008.
- [52] Q. Yang and S. C. Liew, "Asynchronous convolutional-coded physical-layer network coding," *IEEE Transactions on Wireless Communications*, vol. 14, no. 3, pp. 1380–1395, 2015.

- [53] F. Rosas, G. Brante, R. D. Souza, and C. Oberli, "Optimizing the code rate for achieving energy-efficient wireless communications," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '14)*, pp. 775–780, Istanbul, Turkey, April 2014.
- [54] M. F. Brejza, L. Li, R. G. Maunder, B. M. Al-Hashimi, C. Berrou, and L. Hanzo, "20 years of turbo coding and energy-aware design guidelines for energy-constrained wireless applications," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 8–28, 2016.
- [55] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2933–2945, 2007.
- [56] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for physical layer security," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '09)*, pp. 1–6, IEEE, Honolulu, Hawaii, USA, December 2009.
- [57] D. N. K. Jayakody and M. Flanagan, "A soft decode-compress-forward relaying scheme for cooperative wireless networks," *IEEE Transactions on Vehicular Technology*, 2015.
- [58] B.-J. Kwak, N.-O. Song, B. Park, D. Klinc, and S. W. McLaughlin, "Physical layer security with yarg code," in *Proceedings of the 1st International Conference on Emerging Network Intelligence*, pp. 43–48, Sliema, Malta, October 2009.
- [59] F. Gray, "Pulse code communication," U. S. Patent, 2,632,058, 1953.
- [60] M. Baldi, M. Bianchi, and F. Chiaraluce, "Non-systematic codes for physical layer security," in *Proceedings of the IEEE Information Theory Workshop (ITW '10)*, pp. 1–5, Dublin, Ireland, August-September 2010.
- [61] M. H. Taieb and J.-Y. Chouinard, "Enhancing secrecy of the Gaussian wiretap channel using rate compatible LDPC codes with error amplification," in *Proceedings of the 14th Canadian Workshop on Information Theory (CWIT '15)*, pp. 41–45, St. John's, Canada, July 2015.
- [62] Z. Yang, Y. Fan, and A. Wang, "Artificial noise and LDPC code aided physical layer security enhancement," in *Proceedings of the International Conference on Information and Communications Technologies (ICT '14)*, pp. 1–6, Nanjing, China, May 2014.
- [63] M. Baldi, G. Ricciutelli, N. Maturo, and F. Chiaraluce, "Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel," in *Proceedings of the IEEE International Conference on Communications Workshops (ICC '15)*, pp. 435–440, IEEE, London, UK, June 2015.
- [64] Y. Zhang, A. Liu, C. Gong, G. Yang, and S. Yang, "Polar-LDPC concatenated coding for the AWGN wiretap channel," *IEEE Communications Letters*, vol. 18, no. 10, pp. 1683–1686, 2014.

Research Article

Prediction Approach of Critical Node Based on Multiple Attribute Decision Making for Opportunistic Sensor Networks

Qifan Chen,^{1,2} Linlan Liu,^{1,3} Zhiyong Yang,^{1,2} and Kai Guo^{1,3}

¹*Internet of Things Technology Institute, Nanchang Hangkong University, Nanchang 330063, China*

²*School of Software, Nanchang Hangkong University, Nanchang 330063, China*

³*School of Information Engineering, Nanchang Hangkong University, Nanchang 330063, China*

Correspondence should be addressed to Linlan Liu; liulinlan@nchu.edu.cn

Received 14 January 2016; Accepted 29 March 2016

Academic Editor: Fei Yu

Copyright © 2016 Qifan Chen et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Predicting critical nodes of Opportunistic Sensor Network (OSN) can help us not only to improve network performance but also to decrease the cost in network maintenance. However, existing ways of predicting critical nodes in static network are not suitable for OSN. In this paper, the conceptions of critical nodes, region contribution, and cut-vertex in multiregion OSN are defined. We propose an approach to predict critical node for OSN, which is based on multiple attribute decision making (MADM). It takes RC to present the dependence of regions on Ferry nodes. TOPSIS algorithm is employed to find out Ferry node with maximum comprehensive contribution, which is a critical node. The experimental results show that, in different scenarios, this approach can predict the critical nodes of OSN better.

1. Introduction

In Opportunistic Sensor Network (OSN), the critical nodes are very important to keep normal operation of networks. In practical applications, if the critical nodes can be predicted, the network could be optimized according to the attributes of critical nodes, which helps improving the robustness of the network. In network maintenance, maintainers can focus on monitoring the status of critical nodes so that the failures of the network could be resolved immediately, which can dramatically reduce the time and the cost of network maintenance. Therefore, predicting critical nodes of OSN has great significance.

2. Related Work

OSN is a kind of Wireless Sensor Networks. It perceives the surrounding environment by sensor nodes and transports messages by the meeting opportunities of Ferry nodes. Hence, it has the characteristics of Mobile Opportunity Network [1] and Wireless Sensor Network [2]. The current study of OSN critical nodes is very little. Nevertheless, in

some related fields, researchers have made some progress such as node importance evaluation [3–7] and network cut-vertex judgement [8–14].

Corley and Sha [15] proposed that the critical nodes in a weighted network are those whose removal from the network results in the greatest increase in shortest distance between two specified nodes. This method could be applied to estimate the end-to-end nodes. However, it is powerless to estimate the critical nodes in the whole network. Chen et al. [16] studied a method to estimate the relative importance of nodes by comparing the number of spanning trees. Although this method could estimate the critical nodes of the whole network, it has the problem of high computing complexity. So it is not suitable in practical applications. In resistance network, Xiao et al. [17] did the research on the energy consumption model to evaluate the importance degree of nodes. This method estimates the critical node by comparing the increase of the average energy consumption of the network after the nodes are removed. Goyal and Caffery [18] discussed the split of ad hoc networks. They utilized network survivability concepts to detect the critical links in an ad hoc wireless network. This method is based on the precondition

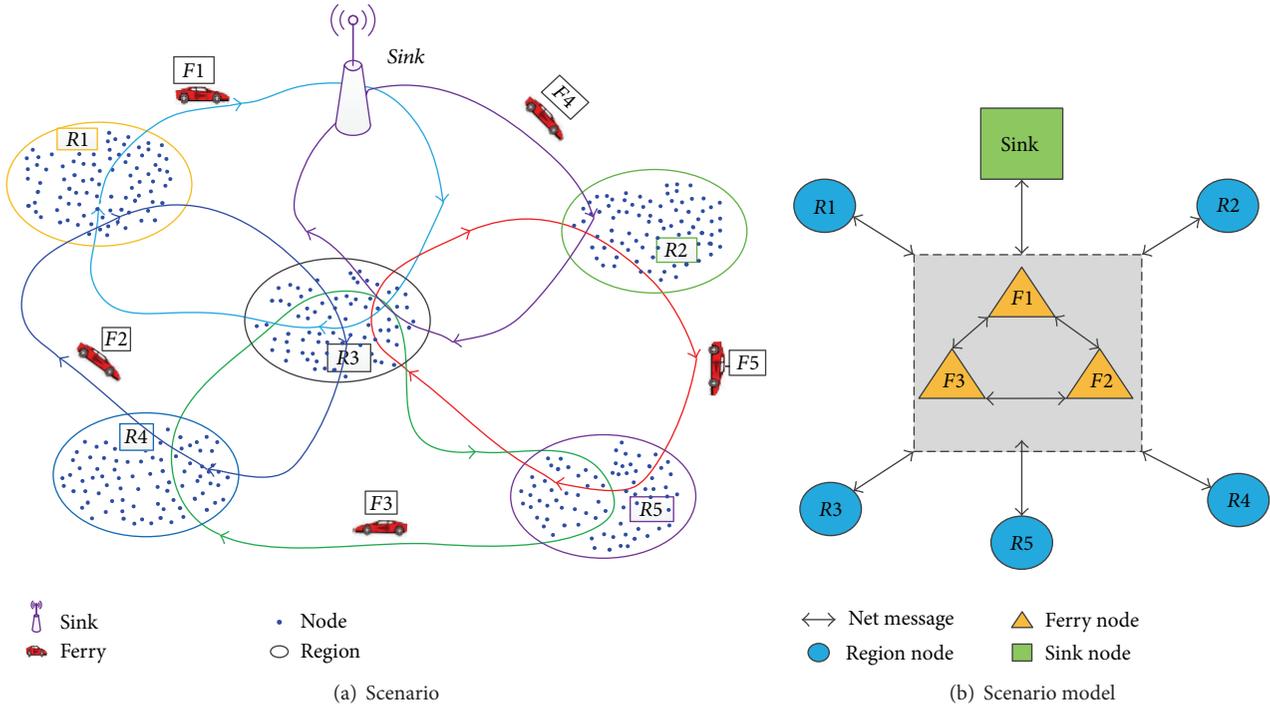


FIGURE 1: OSN scenario.

that the nodes can locate themselves, which has great application limitations.

With the research above, it is always one-sided to evaluate the network through a single evaluation index. Considering the influence of node degree, node closeness, node betweenness, equivalent topology, and neighbor lists, Hu et al. [19] conducted experiments with three real typical networks to show that their method is more accurate than using a single evaluation index. Liu et al. [20] proposed a method to estimate critical nodes by combining the residual lifetime of nodes and the network energy consumption. Due to the shortcomings of the methods of node deletion and node contraction, Zhou et al. [21] exploited the evaluation matrix of node efficiency and node importance to determine the critical nodes in complex network. This method reflects the significance of divergences between two nodes and can evaluate the importance exactly. In a similar way, Fan and Liu [22] discussed the local and global importance of nodes and presented an evaluation method based on transfer efficiency matrix which takes not only the interactions between adjacent nodes but also the nonadjacent nodes' contributions into account, thus obtaining a more accurate node importance evaluation result.

As a dynamic network, current static prediction methods of critical nodes are not appropriate for OSN. Depending upon the researches above, in this paper, the stage contribution and the region contribution are proposed to evaluate the node importance. Then an algorithm is designed which is based on the multiple attribute decision making (MADM) to predict the critical nodes of OSN.

3. Scenario Model and Definitions

3.1. Scenario Model. The monitoring areas of application scenarios like environmental monitoring are very large. Therefore, the maintainers tend to monitor the key regions instead of the whole network. In OSN, the messages of the network are collected through the communication opportunities supported by mobile nodes. As shown in Figure 1(a), our research is proposed for the OSN with multiple regions and the nodes in the regions are fixed. There are Ferry nodes between regions supporting communication opportunities to Sink nodes and the trajectory of Ferry nodes could be a specific way or a random way.

