Wireless Communications and Mobile Computing

Recent Advances in Security and Privacy Issues for Internet of Things Applications

Guest Editors: Ghufran Ahmed, Hasan Ali Khattak, Sarmadullah Khan, Abderrezak Rachedi, and Rafiullah Khan

Recent Advances in Security and Privacy Issues for Internet of Things Applications

Wireless Communications and Mobile Computing

Recent Advances in Security and Privacy Issues for Internet of Things Applications

Guest Editors: Ghufran Ahmed, Hasan Ali Khattak, Sarmadullah Khan, Abderrezak Rachedi, and Rafiullah Khan

Contents

Secure Green-Oriented Multiuser Scheduling for Wireless-Powered Internet of Things
Xiaohui Shang, Hao Yin, Aijun Liu, Mu Li, Yida Wang, and Yong Wang
Research Article (11 pages), Article ID 7845107, Volume 2020 (2020)

Design and Implementation of Directional Sensors for Privacy-Ensured Device-Free Target Localization in Indoor Environment
Ata ur Rehman, Zeeshan Ellahi, Asif Iqbal, Farman Ullah, Ahmed Ali, and Kyung Sup Kwak
Research Article (8 pages), Article ID 8391307, Volume 2019 (2019)

Policy-Based Security Management System for 5G Heterogeneous Networks
Hani Alquhayz, Nasser Alalwan, Ahmed Ibrahim Alzahrani, Ali H. Al-Bayatti, and Mhd Saeed Sharif
Research Article (14 pages), Article ID 4582391, Volume 2019 (2019)

Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 4127341, 1 page
https://doi.org/10.1155/2021/4127341

Erratum

Erratum to "Text Data Security and Privacy in the Internet of Things: Threats, Challenges, and Future Directions"

Umair Khadam,[1] Muhammad Munwar Iqbal,[1] Meshrif Alruily,[2] Mohammed A. Al Ghamdi,[3] Muhammad Ramzan,[4] and Sultan H. Almotiri[3]

[1]*Department of Computer Science, University of Engineering and Technology, Taxila 47050, Pakistan*
[2]*Faculty of Computer and Information Sciences, Jouf University, Sakaka City, Saudi Arabia*
[3]*Computer Science Department, Umm Al-Qura University, Makkah City, Saudi Arabia*
[4]*Department of Computer Science & IT, University of Sargodha, Sargodha, Pakistan*

Correspondence should be addressed to Muhammad Munwar Iqbal; munwariq@gmail.com

Received 19 May 2020; Accepted 28 May 2020; Published 5 March 2021

In the article titled "Text Data Security and Privacy in the Internet of Things: Threats, Challenges, and Future Directions" [1],

(i) Author Muhammad Ramzan was affiliated to Computer Science Department, Umm Al-Qura University, Makkah City, Saudi Arabia, which is incorrect. The correct affiliation for this author is

"Department of Computer Science & IT, University of Sargodha, Sargodha, Pakistan."

(ii) Author Sultan H. Almotiri was affiliated to Department of Computer Science & IT, University of Sargodha, Sargodha, Pakistan, which is incorrect. The correct affiliation for this author is

"Computer Science Department, Umm Al-Qura University, Makkah City, Saudi Arabia."

The corrected list of affiliations is shown in the author information above.

References

[1] U. Khadam, M. M. Iqbal, M. Alruily, M. A. Al Ghamdi, M. Ramzan, and S. H. Almotiri, "Text Data Security and Privacy in the Internet of Things: Threats, Challenges, and Future Directions," *Journal of Wireless Communications and Mobile Computing*, vol. 2020, article 7105625, pp. 1–15, 2020.

Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 2643546, 20 pages
https://doi.org/10.1155/2020/2643546

Review Article

Trust-Based Attack and Defense in Wireless Sensor Networks: A Survey

Weidong Fang,[1,2] **Wuxiong Zhang**,[1,2,3] **Wei Chen**,[4,5] **Tao Pan**,[6,7] **Yepeng Ni**,[8] **and Yinxuan Yang**[9]

[1]*Science and Technology on Microsystem Laboratory, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 201800, China*
[2]*University of Chinese Academy of Sciences, Beijing 100049, China*
[3]*Shanghai Research Center for Wireless Communication, Shanghai 201899, China*
[4]*School of Mechanical Electronic & Information Engineering, China University of Mining and Technology (Beijing), Beijing 100083, China*
[5]*School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, Jiangsu 221116, China*
[6]*Shenhua Information Technology Co., Ltd, Beijing 100011, China*
[7]*Fujian Provincial Key Laboratory of Information Processing and Intelligent Control (Minjiang University), Fuzhou 350121, China*
[8]*School of Data Science and Media Intelligence, Communication University of China, Beijing 100024, China*
[9]*Fuzhou Internet of Things Open Lab Co., Ltd, Fuzhou 350015, China*

Correspondence should be addressed to Wuxiong Zhang; wuxiong.zhang@mail.sim.ac.cn

Received 29 November 2019; Revised 2 August 2020; Accepted 18 August 2020; Published 10 September 2020

Academic Editor: Hasan Ali Khattak

As a key component of the information sensing and aggregating for big data, cloud computing, and Internet of Things (IoT), the information security in wireless sensor network (WSN) is critical. Due to constrained resources of sensor node, WSN is becoming a vulnerable target to many security attacks. Compared to external attacks, it is more difficult to defend against internal attacks. The former can be defended by using encryption and authentication schemes. However, this is invalid for the latter, which can obtain all keys of the network. The studies have proved that the trust management technology is one of effective approaches for detecting and defending against internal attacks. Hence, it is necessary to investigate and review the attack and defense with trust management. In this paper, the state-of-the-art trust management schemes are deeply investigated for WSN. Moreover, their advantages and disadvantages are symmetrically compared and analyzed in defending against internal attacks. The future directions of trust management are further provided. Finally, the conclusions and prospects are given.

1. Introduction

Currently, the standardization works for Narrowband Internet of Things (NB-IoT) have been completed; the wireless sensor network (WSN) is taken as an important component for sensing and aggregating information. As the tentacles of social networks [1–4], the WSNs, which provide sensed information in context-aware and personalized social applications, have been widely deployed in many fields, such as smart cities, intelligent transportation, intelligent connected vehicles, precision agriculture, and environmental monitoring. Meanwhile, there are many research hotspots, including routing and access protocols, image recognition and target tracking, trusted transmission and trust management scheme [5], and energy consumption balance and energy efficiency. However, the information security is of mutual concern. In this regard, scholars focus on ensuring that sensed data is transmitted by the effective security schemes (e.g., secure routing protocol [6], security data fusion [7], and secure network coding [8]), to deliver to the end user in secure. The requirements for social network are shown in literatures [9–12]; the tasks and functions of WSN can be performed

accurately and in real time, even though the network is being attacked by adversary.

Currently, the information security in WSNs is facing the enormous challenge, which comes from the security attacks including external attacks and internal attacks. The traditional security schemes (e.g., encryption [13] and authentication [14]) can only defend against the external attacks instead of the internal attacks. There are a few of studies demonstrate the trust management scheme is one of effective approaches to detect and defend against the internal attacks [15].

Trust management originated from sociology. In WSNs, in order to establish a secure communication link, it is necessary to guarantee that the intermediate nodes forwarding data packets are trusted in the network. Hence, it is essential to establish an effective trust model. In a trust model, each sensor node is allowed to evaluate the trustworthiness of neighbor nodes by interaction between nodes. Moreover, based on trust model, a trust management system is constructed to mitigate or defend against internal attacks, which are launched by captured or compromised nodes. In addition, trust management schemes are also used to evaluate the quality of received information, provide network security services including access control and malicious node detection, and secure resource sharing.

The research on trust management technology in WSNs is a challenging direction. How to construct a trust model is a key issue. By investigating and analyzing a large quantity of related literatures, these scholars mainly focus on two aspects: one is how to detect and defend against internal attacks, and the other is to obtain the trustworthiness of neighbor node to make decisions (e.g., selecting the next hop in secure and achieving the secure aggregation). Compared with the latter, we argue the former is more important.

Considering the above requirements and facilitating the research on attack and defense in the near future, in this paper, the trust management system and the typical internal attacks in WSNs are overviewed and investigated in Section 2. Furthermore, the state-of-the-art trust management schemes and trust models are deeply surveyed in Section 3. The detection and defense against security attacks with trust are comprehensively compared and analyzed in Section 4. Then, some valuable future research directions for trust management in WSNs are suggested in Section 5. Finally, the conclusions are drawn in Section 6.

2. Trust Management System and Internal Attack

In this section, the trust management system (TMS) is overviewed, and the internal attacks in WSNs are investigated.

2.1. Trust Management System. In general, there are five interrelated components in trust management system, including collecting, storing, modelling, transferring, and decision-making.

2.1.1. Collecting. It refers to collecting the trust elements, which involve the status of nodes' interaction, location information, and sensed data. The reputation of the nodes is evaluated based on these collected trust elements. The trust value is further calculated from them. Therefore, the trust value becomes more accurately with more sufficient collected trust elements.

2.1.2. Storing. It refers storing trust element, trust values, and reputation. The storage must be systematically considered due to constrained resources for sensor nodes. Firstly, memory spaces would be impacted by the storage type of the sensed data. For instance, a float number consumes more memory than an integer. Secondly, the storage time of information would be considered; those outdated information should be emptied in time to save space. Finally, the location used to store information would be also concerned. In a clustered WSN, the trust value can be stored in the cluster head. When a cluster member needs to use the trust value, the cluster head may transfer it to this member.

2.1.3. Modelling. It refers to modelling the trust and reputation in WSNs, which is the key component of TMS. How to model needs to consider many factors, including the aging of trust value, whether to use indirect information, the weight of indirect information, the weight of each trust element, and the countermeasures aimed at defending against different attacks. In addition, the computational capabilities and energy supply of sensor nodes, and different network topologies must also be considered. Generally, the reputation model is a probabilistic statistical model, which is typical based on the beta distribution, the Gaussian distribution, or the binomial distribution.

2.1.4. Transferring. It involves reputation transfer and trust transfer between two nodes. The reputation transfer usually refers to when a node i need to evaluate the reputation of a node j, it initiates the reputation request to these common nodes ($m1$, $m2$, $m3$, and $m4$) between nodes i and j, and then they provide the reputation response of node j to node i. The process of reputation transfer is shown in Figure 1. The trust transfer is the Certificate Authority (CA) of the network provides the third-party trust value to the node, in order to complete the trust evaluation. For a hierarchical WSN, the CA is the cluster head, and the Base Station (BS) is CA in planar WSNs.

2.1.5. Decision-Making. Based on calculated trust value, the trust decisions should be made. Currently, decision-making with trust is divided into two categories as follows: (1) defending against the internal attacks: this is to punish a node with a low trust value. It is to directly drag it into the blacklist to exclude the network forever or make the node regain the trust based on the consideration of the selfish node and the energy consumption and (2) selecting the next hop in secure: in short, the trade-off between the security and performance should be comprehensively considered for the resource-constrained sensor nodes.

2.2. Typical Internal Attacks. The internal attacks are launched by the compromised or captured nodes. The attack behaviors involve discarding, replaying, tampering, and forging data packets, as well as providing the fake routing

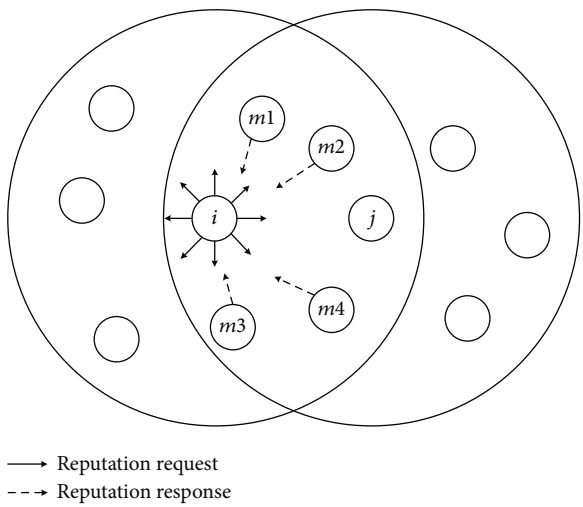


Figure 1: Process of reputation transfer.

information. Since these malicious nodes have obtained the transmission schemes and held the key of the network, the internal attacks are more dangerous, and traditional encryption and other security mechanisms have no effect.

The typical internal attacks in WSNs are investigated and presented as follows: denial of service attack (DoS attack) [16], bad-mouthing attack [17]/slander attack [18], on-off attack [19], garnished attack [20], reputation time-varying attack [21], sleeper attack [22], conflicting behavior attack [23], Sybil attack [24], node replication attack [25], selfish attack [26], flooding attack [27], selective forwarding attack [28], black hole attack [29], ballot stuffing attack [30], collusion attack [31], sinkhole attack [32], data forgery attack [33], etc.

In the next sections, current researches on trust management scheme/trust model will be reviewed, and the capabilities defending against internal attacks with trust will be compared and analyzed.

3. Related Works

Currently, the research on the trust management mainly focuses on several aspects containing trust model, trust management scheme, and protocol optimization in WSNs (shown in Figure 2).

3.1. Trust Model. The trust model provides a framework for establishing and managing trust relationships between two nodes and ensures that the legal nodes can be trusted to participate in the process of information transmission.

Ganeriwal and Srivastava proposed a framework, which was based on RFSN (Reputation-based Framework for high integrity Sensor Networks) [34]. The framework consisted of five components including direct reputation evaluation, indirect reputation evaluation, reputation synthesis, reputation transfer and nodes' behavior trust. Two important units in this framework were watchdog and reputation systems. The watchdog was used to monitor the behaviors of the neighbor nodes, especially to detect invalid information generated by abnormal nodes. It further classified these behaviors into cooperative or noncooperative behaviors. The reputation system was responsible for maintaining, managing, and updating the nodes' reputation, in order to calculate the trust value. The reputation was generated by the observation of watchdog or integration according to other available information. For obtaining more objective trust value, the historical behaviors $R_{i,j}$of sensor nodes were considered to calculate the current trust value. Therefore, based on a given reputation (node i to node j), the trust value $T_{i,j}$ can be generated as follows:

$$T_{\mathrm{i,j}} = E\alpha\left[R_{\mathrm{i,j}}\right] = E\left[beta\left(\alpha_{\mathrm{j}}, \beta_{\mathrm{j}}\right)\right] = \frac{\alpha_{\mathrm{j}}}{\alpha_{\mathrm{j}} + \beta_{\mathrm{j}}}, \quad (1)$$

where α_{j} and β_{j} represented the cooperative and the noncooperative numbers of node j for node i. If the trust value was lower than a set threshold value, the node j would be taken as abnormal, otherwise normal. RFSN provided a scalable scheme to detect the abnormal behaviors caused by malicious and erroneous nodes. Moreover, by introducing the aging factor, the historical behaviors were taken into the trust evaluation. Furthermore, based on RFSN, they also proposed a Beta Reputation System for Sensor Networks (BRSN) by using Bayesian networks. In BRSN, the feasibility of the beta distribution of node reputation was verified in the derivation process, and the calculation of reputation updating, aging, indirect information, and trust value and the updating and sintering the reputation were provided in detail. However, although the positive reputation information in RFSN was only transferred to mitigate the risk attacked by malicious nodes, the efficiency of the system was influenced inevitably. In addition, RFSN could not support the mobility of the nodes, and BRSN could not defend against the internal attacks with a high-reputation malicious nodes.

Yang et al. analyzed the impact on high-reputation malicious nodes and proposed a Multiple Attacks & Three Party-BRSN model (MA&TP-BRSN) [35] to improve BRSN. The proposed model was constructed by two components: one is MA-BRSN trust value calculation approach to solve the single detecting and evaluating attack issue in the existing reputation systems to a certain extent, and the other was TP-BRSN, which made the updating calculation of the third-party indirect reputation more objective, in order to achieve the defense against the internal attacks of the high-reputation malicious nodes. Yin et al. proposed an Improved BRSN (IBRSN) [36] for identifying the malicious recommendation and defending against the slander attack of high-reputation nodes. They introduced the indirect reputation of third-party nodes into IBRSN to eliminate the defects in BRSN to a certain extent. Jiang et al. proposed an Effective Distributed Trust Model (EDTM) for WSN [37]. The EDTM was composed of three parts as follows: direct trust, recommended trust and indirect trust, and the direct trust and the recommendation trust were calculated selectively according to the number of received packets. In EDTM, when calculating direct trust, the communication trust, energy trust, and data trust were considered simultaneously and the

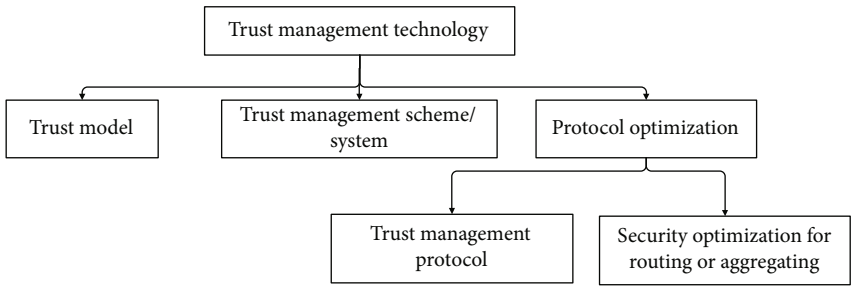


Figure 2: Classification of trust management.

trustworthiness and familiarity were defined to improve the accuracy of the recommendation trust simultaneously. The trust value was calculated more comprehensively, the reputation of the sensor node was evaluated more accurately, and the malicious nodes were effectively prevented from destroying the network security in this model. However, the weights of various trusts needed to be further researched, and the threshold selection was a challenge.

In addition, some scholars also improved BRSN. Zhang et al. introduced the analysis of the social network relevance into the trust model based on BRSN and proposed the Sensor Node Trust Update Algorithm (SNTUA) [38] by using the "social network relevance". In SNTUA, the reputations of nodes and their neighbors were further modified and comprehensively evaluated to improve the detection rate of malicious behaviors and reduce the impact of malicious nodes on WSN. Zhou and Shao proposed an improved trust evaluation model for WSN (referred to as ZHOU) [39] after the analysis of BRSN, based on Bayesian and entropy. In ZHOU, they considered the abnormal behavior brought by nonintrusive factors and introduced anomalous attenuation factor. Moreover, they used the modified Bayesian equation to estimate direct trust, updated it with sliding window and adaptive forgetting factor, and determined whether it was sufficiently reliable according to the level of direct trust as comprehensive trust. In this model, network energy consumption and the impact of malicious feedback were reduced. If a direct trust was not sufficiently trusted, indirect trust was calculated to obtain comprehensive trust. The entropy was used to assign weights to different recommendations. It could overcome the limitations brought about by subjectively deployed weights, in order to enhance the adaptability of the model simultaneously.

Chen et al. proposed an Agent-based Trust model for Sensor Network (ATSN) [40]. In ATSN, an agent node used the promiscuous mode to observe the behaviors of sensor nodes, which were divided into good behaviors and bad behaviors. Furthermore, the agent node calculated all good behaviors which were represented as p and bad behaviors which were represented as n separately; the reputation space was defined as follows:

$$RS = \{\langle p, n\rangle \mid p, n \geq 0\,; t = p + n\}. \tag{2}$$

The trust domain was defined as $TS = \{(pt, nt, ut)\}$, where pt, nt, and ut represented the positive trust, negative trust, and uncertainty, respectively. In ATSN, the storage space and computational complexity could be minimized for the common sensor nodes. The trust value of the nodes was calculated to mitigate the slander attacks and on-off attacks by using the reputation of the direct neighbor node. However, the behaviors of neighboring nodes were difficult to be completely recorded, due to the data packet loss caused by the frequent communication or the hardware failure of cheap nodes. Hence, this would cause the trust and reputation system uncertainty. The security of ATSN relied heavily on the agent node, and the assumption that the agent node could defend against any security threat had no practical meaning. In addition, ATSN did not solve the issues of the updating trust and reputation.

Sinha and Jagannatham proposed a Gaussian-based trust and reputation management system for fading MIMO (Multiple-Input Multiple-Output) WSN [41]. Based on multivariate Gaussian distribution and Bayes' theorem, the system considered the impact on MIMO wireless fading channels. Combining with direct and indirect reputation information, the reputation and trust value in this system were calculated, in order to effectively isolate malicious nodes. However, the calculation process was too complex to be suitable for resource-constrained sensor nodes. In addition, Zhang et al. proposed a dynamic trust establishment and management framework for clustered WSN [42]. They considered and introduced some new impact factors (such as nodes only communication with cluster head and using only the used cluster head reputation), by which made the system more secure.

Chen proposed a Task-based Trust framework for Sensor Networks (TTSN) [43], in which sensor nodes held the reputation of neighbor nodes with several different tasks to evaluate their trust. In TTSN, the trust was established by the task and trust management module, which consisted of three units: monitoring unit, reputation processing unit, and task and trust processing unit. The calculating trust approach referred to RFSN, and each sensor node had several trust values. Relatively speaking, TTSN was more suitable for the applications of large-scale WSN.

Zhu et al. proposed a Rank-based Application-driven Resilient Reputation framework Model (RARRM) in WSNs [44]. In RARRM, based on the driving of application program, the different ranks of trust values depended on different requirements.

Feng et al. proposed the Node Behavioral strategies Banding belief theory of the Trust Evaluation algorithm (NBBTE) [45], which was based on the behavioral strategy binding D-S (Dempster-Shafer) evidence theory. In this model, the sensed area with constrained resource was divided into few logical grids, and each grid was categorized with a unique identification. Then, the sensor nodes deployed in each grid verified location information of their neighbor nodes by using ECHO protocol. Each node further cross-checked the redundant sensed information of neighbors, and evaluated the trustworthiness of neighbors to detect the inconsistent data from malicious nodes. Finally, in the sink node, the sensed data from their grids could be aggregated and transmitted, and the inconsistent data from malicious nodes could be excluded simultaneously.

Hur et al. proposed a trust evaluation model to distinguish forged data of iIllegal nodes, so named DFDI [46]. In this model, the sensed domain with constrained resource was divided into few logical grids, and each grid was categorized with a unique identification. Furthermore, the ECHO protocol was used to verify the location information of the neighbors by deploying the sensor nodes in each grid. The sensor nodes cross-checked the redundant sensed information of neighbors and evaluated the reputation of neighbors based on their own checked results. The trust value was obtained by a weighted summation of the following three parameters: the consistency of the sensed information, the capability of communication, and the remaining duration of the node. At the sink node, the inconsistent data from malicious or compromised nodes could be detected by the transmitted aggregation result of each grid.

Fang et al. researched and found on-off attacks had greater concealment and aggression. Due to dynamically adjusting the reputation value, this attack was difficult to detect. Hence, a trust model based on a beta distribution that could defend against this attack was proposed (abbreviation: FANG) [47]. The different decision approach was adopted under the beta distribution. When the change of the trust value exceeded the set threshold, it indicated that the compromised node was launching the on-off attack. The scheme was easy to implement on resource-constrained sensor nodes. In addition, considering that the behaviors of the reputation time-varying attack were similar to the impact of the mobile obstacle on the wireless signal transmission, they proposed a Time-window-based Resilient Trust Management Scheme (TRTMS) [21]. They further analyzed the behavior of normal/nodes and compromised nodes over a certain time interval and identified the abnormal trust values by the trend analysis. Simultaneously, they introduced control factors and time windows to detect and remove the compromised node that launched the reputation time-varying attack from the suspected malicious nodes. The decision-making process is shown in Equations (3) and (4).

$$N_R = \begin{cases} N_R + 1, & \text{if } \Delta T_{n-1} > 0 \text{ and } \Delta T_n \leq 0 \text{ and } \Delta T_{n+1} < 0, \\ N_R, & \text{else}, \end{cases} \tag{3}$$

$$T_c = \begin{cases} T(n), & N_R < \tau, \\ 0, & N_R \geq \tau, \end{cases} \tag{4}$$

where $N_R$was the reversed number of the trust difference and$\Delta T$was the change trend of trust. The misjudgments caused by the moving obstacles were solved by the TRTMS scheme effectively.

Xiao et al. researched the problem of Determining Faulty Readings (DFR) [48] and argued that arbitrary and noisy readings were fault readings. Furthermore, based on network correlation, they constructed the similarity between two sensor readings by exploring the correlation of sensor readings and then modelled it into a graph $G = (V, E)$, where V represented the sensor network, and E represented the correlation between two nodes. If two neighbor nodes did not have any similarity in readings, then the two nodes were not directly connected. Once a similarity of the network was established, it was easy to infer the similarity between two sensor nodes. In addition, a correlation-based sensor rating scheme could be established by exploring the Markov chain in the network, where the sensor rating represented the reputation of the sensor node. They also proposed an effective intranetwork voting algorithm with trust to detect the fault readings based on sensor ratings. Although simply filtering and discarding abnormal readings might reduce the monitoring accuracy of the important events, it could be effectively avoided when using sensor rating scheme to detect the fault readings.

Inconsistent, unusual, or erroneous readings were usually caused by two different reasons, which include intentional misconduct and unintentional error. The former was mostly caused by malicious nodes, and the latter was caused by hardware failure or interference. The DFR-based approach focused on detecting the fault readings instead of processing them. In order to evaluate the reputation of sensor data properly, Gomez et al. proposed a new Mechanisms based on Data Life Cycle (MDLC) [49], which had three sensor data states: (1) unprocessed, (2) routed, and (3) processed. The data was sensed by the node without any additional routing or processing, and it was considered unprocessed. When the sensor data was transmitted to another node, it was taken as routed. Processed state referred to the fact that the sensed data was filtered, converged, or aggregated. In the mechanism, the trusts of unprocessed, routed, and processed data were calculated based on subjective logic.

Since the establishment processes of most trust models were only based on the interaction of neighbor nodes, this required a very important premise, that is, the sensed data was normal and the energy was evenly consumed. Once the sensed data and energy had a trust risk, a malicious, selfish, or low-competitive node that appeared in a WSN would result in a trusted node that was no longer trusted. To address the issue, Xiao et al. proposed a Trust Model based on Communication trust, Energy trust and Data trust (TMCED) [48] model. In this model, communication trust referred to the relationship value calculated by two cooperative nodes, and this calculation was derived from the successful interaction ratio. Energy trust referred to the remaining energy of a node, whether or not it was

sufficient to complete new communication and data processing tasks. It was calculated by

$$T_d = W_1 T_f + W_2 T_u + W_3 T_v, \tag{5}$$

where T_f, T_u, and T_v were the node fault-tolerant trust value, the trust value of event report, and the data consistency trust value, respectively. By using energy trust, TMCDE could effectively detect the DoS attacks. Once a malicious node launched a DoS attack, it would consume more energy, and the energy trust became lower than normal nodes. Hence, malicious nodes with lower energy trust would be more easily detected.

Nie proposed a Trust model of Dynamic optimization based on entropy method (Trust-Doe) [50], which used Entropy theory to determine the node weights in each group. The standard deviation of Group Local Evaluation (GLE) was then calculated to reflect the overall expectations of all nodes in the group, as well as the Standard Deviation of Local Evaluation (SDL).

$$\frac{\mathrm{GLE}(\mathrm{t}, \rho) = \sum_{\mathrm{j}=1}^{\mathrm{m}_\rho} \mathrm{R_j}(\mathrm{t}) \times \mathrm{W}_\rho(\mathrm{t})}{\mathrm{m}_\rho},$$

$$SDL(\mathrm{t}, \rho) = \sqrt{\frac{1}{\mathrm{m}_\rho - 1} \sum_{k=1}^{N} \left(z_{ik}^*(t) - z_{jk}^*(t) \right)^2}, \quad i \neq j, \tag{6}$$

where $\mathrm{W}_\rho(t)$ was the weight vector under the group ρ and was determined according to the entropy size corresponding to the trust matrix element Z_{ij} of a group. Comparing SDL with GLE of a node, if a SDL was larger than GLE of the group to be δ $(0 \leq \delta \leq 0.5)$ times, it was divided into higher trust value packets; on the contrary, if SDL value was lower than the trust value of each node in a group, and the node was considered a malicious node. Although the model improved the detection capability of abnormal nodes, it did not consider the energy consumption.

Wu and Li established a Multi-domain Trust Management Model (MdTMM) [51] by using the classical interaction number as a mathematical model. This model was usually applied to a hierarchical RFID (Radio Frequency Identification) system. In the model, each RFID reader was taken as a sensor node, and each tag was equivalent to a data carrier. Each domain had a CA to authenticate the readers in its domain, monitor the current events, and detect the abnormal nodes. The D-S evidence theory and time windows were used to rank trust values, in order to effectively defend against information-based attacks including tampering attacks, replay attacks, and forgery attacks.

Gilbert et al. proposed a Time Series Trust Model (TSTM) [52] based on Toeplitz matrix and Trust based Auto Regressive (TAR) process, which was based on data prediction, and the effects of aggregation and reconstruction of Compressed Sensing (CS) were verified by various performance indicators and different attack models. Li et al. designed the Intrusion Sensitivity-based Trust Management Model (ISTMM) [53], which used machine learning technology to automatically assign intrusion sensitivity based on expert knowledge. The performance of three different supervised classifiers in assigning sensitivity values was compared during the evaluation process.

Considering the existing universal trust model was difficult to meet the requirements of multihop routing, Liu et al. proposed a Trust Model based on Bayes Theorem (TMBBT) [54] for the multiple paths in WSNs. In this model, all nodes were divided into two categories: ones were the nodes communicated with other nodes only via one-hop routing; the others were not only communicated via one-hop routing but also via multihop routing for one-hop unreachable. The trust evaluation consisted of two parts: communication trust and data trust. Communication trust was calculated based on cooperative routing information. The reputation and trust of the data depended on the ratio of data successfully received. This was due to the fact there were only direct communication and data instead of indirect communication and data; it could reduce the energy consumption. However, the calculations of trust value were not accurate enough without neighbors' recommendations. In addition, how to combine communication trust with data trust was not mentioned in this article.

Zhang et al. proposed a novel scheme to detect the malicious node based on DPAM-MD (Density-based Partitioning Around Medoids-Malicious node Detection) algorithm [55]. In this scheme, a subaggressive node could be detected by combining Manhattan metrics and DPAM (Density-based Partitioning Around Medoids) algorithm on the basis of the traditional reputation threshold judgment model. Moreover, combining the intercluster with intracluster distance equalization objective functions, a novel density-based clustering algorithm was proposed to classify all nodes. It could effectively shorten the clustering time and improve the efficiency detected malicious node, especially for those obvious compromised nodes. Zeng et al. proposed a Gray Markov-based Model to improve BRSN (GMM-BRSN) [56] and then designed a query routing protocol to address the issue of Selective forwarding attack in the routing protocol on the basis of GMM-BRSN. The GMM-BRSN had higher security and lower energy consumption.

Atakli et al. proposed a Weighted-Trust Evaluation (WTE) scheme [57] for hierarchical WSN to detect malicious nodes. In WTE, the weighted trust was calculated as follows:

$$W_n = \begin{cases} W_n - \theta \times r_n, & \text{if}(U_n \neq E), \\ W_n, & otherwise, \end{cases} \tag{7}$$

where U_n was the sensing data of the evaluated node, E was the aggregated data of cluster head, and θ was the penalty ratio. $r_n = m/s$, where m was the number of nodes that produces inconsistent data and s was the total number of nodes under the cluster head. This scheme had higher security, when there were a small number of compromised nodes in the network; however, when more than a quarter of the nodes were compromised, the performance was unsatisfactory.

Mahmud et al. used an Adaptive Neural-Fuzzy Inference System (ANFIS) and brain-inspired trust management

model (TMM) to enhance the security of IoT devices and relay nodes [58]. The TMM could detect the malicious nodes in the network and utilize both node behavioral trust and data trust to evaluate the nodes trustworthiness. Chen et al. proposed [59] a trust evaluation model, which directs data trust compared real-time monitoring data with historical data. If the value was large, it was considered an abnormal node.

Karthik and Ananthanarayana [60] focused on data trust model, which was called as KARTHIK, especially data fault detection, reconstruction, and quality estimation for reliable event detection involved with Temporal, Spatial, and Attribute data modelling. The correlation of data in multiple dimensions including time and space was calculated to find faulty data. In terms of data trust, the calculation of coefficients was mapped to three integers of -1, 0, and +1, which represented data errors, uncertainty, and complete trust. Liu and Cheng proposed [61] a state space modelling approach for trust evaluation that employs a state space model for time series analysis. This model was named LIU-CHENG by us. The trustworthiness of each node was modelled by a trust index; under the state, it formed a vector. Then, based on improved particle filter, the high-dimensional spatial trust value was calculated to better detect erroneous data. A certain amount of storage spaces and computational capabilities were required both in time and space. Singh and Verma presented a trust model for Flying Ad hoc networks (FANET). We called this model as KULDEEP [62], which consisted of QoS (Quality of Service) trust and social trust, which synthesized trust values through fuzzy logical classification and weight assignment. The features of node contained signal strength, packet delivery ratio, node's energy, and transmission delay, were calculated by percentage. The trust value calculation of the model involved all aspects of transmission to the path consumption and could provide protection against most internal attacks while ensuring network load balancing.

Ghugar et al. proposed a protocol Layer trust-Based Intrusion Detection System (LB-IDS) to secure WSN by detecting the attackers at different layers [63]. The trust value of a node was calculated by using the deviation of trust metrics at each layer with respect to the attacks. They also considered trustworthiness in PHY layer trust, media access control (MAC) layer trust, and network layer trust. Finally, the overall trust value of a node was estimated by combining the individual trust values of each layer. By applying the trust threshold, a sensor node was determined as trusted or malicious. The proposed system could defend against jamming attack at the physical layer, back-off manipulation attack at the MAC layer, and sinkhole attack at the network layer.

Zhao et al. proposed an Exponential-based Trust and Reputation Evaluation System (ETRES) to evaluate the trust and reputation of a node in WSNs [64]. ETRES was used to observe the nodes' behavior, and exponential distribution was applied to represent the distribution of nodes' trust. The trust of the node was used to look for reliable nodes to transmit data and weaken malicious attacks in WSNs. More significantly, the entropy theory was used to measure the uncertainty of direct trust values. Indirect trust was introduced to strengthen interaction information when the uncertainty of direct trust is enough high. In addition, the confidence factor was redefined, which could dynamically adjust the node trust value to weaken the harmful effects of the compromised nodes.

In ETRES, the exponential distribution was applied to represent the distribution of the reputation of a nodes, and the node's behaviours were used to calculate the trust value, which involved the direct trust value and the indirect trust value. More significantly, the entropy theory was introduced to measure the uncertainty of direct trust values. The indirect trust value was adopted to strengthen the certainty of the trust value, when the uncertainty of direct trust was enough high. In addition, a confidence factor was redefined to dynamically adjust the trust value of a node, in order to weaken the harmful effects of the compromised nodes. The ETRES was used to look for secure relay nodes to forward data and prevent the malicious attacks in WSNs.

3.2. Trust Management System/Scheme. Since trust management scheme in WSNs was limited by hardware resources of sensor node, more behavior-based trust management schemes were adopted. These schemes were suitable for addressing the distributed authorization issues, and they had the advantages of flexibility and scalability.

Zhou et al. proposed a a trust and reputation management scheme for cluster-based WSN. [65]. In this scheme, the cluster head elected a node as a Surveillance Node (SN), which monitored the behaviors of cluster member nodes, calculated their reputation and trust, and evaluated their trustworthiness. The cluster head used this information to obtain the trust value of each node, in order to defend against attacks. In addition, a sensor node with higher trust value had a great opportunity to become a SN, thus enhancing the security of this cluster.

Boukerche et al. proposed an Agent-based Trust and Reputation Management scheme (ATRM) for wireless sensor nodes [66]. In ATRM, the trust and reputation were managed by minimized additional messages and time latency, and the trust and reputation information of the node were required to store as t-instrument and r-certificate. Since a node could not manage and calculate its own trust and reputation, each node was also required to have the ability to manage the trust and reputation of its host nodes. Moreover, any transaction was defined as an interaction between two nodes (requestor and provider). It was triggered by the requester, and then the provider chose to accept or reject. Before any interaction, the requester directly queried the local mobile agent to obtain the provider's r-certificate. Depending on the provider's certificate, the requester decided whether to start the interaction. When the interaction was complete, the requestor evaluated the provider's trust based on QoS obtained in the interaction and submitted the evaluation to the local mobile agent, which then generated a t-instrument provider accordingly and sent the t-instrument to the provider's local mobile agent. Based on the t-instrument collected, the mobile agent periodically released the r-certificate updated by its managed nodes. The advantage of ATRM was that there was no need to

centrally store trust and reputation, and the nodes provided their own reputation information when it needed. However, the establishment of ATRM required extraordinary assumptions. It assumed that the mobile agent was resilient to any threat, and the mobile agent was resilient to malicious nodes, which tried to steal or modify the information that the agent carried. The feasibility of these assumptions needs further research.

Yao et al. proposed a Parameterized and Localized trust management Scheme (PLUS) [67]. In PLUS, each sensor node held highly abstract parameters to evaluate the trustworthiness of the interested neighbor nodes, in order to detect the malicious nodes. Specifically, the direct trustworthiness of a node was calculated by the availability of the node and the proportion of the correct grouping. The indirect trustworthiness was calculated based on the neighboring signal value and the number of neighbors. The direct and indirect trustworthiness were synthesized according to different weights, in order to obtain the total trustworthiness. The PLUS was further used to design a routing scheme, named PLUS_R. In PLUS_R, all important control packets generated by the Base Station must contain a Hash Sequence Number (HSN), so that effectively guaranteed their integrity. However, the HSN increased the packet length and the energy consumption of transmission. Since the integrity of a packet was always checked, if checked fails, regardless of whether this packet was maliciously modified by the node, the trust value of this node would be reduced. Thereby, a normal node might be unfairly penalized.

Shaikh et al. proposed a Group-Based Trust Management Scheme (GTMS) [68], which obtained a single trust value in the whole group. In GTMS, the trust value was calculated based on direct and indirect observations. The direct observations referred to successful and unsuccessful interactions, and indirect observations indicated the recommendations of trusted nodes with respect to particular nodes. The interaction referred to the cooperation of two nodes. When a node successfully received a packet, it would send back an ACK to the transmitter. If the transmitting node did not receive the ACK within a predefined threshold time, the data packet would be retransmitted. If the receiving node did not receive the retransmission of the packet within the threshold time of its neighbor node or found that the eavesdropping packet was illegally manufactured, the transmitting node would consider the interaction unsuccessful. If the number of unsuccessful interactions increased, the transmitting node reduced the trust value of the neighboring node and treated it as a malicious node. Compared with the traditional trust management scheme, GTMS focused on the trust value of a set of sensor nodes, rather than always focusing on the trust value of each node. GTMS not only provided a detection scheme for malicious nodes but also provided a certain degree of prevention scheme. Although GTMS took energy consumption into account, reduced the computing and communications expenditure of trust evaluation. However, it relied on a broadcast-based policy to collect many feedbacks, which in turn consumed additional resources and energy at another communication level.

He et al. proposed an attack-Resistant and lightweight Trust management scheme (ReTrust) [69]. In this scheme, a two-layer architecture was composed of the master node and sensor node, and the master node of each cell would manage the trust records of other master nodes and sensor nodes in this cell. Two network topologies were used, which involved an intracell topology and intercell topology. The former managed trust records for sensor nodes in this cell based on past direct interactions, and the latter managed the trust records of other master nodes through direct historical observations, recommendations, and indirect interactions. In addition, an aging parameter was also introduced, which assigned different aging factors to each historical moment in the evaluation window. ReTrust was lightweight and did not add any additional expenditure on resource-constrained sensor nodes; the trust calculation of the master node was simple. ReTrust could not only effectively identify malicious behaviors and eliminate malicious/fault nodes but also significantly improve network performance. However, the drawback of ReTrust was that the master node must have abundant storage resources and energy. Sensor nodes with limited resources did not have the ability to manage trust records of other nodes.

Yu et al. summarized Trust and Reputation Management (TRM) system in wireless communication systems [70]. They divided the existing TRM systems into two categories: the individual-level trust model and the system-level trust model. The individual-level trust model focused on the trust evaluation from one node to another. The system-level trust model included trust and reputation evaluation model and protocol. In TRM systems, by using an examples of the individual-level trust model, they provided the trust and reputation of the initial phase, evaluated the reputation of the synthesized the direct and indirect reputation, and guided the trust evaluation and decision-making. In addition, the rewards and punishments in the system were based on the trustworthiness of nodes; several reward and punishment schemes for the system-level trust model were given. Duan et al. proposed an energy-aware trust derivation scheme with the game theory [71]. They analyzed the requirements of the network security and introduced the Trust Derivation Dilemma Game (TDDG) to design a risk model, in order to get the optimal number of collaboration nodes by encouraging the cooperation between nodes. The game theory was also used for trust derivation, which reduced the calculation cost. Li et al. proposed a Lightweight and Dependable Trust System (LDTS) for clustered WSN [20]. In LDTS, they proposed a lightweight trust decision-making scheme based on the node identity of a clustering WSN, to improve the system efficiency and reduce the harm of malicious nodes by eliminating the interactive feedback between cluster members and cluster heads. Since the cluster heads undertook many important tasks of data forwarding, they defined the trust evaluation method for the interaction between the cluster heads and the adaptive weighting approach. In addition, considering that the traditional entity based trust evaluation scheme was not suitable for the data-centric sensor network, Li et al. proposed a Data-centric Trust for Sensor Network (DTSN) scheme [72]. Simultaneously, a new approach,

Proof-of-Reputation-Relevance (PoRR), was presented to realize DTSN. Zia and Islam proposed a trust scheme based on Communal Reputation and Individual Trust (CRIT) [73]. In this scheme, the behavior of the nodes was monitored by watchdog, and each node held a trust and reputation table for evaluating its neighbors. Fang et al. proposed a multifactor reputation management scheme[74], The multifactor involved event perception, packet forwarding, and data aggregation. The proposed scheme could be used to SPIN protocol to improve the data forwarding rate and delivery success rate in distrusted environment.

Fang et al. proposed a beta distribution-based Trust and Reputation Evaluation System (BTRES) for WSN [75] to address the security issue, which was vulnerable to be attacked from compromised nodes. Based on the interaction information between the nodes, in BTRES, the beta distribution was used to emulate the reputation of nodes, and the trust value was further calculated to obtain. In addition, weights and thresholds were used in combination to construct BTRES. The simulation results had shown that BTRES could effectively defend against the internal attacks and enhance the network security. The trust value of the node in BTRES could be used for the routing protocol or the aggregation scheme. When selecting routing or aggregating information, the node with the current high trust value was firstly selected, so as to ensure the security of information forwarding and transmission. Furthermore, they proposed a Binomial-Based Trust Management System (BTMS) [76] for WSN. The BTMS could only transfer the positive reputation between nodes, so as to mitigate the slander attacks.

Srinivasan et al. proposed a Distributed Reputation-based Beacon Trust System (DRBTS) [77]to detect and remove malicious beacon nodes provided incorrect location information. In DRBTS, the beacon nodes could be monitored each other, and the relevant information was provided for sensor node to select the competition trust. Every beacon node would monitor its neighbor nodes, observe them whether cheated, and update corresponding beacon node reputation in neighbor reputation list. After the error of indirect information of the beacon node was detected, the reputation of the neighbor node could be updated by using it. A sensor node deployed the neighbor node reputation list to decide whether used beacon position information based on simple majority vote scheme. In DRBTS, an undirected graph was built by using a network model, to synthesize the direct information and indirect information into the trust.

Karthik and Ananthanarayana proposed a Hybrid Trust Management Scheme (HTMS) for WSN [78]. In HTMS, it assumed that the network needed to evaluate the degree of trustworthiness of the nodes when it made decisions. Moreover, all trust score was obtained based on the trust component. Therefore, the data quality and transmission trust were considered. By detecting data errors with time-space correlation, the transmission trust and original data were used to estimate the trust score of the intermediate node and information trust score. And then the data trust score was used to make decisions. The direct trust was calculated based on the number of successful interactions. The data trust depended on whether the acquired sensory data was within the predictable scope, and mapped it as three integers: +1, -1, and 0. In addition, they also considered the residual energy level of the node and the uncertainty of the data. The correlation coefficient of the neighbor nodes was calculated by the association between node data in time-space and used as a positive correlation indicator for data trust. By using HTMS, some internal attacks including DoS attacks, bad-mouthing attacks, on-off attacks, attack on information, selective forwarding attacks, replication attacks, Sybil attacks, and collusion attacks were detected and defended against effectively. By setting a certain reward and punishment system, a reliable node and its source node were increased or decreased, and the trust score of the intermediate node could effectively detect those malicious, error, and selfish nodes.

Singh et al. propose a Light Weight Trust Scheme (LWTM) for clustered WSN [79]. In LWTM, each node would monitor the neighbor nodes. The monitoring events divided into two categories: success and failure. If the result of the monitoring event was a predictable result, then the event was taken as a successful interaction. Different from LDTS, the data package, control packet, and their message precision were included in trust measurement for LWTM. All calculation matrix dimensions were based on multiple neighbors of a node. Furthermore, they also considered the positive and negative feedbacks. It could defend against bad-mouthing attack to a certain extent and also consider the energy consumption of the node. However, most of the trust values were deduced based on the form of $(S_{xy} + U_{xy})/(1 + S_{xy} + U_{xy})$ as well as the traditional aging factor. It updated the trust value at different time. Although this scheme could defend against some internal attacks, including bad-mouthing attack and black hole attack in a certain extent, there was a lack of response speed to the attack.

Talbi et al. proposed an Adaptive and dual Data-Communication Trust scheme (ADCT) [80]. In a hierarchical network, a new communication trust T was defined according to the classic interaction number calculation equation:

$$P = \frac{S(t)}{S(t) + U(t)},$$

$$T = \left\lceil 10 \times P^{(1-p)\alpha} \right\rceil, \tag{8}$$

where $S(t)$, $U(t)$, and P represented successful and unsuccessful communications in the time period (t), and the percentage of succeeding corresponding, respectively; $\lceil . \rceil$ represented the integer function latest; $a \geq 2$ was the parameter which affects the order of severity of trust function. The data trust feedback T_{ch} was built as follows:

$$T_{ch} = \left\lceil 10 \times \frac{P_{recommendations} + 1}{P_{recommendations} + N_{recommendations} + 2} \right\rceil. \tag{9}$$

$P_{recommendations}$ and $N_{recommendations}$ represented positive and negative data trust recommendations, respectively.

In ADCT, the duality data communication was used to deal with the unreliable recommendation, in order to establish the feedback from a cluster member to the cluster head. Therefore, it could prevent the recommendation of a harmful node and reduce the communication energy consumption. However, they made the decision without considering the dynamic cluster group (unset boundary) and united node energy level.

Reddy et al. used the D-S evidence theory to propose a communication and data trust for WSN (TWSN) [81]. In this scheme, the direct trust was set up on the number of forwarded packets (p_t) and the number of packet loss (q_t) in a certain moment of a node. Specifically, they compared the relevant Forwarding Ratio (FR) $FR(t) = (p_t)/(p_t + q)$ in a certain moment with last moment, calculated the fluctuation of node forwarding consistency, and dealt with it by penalty factor or excitation factor. Based on the root mean square error, the similarity parameter was customized to correct the recommendation. Among them, the indirect trust weighted and summed multiple recommendations by using the evidence theory and the similarity parameters. Data trust was calculated based on the mean of the sensor data. Moreover, based on the comparison of the size of the sensor values, controlling data trust was increased and decreased by generating two factors after comparing the sizes. This scheme could be done without increasing the time window to realize better control effect of trust value. Combining the screening for recommendations, it could defend against the bad-mouthing attacks and on-off attacks to a certain extent.

Jin et al. proposed the Multi-agent trust-based intrusion detection scheme (Multi-agent) [82]. In this scheme, the data trust included four dimensions (packet loss rate, packet transmission frequency, packet receiver frequency, and energy consumption rate) and considered the speed of energy consumption. Therefore, a more energy-intensive attack such as DoS attacks or flood attacks could be detected by using this scheme.

Firoozi et al. [83] proposed a trust scheme in hierarchical networks, in which the cells were divided evenly by grid in plane space, and the data in a cell were processed. The cell distance and number of nonempty cells were defined for processing. And special situations were taken into consideration in CoSLIP, namely, an SL- (subjective logic-) based in-network data processing scheme for collocated WSNs. Combined with trust management, Janani and Manikandan proposed a secure PKI (Public Key Infrastructure) system [84] called as JANANI. By evaluating the hybrid trust value with the trust evaluation vector method, this scheme was effectively integrated into the hexagonal clusters to secure the PKI framework and detects and classified the misbehaviors, either selfishness or malicious, to take revocation actions on those nodes.

Meng et al. deployed a trust management application into [85] IoT in hierarchical networks; k paths were generated and the cuckoo search algorithm was used to find the optimal path. Combined with the Bayesian based on wireless traffic sampling, it could reduce the excessive data input of IoT devices to defend against black hole attacks and selective forwarding attacks. Sahoo et al. put forward a trust management focus on penalty and reward policy, named RASHMI [86]. Calculating the current time window to set dynamic parameters, RASHMI could defend against reputation time-varying attacks, especially on-off attacks. In RASHMI, the nodes were divided into benevolent/legitimate nodes, persistent malicious nodes, and transient malicious nodes. Then, the direct trust value was calculated using sliding time windows, fractions, and weighted summation root mean squares. Mathematically, size of dynamic timing sliding window was defined as ON period. As for reward and penalty schemes, $(S_{i,j(tk)})/(1 + S_{i,j(tk)})$ signified the reward factor; $(U_{i,j(tk)})^{-1/2}$ signified the punishment factor. Combined with the time window and reward penalty scheme, it could well control the trend of trust value and better detect and discover reputation time-varying attacks. The downside was that the recommendation for trust values and the fusion was weak, and the resistance to similar bad-mouthing attacks was weak.

Khan put the trust management scheme into practice in IoT, namely, called ZEESHAN [87]. In ZEESHAN, the beta distribution was used to calculate the trust value. Combined with the energy-limited IoT device, three different packet forwarding scheme algorithms were set to reduce the corresponding node energy consumption NLDF (no listening for data forwarding), LDF (listen own data forwarding), or LT (listen to all transmissions).

Yang et al. put a novel application into Vehicular Networks [88] blend with blockchain. We called this scheme as YANG. This application inherited the decentralization and tamper resistance of blockchain. All nodes or RSUs (RoadSide Units) collaboratively maintained an updated, reliable, and consistent trust blockchain, so that this system could resist message spoofing attacks, bad-mouthing attacks, and ballot stuffing attacks. Excessive computational capabilities, storage spaces, and energy resources were often required to send encrypted data and calculate hash values. Therefore, the application was limited to RSUs and deployed vehicle network scenarios with sufficient resources. Whether it was an internal attack or an external attack, the combination of blockchain and trust management made the trust management system more secure and reliable.

Smithamol and Rajeswari proposed a trust management middleware (TMM) [89], which applied in service selection in the cloud. The criteria of trust evaluation included CPU percentage, disk read throughput, disk write throughput, and network bandwidth, after the service filtering and selecting, and then through the OTA (Overall Trust Algorithm) with dynamic weight to calculate the overall trust value. This system could defend against the internal attacks including the QoS attacks and bad-mouthing attacks.

Pham and Yeo presented a trust management system that context-aware trust management scheme [90], which was named THI-CHAI. In this scheme, the nodes could be allowed to evaluate the trustworthiness of receiving events by considering the entity reputations of the senders under the vehicle networks. First, it utilized BF-based PSI to enable a node A to recognize the node B trust level. With a decision tree that estimates the entity trust adaptively to the available link ability information with encryption technology, which

means this system can resist the data-relevant attack, such as tampering attack.

For detecting on-off attack in health WSNs, Fang et al. proposed a Binomial Distribution-based Trust Management Scheme (BDTMS) [91]. Firstly, time interval between the highest trust value $(T_h(i))$ and the next highest trust value $(T_h(i+1))$ as a detection period $(P(i))$ was defined. There was the lowest trust value $(T_l(i))$ in a detection period, and this moment represents TIM. Secondly, then presented a descent time $(t_d(i))$, which was a time interval from $T_h(i)$ to $T_l(i)$, as well as an ascent time $(t_a(i))$ from $T_l(i)$ to $T_h(i+1)$. Finally, they gave any trust value $(T_d(i,m))$ during a descent time and any trust value $(T_a(i,n))$ during a descent time. If the following relationship was satisfied, the malicious node that launched the on-off attack can be basically detected. In Equation (10), F_d was the detection flag. If F_d was 0, the detected node was malicious; otherwise, it was a normal nodeFor malicious nodes, they would be remove from the routing table to achieve the defense against On-Off attack.

$$F_D = \begin{cases} 0, \text{ if } |t_d(i) - t_a(i)| < \delta, \\ \left(\begin{array}{c} T_d(i,m) > \dfrac{T_h(i) - T_l(i)}{td(i)} \\ T_a(i,n) < \dfrac{T_h(i+1) - T_l(i)}{t_a(i)} \end{array} \right), \\ \left(\text{or} \displaystyle\sum_{k=0}^{\min\,(t_d(i)-t_a(i))} (T_a(i, TIM+k) - T_d(i, TIM-k)) < \sigma, \right) \\ 1, \qquad \textit{otherwise}. \end{cases} \tag{10}$$

In addition, Ukil proposed a collaborating computing model based on trust and reputationto detect and prevent the malicious attack.[92]; this approach realized the choice of an optimal path, and enhanced the reliability.Ishmanov and Kim proposed a secure trust evaluation scheme to limit the increase in the trust value of malicious nodes for WSN [93]. Different from traditional trust management scheme, the proposedscheme was considered as the influence of abnormal node behaviors.

3.3. Protocol Optimization. Generally speaking, the protocol optimization referred to design the trust management protocol, in order to implement interaction with trust management related information. On the other hand, it referred to security optimization for routing protocols, transmission protocols, and data aggregation protocol by using the trust decision.

Bao et al. proposed a trust-based intrusion detection and Hierarchical Trust Management Protocol (HTMP) [94] in WSNs. The scheme was suitable for the routing protocol based on trust of intrusion detection. Furthermore, they analyzed the different influence on the choice of the minimum trust threshold value.

Gheorghe et al. proposed an Adaptive Trust Management Protocol (ATMP) [95], which was based on the behaviors of nodes to adjust the trust and reputation value. It included three phases: learning phase, exchange phase, and update phase. Learning phase got through the experience received from TinyAFD (Tiny Attack and Fault Detection framework) and judged the node's behavior that was good or bad. Exchange phase was the empirical interaction between two neighbor nodes. Update phase was used to update the reputation and trust value with experience. The adaptivity of ATMP was from experience, and it adjusted reputation and trust value according to the behavior of the sensor node in each cycle. ATMP was interoperability, which embodied in proceeding exchange of respective behavior in exchange phase. Due to the adaptivity and interoperability of ATMP, it could defend against the internal attacks preferably. Tajeddine et al. propose CENtralized Trust-Based Efficient Routing protocol (CENTER) [96]. CENTER took advantage of the information provided from BS, to detect and forbid the badness node which hampers or abuses network function. In CENTER, the BS collected the observed information of every node, and after several observations and calculations, a more accurate global network map was obtained. Furthermore, the BS estimated its service life on account of the condition of node activity, computing node behavior message (malicious, collaborate, compatibility), evaluating the trust value of every node (data trust and transmit trust), and took advantage of effective decision-making system to isolate malicious node of the network.

Priayoheswari et al. proposed a topology management route based on trust [97]. They used the Received Signal Strength Indicator (RSSI) as a characteristic parameter to join the calculation of trust value, in order to estimate the topology of WSN. This protocol could detect the behavior of abnormal node effectively. Mehetre et al. aimed at the internal attack of cluster WSN, used two-stage security scheme and dual assurance scheme, and proposed Trustable and Secure Routing Scheme (TSRS) [98]. Based on initiative trust, TSRS achieved to guarantee route protocol, to defend against a few internal attacks, such as black hole attacks and selective forwarding attacks. By using trust and cuckoo search algorithm to recognize trusted path, this scheme could combine energy selection and provide a secure route path. The scheme also offered the guarantee to prolong the network lifetime.

Chen et al. proposed the Peer-to-Peer (P2P) trust management protocol based on the elliptic curve [99]. This protocol provided the function of authentication and signature to protect the process of the trust value queries and rating reports. Furthermore, the protocol also generated two verified pseudonyms to take the place of node identity, of which one pseudonym was used for events and another pseudonym was used for the peer establishment procedure. Addo et al. proposed a Secure, Private and Trustworthy Protocol (SPTP) [100] to solve the issues of the security, privacy, and trust with mobile and cloud services in a Collective Intelligence (CI) scenario. Shilpa and Ambareesh proposed a trust management protocol in WSNs [101]. The protocol consisted of four parts: trust constitute, trust aggregation, trust formation, and application-level trust optimization design. It combined QoS trust with social trust to obtain a composite trust metric. In addition, the protocol allowed setting best trust in the trust aggregation process, to make subjective trust close to

objective trust in the individual's trust attribute, and realized the minimum of trust deviation.

For trusted routing protocol, ahhal et al. proposed Trust-based Cross-Layer Model (TCLM) [102], which used the concept of cross layer (ACK from data link layer and TCP layer) to design a trust-based model for sensor networks, in order to isolate malicious nodes. Among them, data-packet statistics could be used to calculate values related to neighbor nodes, namely, trust value (denoted as t) and treatment ratio (denoted as r). The trust value characterized the degree of belief that neighboring nodes were reliable relative to packet delivery. The treatment ratio represented the statistical confidence in this trust. Let L be the accumulation of packets forwarded by a sensor node and N for the cumulative total of packets forwarded by the sensor node. Trust (t) and treatment ratio (r) are defined as follows:

$$t = \frac{L}{N}, \quad r = 1 - \frac{\sqrt{12L(N-L)}}{(N+1)N^2}. \tag{11}$$

Wang et al. created an Energy-efficient Trust Routing Mechanism named ETMRM [103]. They firstly extended the sensor flow tables to realize a lightweight trust monitoring and evaluation scheme at the node level, and detected and isolated the malicious nodes based on the trust information collected from sensor nodes. Under this message scheme, neighbor nodes' report messages were aggregated and reported to reduce the size of the packets and the times of forwarding, so that to save energy and ensure the transmission of control traffic.

In addition, Gerrigagoitia et al. proposed a reputation-based intrusion detection system for WSN [104], which analyzed and ensures the source of malicious attacks by using the trust values of different nodes. Ukil proposed a computational approach based on trust and reputation cooperation in WSNs [105], which effectively eliminated malicious nodes with high probability. They found secure forwarding paths among routes, so the approach had good trustworthiness and communication efficiency.

The trust theory originated from sociology. Generally, trust was considered a dependency. Interdependence meant that an interaction relationship existed in two parties. Regardless of the interacted content, it meant that the two parties have at least a certain degree of benefits, and their own benefits to be achieved must rely on the other party [106]. In a distributed network system, trust was defined as a subjective judgment of honesty, security, and trustworthiness, which made by an entity to another entity through observation and historical experience over a given period of time and context. Briefly, trust was a security scheme to defend against internal attacks and realize network self-healing. In WSNs, trust usually refers to predicting the creditability of future behavior of a node. The operation and acquisition of the trust value could only be obtained from sensing data directly, or the recommendation of the neighboring node, which generally changed with the behavior of the node. The trust value was usually used to determine whether the information was interacted between nodes. Moreover, the computational complexity of trust management in WSNs was related to many aspects, which involved different reputation distributions, node behavior trust/data trust, the coupling of direct trust and indirect trust of attack characteristics model, timeliness of trust information, and openness of wireless channels.

4. Security Analysis of Trust Management Technology

The research on the trust management is to detect malicious nodes and defend against internal attacks, in order to enhance the network security. For example, if a malicious node does not forward the received information, the trust value will decrease. The malicious node can be discovered in time by detecting the trust value. In this section, the capabilities of typical trust management schemes/models for defending against internal attacks are listed and analyzed as shown in Table 1.

The typical schemes for detecting and defending against the internal attacks with trust are summarized as follows:

Denial of service attack: after analysis, the power-aware trust model can effectively defend against DoS attacks (such as TMCED and DFDI); however, other trust management approaches based on event reporting will be affected by DoS attacks.

Bad-mouthing attack/slander attack: when defending against this attack, evaluation nodes can dynamically adjust the weight synthesized by indirect reputation according to the trust degree of neighbor nodes to mitigate the harm of slander attacks. Therefore, if the trust scheme only transmits positive information from other nodes, it can effectively defend against such attacks. In addition, the trust approach based on direct neighbor node trust perception or the scheme of multiple behavior observation aggregations is better able to defend against the slander attack. Moreover, GTMS, ReTust, TDDG, LDTS, BTRES, BTMS, CRIT, HTMP, and so on can also defend against this attack.

Ballot stuffing attack: the confederate node of the malicious node improves reputation node by providing a large amount of successful interaction information to the other party. It is necessary to reduce the weight of the indirect trust value provided by the neighbor node in order to deal with such attacks. RFSN and ReTrust can defend against such attacks because of indirect trust values account for a small proportion in them.

Collusion attack: the attack requires more than one malicious node to cooperate, in order to provide the normal node wrong recommended value. Collusion attacks are more destructive, such as RFSN and GTMS can defend against the attack. In general, the trust model based on the direct observation of each node is not easily affected by collusion attacks. However, all of the other approaches of trust calculation are seriously jeopardized by collusion attacks. In defending against collusion attacks, nodes can set a threshold to filter out the indirect evaluation that is too different from direct evaluation to defend against collusion attacks.

Table 1: Defending against internal attack capability with trust management technology.

(a)

Internal attacks	Trust management schemes											
	ADCT	ANFIS-TMM	ATSN	BDTMS	BTMS	BTRES	CRIT	DFDI	DFR	EDTM	ETMRM	FANG
Bad-mouthing attack (slander attack)	√	√	√	√	√	√	√	√	×	√	-	×
Ballot stuffing attack	-	×	-	-	-	-	×	×	-	-	-	×
Black hole attack	√	√	-	×	×	-	-	√	×	-	√	-
Collusion attack	√	√	-	×	+	+	-	-	×	×	×	-
Conflicting behavior attack	×	-	√	×	×	-	√	√	×	-	×	×
Data forgery attack	×	-	×	×	-	√	×	√	√	√	-	×
Denial of service attack	×	-	×	×	-	√	-	√	×	√	×	×
Garnished attack	×	×	×	√	×	-	×	-	-	-	×	√
Node replication attack	×	-	-	√	×	-	×	√	×	-	×	-
On-off attack	×	×	√	√	×	√	√	√	×	√	×	√
Reputation time-varying attack	×	×	×	√	×	-	-	×	-	-	-	-
Selective forwarding attack	√	√	-	×	√	√	-	√	√	√	-	-
Selfish attack	-	-	×	×	√	-	×	×	-	-	√	×
Sinkhole attack	×	√	-	×	√	-	-	√	×	-	√	×
Sleeper attack	×	×	×	×	-	-	×	×	×	×	-	-
Sybil attack	×	√	-	-	√	-	×	√	×	-	×	×

Note: For ease of reference, the names of internal attacks and typical trust management techniques (abbreviations) in this table are arranged in ascending order of their initials. "√" indicates that the trust management scheme can defend against such internal attacks. "+" indicates that the trust management scheme can mitigate the harm of internal attacks or can only detect such internal attacks. "-" indicates that the defense ability of the trust management scheme against the internal attacks is unknown. "×" indicates that the trust management scheme cannot defend against the internal attacks.

(b)

Internal attacks	Trust management schemes											
	GMM-BRSN	GTMS	HTCW	HTMP	HTMS	ISTMM	JANANI	KARTHIK	KULDEEP	LIU-CHENG	LDTS	LWTM
Bad-mouthing attack (slander attack)	-	√	×	√	√	×	×	√	√	-	√	√
Ballot stuffing attack	-	-	×	×	-	×	-	×	×	×	×	-
Black hole attack	×	-	×	×	-	×	√	-	√	√	×	√
Collusion attack	-	-	×	×	-	×	×	-	√	×	×	×
Conflicting behavior attack	×	×	×	-	√	×	-	√	×	-	-	×
Data forgery attack	-	-	√	×	√	×	-	-	-	√	×	×
Denial of service attack	√	×	×	-	√	√	-	×	×	-	-	×
Garnished attack	-	×	×	-	×	×	-	×	×	×	√	×
Node replication attack	×	√	×	×	×	√	-	-	×	×	×	×
On-off attack	-	×	×	-	√	×	×	-	×	×	×	√
Reputation time-varying attack	×	×	×	×	×	×	×	×	×	×	-	×
Selective forwarding attack	√	√	√	-	√	×	√	×	√	√	×	×
Selfish attack	-	-	-	-	√	×	×	×	×	-	-	-
Sinkhole attack	×	√	-	√	-	×	√	-	√	-	×	×
Sleeper attack	×	-	-	×	×	×	-	-	×	-	×	×

Table 1: Continued.

Internal attacks	Trust management schemes											
	GMM-BRSN	GTMS	HTCW	HTMP	HTMS	ISTMM	JANANI	KARTHIK	KULDEEP	LIU-CHENG	LDTS	LWTM
Sybil attack	×	√	√	×	×	√	√	×	√	×	×	×

(c)

Internal attacks	Trust management schemes											
	MdTMM	Multi-agent	NBBTE	PLUS	RARRM	RASHMI	ReTrust	RFSN (BRSN)	SNTUA	TDDG	THI-CHAI	TMBBT
Bad-mouthing attack (slander attack)	×	×	×	×	√	√	√	√	√	√	-	√
Ballot stuffing attack	×	×	-	-	-	×	×	√	-	-	×	×
Black hole attack	×	-	-	-	×	-	×	-	-	×	×	-
Collusion attack	×	×	×	-	-	×	×	√	×	×	×	-
Conflicting behavior attack	×	×	×	×	√	×	-	×	-	×	-	√
Data forgery attack	√	×	-	-	-	×	×	×	-	-	√	√
Denial of service attack	×	√	×	×	×	×	-	×	-	×	×	-
Garnished attack	×	×	√	√	×	×	√	-	-	×	-	×
Node replication attack	×	×	-	×	×	×	-	×	-	×	-	√
On-off attack	√	×	√	√	+	√	√	×	×	×	-	×
Reputation time-varying attack	×	×	×	-	×	√	×	-	-	-	-	-
Selective forwarding attack	×	√	×	-	×	√	×	-	-	-	√	√
Selfish attack	×	×	-	×	-	-	×	-	×	√	×	-
Sinkhole attack	×	√	-	×	×	×	-	-	-	×	-	-
Sleeper attack	×	×	×	-	-	×	×	√	-	-	×	×
Sybil attack	×	×	×	×	×	×	×	×	×	-	-	×

(d)

Internal attacks	Trust management schemes											
	TMCED	TMM	TP-BRSN	TRTMS	TRUST-DOE	TSRS	TSTM	TTSN	TWSN	YANG	ZEESHAN	ZHOU
Bad-mouthing attack (slander attack)	√	√	√	-	-	×	√	√	√	√	√	-
Ballot stuffing attack	×	-	×	-	×	×	×	-	×	√	×	×
Black hole attack	-	-	√	×	×	√	×	×	-	×	√	×
Collusion attack	-	-	×	×	√	×	×	×	√	×	√	×
Conflicting behavior attack	√	×	-	×	×	×	×	√	×	-	×	-
Data forgery attack	-	-	-	×	-	×	√	×	√	×	-	√
Denial of service attack	√	×	√	×	×	×	√	-	×	-	-	×
Garnished attack	×	×	×	√	×	×	×	-	×	-	×	-
Node replication attack	-	×	√	×	×	×	√	×	×	×	-	×
On-off attack	-	√	-	√	×	×	×	√	√	√	×	-
Reputation time-varying attack	×	-	×	√	×	×	×	-	-	-	×	-
Selective forwarding attack	×	-	√	×	×	√	×	×	√	×	√	√
Selfish attack	×	-	√	×	×	-	×	×	-	×	×	×
Sinkhole attack	-	-	-	×	×	×	×	×	×	×	√	√

Table 1: Continued.

Internal attacks	Trust management schemes											
	TMCED	TMM	TP-BRSN	TRTMS	TRUST-DOE	TSRS	TSTM	TTSN	TWSN	YANG	ZEESHAN	ZHOU
Sleeper attack	-	-	-	×	×	×	×	×	×	×	×	×
Sybil attack	×	×	×	-	×	×	-	-	×	-	√	-

Sleeper attack: malicious nodes that act accurately in a certain period create a good reputation for themselves, and then be misbehaving. The aging scheme was introduced effectively to defend against such attacks in RFSN.

On-off attack: in on-off attack, malicious nodes perform sometimes well and sometimes poorly. Malicious nodes can maintain trust values even when they perform poorly. In order to cope with switching attacks, behavioral observations long ago cannot have the same aging weight as recent behavioral observations. Therefore, it can effectively defend against the on-off attack by using the trust approach of the forgetting factor. In this approach, the aging weight of behavioral observations long ago is lighter than the recent behavioral observations. In addition, it can also only use the current behavior observation to calculate the trust of the sensing node to defend against switching attacks. Therefore, TRTMS, FANG, PLUS, ReTrust, CRIT, and so on can effectively defend against the on-off attack.

Selfish attack: the self-node will simply delete the request and will not reserve the resource to send the trust reply after receiving the trust request. TDDG and others can effectively ensure network security through management technology increasing trust value.

Garnished attack and reputation time-varying attack: the behavior of a malicious node may be good or bad; the purpose is to remain undiscovered and cause damage. For example, when they accumulate a high degree of reputation, malicious nodes may attack suddenly. For garnished attacks, LDTS can defend against it, and for reputation time-varying attacks, TRTMS can effectively defend against it.

Sybil attack: ID authentication and centralized trust model are the good approaches to defend against Sybil attack, which can effectively identify the node and can also detect multiple false identities of the malicious node through the network sink node/BS.

Conflict behavior attack: considering that malicious nodes display different characteristics for different nodes, like defending the slander attack, conflict behavior attacks can be defended by trust approaches based on direct neighbor sensing (such as ATSN and TTSN) or aggregate multifactor observations (such as DFDI, TMBBT, and CTRT).

Information attacks such as selective forwarding attack and data forgery attacks: it is possible to obtain error information through the trust model just based on communication behavior, which makes the evaluation of reputation untrustworthy, and trust models or trust management schemes that effectively monitor all data forwarding and data integrity can defend against those attacks well.

Sinkhole attack: the attacker sets up a false aggregation node so that all information in the area "flows" to the false sink node. HTMP can defend against this attack.

Node replication attack: since the security credentials of the replicated nodes are cloned from the captured nodes, these replicated nodes can all be considered legitimate members of the network. Similar to the malicious nodes that launching Sybil attack, this type of replication attack by malicious nodes can also manipulate recommendations and elevate themselves as trusted nodes. Therefore, node replication attacks can be defended by ID verification (such as DFDI) and centralized trust model (such as GTMS), and BS can detect false identity.

The trust management schemes are mainly used to defend against the internal attacks, and different schemes aim at different internal attacks based on the requirements of applications. In addition, the trust value can be taken as a tool to solve the security issues for routing protocol in WSNs, due to the lower computational overhead. For hierarchical WSN, the cluster head is generally considered security, and it acts as a CA to provide the secure third-party recommendation. This can achieve the real-time of trust management. In planar WSNs, the trust decision is made by the cooperation between few neighbor nodes. The latter is suitable for those applications that are not real-time.

5. Future Directions in Trust

With the development of WSN, more and more researchers are paying attention to the trust management and proposing many novel trust models, schemes, and algorithms for WSN. However, the state-of-the-art studies in the field are still in the preliminary stage. In this section, we envision few potential research opportunities in the field as follows.

5.1. Trust Management System Based on Energy Efficiency. The limitation of various resources, including energy supplement, computational capabilities, and storage spaces, is a critical feature of WSN. Among which, the restriction on energy is one of the most important factors that restrict large-scale and long-term deployment of WSN. However, the existing trust management systems tend to require larger computation and additional communication energy consumption emerging from the interaction of some trust parameters, which will inevitably affect the lifetime of the network. On the other hand, effective analytical scheme for energy efficiency is still a blank in existing trust management systems. Therefore, it is of great importance to further investigate the energy-efficient trust management system and establish analytical scheme of energy-efficient system that

owns a certain objective evaluation basis. Meanwhile, in the designing process of trust management system, considering fully energy consumption and optimizing trust evaluation scheme are needed in order to improve the performance of the system.

5.2. Risk Evaluation Scheme for Trust Management. It is suggested that the risk evaluation scheme should be introduced and combined with trust management to establish a risk evaluation scheme oriented to trust management. The WSN is highly application-oriented, and the demand for trust management differs according to the different applications. Risk and trust factors should be taken into account when making decisions in different application environments. For example, the risk of nodes is compromised is different in military and home; the threshold of trust value can be adjusted properly under different risk levels to make the trust management system more stable, practical, and flexible.

5.3. Multiobjective Joint Optimization Mechanism for Node Information Forwarding with Trust. Considering the node's trust value as a constraint condition, it is suggested that introduced it into the node information forwarding mechanism. For WSN, how to select the secure next hop is concerned with security, transmission, and energy consumption. Hence, through the analysis and evaluation of the multiobjective joint optimization method, a trade-off between the trust value, energy level, and transmission performance of neighbor nodes can be designed into a secure forwarding scheme for resource-constrained node. This is to defend against the internal attacks effectively and avoid deploying those high-strength encryption algorithms simultaneously.

Furthermore, the numerical size of trust value gradually becomes linguistic variable from a single decimal and then presents multidimensional matrix form. Apart from some specific dimensions, such as energy, which can be set artificially, other dimensions generally hazily input the unquantifiable dimensions through linguistic variables, such as outputting different grades of trust level through D-S theory. For data fusion in different dimensions, multidimension data was quantified by using multiple-input (including matrix form) single-output algorithms, such as the Analytic Hierarchy Process (AHP) and Gray Decision Model.

6. Conclusions

Although there have been many studies on trust, there is no concentrated research for WSNs. In this article, we systematically survey the research progress of the trust management processes and existing trust management in WSNs. Although trust management technology of traditional network is relatively mature, it cannot be directly applied to the resource-limited systems, such as WSN. Some existing trust management schemes in WSNs improve node security at the expense of other performances of the network, which may lead to the sacrifice of WSN lifetime.

Trust management in WSNs needs to meet the requirements as follows: WSN is a real-time network, so it must have low latency. The cost of memory, computing, and energy are expected to be minimized due to the limitations of sensor nodes' own conditions. Through the analysis of existing trust management technology, further research and optimization are needed into the trust management scheme/system of WSN with the help of traditional network trust management scheme combing with specific application scenarios, especially the changes of wireless channels, the impact on trust valuation, and decision-making are fully considered. In view of this, we will gradually introduce energy efficiency, risk evaluation, and note mobility, as constraints in future work, and carry out research on efficient management scheme based on trust management combined with energy efficiency.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (No. 51874300 and No. 61471346), the Shanxi Provincial People's Government Jointly Funded Project of China for Coal Base and Low Carbon (No. U1510115), the Shanghai Natural Science Foundation (No. 17ZR1429100), the Science and Technology Innovation Program of Shanghai (No. 17511105903), the Fundamental Research Funds for State Key Laboratory of Synthetical Automation for Process Industries (No. PAL-N201703), the Scientific Instrument Developing Project of the Chinese Academy of Sciences (No. YJKYYQ20170074), the Open Fund Project of Fujian Provincial Key Laboratory of Information Processing and Intelligent Control, Minjiang University (No. MJUKF-IPIC201905), and the National Key Research and Development Program of China—Internet of Things and Smart City Key Program (No. 2019YFB2101600, No. 2019YFB2101602, and No. 2019YFB2101602-03).

References

[1] J. Li, T. Cai, K. Deng, X. Wang, T. Sellis, and F. Xia, "Community-diversified influence maximization in social networks," *Information Systems*, vol. 92, p. 101522, 2020.

[2] Z. Ning, L. Liu, F. Xia, B. Jedari, I. Lee, and W. Zhang, "CAIS: a copy adjustable incentive scheme in community-based socially-aware networking," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 3406–3419, 2017.

[3] T. Cai, J. Li, A. S. Mian, R. Li, T. Sellis, and J. X. Yu, "Target-aware holistic influence maximization in spatial social networks," in *IEEE Transactions on Knowledge and Data Engineering*, 2020.

[4] X. Wang, Z. Ning, M. Zhou et al., "Privacy-preserving content dissemination for vehicular social networks: challenges and solutions," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 2, pp. 1314–1345, 2019.

[5] G. Mois, T. Sanislav, and S. C. Folea, "A cyber-physical system for environmental monitoring," *IEEE Transactions on Instrumentation and Measurement*, vol. 65, no. 6, pp. 1463–1471, 2016.

[6] H. Liang and W. Wu, "Secure link status routing protocol based on node trustworthiness," *Journal of Xidian University*, vol. 43, no. 5, pp. 121–127, 2016.

[7] W. Hao, L. Yu, M. Mingrui, and W. Ping, "Secure data fusion method based on supervisory mechanism for industrial Internet of things," *Chinese Journal of Scientific Instrument*, vol. 34, no. 4, pp. 817–824, 2015.

[8] W. D. Fang, L. H. Shan, G. Q. Jia, X. H. Ji, and S. J. Chen, "A low complexity secure network coding in wireless sensor network," *Journal of Internet Technology*, vol. 17, no. 5, pp. 905–913, 2016.

[9] N. A. Haldar, J. Li, M. Reynolds, T. Sellis, and J. X. Yu, "Location prediction in large-scale social networks: an in-depth benchmarking study," *VLDB Journal*, vol. 28, no. 5, pp. 623–648, 2019.

[10] Z. Ning, X. Hu, Z. Chen et al., "A cooperative quality aware service access system for social Internet of vehicles," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2506–2517, 2018.

[11] X. Wang, K. Deng, J. Li, J. X. Yu, C. S. Jensen, and X. Yang, "Efficient targeted influence minimization in big social networks," *World Wide Web*, vol. 23, no. 4, pp. 2323–2340, 2020.

[12] Z. Ning, F. Xia, X. Hu, Z. Chen, and M. S. Obaidat, "Social-oriented adaptive transmission in opportunistic Internet of smartphones," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 810–820, 2017.

[13] M. Zhang, M. Chen, D. He, and B. Yang, "An efficient leakage-resilient and CCA2-secure PKE system," *Chinese Journal of Computers*, vol. 39, no. 3, pp. 492–502, 2016.

[14] J. Xu, Q. Wen, and D. Wang, "A new message authentication code based on hash function and block cipher," *Chinese Journal of Computers*, vol. 38, no. 4, pp. 793–803, 2015.

[15] W. Fang, N. Cui, W. Chen, W. Zhang, and Y. Chen, "A trust-based security system for data collecting in smart city," *IEEE Transactions on Industrial Informatics*, p. 1, 2020.

[16] P. Gope, J. Lee, and T. Q. S. Quek, "Resilience of DoS attacks in designing anonymous user authentication protocol for wireless sensor networks," *IEEE Sensors Journal*, vol. 17, no. 2, pp. 498–503, 2017.

[17] U. Prathap, P. D. Shenoy, and K. R. Venugopal, "CMNTS: catching malicious nodes with trust support in wireless sensor networks," in *2016 IEEE Region 10 Symposium (TENSYMP)*, pp. 77–82, Bali, Indonesia, May 2016.

[18] P. B. B. Velloso, R. P. P. Laufer, O.-C. M. B. Duarte, and G. Pujolle, "A trust model robust to slander attacks in ad hoc networks," in *2008 Proceedings of 17th International Conference on Computer Communications and Networks*, pp. 1–6, St. Thomas, US Virgin Islands, USA, August 2008.

[19] Y. Chae, D. P. LC, and Y. L. Sun, "Trust management for defending on-off attacks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 1178–1191, 2015.

[20] X. Li, F. Zhou, and J. Du, "LDTS: a lightweight and dependable trust system for clustered wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 6, pp. 924–935, 2013.

[21] W. Fang, W. Zhang, Y. Yang, Y. Liu, and W. Chen, "A resilient trust management scheme for defending against reputation time-varying attacks based on beta distribution," *SCIENCE CHINA: Information Science*, vol. 60, no. 4, article 040305, 2017.

[22] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Transactions on Sensor Networks*, vol. 4, no. 3, pp. 1–37, 2008.

[23] X. Anita, M. A. Bhagyaveni, and J. M. L. Manickam, "Fuzzy-based trust prediction model for routing in WSN," *The Scientific World Journal*, vol. 2014, 11 pages, 2014.

[24] W. Dong and X. Liu, "Robust and secure time-synchronization against Sybil attacks for sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 6, pp. 1482–1491, 2015.

[25] C. M. Yu, Y. T. Tsou, C. S. Lu, and S. Y. Kuo, "Localized algorithms for detection of node replication attacks in mobile sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 5, pp. 754–768, 2013.

[26] S. Wagh, A. More, and A. Khavnekar, "Identification of selfish attack in cognitive radio ad-hoc networks," in *2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, pp. 1–4, Madurai, India, December 2015.

[27] H. Kim, R. Chitti, and J. Song, "Novel defense mechanism against data flooding attacks in wireless ad hoc networks," *IEEE Transactions on Consumer Electronics*, vol. 56, no. 2, pp. 579–582, 2010.

[28] D. Acharya, S. L. Agrwal, P. Sharma, and S. K. Gupta, "Performance analysis of detection technique for select forwarding attack on WSN," in *2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, pp. 581–584, Waknaghat, India, December 2016.

[29] G. Bendale and S. Shrivastava, "An improved blackhole attack detection and prevention method for wireless ad-hoc network," in *2016 International Conference on ICT in Business Industry & Government (ICTBIG)*, pp. 1–7, Indore, India, November 2016.

[30] C. Dellarocas, "Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior," in *2000 ACM Conference on Electronic Commerce*, pp. 150–157, Minneapolis, MN, USA, October 2000.

[31] M. Rezvani, A. Ignjatovic, E. Bertino, and S. Jha, "Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp. 98–110, 2015.

[32] G. Kalnoor and J. Agarkhed, "QoS based multipath routing for intrusion detection of sinkhole attack in wireless sensor networks," in *2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, pp. 1–6, Nagercoil, India, March 2016.

[33] Y.-S. Lee, E. Kim, Y.-S. Kim, H.-Y. Jeon, and M.-S. Jung, "A study on secure chip for message authentication between a smart meter and home appliances in smart grid," in *2013 International Conference on IT Convergence and Security (ICITCS)*, pp. 1–3, Macao, China, December 2013.

[34] S. Ganeriwal and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," in *the 2nd ACM workshop on Security of Ad hoc and sensor networks (SASN '04)*, pp. 66–77, Washington DC, USA, October 2004.

[35] G. Yang, G. S. Yin, W. Yang, and D. M. Zuo, "A reputation-based model for malicious node detection in WSN," *Journal of Harbin Institute of Technology*, vol. 10, pp. 158–162, 2009.

[36] G. Yin, G. Yang, Y. Wu, X. Yu, and D. Zuo, "A novel reputation model for malicious node detection in wireless sensor network," in *2008 4th International Conference on Wireless*

Communications, Networking and Mobile Computing, pp. 1–4, Dalian, China, October 2008.

[37] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, "An efficient distributed trust model for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 5, pp. 1228–1237, 2015.

[38] L. J. Zhang, X. Deng, L. Guo, J. P. Zhang, J. Yang, and H. B. Li, "Research on trust model based on social network correlation degree analysis in wireless sensor networks," *Journal of University of Electronic Science and Technology of China*, vol. 44, no. 1, pp. 106–111, 2015.

[39] Z. Zhou and N. Shao, "An improved trust evaluation model based on Bayesian for WSN," *Chinese Journal of Sensors and Actuators*, vol. 29, no. 6, pp. 927–933, 2016.

[40] H. Chen, H. Wu, X. Zhou, and C. Gao, "Agent-based trust model in wireless sensor networks," in *Eighth ACIS international conference on software engineering, artificial intelligence, networking, and parallel/distributed computing (SNPD 2007)*, pp. 119–124, Qingdao, China, August 2007.

[41] R. K. Sinha and A. K. Jagannatham, "Gaussian trust and reputation for fading MIMO wireless sensor networks," in *2014 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, pp. 1–6, Bangalore, India, January 2014.

[42] J. Zhang, R. Shankaran, M. A. Orgun, V. Varadharajan, and A. Sattar, "A dynamic trust establishment and management framework for wireless sensor networks," in *2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, pp. 484–491, Hong Kong, China, January 2010.

[43] H. Chen, "Task-based trust management for wireless sensor networks," *International Journal of Security and Its Applications*, vol. 3, no. 2, pp. 21–26, 2009.

[44] M. Zhu, H. Chen, and H. Wu, "A rank-based application-driven resilient reputation framework model for wireless sensor networks," in *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*, pp. V9-125–V9-129, Taiyuan, China, October 2010.

[45] R. Feng, X. Xu, X. Zhou, and J. Wan, "A trust evaluation algorithm for wireless sensor networks based on node behaviors and D–S evidence theory," *Sensors*, vol. 11, no. 2, pp. 1345–1360, 2011.

[46] J. Hur, Y. Lee, H. Yoon, D. Choi, and S. Jin, "Trust evaluation model for wireless sensor networks," in *The 7th International Conference on Advanced Communication Technology, 2005, ICACT 2005*, pp. 491–496, Phoenix Park, South Korea, February 2005.

[47] W. Fang, Z. Shi, L. Shan, F. Li, and X. Wang, "Trusted scheme for defending on-off attack based on BETA distribution," *Journal of System Simulation*, vol. 27, no. 11, pp. 2722–2728, 2015.

[48] X. Y. Xiao, W. C. Peng, C. C. Hung, and W. C. Lee, "Using sensor ranks for in-network detection of faulty readings in wireless sensor networks," in *the 6th ACM International Workshop on Data Engineering for Wireless and Mobile Access,*, pp. 1–8, Beijing,China, June 2007.

[49] L. Gomez, A. Laube, and A. Sorniotti, "Trustworthiness assessment of wireless sensor data for business applications," in *2009 International Conference on Advanced Information Networking and Applications*, pp. 355–362, May 2009, Bradford, UK.

[50] S. Nie, "A novel trust model of dynamic optimization based on entropy method in wireless sensor networks," *Cluster Computing*, vol. 22, no. S5, pp. 11153–11162, 2019.

[51] X. Wu and F. Li, "A multi-domain trust management model for supporting RFID applications of IoT," *PLoS One*, vol. 12, no. 7, article e0181124, 2017.

[52] E. P. K. Gilbert, B. Kaliaperumal, E. B. Rajsingh, and M. Lydia, "Trust based data prediction, aggregation and reconstruction using compressed sensing for clustered wireless sensor networks," *Computers and Electrical Engineering*, vol. 72, pp. 894–909, 2018.

[53] W. Li, W. Meng, L.-F. Kwok, and H. H. S. IP, "Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management mode," *Journal of Network and Computer Applications*, vol. 77, pp. 135–145, 2017.

[54] Z. Liu, Z. G. Zhang, S. S. Liu, Y. Q. Ke, and J. Chen, "A trust model based on Bayes theorem in WSN," in *2011 7th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1–4, Wuhan, China, September 2011.

[55] L. Zhang, N. Yin, and R. Wang, "Research of malicious nodes identification based on DPAM-DM algorithm for WSN," *Journal on Communications*, vol. 36, no. Z1, pp. 53–59, 2015.

[56] M. M. Zeng, H. Jiang, X. Wang, and W. Q. Liu, "Reputation evaluating model and security routing protocol of wireless sensor networks based on grey Markov model," *Application Research of Computers*, vol. 30, no. 12, pp. 3758–3766, 2013.

[57] I. M. Atakli, H. Hu, Y. Chen, W. S. Ku, and Z. Su, "Malicious node detection in wireless sensor networks using weighted trust evaluation," in *2008 Spring Simulation Multi-conference*, pp. 836–843, Ottawa, Canada, April 2008.

[58] M. Mahmud, M. S. Kaiser, M. M. Rahman et al., "A brain-inspired trust management model to assure security in a cloud based IoT framework for neuroscience applications," *Cognitive Computation*, vol. 10, no. 5, pp. 864–873, 2018.

[59] Z. Chen, L. Tian, and C. Lin, "Trust model of wireless sensor networks and its application in data fusion," *Sensors*, vol. 17, no. 4, 2017.

[60] N. Karthik and V. S. Ananthanarayana, "Data trust model for event detection in wireless sensor networks using data correlation techniques," in *2017 Fourth International Conference on Signal Processing, Communication and Networking (ICSCN)*, pp. 1–5, Chennai, India, March 2017.

[61] B. Liu and S. Cheng, "State space model-based trust evaluation over wireless sensor networks: an iterative particle filter approach," *The Journal of Engineering*, vol. 2017, no. 4, pp. 101–109, 2017.

[62] K. Singh and A. K. Verma, "A fuzzy-based trust model for flying ad hoc networks (FANETs)," *International Journal of Communication Systems*, vol. 3, 2018.

[63] U. Ghugar, J. Pradhan, S. K. Bhoi, and R. R. Sahoo, "LB-IDS: securing wireless sensor network using protocol layer trust-based intrusion detection system," *Journal of Computer Networks and Communications*, vol. 2019, 13 pages, 2019.

[64] J. Zhao, J. Huang, and N. Xiong, "An effective exponential-based trust and reputation evaluation system in wireless sensor networks," *IEEE Access*, vol. 7, pp. 33859–33869, 2019.

[65] Y. Zhou, T. Huang, and W. Wang, "A trust establishment scheme for cluster-based sensor networks," in *Proceedings of the 5th International Conference on Wireless Communications,*

Networking and Mobile Computing, pp. 1–4, Beijing, China, September 2009.

[66] A. Boukerche, X. Li, and K. el-Khatib, "Trust-based security for wireless ad hoc and sensor networks," *Computer Communications*, vol. 30, no. 11-12, pp. 2413–2427, 2007.

[67] Z. Yao, D. Kim, and Y. Doh, "PLUS: parameterized and localized trust management scheme for sensor networks security," in *Proceedings of IEEE International Conference on Mobile ad-hoc and Sensor Systems (MASS)*, pp. 437–446, Vancouver, BC, Canada, October 2008.

[68] R. A. Shaikh, H. Jameel, B. J. d'Auriol, Heejo Lee, Sungyoung Lee, and Young-Jae Song, "Group-based trust management scheme for clustered wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 11, pp. 1698–1712, 2009.

[69] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "ReTrust: attack-resistant and lightweight trust management for medical sensor networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 4, pp. 623–632, 2012.

[70] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," *Proceedings Of IEEE*, vol. 98, no. 10, pp. 1755–1772, 2010.

[71] J. Duan, D. Gao, D. Yang, C. H. Foh, and H. H. Chen, "An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 58–69, 2014.

[72] M. Li, J. Hu, and J. Du, "A data-centric trust evaluation mechanism in wireless sensor networks," in *2010 Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science*, pp. 466–470, Hong Kong, China, August 2010.

[73] T. A. Zia and M. Z. Islam, "Communal reputation and individual trust (CRIT) in wireless sensor networks," in *2010 International Conference on Availability, Reliability and Security*, pp. 347–352, Krakow, Poland, February 2010.

[74] F. Fang, J. Li, and J. Li, "A reputation management scheme based on multi-factor in WSN," in *Proceedings 2013 International Conference on Mechatronic Sciences, Electric Engineering and Computer (Mec)*, pp. 3843–3848, Shengyang, China, December 2013.

[75] W. Fang, C. Zhang, Z. Shi, Q. Zhao, and L. Shan, "BTRES: beta-based trust and reputation evaluation system for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 59, no. 1, pp. 88–94, 2016.

[76] W. Fang, X. Zhang, Z. Shi, Y. Sun, and L. Shan, "Binomial-based trust management system in wireless sensor networks," *Chinese Journal of Sensors and Actuators*, vol. 28, no. 5, pp. 703–708, 2015.

[77] A. Srinivasan, J. Teitelbaum, and J. Wu, "DRBTS: distributed reputation-based beacon trust system," in *Proceeding of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC)*, pp. 277–283, Indianapolis, IN, USA, September 2006.

[78] N. Karthik and V. Ananthanarayana, "A hybrid trust management scheme for wireless sensor networks," *Wireless Personal Communications*, vol. 97, no. 4, pp. 5137–5170, 2017.

[79] M. Singh, A. R. Sardar, K. Majumder, and S. K. Sarkar, "A lightweight trust mechanism and overhead analysis for clustered WSN," *IETE Journal of Research*, vol. 63, no. 3, pp. 1–12, 2017.

[80] S. Talbi, M. Koudil, A. Bouabdallah, and K. Benatchba, "Adaptive and dual data-communication trust scheme for clustered wireless sensor networks," *Telecommunication Systems*, vol. 65, no. 4, pp. 605–619, 2017.

[81] V. B. Reddy, S. Venkataraman, and A. Negi, "Communication and data trust for wireless sensor networks using D–S theory," *IEEE Sensors Journal*, vol. 17, no. 12, pp. 3921–3929, 2017.

[82] X. Jin, J. Liang, W. Tong, L. Lu, and Z. Li, "Multi-agent trust-based intrusion detection scheme for wireless sensor networks," *Computers and Electrical Engineering*, vol. 59, pp. 262–273, 2017.

[83] F. Firoozi, V. I. Zadorozhny, and F. Y. Li, "Subjective logic-based in-network data processing for trust management in collocated and distributed wireless sensor networks," *IEEE Sensors Journal*, vol. 99, 2018.

[84] V. S. Janani and M. S. K. Manikandan, "Efficient trust management with Bayesian-evidence theorem to secure public key infrastructure-based mobile ad hoc networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, pp. 1–25, 2018.

[85] D. Meng, L. Zhang, G. Cao, W. Cao, G. Zhang, and B. Hu, "Liver fibrosis classification based on transfer learning and FCNet for ultrasound images," *IEEE Access*, vol. 5, pp. 5804–5810, 2017.

[86] R. R. Sahoo, S. Ray, S. Sarkar, and S. K. Bhoi, "Guard against trust management vulnerabilities in wireless sensor network," *Arabian Journal for Science & Engineering*, vol. 43, no. 12, pp. 7229–7251, 2018.

[87] A. Z. Khan, "Using energy-efficient trust management to protect IoT networks for smart cities," *Sustainable Cities and Society*, vol. 40, pp. 1–5, 2018.

[88] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495–1505, 2018.

[89] M. B. Smithamol and S. Rajeswari, "TMM: trust management middleware for cloud service selection by prioritization," *Journal of Network & Systems Management*, vol. 6, pp. 1–27, 2018.

[90] T. N. D. Pham and C. K. Yeo, "Adaptive trust and privacy management framework for vehicular networks," *Vehicular Communications*, vol. 13, pp. 1–12, 2018.

[91] W. Fang, C. Zhu, W. Chen, W. Zhang, and J. J. Rodrigues, "BDTMS: binomial distribution-based trust management scheme for healthcare-oriented wireless sensor network," in *Proceedings of the 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pp. 382–387, Limassol, Cyprus, June 2018.

[92] A. Ukil, "Trust and reputation based collaborating computing in wireless sensor networks," in *Proceedings of IEEE Second International Conference on Computational Intelligence, Modelling and Simulation (CIMSiM)*, pp. 464–469, Tuban, Indonesia, September 2010.

[93] F. Ishmanov and S. W. Kim, "A secure trust establishment in wireless sensor networks," in *Proceedings of the 2011 International Conference on Electrical Engineering and Informatics*, pp. 1–6, Bandung, Indonesia, July 2011.

[94] F. Bao, R. Chen, M. Chang, and J. H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," *IEEE*

Transactions on Network and Service Management, vol. 9, no. 2, pp. 169–183, 2012.

[95] L. Gheorghe, R. Rughinis, and R. Tataroiu, "Adaptive trust management protocol based on intrusion detection for wireless sensor network," in *2013 RoEduNet International Conference 12th Edition: Networking in Education and Research*, pp. 1–7, Iasi, Romania, September 2013.

[96] A. Tajeddine, A. Kayssi, and A. Chehab, "CENTER: a centralized trust-based efficient routing protocol for wireless sensor network," in *2012 Tenth Annual International Conference on Privacy, Security and Trust*, pp. 195–202, Paris, France, July 2012.

[97] B. Priayoheswari, K. Kulothungan, and A. Kannan, "A novel trust based routing protocol to prevent the malicious nodes in wireless sensor networks," in *2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM)*, pp. 111–115, Tindivanam, India, February 2017.

[98] D. C. Mehetre, S. E. Roslin, and S. J. Wagh, "Detection and prevention of black hole and selective forwarding attack in clustered WSN with active trust," *Cluster Computing*, vol. 22, no. S1, pp. 1313–1328, 2019.

[99] A. Chen, G. Luo, and J. Ren, "An elliptic curve-based trust management protocol in peer-to-peer networks," *IEICE Transactions on Information & Systems*, vol. 97, no. 6, pp. 1656–1660, 2014.

[100] I. D. Addo, J. J. Yang, and S. I. Ahamed, "SPTP: a trust management protocol for online and ubiquitous systems," in *2014 IEEE 38th Annual Computer Software and Applications Conference*, pp. 590–595, Vasteras, Sweden, July 2014.

[101] N. Shilpa and S. Ambareesh, "Efficient routing protocol with trust management for wireless sensor network," *International Journal of Emerging Technology and Advanced Engineering*, vol. 2, no. 5, pp. 143–148, 2015.

[102] H. A. Rahhal, I. A. Ali, and S. I. Shaheen, "A novel trust-based cross-layer model for wireless sensor networks," in *Proceedings of the 28th National Radio Science Conference (NRSC)*, pp. 1–10, Cairo, Egypt, April 2011.

[103] R. Wang, Z. Zhang, Z. Zhang, and Z. Jia, "ETMRM: an energy-efficient trust management and routing mechanism for SDWSNs," *Computer Networks*, vol. 139, pp. 119–135, 2018.

[104] K. Gerrigagoitia, R. Uribeetxeberria, U. Zurutuza, and I. Arenaza, "Reputation-based intrusion detection system for wireless sensor network," in *2012 Complexity in Engineering (COMPENG)*, pp. 1–5, Aachen, Germany, June 2012.

[105] A. Ukil, "Trust and reputation based collaborating computing in wireless sensor network," in *2010 Second International Conference on Computational Intelligence, Modelling and Simulation*, pp. 464–469, Tuban, Indonesia, September 2010.

[106] D. Hui-hui, G. Ya-jun, Y. Zhong-qiang, and C. Hao, "A wireless sensor networks based on multi-angle trust of node," in *2009 International Forum on Information Technology and Applications*, pp. 28–31, Chengdu, China, May 2009.

Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 1468976, 9 pages
https://doi.org/10.1155/2020/1468976

Research Article

Optimized Scheme to Secure IoT Systems Based on Sharing Secret in Multipath Protocol

Fatna El Mahdi,[1] **Ahmed Habbani**,[1] **Zaid Kartit**,[2] **and Bachir Bouamoud**[1]

[1]*SSL Lab, ENSIAS, University of Mohammed V, Rabat, Morocco*
[2]*SIP Research, EMI, University of Mohammed V, Rabat, Morocco*

Correspondence should be addressed to Fatna El Mahdi; fatna.mahdi@um5s.net.ma

Received 29 November 2019; Revised 6 January 2020; Accepted 20 January 2020; Published 4 April 2020

Guest Editor: Hasan Ali Khattak

Internet of Things (IoT) is a hot and emerging topic nowadays. In the world of today, all kinds of devices are supposed to be connected and all types of information are exchanged. This makes human daily life easier and much more intelligent than before. However, this life mode is vulnerable to several security threats. In fact, the mobile networks, by nature, are more exposed to malicious attacks that may read confidential information and modify or even drop important data. This risk should be taken in consideration prior to any construction of mobile networks especially in the coming 5G technology. The present paper aims to provide a contribution in securing such kinds of environment by proposing a new protocol that can be implemented in ad hoc networks.

1. Introduction

The IoT concept is based on connecting different and heterogeneous devices. This connection aims to make human life easier and more efficient, by automating some tasks and making communication faster and better especially in some important fields such as health service, industry, agriculture, transportation, education, or even our domestic daily life as shown in Figure 1. In smart homes, for example, we could switch on air conditioning before arriving home or unlock door for a visiting friend. We can even switch on or off light while we are kilometers away from home. With smart home applications, users can save time, energy, and money and win more life efficiency and comfort. Smart city surveillance, smart transportation, smart energy systems, smart water distribution, and security systems are all examples of IoT applications for smart cities. The collected data in the IoT environment would be analyzed in order to make right decisions at the right moments. However, in such systems, many challenges encounter the normal functioning, especially security challenge, which is by the way our focus in this paper. In fact, wireless mobile networks, which are the communication platform of IoT systems, are vulnerable to different security threats. These security risks can threaten the network in terms of confidentiality, integrity, availability, and other aspects. Thus, improving security and making these systems reliable become more and more mandatory in research field. Scientists and researchers are invited to perform studies in order to secure IoT especially in critical areas such as military domains or medical services. In addition, the IoT has raised public safety concerns, like cyberattacks and organized crimes which can be a serious risk for organizations and people's private life. In different places of the world, many serious attacks on IoT systems have been detected. On 27 June 2019, the US Food and Drug Administration (FDA) issued an alert about some insulin pumps manufactured by Medtronic that are vulnerable to be remotely accessed and controlled by hackers [1]. The same organization (FDA) confirmed, in 2017, that the implantable cardiac devices in St. Jude Medical could be easily hacked and controlled [2]. These devices are used to supervise patients' heart functioning and prevent or help in case of heart attacks. Nevertheless, hackers are able to access the device, control shocks, manage heartbeat, and give incorrect commands, due to some transmitter vulnerabilities. In April 2017, a malware named BrickerBot was discovered [3]. It attempted to definitively destroy IoT objects by executing harmful commands to delete their data and disable them. In

Figure 1: Example of communication domains in a smart environment.

2016, a certain hacker called Anna Senpai created a malware, called Mirai [4], which gains the access and take control of vulnerable connected objects such as routers and surveillance cameras, and create massive distributed denial of service attacks (DDos). Mirai transforms the infected objects into autonomous and intelligent bots controlled remotely. All these examples and many others show clearly that security issue is an urgent and crucial subject and its development is even more important than the development of IoT itself.

In our research, we focus on security requirement for mobile ad hoc networks (MANETs) which are widely used in IoT environments, thanks to their advantages like ease of implementation ease, being infrastructure-less, being self-organized, and dynamic topology. These advantages in terms of implementation and performance can also be seen as a weakness in terms of security and reliability, because of many factors, especially the lack of centralized infrastructure and the difficult implementation of control mechanisms. This character is our main motivation in this research. This paper is organized as follows: The next section presents some related studies in this security field. Section 3 will be dedicated to describing our architecture inspired from sharing a secret approach to secure communication in MANETs; this new algorithm is called Secure Protocol based on Identification, Detection, and Location and Isolation (SPIDLI) steps. This architecture provides a great solution against black hole, eavesdropping, and message tampering attacks. Section 4 is dedicated to discuss the schema example as a proof of concept. In Section 5, we will analyze some of the simulation results. The last section will conclude this paper.

2. Related Work

Complex network is based on graph theory and social sciences concepts and can be considered as a set of several connected nodes that interact in different ways [5]. The IoT concept is based on connecting different and heterogeneous devices [6]. The information exchanged in these networks varies according to the used context. It can be medical, military, agriculture, education, transport. or simply everyday home information [7]. Since this technology interacts with human activity especially in some sensitive domains, such as military or health service, it is necessary to guarantee that the shared information is highly secure [8].

Wang et al. in [9] presents a new metric called R_{NMI} to assess the robustness of the complex network based on standardized mutual information. Next, a simulated annealing algorithm is designed to reduce the damage. In order to improve the balance between attacks and errors, the authors propose a weighted metric to design connecting process R^{w}_{NMI} and a series of solutions focusing on attacks and errors.

Another study proposed by Wang and Liu in [10] focuses on resisting intentional attacks and cascading failures in complex networks, by proposing a framework called MAGA-NetR to improve the overall performance. This technique takes advantage of the fact that the robustness measures which evaluate the tolerance of the networks are not correlated with each other; therefore, this study proposes a standardized robustness measure R_n and this measure is validated to be effective in the experiments.

In order to facilitate the administration of public key certification, Shamir proposed the identity-based

cryptosystem approach in [11], and later, Boneh and Franklin concretized this approach using Weil coupling to provide an ID-based encryption scheme in [12]. As its name indicates, the ID-based cryptosystems are based on the identity information; therefore, each node in the network can use its identity as a public key instead of extracting it from a certificate generated by a certificate authority (CA) [13].

Shamir [14] and Blakley [15] are the first to introduce the notion of secret sharing scheme using (t, n) threshold. This scheme is based on two main steps as follows:

(i) Dividing step where the secret message is divided into n fragments, and then, each fragment is given to an authorized member

(ii) Rebuilding step where the collector tries to reconstruct the initial secret if and only if he combines at least k fragment received [16]

Zhou et al. proposed in [17] the combination between multipath routing and secret sharing to distribute the CA to multiple servers. Later, Kong et al. were interested in improving operations such as the signing of a certificate so that they can be done locally by the neighbors of the requesting node, distributing the servers more evenly over the network [18].

In the same context, and in order to diminish the effects of frequent topological changes, Tsirigos and Haas [19] proposed the application of concurrent multipath routing at the same time with diversity coding. Lou et al. [20] proposed a protocol named SPREAD to ensure data confidentiality and availability in order to strengthen network security. This method is based on four methods: directional transmission, controlling transmission power, shortest-distance routing, and controlling correlation factor. All concurrent multipath routes between any two nodes are considered in this method, but the limitation resides in the fact that active attacks cannot be detected. Through a multipath routing strategy, this protocol enhances the security and performance of an ad hoc network by providing an invented solution based on network coding techniques and the public key cryptosystem. This solution, however, assumes that a routing or multipath protocol is already implemented, so no study of specific routing algorithm has been carried out. In other words, SPREAD relies on multiple simultaneous paths between the source and the destination in MANET but cannot detect the positions of malicious nodes.

So our goal in this paper is not only to use multipath and secret sharing to improve availability and privacy but also to check the integrity of exchanged messages, in addition to locate the nodes suspected to be malicious.

2.1. System Model. Our architecture (totally invented by the author under patent N 42357 OMPIC, Casablanca, Morocco) is based on three essential steps to ensure *availability*, *confidentiality*, and *integrity*. These three steps are *Identification*, *Detection*, *Localization* and *Isolation* and come after a substep of initializing variables.

2.1.1. Initialization. This step is explained in Algorithm 1.

2.1.2. Identification. As described, the destination will receive r fragments of the message. Each combination of k fragments is a version of the message M. In this step (Figure 2), we will consider a metric called black hole coefficient (BH) that will be assigned to each node in the network based on its observed behavior during transmission. This coefficient will be initialized by 0 for all NEs and will be increased and decreased based on our own algorithm defined in the SPIDLI method as explained below. This coefficient will be used later to detect and isolate malicious nodes (Algorithm 2).

The destination can compare the reconstructed versions of the message using the following combination algorithm to ensure integrity.

Combination Algorithm. The total number of possible combinations is as follows:

$$C_r^k = \frac{A_r^k}{k!} = \begin{cases} 0, & \text{if } k > r, \\ \dfrac{r!}{k!\,(r-k)!}, & \text{if } 0 \le k \le r. \end{cases} \tag{1}$$

In practice, computing all combinations is a waste of time and resources. Thus, to optimize the computation process, we propose a minimal number α of combinations that sweep all received fragments. The idea to achieve this is to put $\alpha = \text{Roundup}(r/k)$ which is the next smallest integer that is larger than r/k. Let P_{rl} and P_{url} be the set of reliable paths and unreliable paths, respectively. Let C_{rl_i} be the reliable combination number i and C_{ssp_o} the suspicious combination number o $(1 \le i, o \le \alpha)$ (Algorithm 3).

So the equal combinations $C_{rl_i}(1 \le i \le \alpha)$ are correct combinations equal to the message M. Therefore, the fragments which constitute these reliable combinations are necessarily all reliable fragments $F_{rl_{i_j}}$ $(1 \le j \le k)$. And the different combinations $C_{ssp_o}(1 \le o \le \alpha)$ are suspect combinations constituted by suspicious fragments $F_{ssp_{o_t}}$ $(1 \le t \le k)$; this is why our method will proceed to the second step to locate the unreliable fragments that have been modified during transmission generating different combinations.

2.1.3. Detection. Let F_{rl} (reliable fragments) be the set of fragments $F_{rl_{i_j}}$ $(1 \le i \le \alpha$ and $1 \le j \le k$ with $F_{rl_{i_j}} = F_{rl_{((i-1)k+j)}})$ which constitute equal and reliable combinations C_{rl_i} $(1 \le i \le \alpha)$. Let F_{ssp} (suspicious fragments) be the set of fragments $F_{ssp_{o_t}}$ $(1 \le o \le \alpha$ and $1 \le t \le k$ with $F_{ssp_{o_t}} = F_{ssp_{((o-1)k+t)}})$ which give different combinations C_{ssp_o} $(1 \le o \le \alpha)$ of suspect combination and then eliminate from F_{ssp} all the reliable fragments which belong to F_{rl} in order to have always $F_{rl} \cap F_{ssp} = \varnothing$.

In this step (Figure 3), we will consider a metric called unreliable coefficient (URL) that will be assigned to each node in the network based on its observed behavior during transmission. This coefficient will be initialized by 0 for all NEs and will be increased and decreased based on our own algorithm defined in the SPIDLI method as explained below. This coefficient will be used later to detect and isolate malicious nodes (Algorithm 4).