In Figure 1(b), $R1\sim R5$ are region nodes; $F1\sim F3$ are Ferry nodes. The region nodes and Sink nodes are fixed and isolated. Those two kinds of nodes cannot communicate with each other without Ferry nodes. The Ferry nodes can move among regions, carrying and transporting messages between Sink nodes and other regions.

In this paper, the following assumptions are made:

- (1) In our research, each region is abstracted as a "super node" called region node.
- (2) Regardless of the Ferry nodes' memory, it is assumed that Ferry node can collect all the messages from each node it meets.
- (3) Regions and Ferry nodes and Sink nodes in the network have unique identity information.
- (4) The network has a time synchronization mechanism.

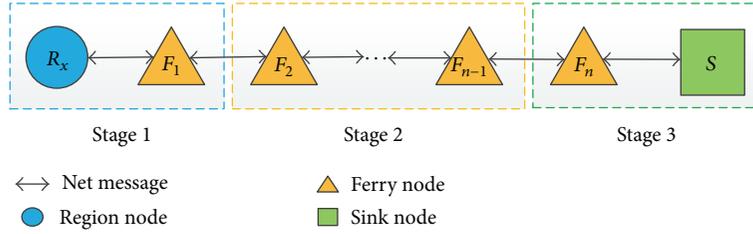


FIGURE 2: OSN message transmission.

In Figure 1, Ferry nodes in the whole network play a role of transport medium so that the Ferry nodes are the key to ensure the connectivity of the whole network. Besides, as a kind of “super node,” the region nodes consist of a group of sensor nodes. Individual sensor node’s failure in regions will have little impact on the whole network. Therefore, we can learn from the research above that the critical node of OSN could be a Ferry node.

3.2. Definition of Critical Nodes. Define Opportunistic Sensor Networks as G . Define F as a critical node of G when the possibility of network split caused by the removal of node F is the largest. According to the definition above, when the cut-vertices of OSN are removed, the network will be divided. Therefore, we can learn that the cut-vertices of OSN must be critical nodes.

OSN is a dynamic network which transfers data by the “Store-Carry-Forward” mechanism. The traditional parameters such as node degree [23, 24], node betweenness [25–29], node closeness [30], aggregation [31, 32], and other network parameters are not suitable for OSN. Therefore, it is necessary to set up an appropriate evaluation index for OSN.

In OSN, Ferry nodes are transport mediums. So their job is to transport messages between Sink nodes and region nodes. In order to accurately estimate each Ferry node’s importance to the network, the effect of Ferry nodes on OSN must be considered properly. With intensive analysis of OSN’s routing mechanism, the region messages’ life cycle can be divided into three stages as shown in Figure 2.

In the first stage, Ferry nodes receive network messages from regions and then carry them out. In the second stage, the network messages will be forwarded among Ferry nodes. At last, Ferry nodes transport messages to the Sink nodes. These three stages can not only depict the message propagation of OSN clearly but also show the important role of Ferry nodes obviously.

3.3. Definition of First Stage Contribution. Define a time slice as T and the Sink node receives M_j pieces of messages from region R_j in T . If the Ferry node F_i has forwarded messages in the first stage, the total number of the forwarding messages is n_{ij} ($n_{ij} \leq M_j$). Define the First Stage Contribution (FSC) of node F_i to region R_j as n_{ij}/M_j , denoted by $FSC(F_i, R_j)$.

3.4. Definition of Second Stage Contribution. Define a time slice as T and the Sink node receives M_j pieces of messages

from region R_j in T . If the Ferry node F_i has forwarded messages in the second stage, the total number of the forwarding messages is m_{ij} ($m_{ij} \leq M_j$). Define the Second Stage Contribution (SSC) of node F_i to region R_j as m_{ij}/M_j , denoted by $SSC(F_i, R_j)$.

3.5. Definition of Third Stage Contribution. Define a time slice as T and the Sink node receives M_j pieces of messages from region R_j in T . If the Ferry node F_i has forwarded messages in the third stage, the total number of the forwarding messages is k_{ij} ($k_{ij} \leq M_j$). Define the Third Stage Contribution (TSC) of node F_i to region R_j as k_{ij}/M_j , denoted by $TSC(F_i, R_j)$.

3.6. Definition of Region Contribution. Define a time slice as T . The stage contributions of Ferry node F_i to region R_j are $FSC(F_i, R_j)$, $SSC(F_i, R_j)$, and $TSC(F_i, R_j)$. Define region contribution (RC) of node F_i to region R_j as $RC(F_i, R_j) = FSC(F_i, R_j) + SSC(F_i, R_j) + TSC(F_i, R_j)$, denoted by $RC(F_i, R_j)$.

The region contribution can reflect both the Ferry nodes’ contributions to regions and the dependence of the regions on Ferry nodes. It means that the bigger region contribution the node has, the higher possibility leading to the network split the node possesses and the node is more likely to be a critical node. If the region contribution from node F_x to region R_y equals 1, it means that region R_y is fully dependent on node F_x ; that is to say, if node F_x is removed, region R_y will be isolated from the whole network.

According to the researches above, we can infer that the node is a cut-vertex of the network when the region contribution equals 1 and it must be a critical node.

4. MADM Based Prediction Method of Critical Node of OSN

According to the research mentioned above, the critical node prediction method for OSN can be described as the following steps.

Step 1. Calculate each Ferry node’s region contributions in order to determine whether the network has cut-vertexes or not. If there are no cut-vertexes in the network, go to Step 2.

Step 2. Find out a node which most likely leads to the network split and it must be a critical node. The region contribution shows the dependence of regions on Ferry nodes. We can learn that the higher region contribution the node has, the higher risk of network split it will have. Based on the theory

above, we first take each Ferry node as a single evaluation scheme. Then, the TOPSIS method is applied to evaluate the comprehensive region contribution of Ferry nodes.

4.1. Algorithm Description. It is meaningless to predict such a dynamic network like OSN by calculating region contributions within a single time slice such as ΔT . However, a single prediction result can be defined as a suspected critical node. After setting $N \cdot \Delta T$ as the total time length of prediction, N suspected critical nodes will be found. Then, the frequency of each node to be estimated as a suspected critical node can be recorded.

We assume an OSN with d Ferry nodes. Each node may lead to network split. If node F_i has been estimated as a suspected critical node q times, the appearance probability of node F_i could be figured out as $P_s(F_i)$:

$$P_s(F_i) = \frac{q}{N(c_d^1 + c_d^1 c_{d-1}^1 + c_d^1 c_{d-1}^2 + \dots + c_d^1 c_{d-1}^{d-1})}. \quad (1)$$

Denote the maximum of $P_s(F_i)$ as $\max(P_s)$ and the corresponding node as F_k , $k \in \{1, 2, 3, \dots, d\}$. We define this node as a predicted critical node.

ΔT is a single time slice of the network. The details of ΔT are defined as follows: it is assumed that there are n Ferry nodes to be determined in the network so that the corresponding solution sets can be denoted by $F = (F_1, F_2, \dots, F_n)$ and there are m regions in the network so the region contribution of each Ferry node can be denoted by an attribute set $S = (S_1, S_2, \dots, S_m)$. j th attribute of i th node is defined as $F_i(S_j)$ ($i = 1, 2, \dots, n$; $j = 1, 2, \dots, m$). The decision matrix is as follows:

$$E = \begin{pmatrix} F_1(S_1) & \dots & F_1(S_m) \\ \vdots & \ddots & \vdots \\ F_n(S_1) & \dots & F_n(S_m) \end{pmatrix}. \quad (2)$$

For comparison, the decision matrix could be optimized by the following normalization processing:

$$r_{ij} = \frac{F_i(S_j)}{\sqrt{\sum_{i=1}^n F_i(S_j)^2}}. \quad (3)$$

Then the decision matrix could be updated to $R = (r_{ij})_{n \times m}$.

Due to the different importance of different regions to the whole network, weight is assigned for each evaluation index to make the algorithm more universal. We denote the j th index weight as ω_j ($j = 1, 2, \dots, m$), and $\sum_{j=1}^m \omega_j = 1$. Then we denote the weighted normalized matrix as

$$C = (c_{ij}) = (\omega_j r_{ij}) = \begin{pmatrix} \omega_1 r_{11} & \dots & \omega_m r_{1m} \\ \vdots & \ddots & \vdots \\ \omega_1 r_{n1} & \dots & \omega_m r_{nm} \end{pmatrix}. \quad (4)$$

According to matrix C , the positive ideal solution F^+ and the negative ideal solution F^- are denoted as follows:

$$F^+ = \{c_1^+, c_2^+, \dots, c_m^+\}, \quad (5a)$$

$$F^- = \{c_1^-, c_2^-, \dots, c_m^-\}, \quad (5b)$$

where $c_j^+ = \max_{i \in k}(c_{ij})$, $c_j^- = \min_{i \in k}(c_{ij})$, and $k = (1, 2, \dots, m)$.

We denote the distance from every solution F_i to the positive ideal solution F^+ and the negative ideal solution F^- , respectively, denoted by

$$D_i^+ = \|F_i - F^+\| = \sqrt{\sum_{j=1}^m (c_{ij} - c_j^+)^2}, \quad (6a)$$

$$D_i^- = \|F_i - F^-\| = \sqrt{\sum_{j=1}^m (c_{ij} - c_j^-)^2}. \quad (6b)$$

Then we calculate and sort the ideal solutions similarity degree Z_i , denoted by

$$Z_i = \frac{D_i^-}{(D_i^- + D_i^+)}. \quad (7)$$

According to the TOPSIS method, the node with maximum Z_i is the suspected critical node.

4.2. Algorithm Process. It is assumed that OSN has n Ferry nodes and m regions. TOPSIS based synthetic evaluation of region contributions algorithm can be described as follows:

- (1) At first, denote the length of time as ΔT . With the sampling analysis on the data of Sink node, the normalization matrix $R = (r_{ij})$ can be figured out by (2).
- (2) Construct weighted normalized matrix C by (2), (3), and (4).
- (3) Determine the positive ideal solution F^+ and the negative ideal solution F^- by (5a) and (5b).
- (4) Calculate the distance from every solution F_i to the positive ideal solution F^+ and the negative ideal solution F^- by (6a) and (6b).
- (5) Calculate the similarity degree between each solution and ideal solution by (7). The node with maximum Z_i is the suspected critical node.
- (6) Repeat the above steps and denote the length of prediction time as $N \cdot \Delta T$. According to (1), the emergence probability of each node can be recorded so that the node with maximum (P_s) is the critical node of the network.

5. Experiments and Analysis

5.1. Experimental Scenarios and Related Parameters. As is shown in Figures 3–6, four typical scenarios are simulated on the Opportunistic Networking Environment (ONE).

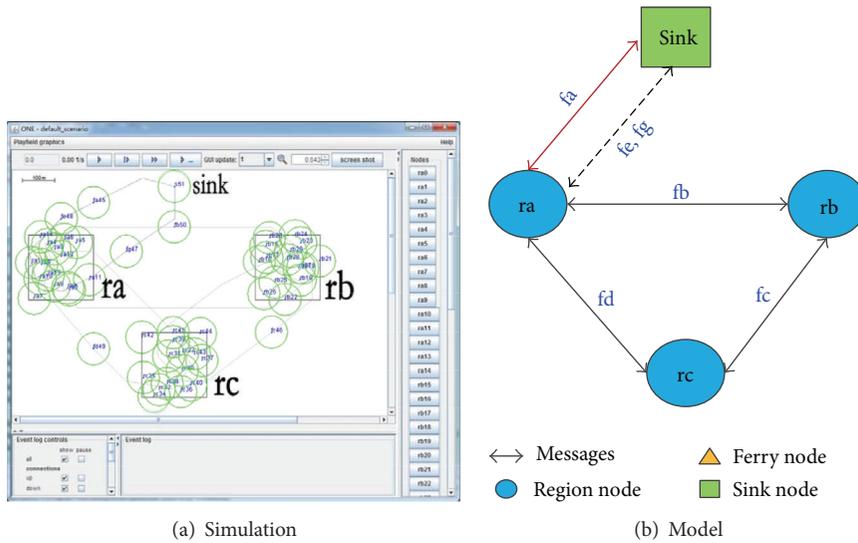


FIGURE 3: Scenario A.

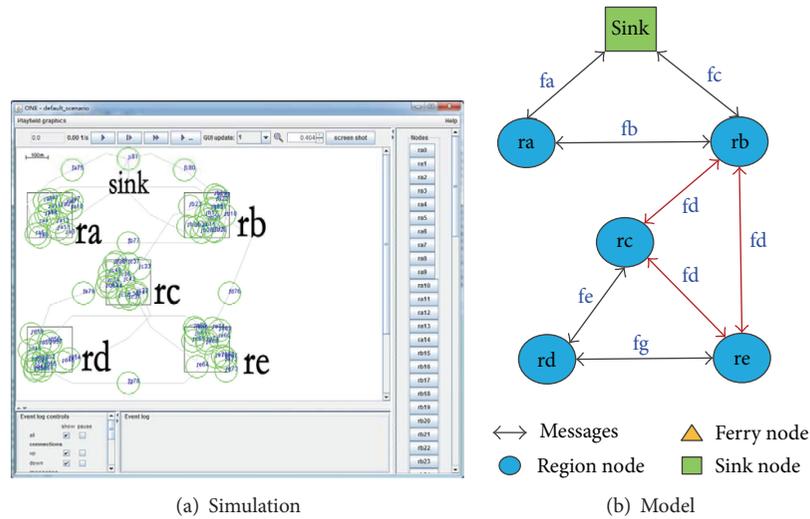


FIGURE 4: Scenario B.

In Figure 3, there is no cut-vertex in Scenario A and there are three region nodes including ra, rb, and rc and four Ferry nodes including fa, fb, fc, and fd. Among the Ferry nodes, fb, fc, and fd only provide the communication opportunities among the regions of ra, rb, and rc. However, Ferry nodes fa, fe, and fg provide the communication opportunities between region ra and Sink node which lead to the connection of the whole network. In addition, the black thick lines show that most of the communication opportunities of region ra are provided by Ferry node fa and the dotted lines show that the communication opportunities supported by fe and fg between ra and Sink node are very few, which indicates that node fa is the critical node of the network in Scenario A.

In Figure 4, Scenario B shows that node fd is the critical node. If node fd is failure or removed, regions rc, rd, and re cannot communicate to Sink node anymore. The network

split occurs so that node fd is the cut-vertex as well as the critical node of the network.

In some more complex situations like Scenario C and Scenario D, in Figure 5, there is no cut-vertex in Scenario C and most of the communication opportunities among regions ra and rb and Sink node are provided by node fa; thus it can be seen that fa is the critical node of the network in Scenario C.

In Figure 6, there are several cut-vertexes in Scenario D such as nodes fc, fd, and fe and they are the critical nodes as well.

5.2. Results Analysis. We have made experiments 100 times for each scenario. Table 1 shows the experimental results after the statistical analysis of experimental data.

As shown in Table 1, the maximum appearance possibility $\max(P_s)$ is 0.33% in Scenario A and 0.44% in Scenario C. Meanwhile, the corresponding prediction results are both fa.

TABLE I: Experiment results.

Scenario	CN	Appearance possibility P_s (%)						$\max(P_s)$ (%)	Result
		fa	fb	fc	fd	fe	fg		
Scenario A	fa	0.33	0.04	0	0.06	0.03	0.06	0.33	fa
Scenario B	fd	0.31	0	0.35	0.52	0.02	0	0.52	fd
Scenario C	fa	0.44	0.02	0.24	0.01	0	0	0.44	fa
Scenario D	fc, fd, fe	0.22	0.17	0.52	0.52	0.52	—	0.52	fc, fd, fe

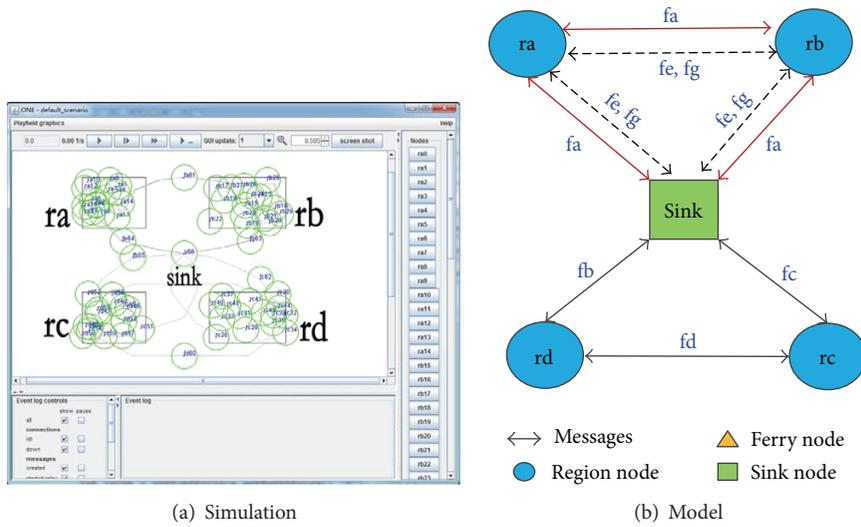


FIGURE 5: Scenario C.

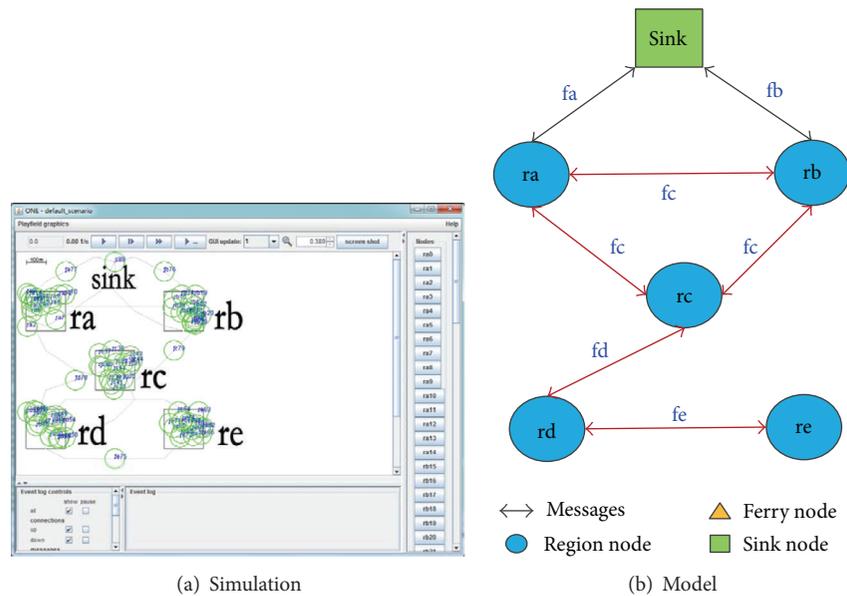


FIGURE 6: Scenario D.

In Scenario B and Scenario D, the max appearance possibility $\max(P_s)$ is for both 0.52%. The prediction result in Scenario B is fd and the results in Scenario D are fc, fd, and fe. Thus it can be seen that the predicted results of these four scenarios are completely the same with the actual value mentioned above. Therefore, our algorithm can well predict the critical nodes of OSN.

6. Conclusions

Considering the dynamic of OSN, this paper proposed a MADM based method to predict critical nodes. First, the region contribution is introduced to present the dependency of regions on Ferry nodes. Then, the comprehensive region contributions are estimated by the MADM method. At last, the experimental results show that, for different OSN scenarios, our method can predict the critical nodes of the network effectively.

Competing Interests

The authors declare no competing interests.

Acknowledgments

This work is supported in part by grants from the National Natural Science Foundation of China (nos. 61262020, 61363015, 61501218, and 61501217).