(i) **Step 1**: source node S marks n paths to the destination D. Let P_n be the set of paths between S and D. The value of n varies from one node to another according to the neighborhood of each node.
(ii) **Step 2**: S divides the message M using Shamir secret sharing scheme to n fragments $\{F_1, F_2, \ldots, F_n\}$
(iii) **Step 3**: the source then chooses one threshold k of the Shamir method $(k \leq n)$, k also varies according to n and the number of the node-disjoint paths
(iv) **Step 4**: S encapsulates each fragment F_i in a packet and then sends it in a path P_i from P_n.
(v) **Step 5**: the destination D receives r packets $(r \leq n)$. Let P_r be the set of paths where D received r packets.
(vi) **Step 6**: S receives r acknowledgments; let us suppose that a path is bidirectionally trusted/untrusted.

Algorithm 1: Initialization steps.

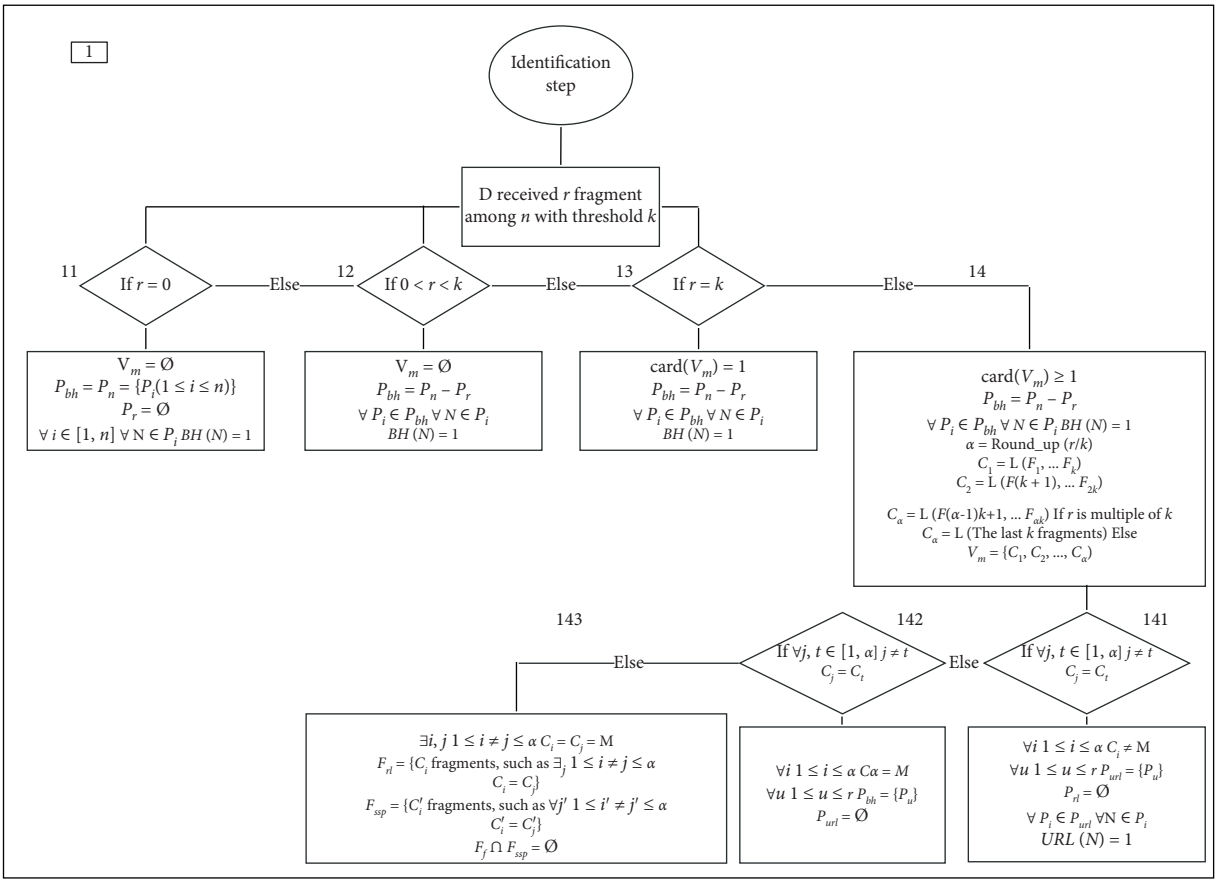


Figure 2: Organizational chart of identification step.

Step 1: in this step, destination D reconstructs the message M from the received fragments. Let V_m be the set of all possible versions of M. Let us discuss the possible scenarios:
(i) **If** $0 \leq r < k$, the destination cannot reconstruct the message M sent by S; $V_m = \varnothing$. The source resends the missing fragments in the paths where the acknowledgments are received. In order to optimize the process for future transmission, the source returns to the initialization step and recalculates n and k so that n becomes equal to r. Let P_{bh} be the set of paths that may contain black holes. In the case $P_{bh} = P_n - P_r$, the source S assigns the value 1 to the black hole coefficient to all the nodes that constitute these paths. $\forall P_i \in P_{bh}$, $\forall N \in P_i$, $BH(N) = 1$
(ii) **If** $r = k$, the destination D can reconstruct one version of the message M using the Shamir method. In the case $\text{card}(V_m) = 1$ and $P_{bh} = P_n - P_r$, the source S assigns the value 1 to the black hole coefficient to all the nodes that constitute these paths. $\forall P_i \in P_{bh}$, $\forall N \in P_i$, $BH(N) = 1$
(iii) **If** $k + 1 \leq r \leq n$, the destination, using Lagrange polynomial (Shamir method), can reconstruct many versions of the message. The associated Lagrange polynomial is written as follows:
$L(0) = \sum_{j=0}^{k-1} f(x_j) \prod_{m=0, m \neq j}^{k-1} x_m / (x_m - x_j)$

Algorithm 2: Identification steps.

Step 1: destination calculates the possible combinations that cover all the elements of our set $\{F_1, F_2, \ldots F_r\}$

$C_1 = L(F_1, \ldots F_k)$

$C_2 = L(F_{k+1}, \ldots F_{2k})$

$C_3 = L(F_{2k+1}, \ldots F_{3k})$

$\ldots$

$$C_\alpha = \begin{cases} L(F_{(\alpha-1)k+1}, \ldots, F\alpha k), & \text{if, } r \text{ is multiple of } k \\ L(\text{The last } k \text{ fragments}), & \text{else} \end{cases}$$

$V_m = \{C_1, C_2, \ldots, C_\alpha\}$

(i) **If** $\forall i, j \in \{1, \alpha\}\, C_i = C_j$:
So all the paths $P_j\ 1 \le j \le r$ are reliable paths, and the initial message sent by the source is equal to C_i,
$\forall i,\ 1 \le i \le \alpha,\ C_i = M,\ P_{url} = \varnothing,\ P_{rl} = \{P_1, P_2, \ldots, P_r\}$

(ii) **If** there are different combinations, and at least two equal combinations: So the equal combinations C_{rli} $(1 \le i \le \alpha)$ are correct combinations equal to the message M. Therefore, the fragments which constitute these reliable combinations are necessarily all reliable fragments F_{rlij} $(1 \le j \le k)$. And the different combinations C_{ssp_o} are suspect combinations constituted by suspicious fragments F_{sspot} $(1 \le t \le k)$, that is why our method will proceed to the second step to locate the unreliable fragments that have been modified during transmission generating different combinations.

Algorithm 3: Combination algorithm.

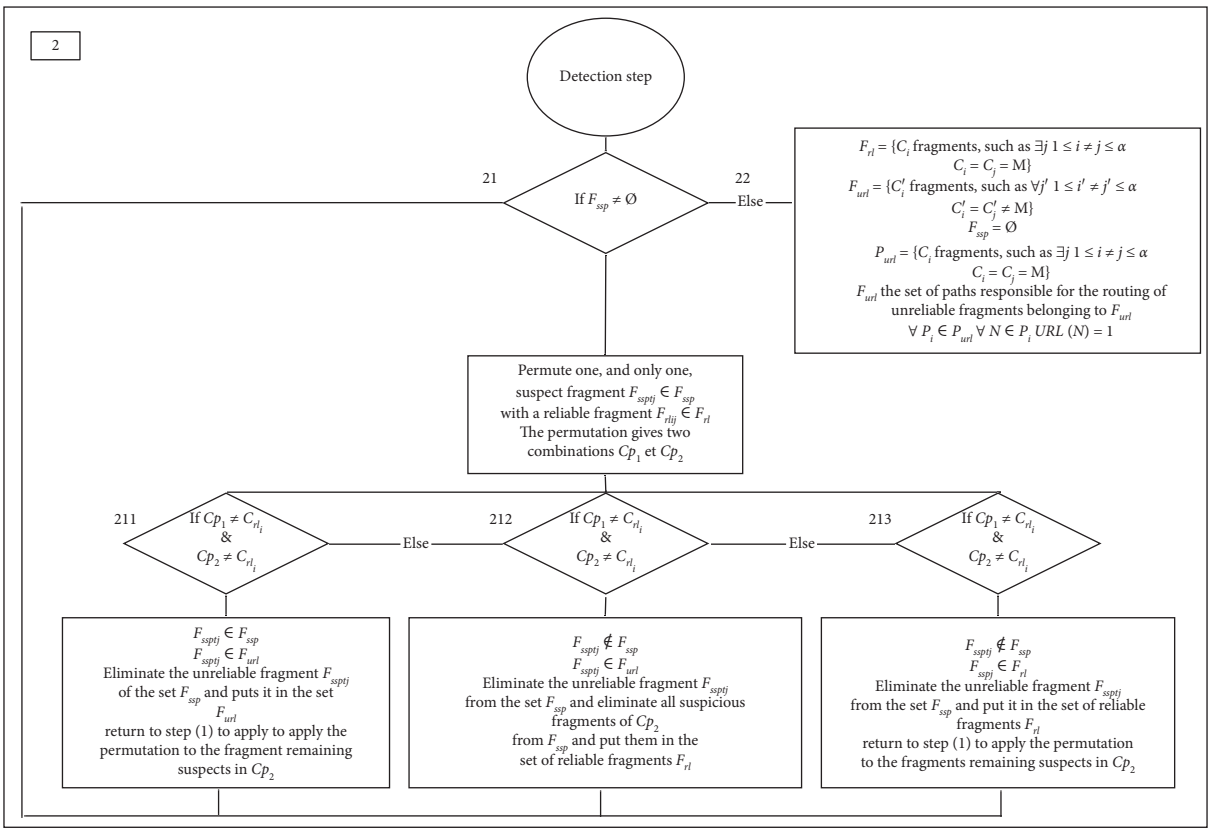


Figure 3: Organizational chart of detection step.

2.1.4. Location and Isolation. In this step (Figure 4), broadcasting the information of the coefficients obtained in the previous steps allows the network to identify and locate black holes and unreliable nodes (Algorithm 5).

Proof of Concept. Let $n = 12$, $k = 4$, and $r = 11$ as shown in Figure 5.

The source divides the message M on $n = 12$ fragments, $F'_1, \ldots F'_{12}$, with a threshold $k = 4$ and sends each fragment F_i in a path P_i (Figure 5):

$$P_n = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_9, P_{10}, P_{11}, P_{12}\}. \quad (2)$$

The destination receives $r = 11$ fragments, $F_1, F_2, .., F_{11}$:

Begin

Step 1: the destination performs permutations of one, and only one, suspect fragment $F_{sspo_j} \in F_{ssp}$, with a reliable fragment $F_{rl_{i_j}} \in F_{rl}$. The permutation gives two combinations

$C_{p_1} = L(F_{rl_{i_1}}, \ldots, F_{ssp_{o_j}}, \ldots, F_{rl_{i_k}})$

$C_{p_2} = L(F_{ssp_{o_1}}, \ldots, F_{rl_{i_j}}, \ldots, F_{ssp_{o_k}})$, $1 \le i, o \le \alpha$

Step 2: each time, the destination compares the computed combinations C_{p_1} and C_{p_2} with one of the reliable combinations C_{rl_i} so

(i) **If** $C_{p_1} \neq C_{rl_i}$ and $C_{p_2} \neq C_{rl_i}, F_{ssp_{o_j}}$ is an unreliable fragment, because it gives an incorrect combination with a set of only reliable fragments. The destination, thus, updates the two sets F_{url} and F_{ssp}; it eliminates the unreliable fragment $F_{ssp_{o_j}}$ from the set F_{ssp} and puts it in the set F_{url}; it returns to step (1) to apply the permutation to the fragments remaining suspects in C_{p_2}.

(ii) **If** $C_{p_1} \neq C_{rl_i}$ and $C_{p_2} = C_{rl_i}, F_{ssp_{o_j}}$ is an unreliable fragment and all C_{p_2} fragments are reliable fragments The destination, thus, updates the sets F_{rl}, F_{url}, and F_{ssp}; it eliminates the unreliable fragment $F_{ssp_{o_j}}$ from the set F_{ssp} and put it in the set of unreliable fragments F_{url}, and it eliminates all suspicious fragments of C_{p_2} from F_{ssp} and put them in the set of reliable fragments F_{rl}.

(iii) **If** $C_{p_1} = C_{rl_i}$ and $C_{p_2} \neq C_{rl_i}, F_{ssp_{o_j}}$ is a reliable fragment, because it gives a correct combination with a set of only reliable fragments. The destination, thus, updates the two sets F_{rl} and F_{ssp}; it eliminates the unreliable fragment $F_{ssp_{o_j}}$ from the set F_{ssp} and puts it in the set F_{rl}; it returns to step (1) to apply the permutation to the fragments remaining suspects in C_{p_2}.

Step 3: D checks if all suspicious fragments of F_{ssp} are swept until $F_{ssp} = \varnothing$.

Step 4: In all previous cases, $P_{bh} = P_n - P_r$; the source S assigns the value 1 to the black hole coefficient to all the nodes that constitute these paths.

$\forall P_i \in P_{bh}, \forall N \in P_i, BH(N) = 1$

The destination D assigns also the value 1 to the coefficient of unreliability URL to all the nodes which constitute the unreliable paths P_{url}. Then, S and D exchange this information.

$\forall P_j \in P_{url}, \forall N \in P_j, URL(N) = 1$

END

Algorithm 4: Detection steps.

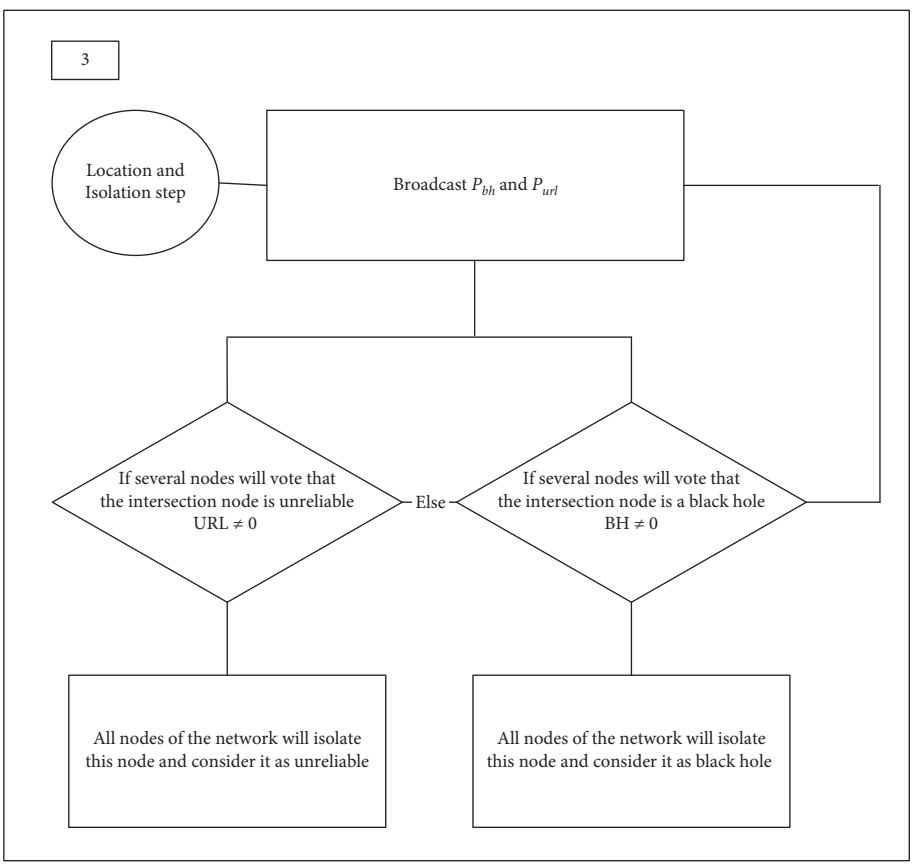


Figure 4: Organizational chart of location and isolation step.

Begin
Step 1: as long as there are intersections between paths containing black holes, several nodes will vote that the intersection node is a black hole; then, its $BH \neq 0$ and BH is higher than a specified threshold that will be fixed in advance. So all the nodes of the network will isolate this node and consider it as black hole.
Step 2: by the same process, the nodes suspected to be unreliable will be located and isolated too.
We initialize at all nodes of the network the coefficients black hole BH and unreliable URL to 0
$\forall$ N is the node of the network BH $(N) = 0$ and URL $(N) = 0$
END

Algorithm 5: Location and isolation steps.

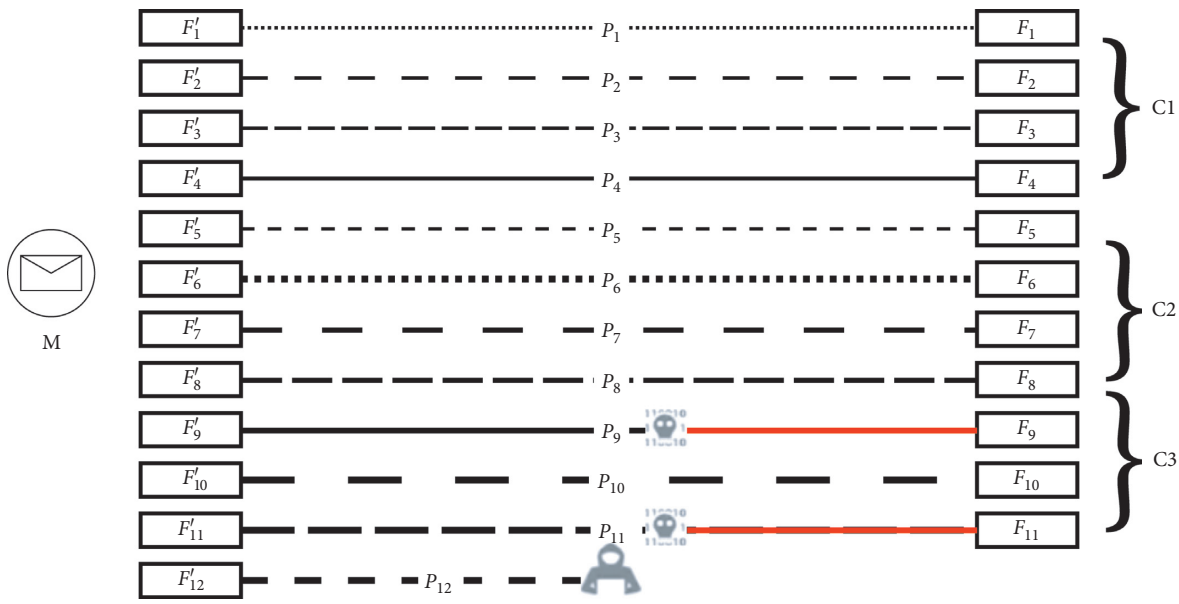


Figure 5: Example scenario of the SPIDLI protocol.

$$\begin{aligned} P_r &= \{P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_9, P_{10}, P_{11}\}, \\ \alpha &= \text{roundup}\left(\frac{r}{k}\right), \\ C_1 &= L(F_1, F_2, F_3, F_4), \\ C_2 &= L(F_5, F_6, F_7, F_8), \\ C_3 &= L(F_8, F_9, F_{10}, F_{11}), \end{aligned} \tag{3}$$

where C_1 and C_2 are two correct combinations equal to the original message M sent by the source, but the combination C_3 is not correct. Then,

$$\begin{aligned} F_{rl} &= \{F_1, F_2, F_3, F_4, F_5, F_6, F_7, F_8\}, \\ F_{ssp} &= \{F_8, F_9, F_{10}, F_{11}\}, \\ F_{url} &= \varnothing. \end{aligned} \tag{4}$$

Since $F_8 \in F_{rl}$, $F_{ssp} = \{F_9, F_{10}, F_{11}\}$.

Swap F_9 from incorrect combination C_3 with F_2 from the correct combination C_1:

$$\begin{aligned} C_1 &= L(F_1, F_2, F_3, F_4), \\ C_{p_1} &= L(F_1, F_9, F_3, F_4), \\ C_3 &= L(F_8, F_9, F_{10}, F_{11}), \\ C'_{p_1} &= L(F_8, F_2, F_{10}, F_{11}). \end{aligned} \tag{5}$$

$C_{p_1} \neq C_1$. So we are sure that the fragment F_9 was modified during the transmission.

So, $F_{rl} = \{F_1, F_2, F_3, F_4, F_5, F_6, F_7, F_8\}$, $F_{url} = \{F_9\}$, and $F_{ssp} = \{F_{10}, F_{11}\}$.

$C'_{p_1} \neq C_1$. So we are not sure if two fragments F_{10} and F_{11} are both unreliable or one of them; therefore, we will repeat another permutation of F_{10} of the new combination C'_{p_1} with F_3 of C_1:

$$\begin{aligned} C_1 &= L(F_1, F_2, F_3, F_4), \\ C_{p_2} &= L(F_1, F_2, F_{10}, F_4), \\ C'_{p_1} &= L(F_8, F_2, F_{10}, F_{11}), \\ C'_{p_2} &= L(F_8, F_2, F_3, F_{11}). \end{aligned} \tag{6}$$

Table 1: Parameters value.

Parameter	Value
Routing protocol	SPIDLI/MPOLSR
Simulation time	250 seconds
Number of nodes	10, 20, 30, 40, 50, 60, 70, 80, 90, and 100 nodes
Environment area	1000 meter × 1000 meter
MAC protocol	IEEE 802.11
Transport layer	Transmission control protocol (TCP)
Maximum speeds	5 meter/second
Mobility model	Random waypoint

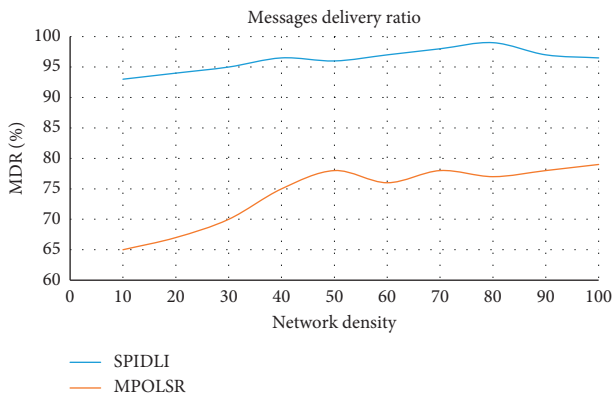


Figure 6: Message delivery ratio graph.

$C_{p_2} = C_1$. So we are sure that the fragment F_{10} was not modified during the transmission; thus, F_{10} is correct.

Then, $F_{rl} = \{F_1, F_2, F_3, F_4, F_5, F_6, F_7, F_8, F_{10}\}$, $F_{url} = \{F_9\}$, and $F_{ssp} = \{F_{11}\}$.

$C'_{p_2} \neq C_1$. So we are sure that the fragment F_{11} has been modified during the transmission.

Then, $F_{rl} = \{F_1, F_2, F_3, F_4, F_5, F_6, F_7, F_8, F_{10}\}$, $F_{url} = \{F_9, F_{11}\}$, and $F_{ssp} = \varnothing$. □

3. Analytical Results

In order to evaluate our protocol SPIDLI, and their impact on network performances, we have implemented a simulation in the NS2 platform with the objective of evaluating the efficiency of our solution. We have compared our method with standard MPOLSR in a medium size ad hoc network under a random black hole attack. The used parameters are shown in Table 1:

In this simulation, we will observe three main metrics: MDR (message delivery ratio), end-to-end delay, and throughput. We will compare the standard MPOLSR and SPIDLI. We used in our simulation the MPOLSR type which is based on load sharing.

Figure 6 shows the evolution of message delivery ratio with network density in both MPOLSR and SPIDLI in case of a black hole attack average of 20% of nodes number. The simulation result shows clearly that our method improves the MDR comparing with standard MPOLSR. The objective of SPIDLI is to increase the chance of a message to reach the destination node. This objective is achieved according to the

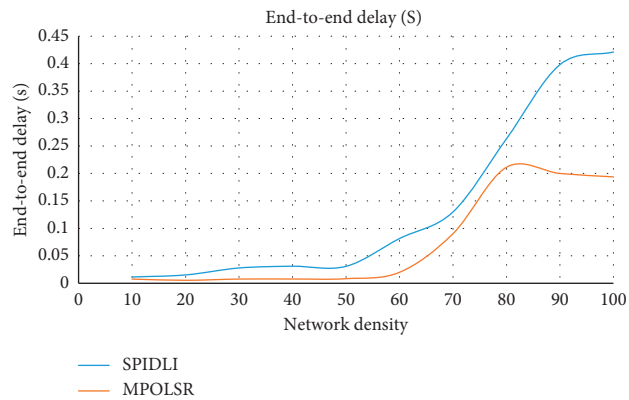


Figure 7: End-to-end delay graph.

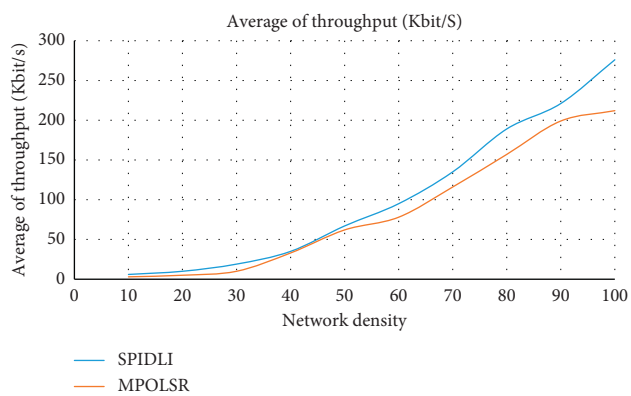


Figure 8: Throughput graph.

simulation result. We can observe also that the MDR increases with network density, which is explained by the fact that having a high number of nodes gives more available routes (high threshold k) to reroute the message from the source to destination.

In this graph (Figure 7), we analyze the average delay evolution according to network density for MPOLSR and SPIDLI protocols with black hole attack. When network density is relatively small, the number of paths in SPIDLI is nearly the same as MPOLSR; thus the threshold k is smaller (equal to 1 or 2). As a result, the calculation processing does not impact the end-to-end delay. However, when the density becomes higher, we observe that the end-to-end delay increases specially in case of SPIDLI. This can be justified by the fact that each node performs extra processing for x or calculation and queuing operations in order to reconstruct the initial message. In addition, the paths selected using SPIDLI may be longer than those selected using standard MPOLSR, which may also generate more delay.

In Figure 8 we analyze the evolution of average throughput in function of network density in a simulation of mobile networks with attacks of both MPOLSR and SPIDLI. We can see that throughput in case of SPIDLI is slightly higher than MPOLSR in a network with more than 50 nodes. This behavior can be explained by the fact that SPIDLI generates extra packets more than MPOLSR. In addition, the

dropped packets in MPOLSR are retransmitted which affects the throughput.

4. Conclusion

As conclusion, with the emerging IoT and smart cities, the security aspect becomes more and more insisting and research and studies are highly recommended. In this context, we have invented a new method named SPIDLI where we provide a scheme aiming to prevent some security threats especially black holes, message tampering, and eavesdropping attacks putting at risk the availability, integrity, and confidentiality (respectively) of data in ad hoc networks. This security prevention is mandatory in some cases of IoT where the exchanged information is sensitive and confidential. We have implemented our solution in the NS2 simulation environment to compare it with the standard MPOLSR protocol and found some considerable results. As future work, we will try to optimize our solution to enhance the performance in terms of end-to-end delay and evaluate other important KPIs such as energy consumption and jitter.

Data Availability

No data were used to support this study.

Conflicts of Interest

All the authors have read the manuscript and have approved this submission. The authors report no conflicts of interest.

References

[1] Medtronic. Cybersecurity notice-legacy exchange program, 2019.

[2] CNN Business, *Fda Confirms that St. Jude's Cardiac Devices Can Be Hacked*, CNN Business, Atlanta, GA, USA, 2017.

[3] D. Goodin, "Brickerbot, the permanent denial-of-service botnet, is back with a vengeance," *Ars Technica*, 2017.

[4] J. Biggs, *Hackers Release Source Code for a Powerful Ddos App Called Mirai*, Vol. 19, TechCrunch, San Francisco Bay Area, CA, USA, 2016.

[5] J. Yan, H. He, and Y. Sun, "Integrated security analysis on cascading failure in complex networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 3, pp. 451–463, 2014.

[6] F. El Mahdi, B. Bouamoud, and H. Ahmed, "Analyzing security in smart cities networking and implementing link quality metric," in *Proceedings of the 2019 Third International Conference on Intelligent Computing in Data Sciences (ICDS)*, pp. 1–8, IEEE, Marrakech, Morocco, October 2019.

[7] F. El Mahdi, H. Ahmed, M. Nada, and B. Essaid, "Study of security in manets and evaluation of network performance using etx metric," in *Proceedings of the 2017 International Conference on Smart Digital Environment*, pp. 220–228, ACM, Rabat, Morocco, July 2017.

[8] F. El Mahdi, H. Ahmed, B. Bouamoud, and M. Souidi, "Bootstrapping services availability through multipath routing for enhanced security in urban iot," in *Proceedings of the 4th International Conference on Smart City Applications*, pp. 1–9, Casablanca, Morocco, October 2019.

[9] S. Wang, J. Liu, and X. Wang, "Mitigation of attacks and errors on community structure in complex networks," *Journal of Statistical Mechanics: Theory and Experiment*, vol. 2017, no. 4, Article ID 043405, 2017.

[10] S. Wang and J. Liu, "Designing comprehensively robust networks against intentional attacks and cascading failures," *Information Sciences*, vol. 478, pp. 125–140, 2019.

[11] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques*, pp. 47–53, Springer, Davos, Switzerland, May 1984.

[12] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology-CRYPTO 2001*, pp. 213–229, Springer, Berlin, Germany, 2001.

[13] Z. Hui, C. Li-Qing, and Q.-Y. Zhu, "The application of threshold secret sharing in key agreement scheme for manets," in *Proceedings of the 2012 International Conference on Computer Science and Service System*, pp. 837–840, IEEE, Nanjing, China, August 2012.

[14] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[15] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of the 1979 International Workshop on Managing Requirements Knowledge (MARK)*, vol. 48, New York, NY, USA, June 1979.

[16] S. Chen and M. Wu, "Secure multipath routing based on secret sharing in mobile ad hoc networks," in *Proceedings of the 2009 IEEE International Conference on Network Infrastructure and Digital Content*, pp. 539–542, IEEE, Beijing, China, November 2009.

[17] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Network*, vol. 13, no. 6, pp. 24–30, 1999.

[18] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing robust and ubiquitous security support for mobile ad hoc networks," in *Proceedings of the Ninth International Conference on Network Protocols. ICNP 2001*, vol. 1, pp. 251–260, Citeseer, Riverside, CA, USA, November 2001.

[19] A. Tsirigos and Z. J. Haas, "Analysis of multipath routing, part 2: mitigation of the effects of frequently changing network topologies," *IEEE Transactions on Wireless Communications*, vol. 3, no. 2, pp. 500–511, 2004.

[20] W. Lou, W. Liu, Y. Zhang, and Y. Fang, "Spread: improving network security by multipath routing in mobile ad hoc networks," *Wireless Networks*, vol. 15, no. 3, pp. 279–294, 2009.

Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 8436917, 12 pages
https://doi.org/10.1155/2020/8436917

Research Article

The Lightweight RFID Grouping-Proof Protocols with Identity Authentication and Forward Security

Zhicai Shi, Xiaomei Zhang, and Jin Liu

School of Electronic & Electrical Engineering, Shanghai University of Engineering Science, Shanghai 201620, China

Correspondence should be addressed to Zhicai Shi; szc1964@163.com

Received 20 July 2019; Accepted 24 December 2019; Published 18 March 2020

Guest Editor: Hasan Ali Khattak

In many fields, multiple RFID tags are often combined into a group to identify an object. An RFID grouping-proof protocol is utilized to prove the simultaneous existence of a group of tags. However, many current grouping-proof protocols cannot simultaneously provide privacy preserving, forward security, and the authentication between reader/verifier and tags, which are vulnerable to trace attack, privacy leakage, and desynchronization attack. To improve the secure performance of the current grouping-proof protocols, we propose two provable lightweight grouping-proof protocols that provide forward security, identity authentication, and privacy preserving. Our protocols involve a trusted reader and an untrusted reader, respectively. In order to avoid verifying some invalid evidences, our protocols complete the authentication of the verifier to the trusted reader and the verified tags before the verifier verifies the grouping-proof evidence. Each tag uses parallel mode to complete its signature to improve the efficiency of the protocols. Moreover, the activate-sleep mechanism and the filtering operation are proposed to effectively reduce the collision probability and computing load of tags. Our protocols complete the authentication to tags twice by a verifier and a trusted reader, respectively. They can resist various attacks such as eavesdropping, replay, trace, and desynchronization. The protocols are proven to be secure, flexible, and efficient. They only utilize some lightweight operations. Therefore, they are very suitable to the low-cost RFID systems.

1. Introduction

As an important sensing method of Internet of Things (IoTs), Radio Frequency IDentification (RFID) has become a pervasive technology and it has been successfully applied to mobile payment, healthcare, supply chain management, transportation, and other fields [1]. A typical RFID deployment is called an RFID system, which has three main components: Radio Frequency (RF) tags, a reader, and a backend server. A backend server is also called a verifier. Tags are some electronic devices and they are usually used to identify some objects. Tags are usually divided into active tags and passive tags. The current popular tags are passive. They are very simple and cheap. They have no internal power source. When these tags communicate with a reader, they are powered with their on-chip antenna coil, which is activated by the RF signal from the reader. Thus, their computation and communication capabilities are very limited. A tag is usually used to identify an object. However, under many circumstances, multiple tags are combined into a group to identify several related objects or different parts of an object. Therefore, it is necessary to read several tags simultaneously and to prove their coexistence.

In 2004, Juels [2] proposed the first application of a group of tags. He combined two tags into a group to identify the container of the medication and the leaflet, respectively. The leaflet describes the side effects of the medication. He proposed a grouping-proof protocol to verify whether each container was dispensed with its leaflet. Another example is that the manufacturer of aircraft equipment uses two tags to identify a certain part and its safety cap. A grouping-proof protocol is utilized to verify whether a part leaves the factory with its safety cap. For the circumstances described above, some grouping-proof protocols have been proposed to prove the coexistence of multiple tags. Due to the hardware resource limitation of tags, the grouping-proof protocols only

use some lightweight cryptographic functions. Hence, the secure level of the current grouping-proof protocols is very limited. The majority of existing protocols do not protect the privacy of the tag and cannot provide forward security [3, 4]. Some grouping-proof protocols usually use serial signature mode so that they need more time to collect the grouping-proof evidence. In order to overcome the flaws above, we propose two novel grouping-proof protocols. These protocols only utilize some lightweight functions to ensure the security and privacy of an RFID system.

The main contributions of our work can be summarized as follows:

(1) We proposed two grouping-proof protocols. These protocols involve a reader and multiple tag groups. The reader may be trusted or untrusted. It is used to collect the grouping-proof evidence. The protocols complete both the mutual authentication between the verifier and the trusted reader and the one-way authentication of the reader/verifier to tags. One of our protocols completes the authentication to tags twice by the verifier and the trusted reader, respectively, which enhances the security level of the protocols.

(2) The protocols ensure the privacy of the RFID system by utilizing some one-way lightweight functions to generate sessions between reader and tags.

(3) The protocols provide forward security by means of secrecy updating. When the secrecy is updated, the old secrecy is reserved in the verifier so that the protocols can resist desynchronization attack.

(4) In order to reduce the collision probability and computation load of tags, a novel activate-sleep mechanism is proposed. The mechanism makes the related tags activated and other tags sleep during the grouping-proof period. When the reader communicates with tags, only the activated tags give their response. Therefore the collision probability and computation load of tags are remarkably reduced.

(5) The protocols utilize the mechanism based on MAC layer protocol of Ethernet. The message broadcasted by a reader is only received by a certain tag and other unrelated tags do not participate in the interaction of the protocols, which is called the filtering operation. Therefore our protocols use a broadcast RF channel to complete the peer-to-peer communication between a reader and a certain tag, which further reduces the computation load of tags and the collision probability between them.

The rest of this paper is organized as follows. In Section 2, we briefly review some typical grouping-proof protocols and analyze their security. In Section 3, we describe the RFID system under the grouping-proof mode and propose its security model. In Section 4, we propose two novel grouping-proof protocols by utilizing parallel communication mode, the activate-sleep mechanism, and the filtering operation. We describe the detail process of the protocols. In Section 5, we prove the security of our protocols. We analyze their security performance and compare them with some typical grouping-proof protocols. Finally, we give the conclusions in Section 6.

2. Some Typical RFID Grouping-Proof Protocols

In this section, we describe some typical and related grouping-proof protocols and discuss their security and vulnerability.

The first grouping-proof protocol is the Yoking-proofs protocol, which is proposed by Juels [2]. This protocol only involves two tags. The protocol gives a proof that a pair of tags has been scanned simultaneously. For the minimalist version of the protocol, the identifiers of the tags are transferred in plaintext. An adversary can intercept these identifiers by eavesdropping the sessions between reader and tags. Then he can get the privacy of the RFID system. Therefore the protocol cannot resist privacy leakage. Saito and Sakurai [5] and Burmester et al. [3] analyzed the Yoking-proofs protocol. They found that it does not resist replay attack and does not check the results from other tags so that some unrelated tags can join the protocol. Another weakness is that a corrupted tag can impersonate a legal tag to generate the valid evidence. Otherwise, the protocol cannot resist interleaving attack [6].

Leng et al. [7] proposed a select-response grouping-proof protocol. Instead of waiting for the computation result from the tags, their protocol allows the reader to actively select the demanded tags. Therefore their protocol can provide collision-free performance and identify the missing tags. But a malicious tag can stop a legitimate proof generation or force creating an invalid proof. So their protocol cannot resist denial of service (DoS) attack. To overcome these problems, they propose an online protocol and the verifier is involved in each step instead of waiting. Therefore, the protocol wastes the time of the verifier.

Huang and Ku [8] proposed a grouping-proof protocol conforming to the Class-1 Gen-2 standard. Their protocol is used to check the correlation of drug and patient so as to enhance medication safety. Peris-Lopez et al. [4] found that the protocol uses CRC functions. These functions are some algorithms based on polynomial arithmetic in F_2. They found that an attacker can exploit the linearity property of CRC functions, such as $\mathrm{CRC}(a \oplus b) = \mathrm{CRC}(a) \oplus \mathrm{CRC}(b)$ to get the private information of the tag. Then he can impersonate this tag in the future grouping-proof protocol. Otherwise, for the protocol proposed by Huang H-H et al., the target tag updates its *pin* once it is interrogated by an attacker. But the verifier does not know that the target tag has been interrogated and the verifier does not update its pin. Therefore the verifier and the tags own different pin and they lose their synchronization. So the protocol cannot resist desynchronization attack.

Chien et al. [9] proposed two grouping-proof protocols for the EPC C1-G2 tags. Their protocols only utilize a 16-bit pseudorandom number generator and bitwise XOR

operation. Peris-Lopez et al. [4] analyzed the online protocol and found a vulnerability. If an adversary detects that the tag and the reader generate the same random number he can generate a fixed session unrelated to the random number. Later he can use the session to impersonate a target tag. Therefore, the protocol cannot resist forgery attack and subset replay attack. To overcome the shortcoming of the online protocol, Chien et al. proposed an offline protocol. But their offline protocol cannot also resist subset replay attack. In addition, their protocol cannot be applied to some special scenarios where the number and type of tags are not known in advance.

Like the two protocols described above, Peris-Lopez et al. [10] also proposed a grouping-proof protocol to enhance medication safety. For their protocol, the unit-dose packages can automatically match the inpatient to avoid human error. Peris-Lopez et al. claimed that the digital evidence from their protocol could be used for medication tracking and auditing. But Yen et al. [11] found that only the nurse signed the evidence. If a medication dispute occurs, the hospital can counterfeit evidence. In order to overcome the security vulnerability described above, Yen et al. proposed another solution. Their protocol involves four entities: the backend server, the nurse's PDA, the inpatient's wristband, and the unit-dose drug packages. However, their protocol could not resist tracing attack. If the inpatient and the unit-dose tags receive the same challenge from the nurse's PDA many times, they will return the same message. Then an adversary can locate the inpatient and his/her unit-dose package. Therefore, it is easy to leak the privacy of the inpatient. Otherwise, the secret keys of the protocol are not updated after each grouping-proof and the protocol cannot ensure forward security.

Liu et al. [12] analyzed some previous grouping-proof protocols. They found that many protocols only involve a single reader and a group of tags. Then they adopted the distributed authentication mode to propose a grouping-proof protocol. They claimed that their protocol can resist some typical attacks such as forgery, tracking, replay, and denial of proof. Later, Shen et al. [13] proposed an enhanced protocol and claimed that their protocol could preserve the privacy of the RFID system and resist replay attack. However, we found that their protocol uses the plaintext of the identifiers for communication. Moreover, these identifiers are fixed during the grouping-proof period. Hence, their protocol cannot resist trace attack and it seriously leaks the privacy of the RFID system. The grouping-proof evidence V_i of each tag is generated independently and there is not any relationship between V_m and $V_n (m \neq n)$. Their grouping-proof protocol does not have any time limitation. So their grouping-proof evidence does not prove the coexistence of the related tags.

By analyzing some previous grouping-proof protocols, Moriyama [14] utilized parallel signature mode to propose a two-round grouping-proof protocol. The protocol only involves two round sessions. The number of the sessions is independent of the number of tags. But the protocol can only resist impersonation attack. The timestamp is generated by the reader. If it is timeout the verifier cannot judge the validness of the grouping-proof evidence.

Sundaresan et al. [15] analyzed some special requirements for a grouping-proof protocol. Then they proposed a robust grouping-proof protocol for the EPC C1-G2 tags. The protocol provides forward security. It utilizes serial signature mode to collect the grouping-proof evidence from each tag so as to degrade its efficiency. Each tag has to complete a large amount of 128-bit operations, which further reduces the efficiency of the protocol. After the ith tag generates its evidence M_i, it updates its secret VT_S. If a grouping-proof collecting process is stopped or aborted the subsequent tag (e.g., the jth tag, $j > i$) cannot update its secret VT_S. Thus some tags' secrets are updated and other tags' secrets are not updated. Their secrets are not synchronous. Therefore, the protocol cannot resist DoS attack. Otherwise, after a reader is only authenticated it can be authorized to complete the grouping-proof. When there are only some untrusted readers near the verifier they cannot be authorized to complete a grouping-proof.

Huang and Mu [16] proposed a grouping-proof protocol that introduced a new method of the key distribution. The protocol only utilizes some lightweight functions (not hash function) to generate the sessions so as to reduce the computing cost of tags. But the protocol updates the secret key of tags twice for each grouping-proof period. After a tag completes the first updating of its secret key c_i, the reader uses the previous c_i to generate $|c_i - a_i + r_{Ti}|$ and send the result to the tag. The tag cannot authenticate the reader because the secret keys c_i they own are different. Hence desynchronization attack occurs and the protocol cannot resist DoS attack. For the protocol, if an adversary impersonates a reader and repeats to transmit S and a random number r_R to a tag, the tag will reply the same $H(b_i \oplus r_R)$ and k_{l2}/k_{l1}. The protocol also cannot resist tracing attack. k_{l2}/k_{l1} is transferred in plaintext so that the protocol cannot preserve the privacy of the tags. Otherwise, the secret keys of the tags are stored in the reader. So the reader must be trusted. Any untrusted reader cannot be used to complete a grouping-proof.

Shen et al. [17] only used some simple bitwise operations to propose a practical grouping-proof protocol. But their protocol utilizes serial signature mode so that it takes more time to collect a grouping-proof evidence. Otherwise, an adversary can deduce the group's key and the tag's sequence number by eavesdropping the sessions. Hence the protocol cannot preserve the privacy of the system. The protocol does not update the secret keys of the system after each authentication. Therefore the protocol cannot provide forward security.

Hong-yan [18] analyzed the grouping-proof protocol proposed by Batina et al. [19] and he found the protocol has some security vulnerability. Then he utilized ECC mechanism to propose an improved grouping-proof protocol. But his protocol cannot provide forward security and it can only complete the grouping-proof for two tags. So it is not suitable for multiple tags.

Sun and Mu [20] analyzed the protocol proposed by Liu et al. [12] and found that the attacker can easily launch some attacks such as replay, forgery, tracking, and denial of proof. Although Liu et al. claimed their protocol can resist these

well-known attacks, the attacker can effectively compromise all secrets and further impersonate a legal reader or a legal tag.

Zhang et al. [21] proposed a scalable grouping-proof protocol. They use the pruning query tree to reduce the collision between tags. Their protocol supposes that the reader is trusted. Before the reader collects the grouping-proof evidence the verifier firstly updates the secret key of the tag. Then the reader sends r_2 to the tag. After the tag verifies r_2 successfully it updates its secret key. Once r_2 is tampered, the tag cannot update its secret key. But the verifier has updated the secret key of the tag and it does not reserve the old secret key of the tag. So the secret key of the tag stored in the verifier is different from the one stored in the tag. Desynchronization attack occurs. Therefore the protocol cannot resist DoS attack.

Tsai et al. [22] discussed grouping-proof protocols and ownership transfer protocols, respectively. They found that no protocol has been proposed which can achieve both requirements. So they only proposed a novel ownership transfer protocol to ensure that ownership of the cargo is transferred to the new designated owner.

Cherneva and Trahan [23] focus on security, privacy, and efficiency. They proposed a light, improved offline protocol: parallel-dependency grouping-proof protocol. But their protocol does not update any stored secret so as to resist desynchronization attack. So the protocol cannot provide forward security.

As analyzed above, many grouping-proof protocols only involve a group of tags rather than multiple tag groups. Sometimes a tag group only contains two tags. When there only exist some untrusted readers near a verifier the grouping-proof protocol cannot be started. Many grouping-proof protocols use serial signature mode to collect a grouping-proof evidence, which remarkably reduces the efficiency of the protocols. In particular, some grouping-proof protocols cannot provide forward security and they are vulnerable to privacy leakage [24].

3. RFID System under the Grouping-Proof Mode and Its Security Model

Under the grouping-proof mode, an RFID system usually includes multiple tags. These tags are combined into several groups, as shown in Figure 1. A grouping-proof protocol is for a reader to give the evidence that multiple RFID tags exist simultaneously within its broadcast range. There are two classification methods for the grouping-proof protocols:

(1) According to the role of the verifier during the grouping-proof period, the grouping-proof protocols are classified into two different modes: online and offline. For the first mode, the verifier involves the entire grouping-proof process. In contrast, for offline mode, the verifier can only send challenges to the reader and it does not need the persistent presence during the entire grouping-proof period. The efficiency of offline mode is greater than that of online mode. Therefore, many current grouping-proof protocols use offline mode.

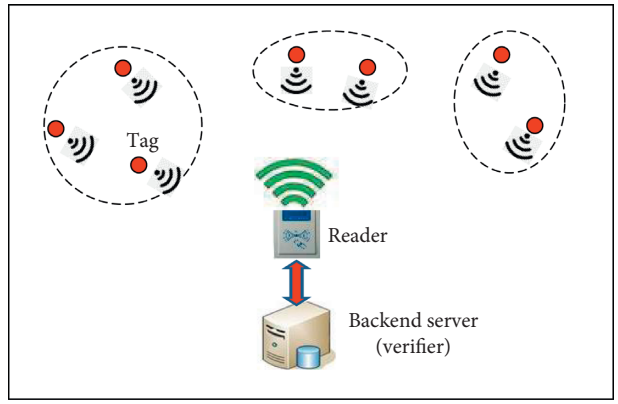


Figure 1: The components of an RFID system under the grouping-proof mode.

(2) According to the sequence for tags to complete their signature, the grouping-proof protocols are classified into two types: serial mode and parallel mode. For the first mode, after one tag finishes its signature another tag begins to sign for generating their grouping-proof evidence. For parallel mode, all tags finish their signatures almost simultaneously. So the grouping-proof protocols under parallel mode are more efficient than those under serial mode.

For an RFID system under the grouping-proof mode, some passive tags are usually used. These tags can only perform some basic cryptographic functions such as pseudorandom number generation and hash operation. We suppose that the verifier is a unique trusted entity and it shares some secrecy with tags. The reader is a potential untrusted entity and it is used to interrogate tags to generate the grouping-proof evidence. Otherwise, we also suppose that the channel between verifier and reader is secure and the channel between reader and tags is insecure. Suppose the verifier and the reader have enough computing and storing resources to complete some advanced cryptographic operations such as asymmetric encryption. For an RFID system under the grouping-proof mode, it should ensure anonymity, confidentiality, and forward security. It can effectively resist privacy leakage, eavesdropping, trace, replay, and desynchronization attack [24].

4. Grouping-Proof Protocols with Identity Authentication and Forward Security

As described above, an RFID system under the grouping-proof mode includes three kinds of entities: verifier, reader, and tag. Generally, we suppose that there are a verifier, a reader, and many tags. These tags are divided into several different groups. Each tag group is only identified by its group identifier. Each tag could be represented by $\{t_{mn}/m \in \{1, 2, \ldots, p\}, n \in \{1, 2, \ldots, q\}\}$, where t_{mn} represents that the tag is the nth tag of the mth group. When we analyze the security of the protocol an adversary must be introduced. It is usually assumed that an adversary is a probabilistic polynomial time algorithm. An adversary can

control each communication channel between reader and tags. He can eavesdrop, intercept, tamper, counterfeit, and replay each session between reader and tags. His main attack goal is to counterfeit a grouping-proof evidence that is verified to be valid by the verifier or to gain the secrecy of the RFID system, such as the secret key and identifier of the tag.

The reader is a potential untrusted entity. It is trusted or untrusted. Now two protocols are proposed for the reader with different security level. They utilize parallel signature mode and they are independent of the sequence accessing to tags. So they are very efficient. For the first protocol, we assume that the reader is untrusted. The reader does not know any secret about tags. So the reader cannot authenticate tags. It only collects the grouping-proof evidence and sends the evidence to the verifier. For the second protocol, the reader is assumed to be trusted and it shares some secrets with the verifier and tags. After a reader is authenticated and authorized by the verifier it can begin to collect the grouping-proof evidence. Then it sends the evidence to the verifier.

For our proposed protocols, each tag stores its current secret key tk_i^{new}, its current identifier tid_i^{new}, and its group identifier gid. A trusted reader stores its identifier rid and its secret key rk. $\{rid, rk\}$ and $\{tk_i^{\text{new}}, tid_i^{\text{new}}, tk_i^{\text{old}}, tid_i^{\text{old}}, gid\}$ are stored in the verifier. tk_i^{old} and tid_i^{old} are the last round secret key and identifier of the ith tag. Let $hash(): \{0,1\}^d \longrightarrow \{0,1\}^d$ be a hash function. Let $prng(): \{0,1\}^d \longrightarrow \{0,1\}^d$ be a pseudorandom number generator. $d \geq 32$ and it is the bit number of the secret key and the identifier. The verified process is started by the reader. The symbols used in our protocols are shown as Table 1.

Table 1: The symbols used in our protocols.

Symbols	Description
gid	The identifier of a tag group
tk_i^{new}, tk_i^{old}	The current and last round secret key of the tag
tid_i^{new}, tid_i^{old}	The current and last round identifier of the tag
rk, rid	The secret key and identifier of the trusted reader
$hash()$	A secure hash function
$prng()$	A pseudorandom number generator
rv, rr, rt_i	Some pseudorandom numbers generated by the different entities
t	The timestamp of the verifier
d	The bit number of the secret key and the identifier
$\oplus$	Bitwise XOR operation

4.1. Grouping-Proof Protocol with the Untrusted Reader. For this protocol, an untrusted reader is used to collect a grouping-proof evidence. When the protocol starts a grouping-proof process, the reader first sends "hello" to the verifier. The verifier sends a message to the reader and the message includes the blinded identifier of the verified tag group. Then the reader collects the coexistence evidence of the tag group and sends the evidence to the verifier. At last, the verifier verifies the validness of the evidence. Because all messages that the reader receives are blinded or encrypted, the reader does not know any secret about the tags and the tag group during the entire grouping-proof period.

The protocol includes four steps as follows:

(1) A reader notifies the verifier that it will start a grouping-proof process.

(2) The verifier starts a timestamp and sends the blinded identifier of the verified tag group to the reader.

(3) The reader collects a grouping-proof evidence and sends the evidence to the verifier.

(4) If it is not timeout the verifier completes the authentication to the tags and verifies the grouping-proof evidence.

The protocol is shown in Figure 2 and is described as follows:

(1) The reader sends "hello" to the verifier.

(2) The verifier stores its current clock to t and starts a timestamp. It generates a pseudorandom number $rv = prng(t)$. Then it uses the verified group's identifier gid to generate the message $m1 = hash(gid \oplus rv)$ and sends $m1 \| rv$ to the reader.

(3) After the reader receives $m1 \| rv$, it broadcasts $m1 \| rv$ to all tags near it.

(4) After each tag receives $m1 \| rv$, it uses its gid to compute $tm1 = hash(gid \oplus rv)$. If $tm1 = m1$ holds, it becomes active. Otherwise, it becomes sleep. The process described above is called the activate-sleep mechanism. Later, only the active tags respond to the reader.

(5) For the ith active tag, it firstly generates a pseudorandom number $rt_i = prng(rv \oplus tk_i)$. Then it uses its tk_i and tid_i to generate $m2_i = hash(tk_i \oplus rt_i)$ and $m3_i = hash(tid_i \oplus rt_i)$, and it sends $m2_i \| m3_i \| rt_i$ to the reader.

(6) After the reader receives $m2_i \| m3_i \| rt_i$ $(i \in \{1, 2, \ldots, k\})$ from each active tag, it calculates $mp = hash(m2_1 \oplus m2_2 \oplus \ldots \oplus m2_k)$ and broadcasts mp to each active tag. k is the total number of the active tags.

(7) After each active tag receives mp, it signs mp with its secret key tk_i and generates $tp_i = hash(tk_i \oplus mp)$. Then it sends tp_i to the reader.

(8) After the reader receives tp_i $(i \in \{1, 2, \ldots, k\})$ from each active tag, it calculates $p = hash(tp_1 \oplus tp_2 \oplus \ldots \oplus tp_k)$. Then it generates the grouping-proof evidence $gp = (rt_1, m2_1, m3_1, rt_2, m2_2, m3_2, \ldots, rt_k, m2_k, m3_k, mp, p)$ and sends gp to the verifier.