References

- [1] H.-D. Ma, P.-Y. Yuan, and D. Zhao, "Research progress on routing problem in mobile opportunistic networks," *Journal of Software*, vol. 26, no. 3, pp. 600–616, 2015.
- [2] Z. Ma, Y. Sun, and T. Mei, "Survey on wireless sensors network," *Journal on Communications*, vol. 25, no. 4, pp. 114–124, 2004.
- [3] J. C. Nacher and T. Akutsu, "Analysis on critical nodes in controlling complex networks using dominating sets," in *Proceedings of the 9th International Conference on Signal-Image Technology and Internet-Based Systems (SITIS '13)*, pp. 649–654, IEEE, Kyoto, Japan, December 2013.
- [4] G. Du, L. He, and J. Fang, "The component importance evaluation of power converter based on complex network," in *Proceedings of the International Power Electronics and Application Conference and Exposition*, pp. 988–992, IEEE, Shanghai, China, November 2014.
- [5] J. Lin, F. Dai, B. Li et al., "Electromagnetic compatibility supernetwork modeling and node importance evaluation," in *Proceedings of the 5th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC '13)*, pp. 306–310, Hangzhou, China, August 2013.
- [6] L. Le and Y. Hewei, "A new method for evaluating node importance in complex networks based on data field theory," in *Proceedings of the 1st International Conference on Networking and Distributed Computing (ICNDC '10)*, pp. 133–136, IEEE, Hangzhou, China, October 2010.
- [7] F. Hu, Y. Liu, and J. Jin, "Multi-index evaluation algorithm based on locally linear embedding for the node importance in complex networks," in *Proceedings of the IEEE 13th International Symposium on Distributed Computing and Applications to Business, Engineering and Science (DCABES '14)*, pp. 138–142, Xianning, China, November 2014.
- [8] J. Li, Y. Tian, M. Sheng et al., "Split detection for large scale," *Ad Hoc Networks*, vol. 29, no. 9, pp. 54–61, 2008.
- [9] C. Huang, W. Furong, H. Benxiong et al., "Preventing natural and malicious network split in ad hoc networks using cooperative healing cell," in *Proceedings of the IEEE International Conference on Communications Workshops (ICC Workshops '08)*, pp. 158–163, Beijing, China, 2008.
- [10] S. Xiong and J. Li, "An efficient algorithm for cut vertex detection in wireless sensor networks," in *Proceedings of the IEEE 30th International Conference on Distributed Computing Systems*, pp. 368–377, Genoa, Italy, June 2010.
- [11] R. Lin, B. Wu, Y. Zhao, H. Zou, and L. Liu, "Critical nodes detecting in virtual networking environment," in *Proceedings of the IEEE World Congress on Services (SERVICES '14)*, pp. 317–322, IEEE, Anchorage, Alaska, USA, June–July 2014.
- [12] D. Zhang and J. P. G. Sterbenz, "Analysis of critical node attacks in mobile ad hoc networks," in *Proceedings of the 6th International Workshop on Reliable Networks Design and Modeling (RNDM '14)*, pp. 171–178, IEEE, Barcelona, Spain, November 2014.
- [13] Y. Shen, N. T. Dinh, and M. T. Thai, "Adaptive algorithms for detecting critical links and nodes in dynamic networks," in *Proceedings of the Military Communications Conference (MILCOM '12)*, pp. 1–6, IEEE, Orlando, Fla, USA, November 2012.
- [14] G. Ausiello, D. Firmani, and L. Laura, "The (betweenness) centrality of critical nodes and network cores," in *Proceedings of the 9th International Wireless Communications and Mobile Computing Conference (IWCMC '13)*, pp. 90–95, IEEE, July 2013.
- [15] H. W. Corley and D. Y. Sha, "Most vital links and nodes in weighted networks," *Operations Research Letters*, vol. 1, no. 4, pp. 157–160, 1982.
- [16] Y. Chen, A. Hu, and X. Hu, "Evaluation method for node importance in communication networks," *Journal on Communications*, vol. 25, no. 8, pp. 129–134, 2004.
- [17] W. Xiao, W. Tan, B. Ge, and F. Li, "Fast method for node importance evaluation in network," *Systems Engineering—Theory & Practice*, vol. 33, no. 7, pp. 1898–1904, 2013.
- [18] D. Goyal and J. Caffery, "Partitioning avoidance in mobile ad hoc networks using network survivability concepts," in *Proceedings of the 7th International Symposium on Computers and Communications (ISCC '02)*, pp. 553–558, July 2002.
- [19] J. Hu, B. Wang, and D. Lee, "Evaluating node importance with multi-criteria," in *Proceedings of the IEEE/ACM International Conference on Green Computing and Communications (GreenCom '10), 2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing (CPSCom '10)*, pp. 792–797, IEEE Computer Society, Hangzhou, China, December 2010.
- [20] B. Liu, W. Wang, Y. Li et al., "Crucial node decision algorithm based on energy in WSN," *Journal of Electronics and Information Technology*, vol. 36, no. 7, pp. 1728–1734, 2014.
- [21] X. Zhou, F.-M. Zhang, K.-W. Li, X.-B. Hui, and H.-S. Wu, "Finding vital node by node importance evaluation matrix in complex networks," *Acta Physica Sinica*, vol. 61, no. 5, Article ID 050201, 2012.
- [22] W. Fan and Z. Liu, "Ranking method for node importance based on efficiency matrix," *Journal of Southwest Jiaotong University*, vol. 49, no. 2, pp. 337–342, 2014.
- [23] M. E. Newman, *Networks: An Introduction*, Oxford University Press, Oxford, UK, 2010.

- [24] J.-W. Wang, L.-L. Rong, and T.-Z. Guo, "A new measure method of network node importance based on local characteristics," *Journal of Dalian University of Technology*, vol. 50, no. 5, pp. 822–826, 2010.
- [25] K.-I. Goh, E. Oh, B. Kahng, and D. Kim, "Betweenness centrality correlation in social networks," *Physical Review E-Statistical, Nonlinear, and Soft Matter Physics*, vol. 67, no. 1, Article ID 017101, 2003.
- [26] A. Budanitsky and G. Hirst, "Evaluating WordNet-based measures of lexical semantic relatedness," *Computational Linguistics*, vol. 32, no. 1, pp. 13–47, 2006.
- [27] R. Burke, "Semantic ratings and heuristic similarity for collaborative filtering," in *Proceedings of the AAAI Workshop on Knowledge-Based Electronic Markets*, Austin, Tex, USA, July 2000.
- [28] G. Ausiello, D. Firmani, and L. Laura, "The (betweenness) centrality of critical nodes and network cores," in *Proceedings of the IEEE 9th International Sardinia Wireless Communications and Mobile Computing Conference (IWCMC '13)*, pp. 90–95, Sardinia, Italy, July 2013.
- [29] J. K. Lou, S. D. Lin, K. T. Chen, and C. L. Lei, "What can the temporal social behavior tell us? An estimation of vertex-betweenness using dynamic social information," in *Proceedings of the International Conference on Advances in Social Networks Analysis and Mining (ASONAM '10)*, pp. 56–63, IEEE, Odense, Denmark, August 2010.
- [30] D. Chen, L. Lü, M.-S. Shang, Y.-C. Zhang, and T. Zhou, "Identifying influential nodes in complex networks," *Physica A: Statistical Mechanics and Its Applications*, vol. 391, no. 4, pp. 1777–1787, 2012.
- [31] Z. Ren, F. Shao, J. Liu et al., "Node importance measurement based on the degree and clustering coefficient information," *Acta Physica Sinica*, vol. 62, no. 12, pp. 522–526, 2013.
- [32] D. T. Nguyen, Y. Shen, and M. T. Thai, "Detecting critical nodes in interdependent power networks for vulnerability assessment," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 151–159, 2013.

Research Article

Multitask Learning-Based Security Event Forecast Methods for Wireless Sensor Networks

Hui He,¹ Dongyan Zhang,² Xing Wang,¹ Min Liu,³ Weizhe Zhang,¹ and Junxi Guo⁴

¹School of Computer Science and Technology, Harbin Institute of Technology, Harbin, Heilongjiang 150001, China

²Department of Software Engineering, University of Science and Technology Beijing, Beijing 100083, China

³Network Information Center, Harbin Institute of Technology, Harbin, Heilongjiang 150001, China

⁴School of Software, Harbin Institute of Technology, Harbin, Heilongjiang 150001, China

Correspondence should be addressed to Dongyan Zhang; zhangdy@ustb.edu.cn

Received 17 December 2015; Accepted 17 February 2016

Academic Editor: Fei Yu

Copyright © 2016 Hui He et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Wireless sensor networks have strong dynamics and uncertainty, including network topological changes, node disappearance or addition, and facing various threats. First, to strengthen the detection adaptability of wireless sensor networks to various security attacks, a region similarity multitask-based security event forecast method for wireless sensor networks is proposed. This method performs topology partitioning on a large-scale sensor network and calculates the similarity degree among regional subnetworks. The trend of unknown network security events can be predicted through multitask learning of the occurrence and transmission characteristics of known network security events. Second, in case of lacking regional data, the quantitative trend of unknown regional network security events can be calculated. This study introduces a sensor network security event forecast method named Prediction Network Security Incomplete Unmarked Data (PNSIUD) method to forecast missing attack data in the target region according to the known partial data in similar regions. Experimental results indicate that for an unknown security event forecast the forecast accuracy and effects of the similarity forecast algorithm are better than those of single-task learning method. At the same time, the forecast accuracy of the PNSIUD method is better than that of the traditional support vector machine method.

1. Introduction

Sensor network is a network system that integrates monitoring, control, and wireless communication and has a high node number (thousands or even tens of thousands) and dense node distribution. Owing to environmental influences and energy depletion, nodes easily break down. Environment interference and node fault change the network topological structure. Wireless sensor networks have strong dynamics and uncertainty, including changes in network topology, node disappearance or addition, and various threats. Therefore, wireless sensor networks should have strong adaptability to various security attacks so that even if one attack behavior succeeds, the influence of such an attack will only be the minimum. However, attackers can cause sensor networks to be in a partial or total paralysis state through fake and signal interference and thus destroy the system availability, such as through the denial of service attack.

A large-scale sensor network has several advantages. The information from different space perspectives has a high information-price ratio. The distributed processing of a large amount of acquired information can improve the monitoring accuracy and decrease the accuracy requirement of a single-node sensor. Numerous redundant nodes provide the system with strong fault-tolerance performance. Numerous nodes can also increase the covered monitoring area and decrease the cave and dead zones.

Studies on the security situation of wireless sensor networks are presently lacking, but some research results have been obtained on common network security situation evaluation and forecast. The results are derived from *three aspects, namely, model, knowledge representation, and assessment methods*.

First, from the *model aspect*, based on data from the Computer Oracle and Password System, Ortalo et al. [1] adopted privilege graph theory to model system bug and

hole and utilized the Markov model to calculate the mean costs when attackers beat the system security objectives and quantitatively measure system safety. Feng et al. [2] utilized vulnerability scanning and other technological means and quantized the evaluation indexes of vulnerability factors to summarize the standards, methods, tools, and models in the field of information security risk evaluation. Xiao and Dai [3] applied a multilayer fuzzy comprehensive evaluation method to evaluate the information system risk level. Tao [4] and Wang et al. [5] proposed an immunity-based quantitative detection model and method for network security risk. On the basis of this model, Wang et al. [6] introduced a fault model-based risk evaluation model for network information system and the formative description of risk management. Yong et al. [7] proposed a multiangle quantitative model as the evaluation system framework and support platform of a network information system security test. Wu et al. [8] provided an efficiency-evaluating approach for the security measures of an information system under the given vulnerability set. This approach employed colored Petri-Net tools for uniform modeling and simulated the interaction among the workflow, attack flow, and security measures of the system.

Second, from the *knowledge representation aspect*, Yan [9] presented concepts of composition independence, combination complementary, and combination relevance security factors. A formative evaluation model of information system security measurement and its realization were provided through a definition of the correlation among access path, standard path, and components. Some methods combined qualitative and quantitative methods for studies on network security evaluation through evaluating the mutual effects of threat, bug, and attack results. For example, the multistage attack model framework proposed by Clark et al. [10] applied vulnerability description, object-oriented network modeling, and attacker expression capacity to carry out qualitative and quantitative complicated vulnerability risk analyses. Zhao et al. [11] also proposed risk level formula and entropy weight, applied likelihood estimation of risk probability, and utilized entropy theory to handle the weight vector of risk factors specific to the analytic hierarchy process and the strong subjectivity of fuzzy logic.

Finally, from the *assessment methods*, Bilar [12] compared the security event data caused by the modified time of bug and patch and quantitatively analyzed the risk of information system network. Cardoso and Freire [13] proposed a quantification evaluation method of an agent-based distributed system. An agent was utilized to monitor the host security statuses of a subnet or other nodes for evaluation. Chen et al. [14] introduced a quantitative evaluation method of service and host-to-network stratification network security threat situation, which further expanded the bug-based vulnerability analysis to the network level. Wang et al. [15, 16] designed a multi-source fusion evaluation system of network security situation awareness. Eom et al. [17] introduced asset indicators of the assessed information system. Machine learning in China and abroad mainly forecasts situations through a neural network method. Shanghai Jiaotong University and Harbin Engineering University, respectively, realized situation forecasts through a radial basis function [18] and a genetic algorithm,

back propagation neural network, as well as providing a preliminary solution to the situation forecast problem. Anwar et al. [19] proposed an index system that converged network equipment, service, vulnerability, access control, and other aspects. Kandula et al. [20] considered fine granularity to assess the problems of the enterprise network—host process level. Gong and Zhuo [21] introduced cyberspace situational awareness (CSA) and its origin, conception, objective, and characteristics. This study provided the development directions of CSA and offered conclusions from issue, technical, and application systems. Recently, [22, 23] proposed a network threat assessment based on alert verification. Tian et al. [24] also proposed a method to quantitatively assess network threat situations based on alerts and contextual information.

For the security event attack features of wireless sensor networks [25], a multitask learning method is adopted for forecasting. This method uses domain information in the training signals of relevant tasks for inductive bias and further improves the generalization performance. Multitask learning refers to the parallel learning of learning tasks with sharing expression, and the learning of each task can help improve the learning of other tasks. Accordingly, multitask learning has better effects on machine learning by a single neural network.

On the whole, the study on wireless sensor network security in this paper is of considerable importance. On the one hand, a large-scale sensor network is used for topology partitioning and for calculating the similarity degree among regional subnets. The occurrence and development trends of unknown network security events can be forecasted and speculated through multitask learning of the occurrence and transmission characteristics of the known network security events, thereby providing bases for the effective control of unknown network attacks and restraining the entire network transmission of attacks. On the other hand, given that many subregions in the network have no security detection methods, the attack data in these regions may not be collected. In this case, part data from this region or data from other similar subregions are utilized to forecast network attacks in data-missing regions. The quantitative evaluation value of unknown regional network security events can also be calculated. This study adopts the PNSIUD method in case of data missing. The method employs the basic idea of the transductive support vector machine (TSVM) method to predict the missing attack data in the target region according to the known data in similar regions.

2. Region Similarity-Based Security Event Forecast for Wireless Sensor Networks

When large-scale security events occur in each subregion of wireless sensors, a situation forecast needs to be made in each subregion of the network according to requirements. However, if a situation forecast is made on the data in this subregion in isolation, it may fail to consider the influences of the surrounding network on the target network and the similarities in other subregions. Hence, the forecast results will not be ideal. In this way, the measurement data from other similarity subregions can be utilized to improve the situation evaluation of the target network and the forecast accuracy.

TABLE 1: Similarity measurement index of the network topological structure.

Network structure (NS)	Topology (Topo)	Nodes	
		Edges	
		Slope of degree distribution linefit (SDDL)	
	Infrastructure (Inf)	Normalized average neighbor degree (NAAND)	
		Slope of coreness distribution linefit (SCDL)	
		Assortative coefficient (AC)	
		Max edge betweenness (MEB)	
Network traffic (NT)	Proportion of traffic classification (PTC)	Standard deviation of distance (SDD)	
		Distribution of bandwidth (DB)	
		Distribution of delay (DD)	
Asset	Proportion of total traffic (PTT)	Traffic distribution within the network (TDN)	
		Number of important assets (NIA)	Important asset value (IAV)
			Position distribution of assets (PDA)
Security appliances (SA)	Traffic monitor (TM)	Number of TM (NTM)	
		Position distribution of TM (PDTM)	
	Intrusion detection system (IDS)	Type (TTM)	
		Number of IDS (NIDS)	
		Position distribution of IDS (PDIDS)	
Network management (NM)	Type of IDS (TIDS)		
	Type of NM (TNM)		

This study adopts a multitask learning method to forecast the situation of the target network. This method fully utilizes data from the surrounding regions of the target network and data from similar regions in the network environment of the target region.

Based on the aforementioned idea, this study forecasts two targets, namely, the topology element-based forecast on target network availability damage and the overall situation forecast of target network security events.

2.1. Similarity Measurement of the Sensor Network. This study utilizes measurement data from other similar subregions in the network as an auxiliary knowledge structure to improve the evaluation of the target region and the forecast accuracy. All similarities of the network are measured. Network similarity measures the similarity of two network environments. If two network environments are similar, then the knowledge structures of data between the two networks may be similar, and they can transfer knowledge to realize shared knowledge.

The coexistence of a heterogeneous environment, multiple vendors, and multiple protocols presently leads to a highly complicated network environment and the gradual diversification of user demands. In this case, the network similarity measurement will be extremely complicated. First, in selecting network similarity indexes, various influence factors of network similarity exist; thus, selecting the proper measurement indexes of target problems is important. Second, after proper measurement indexes are selected, guaranteeing the efficiency and correctness of the similarity calculation is crucial. To satisfy the requirements of quantitative

evaluation and forecast of a large-scale network, this study selects proper network similarity measurement indexes and formalizes and defines the calculation process of network similarity measurement, which establishes a good foundation for forecasting the region similarity-based security event of a national large-scale network.

2.1.1. Measurement Indexes of Network Similarity. Through analysis and argument, we consider that the influence factors of the heterogeneous degree of a large-scale network mainly include network structure, infrastructure, assets, network security device, and network flow information. Each part can be divided into concrete influence factors. Topology vulnerability factor is selected as a measurement index of the overall similarity measurement of the network topological structure. The overall measurement is shown in Table 1.

2.1.2. Design of the Similarity Measurement of Wireless Sensor Subnetworks. The similarity of two networks is formally defined according to the overall measurement indexes. Supposing the two networks are P and Q , $P = (NS_p, NT_p, Asset_p, SA_p)$ and $Q = (NS_q, NT_q, Asset_q, SA_q)$.

First, the vector of the P network is set as follows:

- (1) The network structure similarity measurement is $NS_p = (Topo_p, Inf_p)$, where the network topological structure is $Topo_p = (Node_p, Edges_p, SDDL_p, NAAND_p, SCDL_p, AC_p, MEB_p, SDD_p)$, and the network infrastructure is $Inf_p = (DB_p, DD_p)$.

- (2) The network flow similarity measurement is $NT_p = (PTC_p, PTT_p, TDN_p)$.
- (3) The network asset similarity measurement is $Asset_p = (NIA_p, IAV_p, PDA_p)$.
- (4) The network security equipment similarity measurement is $SA_p = (TM_p, IDS_p, NM_p)$, where the flow monitoring is set as $TM_p = (NTM_p, PDTM_p, TTM_p)$, the intrusion detection is $IDS_p = (NIDS_p, PDIDS_p, TIDS_p)$, and the network management is $NM_p = (TNM_p)$.

Second, the vector of the Q network is set as follows:

- (1) The network structure similarity measurement is $NS_Q = (TOPO_Q, Inf_Q)$, where the network topological structure is $Topo_Q = (Node_Q, Edges_Q, SDDL_Q, NAAND_Q, SCDL_Q, AC_Q, MEB_Q, SDD_Q)$, and the network infrastructure is $Inf_Q = (DB_Q, DD_Q)$.
- (2) The network flow similarity measurement is $NT_Q = (PTC_Q, PTT_Q, TDN_Q)$.
- (3) The network asset similarity measurement is $Asset_Q = (NIA_Q, IAV_Q, PDA_Q)$.
- (4) The network security equipment similarity measurement is $SA_Q = (TM_Q, IDS_Q, NM_Q)$, where

the flow monitoring is set as $TM_Q = (NTM_Q, PDTM_Q, TTM_Q)$, the intrusion detection is $IDS_Q = (NIDS_Q, PDIDS_Q, TIDS_Q)$, and the network management is $NM_Q = (TNM_Q)$.

2.1.3. Formalized Network Similarity Measurement

(1) *Overall Network Environment Similarity.* Consider the following:

$$S_{\text{Network}}(P, Q) = S_{\text{NS}}(P, Q) + S_{\text{NT}}(P, Q) + S_{\text{Asset}}(P, Q) + S_{\text{SA}}(P, Q). \quad (1)$$

(2) *Network Structure Similarity.* The network structure similarity is $S_{\text{NS}}(P, Q) = \omega_1 S_{\text{Topo}}(P, Q) + \omega_2 S_{\text{Inf}}(P, Q)$, where $VS_{\text{Topo}} = (S_{\text{Nodes}}(P, Q), S_{\text{Edges}}(P, Q), S_{\text{SDDL}}(P, Q), S_{\text{NAAND}}(P, Q), S_{\text{SCDL}}(P, Q), S_{\text{AC}}(P, Q), S_{\text{MEB}}(P, Q), S_{\text{SDD}}(P, Q))$; and the network topological structure similarity is $S_{\text{Topo}}(P, Q) = \sum VS_{\text{Topo}} \omega_i / \sum \omega_i$, where ω_i is the weight of similarity measurement i . The influence of different node numbers of the network router on the network similarity is not linear. Thus, exponential transformation is performed on the network similarity, and the similarity of node numbers of the network router can be expressed as

$$S_{\text{Nodes}}(P, Q) = \begin{cases} M, & |\text{Nodes}_P - \text{Nodes}_Q| \leq \alpha, \\ L + (M - L) \exp(-k(|\text{Nodes}_P - \text{Nodes}_Q| - \alpha)), & |\text{Nodes}_P - \text{Nodes}_Q| > \alpha. \end{cases} \quad (2)$$

Compared with the influences of the node number of the router, the influence of connected sides on the network

similarity is relatively moderate. Power function transformation is conducted, and the similarity is

$$S_{\text{Edges}}(P, Q) = \begin{cases} M, & |\text{Edges}_P - \text{Edges}_Q| \leq \alpha, \\ L + \frac{(M - L)}{\left(1 + k(\alpha - |\text{Edges}_P - \text{Edges}_Q|)^\beta\right)}, & |\text{Edges}_P - \text{Edges}_Q| > \alpha, \end{cases} \quad (3)$$

where L is usually set to 0, M is set to 1, and the result is normalized. α represents the node tolerance, and k and β represent the coordinate coefficients used to adjust the similarity decay rate.