(9) After the verifier receives gp, it firstly judges whether it is timeout. If it is timeout, the protocol exits. Otherwise, the protocol goes to the next step.

(10) The verifier calculates $tm2_i = hash(tk_i^x \oplus rt_i)$ and $tm3_i = hash(tid_i^x \oplus rt_i)$ for $\forall x \in \{\text{new}, \text{old}\}$ and $i \in \{1, 2, \ldots, k\}$. If $tm2_i = m2_i$ and $tm3_i = m3_i$ hold for $\forall i \in \{1, 2, \ldots, k\}$, the verifier completes the

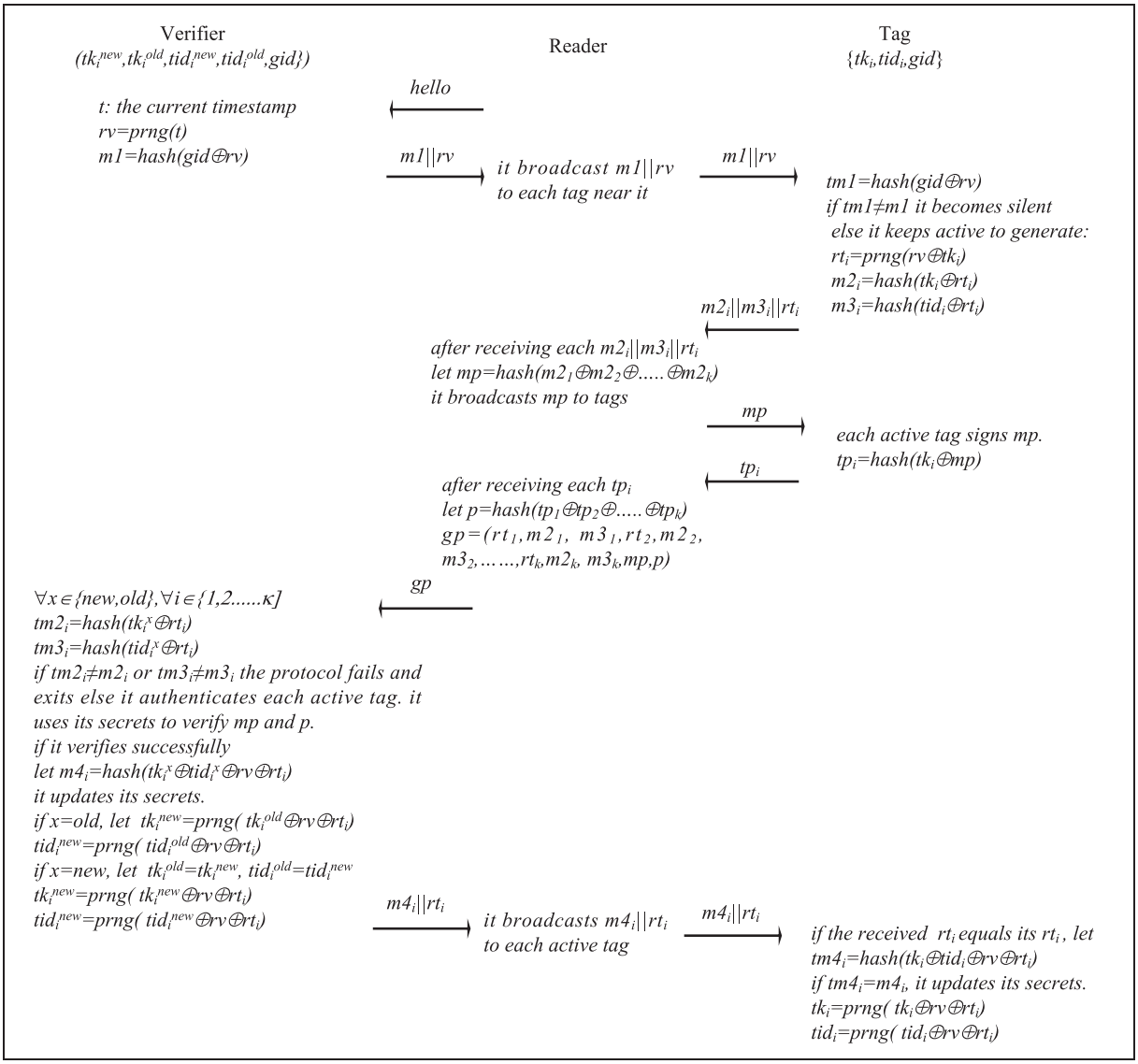


Figure 2: The grouping-proof protocol with the untrusted reader.

authentication to each active tag and begins to verify gp. Otherwise, the protocol fails and exits.

(11) The verifier uses its stored secret information about each active tag and the received rt_i to calculate mp and p. If they equal the received values, the verifier verifies gp successfully and the protocol goes to the next step. Otherwise, the protocol fails and exits.

(12) The verifier generates the message $m4_i = hash(tk_i^x \oplus tid_i^x \oplus rv \oplus rt_i)$. It begins to update its secrets. If $x = \text{old}$ holds, let $tk_i^{\text{new}} = prng(tk_i^{\text{old}} \oplus rv \oplus rt_i)$ and $tid_i^{\text{new}} = prng(tid_i^{\text{old}} \oplus rv \oplus rt_i)$. If $x = \text{new}$ holds, let $tk_i^{\text{old}} = tk_i^{\text{new}}$ and $tid_i^{\text{old}} = tid_i^{\text{new}}$, $tk_i^{\text{new}} = prng(tk_i^{\text{new}} \oplus rv \oplus rt_i)$, and $tid_i^{\text{new}} = prng(tid_i^{\text{new}} \oplus rv \oplus rt_i)$. Then the verifier broadcasts $m4_i \| rt_i$ to each active tag by the reader. rt_i is used to state that $m4_i \| rt_i$ is to send the ith tag and other tags do not respond to the message, although they receive the message, which is called the filtering operation.

(13) After each active tag receives $m4_i \| rt_i$, it compares its rt_i with the received rt_i. If they are not equal, the tag discards the message. Or the tag calculates $tm4 = hash(tk_i \oplus tid_i \oplus rv \oplus rt_i)$. Then it compares $tm4$ with $m4_i$. If they are equal, it updates its secrets: $tk_i = prng(tk_i \oplus rv \oplus rt_i)$ and $tid_i = prng(tid_i \oplus rv \oplus rt_i)$.

4.2. Grouping-Proof Protocol with the Trusted Reader. For this protocol, a trusted reader is used to collect a grouping-proof evidence. The reader stores its identifier rid and its secret key rk, which are also stored in the verifier. When a trusted reader begins to collect a grouping-proof evidence, it first completes the mutual authentication with the verifier. If the authentication succeeds, the verifier sends the related information of the verified group to the reader and the

information includes the secret key and identifier of the verified tags. Then the reader begins to collect the coexistence evidence of the tags and sends the evidence to the verifier.

The protocol includes the following steps:

(1) The reader notifies the verifier and it will start a grouping-proof.

(2) The verifier completes the mutual authentication with the reader and authorizes it.

(3) The verifier starts a timestamp and sends the related information of the verified tags to the reader.

(4) The reader completes the first authentication to each verified tag, collects a grouping-proof evidence, and sends the evidence to the verifier.

(5) If it is not timeout, the verifier completes the second authentication to each verified tag. Then it begins to verify the grouping-proof evidence and updates its secrets.

(6) The verifier notifies the related tags to update their secrets.

The protocol includes three phases. The first phase completes the authentication and authorization of the verifier to the reader. It is shown in Figure 3 and is described as follows:

(1) The reader sends "hello" to the verifier.

(2) The verifier stores its current clock to t, starts a timestamp, and generates a pseudorandom number $rv = prng(t)$. It sends rv to the reader.

(3) The reader generates a pseudorandom number $rr = prng(rv \oplus rk)$ and a message $m1 = hash(rid \oplus rr)$. It sends $rr \| m1$ to the verifier.

(4) The verifier uses rid, which is stored in its database, to generate $tm1 = hash(rid \oplus rr)$. If $m1 = tm1$ holds, it completes the authentication to the reader. Then it generates $m2 = hash(rk \oplus rv \oplus rr)$ and sends $m2$ to the reader. Otherwise, the protocol fails and exits.

(5) The reader uses its rk to generate $tm2 = hash(rk \oplus rv \oplus rr)$ and compares $tm2$ with $m2$. If they are equal, the reader completes the authentication to the verifier. Then it generates $m3 = hash(rk \oplus rr)$ and sends $m3$ to the verifier. If they are unequal, the protocol fails and exits.

(6) The verifier uses its rk, which is stored in its database, to compute $tm3 = hash(rk \oplus rr)$ and compares $tm3$ with $m3$. If they are equal, the verifier completes the mutual authentication with the reader. If they are unequal, the protocol fails and exits.

(7) After the verifier completes the mutual authentication with the reader, it transfers (tk_i^x, tid_i^x) of each verified tag and the verified group identifier gid to the reader by a secure channel or a secure cryptographic primitive, where $x \in \{\text{new}, \text{old}\}$; $i \in \{1, 2, \ldots, k\}$, k is the total number of the verified tags. The reader is authorized to collect a grouping-proof evidence.

In the second phase, the reader wakes up the related tags and completes the first authentication to each verified tag. It is shown in Figure 4 and is described as follows:

(1) The reader generates the message $m4 = hash(gid \oplus rr)$ and broadcasts $m4 \| rr \| rv$ to each tag near it.

(2) After a tag receives $m4 \| rr \| rv$, it uses its gid to generate $tm4 = hash(gid \oplus rr)$. If $m4 = tm4$ holds, it remains active. Otherwise, it becomes sleep.

(3) For the ith active tag, it generates a pseudorandom number $rt_i = prng(tk_i \oplus rr)$ and two messages $mk5_i = hash(tk_i \oplus rt_i)$ and $mid5_i = hash(tid_i \oplus rt_i)$ and sends $mk5_i \| mid5_i \| rt_i$ to the reader.

(4) The reader uses the secret information from the verifier and calculates $tmk5_i = hash(tk_i^x \oplus rt_i)$ and $tmid5_i = hash(tid_i^x \oplus rt_i)$, where $x \in \{\text{new}, \text{old}\}$ and $i \in \{1, 2, \ldots, k\}$. If $tmk5_i = mk5_i$ and $tmid5_i = mid5_i$ hold for $\forall i \in \{1, 2, \ldots, k\}$, the reader completes the first authentication to each active tag. Otherwise, the protocol fails and exits.

(5) Once the reader completes the authentication to each active tag, it begins to collect the grouping-proof evidence and enter the verification period.

The third phase completes the collection and verification of the grouping-proof evidence. It is shown in Figure 5 and is described as follows:

(1) The reader calculates $mp = hash(mk5_1 \oplus mk5_2 \oplus \ldots \oplus mk5_k)$ and broadcasts mp to each active tag.

(2) After each active tag receives mp, it signs mp with its secret key tk_i and generates $tp_i = hash(tk_i \oplus mp)$. Then it sends tp_i to the reader.

(3) After the reader receives each tp_i it calculates $p = hash(tp_1 \oplus tp_2 \oplus \ldots \oplus tp_k)$. Then it generates the grouping-proof evidence $gp = (rt_1, mk5_1, mid5_1, \ldots, rt_k, mk5_k, mid5_k, mp, p)$ and sends gp to the verifier.

(4) After the verifier receives gp, it firstly judges whether it is timeout. If it is timeout, the protocol exits. Otherwise, the protocol goes to the next step.

(5) The verifier utilizes its stored secret information about tags and the received rt_i to calculate $vmk_i = hash(tk_i^x \oplus rt_i)$ and $vmid_i = hash(tid_i^x \oplus rt_i)$ for $\forall i \in \{1, 2, \ldots, k\}$. If $vmk_i = mk5_i$ and $vmid_i = mid5_i$ hold for $\forall i \in \{1, 2, \ldots, k\}$, the verifier completes the second authentication to the verified tags and it begins to verify gp. Otherwise, the protocol fails and exits.

(6) The verifier generates $vmp = hash(vmk5_1 \oplus vmk5_2 \oplus \ldots \oplus vmk5_k)$ and calculates $vtp_i = hash(tk_i \oplus vmp)$ for $\forall i \in \{1, 2, \ldots, k\}$. Finally it generates $vp = hash(vtp_1 \oplus vtp_2 \oplus \ldots \oplus vtp_k)$. If $vmp = mp$

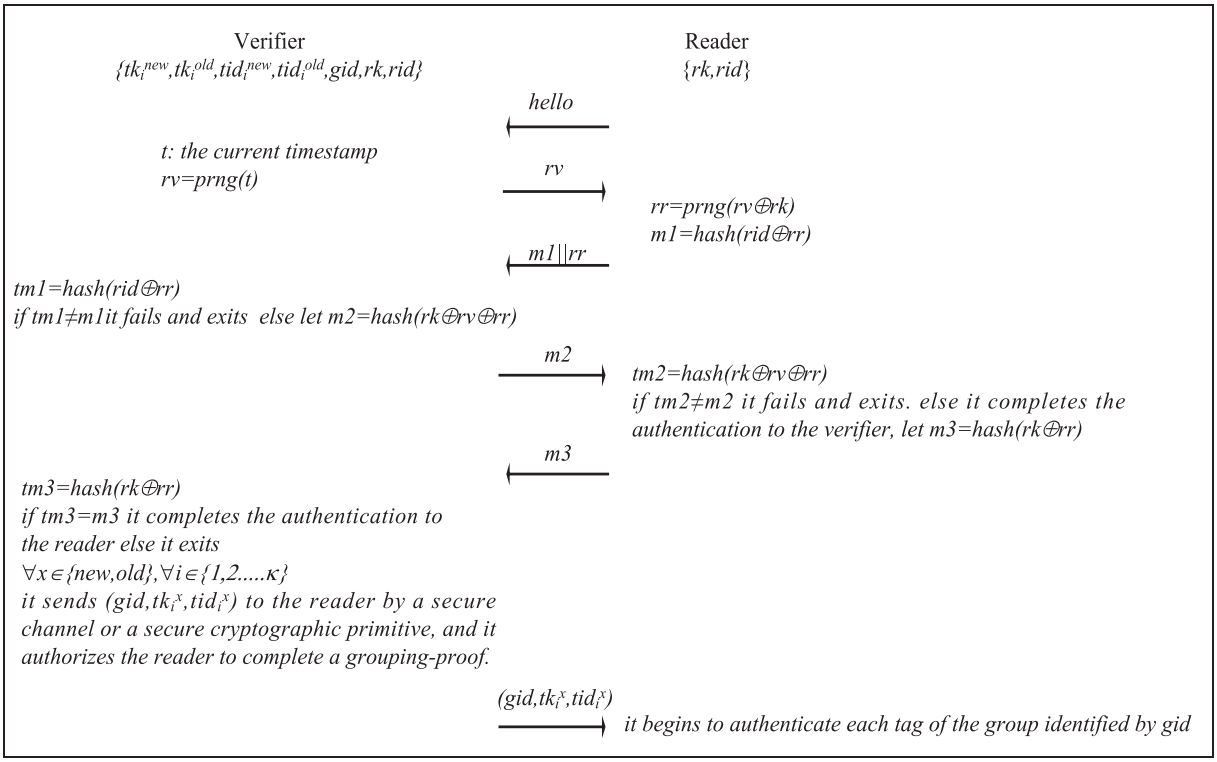


Figure 3: The authentication and authorization of the verifier to the reader.

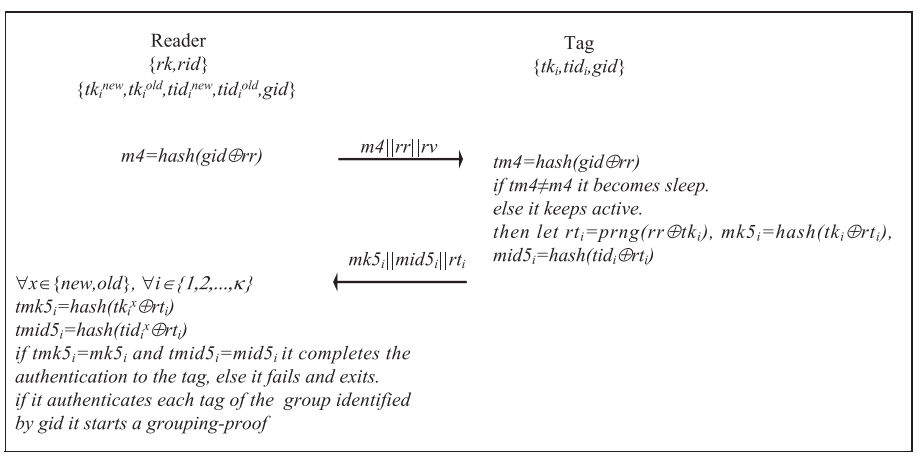


Figure 4: The reader authenticates each verified tag.

and $vp = p$ hold, the verifier gets a valid grouping-proof evidence.

(7) After the verifier verifies gp successfully, it generates the message, $m6_i = hash(tk_i^x \oplus tid_i^x \oplus rt_i)$ for $\forall i \in \{1, 2, \ldots, k\}$, and updates its secrets. If $x = \text{old}$ holds, let $tk_i^{\text{new}} = prng(tk_i^{\text{old}} \oplus rv \oplus rt_i)$ and $tid_i^{\text{new}} = prng(tid_i^{\text{old}} \oplus rv \oplus rt_i)$. If $x = \text{new}$ holds, let $tk_i^{\text{old}} = tk_i^{\text{new}}$, $tid_i^{\text{old}} = tid_i^{\text{new}}$, $tk_i^{\text{new}} = prng(tk_i^{\text{new}} \oplus rv \oplus rt_i)$, and $tid_i^{\text{new}} = prng(tid_i^{\text{new}} \oplus rv \oplus rt_i)$. Then the verifier broadcasts $m6_i \| rt_i$ to each active tag through the reader.

(8) After an active tag receives $m6_i \| rt_i$, it compares its rt_i with the received rt_i. If they are equal, the tag calculates $tm6 = hash(tk_i \oplus tid_i \oplus rt_i)$. If $m6_i = tm6$ holds, it updates its secrets: $tk_i = prng(tk_i \oplus rv \oplus rt_i)$ and $tid_i = prng(tid_i \oplus rv \oplus rt_i)$.

5. Security and Efficiency Analysis of Our Proposed Protocols

For an RFID system under the grouping-proof mode, A is assumed to be a probabilistic polynomial time adversary. He

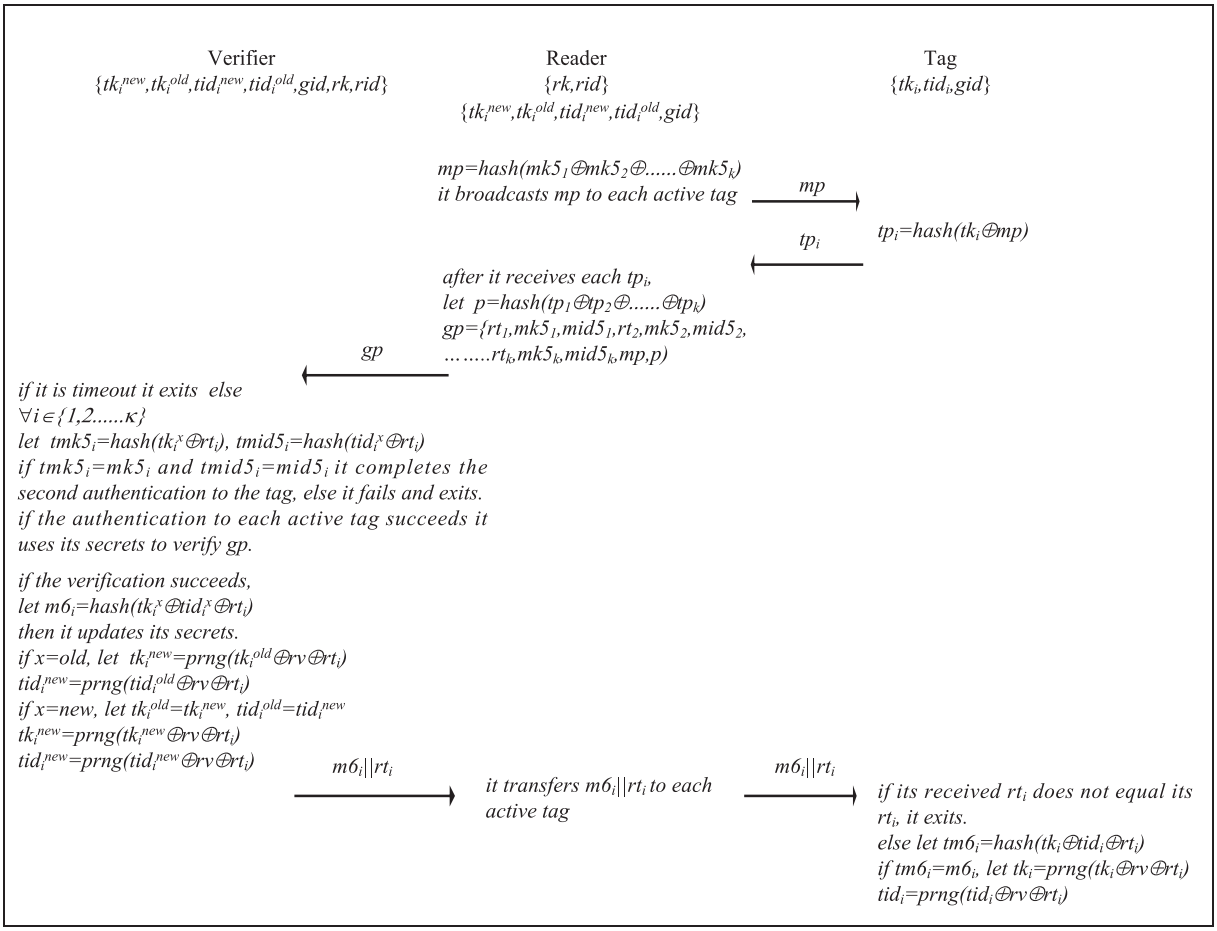


Figure 5: The generation and verification of the grouping-proof evidence.

can eavesdrop, intercept, tamper, counterfeit, and replay each session between reader and tags. He can counterfeit a grouping-proof evidence and transfer it to the verifier in limited time. If the evidence is successfully verified by the verifier, adversary A is considered to win.

Definition 1. Adversary A can continuously issue the oracle queries to $prng()$ and $hash()$. The output of $prng()$ and $hash()$ is d bits. Let σ denote the probability that the adversary guesses successfully the output of the functions. Then we have $\sigma \leq 2^{-d}$.

Definition 2. For a probabilistic polynomial time adversary A, let σ be the probability that he reveals the secret information of an RFID system. If σ is negligible the grouping-proof protocol is considered to be privacy-secure.

Definition 3. For a probabilistic polynomial time adversary A, let σ denote the probability that he distinguishes two different tags. σ is defined as follows:

$$\sigma = 2\Pr\left[tid_m = tid_n\right] - 1 \tag{1}$$

where $m \neq n$. If σ is negligible, the grouping-proof protocol is considered to be indistinguishable-secure.

Definition 4. For a probabilistic polynomial time adversary A, a grouping-proof protocol is defined to be forward-secure if and only if he cannot decrypt any previous session, although he has acquired the current secret key of the RFID system. Let σ denote the probability that he could derive the previous secret key from the current secret key of the protocol. If σ is negligible and the adversary cannot decrypt the previous sessions, the grouping-proof protocol is considered to be forward-secure.

5.1. Security Analysis to the Grouping-Proof Protocol with the Untrusted Reader. For the first grouping-proof protocol proposed by us, an untrusted reader is involved. We assume that an adversary A easily disguises a legal reader to communicate with the verifier or the tags. He can intercept each session from the RFID system, such as $m2_i \| m3_i \| rt_i$, tp_i and $m4_i \| rt_i$. On the one hand, $m2_i$, rt_i, tp_i, and $m4_i$ are four messages that include the secret key tk_i of the ith tag. Suppose adversary A intercepts these messages. Let $\varepsilon 1$ denote the probability that adversary A guesses tk_i from the messages. We have $\varepsilon 1 \leq 2^{-32} \times 4 = 2^{-30}$. On the other hand, $m3_i$ and $m4_i$ are two messages that include the identifier tid_i of the ith tag. Let $\varepsilon 2$ denote the probability that adversary A guesses

tid_i from the messages. We have $\varepsilon 2 \le 2^{-32} \times 2 = 2^{-31}$. It is obvious that $\varepsilon 1$ and $\varepsilon 2$ are negligible. It means that it is very difficult for the adversary to guess any secret information from the intercepted sessions. Therefore the protocol is privacy-secure.

For a probabilistic polynomial time adversary A, we assume that he can intercept each session from tags. Suppose the adversary intercepts $m3_m$ and $m3_n$ from the mth and n^{th} tag, where $m, n \in \{1, 2, \ldots, k\}$ and $m \ne n$. If the adversary can distinguish these two tags, his successful probability can be defined as follows [25]:

$$\Pr[tid_m = tid_n] = 2^{-1} + \varepsilon \tag{2}$$

where ε is the probability that the adversary can guess tid_m and tid_n simultaneously. By Definition 1, we have $\varepsilon \le 2^{-d} \times 2^{-d}$. When $d \ge 32$, we have $\varepsilon \le 2^{-64}$. By Definition 3, we have $\sigma = 2\Pr[tid_m = tid_n] - 1 = 2\varepsilon \le 2^{-63}$. Therefore σ is negligible. The grouping-proof protocol is indistinguishable-secure.

For our proposed grouping-proof protocol with an untrusted reader, $m2_i$, rt_i, tp_i, and $m4_i$ are four messages that include the secret key tk_i of the ith tag. Suppose adversary A intercepts these messages. Let $\varepsilon 1$ denote the probability that adversary A guesses tk_i successfully from the messages. We have $\varepsilon 1 \le 2^{-32} \times 4 = 2^{-30}$. After each successful grouping-proof, the secret key of each tag is updated by $tk_i^{\text{new}} = prng(tk_i^{\text{new}} \oplus rv \oplus rt_i)$. If the adversary wants to get the last round secret key it has to issue the oracle query to $prng()$. Suppose the adversary can deduce the last round secret key from the current secret key by querying $prng()$. His successful probability is $\varepsilon 2$. Then we have $\varepsilon 2 \le 2^{-32}$. There are two cases:

(1) The adversary does not corrupt the ith tag and it does not know the current secret key tk_i. Firstly, the adversary has to guess the current secret key from the intercepted sessions. Then he guesses the previous secret key from the guessed current secret key by issuing the random queries to $prng()$. Let $\sigma 1$ be the probability that the adversary guesses the last round secret key. We have $\sigma 1 = \varepsilon 1 \times \varepsilon 2 \le 2^{-30} \times 2^{-32} = 2^{-62}$.

(2) The adversary corrupts the ith tag and it gets the current secret key tk_i; he can guess the last round secret key only by issuing the oracle queries to $prng()$. Let $\sigma 2$ be the probability that the adversary wins. Then we have $\sigma 2 = \varepsilon 2 \le 2^{-32}$.

It is obvious that $\sigma 1$ and $\sigma 2$ are negligible. The adversary cannot guess the last round secret key from the current secret key. So he cannot reveal the previous sessions and the grouping-proof protocol is forward-secure.

5.2. Security Analysis to the Grouping-Proof Protocol with the Trusted Reader. The second grouping-proof protocol proposed by us involves a trusted reader. Under this circumstance, the verifier and the reader can use some complicated cryptographic primitives to ensure the confidential communication between them. So we assume that the communication between verifier and reader is secure. An adversary can only intercept sessions between reader and tags. If adversary A wants to guess the secret key and identifier of tags from the intercepted sessions it has to issue the oracle queries to $hash()$ and $prng()$. On the one hand, rt_i, $mk5_i$, tp_i, and $m6_i$ include the secret key tk_i of the ith tag. Let σ denote the probability that an adversary successfully guesses the secret key of the tag from these sessions and we have $\sigma \le 4 \times 2^{-32} = 2^{-30}$. It is obvious that σ is negligible. On the other hand, only $mid5_i$ and $m6_i$ include the identifier tid_i of the ith tag. Suppose an adversary can guess the identifier by issuing the oracle queries to $hash()$. Let σ be the probability that he wins by querying $mid5_i$ and $m6_i$. Then we have $\sigma \le 2 \times 2^{-32} = 2^{-31}$. It is obvious that σ is also negligible. So our proposed protocol is privacy-secure.

Adversary A can distinguish two different tags by intercepting some sessions that include the identifier of these tags. We assume that adversary A intercepts $mid5_m$ and $mid5_n$ from the mth and n^{th} tag, where $m, n \in \{1, 2, \ldots, k\}$ and $m \ne n$. If A can distinguish these two tags, his successful probability is defined by equation (2). As discussed in the last subsection, we have $\varepsilon \le 2^{-d} \times 2^{-d}$. When $d \ge 32$, we have $\varepsilon \le 2^{-64}$. By Definition 3, we have $\sigma = 2\Pr[tid_m = tid_n] - 1 = 2\varepsilon \le 2^{-63}$. So σ is negligible and our grouping-proof protocol is indistinguishable-secure.

Now we discuss the forward security of the protocol. For our proposed grouping-proof protocol with the trusted reader, rt_i, $mk5_i$, tp_i, and $m6_i$ are some sessions that include the secret key tk_i to the ith tag. Suppose adversary A can intercept these sessions. He can issue any oracle query to $hash()$ and $prng()$. $\varepsilon 1$ is the probability that he can guess tk_i from the messages described above. We have $\varepsilon 1 \le 4 \times 2^{-32} = 2^{-30}$. After each successful grouping-proof, the secret key to each tag is updated by $tk_i^{\text{new}} = prng(tk_i^{\text{new}} \oplus rv \oplus rt_i)$. If the adversary wants to get the last round secret key he has to issue the oracle query to $prng$. Let $\varepsilon 2$ denote the probability that the adversary guesses the last round secret key from the current secret key by issuing the random queries to $prng()$. We have $\varepsilon 2 \le 2^{-32}$. There exist two cases as described in the last subsection. The probability that the adversary gains the last round secret key from the current secret key is negligible. The adversary cannot guess the previous secret key from the current secret key. So he cannot decrypt the previous sessions and the grouping-proof protocol is forward-secure.

5.3. Resistance to Other Attacks. In addition to resisting the attacks described above, our proposed grouping-proof protocols can also resist eavesdropping attack, replay attack, and desynchronized attack.

(i) Eavesdropping: during the grouping-proof period, all session messages, which include the secret information of the RFID system, are generated by *hash* or randomized by *prng*. An adversary can intercept each session from the protocol. But he cannot reveal any secret information about the tag and the tag group from the intercepted sessions. Eavesdropping to the communication channels is invalid.

Table 2: The comparison of some typical grouping-proof protocols with our protocols.

Protocols	Privacy	Anonymity	Trace attack	Replay attack	Forward security	DoS attack	The number of tag groups
Ref. [2]	×	×	×	×	×	—	One (only two tags)
Ref. [15]	✓	✓	✓	✓	✓	×	One
Ref. [16]	×	×	×	✓	✓	×	Multiple
Ref. [18]	✓	✓	✓	✓	×	—	One (only two tags)
Ref. [19]	✓	✓	×	✓	×	—	One (only two tags)
Ours	✓	✓	✓	✓	✓	✓	Multiple

(ii) Interleaving and replay attack: this type of attack means that an adversary replays the grouping-proof evidence that he intercepted and the replayed evidence can be successfully verified by the verifier. The intercepted evidence may be from the same or different grouping-proof process. In order to prevent interleaving and replay attack, the clock of the verifier is utilized as timestamp and seed to generate some pseudorandom numbers. These pseudorandom numbers are different for different grouping-proof processes and they are utilized to randomize the sessions between reader and tags. On the one hand, the sessions from the same grouping-proof process can be replayed later. But they are timeout and they cannot be verified successfully. So our protocols can resist replay attack. On the other hand, the sessions from the different grouping-proof processes include the different timestamps. So they cannot be combined to construct any valid grouping-proof evidence. Hence our protocols can resist interleaving attack.

(iii) Desynchronization: in order to resist desynchronization attack, our protocols reserve the last round secrecy and the current secrecy in the verifier when the secrecy of the RFID system is updated. An adversary can tamper or block $m6_i||rt_i$ so that the tag cannot update its current secrecy. But the verifier reserves the last round secrecy and it can use this secrecy to communicate with tags. So our protocols can complete the grouping-proof regardless of whether the tag updates its current secrecy. The protocol can avoid desynchronization attack.

5.4. Analysis to the Efficiency of Our Proposed Protocols. In order to avoid the collision between tags and reduce the computing load of the RFID system, the novel activate-sleep mechanism and the special filtering operation are proposed for our grouping-proof protocols.

(i) The activate-sleep mechanism: for our protocols, maybe there exist many tag groups. Each tag group is only identified by its group identifier *gid*. Before our protocols begin to authenticate tags and generate the grouping-proof evidence, the reader sends the message $m1$ or $m4$ to each tag group so that the tags with other group identifiers become sleep. During the later period of the protocol, only the tags with the group identifier *gid* can communicate with the reader. When there exist many tag groups, the collision probability between tags is reduced remarkably. Otherwise, the reader only receives the messages from the objective group and other tag groups do not send any message to it. Its processing load is reduced efficiently.

(ii) The filtering operation: the computing ability of tags is very limited. So it is necessary to reduce the computing load of tags. For our grouping-proof protocols, the reader uses the broadcast channel to communicate with tags. But sometimes the reader sends a message only to one tag (e.g., $m6_i\|rt_i$ in Figure 5). In order to complete the peer-to-peer communication through the RFID broadcast channel, the theorem of the data link layer of Ethernet is utilized. rt_i is defined as MAC address of the ith tag. The message that is only sent to the ith tag is attached with rt_i. After a tag receives the messages, it first recognizes whether the received rt_i equals its stored rt_i. After the tag is sure that the received message is sent to it, it calls $hash()$ to calculate $m6_i$. Therefore the computing load of the tag is reduced remarkably.

The comparison of our proposed protocols with some typical grouping-proof protocols is shown in Table 2.

6. Conclusions

For some RFID applications, multiple tags are often combined together to identify a group of different objects or different parts of an object. Therefore, it is necessary to acquire the coexistence evidence of a group of tags. As an important component of an RFID system, the tags usually are some passive ones and they only have some very limited computing and memory resources. It is difficult for these tags to complete some advanced cryptographic operations. Therefore, we only use some lightweight functions and bitwise operation to propose two grouping-proof protocols. These protocols involve multiple tag groups. They efficiently use the activate-sleep mechanism and the filtering operation to reduce the collision between tags and the computing load of the RFID system. They only utilize a hash function and a pseudorandom number generator to encrypt all sessions transferred between reader and tags. This ensures the confidentiality and privacy of the RFID system. Meanwhile, our protocols use pseudorandom numbers to randomize each session of the protocols so as to resist trace attack and replay attack. After each grouping-proof, the secrecy of tags is updated and the last round secrecy of tags is preserved. Therefore, our proposed protocols provide forward security

and resist desynchronization attack. Otherwise, our protocol can complete a grouping-proof regardless of whether the reader is untrusted or trusted.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (nos. 61802252 and 61701296) and the Opening Project of Shanghai Key Laboratory of Integrated Administration Technologies for Information Security (AGK2019004).

References

[1] J. Kang, "Lightweight mutual authentication RFID protocol for secure multi-tag simultaneous authentication in ubiquitous environments," *The Journal of Supercomputing*, vol. 75, no. 8, pp. 4529–4542, 2019.

[2] A. Juels, "Yoking-proofs for RFID tags," in *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, pp. 138–143, Orlando, FL, USA, March 2004.

[3] M. Burmester, B. de Medeiros, and R. Motta, "Provably secure grouping-proofs for RFID tags," Smart Card Research and Advanced Applications, In Proceedings of the 8th IFIP WG 8.8/11.2 international conference on Smart Card Research and Advanced Applications-CARDIS'08, Springer, London, UK, 2008, pp. 176–190.

[4] P. Peris-Lopez, A. Orfila, J. C. Hernandez-Castro, and J. C. A. van der Lubbe, "Flaws on RFID grouping-proofs. Guidelines for future sound protocols," *Journal of Network and Computer Applications*, vol. 34, no. 3, pp. 833–845, 2011.

[5] J. Satio and K. Sakurai, "Grouping-proof for RFID tags," in *Proceedings of the 19th International Conference on Advanced Information Networking and Applications*, pp. 621–624, Taipei, Taiwan, March 2005.

[6] D. Sun and Z. Zhu, "Improved RFID yoking proof protocol," *Computer Engineering and Design*, vol. 38, no. 8, pp. 2076–2080, 2017, in Chinese.

[7] X. Leng, Y. Lien, K. Mayes, K. Markantonakis, and J.-H. Chiu, "Select-response grouping-proof for RFID tags," *Asian Conference on Intelligent Information and Database Systems,* pp. 73–77, IEEE Computer Society, Dong Hoi City, Vietnam, April 2009.

[8] H.-H. Huang and C.-Y. Ku, "A RFID grouping proof protocol for medication safety of inpatient," *Journal of Medical Systems*, vol. 33, no. 6, pp. 467–474, 2009.

[9] H.-Y. Chien, C.-C. Yang, T.-C. Wu, and C.-F. Lee, "Two RFID-based solutions to enhance inpatient medication safety," *Journal of Medical Systems*, vol. 35, no. 3, pp. 369–375, 2011.

[10] P. Peris-Lopez, A. Orfila, A. Mitrokotsa, and J. C. A. van der Lubbe, "A comprehensive RFID solution to enhance inpatient medication safety," *International Journal of Medical Informatics*, vol. 80, no. 1, pp. 13–24, 2011.

[11] Y.-C. Yen, N.-W. Lo, and T.-C. Wu, "Two RFID-based solutions for secure inpatient medication administration," *Journal of Medical Systems*, vol. 36, no. 5, pp. 2769–2778, 2012.

[12] H. Liu, H. Ning, Y. Zhang, D. He, Q. Xiong, and L. T. Yang, "Grouping-proofs-based authentication protocol for distributed RFID systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 7, pp. 1321–1330, 2013.

[13] J. Shen, H. Tan, Y. Wang, S. Ji, and J. Wang, "An enhanced grouping proof for multiple RFID readers and tag groups," *International Journal of Control and Automation*, vol. 7, no. 12, pp. 239–246, 2014.

[14] D. Moriyama, "Provably secure two-round RFID grouping-proof protocols," in *Proceedings of the 2014 IEEE RFID Technology and Applications (RFID-TA) Conference*, pp. 272–276, Tampere, Finland, September 2014.

[15] S. Sundaresan, R. Doss, S. Piramuthu, and W. Zhou, "A robust grouping proof protocol for RFID EPC C1G2 tags," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 6, pp. 961–975, 2014.

[16] P. Huang and H. Mu, "A high-security RFID grouping proof protocol," *International Journal of Security and Its Applications*, vol. 9, no. 1, pp. 35–44, 2015.

[17] J. Shen, H. Tan, Y. Ren, L. Qi, and D. Wang, "A practical FRID grouping authentication protocol in multiple-tag arrangement with adequate security assurance," in *Proceedings of the 2016 18th International Conference on Advanced Communication Technology*, pp. 693–699, Pyeongchang Kwangwoon Do, South Korea, January 2016.

[18] K. Hong-yan, "Analysis and improvement of ECC-based grouping-proof protocol for RFID," *International Journal of Control and Automation*, vol. 9, no. 7, pp. 343–352, 2016.

[19] L. Batina, Y. K. Lee, S. Seys, D. Singelée, and I. Verbauwhede, "Privacy-preserving ECC-based grouping proofs for RFID," *Lecture Notes in Computer Science*, vol. 6531, pp. 159–165, 2011.

[20] D. Sun and Y. Mu, "Security of grouping-proof authentication protocol for distributed RFID systems," *IEEE Wireless Communications Letters*, vol. 7, no. 2, pp. 254–257, 2018.

[21] W. Zhang, S. Qin, S. Wang, L. Wu, and B. Yi, "A new scalable lightweight grouping proof protocol for RFID systems," *Wireless Personal Communications*, vol. 103, no. 1, pp. 133–143, 2018.

[22] K.-Y. Tsai, M. Yang, J. Luo, and W.-T. Liew, "Novel designated ownership transfer with grouping proof," *Applied Sciences*, vol. 9, no. 4, p. 724, 2019.

[23] V. Cherneva and J. Trahan, "A secure and efficient parallel-dependency RFID grouping-proof protocol," in *Proceedings of the IEEE International Conference on RFID*, pp. 1–8, Phoenix, AZ, USA, April 2019.

[24] Z. Shi, X. Zhang, and Y. Wang, "A lightweight RFID grouping-proof protocol based on parallel mode and DHCP mechanism," *Information*, vol. 8, no. 3, p. 85, 2017.

[25] Y. Zhou and D. Feng, "Design and analysis of cryptographic protocols for RFID," *Chinese Journal of Computers*, vol. 29, no. 4, pp. 581–589, 2006, in Chinese.

Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 8545128, 14 pages
https://doi.org/10.1155/2020/8545128

Research Article

Calculating Trust Using Multiple Heterogeneous Social Networks

Muhammad Imran,[1] **Hasan Ali Khattak**,[1] **David Millard**,[2] **Thanassis Tiropanis**,[2] **Tariq Bashir**,[3] **and Ghufran Ahmed**[4]

[1]*Department of Computer Science, COMSATS University Islamabad, Islamabad 44500, Pakistan*
[2]*School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, UK*
[3]*Department of Electrical and Computer Engineering, COMSATS University Islamabad, Islamabad 44500, Pakistan*
[4]*Department of Computer Science, FAST National University of Computer and Emerging Sciences, Karachi, Pakistan*

Correspondence should be addressed to Muhammad Imran; mimran@comsats.edu.pk and
Hasan Ali Khattak; hasan.alikhattak@comsats.edu.pk

Received 20 November 2019; Accepted 24 January 2020; Published 21 February 2020

Academic Editor: Nathalie Mitton

In today's Internet, a web user becomes members of multiple social networks due to different types of services provided by each of these networks. This creates an opportunity to make trust decisions that go beyond individual social networks, since these networks provide single perspective of trust. To make trust inference over multiple social networks, these networks need to be consolidated. It is nontrivial as these networks are of heterogeneous nature due to different naming conventions used in these networks. Furthermore, trust metrics extracted from these networks are also varied in nature due to different trust evaluation algorithms used in each of these networks. Heterogeneity of these social networks can be overcome by using semantic technologies as it allows us to represent knowledge using ontologies. Trust data can be consolidated by using such data fusion techniques which not only provide but also preserve trust data integrity from each of the individual social network profiles. The proposed semantic framework is evaluated using two sets of experiments. Through simulations in this work, we analysed various techniques for data fusion. For identifying suitable technique that preserves the integrity of trust consolidated from each of the individual networks, analysis revealed that Weighted Ordered Weighted Averaging parameter best aggregated trust data, and, unlike other techniques, it preserved the integrity of trust from each individual network for varying participant overlap and tie overlap ($p \leq 0.05$). Similarly, for experimental analysis, we used findings of the simulation study about the best trust aggregation technique and applied the proposed framework on real-life trust data between participants, which we extracted from pairs of professional social networks. Analysis partially proved our hypothesis about generating better trust values from consolidated multiple heterogeneous networks. We witnessed an improvement in overall results for all the participants who were part of multiple social networks ($p \leq 0.05$), while disproving the claim for those existing in nonoverlapping regions of the social networks.

1. Introduction

At present, online social networks (OSNs) replace real-world social networks, where people interact with each other remotely [1, 2]. Due to these social networks, several interactions and activities that required physical interaction are conveniently possible now while sitting at distant locations through World Wide Web. A survey conducted by Pew (https://www.pewresearch.org/internet/fact-sheet/social-media/) in February 2019 about the use of online social networks in the US disclosed that adult web users account for 72% of utilizing online social networks for online interaction [3]. The same survey also revealed statistics about the use of multiple social networks. It stated that 56% of online adults use more than one social network, wherein 95% of Twitter users and 92% of LinkedIn users also use Facebook. It indicates the increasing trend of using multiple social networks due to the different nature of services provided by these networks. We describe this situation as individuals belonging to multiple heterogeneous (MuHe) social networks; "multiple" because there is

more than one network structure, and "heterogeneous" because the networks represent different types of relationships. MuHe networks usually are made up of networks owned and managed by various organizations, so, typically, users have different virtual identities in each system.

The researchers have developed a range of trust algorithms for individual social networks [4, 5]. These examine personal information and interaction history of the users to calculate trust metrics in their respective networks. Such mechanisms have become essential features for some successful social networks; for example, the eBay (http://www.ebay.com) network evaluates the reputation of sellers based on the ratings of buyers, which helps it to ensure high standards of online shopping. Similarly, expertise recommendation mechanism in the LinkedIn (http://www.linkedin.com) network uses recommendations provided by other professionals in the network, which are of great help for new users.

There are several definitions of trust in the literature, but we have taken the definition as given by [6] as it is both general and concise: "*Trust of party X to a party Y for a service A is a measurable belief of X in that Y behaves dependably for a specified period (and within a specified context in relation to service A)*" [3].

OSNs may be categorised based on the services provided by these networks such as friendship networks, professional networks, and e-commerce networks. When considered in context of trust, these networks represent multifaceted information which may be helpful if trust is to be modelled for multiple networks. However, existing trust mechanisms tend to be restricted to a single network, whereas users are typically involved in MuHe networks. Basing trust decisions on MuHe networks would have two distinct advantages: (1) it increases the chance of calculating a trust value, as individuals need not share the same network, and (2) it bases trust values upon diversified information that can reflect accurately a user's behaviour on multiple social networking platforms. Our definition of trust notes that trust is calculated in a specific content, and therefore we expect that MuHe networks will be related to a particular trust domain (such as professional networks) rather than a general aggregation of all these networks in which individuals are present.

Unfortunately, the task of linking multiple social networks to generate a single big social network for performing trust calculations is not trivial, the reason being varying structures of the networks and weights on the links between professionals on these diverse networks [7, 8]. The aggregation mechanism should not inflate or dampen trust values artificially based on the availability of information from either some or all of the constituent networks. It should be able to particularly differentiate between *absence of trust* and *distrust* as unavailability of information from certain networks does not mean distrust.

This paper proposes a novel framework for performing trust calculations on MuHe networks. The framework is based on semantic web technology and uses data fusion techniques such as Weighted Ordered Weighted Averaging to aggregate individual networks without distorting trust values. We then present two evaluations of this framework. The first uses a simulation environment to look at the impact of consolidating two networks on their trust properties (strength of trust ties and length of trust path); based on this simulation, we then select the most appropriate data fusion technique. The second uses the proposed framework and this chosen technique to conduct a comparative evaluation of trust calculations based on existing single social networks against those based on MuHe networks. It uses real-world trust values elicited from participants as the gold standard.

The remainder of the paper is structured as follows: the related work about semantic web, data fusion, and online trust is described in Section 2. Section 3 presents the proposed semantic web framework and gives an overview of the data fusion techniques. It further describes the characteristics by which different data fusion techniques can be compared. Section 4 presents the simulation experiment and justifies the choice of data fusion technique. Section 5 presents the real-word experiment that compares trust values calculated using existing single networks to those calculated using MuHe networks. Finally Section 7 presents potential future extensions and concludes the paper.

2. Related Work

There are various studies reported in the literature, which attempt to consolidate multiple social networks, but they merely focus on combining these networks rather than exploring their impact on trust-related measures. For example, the work in [9] attempts to merge trust and distrust relations from multiple trust networks but lacks two dimensions; first, it fails to differentiate between distrust and absence of trust, and, second, the impact of that consolidation on the accuracy of trust metrics is not examined [3].

In semantic web, the concept of coreference resolution resolves the problem of users having distinct identities in multiple social networks. There are many existing methods that address this issue such as [10], which discusses two methods of URI coreference resolution: (1) logical inference and (2) label comparison. Logical inference matches IFPs (Inverse Functional Properties) to evaluate whether a pair of URIs are coreferred, while label comparison compares data properties to classify URI pairs as coreferred or non-coreferred URIs. The URIs classified as coreferred may be linked using the predicate owl:sameAs provided as part of the OWL DL specification in the semantic web [11, 12]. Trust data can be annotated using either of the URIs defined in the existing network or by using afresh generated URI using the target namespace [13]. The resultant annotated information in the MuHe environment may be published as a separate named graph [14]. It helps those reusing the data to scope down their queries to target graph rather than writing long query patterns over existing graphs.

Multiple trust values emerge between coreferred users when MuHe networks are consolidated. These trust values represent subjective trust in the context of a particular network. While integrating these values, the data fusion algorithm should respect the trust integrity of these social networks. A number of data fusion techniques exist in the

state-of-the-art literature such as [15], where the authors have proposed an aggregation operator based upon Ordered Weighted Averaging (OWA), which takes into account the multiple trust values based upon relative importance by ranking data values in descending order. Similarly, another technique, WOWA, proposed by [16] considers importance of both data and their sources. IOWA behaves similar to WOWA but allows ranking data points with respect to different trust sources [17, 18].

Furthermore, there are different implementations in the literatures that have used these techniques for aggregating trust. For example, the work in [19] collects trust scores between any two users from multiple paths in a single network and aggregates them using different data fusion techniques. This scenario is similar to consolidating trust metrics from multiple social networks. The results of the knowledge awarding-OWA (K-OWA) and knowledge awarding-averaging (KAAV) approaches showed better performance when compared with other techniques. Similarly, [20] presents aggregation techniques used for generating trust scores over transitive triads in a realistic fashion. Advanced deep learning techniques have been used in order to perform recommendation based upon trust score in social networks [21].

Consolidation of MuHe networks also helps to discover links among isolated users. This emanates the scenario of quantifying indirect trust and trust decay is one of the approaches discussed in the literature. Trust decay uses the principle of trust transitivity and was first discussed by a psychologist to analyse the existence of transitivity in real-world social networks [22]. The experiment was conducted to test the transitivity of positive interpersonal sentiments. This work was later extended by social psychologists to examine this in terms of social relations by running an experiment over a set of 917 sociograms [23]. A random group of people were asked about their sentiments towards other people in the group. They found that in 70% of the cases there was a strong inclination towards the transitivity.

A number of trust algorithms are developed using the concept of trust decay; for example, [24] proposed an approach for trust and distrust propagation, "*Appleseed*," which uses the theory of spreading activation [25]. According to that, trust or distrust in a friend flows along all paths leading from the friend. They chose a realistic decay factor based on the empirical experiment and a normalised local edge weight, $e_{x \longrightarrow y}$, is assigned to each link in the network. The work in [26] uses reinforcement learning for calculating local trust values in social networks. The trust from the source is propagated towards the destination using different strategies. Experimental results revealed that the hybrid approach of weighted mean aggregation and min-max over shortest paths turned out to be the best approach. Similarly, [27] presents an idea of incorporating multiple trust paths of varied lengths for enhancing accuracy of trust calculations. The decay of trust is considered and trust is calculated for both shortest and longest trust paths. Results showed that shorter paths generate more accurate trust measures than longer paths. The method proposed in [28] extracts domain-specific trust network from large-scale heterogeneous network, with the claim that trust propagation is a domain-dependent phenomenon and cannot work through heterogeneous relations [3]. Another study elaborates trust decay as a function of leakage in network flow and proposed network flow based trust evaluation scheme *GFTrust* [29]. The work carried out in [30] develops an algorithm for Trust Path Searching (TPS) to evaluate trust for indirectly connected users using the principle of trust transitivity. The research conducted in [31] summarizes different trust decay methods used by the literature and provides comparative analysis of these techniques.

3. Proposed Semantic Web Framework

The proposed framework uses semantic web technology to model constituent networks in uniform format and then allows different data fusion techniques to be used to integrate them. The key idea behind semantic web is that each resource should have a unique identifier (URI), but, in practice, different online networks have different namespaces for knowledge representation. Resultantly, individuals have multiple URIs across MuHe social networks. The proposed framework should resolve multiple URIs, which refer to the single user in the real life. Further, it should provide a mechanism to aggregate multiple trust values that originate between users due to their existence in MuHe networks.

The MuHe consolidation framework is shown in Figure 1, which presents our solution for building trust applications over multiple distributed social networks. The experimental setup to test the feasibility of framework for linking multiple networks resides on top of the Sesame triplestore (http://rdf4j.org/). A number of preprocessing modules are written in Python (https://www.python.org/), which gather data from multiple sources (including local RDF files, local and remote triplestores) and convert them into a single semantic representation for consolidation. They then apply different trust evaluation algorithms for calculating trust metrics for both directly and indirectly connected users.

The first module, named *Data Acquisition Module*, uses Python SPARQL wrapper classes (http://rdflib.github.io/sparqlwrapper/) for extracting RDF data between users from MuHe networks. It particularly targets information that can help in building linked networks with nodes of the network representing people and weights on the links show trust ranks between them.

The remaining three modules are more complex and are described in the following subsections.

3.1. Coreference Resolution Module. The coreference module locates different URIs from MuHe networks (defined in different ontologies) that represent the same person and allows us to generate afresh URI from the target namespace (defined in our own ontology). The resultant annotations may be added as a separate graph linked with existing graphs using *owl:sameAs* predicates. The concept of named graph [14, 32] is helpful when consolidating MuHe Networks. It

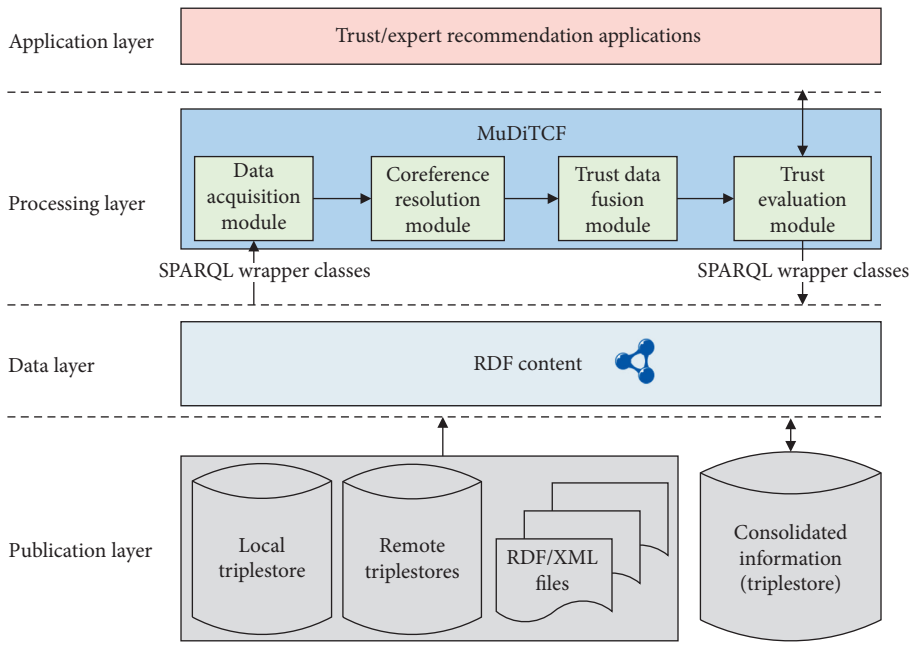


Figure 1: A semantic web framework for building trust applications over MuHe social networks.

allows us to represent consolidated networks as a separate layer built over existing graphs acting as an overlay network. The sample representation of such a network is shown in Figure 2. The individual networks layer represents two publication networks, where square shapes represent publications, while researchers are depicted using oval shape. This layer is linked with existing published information using *owl:sameAs* statements specifying which of the URIs in the consolidated network correspond to URIs in each of the individual networks. Once published, this eliminates the need to write long query patterns over individual networks for coreferencing or retrieving trust information between users.