Network infrastructure similarity can be concluded as its weighted Euclidean distance:

$$S_{\text{Inf}}(P, Q) = \sqrt{\omega_1 |\text{DB}_P - \text{DB}_Q|^2 + \omega_2 |\text{DD}_P - \text{DD}_Q|^2}. \quad (4)$$

(3) *Network Flow Similarity.* Consider the following:

$$S_{\text{NT}}(P, Q) = \omega_1 S_{\text{PTC}}(P, Q) + \omega_2 S_{\text{PTT}}(P, Q) + \omega_3 S_{\text{TDN}}(P, Q). \quad (5)$$

The similarities of flow classification ratio, exit, and entrance total flow rate and network flow distribution can be measured by covariance:

$$\begin{aligned} S_{\text{PTC}}(P, Q) &= E((\text{PTC}_P - \mu_P)(\text{PTC}_Q - u_Q)), \\ S_{\text{PTT}}(P, Q) &= E((\text{PTT}_P - \mu_P)(\text{PTT}_Q - u_Q)), \\ S_{\text{TDN}}(P, Q) &= E((\text{TDN}_P - \mu_P)(\text{TDN}_Q - u_Q)). \end{aligned} \quad (6)$$

(1) *Asset Similarity*. Consider the following:

$$S_{\text{Asset}}(P, Q) = \omega_1 E((\text{NIA}_P \cdot \text{IAV}_P - \mu_P)(\text{NIA}_Q \cdot \text{IAV}_Q - u_Q)) + \omega_2 E((\text{PDA}_P - \mu_P)(\text{PDA}_Q - u_Q)). \quad (7)$$

(2) *Network Security Equipment Similarity*. Consider the following:

$$S_{\text{SA}}(P, Q) = \omega_1 S_{\text{TM}}(P, Q) + \omega_2 S_{\text{IDS}}(P, Q) + \omega_3 S_{\text{NM}}(P, Q), \quad (8)$$

where

$$S_{\text{ITM}}(P, Q) = \sqrt{\frac{\omega_1 S_{\text{NTM}}(P, Q)^2 + \omega_1 S_{\text{PDTM}}(P, Q)^2 + \omega_1 S_{\text{TTYPE}}(P, Q)^2}{\sum \omega}},$$

$$S_{\text{NTM}}(P, Q) = \begin{cases} M, & |\text{NTM}_P - \text{NTM}_Q| \leq \alpha, \\ L + (M - L) \exp(-k(|\text{NTM}_P - \text{NTM}_Q| - \alpha)), & |\text{NTM}_P - \text{NTM}_Q| > \alpha, \end{cases} \quad (9)$$

$$S_{\text{PDTM}}(P, Q) = E((\text{PDTM}_P - \mu_P)(\text{PDTM}_Q - u_Q)),$$

$$S_{\text{IDS}}(P, Q) = \sqrt{\frac{\omega_1 S_{\text{NIDS}}(P, Q)^2 + \omega_1 S_{\text{PDIDS}}(P, Q)^2 + \omega_1 S_{\text{TIDS}}(P, Q)^2}{\sum \omega}}.$$

The influences of location number difference in the network intrusion detection system (IDS) on network similarity are

not in linear relation. Thus, exponential transformation is conducted to obtain the network IDS location number similarity. Consider

$$S_{\text{NIDS}}(P, Q) = \begin{cases} M, & |\text{NIDS}_P - \text{NIDS}_Q| \leq \alpha, \\ L + (M - L) \exp(-k(|\text{NIDS}_P - \text{NIDS}_Q| - \alpha)), & |\text{NIDS}_P - \text{NIDS}_Q| > \alpha, \end{cases} \quad (10)$$

where L is 0, M is 1, and α represents the node tolerance. Given that the IDS number in the actual network is small, the value of α is set small, whereas k is set large to increase the similarity decay speed.

2.2. Region Similarity-Based Security Event Damage Prediction for Wireless Sensor Network. A multitask learning method is used to forecast; it utilizes the domain information in dependent-task training signals for induction bias and improving generalization performance. Multitask learning performs parallel learning on multiple learning tasks with sharing expression, and the learning of each task can help other tasks learn better. Furthermore, it has better effects than single-task machine learning.

People have proposed an algorithm that considers the connections among subproblems to improve the forecast accuracy and overall noise resistance of complex problems. This approach is called multitask learning algorithm.

Unlike single-task learning, multitask learning aims to address multielement and multidimensional learning problems. The input and output values of a system are considered multielements. The task number of multitask learning is generally determined by the dimensionality of the output

value of the system. For example, if the system outputs a T -dimensional vector, then multitask learning learns T tasks at the same time.

Figure 1 shows the multitask learning algorithm process, which inherits the consistent aim of machine learning and where training dataset is directly constituted of the input and output values of the complex system. In the learning process, parallel learning is conducted on four learning tasks, and their results influence one another mutually. This process is the core idea of the multitask learning problem. Multitask learning can overcome the performance bottleneck of single-task learning and further improve the noise resistance of the algorithm and the accuracy of learning outcome.

Based on the security event evaluation data of a large-scale wireless sensor network, the primary algorithm of region similarity-based security event forecast for a large-scale network is as shown in Algorithm 1.

The basic idea of the algorithm is setting the target zone p as the main task and inputting measured index, task weight, regulation parameter h , and similarity positive threshold t_{positive} as the measurement network of all subregions. The output is the output set and errors verified by cross-validation. The algorithm first calculates the network

```

(1) Input: data for all sub-regions  $\{(X_i^l, Y_i^l)\} (l = 1, \dots, m)$ 
(2) Parameters:  $h$  and  $\lambda_1, \dots, \lambda_m$ , main task  $p$  and threshold  $t_{\text{positive}}$ 
(3) Output: main task prediction data  $(X_i^p, Y_i^p)$ , sim tasks  $S_j^p$ , and class loss  $CL_p$ 
(4) Initialize:  $u_l = 0 (l = 1, \dots, m) j = 1$ , arbitrary  $h \times p$  dimensional matrix  $\Theta$ ,  $S_j^p = 0$ 
(5) iterate
(6)   for  $l = 1$  to  $m$  do
(7)     If  $l \sim p$ 
(8)       similarity =  $S_{\text{Network}}((X_i^p, Y_i^p), (X_i^l, Y_i^l))$ 
(9)       If similarity  $\geq t_{\text{positive}}$ 
(10)         $S_j^p = \text{similarity}, j = j + 1$ 
(11)        With fixed  $\Theta$  and  $v_l = \Theta u_l$  approximately solve for  $\widehat{w}_l$ :
(12)         $\widehat{w}_l = \arg \min_{w_l} \left[ \left( \frac{1}{n_l} \right) \sum_{i=1}^{n_l} L(w_l^T X_i^l + (v_l^T \Theta) X_i^l, Y_i^l) + \lambda_l \|w_l\|_2^2 \right]$ 
(13)        Let  $u_l = w_l + \Theta^T v_l$ 
(14)      end if
(15)    end if
(16)  end for
(17)  Compute the singular value decomposition of  $U = [\sqrt{\lambda_1} u_1 \dots \sqrt{\lambda_m} u_m]$ :
(18)   $U = V_1 D V_2^T$  (with diagonals of  $D$  in descending order)
(19)  Let the rows of  $\Theta$  be the first  $h$  rows of  $V_1^T$ 
(20) until converge
(21) using  $\Theta$  through CV output  $(X_i^p, Y_i^p)$  and  $CL_p$ 

```

ALGORITHM 1

similarities of target tasks in the network region and other subregions. If this similarity is larger than the set threshold, then its subregions are taken in learning tasks and iterate until convergence. Finally, the algorithm output is obtained through cross-validation.

2.3. Experimental Results and Analysis. A network topology with 66,072 routing nodes and 96,073 links is classified, and the connected subgraph with a topology size of approximately 1,000 nodes is selected as the experimental topology. A national topology with an actual measure of 66,072 routing nodes and 96,073 links is classified, and the connected subgraphs with a topology size of approximately 1,000 nodes are selected as experimental topology.

This topology is derived from Harbin Institute of Technology in the network topology nodes on the main stem distribution obtained from the measurements of actual topology data. The topology contains 66,072 routing nodes and 96,073 links. We divide the connected subgraphs with 1,000 (+50 or -50) nodes from the actual topology and experiment with 100 groups. The topological division algorithm metis [26] is used to divide the large-scale topology graph into approximately 1,000 nodes. The subtopology graph is connected.

In this topology, four worm attacks and Gnutella application are simulated, in which worm 1 attacks 159 groups, worm 2 attacks 30 groups, worm 3 attacks 30 groups, worm 4 attacks 30 groups, and Gnutella applies 89 groups.

The multitask learning algorithm adopts a linear classifier; therefore, the network damage characteristic value is obtained with weighted sum and discretization. The analyzed topology characteristic value is taken as input, and whether damage value can fall in this interval is taken as output. Each

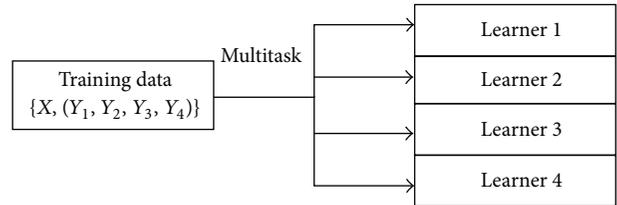


FIGURE 1: Diagram of the multitask learning algorithm.

interval is taken as one learning task, in which the damage value of the worm 1 attack is discretized into seven learning tasks, the damage values of the worm 2–worm 4 attacks are discretized into five learning tasks, and the damage value of the Gnutella application is discretized into four learning tasks. Thus, $159 * 7 + 30 * 5 * 3 + 89 * 4 = 1,919$ groups of samples are obtained.

The fifth learning task in the worm 1 attack is taken as the main task, and other tasks are taken as auxiliary tasks for learning. Cross-validation is also conducted. This process is mainly used in modeling application. In the given modeling samples, most samples are taken for modeling, whereas a small number of samples are established for forecasting. Their forecast error can be made to record their square sum. This process proceeds until all samples are forecasted once and only once. In the training process, fivefold cross-validation is performed; specifically, the dataset is divided into five, four for training and one for testing. The mean of five results is taken as the estimation of the algorithm precision. The final experimental results are as follows.

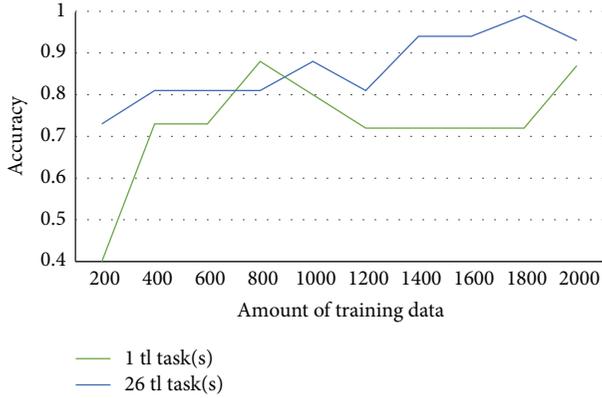


FIGURE 2: Mean square error of results.

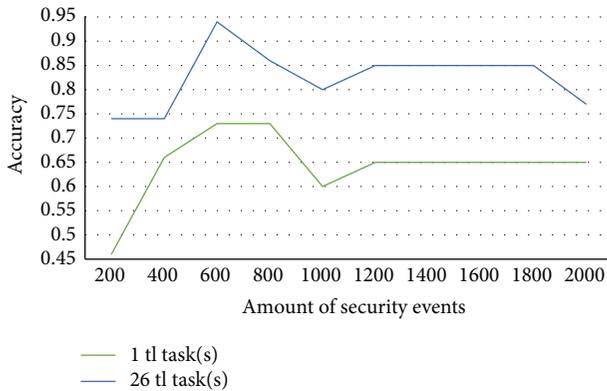


FIGURE 3: Comparison of the forecast results of unknown security events.

In the first experiment, one region is selected from the divided topology subdomain as the main zone. A total of 26 similar subregions are then selected as associated learning tasks to study the influences of increasing data amount of tasks on forecast accuracy. The training results of the experiment are shown in Figure 2.

Figure 2 presents that the accuracy of the task-joint-training results of 26 subregions is obviously higher than that of the single-training result of one subregion. In nearly 800 groups of training data, the forecast accuracy of the similarity region forecast is lower than that of single-task learning. The reason may be the cross-validation of the similarity region forecast. However, the data distribution characteristics of the randomly segmented training set and the validation set differ considerably, which decreases forecast accuracy. In general, the similarity region forecast algorithm has obvious effects on improving forecast accuracy.

Figure 3 indicates that for unknown security event forecasts the forecast accuracy of the classifier after training of the similarity forecast algorithm is higher and the effects are obviously better than those of the classifier after training of single-task learning.

In the second experiment, a region with a higher forecast error from 60 national subregions is selected as the target region. The task of the region is the main task. The data of

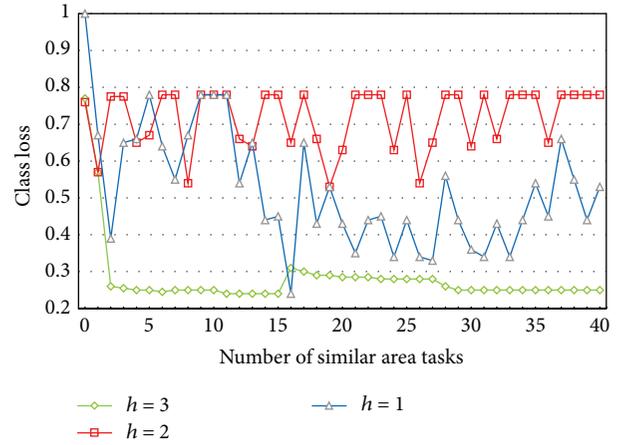


FIGURE 4: Regional similarity security event forecast error.

other subregions form a set, and each task in the set is the forecast task of a region. The data in the set are then filtered. The sets that are completely dissimilar to the target subregion are removed, which results in a set that has remaining data of 47 regions.

In the experiment, tasks in this set are gradually added in the forecast algorithm. The forecast error of adjusting different parameter h is shown in Figure 4.

Experimental results show that when the similarity network regions participating in learning are 3, the forecast error decreases to 0.26, which indicates that the tasks in the similarity region have good effects on improving forecast accuracy. However, when the tasks in the similarity region continue increasing, the improvement of forecast accuracy is not obvious. When the forecast tasks reach 17, error increases. Through checking, we find that the network environment of the 17th subregion is basically consistent with that of the target region, but its security events in the network are dense, thereby forming forecast noise of the target region. Therefore, the selection of proper similar regions requires both similarity measurement and analysis process with expert participation.

3. Security Event Forecast for Sensor Network in Case of Data Missing

When large-scale security spreads in each subregion, data (including throughput, packet loss probability, delay, and invasion index) in each subregion need to be collected to perform quantitative evaluations on network availability. However, given that many subregions have no IDS, the invasion index data of these regions may not be collected. In this case, part data of this region or data from other similarity subregions can be used to forecast the invasion index in data-missing regions and further obtain the quantitative evaluation values of network security events.

The PNSIUD method in case of data missing is adopted to solve the above problem. The data of the missing invasion index in the target region are forecasted in accordance with the basic idea of TSVM and the known data of similar regions

(including throughput, packet loss probability, delay, and invasion index).

3.1. TSVM Theory. The proposal of the transductive learning concept is established mainly from two facts. First, in the numerous actual applications of machine learning, tagged training samples usually cost significant manpower and material resources. Therefore, the tagged training sample from learning machine is usually limited, whereas numerous untagged samples are easy to obtain. The classification of missing invasion web pages in this study is a typical sample. In this application, manual or semiautomatic tagging of known web pages is usually trivial and dull. However, obtaining thousands of untagged web pages is easy. Considering that tagged training samples are few, the overall distribution characteristics of data cannot be well described, and the classifier that directly adopts tagged samples for learning usually has poor performance. Can the easily obtained untagged samples be used for improvement? Generating a problem on how to use a few tagged samples and numerous untagged samples to train a learning machine is natural.

Second, in the traditional inductive learning, a learning machine tries to summarize a discriminant function according to known tagged training samples. Consequently, the entire sample spatial distribution may have a low expected discriminant error. However, many actual problems only aim at the identification and classification of some specific samples, attempting to obtain the classification of a specific test set with a small error. If this specific test set is organically added in the design and training processes of the classifier, not only can this specific test set obtain good classification effects, but also the generalization performance of the original inductive learning algorithm can also be improved to a great extent. Furthermore, the shortcoming caused by few training data in the inductive learning algorithm can be made up for. This feature is the basic idea of transductive learning.

In transductive learning, a learning machine can use less tagged samples and more untagged samples in the training process for learning. An important feature of transductive learning lies in the sample distribution information of the test set being transferred from untagged samples to the final classifier in the learning process of mixed samples. Given numerous untagged samples, tagged samples can better describe the data characteristics of the entire sample space, such that the trained classifier can achieve improved generalization performance. Transductive learning is applied to different degrees of studies and applications in each field of mode recognition.

3.2. PNSIUD Method in Case of Data Missing. Based on the above theory, data without invasion index in the target region are called untagged data, whereas data with invasion index in the target region are called tagged data. Tagged data from this region or other similarity subregions are utilized to forecast the invasion index in the data-missing region. The principle and implementation of the PNSIUD algorithm are introduced below.

The training sample points with invasion indexes in the known similar subregions are

$$(x_1, y_1), \dots, (x_n, y_n), \quad x_i \in R^m, \quad y_i \in \{-1, +1\}. \quad (11)$$

The training points without invasion indexes in the target region are $x_1^*, x_2^*, x_3^*, \dots, x_k^*$.

Under general linear inseparable conditions, the training process of the network security event forecast method in case of data missing can be described as the following optimization problems:

$$\begin{aligned} \text{Minimize} \quad & \text{over } (y_1^*, \dots, y_k^*, w, b, \xi_1, \dots, \xi_n, \xi_1^*, \dots, \xi_k^*) \\ & \frac{1}{2} \|\omega\|^2 + C \sum_{i=1}^n \xi_i + C^* \sum_{j=1}^k \xi_j^* \\ \text{subject to} \quad & y_i [w \cdot x_i + b] \geq 1 - \xi_i, \quad \forall_{i=1}^n \\ & y_j [w \cdot x_j^* + b] \geq 1 - \xi_j^*, \quad \forall_{j=1}^k \\ & \xi_i \geq 0, \quad \forall_{i=1}^n \\ & \xi_j^* \geq 0, \quad \forall_{j=1}^k, \end{aligned} \quad (12)$$

where parameters C and C^* are named as regulation parameters. Their functions are similar to parameter C in formulae (12). Parameter C^* is called the influence factor of untagged samples in the training process, and $C^* \xi_j^*$ is called the influence item of untagged sample j in the objective function.

The training process of PNSIUD is the solving process of the above optimization problems. The training algorithm can be roughly divided into several steps.

Step 1. Parameters C and C^* are specified, and inductive learning is used to have an initial learning on tagged samples, thereby obtaining an initial classifier. According to one rule, positive tagged samples, N , in an untagged sample are specified.

Step 2. The initial classifier is used to classify untagged samples. According to the discriminant function output of each untagged sample N untagged sample with a maximum output can be temporarily assigned with a tag value, whereas others are endowed with a negative tag value. A temporary influence factor, C_{tmp}^* , is assigned.

Step 3. All samples are retrained. For new classifiers, a pair of tag signs in test samples with different tag values are exchanged according to certain rules. In this way, the objective function value in optimization problem (11) can decrease to the maximum. This step can be implemented repeatedly until no sample conforming to exchange conditions can be found.

Step 4. Temporary influence factor C_{tmp}^* is evenly increased, and Step 3 is repeated. When $C_{\text{tmp}}^* \geq C^*$, the algorithm ends, and results are considered as the output.

The tag sign exchange in Step 3 guarantees that the solution after exchange is better than that before exchange. The temporary influence factor in Step 4 from small to large gradually increases, and gradually increasing the influences of untagged samples on untagged samples can minimize the classification error of untagged samples. The specified C^* in Step 1 is limited. From the exit criteria in Step 4, the algorithm can end after limited-time implementation and output results.

3.3. Analysis of the Experimental Results of PNSIUD-Based Security Event Invasion Index Forecast. In this study, the sample data without invasion index in the target region are considered untagged, and they need to be tagged by the tagged sample training from this region or similar regions. Owing to the numerous untagged samples and the identification and forecast of specified target regions, PNSIUD has better forecast performance (tagging) than the traditional support vector machine (SVM) method.

The topological region with 66,072 routing nodes and 96,073 links is divided into several subregions, and the data of national security events that spread in each subregion in unit interval (there are many data without invasion index) are taken as experimental data. Tagged samples are taken as the auxiliary data for knowledge structure mining and further obtaining transfer knowledge structure. PNSIUD is utilized to forecast the region of untagged samples.