The intuitive way to identify coreferred users from these networks is to compare metadata. In semantic web, this information can be extracted from *owl:DP* (data property) predicates. Equation (1) provides a rule to perform coreference resolution for two URIs: *?1* and *?a*. Here, *?1* and *?a* are URIs in individual networks and *?1a* is the newly allocated URI in the aggregated single network. *?p* represents the set of data properties selected for comparison. If both data properties hold the same values for both the URIs, *?1* and *?a*, then they are resolved to represent the same person in multiple networks and the resultant URI may be *?1a* in the consolidated version of these networks. Further, it can be linked with both *?1* and *?a* in individual networks using *owl: sameAs* predicate, thereby stating that both URIs are the same. Note that the numeric value *?1* and a character *?a* in individual networks and *?1a* in consolidated version are shorthand of the original URIs.

$$\{?p \;\; a \;\; owl{:}\, DP\,.\;\; ?1 \;\; ?p \;\; ?x.\;\; ?a \;\; ?p \;\; ?x.\} \Longrightarrow \begin{cases} ?1a\, owl{:}\; sameAs \quad ?1. \\ ?1a\, owl{:}\; sameAs \quad ?a. \end{cases} \tag{1}$$

An ontology is needed for making annotations in the consolidated graph. Figure 3 presents the classes and properties defined in the proposed ontology. It extends existing ontology given in [33] and adds object and data properties, which are particularly needed for annotating trust in the context of MuHe networks. The single new class TrustRelationship defines the trust relationship between instances of trustor and trustee classes using has_trustor and has_trustee properties. The trustor class holds the identity of trustor, while the trustee class represents the person being trusted by the trustor. Both the trustor and trustee are persons, so their URIs are generated using person class of the *FOAF* namespace.

The ontology allows us to model trust in three different formats: absolute, processed, and fuzzy. Absolute trust is the subjective trust value extracted from any particular network. For example, consider the example of a publication network, where trust between researchers is measured in terms of coauthorship frequency; in this case, absolute value is the count of the number of times that a pair of researchers have appeared in publications together. Processed value in this context is an absolute value normalised in the range between 0 and 1. It is a translated value that transforms trust from multiple contexts into a format that can be compared or combined. Fuzzy trust is the human understandable version of numerical trust values such as high trust and medium

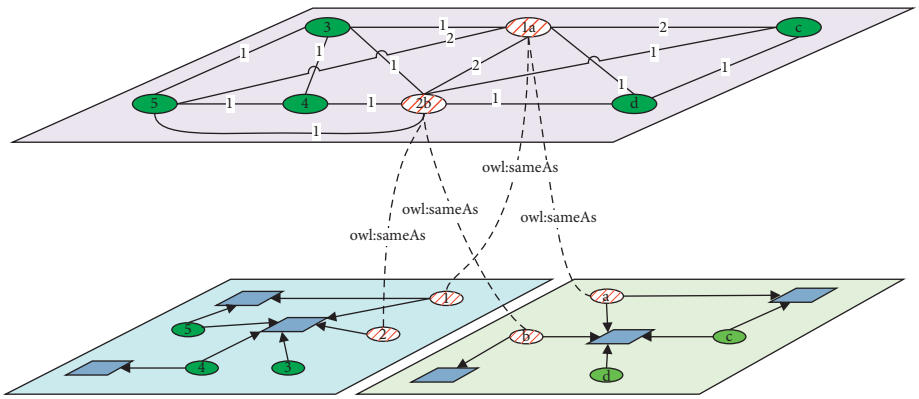


Figure 2: Linked trust graph shown as an overlay network over individual networks. *owl:sameAs* predicates are used to corefer newly assigned URI in overlapping region of consolidated graph to individual graphs.

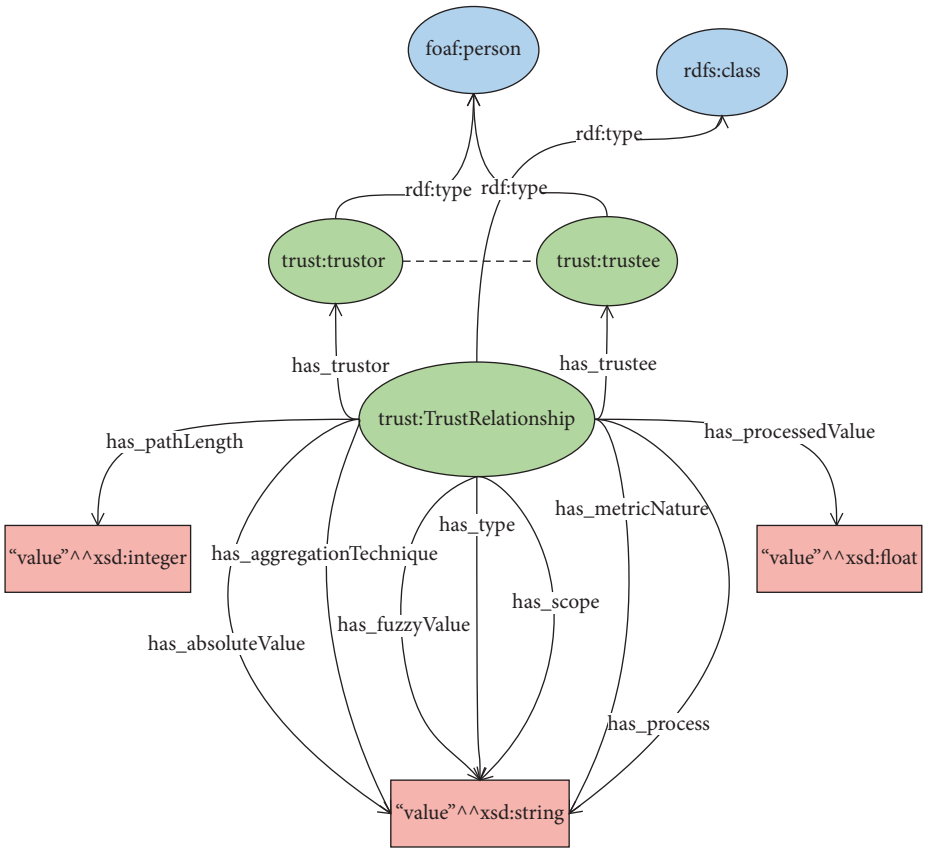


Figure 3: Trust ontology for trust over MuHe social networks.

trust. There are various techniques of modelling fuzzy trust; however, trust modelling using fuzzy logic is out of the scope of this work.

Trust in MuHe social networks can be viewed as a set of direct experiences from multiple social networks or recommendations provided by other members of those networks. In our ontology, it is modelled using has_type data property, where the *domain* of the property is the URI of the relevant person and *range* is the string value of "direct" or "indirect." The direct trust is extracted based on the direct interactions (which can be either of the explicit or implicit activities), whereas indirect trust is calculated between isolated users, typically belonging to multiple social networks. There are various methods of calculating indirect trust, so the has_process object property records the technique used and the has_pathLength object property stores the length of the trust path involved.

The trust definition used in this work takes it as a subjective value, so the has_scope data property specifies the area that any particular trust value belongs to. It is particularly important when trust data only related to certain area needs to be consolidated such as if the system has to aggregate trust information about trusted academics in the fields of semantic web, machine learning, and so forth.

The outcome of the coreferencing technique is a linked network having consolidated URIs for overlapped users and multiple trust values between them extracted from MuHe networks. The next step is to combine these multiple trust values into a single one, using the data fusion technique. The ontology must therefore also record this process, which is modelled using two properties: has_metricNature and has_aggregationTechnique. The former defines whether the target pair of users were *overlapping* or *nonoverlapping*, therefore having to establish whether there are multiple values to aggregate or only a single value to be reevaluated. The later one stores the name of the data fusion technique used to aggregate if multiple trust values are present or reevaluate if only singular value is available.

3.2. Trust Data Fusion Module. Data fusion module aggregates trust values between users belonging to multiple social networks and generates a single value that represents multifaceted trust. The task of consolidating multiple trust relationships is basically a data fusion problem and particularly it may be considered as a data aggregation case study. One of the simplest approaches is to perform summation (S) or an average (A) of the trust values. This may work for simple numerical quantities, but in the case of trust it could damage trust values by either inflating them unnecessarily (through summation) or deflating them drastically (as some of the trust values may be effectively zero due to missing information from some of the networks being consolidated). Therefore, more comprehensive techniques are needed to aggregate trust values because they represent trust in varied context and naive methods of aggregation can distort the integrity of trust.

The trust metrics between a pair of users can range from *one* to the n number of networks involved in consolidation. Suppose that N_p represents a pair of users from multiple social networks and T_{N_p} is the set of trust values between them from n social networks; i.e., $T_{N_p} = \{T_{N_p1}, T_{N_p2}, \ldots, T_{N_pn}\}$. There are two parameters involved in trust aggregation: (1) importance of the trust values from individual social networks, denoted as $\omega = \{\omega_1, \omega_2, \ldots, \omega_n\}$, and (2) importance of the sources of that information, denoted as $p = \{p_1, p_2, \ldots, p_n\}$. The values of both parameters stay in the range of [0, 1], where zero value shows low importance, while a value of *one* represents higher importance. The function $f(T_{N_p})$ aggregates these values and generates a single value T^{N_p} by considering ω_i and p_i for each T_{N_pi} in the dataset T_{N_p}.

There are various data fusion techniques discussed in the literature and Section 2 presents their detailed background. A richer description of these methods can be found in [34], which reported on a subset of the simulation experiment but the full experiment focused on the following, all of which have been implemented within the data fusion module:

Weighted Average (WA) technique consolidates multiple trust values by only considering the importance of data sources. The individual trust data points in T_{N_p} are aggregated by multiplying them with the weights of the corresponding sources. The importance of each source network is represented using a weight vector p, and its size is equal to the number of trust values.

Ordered Weighted Averaging (OWA) works in a similar way to WA instead of the weights being associated with a given source, the sources are ordered (according to which is most trusted) and the weight is associated with the position within the ordering. The trust data points in T_{N_p} are sorted in an order from high to low; then already permuted trust values are multiplied with the corresponding weights from the weight vector w to generate a single aggregated value T^{N_p}.

Weighted Order Weighted Average (WOWA) associates importance parameters to both source and the order of the trust values. It takes two sets of weights other than the set of trust values T_{N_p}: first is the weight vector w that shows the importance of trust data points; and second is the weight vector p to show the relevancy of the sources of trust information. The vector w can have both integer and fraction values, while T_{N_p} and p vectors are continuous values in the range of [0, 1].

3.3. Trust Evaluation Module. The trust between isolated users is calculated using trust propagation algorithm. It works on the principal of transitivity and existing studies (mentioned in Section 2) empirically prove that trust decreases as the length of path between indirectly connected users increases. In short, people, in both real life and online social networks, have high degree of trust towards friends of their friend rather than strangers, but this trust decreases as the length of trust path increases. Drawing on this knowledge, we have used a transitive decay-based trust calculation within the module.

The first step is to calculate all possible trust paths between any two users; the trust value associated with a given path is the result of multiplying all the trust values (in between [0, 1]) between all the nodes in that path. There are then two possible options for choosing the trust path. The first is the strongest path where the algorithm returns the trust path having the maximum strength of the trust ties between users without considering its length, that is, the number of users involved in the path. The second is the shortest path, which chooses the path with the shortest length, regardless of its trust value. However, if multiple trust paths of the same shortest length exist, then the one with the highest trust value is chosen. In this work, we have used the shortest path approach for experimentation, while the strongest path approach is already published in [34].

4. Experiment 1: Simulation Experiment for Trust Inference over Consolidated MuHe Social Networks

The simulation experiment discussed in this paper is an extension of the works described in [3, 34] and it further extends these works to include the OWA data fusion method

and shortest trust path algorithm. The simulation examines the impact of the consolidation of MuHe networks on trust properties used by the shortest trust path algorithm (described in Section 3.3 above). The simulation is based around a consolidation of pairs of networks, using four data fusion techniques starting from naive ones such as summation (S) and weighted average (WA) and then extending up to more complex techniques such as Weighted Ordered Weighted Averaging (WOWA) and Ordered Weighted Averaging (OWA). The technique that best satisfies trust properties qualifies to be used for making trust computations over real-world data. Both the simulation and real-world experiments are implemented using the NetworkX (http://networkx.github.io/documentation/latest/reference/introduction.html) library of the Python programming language. It includes the code for generating networks, consolidation them, measuring network properties, and applying trust inference algorithms.

4.1. Experiment Design. The pairs of social networks were generated, with randomly assigned trust values on the links between users, having a varying percentage of participant overlap (PO) and tie overlap (TO) in each pair of networks. It was to assess the values of trust properties when the networks with varying percentage of overlaps were consolidated. N1 and N2 represent the original networks generated by the simulation; MuHe was the final linked network, while CN1 and CN2 represent subnetworks in the MuHe mapped to N1 and N2. We can then see the impact of consolidation by comparing CN1 to N1 and CN2 to N2.

The impact of consolidation on trust properties is measured using the approximation of two metrics: average tie strength (TS) and average tie length (TL). TS is the average trust of the network using shortest trust paths, and TL is the average length of the shortest trust paths in the network. Ideally, TS metric from CN1 and CN2 and MuHe should be similar to that of N1 and N2, even if there are no significant PO and TO. This indicates that trust is not being inflated in the consolidation process. Furthermore, it is desirable that, due to the emergence of additional trust paths, TL metric be overall decreased in CN1 and CN2 and MuHe as compared to N1 and N2. If TS remains steady and TL reduces, it may be deduced that the consolidation has successfully enhanced trust calculations by opening up new trust paths without escalating trust values in the network. More formally, we can say that any data fusion technique chosen for trust should satisfy the following set of propositions (adapted from [15–17]).

Proposition 1 (boundary conditions). *The trust aggregation function should keep consolidated trust value within the maximum and minimum range.*

$$\min\left\{T_{N_p1}, T_{N_p2}, \ldots, T_{N_pn}\right\} \le f\left(T_{N_p1}, T_{N_p2}, \ldots, T_{N_pn}\right) \le \max\left\{T_{N_p1}, T_{N_p2}, \ldots, T_{N_pn}\right\}. \quad (2)$$

Proposition 2 (idempotence). *The resultant value of trust aggregation function should be equal to T_{N_p1} if all the trust values are the same; that is, $x \in T_{N_p}$.*

$$f\left(T_{N_p1}, T_{N_p1}, \ldots, T_{N_p1}\right) = T_{N_p1}. \quad (3)$$

Proposition 3 (monotonicity). *The trust aggregation function should be monotonic, which means that it should generate high aggregated trust for high trust values as compared to low trust values.*

$$f\left(T_{N_p1}, T_{N_p2}, \ldots, T_{N_p1}\right) \ge f\left(T_{N_q1}, T_{N_q2}, \ldots, T_{N_qn}\right), \quad \text{if } T_{N_pi} \ge T_{N_qi}, \text{for } i = \{1, 2, \ldots, n\}. \quad (4)$$

The final property, known as *Trust Absence*, ensures the integrity of trust from individual networks. It refers towards the missing trust information from any of the constituent networks and recommends to consider it as the absence of trust and not distrust between individuals.

Proposition 4 (trust absence). *The trust aggregation function should differentiate between absence of trust and a distrust. The numeric value of zero, in this study, represents absence of trust information from either of the individual networks, so their aggregate should generate trust value that is approximately similar to the one generated without that numeric zero.*

$$f\left(T_{N_p1}, 0, \ldots, T_{N_pn}\right) \approx f\left(T_{N_p1}, \ldots, T_{N_pn}\right). \quad (5)$$

This simulation generates networks for four different participant overlap (PO) percentages, that is, 40%, 60%, 80%, and 100%, and then for each value of PO (except 40% PO) TO is varied from 0 to PO in increments of 20%. In each of the simulations, trust information on the links is aggregated using different aggregated schemes named S, WA, WOWA, and OWA. Table 1 provides details about network and consolidation parameters used in this simulation.

4.2. Results and Analysis. In our analysis, we considered the impact of consolidation on both average strength of trust ties (TS) and average length of trust path (TL). These are discussed separately in the following sections.

4.2.1. Average Strength of Trust Ties. The results in Table 2 present the values of TS metric for varying consolidation parameters PO and TO using the shortest path algorithm. It shows that the TS metric using WOWA approach has more stable measurements for CN1, CN2, and MuHe than all the other approaches (S, WA, and OWA). Simple techniques S and WA severely distort TS metric for two extreme values, that is, at 100% PO and 100% TO, with a value of 0.93, and at 40% PO and 0% TO, it stood at 0.17. Similarly, OWA also performs

Table 1: Network and consolidation parameters used for this study.

	Description
Network parameters	
Number of nodes	30
Density of networks (D)	0.43
Averaging clustering coefficient of networks (C)	0.45 ± 0.02
Average length of shortest paths in networks (L)	1.57
Ratio of C, D, and L between N1 and N2	1
Consolidation parameters	
Participant overlap (PO)	[40%, 100%]
Tie overlap (TO)	[0, PO]

Table 2: TS for shortest path trust evaluation algorithm using four different data fusion techniques with varying percentage of participant overlap and tie overlap. CN1 and CN2 represent original networks N1 and N2 in the consolidated version of MuHe networks.

PO	TO	N1	N2	Average strength of ties in the network (TS)											
				CN1				CN2				MuHe			
				S	WA	WOWA	OWA	S	WA	WOWA	OWA	S	WA	WOWA	OWA
40	0	0.53	0.55	0.56	0.21	0.48	0.44	0.58	0.21	0.50	0.17	0.52	0.17	0.44	0.22
	20	0.52	0.55	0.59	0.24	0.47	0.39	0.64	0.26	0.52	0.15	0.54	0.19	0.44	0.19
	30	0.55	0.52	0.66	0.26	0.52	0.42	0.61	0.25	0.49	0.14	0.55	0.19	0.44	0.20
60	0	0.58	0.55	0.61	0.23	0.53	0.51	0.60	0.23	0.52	0.28	0.58	0.20	0.49	0.30
	20	0.55	0.58	0.65	0.27	0.53	0.39	0.67	0.27	0.55	0.19	0.62	0.23	0.51	0.24
	40	0.55	0.54	0.68	0.30	0.54	0.42	0.66	0.29	0.53	0.21	0.61	0.24	0.49	0.25
	60	0.46	0.55	0.63	0.29	0.48	0.37	0.73	0.32	0.56	0.23	0.61	0.23	0.46	0.23
80	0	0.56	0.54	0.59	0.24	0.51	0.50	0.59	0.25	0.52	0.38	0.59	0.23	0.51	0.38
	20	0.61	0.56	0.69	0.29	0.57	0.39	0.67	0.29	0.55	0.27	0.67	0.27	0.55	0.30
	40	0.57	0.60	0.74	0.34	0.59	0.42	0.75	0.34	0.59	0.30	0.71	0.31	0.57	0.32
	60	0.55	0.54	0.76	0.38	0.57	0.45	0.76	0.38	0.57	0.34	0.70	0.32	0.53	0.33
	80	0.50	0.53	0.74	0.38	0.55	0.44	0.78	0.39	0.58	0.37	0.69	0.32	0.51	0.32
100	0	0.58	0.56	0.59	0.27	0.53	0.53	0.59	0.27	0.53	0.53	0.59	0.27	0.53	0.53
	20	0.54	0.53	0.64	0.29	0.54	0.32	0.64	0.29	0.54	0.32	0.64	0.29	0.54	0.32
	40	0.55	0.59	0.72	0.34	0.59	0.37	0.72	0.34	0.59	0.37	0.72	0.34	0.59	0.37
	60	0.52	0.55	0.77	0.38	0.59	0.40	0.77	0.38	0.59	0.40	0.77	0.38	0.59	0.40
	80	0.57	0.58	0.87	0.46	0.65	0.48	0.87	0.46	0.65	0.48	0.87	0.46	0.65	0.48
	100	0.58	0.52	0.93	0.50	0.66	0.53	0.93	0.50	0.66	0.53	0.93	0.50	0.66	0.53

poorly for low participant and tie overlap and its value for MuHe at 40% PO and 0% TO dropped to 0.22. The TS metric recorded by WOWA approach remained stable throughout varying values of PO and TO and it stood at 0.66 for 100% PO and 100% TO and 0.44 for 40% PO and 0% TO. Based on the results of all the data fusion techniques, WOWA appears to be the better technique for aggregating trust information.

The statistical significance of the apparent preservation of trust integrity by WOWA is assessed using a two-tailed paired t-test. It evaluates whether the results of WOWA approach are significantly better than those of the other two techniques. This test generates a p value and a value of $p \leq 0.05$ indicates significance. Table 3 shows p values for two types of participant overlaps (PO); the first four rows show p values for varying percentage of PO, while the last measurement, that is, *overall*, shows the collective performance of the system by including TS metrics for all percentages of PO. The analysis of the p values reveals that the claim of WOWA being better than the other two techniques, WA and IOWA, is statistically significant and holds true for all values of PO.

4.2.2. Average Length of Trust Ties (TL). Table 4 presents the results of the TL metric for varying percentages of PO and TO using the shortest path trust algorithm. It shows that the values of TL metric for CN1, CN2, and MuHe are the same for similar participant and tie overlaps across all the data fusion techniques. For subnetworks CN1 and CN2, it decreases with the increase in PO and TO due to emergence of new trust paths, but, for MuHe, it only decreases when PO $\geq$ 80 and then it starts increasing again with an increase in TO. The reason is that less value of participant overlap between the networks creates bottleneck due to more number of nonoverlapping nodes, which results in longer trust paths between users. This trend reduces when the value of PO increases. When compared with original networks $N1$ and $N2$, both have an average length of trust paths (TL) of 1.57; TL is higher (i.e., 1.69) than both the original networks when the participant overlap and tie overlap are 40% and 0%, respectively. It becomes even higher (i.e., 1.79) when the value of PO and TO reaches 60%. The number of new shortest paths becomes

Table 3: t-Test results (p value) between corresponding TS metrics of WOWA and WA, OWA for shortest path algorithm.

PO (%)	WA			OWA		
	CN1	CN2	MuHe	CN1	CN2	MuHe
40	< 0.010	< 0.010	< 0.010	0.050	< 0.010	< 0.010
60	< 0.010	< 0.010	< 0.010	0.040	< 0.010	< 0.010
80	< 0.010	< 0.010	< 0.010	0.020	< 0.010	< 0.010
100	< 0.010	< 0.010	< 0.010	< 0.010	< 0.010	< 0.010
Overall	< 0.010	< 0.010	< 0.010	< 0.010	< 0.010	< 0.010

Table 4: TL for shortest path trust algorithm using four different data fusion techniques with varying percentage of PO and TO. CN1 and CN2 represent original networks N1 and N2 in the consolidated version of MuHe networks.

PO	TO	Average length of trust paths (TL)													
		N1	N2	CN1				CN2				MuHe			
				S	WA	WOWA	OWA	S	WA	WOWA	OWA	S	WA	WOWA	OWA
40	0	1.57	1.57	1.52	1.52	1.52	1.52	1.50	1.50	1.50	1.50	1.69	1.69	1.69	1.69
	20	1.57	1.57	1.56	1.56	1.56	1.56	1.54	1.54	1.54	1.54	1.76	1.76	1.76	1.76
	30	1.57	1.57	1.57	1.57	1.57	1.57	1.57	1.57	1.57	1.57	1.79	1.79	1.79	1.79
60	0	1.57	1.57	1.44	1.44	1.44	1.44	1.43	1.43	1.43	1.43	1.57	1.57	1.57	1.57
	20	1.57	1.57	1.48	1.48	1.48	1.48	1.50	1.50	1.50	1.50	1.62	1.62	1.62	1.62
	40	1.57	1.57	1.53	1.53	1.53	1.53	1.53	1.53	1.53	1.53	1.68	1.68	1.68	1.68
	60	1.58	1.58	1.55	1.55	1.55	1.55	1.56	1.56	1.56	1.56	1.79	1.79	1.79	1.79
80	0	1.57	1.57	1.33	1.33	1.33	1.33	1.30	1.30	1.30	1.30	1.41	1.41	1.41	1.41
	20	1.57	1.57	1.39	1.39	1.39	1.39	1.38	1.38	1.38	1.38	1.47	1.47	1.47	1.47
	40	1.57	1.57	1.46	1.46	1.46	1.46	1.46	1.46	1.46	1.46	1.53	1.53	1.53	1.53
	60	1.57	1.57	1.50	1.50	1.50	1.50	1.50	1.50	1.50	1.50	1.59	1.59	1.59	1.59
	80	1.62	1.60	1.59	1.59	1.59	1.59	1.56	1.56	1.56	1.56	1.73	1.73	1.73	1.73
100	0	1.57	1.57	1.14	1.14	1.14	1.14	1.14	1.14	1.14	1.14	1.14	1.14	1.14	1.14
	20	1.57	1.57	1.23	1.23	1.23	1.23	1.23	1.23	1.23	1.23	1.23	1.23	1.23	1.23
	40	1.57	1.57	1.31	1.31	1.31	1.31	1.31	1.31	1.31	1.31	1.31	1.31	1.31	1.31
	60	1.57	1.57	1.40	1.40	1.40	1.40	1.40	1.40	1.40	1.40	1.40	1.40	1.40	1.40
	80	1.57	1.57	1.49	1.49	1.49	1.49	1.49	1.49	1.49	1.49	1.49	1.49	1.49	1.49
	100	1.57	1.57	1.57	1.57	1.57	1.57	1.57	1.57	1.57	1.57	1.57	1.57	1.57	1.57

maximum at [100% PO, 0% TO] and as a result TL drops to 1.14, which was 1.57 and 1.57 in N1 and N2. However, at 100% participant and tie overlaps, it again becomes equal to N1 and N2 due to consolidated MuHe networks being exactly similar to original networks.

The results of the TL metric show that the aggregated version of the networks, that is, MuHe network, is basically dependent on the PO. When the percentage of PO is low, a path bottleneck exists in the consolidated network, which makes the TL metric worse as compared to original networks N1 and N2. This is due to the less number of fresh trust paths being generated as a result of low value of participant overlap. When the value of PO increases, it causes TL to fall due to increase in number of overlapped users, which reduces the bottleneck issue. Furthermore, TL is lower in each of the subnetworks CN1 and CN2 than in the corresponding original networks N1 and N2, respectively, irrespective of the value of PO. This shows the emergence of additional trust paths due to consolidation. The results from this simulation and the one discussed in [34] prove that the WOWA consolidation is the best approach along all the varying overlap values, while other techniques show poor performance for certain values of PO and TO. At low participant overlap, it respects the integrity of trust (as measured by stability in TS, average strength of ties) while creating new trust paths (as measured by decrease in TL, average length of trust paths).

5. Experiment 2: Network Trust versus Declared Proxy Trust

The simulation demonstrates that in principle the WOWA aggregation technique can result in a MuHe network with improved trust characteristics; however, without applying the technique to real-world networks, it is impossible to evaluate whether the trust values that emerge as a result are better than those calculated by single networks. To test this, we undertook an evaluation that compared trust values calculated from two real-world networks and their consolidation against trust values obtained from directly surveying members of that network.

Networks with pure trust values are rare, so a pair of professional social networks are extracted from publication and projects domain. These networks are managed by the University of Southampton and they represent proxy trust between users using the coauthorship and collaboration

frequencies. The assumption is that individuals who had worked together (manifest as joint publications or participation in the same project) would exhibit higher trust. The coauthorship frequency was extracted from ePrints' (http://www.eprints.soton.ac.uk) publication network, while collaboration frequency was taken from the public catalogue of research projects undertaken by the WAIS (Web and Internet Science) research group at Southampton (http://www.wais.ecs.soton.ac.uk/projects) and contained details about the projects and staff associated with those projects. The dataset included information about both active and past projects that are being completed under the WIAS research group.

Both networks are available online in RDF format, and these were transformed into the ontology described in Figure 3 and passed into the MuHe consolidation framework (described in Section 3). This then performs the WOWA aggregation and links the resultant consolidated graph with the existing graphs using *owl:sameAs* predicates.

Both of these networks are in the same environment, so there are significant PO (participant overlap) and TO (tie overlap), with the collaboration network nearly a subset of the coauthorship network, discounting users outside the university who work on projects. The PO and TO with respect to the WAIS were 51% and 78%, while for ePrints they were 2% and 1.4%, respectively. Table 5 shows description of the network parameters used in this experiment. Both these networks contain bidirectional symmetric trust, as coauthorship and collaboration represent the same trust values in both directions.

5.1. Experiment Design. A survey experiment is designed to test the accuracy of the proposed framework for real-world social networks. It collects proxy trust values between users in the professional context, which are then compared with the trust measurements from the original and consolidated pair of networks. This is a web application (developed using Django (https://www.djangoproject.com/) framework), which first examines the presence of user in one or both of the networks and then presents each user with a randomly selected set of related people from these networks, based on the presence of the user in these networks. A set of questions were asked, which represent proxy trust helping us to measure the level of trust between them.

5.1.1. Participants. The designed survey has two types of participants. The first set of participants is known as rating participants and they represent those taking part in the survey. The second group of people comprised those about whom rating participants expressed their trust by answering proxy trust questions. This set of people is known as rated participants. The rated participants were selected from the egocentric network created by taking rating participant as an ego-node and randomly selecting set of users. As the simulation experiment claims the existence of trust decay along paths in social networks, the accuracy of indirect trust was evaluated by selecting rated participants belonging to path lengths of one, two, and three. If the rating participant was present in both the selected networks, then four of the rated participants were selected from each of the networks; otherwise, all the eight rated participants were selected from one of the networks.

Table 5: Network and consolidation parameters used for the real-world experiment for measuring the accuracy of aggregated trust.

Parameters	ePrints	WAIS
N	3286	154
PO (%)	2	51
TO (%)	1.4	78

5.1.2. Questionnaire. The survey aimed to extract the trust that participants feel towards one another in a professional context. The substance of a trust survey can be ethically difficult, as participants can be unwilling to disclose genuine trust ratings for others; our solution was to ask less sensitive questions about the closeness of professional ties and to treat these as proxy trust values. There are two questions asked to each of the rating participants. *First* one is about the *past work* experience with some randomly chosen related person and *second* question is about the likelihood of them *working together in future* should there be the opportunity. The numerical data from this portion of the survey was in the range (0, 0.8) with the value of 0.8 corresponding to working *very closely*, while 0 means working *hardly at all*. The survey values are then compared with the data available from the system, which is already in the range (0, 1). The *last* question in the survey asked rating participant to briefly explain their relationship with each of the rated persons separately. This was so we could explore whether different categories were more accurately represented by the proxy networks or improved by the consolidated network.

5.1.3. System and Survey Trust Metrics. Figure 4 shows the number of nodes (people) and ties (relationships) in ePrints and project networks used for the experiment. Of these, a total of 26 individuals participated in this survey experiment; on average, each rating participant provided trust ratings on 3.15 out of 5.38 rated participants presented. The maximum number of trust ratings was provided for path length one, and, as might be expected, this number decreased as the length of path increased.

As discussed in Section 3.2, trust data from consolidated MuHe networks can be categorised into two types, complete and partial. With reference to Figure 4, complete data originated from the region EW, and user pairs belonging to this region are known as $N_p^{\text{overlapping}}$ users, while partial trust information came from either regions E or W or across different regions, for instance, E $\longrightarrow$ EW, and user pairs belonging to this category are known as $N_p^{\text{non-overlapping}}$ users. Table 6 shows different trust parameters of the experiment along with their values. It can be categorised as system and survey readings.

System readings are the ones generated by evaluating trust over ePrints and WAIS networks, while survey readings

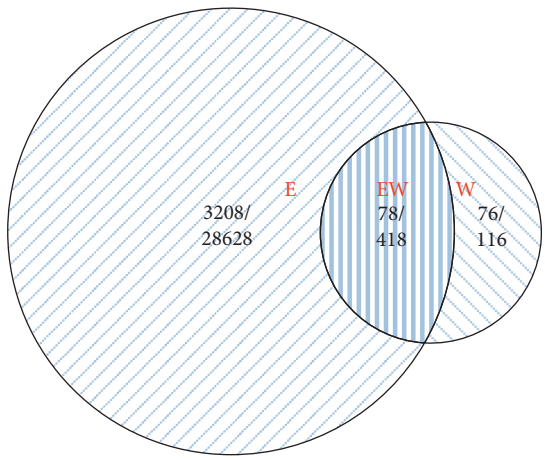


Figure 4: The two real-world professional networks (E for ePrints and W for WAIS) are shown as a Venn diagram (including their intersection EW), with the number of nodes/ties shown for each region.

Table 6: Description of the trust parameters obtained from system and survey experiments of the real-world experiment. The relationship terms Team Member, ECS Colleague, WAIS Colleague, and Supervisor are abbreviated as TM, EC, WC, and SP, respectively.

Data type	Trust ratings	Range
System readings	ePrints coauthorship proxy trust ($\text{trust}^{\text{eprints}}$)	(0, 1)
	WAIS projects collaboration proxy trust ($\text{trust}^{\text{wais}}$)	(0, 1)
	Consolidated proxy trust ($\text{trust}^{\text{muhe}}$)	(0, 1)
Survey readings	Past proxy trust ($\text{trust}^{\text{past}}$)	[0, 0.2, 0.4, 0.6, 0.8]
	Future proxy trust ($\text{trust}^{\text{future}}$)	[0, 0.2, 0.4, 0.6, 0.8]
	Relationship (Rel)	[TM, EC, WC, SP]

are collected from the corresponding real-world users. For the two categories of users specified above, there are always two trust values available from the survey experiment, but there are a variable number of trust values available from system readings. The trust values extracted from the survey are represented as $\text{trust}^{\text{past}}$ and $\text{trust}^{\text{future}}$ for representing past trust and future trust, respectively. There are three system-generated trust values for overlapping pairs of participants, represented as $N_p^{\text{overlapping}}$: two from each of the individual networks ePrints ($\text{trust}^{\text{eprints}}$) and WAIS ($\text{trust}^{\text{wais}}$) and one from the consolidated version, represented as $\text{trust}^{\text{muhe}}$. For $N_p^{\text{non-overlapping}}$ pairs of participants, however, there were only two values available, one from either of the individual networks ePrints ($\text{trust}^{\text{eprints}}$) or WAIS ($\text{trust}^{\text{wais}}$) based on the user presence and the other from their consolidated version, represented as MuHe ($\text{trust}^{\text{muhe}}$) networks. Beside this, there was one additional parameter that describes the type of relationship (Rel) between each of the user pairs. This was to assess the accuracy of aggregated trust metric with respect to each of the relationship categories.

5.2. Results and Analysis. Results of this experiment were thoroughly analysed to test whether the trust metrics from MuHe networks ($\text{trust}^{\text{muhe}}$) are *closer* to real-life trust metrics ($\text{trust}^{\text{past}}$ and $\text{trust}^{\text{future}}$) than from individual networks ($\text{trust}^{\text{eprints}}$ and $\text{trust}^{\text{wais}}$). The test was conducted by first taking the mean of the absolute difference between system and survey readings for each category of users from individual and consolidated networks and then evaluating p value between datasets using t-test to deduce whether the difference is statistically significant.

5.2.1. Overlapping Users' Data. To analyse the overlapping users' data for improvement, we calculated the mean value of the absolute differences between system and survey readings. Table 7 presents means for strongest and shortest path algorithms. It shows that, for both the algorithms, EP ($\text{trust}^{\text{eprints}} - \text{trust}^{\text{past}}$) and WP ($\text{trust}^{\text{wais}} - \text{trust}^{\text{past}}$) are larger than MP ($\text{trust}^{\text{muhe}} - \text{trust}^{\text{past}}$), which manifests that consolidated MuHe networks reduced the difference between system and survey metrics and brought trust metrics closer to real-life metrics than individual networks. Similar results are demonstrated by EF ($\text{trust}^{\text{eprints}} - \text{trust}^{\text{future}}$) and WF ($\text{trust}^{\text{wais}} - \text{trust}^{\text{future}}$) when compared with the MF ($\text{trust}^{\text{muhe}} - \text{trust}^{\text{future}}$).

To test whether the apparent improvement of $\text{trust}^{\text{muhe}}$ over $\text{trust}^{\text{eprints}}$ and $\text{trust}^{\text{wais}}$ is statistically significant, p value was calculated by conducting one-tailed paired t-test over the set of absolute differences between system and survey readings. If $p \leq 0.05$, we judge that this improvement is statistically significant for this dataset. Table 8 presents the evaluated p value. Results show that $p \leq 0.05$ for all categories of users, which proves the claim of generating trust metrics from consolidated MuHe metrics being closer to real-life trust metrics for $N_p^{\text{overlapping}}$ true for this dataset.

Table 7: Mean (M) of the difference between the system and survey readings for shortest path trust algorithm.

User category	EP	WP	MP	EF	WF	MF
Mean	0.23	0.23	0.20	0.23	0.22	0.19

$EP = (trust^{eprints} - trust^{past})$, $EF = (trust^{eprints} - trust^{future})$
$WP = (trust^{wais} - trust^{past})$, $WF = (trust^{wais} - trust^{future})$
$MP = (trust^{muhe} - trust^{past})$, $MF = (trust^{muhe} - trust^{future})$

Table 8: p value to evaluate the statistical significance of *closeness* between system and survey readings for overlapping ($N_p^{overlapping}$) users.

	EP	WP
MP	**0.01**	**0.02**
	EF	WF
MF	< **0.01**	**0.01**

$EP = (trust^{eprints} - trust^{past})$, $EF = (trust^{eprints} - trust^{future})$
$WP = (trust^{wais} - trust^{past})$, $WF = (trust^{wais} - trust^{future})$
$MP = (trust^{muhe} - trust^{past})$, $MF = (trust^{muhe} - trust^{future})$

Table 9: Mean (M) of the difference of system and survey readings for shortest path trust algorithm.

EP	MP	EF	MF
0.31	0.32	0.21	0.22

$EP = (trust^{eprints} - trust^{past})$, $EF = (trust^{eprints} - trust^{future})$
$WP = (trust^{wais} - trust^{past})$, $WF = (trust^{wais} - trust^{future})$
$MP = (trust^{muhe} - trust^{past})$, $MF = (trust^{muhe} - trust^{future})$

5.2.2. Nonoverlapping Users' Data. As mentioned earlier, nonoverlapping set of user pairs has partial trust information, so there is only one system trust metric available between them other than the one obtained from the consolidated network.

Like for the $N_p^{overlapping}$ users, means of the absolute difference between system and survey readings are calculated and Table 7 shows the results. Here, it shows opposite behaviour to the one existent in the case of $N_p^{overlapping}$ users; that is, MP and MF are greater than EP and EF, respectively, for both the strongest and shortest path algorithms—see Table 9 for description of MP, WP, MF, and WF. This shows that the consolidated MuHe networks took the trust values farther from the survey values, which resulted in deterioration of trust values for $N_p^{non-overlapping}$ users.

6. Discussion

If a trust-based system is developed for real-world social networks, the concept of implicit trust may be used to extract numeric values based on the activities of users in their individual social networks. This is due to unavailability of explicit trust metrics in all of the well-known social networks in use nowadays. The trust metrics in these networks may be based on the frequency of likes/favourites or retweets in the kind of social networks, for example, Facebook or Twitter. In likes of professional social networks such as Stack Overflow or Quora, the frequency of up votes/shares may become a metric of trust.

The task of fusing data from real-world MuHe networks is also nontrivial. In federated networks, it is relatively straightforward as multiple accounts of a single user are not allowed in these networks. The professional social networks selected for experimentation also belong to this category. The trust metrics from such networks may be extracted from each of the networks using implicit activities and can easily be aggregated using the techniques discussed in this article. However, for networks without any federated control, there may be fake or duplicate accounts, which can create data fusion problems. They may contribute wrong information, which is not reflective of the person in the real life. In such scenarios, the data should be rigorously preprocessed to eliminate any discrepancies before being fed to this framework for analysis. An absence of such preprocessing layer may generate distorted aggregation, which can mislead other users in making wrong predictions if they are totally relying on digital world for trust-related decision-making.

The future research directions that emerge out of this work are to implement the proposed model keeping in view the challenges that may arise due to federated and non-federated types of real-world social networks. Another research direction may be to explore the value of MuHe networks created from multiple constituent networks and also to understand the impact of networks due to differing quality and size. Our hope is that this work will persuade developers of trust systems to go beyond individual social networks for trust calculations. This could improve existing trust systems by enabling them to make more intelligent trust decisions by incorporating information from a variety of sources on the web.

7. Conclusion

Since the inception of Web 2.0, the use of online social networks has been increasing and existence of users in multiple networks is a great opportunity to make trust metrics on the web more sophisticated by incorporating a variety of information. This paper describes this as calculating trust on multiple heterogeneous (MuHe) networks and makes three contributions.

Firstly, it presents a semantic web based framework for modelling and consolidating heterogeneous trust networks and for performing trust calculations on both the individual and consolidated MuHe networks.

Secondly, it demonstrates the efficacy of the framework via a simulation that creates MuHe networks from individual networks with varying node and tie overlap. The simulation allowed us to investigate the impact of different data fusion techniques on the trust metrics of the MuHe network, and we showed that the Weighted Order Weighted Average (WOWA) technique produces a MuHe network with new trust paths, which protects trust values (that could be overinflated or suppressed with other consolidation techniques).

Thirdly, we explored how the MuHe network approach could work with real-life networks and applied the framework to two professional networks (ePrints, a publication network, and WAIS, a project network). This showed that,

for overlapped users, the MuHe network was closer to the assessments of the individuals within those networks (as gathered via a survey), but there was no substantial difference for nonoverlapped users (individuals who only appeared in one of the two networks).

Our simulation experiment clearly shows that, with appropriate data fusion techniques, MuHe networks can be constructed with better trust properties than their constituent networks. But we have also shown that the value of this in the real world is strongly effected by how close the trust represented in the constituent networks is to the trust required by the application and that in the real world the network sizes can be uneven, resulting in more complex interactions than those shown in our simulation. So, while MuHe networks appear to be a promising technique for improving trust calculations, they are not a panacea and still depend heavily on the quality of the constituent networks and how closely those networks reflect the type of trust required for a particular application.

Data Availability

The datasets generated and/or analysed in this study are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the Higher Education Commission, Pakistan, under the Startup Research Grant no. 21-1115.

References

[1] D. M. Boyd and N. B. Ellison, "Social network sites: definition, history, and scholarship," *Journal of Computer-Mediated Communication*, vol. 13, no. 1, pp. 210–230, 2007.

[2] L. Garton, C. Haythornthwaite, and B. Wellman, "Studying online social networks," *Journal of Computer-Mediated Communication*, vol. 3, no. 1, 2006.

[3] M. Imran, *The impact of consolidating web based social networks on trust metrics and expert recommendation systems*, Ph.D. thesis, University of Southampton, Southampton, UK, 2015.

[4] J. Golbeck, "Trust on the world wide web: a survey," *Foundations and Trends in Web Science*, vol. 1, no. 2, pp. 131–197, 2006.

[5] J. Golbeck and J. Hendler, "Filmtrust: movie recommendations using trust in web-based social networks," in *Proceedings of the 3rd IEEE Consumer Communications and Networking Conference (CCNC)*, vol. 1, pp. 282–286, Las Vegas, NV, USA, 2006.

[6] D. Olmedilla, O. F. Rana, B. Matthews, and W. Nejdl, "Security and trust issues in semantic grids," *Dagstuhl Seminar Proceedings*, vol. 5271, pp. 10–18, 2006.

[7] Q. Gong, Y. Chen, J. Hu, Q. Cao, P. Hui, and X. Wang, "Understanding cross-site linking in online social networks," *ACM Transactions on the Web*, vol. 12, no. 4, pp. 1–29, 2018.

[8] K. Shu, S. Wang, J. Tang, R. Zafarani, and H. Liu, "User identity linkage across online social networks," *ACM SIGKDD Explorations Newsletter*, vol. 18, no. 2, pp. 5–17, 2017.

[9] S. Bistarelli and F. Santini, "On merging two trust-networks in one with bipolar preferences," *Mathematical Structures in Computer Science*, vol. 27, no. 2, pp. 215–233, 2017.

[10] L. Shi, D. Berrueta, S. Fernandez, L. Polo, and S. Fernandez, "Smushing RDF instances: are alice and bob the same open source developer," in *Proceedings of the 3rd Personal Identification and Collaborations: Knowledge Mediation and Extraction (PICKME) Workshop with 7th International Conference on Web Semantics*, pp. 10–18, Berlin/Heidelberg: Springer, Karlsruhe, Germany, 2008.

[11] H. Glaser, I. Millard, A. Jaffri, T. Lewy, I. Millard, and B. Dowling, "On coreference and the semantic web," in *Proceedings of the 7th International Semantic Web Conference (ISWC)*, pp. 26–30, Karlsruhe, Germany, October 2008.

[12] M. Hussain, M. Ahmed, H. A. Khattak et al., "Towards ontology-based multilingual url filtering: a big data problem," *The Journal of Supercomputing*, vol. 74, no. 10, pp. 5003–5021, 2018.

[13] H. Glaser, A. Jafri, and I. Millard, "Managing co-reference on the semantic web," in *Proceedings of the Linked Data on the Web (LDOW) Workshop with 18th International Conference on World Wide Web (WWW)*, pp. 288–293, Madrid, Spain, 2009.

[14] J. J. Carroll, C. Bizer, P. Hayes, and P. Stickler, "Named graphs," *Journal of Web Semantics*, vol. 3, no. 4, pp. 247–267, 2005.

[15] R. R. Yager, "On ordered weighted averaging aggregation operators in multicriteria decisionmaking," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 18, no. 1, pp. 183–190, 1988.

[16] T. Vicenc, "The weighted OWA operator," *International Journal of Intelligent Systems*, vol. 12, no. 2, pp. 153–166, 1997.

[17] R. R. Yager and D. Filev, "Operations for granular computing: mixing words and numbers," in *Proceedings of the 1998 IEEE International Conference on Fuzzy Systems Proceedings, 1998: IEEE World Congress on Computational Intelligence*, vol. 1, pp. 123–128, IEEE, Anchorage, AK, USA, May 1998.

[18] R. R. Yager and D. P. Filev, "Induced ordered weighted averaging operators," *IEEE Transactions on Systems, Man and Cybernetics, Part B (Cybernetics)*, vol. 29, no. 2, pp. 141–150, 1999.

[19] P. Victor, C. Cornelis, M. De Cock, and E. Herrera-Viedma, "Practical aggregation operators for gradual trust and distrust," *Fuzzy Sets and Systems*, vol. 184, no. 1, pp. 126–147, 2011.

[20] Y. Ma, H. Lu, Z. Gan, and X. Ma, "Trust discounting and trust fusion in online social networks," in *Web Technologies and Applications, Volume 8709 of Lecture Notes in Computer Science*, pp. 619–626, Springer International Publishing, Berlin, Germany, 2014.

[21] S. Deng, L. Huang, G. Xu, X. Wu, and Z. Wu, "On deep learning for trust-aware recommendations in social networks," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 28, no. 5, pp. 1164–1177, 2017.

[22] F. Heider, *The Psychology of Interpersonal Relations*, Psychology Press, London, UK, 2013.

[23] P. W. Holland and S. Leinhardt, "Holland and leinhardt reply: some evidence on the transitivity of positive interpersonal sentiment," *American Journal of Sociology*, vol. 77, no. 6, pp. 1205–1209, 1972.

[24] C.-N. Ziegler and G. Lausen, "Propagation models for trust and distrust in social networks," *Information Systems Frontiers*, vol. 7, no. 4-5, pp. 337–358, 2005.

[25] C.-N. Ziegler and G. Lausen, "Spreading activation models for trust propagation," in *Proceedings of the IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE)*, pp. 83–97, Taipei, Taiwan, March 2004.

[26] Y. A. Kim and H. S. Song, "Strategies for predicting local trust based on trust propagation in social networks," *Knowledge-Based Systems*, vol. 24, no. 8, pp. 1360–1371, 2011.

[27] N. Verbiest, C. Cornelis, P. Victor, and E. Herrera-Viedma, "Trust and distrust aggregation enhanced with path length incorporation," *Fuzzy Sets and Systems*, vol. 202, pp. 61–74, 2012.

[28] C. Jiang, S. Liu, Z. Lin, G. Zhao, R. Duan, and K. Liang, "Domain-aware trust network extraction for trust propagation in large-scale heterogeneous trust networks," *Knowledge-Based Systems*, vol. 111, pp. 237–247, 2016.

[29] W. Jiang, J. Wu, F. Li, G. Wang, and H. Zheng, "Trust evaluation in online social networks using generalized network flow," *IEEE Transactions on Computers*, vol. 65, no. 3, pp. 952–963, 2016.

[30] S. Hamdi, A. L. Gancarski, A. Bouzeghoub, and S. B. Yahia, "TISoN: trust inference in trust-oriented social networks," *ACM Transactions on Information Systems*, vol. 34, no. 3, pp. 1–32, 2016.

[31] W. Jiang, G. Wang, M. Z. A. Bhuiyan, and J. Wu, "Understanding graph-based trust evaluation in online social networks: methodologies and challenges," *ACM Computing Surveys*, vol. 49, no. 1, pp. 1–35, 2016.

[32] J. Carroll, C. Bizer, P. Hayes, and P. Stickler, "Named graphs, provenance and trust," in *Proceedings of the 14th International Conference on World Wide Web (WWW)*, pp. 613–622, ACM, Chiba, Japan, May 2005.

[33] T. Heath and E. Motta, "The Hoonoh ontology for describing trust relationships in information seeking," in *Proceedings of the 3rd Personal Identification and Collaborations: Knowledge Mediation and Extraction (PICKME) Workshop with 7th International Conference on Web Semantics*, pp. 67–75, Berlin/Heidelberg: Springer, Karlsruhe, Germany, 2008.

[34] M. Imran, D. Millard, and T. Tiropanis, "Impact of consolidating social networks on derived trust factors," *ASE Human Journal*, vol. 1, no. 2, pp. 88–99, 2012.

Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 7105625, 15 pages
https://doi.org/10.1155/2020/7105625

Review Article

Text Data Security and Privacy in the Internet of Things: Threats, Challenges, and Future Directions

Umair Khadam,[1] Muhammad Munwar Iqbal,[1] Meshrif Alruily,[2] Mohammed A. Al Ghamdi,[3] Muhammad Ramzan,[3] and Sultan H. Almotiri[4]

[1]*Department of Computer Science, University of Engineering and Technology, Taxila 47050, Pakistan*
[2]*Faculty of Computer and Information Sciences, Jouf University, Sakaka City, Saudi Arabia*
[3]*Computer Science Department, Umm Al-Qura University, Makkah City, Saudi Arabia*
[4]*Department of Computer Science & IT, University of Sargodha, Sargodha, Pakistan*

Correspondence should be addressed to Muhammad Munwar Iqbal; munwariq@gmail.com

Received 22 November 2019; Accepted 8 January 2020; Published 19 February 2020

Academic Editor: Ghufran Ahmed

In our daily life, Internet-of-Things (IoT) is everywhere and used in many more beneficial functionalities. It is used in our homes, hospitals, fire prevention, and reporting and controlling the environmental changes. Data security is the crucial requirement for IoT since the number of recent technologies in different domains is increasing day by day. Various attempts have been made to cater the user's demands for more security and privacy. However, a huge risk of security and privacy issues can arise among all those benefits. Digital document security and copyright protection are also important issues in IoT because they are distributed, reproduced, and disclosed with extensive use of communication technologies. The content of books, research papers, newspapers, legal documents, and web pages are based on plain text, and the ownership verification and authentication of such documents are essential. In the current domain of the Internet of Things, limited techniques are available for ownership verification and copyright protection. In the said perspective, this study includes the discussion about the approaches of text watermarking, IoT security challenges, IoT device limitations, and future research directions in the area of text watermarking.

1. Introduction

With the rapid development of embedded technology, computer technology, mobile communication network, and the Internet, IoT emerges at a historic moment. The primary feature of IoT is global perception, reliable transfer, and intelligent processing of information. The key is to realize the interaction of information between people and machine or machine and machine. Since its introduction, the IoT has caused major repercussions around the world because many human and material resources have been invested in supporting research, and remarkable results have been achieved. The rapid growth of IoT has brought significant changes to the industry, which is considered the third wave of the global information industry after the computer and the Internet. The Internet of Things is a collection of elements embedded in software, actuators, and electronic components that share and collect data over an Internet connection. IoT devices can be used in many environments that are equipped with sensors and low processing power [1]. The significant difference between the traditional internet and IoT is the absence of human role. IoT devices can create, analyze, and take action on information about an individual's behavior [2]. IoT offers a lot of benefits for humans but facing many issues regarding security and privacy [3].

Current security challenges for IoT that need to be sorted out are presented in Figure 1. This shows that data integrity, security, privacy, automation, updating, a common framework, and encryption capabilities are the main challenges. In IoT, text documents integrity and security issues are exist in a modern digital world [5]. A large number of text documents are generated daily and shared through IoT. Due to

Figure 1: Recent security challenges in IoT [4].

advanced technologies, these documents can be easily copied and redistributed [6]. IoT has unlimited benefits, but on the contrary, illegal use of these documents creates a problem for the original. Nowadays, a number of ways have been used by hackers to infect or access the information. Digital text document protection is a crucial issue for researchers in the modern world [7]. The use of digital libraries, Internet technologies, mobile phones, e-commerce, and iPods are a fast and easy way of broadcasting information [8]. However, the security and privacy of digital content are difficult to handle. In this case, it is necessary to provide protection to digital materials that are traveling over the internet [9, 10].

2. IoT Security Challenges

Currently, 23 billion IoT devices are connected worldwide. By the end of 2020, it will further rise and reach up to 30 billion, and by the end of 2025, it will reach over 60 billion [11]. The security challenges for IoT are mention below.

2.1. Updating. The majority of IoT devices update their software automatically, while other devices had to be updated manually [12]. Some manufacturers only offer updates for a short period of time and then stop it. It is challenging to manage the upgrade of millions of devices that are connected to IoT. All the devices do not support the automatic update and require manual updating, which are time-consuming and lead to security loopholes if any mistake happens [13].

2.2. Automation. As in our daily lives, IoT devices continue to invade and deal with the number of IoT devices. It is challenging to manage an enormous amount of user data. The fact cannot be denied that any single error in an algorithm will bring down the entire infrastructure [14].