Below is the comparison of the forecast results between PNSIUD and SVM in one region. With an increase in untagged training samples, namely, samples without invasion index, from 100 to 1,000, the overall distribution characteristics of data can be better described because the PNSIUD method can utilize the knowledge of similar regions for learning. In this way, more samples lead to higher prediction accuracy. However, SVM only forecasts according to the known tagged samples and does not learn the knowledge of other similar regions. Consequently, its accuracy decreases, as shown in Figure 5.

Figure 6 is the forecast of those methods on data without invasion index in the same subregion. The forecast accuracy of PNSIUD is 64.48%, whereas that of SVM is 33.56%. Thus, PNSIUD has higher forecast accuracy than SVM.

The experiment indicates that when numerous untagged samples and a few tagged samples exist, the distribution characteristics of tagged samples cannot reflect the characteristics of the entire dataset. The accuracy of the SVM algorithm thus decreases. However, the PNSIUD method can learn from untagged samples and well reflect the data distribution characteristics of the entire dataset; hence, its accuracy can be improved.

4. Conclusion

This study conducts topology partitioning of a network from the characteristics of a large-scale sensor network. On this basis, this study proposes multitask learning-based

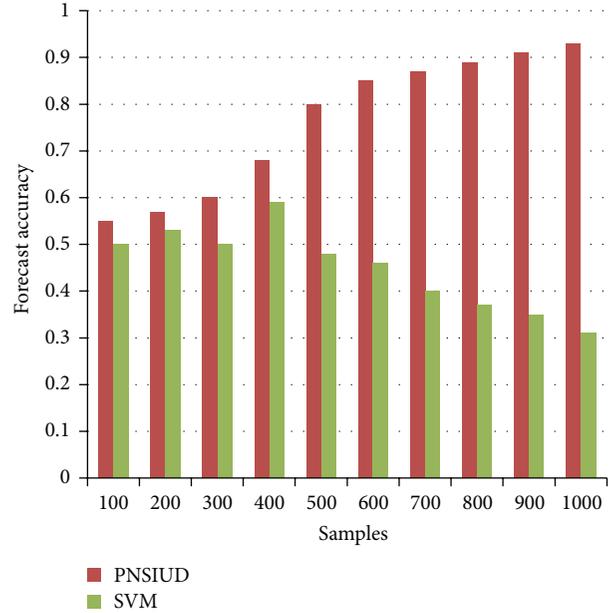


FIGURE 5: Comparison of forecast accuracy.

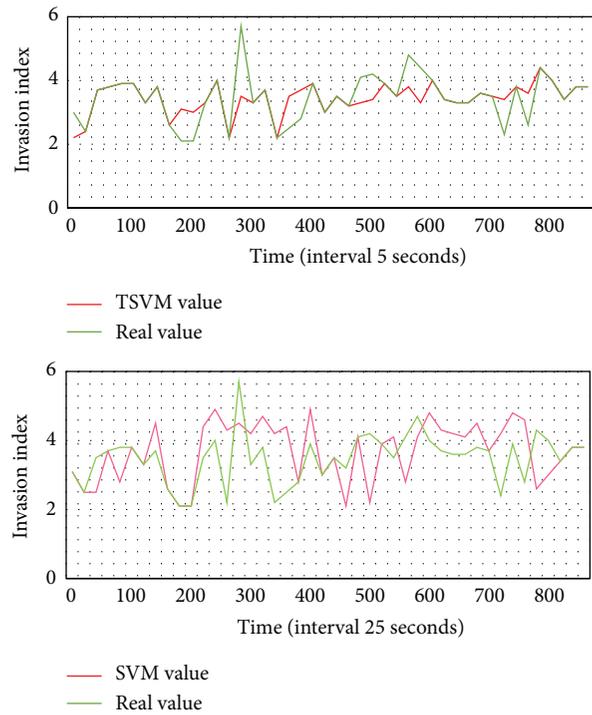


FIGURE 6: Network security event forecast in case of missing sensor network data.

similar region network security event forecast of wireless sensor networks. The experimental results show that for an unknown security event forecast the forecast accuracy and effects of classifier after the training of the similarity forecast algorithm are significantly better than those after the training of single-task learning. For data without invasion indexes in the same subregion, the forecast accuracy of PNSIUD is

64.48%, whereas that of SVM is 33.56%. Thus, PNSIUD has higher forecast accuracy than SVM.

Wireless sensor networks have strong dynamics and uncertainty, especially network topological changes. In this study, we take the topology and main factors in Table 1 as examples to illustrate how to forecast the missing attack data in the target region according to the known data in similar regions. Our work lacks some detailed factors in subregions. In the future, we will add more detailed factors into our research experiment, such as user characteristics and attack behavior. We will also introduce transfer learning into wireless sensor network security event forecast to improve the forecast adaptability.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was supported in part by the National Basic Research Program of China under Grant no. G2011CB302605. This work is partially supported by the National Natural Science Foundation of China (NSFC) under grant nos. 61472108, 61173145.

References

- [1] R. Ortalo, Y. Deswarte, and M. Kaâniche, "Experimenting with quantitative evaluation tools for monitoring operational security," *IEEE Transactions on Software Engineering*, vol. 25, no. 5, pp. 633–650, 1999.
- [2] D.-G. Feng, Y. Zhang, and Y.-Q. Zhang, "Survey of information security risk assessment," *Journal-China Institute of Communications*, vol. 25, no. 7, pp. 10–18, 2004.
- [3] L. Xiao and Z.-K. Dai, "Model of multilevel fuzzy comprehensive risk evaluation of information system," *Journal of Sichuan University (Engineering Science Edition)*, vol. 36, no. 5, pp. 98–102, 2004.
- [4] L. Tao, "An immunity based network security risk estimation," *Science in China—Series F: Information Sciences*, vol. 48, no. 5, pp. 557–578, 2005.
- [5] Y.-F. Wang, T. Li, X.-Q. Hu, and C. Song, "Real-time method of risk evaluation based on artificial immune system for network security," *Acta Electronica Sinica*, vol. 33, no. 5, pp. 945–949, 2005.
- [6] Y. Wang, Z. L. Zeng, and X. Chen, "Quantitative method for risk assessment and management of information system," *Computer Engineering and Application*, vol. 22, pp. 8–10, 2005.
- [7] Z. Yong, T. Xiaobin, and X. Hongsheng, "A novel approach to network security situation awareness based on multi-perspective analysis," in *Proceedings of the International Conference on Computational Intelligence and Security*, pp. 768–772, IEEE, Harbin, China, December 2007.
- [8] D. Wu, D.-G. Feng, Y.-F. Lian, and K. Chen, "Efficiency evaluation model of system security measures in the given vulnerabilities set," *Journal of Software*, vol. 23, no. 7, pp. 1880–1898, 2012.
- [9] Q. Yan, "Information system security metrics and evaluation model," *Acta Electronica Sinica*, vol. 31, no. 9, pp. 1351–1355, 2003.
- [10] K. Clark, S. Tyree, J. Dawkins, and J. Hale, "Qualitative and quantitative analytical techniques for network security assessment," in *Proceedings from the 5th Annual IEEE System, Man and Cybernetics Information Assurance Workshop (SMC '04)*, pp. 321–328, June 2004.
- [11] D.-M. Zhao, J.-H. Wang, W. U. Jing, and J.-F. Ma, "Using fuzzy logic and entropy theory to risk assessment of the information security," in *Proceedings of the International Conference on Machine Learning and Cybernetics (ICMLC '05)*, vol. 4, pp. 2448–2453, IEEE, Guangzhou, China, August 2005.
- [12] D. Bilar, *Quantitative risk analysis of computer networks [Ph.D. thesis]*, Dartmouth College, Hanover, Germany, 2003.
- [13] R. C. Cardoso and M. M. Freire, "Intelligent assessment of distributed security in TCP/IP networks," in *High Speed Networks and Multimedia Communications*, pp. 1092–1099, Springer, Berlin, Germany, 2004.
- [14] X.-Z. Chen, Q.-H. Zheng, X.-H. Guan, and C.-G. Lin, "Quantitative hierarchical threat evaluation model for network security," *Journal of Software*, vol. 17, no. 4, pp. 885–897, 2006.
- [15] H. Wang, J. Lai, L. Zhu, Y. Liang et al., "Survey of network situation awareness system," *Computer Science*, vol. 33, no. 10, pp. 5–10, 2006.
- [16] H. Wang, J. Lai, M. Hu, and Y. Liang, "Research on key technologies for implementing network security situation awareness," *Geomatics and Information Science of Wuhan University*, vol. 33, no. 10, pp. 995–998, 2008.
- [17] J.-H. Eom, S.-H. Park, Y.-J. Han, and T.-M. Chung, "Risk assessment method based on business process-oriented asset evaluation for information system security," in *Computational Science—ICCS 2007*, pp. 1024–1031, Springer, Berlin, Germany, 2007.
- [18] W. Ren, *The intelligent study of networks security situation assesment [M.S. thesis]*, Shanghai Jiao Tong University, 2007.
- [19] Z. Anwar, R. Shankesi, and R. H. Campbell, "Automatic security assessment of critical cyber-infrastructures," in *Proceedings of the IEEE International Conference on Dependable Systems and Networks With FTCS and DCC (DSN '08)*, pp. 366–375, Anchorage, Alaska, USA, June 2008.
- [20] S. Kandula, R. Mahajan, P. Verkaik, S. Agarwal, J. Padhye, and P. Bahl, "Detailed diagnosis in enterprise networks," *SIGCOMM Computer Communication Review*, vol. 39, no. 4, pp. 243–254, 2009.
- [21] Z.-H. Gong and Y. Zhuo, "Research on cyberspace situational awareness," *Journal of Software*, vol. 21, no. 7, pp. 1605–1619, 2010.
- [22] R. Xi, X. Yun, S. Jin, and Y. Zhang, "Network threat assessment based on alert verification," in *Proceedings of the 12th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT '11)*, pp. 30–34, IEEE, Gwangju, South Korea, October 2011.
- [23] A. B. Mohamed, N. B. Idris, and B. Shanmugum, "Alert correlation framework using a novel clustering approach," in *Proceedings of the IEEE International Conference on Computer & Information Science (ICIS '12)*, vol. 1, pp. 403–408, Kuala Lumpur, Malaysia, June 2012.

- [24] Z. Tian, B. Wang, W. Zhang, J. Ye, and H. Zhang, "Network intrusion detection model based on context verification," *Journal of Computer Research and Development*, vol. 50, no. 3, pp. 498–508, 2013.
- [25] W. Zhang, Y. Zhang, and T.-H. Kim, "Detecting bad information in mobile wireless networks based on the wireless application protocol," *Computing*, vol. 96, no. 9, pp. 855–874, 2014.
- [26] G. Karypis and V. Kumar, "METIS—unstructured graph partitioning and sparse matrix ordering system," version 2.0., 1995.