2.3. Common Framework. In IoT, there is an absence of a common framework, so all the manufacturers retain privacy and security at their own risk. Once a standard framework is implemented, then the security issue will be resolved [15].

2.4. Security and Privacy Issues. Different IoT devices can share data among various platforms. The IoT devices exchange and gather data for multiple reasons, such as decision-making, better service, and improving efficiency. Thus, it is essential that the endpoint of data shall be secured completely.

2.5. Data Integrity. Billions of IoT devices are interlinked and exchange data on a daily basis. The data integrity is the main issue in the IoT that no one can manipulate data at any point. Digital watermarking and blockchain should be implemented in order to ensure data integrity [16, 17].

3. IoT Device Limitations

There are two main issues IoT devices have: first one is battery capacity, and the second one is computing power [18]. Since some IoT devices are placed in such environments where we cannot charge them or charge is not available, the devices should perform the designed functionality in limited energy, and heavy security instructions may drain with limited power [19]. To mitigate this issue, three possible techniques can be used: first, to minimize the security requirements, and second, to raise the capacity of the battery. That seems impossible because most IoT devices are small in size and designed to be lightweight. However, a large battery has no extra room. The third approach is to harvest energy from natural resources such as heat, light, wind, and vibration, but such techniques are required on hardware upgradations and increase the monetary cost. The IoT devices have limited memory space that cannot store and handle the computational requirements of advanced security algorithms [19]. The IoT devices should be smart and manage all these requirements.

4. IoT Devices Architecture

Internet of Things includes many connected sensors and devices, and every device uses different communication standards and protocols. There are no precisely defined rules and standards for communication. In addition, the applications of the Internet of Things would not be limited and increase from day today. Different IoT devices are produced by different manufacturers even if they perform the same functionality. So, this challenge is related to the nature of the IoT and may lead to a lack of unified standardization.

4.1. IoT Devices Data Storage Issues. Data storage becomes a significant issue, as the amount of data increases rapidly. When the stored information is damaged, it is a challenging task to back up all. There is no assurance that data and information are securely transmitted over the IoT devices. Furthermore, it is a significant challenge for management

companies and data storage to develop tools and standards that handle data provided and security issues.

4.2. Limited Resources of Infrastructure. IoT devices generally have limited memory and low processing capacities. Designing comprehensive security measures in 64 kB to 640 kB memory is a big challenge for software developers and IoT hardware manufacturers. In addition, they must have enough storage for security software to defend against security threats.

4.3. Data Privacy Protection. Anyone can access integrated devices from anywhere with IoT, which affects sensitive data confidentiality and privacy. Therefore, specific standards or rules must be defined to avoid the privacy violation. For example, some IoT devices share data with other devices, and in this case, the data become unsafe. This helps attackers and intruders to breach the security of the IoT system.

4.4. Lack of Skills. Specific skills and expertise are critical factors in the design, development, implementation, and management of security that must be considered. Any of this factor disruption may cause damage to the IoT security system. In addition, the lack of skills and expertise slows down the adoption of IoT technologies [20]. There are very limited people who can adequately handle the IoT system. The number of qualified people who master in IoT techniques is very limited. The benefits of IoT technology and dealing with its challenges depend mostly on individual capabilities.

5. Digital Watermarking

Digital watermarking belongs to information hiding and plays an essential role in copyright protection, ownership verification, and authentication [21]. In digital media, when we talk about information hiding, text watermarking is the least discussed subject. The protection of digital content is a difficult task, especially plain text [22–24]. The information hiding is categorized into steganography, cryptography, and watermarking as shown in Figure 2. A secret message is embedded in digital content without affecting the original text, which authenticates the ownership verification [25, 26].

Researchers have significant challenges that information growth rate is higher, which requires an appropriate technique for watermarking. It is crucial to maintain data integrity while ensuring the confidentiality and availability of information [27]. However, with the practical development of the watermarking application, security issues of watermarking have emerged and achieved significant progress in this field [28].

Many techniques have been proposed in the last two decades, for hiding information in terms of steganography and text watermarking for copyright protection [29], authentication, copy control [30], ownership verification [31–37]. The main contributions of this study are listed as follows:

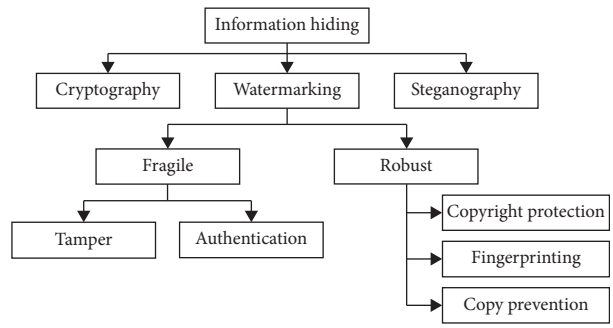


Figure 2: Common information hiding techniques.

(i) We briefly describe the IoT current security and privacy issues and recommendations

(ii) We conduct an extensive investigation about the approaches of text watermarking, IoT security challenges, IoT device limitations, and future research directions

(iii) We summarize the text watermarking approaches/techniques that are used for digital watermarking

(iv) A comparative analysis of previous techniques has been conducted on the basis of robustness, security, capacity, and imperceptibility. Their efficiency evaluated on the basis of set criteria, also identifying the drawbacks of exiting techniques

6. Digital Watermarking and Its Applications

In the real-world, watermarking can be used in a variety of applications that categorized into image, audio, video, and text [38]. Authorized documents, such as websites, certificates, business plans, articles, poems, books, corporate documents, e-mails, and SMS, can be protected through watermarking [39]. The applications of digital watermarking can be used for authentication, copyright protection. Some other application of the watermarking in the text listed below [40–42].

6.1. Authentication. The plain text in articles and newspapers highlighted various problems with authentication. Watermarking is a verification tool to authenticate the integrity of the plain text. To prove the authentication if the watermark (author information) is perceived, then it has genuine document else text has been tempered and cannot be measured. The authentication mechanism can be used for a text document to detect any tampering. If tampering is identified, then the document cannot be considered as original, also for legal purposes, and it is necessary to authenticate text document [43].

6.2. Copyright Protection. Watermarking is also used in copyright protection of digital contents, like e-books, web content, research papers, poetry, and other documents. The author inserts a watermark in the document for copyright, and this watermark is extracted in the future from the given material to prove ownership. Digital watermarking is very helpful to settle the copyright issues in court.

6.3. Tamper Detection. A large number of text documents are available for users to read online, and these documents can be confronted with a series of attacks such as copying, unauthorized access, and redistribution. Tamper detection is one of the digital watermarking applications that can detect and recover the tampered region from the digital contents. Text watermarking is used as a fragile tool against these attacks [34, 44].

6.4. Copy Control. Publishers are looking for more consistent ways to control the copy of their important documents. Likewise, they want their essential documents to be available on the Internet for revenue generation. The watermarking is also applied here to provide access control and stop illegal copying [43].

6.5. Forgery Detection. Text documents reproduction and plagiarism are serious issues, and it is rapidly growing. Text watermarking is applied here to embedding watermark in the original document before publishing online [45]. Almost every private and public organizations deal with text documents on a daily basis, and digital text watermarking application can be applied here to control the forgery detection problem.

Watermarking major applications [46] is shown in Figure 3.

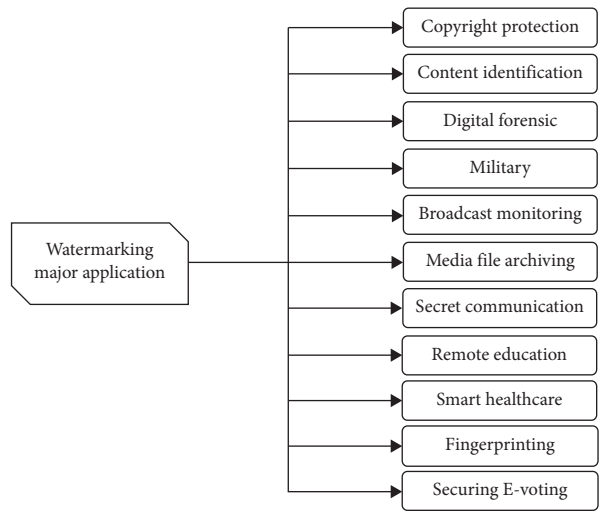


Figure 3: Watermarking major applications.

7. Text Watermarking Evaluation Criteria

The researchers count a lot of parameters while developing novel techniques. However, digital text watermarking evaluation criteria can be classified into security, capacity, robustness, imperceptibility, and computational cost. It is not possible to design such a system of watermarking that can cover all these properties. In the below content, each property of watermarking mentioned above is described [44, 47, 48].

7.1. Robustness. Robustness means that if watermark information is tempered and then it is still survived [49]. The mean of robustness is that it will be almost impossible without a license and without the content that defeat marked a great extent the content is not suitable and reliable [50]. When a technique of watermarking is designed, it is essential to revenue in consideration of the future application and the equivalent number of attacks that are possible. On the bases of watermark distortion rate (WDR) and pattern matching rate (PMR), the robustness of text watermarking is computed. That is formalized from (1) and (2).

$$\mathrm{PMR} = \frac{N_{\mathrm{m}}}{N_{\mathrm{w}}}. \tag{1}$$

$$\mathrm{WDR} = 1 - \frac{N_{\mathrm{m}}}{N_{\mathrm{w}}}, \tag{2}$$

where N_{m} determines the number of patterns matched correctly and N_{w} defines the number of watermark patterns.

7.2. Imperceptibility. The imperceptibly in the primary and fundamental requirement that means the watermark is securely embedded into the document objects. The watermark information could not feel the audience, or the watermark should not affect the original text. The watermarked and original information should be similar, and the content should be perceptually equal [51]. Peak signal–to-noise ratio (PSNR) and similarity percentage (SIM) is used to ensure the imperceptibility using the following equation (3) [52]:

$$\mathrm{PSNR} = 20\ \log_{10}.\frac{O_{\mathrm{doc}}\ (\max)}{\mathrm{RMSE}}, \tag{3}$$

where O_{doc} (Max) is the maximum pixel value in the document image, RMSE stands for root–mean-squared error, and it is calculated using the following equation (4):

$$\mathrm{RMSE} = \sqrt{\frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \left[O_{\mathrm{doc}}(\mathrm{i},\mathrm{j}) - W_{\mathrm{doc}}(\mathrm{i},\mathrm{j})\right]^2}. \tag{4}$$

The following equation (5) is used to calculate the similarity parentage (SIM):

$$\mathrm{SIM} = \left[1 - \frac{\mathrm{RMSE}}{O_{\mathrm{doc}}\ (\max)} \times 100\right]. \tag{5}$$

7.3. Capacity. The capacity indicates that the maximum bits of watermark information that can be stored in the host document. If a technique can hold large hiding capacity without affecting the visibility, then it is considered. The capacity can be measured using the following equation (6):

$$\mathrm{capacity} = \frac{\text{total no of bits (secret data)}}{\text{total no of cover file data (kB)}} \times 100. \tag{6}$$

7.4. Security. There is another scheme for watermarking which is security. It states that the information of the author (watermark) is hidden from unauthorized users. They do not

have access to detect the watermark. Watermark still exists and the payload still remains coved is the mean of security. Unapproved and unauthorized parties are not capable of identifying the author's information. Security is measured on the bases of the imperceptibility, capacity, and robustness as shown in the following equation (7):

$$\text{security} = [\text{imperceptibility} + \text{capacity} + \text{robustness}]. \tag{7}$$

7.5. Computational Cost. Text watermarking techniques are computationally less complex for small text documents. More computation power is required for text documents that occupy many pages. In general, less complex algorithms are used for systems with limited resources to reduce the cost [44].

8. Watermarking Embedding and Extraction Process

Watermarking is the technique of information hiding that provides ownership verification and copyright protection to text documents against illegal usage [53–55]. Digital watermarking has two steps: the first one is watermark embedding, and the second step is watermarking extraction or verification. In watermark embedding, secret information (watermark) is inserted into the original document without affecting the content of the document. A key can be used to encrypt the secret information for security purposes, and then the same key is applied for decryption. When an illegal attempt happens, then the watermark information is used to verify the original owner of the document. The reverse process of watermark embedding is called watermark extraction. Basically, this process is applied to verify the originality of the document. The architecture of watermarking is presented in Figure 4.

9. Existing Techniques of Text Watermarking

Digital text watermarking arose in 1994 [56, 57] and grew with the passage of time, as the communication and Internet start all over the world. These techniques are based on words and sentences, acronym, synonym, presupposition, syntactic tree, typo error, noun-verb, and text images for German, Persian, French, Spanish, and English languages. The text watermarking techniques and attacks are presented in Figure 5.

An information hiding technique is proposed in [58] that hides information in a binary text document; they use the boundary of characters for information hiding. Five pixels long, 100 pairs of border patterns were defined. There were two different models for each pair, an "A" model and a "D" model, which can be changed into each other when the pair is returned. A bit is embedded in the five-pixel long border by browsing the patterns. Kim et al. suggested a technique based on the classification of words and interword spaces to insert a watermark [59]. All words are classified in the document according to adjacent words and specific text attributes which comprise a segment, and it is further categorized according to the names of the class and the words in the segment. Each segment class contains the same amount of information.

Zhou et al. [60] introduced a method which used a chaotic encrypting algorithm to generate the watermarks, and the host document splits into two blocks using Chinese mathematical expressions. Two different text blocks and keys were generated to calculate the stoke numbers and the Chinese character frequency. When the content of the watermarked text document is modified, results from two blocks of text do not match, and text document result authentication will be false. In [61], a technique is proposed that is based on a particular part of speech (POS) for text zero watermarking. POS is the category of a word which has similar grammatical properties. The chaotic function is used to extract the sequences that are used to develop a watermark without altering cover data, and the imperceptibility problem is also resolved. This method provides excellent security because the order of the selected POS tag is unknown by an attacker.

Meng et al. [62] introduced a technique where sentence entropy is used to calculate the watermark key. Entropy defines as the average expected value of data that a message contains. Through word frequency and important selection, the sentence entropy is calculated, and according to the order of the crucial sentence, the watermark is embedded. Some unknown attacks were also applied to this method, which includes insertion, deletion and synonym substitution to check the robustness of this method, which is good but shows a very low success rate. Jalil et al. [63] suggested a technique that embeds through generating a watermark key. To find the nonvowel character that occurs most frequently, the occurrence of nonvowel ASCII character analyzes first in each partition. The maximum occurrence of nonvowel and author key letters is used for watermark generation. Certification authorities are used to a registered watermark in order to provide security. Extracted watermark accuracy is analyzed through insertion and deletion attacks. In [64], the author proposed a watermarking technique that generates watermark key on the bases of the preposition, double letters, and cover file partition is analyzed through the repeating letter frequency. The key is generated through a count of double letters in a time interval. The conversion of the image into the text is performed to generate the hidden data that is included in the host document. In insertion, deletion, reordering, and other attacks, the proposed method is robust and more secure.

Cheng et al. [65] introduced an algorithm on the strategy of fragments regrouping for watermark embedding. The original watermark is divided into different fragments of order numbers and then embedded in the characters of the document. After deleting and tamper attack when some fragments are deleted or changed, the destroyed fragment is recovered using other correct fragments that are embedded in the phrases. Kim et al. [66] proposed a method that is based on syntactic displacement and morphological division in natural language watermarking for Korean. Syntax-based watermarking is used in this approach, usually, a Korean

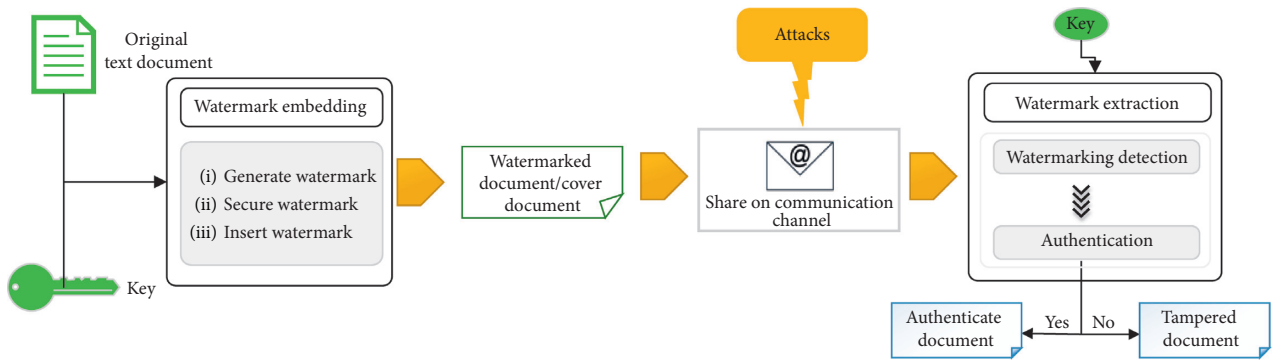


Figure 4: Digital watermarking architecture.

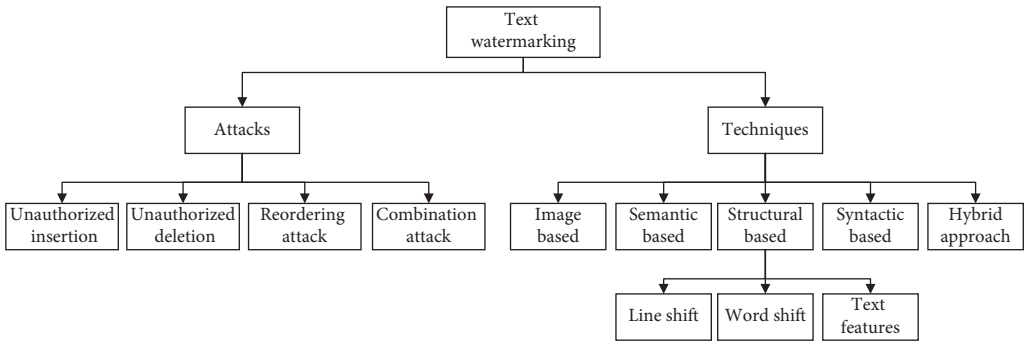


Figure 5: Text watermarking techniques and attacks.

word consists of function morpheme and content morpheme. Through the use of word characteristics, the word is divided into two content morphemes into two new words, which are used for watermark embedding.

In [67], a model based on 3-D using 2-D coordinates of word-level and weights of sentences to construct zero watermarking is introduced. The structure of the 2D word space includes the length and frequency of words, then that the 2-D model is extended into 3-D. Three frequent attacks are tested on the proposed model that are synonym replacement, syntactic transformation, and deleting attack. The test report shows that the proposed method is robust, secure, and useful imperceptibility. Al-Wesabi et al. [68] proposed Markov's model-based approach for watermarking, where the watermark key is generated through cover file probabilistic features. The use of the hidden Markov model information for text watermarking is analyzed and stored in the document for authentication. It offers protection against attacks with a higher percentage of watermark distortion than all attacks. In [69], the author suggests a zero watermark approach that uses the Arabic character's characteristics for embedding the watermark without changing the original text. In an initial phrase, name/number of sura and number of verses are checked, and then from each verse of Holy Quran, key is generated. With this algorithm, a character watermark bit of the word set is inserted. The proposed method built a system to verify the sensitive of the Holy Quran digital text. With this technique, changes in the original text content can be detected and only minimal hardware resources are required.

Alginahi et al. [70] introduced an approach that generates the watermark key by converting the image into text. A duplicated cover file is used for embedding the image logo where it is classified and processed, and using its characteristics watermarking key is generated. The proposed technique offers authorized content manipulation and copyright protection. Through using blind and fragile watermarking approaches, the watermark key is secured. This method produces excellent results after evaluating the computational time of watermark encoding and decoding. Ba-Alwi et al. [71] presented a novel technique based on probabilistic models for ownership verification and tamper detection in English documents. The probabilistic pattern is extracted by using natural language processing based on the Markov model. Each text document content is analyzed in English and extracts the probabilistic characteristics between these contents.

In [72], the authors suggested a technique based on word items and particular attributes of robustness and excellent performance, which can hide information in a Word document. A novel method is proposed to enhance the robustness of the watermark. Watermarking information is divided into 5 groups. After this, it is embedded into the plain text one by one as a group no. An advantage of this method is challenging to extract hidden information because its first encrypted information is divided into several groups and then embedded into word properties. After the experiments, most of the watermarked text is the same, but in two or three lines, some characters are changed which also changes text meaning. The scheme is not very good on the

base of imperceptibility. Chen et al. [73] suggested a semantic technique for embedding watermark information in the text. The watermark information is embedded through the mapping location of each digit. The proposed algorithm does not change the integration of text and format. The author claims that it is robust against watermarking attacks and text format transformation.

Ahvanooey et al. [29] offer a novel text watermarking method for web pages. Structural and syntactic rules are used to embed watermark, which is encoded and converted into zero-width control characters with a binary model classification. Hypertext Markup Language (HTML) is used as a cover file to embed the transparent zero-width watermark. In [74], the author suggests a novel method for embedding information in text, which is based on font code that embeds a watermark into text by disrupting text character glyphs while retaining text content. The glyph recognition method is also presented to restore the information that is embedded in the encrypted document. A new approach is proposed for Arabic text using pseudospace in [75]. The connected letters are isolated with pseudospace to hide watermark bits, which are used to hide watermark bits. In the first method, the watermark is embedded in the punctuation of the Arabic text by inserting a pseudorandom, and in the second method, the pseudospace is added to the standard space, thus increasing the capacity. The proposed method is robust and imperceptible against formatting and tampering attacks. Wen et al. [76] suggested algorithms for Extensible Markup Language (XML) document to hide information. The first method is the eXtensible Stylesheet Language Transformation- (XSLT-) related that is designed with the inclusion of additional codes to provide copyright protection. In the second method, the functional dependency is used for the XML file as a function for zero watermark. The proposed method performs well in alternation attacks, compression attacks, reorganization attacks, and selection attacks. From the study of Hakak et al. [77] in this work, a complete framework is presented with regard to the automatic authentication and distribution of the digital Quran and Hadith verses. The verification process is divided into two phases, security and verification. The watermarking technique in case of the security phase secured the confirmed and tested verse. For verification, the Boyer–Moore algorithm is used for extraction. The efficiency analysis of the existing techniques is presented in Table 1.

10. Attacks in Text Watermarking

Watermark content has specific attacks depending on the application. Some attacks are significant from other attacks. The basic types of attacks are an illegal insertion, illegal updation, illegal deletion, reordering attack, and the mixture of all these attacks. Table 2 presents the analysis of robustness attacks. This includes insertion, deletion, reordering, formatting, copy and paste, and retyping attacks. In the following categories, these attacks are placed [7, 72, 99–104].

10.1. Unauthorized Insertion. When an attacker wants to add false information, then such type of attack occurs, i.e., in the case of legal documents. Each time a dispute concerning the application of copyright occurs, and this type to identify the first recorded content stamp is used.

10.2. Unauthorized Detection. The ability to be detected in some applications is restricted. It is believable that the aptitude of a challenger to quickly identify whether a mark in a particular plant is present endangers the security of the watermarking system.

10.3. Unauthorized Deletion. An attacker can delete some words or sentences from the text to remove the original author's identity. All watermark application required security against illegal deletion. It is crucial to restrict the attacker to remove watermark information. The system is called secure if the watermark is still extracted from the text after applying the attack.

11. Research Challenges and Future Direction

Text watermarking research is at an early stage, although the watermarking process has been extensively studied. There are several significant issues in text watermarking that have remained unresolved. In addition, applications continue to pose new challenges, and many organizations still need to implement text watermarks.

11.1. Information Availability. Information availability means that a user can access information easily and securely. Millions of Internet users around the world generated and shared information on a daily basis, which required protection against illegal usage fully. In the text watermarking context, the availability of information remains constant and prevents any change in the text content. An active system is required to ensure data availability in secure manners, where a user can access information after an independent self-monitoring system.

11.2. Data Integrity. Data integrity is one of the critical aspects of text watermarking, which is related to reliability, usability, relevance, value, and quality. Data consistency and accuracy assurance can be part of integrity [105]. The explosion of the internet allows users to access a vast amount of information, where the integrity of information also required. With the development of internet technologies such as cloud, data can be easily shared through different communication. The main issue is how to ensure the integrity of data over the Internet.

11.3. Originality Protection. It is difficult to identify the originality and quality of data that is available online or come from all sorts of databases that are always well preserved in all cases. The implemented techniques' processing time is still high and lacks imperceptibility. The challenge is how to find the appropriate method that protects the originality of

Table 1: Efficiency analysis chart.

No.	Authors and Years	Parameters					Efficiency analysis	Drawbacks
		Medium	Capacity	Security	Imperceptibility	Robustness		
1	Hamdan and Hamarsheh [26]—2016	Text	Low	High	Medium	High	High robustness and security	The main drawback is the length (capacity) of the cover message
2	Gutub et al. [78]—2010	Text	High	Medium	Low	Low	High capacity	Imperceptibility and robustness are low when applying formatting attacks
3	Kim et al. [59]—2003	Text	High	NA	High	Low	High capacity and imperceptibility	Low robustness when applying distance algorithm spaces between words are deleted
4	Yang and Kot [79]—2004	Text	Low	High	High	Medium	The proposed system has a high capacity, imperceptibility, and capacity	Robustness is down when applying distance algorithms
5	Alginahi et al. [80]—2013	Text	Low	Medium	High	Medium	High imperceptibility	Capacity is low and no robustness against formatting attacks
6	Meng et al. [62]—2010	Text	Medium	Medium	High	High	High imperceptibility and robustness	Low capacity
7	Jalil and Mirza [41]—2010	Image plus text	Low	High	Low	High	High robustness and security	Low imperceptibility and capacity
8	Jaiswal and Patil [81]—2013	Text	High	Low	High	Low	High imperceptibility	Robustness and security are down
9	Cheng et al. [65]—2010	Text	High	Medium	Low	Medium	High capacity	Low imperceptibility and no robustness against reformatting attack
10	Mir [82]—2014	Text	Medium	High	High	Medium	High security and imperceptibility	No robustness against attacks
11	Meng et al. [67]—2011	Text	Low	Medium	High	High	High robustness, security, and imperceptibility	Low capacity
12	Zhang et al. [72]—2010	Text	High	High	Low	Medium	High capacity and security	No robust against copy paste and retyping attacks and low imperceptibility
13	Liu et al. [83]—2015	Text	Low	High	High	High	High robustness, security, and imperceptibility	Low capacity
14	Alginahi et al. [35]—2014	Text	High	Medium	Low	Low	High capacity	Low imperceptibility and no robust against attacks
15	Liang and Iranmanesh [84]—2016	Text	Low	Medium	High	Low	High imperceptibility	No robustness against attacks and low embedding capacity
16	Alotaibi and Elrefaei [75]—2017	Text	High	Medium	High	Medium	High capacity and imperceptibility	Robustness is medium because vulnerable to retyping attacks
17	Yingjie et al. [85]—2017	Text	Low	High	Medium	High	High robustness and security	Low capacity
18	Wen et al. [76]—2018	Text	Low	High	Medium	High	High robustness and security	Low capacity
19	Kuribayashi et al. [86]—2018	Text	High	Medium	Low	High	High robustness and capacity	Low imperceptibility
20	Jalil and Mirza [41]—2010	Image plus text	Low	High	Low	High	High robustness and security	Low imperceptibility and capacity
21	Taha et al. [87]—2018	Text	High	Medium	Medium	Low	High capacity	Not robust against formatting attacks
22	Xiao et al. [74] 2018	Text	Low	High	Medium	High	High robustness and security	Low capacity and only applicable to one font

Table 1: Continued.

No.	Authors and Years	Parameters					Efficiency analysis	Drawbacks
		Medium	Capacity	Security	Imperceptibility	Robustness		
23	Tan et al. [88] 2018	Text	High	High	Low	Medium	High capacity and security	Low imperceptibility

Table 2: Robustness analysis against attacks

Sr. No	Authors	Insertion	Deletion	Reordering	Reformatting	Copy and paste	Retyping
1	Al-Nofaie et al. [89]	✓	✓		✓	✓	
2	Rizzo et al. [90]			✓	✓	✓	
3	Alotaibi et al. [75]	✓			✓	✓	
4	Ahvanooey et al. [29]	✓		✓	✓	✓	✓
5	Alotaibi et al. [91]	✓			✓	✓	
6	Ahvanooey et al. [31]	✓		✓	✓	✓	
7	Mir. [82]		✓				✓
8	Por et al. [36]	✓			✓	✓	
9	Chou et al. [92]	✓			✓	✓	
10	Umair et al. [7]	✓		✓	✓	✓	✓
11	Alginahi et al. [35]	✓	✓		✓	✓	
12	Gutub et al. [78]	✓			✓	✓	
13	Lee et al. [93]	✓		✓	✓	✓	
14	Bender et al. [94]	✓			✓	✓	
15	Lu et al. [95]		✓		✓	✓	✓
16	Mali et al. [24]	✓			✓	✓	✓
17	Halvani et al. [96]	✓		✓	✓	✓	✓
18	Kim et al. [66]		✓		✓	✓	✓
19	Meral et al. [97]		✓	✓	✓	✓	✓
20	Topkara et al. [98]	✓			✓	✓	✓

data and balance between robustness, capacity, and imperceptibility. Most of the prior techniques are either robust or imperceptible or improves the hiding capacity but failed to maintain the balance between all these parameters.

11.4. Sensitive Information Protection. Sensitive information cannot support the smallest change, such as a slight change in a character or word. When we alter confidential information, then the meaning of the text can change, or the original purpose of the text also changed [106]. This case usually involves religious writings, financial documents, government documents, and political documents. Such issues in text watermarking have been addressed with regard to the protection of the religious scriptures of the Arabic text. A lot of studies address the sensitive issue in text watermarking but not to be resolved yet. A precise text watermarking technique is required to resolve the sensitive issue.

11.5. Confidentiality of Information. Confidentiality or secrecy of information means it is not available for unauthorized persons or organizations. Specific measures need to be taken for information protected from unauthorized persons. Specific techniques must be implemented to control the confidentiality of the content in text watermarking. A suitable technique is required for the protection of information confidentiality.

11.6. Cryptography. The embedded data security must be further secured using cryptography, which helps prevent the key and make sure that watermark information is out of reach for an unauthorized user. A lot of methods have been proposed in the past to solve the copyright issues but still needs improvements. A new security framework is necessary for a trusted organization that relies on text watermarking techniques.

11.7. Language Flexibility. The majority of text watermarking techniques is only applicable for certain languages such as English, Arabic and Chinese, which reduce the usability and applicability of the techniques. It is a core challenge for the researcher to identify a suitable and proper text watermarking technique that should be implemented in any type of text language.

11.8. Document Transformation. When a watermarked document is transformed into other formats like Word to PDF and vice versa, there is a risk of losing the watermark information. It is crucial for the researcher to identify a proper text watermarking technique that supports the format transformation.

12. Recommendations

Text documents belong to almost all companies or organizations, such as banks, audit firms, or any public or private organizations. Both electronic and soft copies of sensitive

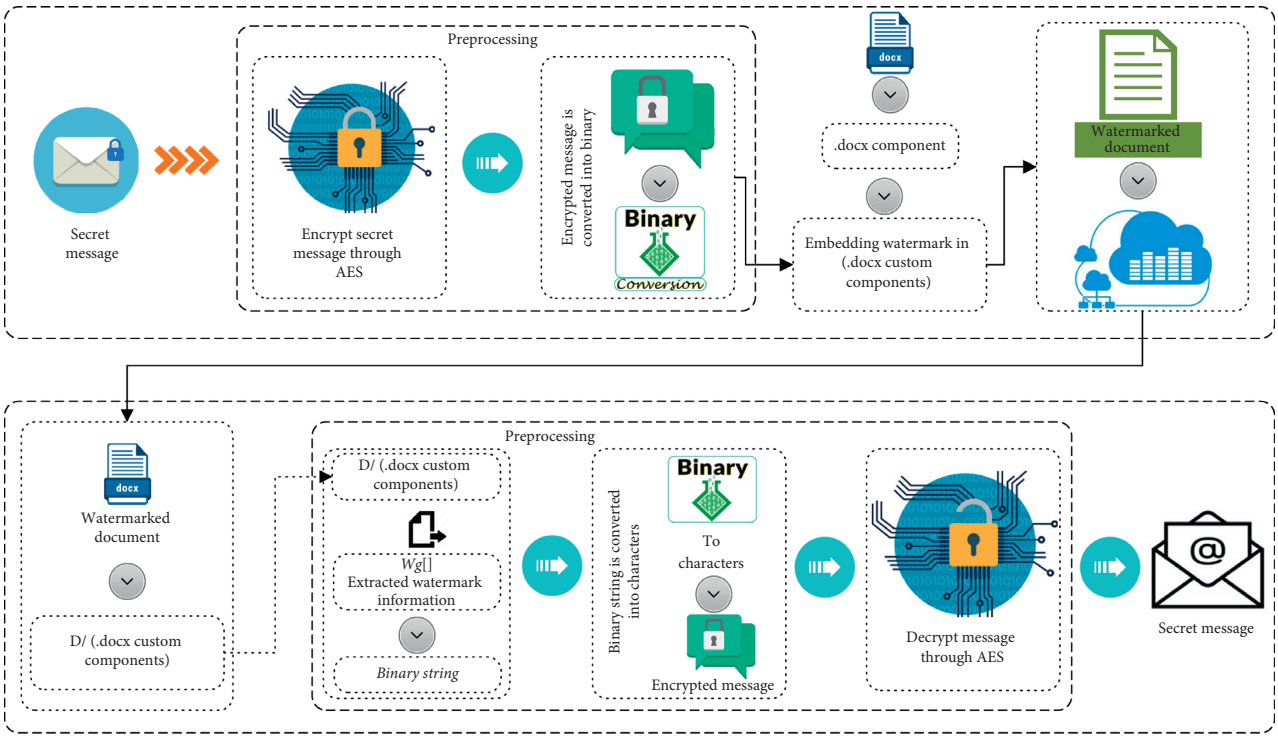


Figure 6: Proposed model for text document security and privacy in IoT.

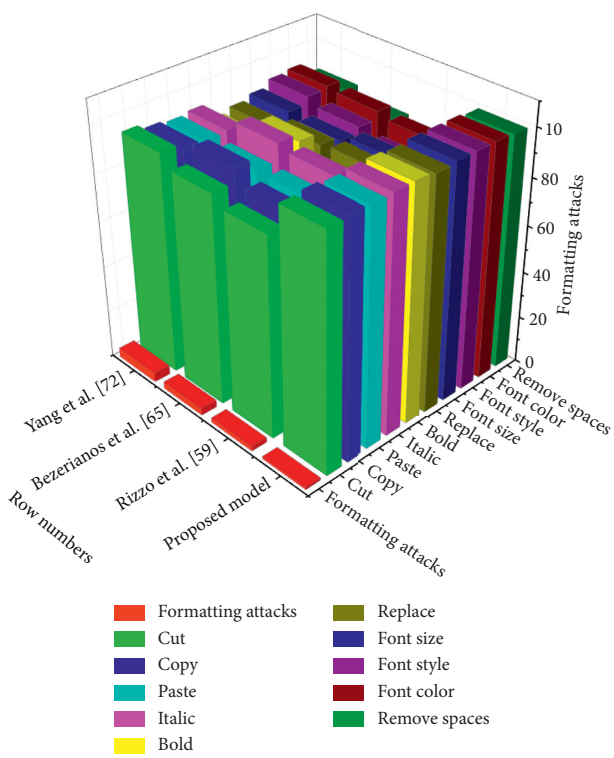


Figure 7: Robustness results of the proposed model with existing techniques.

text documents are processed. Such as soft degrees, birth certificates, legal notes, financial statements, classified reports, and declarations. The challenge is to define a reliable method to authenticate these documents and to guarantee the originality and protection of textual documents by copyright. An appropriate watermark technique is needed that is robust against formatting attacks and improves hiding capacity, imperceptible, and secure. This problem can be solved by a new framework to address the current challenges in text watermarking.

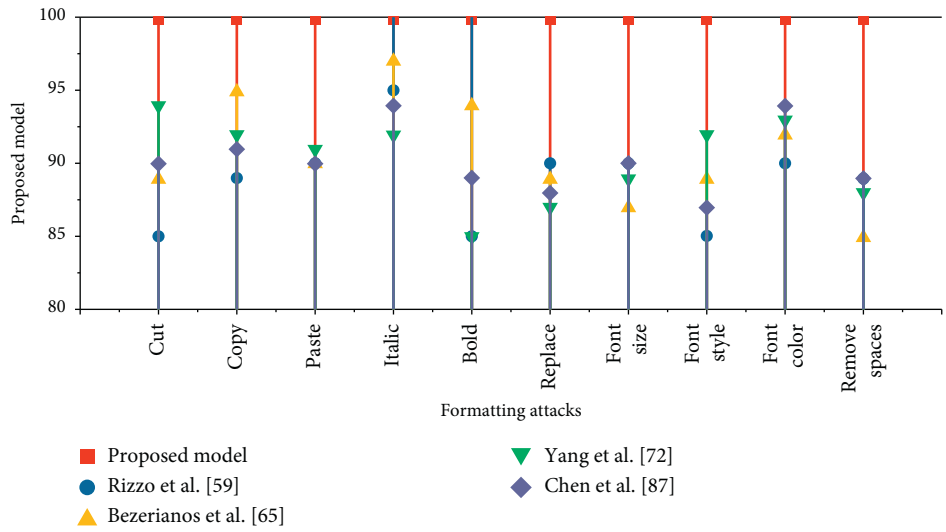


Figure 8: Proposed model and existing technique result against formatting attacks.

12.1. Proposed Model. We proposed a novel framework that overcomes the current challenges of security and privacy in the IoT paradigm based on digital watermarking as shown in Figure 6. The proposed system can provide secure communication of text documents on both local and cloud paradigms. In the proposed framework, the watermark is embedded into the custom properties of a text document. These custom properties are suitable for three reasons. First, they are not referred to with the parts of the primary document. Second, the watermarking process does not change to the original content of the document. Third, it can hide an adequate amount of secret message.

In the proposed model, the secret message (M_S) is given as input, and then in the pre-processing phase, M_S is encrypted through Advanced Encryption Standard (AES). The ASE is a simple encryption technique that is used to secure M_S. The encrypted message (M_E) is converted into a binary string, and then it is divided into n number of groups. The suitable components of the original document D_O are inspected, and M_E groups are embedded into these components. As mentioned above, the custom components are ideal for three reasons, capacity, security, and robustness. M_S has no influence on the original content of the document and does not disturb the imperceptibility. After concealing the secret information, the watermarked document (D_W) is generated that is stored or shared via the local and cloud paradigm.

Through the experimental results, our proposed model achieves excellent results against all the parameters. The proposed method is robust against all formatting attacks and more secure as compared with previous techniques, as revealed in Figure 7. Various kinds of brute force attacks are applied to check the robustness of the watermarked document. These attacks include content and format-based attacks. Figure 8 presents the comparison of the proposed method with [59, 65, 72, 83] against content and format-based attacks, which illustrate that the proposed model is robust against all possible mentioned attacks.

Our system can be applied for copyrights and owner authentication of text documents on both local and cloud computing paradigm. It can also protect the text documents against illegal use.

In addition, through the initial experimental results, we found that the proposed framework is robust, imperceptible, and supports high embedding capacity because the watermark information is stored in document components.

13. Conclusion

In this investigation, we have presented security and privacy issues in IoTs, text watermarking issues, current techniques, attacks, future research direction, and recommendations. We also classified the existing approaches of text watermarking, security and privacy issues. IoT emerging technologies and the latest applications brought new challenges for the researchers to required their attention. We have discussed and summarized the main difficulties for text document protection in IoT. This article deliberated the most common challenges and issues in text watermarking. The text is the most common medium that travels across the internet and needs full protection. Digital text watermarking is more famous for copyright protection and also hides secret information in digital contents. A lot of techniques have been proposed in this field of research, but still a new model that identifies the approaches, requirements, application of text watermarking, and its embedding process is needed. This article deliberated the most common challenges and issues in text watermarking and proposed a novel method. A novel framework for evaluating text watermarking methods is proposed that is easily and readily accessible. It is consulted by the relevant organizations and the research community. The experimental results and analysis prove that the proposed model is robust against content format-based attacks and improves the ability of concealment as compared to the previous techniques. In future research, the main tasks have been marked, and

further investigation in the area of watermarking in IoT is awaited. We also analyzed the other possible attacks in the further, which enhance the robustness and improves the ability of concealment. In future, other Microsoft Word and Excel documents other than special properties will be examined for watermarking. We also investigated the Portable Document Format (PDF) document that is the most popular document format in the world.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] M. Dabbagh and A. Rayes, "Internet of things security and privacy," in *Internet of Things from Hype to Reality*, pp. 211–238, Springer, Berlin, Germany, 2019.

[2] M. A. Habib, M. Ahmad, S. Jabbar, S. H. Ahmed, and J. J. P. C. Rodrigues, "Speeding up the internet of things: LEAIoT: a lightweight encryption algorithm toward low-latency communication for the internet of things," *IEEE Consumer Electronics Magazine*, vol. 7, no. 6, pp. 31–37, 2018.

[3] M. A. Habib, M. Ahmad, S. Jabbar et al., "Security and privacy based access control model for internet of connected vehicles," *Future Generation Computer Systems*, vol. 97, pp. 687–696, 2019.

[4] Colocation America, *Current Security Challenges Facing the Internet of Things*, Colocation America, Los Angeles, CA, USA, 2018.

[5] U. Khadam, M. M. Iqbal, M. A. Azam, S. Khalid, S. Rho, and N. Chilamkurti, "Digital watermarking technique for text document protection using data mining analysis," *IEEE Access*, vol. 7, pp. 64955–64965, 2019.

[6] M. Ahmad, A. Ahmad, S. Jabbar et al., "TCP CUBIC: a transport protocol for improving the performance of TCP in long distance high bandwidth cyber-physical systems," in *Proceedings of the 2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, May 2018.

[7] U. Khadim, "Information hiding in text to improve performance for word document," *International Journal of Technology and Research*, vol. 3, no. 3, p. 50, 2015.

[8] S. D. Lin and Y.-H. Huang, "An integrated watermarking technique with tamper detection and recovery," *International Journal of Innovative Computing, Information and Control*, vol. 5, no. 11, pp. 4309–4316, 2009.

[9] Q. Gu, Q. Han, Q. Gao, and Q. Chen, "A novel adaptive reversible watermarking algorithm based on wavelet lifting scheme," in *Proceedings of the 2009 International Conference on Information Engineering and Computer Science*, December 2009.

[10] I. Ghafir, J. Saleem, M. Hammoudeh et al., "Security threats to critical infrastructure: the human factor," *The Journal of Supercomputing*, vol. 74, no. 10, pp. 4986–5002, 2018.

[11] H.-N. Dai, H. Wang, G. Xu, J. Wan, and M. Imran, "Big data analytics for manufacturing internet of things: opportunities, challenges and enabling technologies," *Enterprise Information Systems*, pp. 1–25, 2019.

[12] C. Alcaraz, *Security and Privacy Trends in the Industrial Internet of Things*, Springer, Berlin, Germany, 2019.

[13] K. R. Sollins, "IoT big data security and privacy versus innovation," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1628–1635, 2019.

[14] M. M. Gaber, A. Aneiba, S. Basurra et al., "Internet of Things and data mining: from applications to techniques and systems," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 9, no. 3, Article ID e1292, 2019.

[15] H.-J. Kim, H.-J. Chang, H.-J. Suh, and H.-J. Shon, "A study on device security in IoT convergence," in *Proceedings of the 2016 International Conference on Industrial Engineering, Management Science and Application (ICIMSA)*, May 2016.

[16] X. Zheng, Z. Cai, and Y. Li, "Data linkage in smart internet of things systems: a consideration from a privacy perspective," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 55–61, 2018.

[17] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: research issues and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2188–2204, 2018.

[18] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[19] S. Sicari, A. Rizzardi, L. A. Rizzardi, and A. Coen-Porisini, "Security, privacy and trust in internet of things: the road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[20] L. Mainetti, L. Manco, L. Patrono, I. Sergi, and R. Vergallo, "Web of topics: an iot-aware model-driven designing approach," in *Proceedings of the 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, December 2015.

[21] A. Čolaković and M. Hadžialić, "Internet of Things (IoT): a review of enabling technologies, challenges, and open research issues," *Computer Networks*, vol. 144, pp. 17–39, 2018.

[22] X. Zhou, W. Zhao, Z. Wang, and L. Pan, "Security theory and attack analysis for text watermarking," in *Proceedings of the 2009 International Conference on E-Business and Information System Security*, May 2009.

[23] Z. Jalil and A. M. Mirza, "A Review of Digital Watermarking Techniques for Text documents," in *Proceedings of the 2009 International Conference on Information and Multimedia Technology*, December 2009.

[24] M. L. Mali, N. N. Patil, and J. Patil, "Implementation of text watermarking technique using natural language watermarks," in *Proceedings of the 2013 International Conference on Communication Systems and Network Technologies*, June 2013.

[25] X. Liu, J. Zhang, H. Wang, X. Gong, and X. Cheng, "A novel text watermarking algorithm based on graphic watermarking framework," in *Proceedings of the 2014 Ninth International Conference on Broadband and Wireless Computing, Communication and Applications*, November 2014.

[26] A. M. Hamdan and A. Hamarsheh, "AH4S: an algorithm of text in text steganography using the structure of omega network," *Security and Communication Networks*, vol. 9, no. 18, pp. 6004–6016, 2016.

[27] N. S. Kamaruddin, A. Kamsin, L. Y. Por, and H. S. Rahman, "A review of text watermarking: theory, methods and applications," *IEEE Access*, vol. 6, pp. 8011–8028, 2018.

[28] M. Barni, I. Cox, T. Kalker, and H. J. Kim, "Digital Watermarking," in *Proceedings of the 4th International Workshop, IWDW 2005*, vol. 3710, Springer, Siena, Italy, September 2005.

[29] M. Taleby Ahvanooey, H. Dana Mazraeh, and S. H. Tabasi, "An innovative technique for web text watermarking

(AITW)," *Information Security Journal: A Global Perspective*, vol. 25, no. 4-6, pp. 191–196, 2016.

[30] A. A. Mohamed, "An improved algorithm for information hiding based on features of Arabic text: a Unicode approach," *Egyptian Informatics Journal*, vol. 15, no. 2, pp. 79–87, 2014.

[31] M. Talebi Ahvanooei and S. H. Tabasi, "A new method for copyright protection in digital text documents by adding hidden unicode characters in Persian/English texts," *International Journal of Current Life Sciences*, vol. 4, no. 8, pp. 4895–4900, 2014.

[32] M. T. Ahvanooei, S. H. Tabasi, and S. Rahmani, "A novel approach for text watermarking in digital documents by zero-width interword distance changes," *DAV International Journal of Science*, vol. 4, no. 3, pp. 550–558, 2015.

[33] Z. Jalil and A. M. Mirza, "A robust zero-watermarking algorithm for copyright protection of text documents," *Journal of the Chinese Institute of Engineers*, vol. 36, no. 2, pp. 180–189, 2013.

[34] M. Bashardoost, M. S. M. Rahim, and N. Hadipour, "A novel zero-watermarking scheme for text document authentication," *Jurnal Teknologi*, vol. 75, no. 4, pp. 49–56, 2015.

[35] Y. M. Alginahi, M. N. Kabir, and O. Tayan, "An enhanced Kashida-based watermarking approach for increased protection in Arabic text-documents based on frequency recurrence of characters," *International Journal of Computer and Electrical Engineering*, vol. 6, no. 5, pp. 381–392, 2014.

[36] L. Y. Tayan, K. Wong, and K. O. Chee, "UniSpaCh: a text-based data hiding method using Unicode space characters," *Journal of Systems and Software*, vol. 85, no. 5, pp. 1075–1082, 2012.

[37] M. Dalla Preda and M. Pasqua, "Software watermarking: a semantics-based approach," *Electronic Notes in Theoretical Computer Science*, vol. 331, pp. 71–85, 2017.

[38] K. Gopalakrishnan, N. Memon, and P. L. Vora, "Protocols for watermark verification," *IEEE MultiMedia*, vol. 8, no. 4, pp. 66–70, 2001.

[39] M. Naseri, S. Heidari, M. Baghfalaki et al., "A new secure quantum watermarking scheme," *Optik*, vol. 139, pp. 77–86, 2017.

[40] M. H. Shirali-Shahreza and M. Shirali-Shahreza, "A new synonym text steganography," in *Proceedings of the 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, August 2008.

[41] Z. Jalil and A. M. Mirza, "Text watermarking using combined image-plus-text watermark," in *Proceedings of the 2010 Second International Workshop on Education Technology and Computer Science*, March 2010.

[42] A. M. Alattar and O. M. Alattar, "Watermarking electronic text documents containing justified paragraphs and irregular line spacing," in *Proceedings of the Security, Steganography, and Watermarking of Multimedia Contents VI*, San Jose, CA, USA, January 2004.

[43] R. Petrovic, B. Tehranchi, and J. M. Winograd, "Security of copy-control watermarks," in *Proceedings of the 2007 8th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services*, September 2007.

[44] M. H. Alkawaz, G. Sulong, T. Saba, A. S. Almazyad, and A. Rehman, "Concise analysis of current text automation and watermarking approaches," *Security and Communication Networks*, vol. 9, no. 18, pp. 6365–6378, 2016.

[45] P. Singh and R. Chadha, "A survey of digital watermarking techniques, applications and attacks," *International Journal of Engineering and Innovative Technology (IJEIT)*, vol. 2, no. 9, pp. 165–175, 2013.

[46] C. Kumar, A. K. Singh, and P. Kumar, "A recent survey on image watermarking techniques and its application in e-governance," *Multimedia Tools and Applications*, vol. 77, no. 3, pp. 3597–3622, 2018.

[47] M. Agarwal, "Text steganographic approaches: a comparison," 2013, https://arxiv.org/abs/1302.2718.

[48] J. Guru and H. Damecha, "Digital watermarking classification: a survey," *International Journal of Computer Science Trends and Technology (IJCST)*, vol. 5, pp. 8–13, 2014.

[49] H. Kabetta and B. Y. Dwiandiyanta, "Information hiding in CSS: a secure scheme text-steganography using public key cryptosystem," 2012, https://arxiv.org/abs/1201.1968.

[50] M. Nazari, A. Sharif, and M. Mollaeefar, "An improved method for digital image fragile watermarking based on chaotic maps," *Multimedia Tools and Applications*, vol. 76, no. 15, pp. 16107–16123, 2017.

[51] M. Shirali-Shahreza, "Text steganography by changing words spelling," in *Proceedings of the 2008 10th International Conference on Advanced Communication Technology*, February 2008.

[52] N. A. S. Al-maweri, "Robust digital text watermarking algorithm based on unicode extended characters," *Indian Journal of Science and Technology*, vol. 9, no. 48, 2016.

[53] L. Robert and T. Shanmugapriya, "A study on digital watermarking techniques," *International Journal of Recent Trends in Engineering*, vol. 1, no. 2, pp. 223–225, 2009.

[54] J.-M. Shieh, D.-C. Lou, and M.-C. Chang, "A semi-blind digital watermarking scheme based on singular value decomposition," *Computer Standards & Interfaces*, vol. 28, no. 4, pp. 428–440, 2006.

[55] L. Gongshen, X. Ding, B. Su, and K. Meng, "A text information hiding algorithm based on alternatives," *Journal of Software*, vol. 8, no. 8, 2013.

[56] J. T. Brassil, S. Low, N. F. Maxemchuk, and L. O'Gorman, "Electronic marking and identification techniques to discourage document copying," *IEEE Journal on Selected Areas in Communications*, vol. 13, no. 8, pp. 1495–1504, 1995.

[57] J. Brassil, "Hiding information in document images," in *Proceedings of the Conference Information Sciences and Systems (CISS-95)*, pp. 482–489, Johns Hopkins University, Baltimore, MD, USA, 1995.

[58] Q. G. Mei, E. K. Wong, and N. D. Memon, "Data hiding in binary text documents," in *Proceedings of the Security and Watermarking of Multimedia Contents III. International Society for Optics and Photonics*, San Jose, CA, USA, 2001.

[59] Y.-W. Kim, K.-A. Moon, and I.-S. Oh, "A text watermarking algorithm based on word classification and inter-word space statistics," in *Proceedings of the ICDAR*, Edinburgh, UK, August 2003.

[60] X. Zhou, S. Wang, W. Zhao, and R. Peng, "A semi-fragile watermarking scheme for content authentication of Chinese text documents," in *Proceedings of the 2009 2nd IEEE International Conference on Computer Science and Information Technology*, August 2009.

[61] L. He, "A part-of-speeach tag sequence text zero-watermarking," in *Proceedings of the Second Symposium International Computer Science and Computational Technology (ISCSCT'09)*, Citeseer, Huangshan, China, December 2009.

[62] Y. Meng, T. Guo, Z. Guo, and L. Gao, "Chinese text zero-watermark based on sentence's entropy," in *Proceedings of the 2010 International Conference on Multimedia Technology*, October 2010.

[63] Z. Jalil, H. Aziz, S. B. Shahid, M. Arif, and A. M. Mirza, "A zero text watermarking algorithm based on non-vowel ASCII characters," in *Proceedings of the 2010 International Conference on Educational and Information Technology*, September 2010.

[64] Z. Jalil and A. M. Mirza, "An invisible text watermarking algorithm using image watermark," in *Innovations in Computing Sciences and Software Engineering*, pp. 147–152, Springer, Berlin, Germany, 2010.

[65] W. Cheng, H. Feng, and C. Yang, "A robust text digital watermarking algorithm based on fragments regrouping strategy," in *Proceedings of the 2010 IEEE International Conference on Information Theory and Information Security*, December 2010.

[66] M.-Y. Kim, O. R. Zaiane, and R. Goebel, "Natural language watermarking based on syntactic displacement and morphological division," in *Proceedings of the 2010 IEEE 34th Annual Computer Software and Applications Conference Workshops*, July 2010.

[67] Y. Meng, L. Gao, X. Wang, and T. Gao, "Chinese text zero-watermark based on space model," in *Proceedings of the 2011 3rd International Workshop on Intelligent Systems and Applications*, May 2011.

[68] F. N. Al-Wesabi, A. Z. Alshakaf, and K. U. Vasantrao, "A zero text watermarking algorithm based on the probabilistic weights for content authentication of text documents," in *IJCA Proceedings on National Conference on Recent Trends in Computing (NCRTC)*, pp. 26–31, Foundation of Computer Science, New York, USA, May 2012.

[69] Y. M. Alginahi, O. Tayan, and M. N. Kabir, "A zero-watermarking verification approach for Quranic verses in online text documents," in *Proceedings of the 2013 Taibah University International Conference on Advances in Information Technology for the Holy Quran and Its Sciences*, December 2013.

[70] Y. M. Alginahi, O. Tayan, and M. N. Kabir, "An adaptive zero-watermarking approach for authentication and protection of sensitive text documents," in *Proceedings of the International Conference on Advances in Computer and Information Technology—ACIT 2013*, Kuala Lumpur, Malaysia, May 2013.

[71] F. M. Ba-Alwi, M. M. Ghilan, and F. N. Al-Wesabi, "Content authentication of English text via internet using zero watermarking technique and Markov model," *International Journal of Applied Information Systems (IJAIS)*, vol. 7, no. 1, pp. 25–36, 2014.

[72] Y. Zhang, H. Qin, and T. Kong, "A novel robust text watermarking for word document," in *Proceedings of the 2010 3rd International Congress on Image and Signal Processing*, October 2010.

[73] J. Chen, J. Yang, J. Ma, and J. Lu, "Text watermarking algorithm based on semantic role labeling," in *Proceedings of the 2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC)*, July 2016.

[74] C. Xiao, C. Zhang, and C. Zheng, "FontCode: embedding information in text documents using glyph perturbation," 2017, https://arxiv.org/abs/1707.09418.

[75] R. A. Alotaibi and L. A. Elrefaei, "Improved capacity Arabic text watermarking methods based on open word space," *Journal of King Saud University-Computer and Information Sciences*, vol. 30, no. 2, pp. 236–248, 2017.

[76] Q. Wen, Y. Wang, and P. Li, "Two Zero-Watermark methods for XML documents," *Journal of Real-Time Image Processing*, vol. 14, no. 1, pp. 183–192, 2018.

[77] S. Hakak, A. Kamsin, J. Veri, R. Ritonga, and T. Herawan, "A framework for authentication of digital Quran," in *Information Systems Design and Intelligent Applications*, pp. 752–764, Springer, Berlin, Germany, 2018.

[78] A. A.-A. Gutub, F. Al-Haidari, K. M. Al-Kahsah, and J. Hamodi, "E-Text watermarking: Utilizing "Kashida" extensions in Arabic language electronic writing," *Journal of Emerging Technologies in Web Intelligence*, vol. 2, no. 1, pp. 48–55, 2010.

[79] H. Yang and A. C. Kot, "Text document authentication by integrating inter character and word spaces watermarking," in *Proceedings of the 2004 IEEE International Conference on Multimedia and Expo (ICME) (IEEE Cat. No.04TH8763)*, June 2004.

[80] Y. M. Alginahi, M. N. Kabir, and O. Tayan, "An enhanced Kashida-based watermarking approach for Arabic text-documents," in *Proceedings of the International Conference on Electronics, Computer and Computation (ICECCO)*, November 2013.

[81] R. J. Jaiswal and N. N. Patil, "Implementation of a new technique for web document protection using unicode," in *Proceedings of the 2013 International Conference on Information Communication and Embedded Systems (ICICES)*, Febuary 2013.

[82] N. Mir, "Copyright for web content using invisible text watermarking," *Computers in Human Behavior*, vol. 30, pp. 648–653, 2014.

[83] Y. Liu, Y. Zhu, and G. Xin, "A zero-watermarking algorithm based on merging features of sentences for Chinese text," *Journal of the Chinese Institute of Engineers*, vol. 38, no. 3, pp. 391–398, 2015.

[84] O. W. Liang and V. Iranmanesh, "Information hiding using whitespace technique in microsoft word," in *Proceedings of the 2016 22nd International Conference on Virtual System & Multimedia (VSMM)*, October 2016.

[85] M. Yingjie, L. Huiran, S. Tong, and T. Xiaoyu, "A zero-watermarking scheme for prose writings," in *Proceedings of the 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, October 2017.

[86] M. Kuribayashi, T. Fukushima, and N. Funabiki, *Data Hiding for Text Document in PDF File*, Springer International Publishing, Cham, Switzerland, 2018.

[87] A. Taha, A. S. Hammad, and M. M. Selim, "A high capacity algorithm for information hiding in Arabic text," *Journal of King Saud University-Computer and Information Sciences*, 2018.

[88] L. Tan, K. Hu, X. Zhou, R. Chen, and W. Jiang, "Print-scan invariant text image watermarking for hardcopy document authentication," *Multimedia Tools and Applications*, vol. 78, no. 10, pp. 13189–13211, 2018.

[89] S. Al-Nofaie, M. Fattani, and A. A.-A. Gutub, "Capacity improved Arabic text steganography technique utilizing 'kashida'with whitespaces," in *Proceedings of the 3rd International Conference on Mathematical Sciences and Computer Engineering (ICMSCE 2016)*, Lankawi, Malaysia, February 2016.

[90] S. G. Rizzo, F. Bertini, D. Montesi, and C. Stomeo, "Text watermarking in social media," in *Proceedings of the 2017 IEEE/ACM International Conference on Advances in*

Social Networks Analysis and Mining-ASONAM '17, July 2017.

[91] R. A. Alotaibi and L. A. Elrefaei, "Utilizing word space with pointed and un-pointed letters for Arabic text watermarking," in *Proceedings of the 2016 UKSim-AMSS 18th International Conference on Computer Modelling and Simulation (UKSim)*, April 2016.

[92] Y.-C. Chou, C.-Y. Huang, and H.-C. Liao, "A reversible data hiding scheme using cartesian product for HTML file," in *Proceedings of the 2012 Sixth International Conference on Genetic and Evolutionary Computing*, August 2012.

[93] I.-S. Lee and W.-H. Tsai, "Secret communication through web pages using special space codes in HTML files," *International Journal of Applied Science and Engineering*, vol. 6, no. 2, pp. 141–149, 2008.

[94] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Systems Journal*, vol. 35, no. 3.4, pp. 313–336, 1996.

[95] H. Lu, G. P. Ma, D. Y. Fang, and X. L. Gui, "Resilient natural language watermarking based on pragmatics," in *Proceedings of the 2009 IEEE Youth Conference on Information, Computing and Telecommunication*, September 2009.

[96] O. Halvani, M. Steinebach, P. Wolf, and R. Zimmermann, "Natural language watermarking for German texts," in *Proceedings of the First ACM Workshop on Information Hiding and Multimedia Security*, June 2013.

[97] H. M. Meral, B. Sankur, A. Sumru Özsoy, T. Güngör, and E. Sevinç, "Natural language watermarking via morphosyntactic alterations," *Computer Speech & Language*, vol. 23, no. 1, pp. 107–125, 2009.

[98] U. Topkara, M. Topkara, and M. J. Atallah, "The hiding virtues of ambiguity: quantifiably resilient watermarking of natural language text through synonym substitutions," in *Proceedings of the 8th Workshop on Multimedia and Security-MM&Sec '06*, September 2006.

[99] K. Bennett, *Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text*, Purdue University, West Lafayette, IN, USA, 2004.

[100] D. Huang and H. Yan, "Interword distance changes represented by sine waves for watermarking text images," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 11, no. 12, pp. 1237–1245, 2001.

[101] M. Khairullah, "A novel text steganography system using font color of the invisible characters in microsoft word documents," in *Proceedings of the 2009 Second International Conference on Computer and Electrical Engineering*, December 2009.

[102] L. Guoyuan and W. Guohui, "A new information hiding method based on word 2007," in *Proceedings of the IEEE 2nd International Conference on Software Engineering and Service Science*, July 2011.

[103] H. H. Nasereddin, "Digital watermarking a technology overview," *International Journal of Research and Reviews in Applied Sciences*, vol. 6, no. 1, pp. 89–93, 2011.

[104] M. M. Iqbal, U. Khadam, K. J. Han, J. Han, and S. Jabbar, "A robust digital watermarking algorithm for text document copyright protection based on feature coding," in *Proceedings of the 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, June 2019.

[105] J. E. Boritz, "IS practitioners' views on core concepts of information integrity," *International Journal of Accounting Information Systems*, vol. 6, no. 4, pp. 260–279, 2005.

[106] S. Hakak, A. Kamsin, O. Tayan, M. Y. Idna Idris, and G. Amin Gilkar, "Approaches for preserving content integrity of sensitive online Arabic content: a survey and research challenges," *Information Processing & Management*, vol. 56, no. 2, pp. 367–380, 2017.

Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 3805058, 15 pages
https://doi.org/10.1155/2020/3805058

Research Article

A Robust IoT-Based Three-Factor Authentication Scheme for Cloud Computing Resistant to Session Key Exposure

Feifei Wang,[1] **Guosheng Xu**,[1,2] **Guoai Xu**,[1,2] **Yuejie Wang**,[3] **and Junhao Peng**[4]

[1]*Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2]*National Engineering Laboratory of Mobile Network Security, Beijing 100876, China*
[3]*Peking University, Beijing 100871, China*
[4]*Guangzhou University, Guangzhou 510006, China*

Correspondence should be addressed to Guosheng Xu; guoshengxu@bupt.edu.cn

Received 1 November 2019; Revised 5 January 2020; Accepted 20 January 2020; Published 18 February 2020

Academic Editor: Ghufran Ahmed

With the development of Internet of Things (IoT) technologies, Internet-enabled devices have been widely used in our daily lives. As a new service paradigm, cloud computing aims at solving the resource-constrained problem of Internet-enabled devices. It is playing an increasingly important role in resource sharing. Due to the complexity and openness of wireless networks, the authentication protocol is crucial for secure communication and user privacy protection. In this paper, we discuss the limitations of a recently introduced IoT-based authentication scheme for cloud computing. Furthermore, we present an enhanced three-factor authentication scheme using chaotic maps. The session key is established based on Chebyshev chaotic-based Diffie–Hellman key exchange. In addition, the session key involves a long-term secret. It ensures that our scheme is secure against all the possible session key exposure attacks. Besides, our scheme can effectively update user password locally. Burrows–Abadi–Needham logic proof confirms that our scheme provides mutual authentication and session key agreement. The formal analysis under random oracle model proves the semantic security of our scheme. The informal analysis shows that our scheme is immune to diverse attacks and has desired features such as three-factor secrecy. Finally, the performance comparisons demonstrate that our scheme provides optimal security features with an acceptable computation and communication overheads.

1. Introduction

With the rapid growth of Internet of Things (IoT) technologies, Internet-enabled devices have had a tremendous impact on people's works and lives [1–3]. However, the Internet-enabled devices have limited storage, computing power, and communication ability. To solve this limitation, cloud computing emerged as a new service paradigm [4]. It provides a new method with high efficiency and convenience to realize information and resource sharing. The users are able to access the resources, services, or applications that are deployed in distributed cloud servers by utilizing a handheld device anywhere and anytime. And the control server is in charge of authorizing the users and distributed servers.

As the communication channel is open and unprotected, there are diverse and severe security threats for stealing sensitive data and resource in cloud computing environment [5, 6]. An authentication protocol is indispensable to prevent unauthorized access and protect the sensitive data and user privacy. From the first smart card-based authentication protocol [7] introduced by Yang and Shieh in 1999, there have been a large number of enhanced schemes proposed [2, 8–13]. Based on the authentication factors the user employs, the authentication schemes are divided into two-factor authentication schemes and three-factor authentication schemes. Based on the cryptosystem the authentication scheme adopts, the authentication schemes are divided into hash-based schemes, symmetric cryptosystem-based schemes, and public key cryptosystem-based schemes.

1.1. Related Works. In terms of authentication schemes for cloud computing, some proposals have been presented one after another to improve the security and efficiency [14–17]. In 2015, Tsai and Lo [18] put forward an anonymous authentication protocol using bilinear pairing, in which the user can directly login the distributed server without the help of control server. Afterwards, He et al. [19] revealed that their scheme is not resistant to server impersonation attack and put forward an enhanced scheme. In 2017, Kumari et al. [20] presented a biometric-based authentication protocol employing elliptic curve cryptosystem (ECC). However, their scheme cannot withstand known session-specific temporary information attack and fails to preserve three-factor secrecy. In 2018, Amin et al. [21] pointed out that two anonymous authentication schemes [22, 23] have weaknesses like forgery attack and session key disclosure attack and introduced a hash-based two-factor authentication scheme. Unfortunately, Wang et al. [24] revealed that their scheme still cannot resist session key disclosure attack. In 2019, Mo et al. [25] introduced an ECC-based single-server two-factor authentication protocol. But this protocol is not resistant to stolen-verifier attack. In the same year, Zhou et al. [26] put forward a two-factor authentication scheme employing hash function. But we observe that their scheme suffers from forgery attack and replay attack and does not preserve forward secrecy. For better understanding, we summarize these schemes in Table 1.

Among these schemes, the hash-based schemes [21–23, 26] are highly efficient, but they have diverse vulnerabilities, such as desynchronization attack, forgery attack, and failure to achieve forward secrecy and user anonymity. Wang et al. [27, 28] have demonstrated that public key technique is essential for achieving some security attributes such as user anonymity. However, the existing public key cryptosystem-based schemes [18, 20, 25] still have more or less security vulnerabilities due to design deficiencies. Besides, they have high computation overhead as time-consuming operations such as bilinear pairing and scalar multiplication are involved.

In addition, the security of the session key is a noteworthy issue. The existing schemes are not secure against various session key exposure attacks. A great many schemes such as the schemes in [20, 21, 25, 26] cannot withstand known session-specific temporary information attack. And many schemes such as the schemes in [21–23, 26] cannot provide forward secrecy. Besides, in some schemes like the scheme of Amin et al. [21], the attacker can even reveal the session key when he obtains the smart card [29].

1.2. Motivation and Contributions. The existing schemes suffer from various security defects or involve high computation overhead. The security attributes or the efficiency needs to be improved. In particular, the great majority of schemes fail to guarantee the security of session key, as they are subjected to various session key exposure attacks. It motivates us to present an enhanced authentication scheme that can meet the security requirements at minimum cost and be secure against all the possible session key exposure attacks. We sum up the contributions of the paper as below:

(1) We reveal that Zhou et al.'s scheme [26] does not consider impersonation attack, known session-specific temporary information attack, and forward secrecy.

(2) We put forward an enhanced three-factor authentication scheme using chaotic maps. The session key comprises of a long-term secret value and the secret key generated by Chebyshev chaotic-based Diffie–Hellman key exchange. It can prevent all kinds of session key exposure attacks. The use of Chebyshev chaotic maps contributes to the establishment of secure session key and simultaneously reduces the computation cost.

(3) The Burrows–Abadi–Needham logic proof confirms the completeness of our scheme. The formal analysis under the random oracle model proves the semantic security of session key. And the informal analysis shows that our scheme can resist all kinds of potential attacks and provide desired properties like three-factor secrecy. The performance comparisons demonstrate that our scheme has high security, and its computation and communication overheads are acceptable.

1.3. Organization of the Paper. The rest of the paper is formed as below. We give some background materials in Section 2. We reveal the security defects of Zhou et al.'s scheme in Section 3. We present the enhanced three-factor authentication scheme in Section 4. We discuss the security of our scheme using several widely accepted security analysis methods in Section 5. We present the performance comparisons of our scheme and related schemes in Section 6. The conclusion is given in Section 7.

2. Preliminaries

2.1. Chebyshev Chaotic Maps. According to Zhang [30], the enhanced Chebyshev polynomial is defined as $T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) \bmod p$, where $n \geq 2$, $x \in [-\infty, +\infty]$, and p is a big prime. The Chebyshev polynomials satisfy commutative law, i.e., $T_a(T_b(x)) \equiv T_b(T_a(x)) \bmod p$.

There is a hard mathematical problem on Chebyshev polynomials:

(i) Chebyshev chaotic Diffie–Hellman problem (CHDHP): for given $T_a(x)$, $T_b(x)$, and x, the computation of $T_{ab}(x) \equiv T_a(T_b(x)) \equiv T_b(T_a(x)) \bmod p$ is infeasible.

2.2. Adversary Model. Based on [31], the abilities of adversary are summarized as below:

(i) The adversary can eavesdrop, replay, block, or alter the transmitted messages in open channel

Table 1: Related authentication schemes for cloud computing.

Category	Schemes	Authentication factors	Cryptographic primitive	Security limitations
Public key cryptosystem-based schemes	Tsai and Lo [18]	Three-factor	Bilinear pairing	Server impersonation attack
	He et al. [19]	Two-factor	Bilinear pairing	Inefficient typo detection
	Kumari et al. [20]	Three-factor	Elliptic curve cryptosystem	Known session-specific temporary information attack Fails to preserve three-factor secrecy Stolen-verifier attack
	Mo et al. [25]	Two-factor	Elliptic curve cryptosystem	Forgery attack Replay attack Known session-specific temporary information attack
Hash-based schemes	Amin et al. [21]	Two-factor	Hash function	Off-line guessing attack Session key disclosure attack Fails to preserve forward secrecy Known session-specific temporary information attack
	Xue et al. [22]	Two-factor	Hash function	User anonymity Privileged insider attack Off-line password guessing attack Fails to preserve forward secrecy
	Chuang and Chen [23]	Three-factor	Hash function	User impersonation attack Session key discloser attack Fails to preserve forward secrecy
	Zhou et al. [26]	Two-factor	Hash function	Forgery attack Replay attack Fails to preserve forward secrecy Known session-specific temporary information attack

(ii) When testing forward secrecy, the adversary can obtain control server's master key or cloud server's secret key

(iii) The adversary can disclose the password or the parameters of smart card

(iv) When testing three-factor secrecy, the adversary is capable of obtaining any two kinds of authentication factors

2.3. Notations. The notations of the paper are presented in Table 2.

Table 2: Notations.

Symbols	Description
CS	Control server
$\mathrm{ID}_{\mathrm{CS}}$	Identity of control server
s	Master key of CS
y	Secret value of CS
U_i	User
ID_i, PW_i, b_i	Identity, password, biometric of user
PID_i	Pseudoidentity of user
S_j	Cloud server
SID_j	Identity of cloud server
sm_j	Secret key of cloud server
T_1, T_2, T_3, T_4	Timestamps
SK	Session key
E_k/D_k	Symmetric encryption/decryption algorithm with key k
$\|$	The string concatenation operation
$\oplus$	The bitwise XOR operation
H_1	Hash function
H_2	Biohash function, on the basis of user's biometric B_i, along with a tokenized random number, it outputs a random string

3. Cryptanalysis of Zhou et al.'s Scheme

We briefly review Zhou et al.'s scheme [26] and point out its limitations in this section. In their scheme, the attacker can perform impersonation attack by replaying the intercepted message. Besides, their scheme is vulnerable to two kinds of session key exposure attacks.

3.1. Review of Zhou et al.'s Scheme

3.1.1. User Registration Phase. U_i delivers an enrollment request to CS in this phase.

Step 1: U_i picks his identity ID_i, pseudoidentity PID_i, and password PW_i. Then U_i selects a random number r_i and calculates $P_i = H_1(\mathrm{PW}_i \| r_i)$. Afterwards, U_i delivers the registration request $\{\mathrm{ID}_i, \mathrm{PID}_i\}$ to CS via the secure channel.

Step 2: after getting $\{\mathrm{ID}_i, \mathrm{PID}_i\}$, CS checks if ID_i is valid. If it holds, CS computes $A_i = H_1(\mathrm{PID}_i \| \mathrm{ID}_{\mathrm{CS}} \| s)$ and $B_i = H_1(\mathrm{ID}_i \| s)$. CS saves ID_i in its database and returns $\{A_i, B_i, \mathrm{ID}_{\mathrm{CS}}\}$ to U_i via the secure channel.

Step 3: after receiving $\{A_i, B_i, \mathrm{ID}_{\mathrm{CS}}\}$, U_i computes $C_i = A_i \oplus P_i$, $D_i = B_i \oplus H_1(\mathrm{ID}_i \| P_i)$, and $E_i = r_i \oplus H_1(\mathrm{ID}_i \| \mathrm{PW}_i)$. Then, U_i stores $\langle C_i, D_i, E_i, \mathrm{PID}_i, \mathrm{ID}_{\mathrm{CS}}\rangle$ in the memory of a smart card.

3.1.2. Cloud Server Registration Phase. CS distributes the secret key to S_j in this phase.

Step 1: S_j chooses its identity SID_j and pseudoidentity PSID_j and delivers $\{\mathrm{SID}_j, \mathrm{PSID}_j\}$ to CS via the secure channel.

Step 2: after getting $\{\mathrm{SID}_j, \mathrm{PSID}_j\}$, CS computes $sm_1 = H_1(\mathrm{PSID}_j \| \mathrm{ID}_{\mathrm{CS}} \| s)$ and $sm_2 = H_1(\mathrm{SID}_j \| s)$. CS delivers $\{sm_1, sm_2, \mathrm{ID}_{\mathrm{CS}}\}$ to S_j via the secure channel.

Step 3: S_j keeps $\{sm_1, sm_2, \mathrm{ID}_{\mathrm{CS}}\}$ as secret.

3.1.3. Login and Authentication Phase. U_i and S_j authenticate each other in the assistance of CS as shown in Figure 1.

Step 1: U_i inputs ID_i^* and PW_i^*. The smart card picks a new pseudoidentity $\mathrm{PID}_i^{\mathrm{new}}$, computes $r_i^* = E_i \oplus H_1(\mathrm{ID}_i^* \| \mathrm{PW}_i^*)$, $P_i^* = H_1(\mathrm{PW}_i^* \| r_i^*)$, $A_i^* = C_i \oplus P_i^*$, $B_i^* = D_i \oplus H_1(\mathrm{ID}_i \| P_i^*)$, $f_1 = A_i^* \oplus \alpha$, $f_2 = H_1(\alpha \| \mathrm{PID}_i \| \mathrm{ID}_{\mathrm{CS}}) \oplus \mathrm{ID}_i$, $f_3 = B_i^* \oplus \mathrm{PID}_i^{\mathrm{new}} \oplus H_1(\alpha \| \mathrm{ID}_i)$, and $f_4 = H_1(\mathrm{ID}_i \| \mathrm{PID}_i \| \mathrm{PID}_i^{\mathrm{new}} \| \alpha \| f_3)$, where α is a nonce. The smart card delivers the login request $\{\mathrm{PID}_i, f_1, f_2, f_3, f_4\}$ to S_j via the public channel.

Step 2: upon receiving $\{\mathrm{PID}_i, f_1, f_2, f_3, f_4\}$, S_j picks a new pseudoidentity $\mathrm{PSID}_j^{\mathrm{new}}$. S_j computes $f_5 = sm_1 \oplus \beta$, $f_6 = H_1(\beta \| \mathrm{PSID}_j \| \mathrm{ID}_{\mathrm{CS}}) \oplus \mathrm{SID}_j$, $f_7 = sm_2 \oplus \mathrm{PSID}_j^{\mathrm{new}} \oplus H_1(\beta \| \mathrm{SID}_j)$, and $f_8 = H_1(\mathrm{SID}_j \| \mathrm{PSID}_j \| \mathrm{PSID}_j^{\mathrm{new}} \| \beta \| f_7)$, where β is a random number. S_j sends $\{\mathrm{PID}_i, f_1, f_2, f_3, f_4, \mathrm{PSID}_j, f_5, f_6, f_7, f_8\}$ to CS via the public channel.

Step 3: after receiving $\{\mathrm{PID}_i, f_1, f_2, f_3, f_4, \mathrm{PSID}_j, f_5, f_6, f_7, f_8\}$, CS computes $\alpha = f_1 \oplus H_1(\mathrm{PID}_i \| \mathrm{ID}_{\mathrm{CS}} \| s)$, $\mathrm{ID}_i = f_2 \oplus H_1(\alpha \| \mathrm{PID}_i \| \mathrm{ID}_{\mathrm{CS}})$, $\mathrm{PID}_i^{\mathrm{new}} = f_3 \oplus H_1(\mathrm{ID}_i \| s) \oplus H_1(\alpha \| \mathrm{ID}_i)$, and $f_4' = H_1(\mathrm{ID}_i \| \mathrm{PID}_i \| \mathrm{PID}_i^{\mathrm{new}} \| \alpha \| f_3)$, and verifies if $f_4' = f_4$. If the equation holds, CS computes $\beta = f_5 \oplus H_1(\mathrm{PSID}_j \| \mathrm{ID}_{\mathrm{CS}} \| s)$, $\mathrm{SID}_j = f_6 \oplus H_1(\beta \| \mathrm{PSID}_j \| \mathrm{ID}_{\mathrm{CS}})$, $\mathrm{PSID}_j^{\mathrm{new}} = f_7 \oplus H_1(\mathrm{SID}_j \| s) \oplus H_1(\beta \| \mathrm{SID}_j)$, and $f_8' = H_1(\mathrm{SID}_j \| \mathrm{PSID}_j \| \mathrm{PSID}_j^{\mathrm{new}} \| \beta \| f_7)$, and verifies if $f_8' = f_8$. If it holds, proceed next step, otherwise, the protocol aborts.

Step 4: CS computes $\mathrm{SK} = H_1(\alpha \oplus \beta \oplus \gamma)$, $f_9 = H_1(\mathrm{PSID}_j^{\mathrm{new}} \| \mathrm{ID}_{\mathrm{CS}} \| s) \oplus H_1(\beta \| \mathrm{PSID}_j^{\mathrm{new}})$, $f_{10} = H_1(\mathrm{PSID}_j^{\mathrm{new}} \| \beta \| \mathrm{PSID}_j) \oplus (\alpha \oplus \gamma)$, $f_{11} = H_1(\mathrm{SK} \| f_9 \| f_{10} \| H_1(\mathrm{SID}_j \| s))$, $f_{12} = H_1(\mathrm{PID}_i^{\mathrm{new}} \| \mathrm{ID}_{\mathrm{CS}} \| s) H_1(\alpha \| \mathrm{PID}_i^{\mathrm{new}})$, $f_{13} = H_1(\mathrm{PID}_i^{\mathrm{new}} \| \alpha \| \mathrm{PID}_i) \oplus (\beta \oplus \gamma)$, and $f_{14} = H_1(\mathrm{SK} \| f_{12} \| f_{13} \| H_1(\mathrm{ID}_i \| s))$, where γ is a nonce. CS sends $\{f_9, f_{10}, f_{11}, f_{12}, f_{13}, f_{14}\}$ to S_j.

Step 5: after receiving $\{f_9, f_{10}, f_{11}, f_{12}, f_{13}, f_{14}\}$, S_j computes $(\alpha \oplus \gamma) = f_{10} \oplus H_1(\mathrm{PSID}_j^{\mathrm{new}} \| \beta \| \mathrm{PSID}_j)$, $\mathrm{SK} = H_1(\alpha \oplus \gamma \oplus \beta)$, $f_{11}' = H_1(\mathrm{SK} \| f_9 \| f_{10} \| sm_2)$ and verifies if $f_{11}' = f_{11}$. If it holds, S_j computes $sm_1^{\mathrm{new}} = f_9 \oplus H_1(\beta \| \mathrm{PSID}_j^{\mathrm{new}})$. S_j keeps $sm_1^{\mathrm{new}}, \mathrm{PSID}_j^{\mathrm{new}}$ as secret and removes sm_1, PSID_j. S_j delivers $\{f_{12}, f_{13}, f_{14}\}$ to U_i.

Step 6: after receiving $\{f_{12}, f_{13}, f_{14}\}$, the smart card computes $(\beta \oplus \gamma) = f_{13} \oplus H_1(\mathrm{PID}_i^{\mathrm{new}} \| \alpha \| \mathrm{PID}_i)$, $\mathrm{SK} = H_1(\alpha \oplus \beta \oplus \gamma)$, $f_{14}' = H_1(\mathrm{SK} \| f_{12} \| f_{13} \| B_i^*)$ and checks if $f_{14}' = f_{14}$. If they are equal, the smart card calculates $C_i^{\mathrm{new}} = f_{12} \oplus H_1(\alpha \| \mathrm{PID}_i^{\mathrm{new}}) \oplus P_i$, stores $C_i^{\mathrm{new}}, \mathrm{PID}_i^{\mathrm{new}}$, and removes C_i, PID_i.

3.2. Cryptanalysis of Zhou et al.'s Scheme. In this section, we reveal that Zhou et al.'s scheme suffers from replay attack, user impersonation attack, server impersonation attack, and known session-specific temporary information attack and fails to provide forward secrecy.

3.2.1. Forward Secrecy. Forward secrecy ensures that when the long-term secret is compromised, the attacker still cannot reveal the established session key. In Zhou et al.'s scheme, with the master key s, the attacker can reveal SK as follows:

Step 1: the attacker intercepts $\{\mathrm{PID}_i, f_1, f_2, f_3, f_4\}$ and $\{f_{12}, f_{13}, f_{14}\}$ from the public channel

Step 2: the attacker computes $\alpha = f_1 \oplus H_1(\mathrm{PID}_i \| \mathrm{ID}_{\mathrm{CS}} \| s)$, $\mathrm{ID}_i = f_2 \oplus H_1(\alpha \| \mathrm{PID}_i \| \mathrm{ID}_{\mathrm{CS}})$, $\mathrm{PID}_i^{\mathrm{new}} = f_3 \oplus H_1(\mathrm{ID}_i \| s) \oplus H_1(\alpha \| \mathrm{ID}_i)$, $(\beta \oplus \gamma) = f_{13} \oplus H_1(\mathrm{PID}_i^{\mathrm{new}} \| \alpha \| \mathrm{PID}_i)$, and $\mathrm{SK} = H_1(\alpha \oplus \beta \oplus \gamma)$

When the long-term secret s is compromised, all the established session keys will be disclosed.

3.2.2. User Impersonation Attack. User impersonation attack denotes that the attacker can masquerade as a valid user to login the cloud server. This attack is performed as follows:

Step 1: the attacker intercepts $\{\mathrm{PID}_i, f_1, f_2, f_3, f_4\}$ from the public channel and sends this message to S_j.

Step 2: upon receiving $\{\mathrm{PID}_i, f_1, f_2, f_3, f_4\}$, S_j handles this message and sends $\{\mathrm{PID}_i, f_1, f_2, f_3, f_4, \mathrm{PSID}_j^{\mathrm{new}}, f_5^*, f_6^*, f_7^*, f_8^*\}$ to CS.

Step 3: CS handles the message $\{\mathrm{PID}_i, f_1, f_2, f_3, f_4, \mathrm{PSID}_j^{\mathrm{new}}, f_5^*, f_6^*, f_7^*, f_8^*\}$. As $f_4' = f_4$, $f_8' = f_8^*$, CS sends back $\{f_9^*, f_{10}^*, f_{11}^*, f_{12}^*, f_{13}^*, f_{14}^*\}$ to S_j.

Step 4: S_j handles $\{f_9^*, f_{10}^*, f_{11}^*, f_{12}^*, f_{13}^*, f_{14}^*\}$. As $f_{11}' = f_{11}^*$, S_j sends $\{f_{12}^*, f_{13}^*, f_{14}^*\}$ to the attacker.

S_j and CS believe that $\{\mathrm{PID}_i, f_1, f_2, f_3, f_4\}$ comes from the legitimate user U_i. Without compromising the smart card, the attacker can impersonate the user U_i by replaying $\{\mathrm{PID}_i, f_1, f_2, f_3, f_4\}$. Zhou et al.'s scheme is vulnerable to user impersonation attack.

3.2.3. Server Impersonation Attack. Server impersonation attack denotes that the attacker can masquerade as a valid cloud server to deceive the user. This attack is performed as follows:

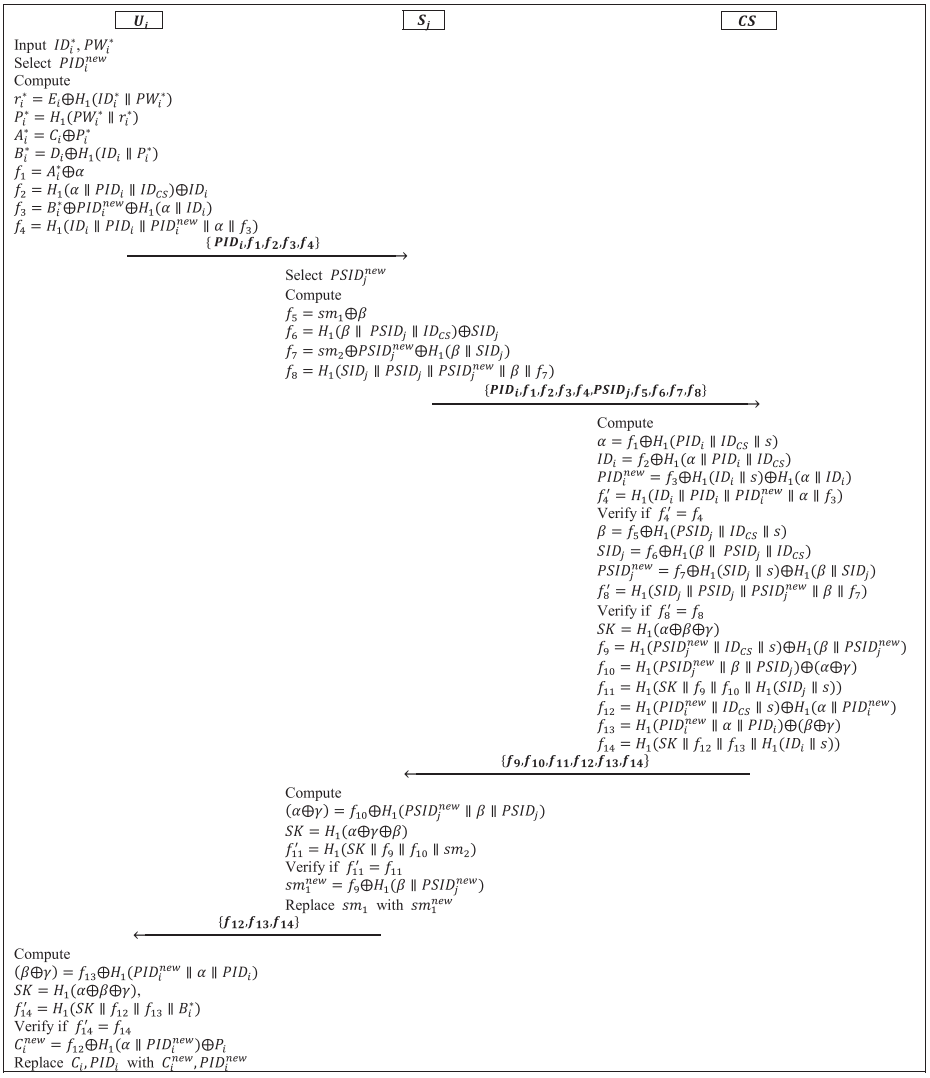


Figure 1: Login and authentication phase of Zhou et al.'s scheme.

Step 1: the attacker intercepts the message $\{\mathrm{PID}_i, f_1, f_2, f_3, f_4, \mathrm{PSID}_j, f_5, f_6, f_7, f_8\}$ from the public channel.

Step 2: when intercepting a new login request $\{\mathrm{PID}_i^{\mathrm{new}}, f_1^*, f_2^*, f_3^*, f_4^*\}$ from the public channel, the attacker sends $\{\mathrm{PID}_i^{\mathrm{new}}, f_1^*, f_2^*, f_3^*, f_4^*, \mathrm{PSID}_j, f_5, f_6, f_7, f_8\}$ to CS.

Step 3: CS handles $\{\mathrm{PID}_i^{\mathrm{new}}, f_1^*, f_2^*, f_3^*, f_4^*, \mathrm{PSID}_j, f_5, f_6, f_7, f_8\}$. As $f_4' = f_4^*$, $f_8' = f_8$, CS returns $\{f_9^*, f_{10}^*, f_{11}^*, f_{12}^*, f_{13}^*, f_{14}^*\}$ to the attacker.

Step 4: the attacker delivers $\{f_{12}^*, f_{13}^*, f_{14}^*\}$ to U_i.

Step 5: after receiving $\{f_{12}^*, f_{13}^*, f_{14}^*\}$, as $f_{14}' = f_{14}^*$, U_i believes that the attacker is the legitimate cloud server S_j.

In $\{\mathrm{PID}_i, f_1, f_2, f_3, f_4, \mathrm{PSID}_j, f_5, f_6, f_7, f_8\}$ that S_j delivers to CS, $\{\mathrm{PSID}_j, f_5, f_6, f_7, f_8\}$ is completely independent with $\{\mathrm{PID}_i, f_1, f_2, f_3, f_4\}$. CS verifies the validity of the two messages independently. It leads that the attacker can impersonate the cloud server by replaying $\{\mathrm{PSID}_j, f_5, f_6, f_7, f_8\}$.

3.2.4. Known Session-Specific Temporary Information Attack. This attack denotes that when the temporary secret such as random number is compromised, the attacker can reveal the established session key. With the random number α, the attacker reveals the session key as follows:

Step 1: the attacker intercepts $\{\mathrm{PID}_i, f_1, f_2, f_3, f_4\}$ and $\{f_{12}, f_{13}, f_{14}\}$ from the public channel.

Step 2: when U_i generates a new login request using $\mathrm{PID}_i^{\mathrm{new}}$ and sends $\{\mathrm{PID}_i^{\mathrm{new}}, f_1^*, f_2^*, f_3^*, f_4^*\}$ to S_j. The attacker intercepts $\{\mathrm{PID}_i^{\mathrm{new}}, f_1^*, f_2^*, f_3^*, f_4^*\}$ from the public channel.

Step 3: the attacker computes $(\beta \oplus \gamma) = f_{13} \oplus H_1(\mathrm{PID}_i^{\mathrm{new}} \| \alpha \| \mathrm{PID}_i)$ and $\mathrm{SK} = H_1(\alpha \oplus \beta \oplus \gamma)$.

In Zhou et al.'s scheme, if the random number α is compromised, the attacker can reveal the session key. Zhou et al.'s scheme is vulnerable to known session-specific temporary information attack.

4. The Proposed Scheme

A robust three-factor authentication scheme for cloud computing is put forward in this section. The proposed scheme is described as below.

4.1. System Setup Phase. CS picks its master key s. CS also selects a nonce y as its secret value. CS picks a hash function $H_1()$ and a symmetric cryptosystem $E_k()/D_k()$. In addition, CS publishes the Chebyshev polynomial's parameters x, p.

4.2. User Registration Phase. U_i transmits the enrollment request to CS in this phase, as shown in Figure 2.

Step 1: U_i selects his identity ID_i and password PW_i as he wishes, imprints his biometric b_i, and calculates $A_i = H_1(\mathrm{PW}_i \| H_2(b_i))$. Then, U_i delivers $\{\mathrm{ID}_i, A_i\}$ to CS through the secure channel.

Step 2: after receiving $\{\mathrm{ID}_i, A_i\}$, CS picks two random numbers t_i, r_1, calculates $C_i = H_1(s\|\mathrm{ID}_i)$, $D_i = A_i \oplus C_i$, $Z_i = H_1(A_i \oplus \mathrm{ID}_i) \bmod \mu$, and $\mathrm{PID}_i = E_y(\mathrm{ID}_i\|r_1)$, where the integer μ satisfies $2^8 \le \mu \le 2^{10}$. CS saves $\{\mathrm{ID}_i, t_i, \mathrm{Counter} = 0\}$ into its database. Moreover, CS stores parameters $\langle D_i, Z_i, \mathrm{PID}_i, t_i, H_1(y\|r_1), \mu\rangle$ in a smart card and delivers it to U_i.

4.3. Cloud Server Registration Phase. CS issues the secret key to S_j in this phase.

Step 1: S_j delivers its identity SID_j to CS through the secure channel.

Step 2: after receiving $\{\mathrm{SID}_j\}$, CS calculates $sm_j = H_1(\mathrm{SID}_j\|s)$. CS sends back $\{sm_j\}$ to S_j through the secure channel.

Step 3: S_j keeps sm_j as secret.

4.4. Login and Authentication Phase. U_i and S_j perform mutual authentication by the aide of CS in this phase, as shown in Figure 3.

Step 1: U_i inputs his identity ID_i^* and password PW_i^* and imprints the biometric b_i^*. Then, the smart card calculates $A_i^* = H_1(\mathrm{PW}_i^*\|H_2(b_i^*))$ and $Z_i^* = H_1(A_i^* \oplus \mathrm{ID}_i^*) \bmod \mu$ and verifies whether Z_i^* is equal to Z_i. If it holds, the smart card calculates $O_i = t_i \oplus H_1(T_1\|H_1(y\|r_1)), C_i^* = D_i \oplus A_i^*, R_i = T_\alpha(x)$, and $L_i = H_1(\mathrm{ID}_i^*\|C_i^*\|R_i\|\mathrm{SID}_j\|O_i\|T_1)$, where α is a nonce and T_1 is the current timestamp. $\{\mathrm{PID}_i, R_i, L_i, O_i, T_1\}$ is delivered to S_j through the open channel.

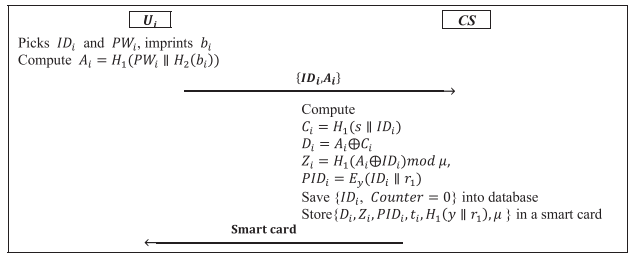


Figure 2: User registration phase.

Step 2: after getting $\{\mathrm{PID}_i, R_i, L_i, O_i, T_1\}$, S_j verifies whether T_1 is fresh. If it holds, S_j generates a random number β and calculates $R_S = T_\beta(x)$, $G_i = H_1(\mathrm{PID}_i\|R_i\|R_S\|sm_j\|T_2)$, $Q_i = H_1(sm_j\|R_i)$, and $N_i = E_{Q_i}(R_S\|G_i)$, where T_2 is the current timestamp. S_j sends $\{\mathrm{PID}_i, R_i, L_i, O_i, T_1, N_i, T_2\}$ to CS via the public channel.

Step 3: after receiving $\{\mathrm{PID}_i, R_i, L_i, O_i, T_1, N_i, T_2\}$, CS checks the freshness of T_2 and computes $(\mathrm{ID}_i\|r_1') = D_y(\mathrm{PID}_i)$, $t_i' = O_i \oplus H_1(T_1\|H_1(y\|r_1'))$, $C_i = H_1(s\|\mathrm{ID}_i)$, and $L_i' = H_1(\mathrm{ID}_i\|C_i\|R_i\|\mathrm{SID}_j\|O_i\|T_1)$ and verifies $t_i' \stackrel{?}{=} t_i$, $L_i' \stackrel{?}{=} L_i$. If $t_i' = t_i$, $L_i' \ne L_i$, the smart card is probably compromised. For the item $\{\mathrm{ID}_i,\ t_i,\ \mathrm{Counter}\}$, CS performs Counter = Counter + 1. When it reaches the preset value, CS suspends U_i. If $t_i' = t_i$, $L_i' = L_i$, CS believes the authenticity of U_i and performs the next step.

Step 4: CS computes $sm_j = H_1(\mathrm{SID}_j\|s)$, $Q_i = H_1(sm_j\|R_i)$, $(R_S'\|G_i') = D_{Q_i}(N_i)$, and $G_i'' = H_1(\mathrm{PID}_i\|R_i\|R_S'\|sm_j\|T_2)$, and verifies $G_i' \oplus G_i''$. If it holds, CS believes the authenticity of S_j. Otherwise, the protocol terminates.

Step 5: CS picks a nonce r_2, computes $\mathrm{PID}_i^{\mathrm{new}} = E_y(\mathrm{ID}_i\|r_2)$, $K_i = H_1(C_i\|R_i)$, $F_i = E_{K_i}(Q_i\|R_S'\|\mathrm{PID}_i^{\mathrm{new}})$, and $M_1 = H_1(sm_j\|R_i\|F_i\|T_3)$, where T_3 is the current timestamp. CS transmits $\{F_i, M_1, T_3\}$ to S_j through the open channel.

Step 6: after getting $\{F_i, M_1, T_3\}$, S_j checks the freshness of T_3 and computes $M_1' = H_1(sm_j\|R_i\|F_i\|T_3)$, and verifies $M_1' \stackrel{?}{=} M_1$. If they are equal, S_j authenticates the user U_i successfully. S_j computes $E_i = T_\beta(R_i)$, $\mathrm{SK} = H_1(E_i\|Q_i)$, and $M_2 = H_1(\mathrm{SK}\|F_i\|Q_i\|T_4)$. S_j transmits $\{F_i, M_2, T_4\}$ to U_i via the public channel.

Step 7: upon receiving $\{F_i, M_2, T_4\}$, the smart card checks the freshness of T_4. Then, the smart card computes $K_i = H_1(C_i^*\|R_i)$, $(Q_i'\|R_S''\|\mathrm{PID}_i^{\mathrm{new}}) = D_{K_i}(F_i)$, $E_i = T_\alpha(R_S'')$, $\mathrm{SK} = H_1(E_i\|Q_i')$, and $M_2' = H_1(\mathrm{SK}\|F_i\|Q_i'\|T_4)$, and checks $M_2' \stackrel{?}{=} M_2$. If it holds, U_i authenticates the cloud server S_j successfully. The smart card replaces PID_i with $\mathrm{PID}_i^{\mathrm{new}}$ in the memory.

4.5. Password Update Phase. The original password is replaced by a new password in this phase.

Step 1: U_i enters ID_i^* and PW_i^* and imprints b_i^*. The smart card calculates $A_i^* = H_1(\mathrm{PW}_i^*\|H_2(b_i^*))$ and $Z_i^* = H_1(A_i^* \oplus \mathrm{ID}_i^*) \bmod \mu$, and verifies whether Z_i^* is equal to Z_i. If they are not equal, the protocol terminates.

Step 2: U_i keys a new password $\mathrm{PW}_i^{\mathrm{new}}$. The smart card computes $A_i^{\mathrm{new}} = H_1(\mathrm{PW}_i^{\mathrm{new}}\|H_2(b_i^*))$, $Z_i^{\mathrm{new}} =$

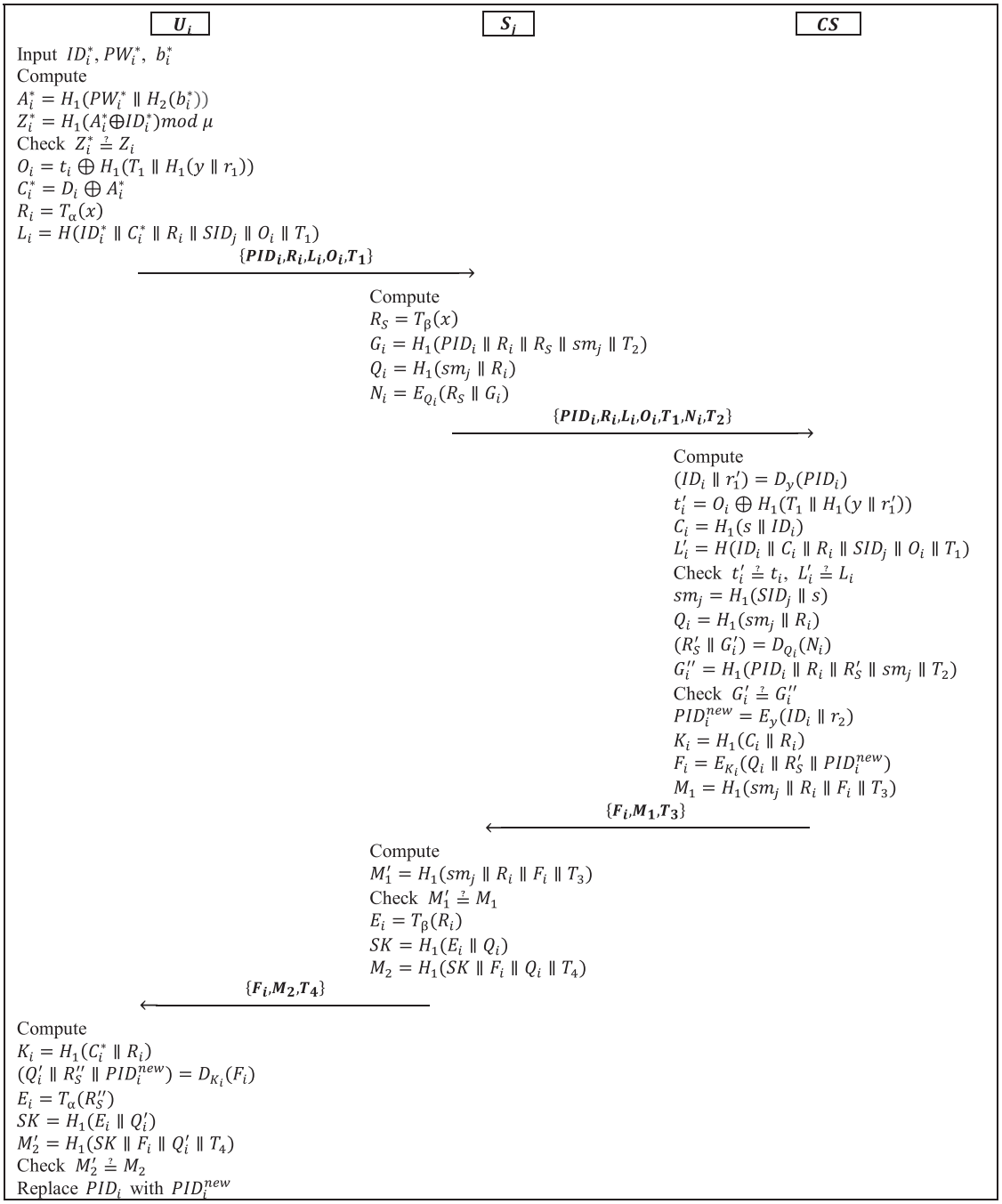


Figure 3: Login and authentication phase of the proposed scheme.

$H_1(A_i^{\text{new}} \oplus \text{ID}_i^*) \text{mod}\, \mu$, and $D_i^{\text{new}} = D_i \oplus A_i^* \oplus A_i^{\text{new}}$. The smart card replaces Z_i, D_i, with Z_i^{new}, D_i^{new}.

5. Security Analysis

In this section, Burrows–Abadi–Needham (BAN) logic [32] proof demonstrates the completeness of our scheme. The formal analysis under the random oracle model shows that our scheme provides semantic security. Moreover, the informal analysis proves that our scheme is not susceptible to known attacks.

5.1. BAN Logic Proof. We confirm the correctness of our scheme in this section. Table 3 lists the notations and rules of BAN logic.

Our scheme ought to fulfil the goals as below.

Goal 1: $S_j| \equiv U_i| \equiv (U_i \overset{\text{SK}}{\longleftrightarrow} S_j)$

Goal 2: $S_j| \equiv (U_i \overset{\text{SK}}{\longleftrightarrow} S_j)$

Goal 3: $U_i| \equiv S_j| \equiv (U_i \overset{\text{SK}}{\longleftrightarrow} S_j)$

Goal 4: $U_i| \equiv (U_i \overset{\text{SK}}{\longleftrightarrow} S_j)$

We idealize our scheme as below:

Table 3: The notations and rules in BAN logic.

Symbols	Description
P, Q	The principals
X	A statement
$P \lhd X$	P see X, P gets a message that consists of X
$P\mid\sim X$	P said X, P sent a message that consists of X
$P\mid\equiv X$	P is convinced that X is true
$P\Longrightarrow X$	P has jurisdiction over X
$P\overset{K}{\longleftrightarrow}Q$	K is a secret shared by P and Q
$\langle X\rangle_K$	X is combined with a secret K
$\{X\}_K$	X is encrypted with a key K
$\#(X)$	X is fresh
Belief rule	$(P\mid\equiv Q\mid\equiv(X,Y)/P\mid\equiv Q\mid\equiv X)$
Message meaning rule (Rule 1)	$(P\mid\equiv P\overset{K}{\longleftrightarrow}Q, P\lhd\langle X\rangle_K/P\mid\equiv Q\mid\sim X)$ or $(P\mid\equiv P\overset{K}{\longleftrightarrow}Q, P\lhd\{X\}_K/P\mid\equiv Q\mid\sim X)$
Nonce-verification rule (Rule 2)	$(P\mid\equiv\#(X), P\mid\equiv Q\mid\sim X/P\mid\equiv Q\mid\equiv X)$
Jurisdiction rule (Rule 3)	$(P\mid\equiv Q\Longrightarrow X, P\mid\equiv Q\mid\equiv X/P\mid\equiv X)$

M1: $U_i \longrightarrow S_j\langle \mathrm{ID}_i, U_i\mid\equiv R_i, T_1\rangle_{C_i}$

M2a: $S_j \longrightarrow \mathrm{CS}\langle \mathrm{ID}_i, U_i\mid\equiv R_i, T_1\rangle_{C_i}$

M2b: $S_j \longrightarrow \mathrm{CS}\left\{\langle \mathrm{PID}_i, R_i, R_S, T_2\rangle_{sm_j}, R_s\right\}_{Q_i}$

M3: $\mathrm{CS} \longrightarrow S_j\left\{U_i\overset{Q_i}{\longleftrightarrow}S_j, R_S, \mathrm{PID}_i^{\mathrm{new}}, R_i\right\}_{K_i}, \langle U_i\mid\equiv R_i, F_i, T_3\rangle_{sm_j}$

M4a: $S_j \longrightarrow U_i\left\{U_i\overset{Q_i}{\longleftrightarrow}S_j, R_S, \mathrm{PID}_i^{\mathrm{new}}, R_i\right\}_{K_i}$

M4b: $S_j \longrightarrow U_i\langle U_i\overset{\mathrm{SK}}{\longleftrightarrow}S_j, F_i, T_4\rangle_{Q_i}$

The analysis of our scheme is based on the following initial assumptions:

A1: $\mathrm{CS}\mid\equiv U_i\overset{C_i}{\longleftrightarrow}\mathrm{CS}$

A2: $\mathrm{CS}\mid\equiv\#(T_1)$

A3: $\mathrm{CS}\mid\equiv U_i\underset{sm_j}{\Rightarrow}U_i\mid\equiv R_i$

A4: $S_j\mid\equiv\mathrm{CS}\overset{}{\longleftrightarrow}S_j$

A5: $S_j\mid\equiv\#(T_3)$

A6: $S_j\mid\equiv\mathrm{CS}\Rightarrow U_i\mid\equiv R_i$

A7: $S_j\mid\equiv U_i\Rightarrow U_i\overset{\mathrm{SK}}{\longleftrightarrow}S_j$

A8: $U_i\equiv U_i\overset{K_i}{\longleftrightarrow}\mathrm{CS}$

A9: $U_i\mid\equiv\#(R_i)$

A10: $U_i\mid\equiv\mathrm{CS}\Rightarrow U_i\overset{Q_i}{\longleftrightarrow}S_j$

A11: $U_i\mid\equiv\#(T_4)$

A12: $U_i\mid\equiv S_j\Rightarrow U_i\overset{\mathrm{SK}}{\longleftrightarrow}S_j$

The analysis of the proposed scheme is as follows. According to M2a, we get

(1) $\mathrm{CS}\lhd\langle \mathrm{ID}_i, U_i\mid\equiv R_i, T_1\rangle_{C_i}$

From (1), A1, applying Rule 1, we get

(2) $\mathrm{CS}\mid\equiv U_i\mid\sim\langle \mathrm{ID}_i, U_i\mid\equiv R_i, T_1\rangle$

From (2), A2, applying Rule 2, we get

(3) $\mathrm{CS}\equiv U_i\mid\equiv(U_i\equiv R_i)$

From (3), A3, applying Rule 3, we get

(4) $\mathrm{CS}\mid\equiv U_i\mid\equiv R_i$

According to M3, we get

(5) $S_j\lhd\langle U_i\mid\equiv R_i, F_i, T_3\rangle_{sm_j}$

From (5), A4, applying Rule 1, we get

(6) $S_j\mid\equiv\mathrm{CS}\mid\sim\langle U_i\mid\equiv R_i, F_i, T_3\rangle$

From (6), A5, applying Rule 2, we get

(7) $S_j\mid\equiv\mathrm{CS}\mid\equiv(U_i\mid\equiv R_i)$

From (7), A6, applying Rule 3, we get

(8) $S_j\mid\equiv U_i\mid\equiv R_i$

From (8), and $\mathrm{SK}=H_1(T_\beta(R_i)\|H_1(sm_j\|R_i))$, we get

(9) $S_j\mid\equiv U_i\mid\equiv U_i\overset{\mathrm{SK}}{\longleftrightarrow}S_j$ **Goal 1**

From (9), A7, applying Rule 3, we get

(10) $S_j\mid\equiv U_i\overset{\mathrm{SK}}{\longleftrightarrow}S_j$ **Goal 2**

According to M4a, we get

(11) $U_i\lhd\left\{U_i\overset{Q_i}{\longleftrightarrow}S_j, R_S, \mathrm{PID}_{\mathrm{new}}, R_i\right\}_{K_i}$

From (11), A8, applying Rule 1, we get

(12) $U_i\mid\equiv\mathrm{CS}\mid\sim\left\{U_i\overset{Q_i}{\longleftrightarrow}S_j, R_S, \mathrm{PID}_{\mathrm{new}}, R_i\right\}$

From (12), A9, applying Rule 2, we get

(13) $U_i\mid\equiv\mathrm{CS}\mid\equiv(U_i\overset{Q_i}{\longleftrightarrow}S_j)$

From (13), A10, applying Rule 3, we get

(14) $U_i\mid\equiv U_i\overset{Q_i}{\longleftrightarrow}S_j$

According to M4b, we get

(15) $U_i\lhd\langle U_i\overset{\mathrm{SK}}{\longleftrightarrow}S_j, F_i, T_4\rangle_{Q_i}$

From (14), (15), applying Rule 1, we get

(16) $U_i\mid\equiv S_j\mid\sim\langle U_i\overset{\mathrm{SK}}{\longleftrightarrow}S_j, F_i, T_4\rangle$

From (16), A11, applying Rule 2, we get

(17) $U_i\mid\equiv S_j\mid\equiv U_i\overset{\mathrm{SK}}{\longleftrightarrow}S_j$ **Goal 3**

From (17), A12, applying Rule 3, we get

(18) $U_i\mid\equiv U_i\overset{\mathrm{SK}}{\longleftrightarrow}S_j$ **Goal 4**

5.2. Formal Security Analysis. Based on the security model of two-factor authentication presented by Wang and Wang [33], we put forward a security model of three-factor authentication for cloud computing. Afterwards, we prove the semantic security of our scheme in this model.

5.2.1. Formal Security Model

(1) Participants. There are multiple instances of the control server CS, the cloud server S_j, and the user U_i in the authentication scheme for cloud computing. We use CS^a, S_j^a, and U_i^a to denote these instances.

(2) Queries. The attacker is capable of making the queries as follows:

Execute $(\mathrm{CS}^a/S_j^a n/U_i^a)$: by making this query, the attacker can obtain the messages delivered via the open channel.

Send $(\mathrm{CS}^a/S_j^a n/U_i^a h, xm)$: by making this query, the attacker can impersonate the principal (U_i^a, S_j^a, GWN^a) to send a message m. If m is valid, a response is sent back to the attacker.

Reveal (S_j^a/U_i^a): by making this query, the attacker can get the session key of (S_j^a/U_i^a), if the principal involves a session key.

Corrupt (U_i^a, τ): by making this query, the attacker is capable of getting one or two types of user authentication information.

When $\tau = 1$, the attacker acquires the password.
When $\tau = 2$, the attacker acquires the smart card.
When $\tau = 3$, the attacker acquires the biometric.

Corrupt (S_j^a/CS^a): by making this query, the attacker can obtain cloud server's secret key or CS's master key. This oracle corresponds to the forward secrecy.

Test (S_j^a/U_i^a): if the principal is fresh (see below) and involves a session key SK, the oracle spins a coin b. When $b = 1$, it sends back SK to the attacker. When $b = 0$, it sends back a random string to the attacker. This oracle is used to simulate the semantic security of session key. The attacker is capable of asking this query only once.

(3) Freshness. We say (S_j^a/U_i^a) is fresh, if the following conditions are met:

(1) (S_j^a/U_i^a) is accepted and involves a SK
(2) The attacker never makes Corrupt (S_j^a/CS^a) or Reveal (S_j^a/U_i^a) query

(4) Semantic Security. After making the above queries, the attacker tries to reveal the value of b in test query. The advantage of the attacker in breaking the semantic security is defined as follows:

$$Adv_P^{ake}(\mathscr{A}) = 2\Pr(b' = b) - 1. \tag{1}$$

If for all the attackers, $Adv_P^{ake}(\mathscr{A})$ is negligible, the authentication scheme provides semantic security.

5.2.2. Formal Security Analysis

Theorem 1. *Let the password space D_{PW} be subject to Zipf distribution [34]. A polynomial-time attacker $\mathscr{A}$ runs against our scheme. We presume $\mathscr{A}$ can ask less than q_e Execute queries, q_s Send queries, q_b Biohash queries, q_h Hash queries, and q_ε Encryption/Decryption queries. We have*

$$Adv_P^{ake}(\mathscr{A}) \le 2C' * q_s^{s'} + \frac{(q_s+q_e)^2}{p} + \frac{6q_s+q_h^2}{2^{l_1}} + \frac{2q_s+q_b^2}{2^{l_2}} + \frac{q_\varepsilon^2}{2^{l_3}} + 2q_h Adv_P^{\mathrm{CHDHP}}, \tag{2}$$

where l_1, l_2, l_3 are the length of hash output, bio-hash output, and symmetric encryption output, respectively. Adv_P^{CHDHP} is the advantage of $\mathscr{A}$ in solving CHDHP. When using the Tianya password distribution [34], we have $|D_{PW}| \approx 13$ million, $C' = 0.062239$, and $s' = 0.155478$.

Proof. In order to obtain $Adv_P^{ake}(\mathscr{A})$, we define the games Φ_i $(0 \le i \le 6)$, where Φ_0 corresponds to the real attack. $\Pr[\chi_i]$ is the advantage of $\mathscr{A}$ in revealing b in game G_i.

Φ_0: as it simulates the real attack, we get,

$$Adv_P^{ake}(\mathscr{A}) = 2(\Pr[\chi_0]) - 1. \tag{3}$$

Φ_1: in this game, a hash list Λ_H is used to simulate the hash oracle. A biohash list Λ_{BH} is used to simulate the biohash oracle. And an encryption/decryption list Λ_ε is used to simulate the encryption/decryption oracle. For a hash query $H_1(\alpha)$, if the hash value of α already exists in Λ_H, the oracle sends back the hash value. Otherwise, the oracle selects a nonce β as the answer of $H_1(\alpha)$ and stores (α, β) in Λ_H. The biohash oracle is performed in the similar way. For an encryption query $E_k(\varphi)$, the oracle firstly uses φ and k to search Λ_ε, If there exists an tuple (k, φ, ω), it answers ω. Otherwise, it sends back a random string ω to the adversary and stores (k, φ, ω) in Λ_ε. For an decryption query $D_k(\omega)$, the oracle uses ω and k to search Λ_ε. If there exists a tuple (k, φ, ω), it answers φ. Otherwise, it sends back a random string φ to the adversary, and stores (k, φ, ω) in Λ_ε. Φ_1 is indistinguishable from Φ_0. We get

$$\Pr[\chi_0] - \Pr[\chi_1] = 0. \tag{4}$$

Φ_2: in this game, we terminate the execution when encountering some collisions.

(1) The collision occurs on the outputs of hash function or biohash function with the probability of $(q_h^2/2^{l_1+1}) + (q_b^2/2^{l_2+1})$
(2) The collision occurs on the outputs of symmetric encryption with the probability of $(q_\varepsilon^2/2^{l_3+1})$
(3) The collision occurs on the transcripts of messages, with the probability of $((q_s+q_e)^2/2p)$

We get

$$|\Pr[\chi_1] - \Pr[\chi_2]| \le \frac{q_h^2}{2^{l_1+1}} + \frac{q_b^2}{2^{l_2+1}} + \frac{q_\varepsilon^2}{2^{l_3+1}} + \frac{(q_s+q_e)^2}{2p}. \tag{5}$$

Φ_3: in this game, we terminate the execution when $\mathscr{A}$ guesses $\{L_i, G_i, M_1, M_2\}$. The probability is at most $(q_s/2^{l_1})$. We get

$$\left|\Pr[\chi_3] - \Pr[\chi_2]\right| \le \frac{q_s}{2^{l_1}}. \quad (6)$$

Φ_4: in this game, we terminate the execution when $\mathscr{A}$ guesses user's authentication value C_i. The probability is less than $(q_s/2^{l_1})$. We obtain

$$\left|\Pr[\chi_4] - \Pr[\chi_3]\right| \le \frac{q_s}{2^{l_1}}. \quad (7)$$

Φ_5: in this game, we terminate the execution when $\mathscr{A}$ has computed C_i with the help of Corrupt (U_i^a, z).

(1) When Corrupt $(U_i^a, z = 1, 2)$, $\mathscr{A}$ is able to guess the biometric with the probability of $(q_s/2^{l_1})$
(2) When Corrupt $(U_i^a, z = 2, 3)$, $\mathscr{A}$ is able to guess the password with the probability of $C' * q_s^{s'}$.
(3) When Corrupt $(U_i^a, z = 1, 3)$, $\mathscr{A}$ is able to guess D_i with the probability of $(q_s/2^{l_1})$.

We obtain

$$\left|\Pr[\chi_5] - \Pr[\chi_4]\right| \le \frac{q_s}{2^{l_1}} + C' * q_s^{s'} + \frac{q_s}{2^{l_1}}. \quad (8)$$

Φ_6: we use the private hash oracle H_1' rather than the hash oracle H_1 to compute the session key. $\mathscr{A}$ knows nothing about H_1'. Thus, we have

$$\Pr[\chi_6] = \frac{1}{2}. \quad (9)$$

Φ_6: it is indistinguishable from Φ_5, unless a hash query $H_1(E_i \| Q_i)$ is made by $\mathscr{A}$. We use Γ_1 to denote this event. We have

$$\left|\Pr[\chi_6] - \Pr[\chi_5]\right| \le \Pr[\Gamma_1]. \quad (10)$$

□

If the hash query $H_1(E_i \| Q_i)$ has been asked, by selecting randomly in Λ_H, we can obtain $E_i = T_\alpha(R_S) = T_\beta(R_i)$ with the probability of $(1/q_h)$. We get

$$\Pr[\Gamma_1] \le q_h Adv_P^{\mathrm{CHDHP}}. \quad (11)$$

From (3)–(11), we have

$$Adv_P^{ake}(\mathscr{A}) \le 2C' * q_s^{s'} + \frac{(q_s + q_e)^2}{p} + \frac{6q_s + q_h^2}{2^{l_1}} + \frac{2q_s + q_b^2}{2^{l_2}} + \frac{q_\varepsilon^2}{2^{l_3}} + 2q_h Adv_P^{\mathrm{CHDHP}}. \quad (12)$$

5.3. Informal Security Analysis. In this section, we prove that our scheme is resistant to diverse attacks. Particularly, our scheme is secure against all kinds of session key exposure attacks, as the session key is generated based on the long-term secret and Chebyshev chaotic-based Diffie–Hellman key exchange. Besides, we demonstrate that the proposed scheme preserves desired properties such as user anonymity and three-factor secrecy.

5.3.1. User Anonymity. In our scheme, only the control server who has the secret key y can retrieve ID_i from PID_i. In addition, after authenticating U_i, CS generates a new pseudoidentity $\mathrm{PID}_i^{\mathrm{new}}$ and delivers the encrypted $\mathrm{PID}_i^{\mathrm{new}}$ to U_i. $\mathrm{PID}_i^{\mathrm{new}}$ is encrypted with the secret key K_i by CS. Only U_i is able to compute K_i and obtain $\mathrm{PID}_i^{\mathrm{new}}$. The attacker knows nothing about $\mathrm{PID}_i^{\mathrm{new}}$, and hence he cannot link $\mathrm{PID}_i^{\mathrm{new}}$ with PID_i. It makes the user identity untraceable. Consequently, our scheme achieves user anonymity.

5.3.2. Resistance to Off-Line Guessing Attack. As the fuzzy verifier Z_i is employed in our scheme as suggested in [33], even if the attacker obtains the smart card as well as biometric at the same time, he is unable to reveal the password. With the smart card and biometric, the attacker chooses one pair of identity and password from dictionary space and checks if $Z_i^* = Z_i$. However, there are a great many candidates conforming to $Z_i^* = Z_i$. In order to distinguish the correct one from so many candidates, there is no alternative but to launch online guessing attack. However, we employ the "honeywords" technique [33] to prevent this attack. When the number of online guessing attacks reaches the preset value, for example, 10, U_i is suspended. Consequently, our scheme can resist off-line guessing attack.

5.3.3. Resistance to Session Key Disclosure Attack. The session key SK is computed using E_i and Q_i. E_i is the secret key generated by the Chebyshev chaotic-based Diffie–Hellman key exchange. Only U_i and S_j who know the random number α or β are able to compute E_i. Q_i is computed based on the long-term secret sm_j. Only S_j and CS who have sm_j are able to compute Q_i. Besides, Q_i is transmitted to U_i by means of symmetric encryption with the secret key $H_1(C_i \| R_i)$. Only U_i and CS who have C_i are able to reveal Q_i. Both E_i and Q_i are unavailable to the attacker. Therefore, our scheme can resist this attack.

5.3.4. Forward Secrecy. Suppose that the attacker has acquired the master key s, he is able to compute Q_i. However, E_i is the secret key generated by the Chebyshev chaotic-based Diffie–Hellman key exchange. To reveal E_i, there is no alternative but to solve the CHDHP. Therefore, our scheme preserves forward secrecy.

5.3.5. Resistance to Session-Specific Temporary Information Attack. Assume that the attacker has acquired the random number α. To compute $E_i = T_\alpha(R_s)$, R_s is required. R_S is encrypted using the secret key Q_i or K_i, where $Q_i = H_1(sm_j \| R_i)$ and $K_i = H_1(C_i \| R_i)$. To retrieve R_S, the attacker needs to reveal C_i or sm_j. Assume that the attacker has acquired the random number β, the attacker can calculate $E_i = T_\beta(R_i)$. Afterwards, to derive Q_i, the attacker has to get C_i or sm_j. However, sm_j is only known to S_j and CS, C_i is only known to U_i and CS. Therefore, the attacker cannot reveal the session key when the nonce is disclosed.

5.3.6. Resistance to Forgery Attack. In our scheme, the hash values (L_i, G_i, M_1, M_2) of the transmitted parameters and

the secret value A_i, sm_j are used to ensure message integrity and verify the sender's identity. As C_i and sm_j are unavailable to the attacker, he cannot generate a message that is verified to be valid by the recipient.

5.3.7. Resistance to Desynchronization Attack. In each message, the hash value (L_i, G_i, M_1, M_2) is used to ensure that the transmitted parameters are not tampered with. If the attacker alters a parameter of a message, the receiver will find that the received hash value is not equal to the one he computes, and the protocol terminates. Besides, if the attacker blocks a message, as it does not change the long-term parameters the participants have, it does not affect the user's next login. For instance, if the attacker blocks the message $\{F_i, M_2, T_4\}$, the user fails to update his pseudoidentity. But with PID_i, the user still is able to access the cloud server.

5.3.8. Resistance to Replay Attack. In the proposed scheme, every message contains a timestamp. And the timestamps are involved in the hash values (L_i, G_i, M_1, M_2). Upon receiving a message, the receiver first verifies whether the timestamp is fresh. If it holds, the receiver continues to process the message. Otherwise, the protocol aborts.

5.3.9. Resistance to Privileged Insider Attack. The user never submits his biometric or password to CS at registration. On the other hand, the user cannot masquerade as a cloud server or CS, as sm_j is unavailable. The cloud server cannot masquerade as a user or CS, as C_i is unavailable. Therefore, our scheme is immune to such an attack.

5.3.10. Resistance to Man-in-the-Middle Attack. In each message, the hash value (L_i, G_i, M_1, M_2) of the transmitted parameters and the secret A_i, sm_j are computed to ensure message integrity and verify the sender's identity. As A_i and sm_j are unavailable, the attacker is unable to generate a valid message to replace the intercepted one. Consequently, the attacker is unable to launch man-in-the-middle attack.

5.3.11. Mutual Authentication. In our scheme, based on the authentication value C_i, CS verifies the authenticity of U_i by checking $L_i' \stackrel{?}{=} L_i$. Based on the secret key sm_j, CS verifies the authenticity of S_j by checking $G_i' \stackrel{?}{=} G_i''$. If $L_i' = L_i$ and $G_i' = G_i''$, CS believes that U_i and S_j are legitimate and sends a response message to S_j. After getting the response message from CS, S_j verifies the authenticity of CS and U_i by checking $M_1' \stackrel{?}{=} M_1$. If it holds, S_j believes that U_i and CS are legitimate and sends back a response message to U_i. Afterwards, U_i verifies the authenticity of CS and S_j by checking $M_2' \stackrel{?}{=} M_2$. If it holds, U_i believes that CS and S_j are legitimate. Therefore, our scheme provides mutual authentication among CS, U_i, and S_j.

5.3.12. Resistance to Eavesdropping Attack. The attacker can intercept messages from public channel. However, the secret parameters such as the user authentication value C_i, the user identity, the cloud server's secret key sm_j, and the session key SK are protected with hash function and symmetric encryption. The attacker cannot acquire any useful information from the intercepted messages and uses them to launch active attacks.

5.3.13. Resistance to All Kinds of Session Key Exposure. The session key consists of two parts, E_i and Q_i. E_i is generated by Chebyshev chaotic-based Diffie–Hellman key exchange. Q_i is computed using the cloud server's secret key as well as a Chebyshev polynomial. The purpose of E_i is to make sure that our scheme can be resistant to known key attack, as well as preserve forward secrecy. The purpose of Q_i is to make sure that our scheme can withstand session-specific temporary information attack. The attacker can reveal neither E_i nor Q_i. Hence, our scheme is resistant to all kinds of session key exposure attacks.

5.3.14. Three-Factor Secrecy. When the attacker reveals the biometric and smart card, he cannot retrieve the password as shown in 5.3.2. When the attacker reveals the smart card and password, he cannot retrieve the biometric from Z_i as the hash function is irreversible. With the biometric and password, the attacker cannot retrieve the critical data of smart card. Hence, our scheme preserves three-factor secrecy.

Most of the existing three-factor authentication schemes fail to preserve three-factory secrecy, because when the biometric and smart card is disclosed, the attacker can guess user's password based on the verification value that is used to verify the validity of the inputted password and biometric in smart card. However, our scheme employs the fuzzy verifier and "honeywords" technique to prevent revealing of the password.

6. Performance Comparisons

We give the comparisons of our scheme and the recently proposed schemes [20, 21, 25, 26, 35, 36] with regard to security attributes, communication, and computation costs in this section.

The security comparison is given in Table 4. Note that, as Mo et al.'s scheme is designed for single-server environment, it only involves a single cloud server. Ghani et al.'s scheme does not establish session key. We summarize the security requirements of authentication protocol, and based on it, we analyzes the security properties of related schemes in Table 4. It indicates that only the proposed scheme meets all the security requirements, while the related schemes have diverse weaknesses. The security of our scheme is superior to the hash function-based schemes [21, 26], the symmetric cryptosystem-based schemes [35, 36], as well as ECC-based schemes [20, 25].

In Table 5, we presents the computation cost, the communication overhead, and the smart card storage cost of the related schemes concerning the login and authentication phase. Furthermore, the computation cost comparison, communication overhead comparison, and smart card

Table 4: Security features of related schemes.

Security properties	Zhou et al. [26]	Amin et al. [21]	Kumari et al. [20]	Mo et al. [25]	Ghani et al. [35]	Martinez-Pelaez et al. [36]	Our scheme
User anonymity	√	√	√	√	×	√	√
Efficient typo detection	×	√	√	√	×	√	√
Resist desynchronization attack	√	√	√	√	×	×	√
Resist off-line guessing attack	√	×	√	√	√	×	√
Resist session key disclosure attack	√	×	√	√	−	×	√
Resist forgery attack	×	×	√	×	×	×	√
Resist replay attack	×	√	√	√	×	√	√
Resist known session-specific temporary information attack	×	×	×	×	−	×	√
Forward secrecy	×	×	√	√	−	×	√
Three-factor secrecy	−	−	×	−	−	−	√
Stolen-verifier attack	√	√	√	×	×	√	√
Resist all kinds of session key exposure attacks	×	×	×	×	−	×	√

Table 5: Computation and communication costs and smart card storage cost of related schemes.

	Computation overhead			Running time (ms)	Communication cost (bits)	Storage cost (bits)
	User	Server	CS			
Zhou et al. [26]	$10T_H$	$7T_H$	$19T_H$	18	3584	640
Amin et al. [21]	$9T_H$	$4T_H$	$10T_H$	11.5	2560	512
Kumari et al. [20]	$2T_{BH} + 5T_H + 3T_P$	$5T_H + 3T_P$	$6T_H + 2T_P$	554.64	2624	576
Mo et al. [25]	$7T_H + 1T_A + 3T_P$	$6T_H + 1T_A + 3T_P$	−	385.998	960	712
Ghani et al. [35]	$2T_H$	$2T_H$	$4T_H + 2T_s$	21.4	1792	384
Martinez-Pelaez et al. [36]	$7T_H + 3T_s$	$6T_H + 3T_s$	$26T_H + 2T_s$	89.1	3456	640
Our scheme	$1T_{BH} + 2T_C + 7T_H + 1T_s$	$5T_H + 2T_C + 1T_s$	$9T_H + 3T_s$	159.1	2304	532

storage cost comparison are shown in Figure 4, Figure 5, and Figure 6, respectively. As shown in Figure 4, the computation overhead of our scheme is not as good as the hash-based schemes and the symmetric cryptosystem-based schemes, as public key operations are used to guarantee the security. But it is obviously better than the ECC-based schemes. As shown in Figure 5, the communication cost of our scheme is higher than Mo et al.'s scheme and Ghani et al.'s scheme, but it is lower than the other schemes. As shown in Figure 6, the storage cost of our scheme is inferior to Amin et al.'s scheme and Ghani et al.'s scheme, but it is superior to the other schemes.

T_H, T_{BH}, T_S, and T_C denote a hash function, a biohash function, a symmetric encryption/decryption, and a Chebyshev polynomial, respectively. T_P and T_A denote a point multiplication and a point addition on elliptic curve group. The computing time of lightweight operation "XOR" is negligible. In accordance with [3, 37], when performed on a smart phone with a Hisilicon kirin 960 CPU, 6 GB RAM, and the storage of 64 GB, the computations of T_H, T_S, T_P, T_A, T_C, and T_{BH} take 0.5 ms, 8.7 ms, 63.075 ms, 0.262 ms, 21.02 ms, and 21.02 ms, respectively. Besides, we assume that the bit length of timestamp, random number, the user identity, the identity of cloud server, the hash value, Chebyshev polynomial, and the output of symmetric encryption are 128 bits. The point on elliptic curve group is 160 bits.

The hash-based schemes and the symmetric cryptosystem-based schemes have obvious advantage in efficiency as

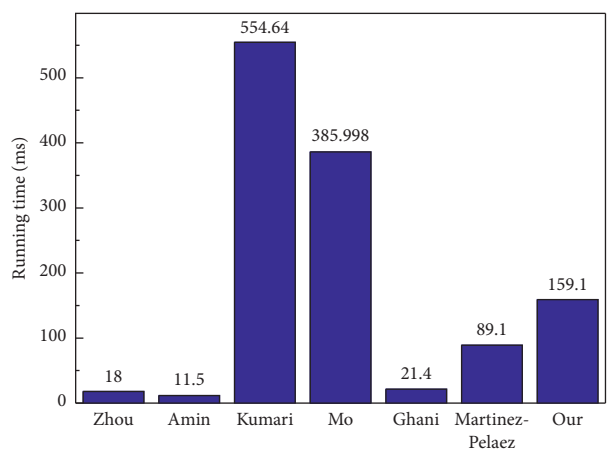


Figure 4: The computation cost of related schemes.

they just involve lightweight cryptographic operations. However, they suffer from various security vulnerabilities. In Zhou et al.'s scheme, the attacker is capable of impersonating the user and the cloud server by replaying the intercepted message. In Amin et al.'s scheme, the attacker can retrieve user's password, disclose the session key, and impersonate the user when smart card is compromised. Martinez-Pelaez et al.'s scheme and Ghani et al.'s scheme are vulnerable to diverse and serious security weaknesses. They are unable to provide the essential security protection.

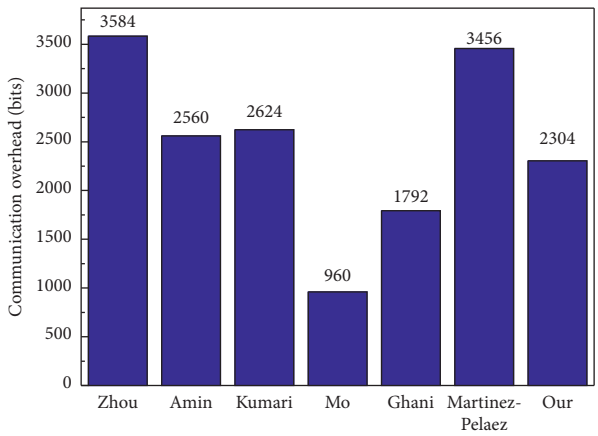


Figure 5: The communication cost of related schemes.

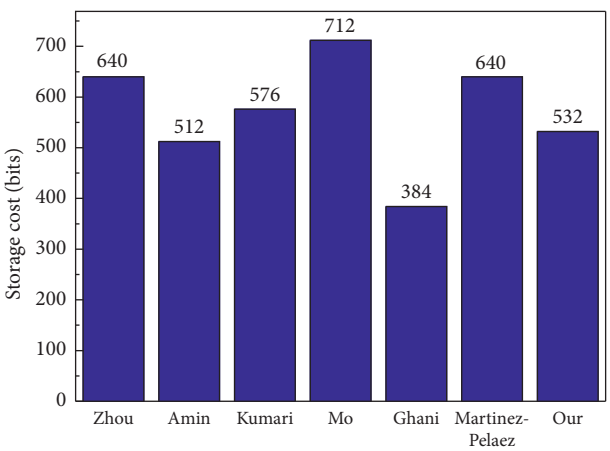


Figure 6: The smart card storage cost of related schemes.

The ECC-based schemes have low efficiency. They have better security than the hash-based schemes and the symmetric cryptosystem-based schemes, but still have security flaws. In Mo et al.'s scheme, the attacker can impersonate the user when the verifier table is leaked. Kumari et al.'s scheme achieves many security features, but it does not provide three-factor secrecy.

In terms of the security of session key, only our scheme is resistant to all kinds of session key exposure attacks, as Chebyshev chaotic-based Diffie–Hellman key exchange and the long-term secret are used to establish the session key. None of the related schemes can withstand known session-specific temporary information attack. If one communication end uses unsecure random number generator, it will lead to the disclosure of the session key. The hash-based schemes and the symmetric cryptosystem-based schemes are unable to provide forward secrecy. The ECC-based schemes provide forward secrecy, as the elliptic curve-based Diffie–Hellman key exchange is employed. Furthermore, in Amin et al.'s scheme and Martinez-Pelaez et al.'s scheme, the attacker can retrieve the session key when the smart card is compromised.

To sum up, the security of our scheme is optimal. In addition, its computation and communication overheads are obviously lower than the ECC-based schemes. Hence, our scheme is more practical.

7. Conclusion

In this paper, we pointed out that Zhou et al.'s scheme is unable to provide the essential security protection for cloud computing, as it does not consider replay attack, known session-specific temporary information attack, and forward secrecy. Furthermore, we present a novel IoT-based three-factor authentication scheme for cloud computing using chaotic maps. The use of Chebyshev chaotic maps guarantees the security of session key and simultaneously reduces the computation cost. In addition, the BAN logic analysis demonstrates that our scheme achieves mutual authentication as well as session key negotiation. The formal analysis confirms the semantic security of session key. The informal analysis proves that our scheme can withstand known attacks and achieve desired attributes such as user anonymity and resistance to all kinds of session key exposure attacks. Finally, the performance comparisons show that our scheme has significant advantage compared with the related schemes. As our scheme has high security, it is especially applicable to the security-critical cloud applications such as cloud-based healthcare systems. Afterwards, on the basis of our current work, we plan to make further study on the authentication protocol for smart healthcare systems.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This research was funded by the National Key Research and Development Program of China under Grant no. 2018YFB0803600, the National Natural Science Foundation of China under Grant no. 61831003, and the National Natural Science Foundation of China under Grant no. 61873069.

References

[1] W. Ding, X. Jing, Z. Yan, and L. T. Yang, "A survey on data fusion in Internet of Things: towards secure and privacy-preserving fusion," *Information Fusion*, vol. 51, pp. 129–144, 2019.

[2] Q. Jiang, Y. Qian, J. Ma, X. Ma, Q. Cheng, and F. Wei, "User-centric three-factor authentication protocol for cloud-assisted wearable devices," *International Journal Communication Systems*, vol. 32, no. 6, p. e3900, 2019.

[3] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, S. Kumari, and M. Jo, "Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2884–2895, 2018.

[4] J. Tang, Y. Cui, Q. Li, K. Ren, J. Liu, and R. Buyya, "Ensuring security and privacy preservation for cloud data services," *ACM Computing Surveys*, vol. 49, no. 1, pp. 1–39, 2016.

[5] W. Meng, W. H. Lee, S. R. Murali, and S. P. T. Krishnan, "Charging me and I know your secrets!: towards juice filming attacks on smartphones," in *Proceedings of the 2015 ACM Workshop on Cyber-Physical System Security*, ACM, Singapore, April 2015.

[6] P. Gope and A. K. Das, "Robust anonymous mutual authentication scheme for," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1764–1772, 2017.

[7] W. H. Yang and S. P. Shieh, "Password authentication schemes with smart cards," *Computers & Security*, vol. 18, no. 8, pp. 727–733, 1999.

[8] F. Wu, L. Xu, and X. Li, "A new chaotic map-based authentication and key agreement scheme with user anonymity for multi-server environment," in *Proceedings of the International Conference on Frontiers Computing 2017*, vol. 464, pp. 335–344, Osaka, Japan, July 2017.

[9] Q. Jiang, J. Ma, C. Yang, X. Ma, J. Shen, and S. A. Chaudhry, "Efficient end-to-end authentication protocol for wearable health monitoring systems," *Computers & Electrical Engineering*, vol. 63, pp. 182–195, 2017.

[10] A. Ostad-Sharif, H. Arshad, M. Nikooghadam, and D. Abbasinezhad-Mood, "Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme," *Future Generation Computer Systems*, vol. 100, pp. 882–892, 2019.

[11] X. Huang, X. Chen, J. Li, Y. Xiang, and L. Xu, "Further observations on smart-card-based password-authenticated key agreement in distributed systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 7, pp. 1767–1775, 2014.

[12] M. Wazid, A. K. Das, S. Kumari, X. Li, and F. Wu, "Design of an efficient and provably secure anonymity preserving three-factor user authentication and key agreement scheme for TMIS," *Security and Communication Networks*, vol. 9, no. 13, pp. 1983–2001, 2016.

[13] F. Wang, G. Xu, C. Wang, and J. Peng, "A provably secure biometrics-based authentication scheme for multiserver environment," *Security and Communication Networks*, vol. 2019, Article ID 2838615, 15 pages, 2019.

[14] V. Odelu, A. K. Das, S. Kumari, X. Huang, and M. Wazid, "Provably secure authenticated key agreement scheme for distributed mobile cloud computing services," *Future Generation Computer Systems*, vol. 68, pp. 74–88, 2017.

[15] P. Chandrakar and H. Om, "A secure and robust anonymous three-factor remote user authentication scheme for multi-server environment using ECC," *Computer Communications*, vol. 110, pp. 26–34, 2017.

[16] C. Wang, K. Ding, B. Li et al., "An enhanced user authentication protocol based on elliptic curve cryptosystem in cloud computing environment," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 3048697, 13 pages, 2018.

[17] M. R. Ogiela and L. Ogiela, "Expert knowledge-based authentication protocols for cloud computing applications," in *Proceedings of the 10th International Conference on Intelligent Networking and Collaborative Systems*, vol. 23, pp. 82–27, Oita, Japan, September 2019.

[18] J. L. Tsai and N. W. Lo, "A privacy-aware authentication scheme for distributed mobile cloud computing services," *IEEE Systems Journal*, vol. 9, no. 3, pp. 805–815, 2015.

[19] D. He, N. Kumar, M. K. Khan, L. Wang, and J. Shen, "Efficient privacy-aware authentication scheme for mobile cloud computing services," *IEEE Systems Journal*, vol. 12, no. 2, pp. 1621–1631, 2018.

[20] S. Kumari, X. Li, F. Wu, A. K. Das, K. R. Choo, and J. Shen, "Design of a provably secure biometrics-based multi-cloud-server authentication scheme," *Future Generation Computer Systems*, vol. 68, pp. 320–330, 2017.

[21] R. Amin, N. Kumar, G. P. Biswas, R. Iqbal, and V. Chang, "A lightweight authentication protocol for IoT-enabled devices in distributed cloud computing environment," *Future Generation Computer Systems*, vol. 78, pp. 1005–1019, 2018.

[22] K. Xue, P. Hong, and C. Ma, "A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture," *Journal of Computer and System Sciences*, vol. 80, no. 1, pp. 195–206, 2014.

[23] M. C. Chuang and M. C. Chen, "An anonymous multi-server authenticated key agreement scheme based on trust computing using smartcards and biometrics," *Expert Systems with Applications*, vol. 41, no. 4, pp. 1411–1418, 2014.

[24] P. Wang, B. Li, H. Shi, Y. Shen, and D. Wang, "Revisiting anonymous two-factor authentication schemes for IoT-enabled devices in cloud computing environments," *Security and Communication Networks*, vol. 2019, Article ID 2516963, 13 pages, 2019.

[25] J. Mo, Z. Hu, H. Chen, and W. Shen, "An efficient and provably secure anonymous user authentication and key agreement for mobile cloud computing," *Wireless Communications and Mobile Computing*, vol. 2019, Article ID 4520685, 12 pages, 2019.

[26] L. Zhou, X. Li, K. Yeh, C. Su, and W. Chiu, "Lightweight IoT-based authentication scheme in cloud computing circumstance," *Future Generation Computer Systems*, vol. 91, pp. 244–251, 2019.

[27] D. Wang, D. He, P. Wang, and C. Chu, "Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 4, pp. 428–442, 2015.

[28] D. Wang and P. Wang, "On the anonymity of two-factor authentication schemes for wireless sensor networks: attacks, principle and solutions," *Computer Networks*, vol. 73, pp. 41–57, 2014.

[29] S. Chatterjee, S. Roy, A. K. Das, S. Chattopadhyay, N. Kumar, and A. V. Vasilakos, "Secure biometric-based authentication scheme using Chebyshev chaotic map for multi-server environment," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 824–839, 2018.

[30] L. Zhang, "Cryptanalysis of the public key encryption based on multiple chaotic systems," *Chaos Solitons & Fractals*, vol. 37, no. 3, pp. 669–674, 2008.

[31] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[32] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Tansactions on Computer Systems*, vol. 8, no. 1, pp. 18–36, 1990.

[33] D. Wang and P. Wang, "Two birds with one stone: two-factor authentication with security beyond conventional bound," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 708–722, 2018.

[34] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf's law in passwords," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2776–2791, 2017.

[35] A. Ghani, K. Mansoor, S. Mehmood, S. A. Chaudhry, A. U. Rahman, and M. N. Saqib, "Security and key

management in IoT-based wireless sensor networks: an authentication protocol using symmetric key," *International Journal of Communication Systems*, vol. 32, no. 16, p. e4139, 2019.

[36] R. Martínez-Peláez, H. Toral-Cruz, J. Parra-Michel et al., "An enhanced lightweight IoT-based authentication scheme in cloud computing circumstances," *Sensors*, vol. 19, no. 9, p. 2098, 2019.

[37] D. Abbasinezhad-Mood and M. Nikooghadam, "Efficient anonymous password-authenticated key exchange protocol to read isolated smart meters by utilization of extended Chebyshev chaotic maps," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4815–4828, 2018.

Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 2509081, 10 pages
https://doi.org/10.1155/2020/2509081

Research Article

A Genetic Algorithm-Based Soft Decision Fusion Scheme in Cognitive IoT Networks with Malicious Users

Muhammad Sajjad Khan,[1,2] **Noor Gul**,[3] **Junsu Kim**,[1] **Ijaz Mansoor Qureshi**,[4] **and Su Min Kim**[1]

[1]*Department of Electronics Engineering, Korea Polytechnic University, Siheung, Republic of Korea*
[2]*Department of Electrical Engineering, International Islamic University Islamabad, Islamabad, Pakistan*
[3]*Department of Electronics, University of Peshawar, Peshawar, Pakistan*
[4]*Department of Electrical Engineering, Air University, Islamabad, Pakistan*

Correspondence should be addressed to Su Min Kim; suminkim@kpu.ac.kr

Received 4 November 2019; Accepted 30 December 2019; Published 31 January 2020

Guest Editor: Hasan Ali Khattak

Internet of Things (IoT) is a new challenging paradigm for connecting a variety of heterogeneous networks. Since its introduction, many researchers have been studying how to efficiently exploit and manage spectrum resource for IoT applications. An explosive increase in the number of IoT devices accelerates towards the future-connected society but yields a high system complexity. Cognitive radio (CR) technology is also a promising candidate for future wireless communications. CR via dynamic spectrum access provides opportunities to secondary users (SUs) to access licensed spectrum bands without interfering primary users by performing spectrum sensing before accessing available spectrum bands. However, multipath effects can degrade the sensing capability of an individual SU. Therefore, for more precise sensing, it is helpful to exploit multiple collaborative sensing users. The main problem in cooperative spectrum sensing is the presence of inaccurate sensing information received from the multipath-affected SUs and malicious users at a fusion center (FC). In this paper, we propose a genetic algorithm-based soft decision fusion scheme to determine the optimum weighting coefficient vector against SUs' sensing information. The weighting coefficient vector is further utilized in a soft decision rule at FC in order to make a global decision. Through extensive simulations, the effectiveness of the proposed scheme is evaluated compared with other conventional schemes.

1. Introduction

Wireless communication networks have a tremendous progress for the last 30 years to support the growth of application devices from 1G to 4G LTE-advanced wireless networks [1]. Each generation has played its role in order to enhance data rate, reliability, latency, and so on. During the past years, connecting each device with another device at anytime and anywhere is a big challenge in wireless communication networks. In a line of evolutions, 5G will provide an unexpected contribution and a big step forward toward spectrum management, public safety, energy efficiency, high data rate, low latency, and so on [2–4]. The future 5G wireless system is on the horizon, and Internet of Things (IoT) is going to take the center stage since the IoT devices are expected to form a major portion of this 5G network paradigm [5].

IoT was first mentioned by Ashton, who introduces a technological revolution to bring heterogeneous networks under a single umbrella of IoT [6], and it has drastically changed landscape of various industries [7]. IoT is a promising subject of technical, social, and economic implications; it can be presumed that IoT has a strong and meaningful impact on daily life in the near future, such as automation, improvised learning, logistic, intelligent transportation, and e-health care [8, 9]. Technically, the most focused area of paradigm is computing, communication, and connectivity. Among them, the connectivity and

spectrum management are more challenging and of great concern. As over 50 billion wireless devices will be connected by 2020, all of which will demand a lot of spectrum resources [10]; the authors in [11] argued the importance of cognitive capability, that is, without comprehensive cognitive capability, IoT is just like an awkward stegosaurus: all brawn and no brains. Today, we already have over a dozen wireless technologies in use: WiFi, Bluetooth, ZigBee, NFC, LTE, earlier 3G standards, satellite services, and so on. Due to proliferation of these wireless networks and explosive increase in the number of users, a spectrum scarcity problem is raised and becomes more serious. The static allocation and management of spectrum resources are not efficient to meet requirements of wireless devices and applications. With the static allocation, some of spectrum bands are able to be heavily overloaded, whereas another part of spectrum bands is rarely used. Federal communication commission (FCC) has been considering a more flexible and comprehensive use of the spectrum resources using cognitive radio (CR) technology by allowing secondary users (SUs) to utilize free spectrum holes, which are not used by primary users (PUs) [12]. In CR networks (CRNs), efficient spectrum sensing and reporting is mandatory to avoid interference to the legitimate PUs [13, 14].

In the CRN, a PU owns a right to access spectrum bands, and therefore, the interference level caused by SUs must be limited to a certain level. In the literature, SUs adopt different types of sensing detectors such as matched filter detector (MFD), cyclostationary detector, feature detector, and energy detectors (ED) [15, 16]. Although the MFD has a superior performance, it requires prior knowledge on the PU channel which makes it difficult to implement. On the contrary, the ED is easy to implement, thanks to its simple hardware requirements and less complexity. In distributed sensing environments, the sensing information provided by individual sensing users cannot be trusted due to wireless channel effects, such as multipath fading, shadowing, and receiver uncertainties. Hence, it is more feasible to adopt cooperative spectrum sensing (CSS) techniques to overcome these matters [17].

Cooperation among sensing users can be implemented in a centralized or distributed manner. In the distributed CSS, individual users can share the sensing information with each other without the fusion center (FC), while in the centralized CSS, the fusion center (FC) collects sensing reports from individual users in order to make an appropriate final decision [18, 19]. The combination of local sensing reports at the fusion center (FC) is categorized as soft and hard decision fusion schemes. The hard decision fusion (HDF) schemes such as logical AND, logical OR, and voting allow each user to take a local decision and send a binary decision result to the FC [20, 21]. The benefit of HDF is optimality in transmitting energy while reporting to the FC, but it is not fully capable of accurately estimating the PU's status [22]. In soft decision fusion (SDF) such as maximum gain combining (MGC), equal gain combining (EGC), and Kullback–Leibler (KL) divergence-based combining techniques, the SUs sense and forward energy statistics on the PU's channel to the FC, where the final channel estimation is carried out [23–26].

The CSS leads to a high detection probability with minimum false alarm that results in reduced error probability at the FC. Meanwhile, the CRN is highly vulnerable to security threats. The security threat is an important part, which disturbs the normal operation of the underlying network infrastructure [27, 28]. Various attacks which severely degrade the performance of the CSS have been studied in the CRN. The representative attacks are Byzantine users' attack, jamming attack, and primary user emulation attack (PUEA) [29–33]. The Byzantine users' attack is a type of spectrum sensing data falsification (SSDF) attack, where malicious users (MUs) report false information to the FC. SSDF attacks severely degrade the spectrum sensing reliability and spectrum utilization. SSDF attacks are always yes, always no, and random attacks. In [30], the authors isolated SSDF outliers by utilizing Z-test; the SSDF attack is mitigated via q-out-of-m scheme. Similarly, in [31], the authors utilized a linear-weighted combination scheme to eliminate the effect of the SSDF attack on the final sensing decision. Furthermore, an adaptive reputation evaluation mechanism is introduced to discriminate malicious users from legitimate users. The traditional jamming attack targets to inject malicious signals into an operating frequency band so that the desired signals are interfered from them [32]. The PUEA prevents access to licensed user's spectrum by masquerading as a PU so that legitimate PUs cannot successfully access their own spectrum [33].

Some heuristic approaches in CSS can lead to an optimal global decision. Among them, a genetic algorithm (GA), which is a class of computational algorithm motivated by evolution, is a good candidate to find the optimal solution by adopting biologically inspired approaches to given problems [34, 35]. In [36], the authors highlighted and discussed GA techniques which can be applied to various applications and issues for wireless networks. In [35, 37], the authors focused on optimization of detection and false alarm probabilities of a particular SU using the GA in a centralized CRN.

In this paper, we evaluate the performance of CSS in the presence of MUs in CRNs. We consider several different operating criteria of MUs: always yes (AY), always no (AN), always opposite (AO), and random opposite (RO). Cooperative users are assumed to be located at different geographical locations and experience independent Rayleigh fading. Therefore, it is almost impossible to treat all the sensing information. In this paper, we exploit a GA approach to determine the optimal weighting coefficient vector. Once the optimal weighting coefficient vector is found by the proposed GA-based SDF scheme, the weighting vector is further utilized in SDF at the FC to make a final global decision. To this end, we employ an energy detector for each sensing user, where the observed energy is compared with an adaptive threshold determined by the proposed GA-based SDF scheme. Through extensive simulations, it is shown that the proposed GA-based SDF scheme achieves better detection and error performance than conventional count (voting)-HDF, MGC-SDF, and KL-SDF schemes.

The rest of the paper is organized as follows. In Section 2, the system model considered in this paper is presented. In Section 3, a GA-based SDF scheme is proposed and discussed in detail. In Section 4, the proposed scheme is evaluated through extensive simulations, compared with conventional schemes. Finally, conclusive remarks are drawn in Section 5.

2. System Model

We consider a cooperative spectrum sensing scenario that consists of a PU, normal SUs, malicious SUs (MUs), and FC as shown in Figure 1. All SUs perform spectrum sensing to determine presence or absence of the PU in the network.

At the beginning, each SU performs own local sensing. The local sensing can be represented as a binary hypothesis testing for presence or absence of the PU in the network and is measured as

$$\left\{\begin{array}{c} H_0\colon X_i[n] = W_i[n] \\ H_1\colon X_i[n] = g_i S[n] + W_i[n] \end{array}\right\}, \quad \begin{array}{l} i \in 1, 2, \ldots, M, \\ n \in 1, 2, \ldots, K, \end{array} \tag{1}$$

where H_0 denotes the hypothesis when no PU is active and H_1 denotes the hypothesis when a PU is active on the channel. $X_i[n]$ is the received signal at the ith user in the nth time slot. The total number of samples for sensing is $K = 2BT_s$, where B is the used bandwidth and T_s is the sensing time period. We assume that K is a sufficiently large value so that sensing energy of the signal follows a Gaussian distribution. In (1), g_i denotes the channel gain between the ith user and the PU. Similarly, $S[n]$ is the nth sample of the PU signal that is regarded as an independent and identically distributed (i.i.d.) Gaussian random variable with zero mean and variance σ_S^2, i.e., $S[n] \sim N(0, \sigma_S^2)$. $W_i[n]$ denotes the additive white Gaussian noise (AWGN) at the ith user, which follows a Gaussian distribution with zero mean and variance $\sigma_{W_i}^2$, i.e., $W_i[n] \sim N(0, \sigma_{W_i}^2)$.

The total sensing energy reported by the ith user to the FC is expressed as

$$Z_i = \sum_{n=1}^{K} \left|U_i[n]\right|^2, \tag{2}$$

where $U_i[n] = \sqrt{P_{R,i}} h_i X_i[n] + N_i[n]$ is the signal received at the FC reported from the ith user in the nth time slot. Here, $P_{R,i}$ is the transmit power of the ith user, h_i is the channel gain between the ith user and the FC, and $N_i[n]$ is an AWGN with zero mean and variance δ_i^2, i.e., $N_i[n] \sim N(0, \delta_i^2)$.

3. Proposed Cooperative Spectrum Sensing and Soft Decision Fusion Schemes

In this section, we provide detailed descriptions of the proposed cooperative spectrum sensing (CSS) scheme in the presence of MUs and the proposed GA-based SDF scheme that determines the optimal weighting coefficient vector.

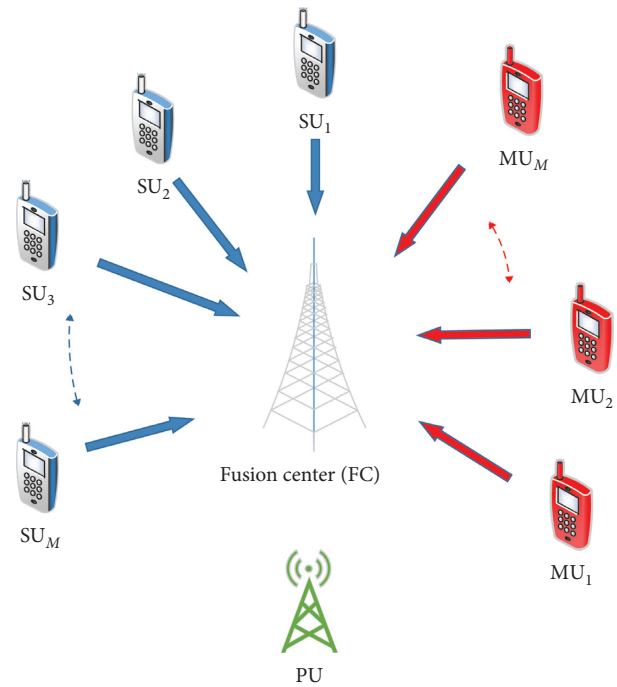


Figure 1: System model.

3.1. Proposed Cooperative Spectrum Sensing Scheme. The proposed CSS scheme using weighted SDF is shown in Figure 2. In the figure, an FC receives sensing statistics of the PU channel from M users including both normal SUs and MUs. According to the operating criteria of MUs, an AY MU reports higher energy statistics to the FC irrespective of the actual status of the PU channel as if the PU channel is always busy [29]. Thus, if there exist AY MUs in CSS, the data rate of the secondary system can be severely reduced. In contrast, AN MU reports lower energy statistic to the FC than the actual PU channel condition, and thus, interference to the legitimate PU occurs. Similarly, since an AO MU always feedbacks opposite energy statistics to the FC, the data rate of the secondary system is reduced, and interference to the legitimate PU occurs. Finally, an RO MU probabilistically operates as an AO MU with probability p and as a normal SU with probability $(1-p)$. The role of cooperative SUs in Figure 2 is similar to cooperative relays that receive and forward the statistics of the PU channel to the FC. Consequently, the FC makes the global decision on the PU channel status based on a linearly weighted SDF approach using channel sensing statistics collected from multiple SUs.

For M cooperative SUs, the final test statistic observed at the FC is expressed as

$$Z = \sum_{i=1}^{M} (w_i Z_i), \tag{3}$$

where w_i is the weighting factor assigned to the sensing energy of the ith user. Since the sensing reports Z_i for the ith user are Gaussian-distributed, the final test statistic Z is also Gaussian-distributed [37].

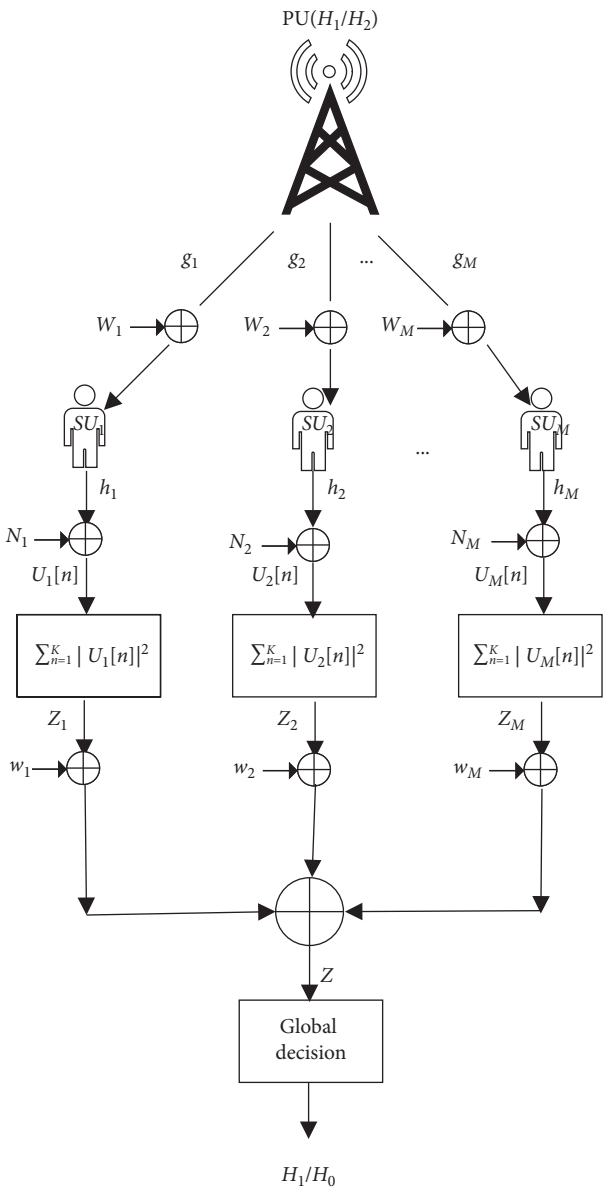


Figure 2: Proposed CSS scheme.

$$E\left(Z|H_0|\right) = \sum_{i=1}^{M} w_i K \sigma_{0,i}^2, \tag{4}$$

$$E\left(Z|H_1|\right) = \sum_{i=1}^{M} w_i K \sigma_{1,i}^2, \tag{5}$$

$$\mathrm{var}\left(Z|H_0|\right) = \sum_{i=1}^{M} 2w_i^2 K\left(\sigma_{0,i}^2 + \delta_i^2\right)^2 = \vec{w}^T \Phi_{H_0} \vec{w}, \tag{6}$$

$$\mathrm{var}\left(Z|H_1|\right) = \sum_{i=1}^{M} 2w_i^2 K\left(\sigma_{1,i}^2 + \sigma_{0,i}^2\right)^2 = \vec{w}^T \Phi_{H_1} \vec{w}, \tag{7}$$

where $\sigma_{0,i}^2$ and $\sigma_{1,i}^2$ are the variances of $U_i[n]$ under the H_0 and H_1 hypotheses for the ith user that are equivalent to $\sigma_{0,i}^2 = P_{R,i}|h_i|^2\sigma_{W_i}^2 + \delta_i^2$ and $\sigma_{1,i}^2 = P_{R,i}|g_i|^2|h_i|^2\sigma_s^2 + \sigma_{0,i}^2$, respectively.

In (4)–(7), $\vec{\mathbf{w}} = [\, w_1 \;\; w_2 \;\; \ldots \;\; w_M \,]^T$ is the weighting coefficient vector to be optimized in order to determine an appropriate threshold value β for minimizing sensing error probability.

The covariance matrices for H_0 and H_1 hypotheses are given by

$$\begin{aligned} \Phi_{H_0} &= \mathrm{diag}\left(2K\sigma_{0,i}^4\right), \\ \Phi_{H_1} &= \mathrm{diag}\left(2K\left(P_{R,i}|g_i|^2|h_i|^2\sigma_S^2 + \sigma_{0,i}^2\right)^2\right), \end{aligned} \tag{8}$$

where diag(.) is a diagonalization operation of a matrix. Finally, the detection and false alarm probabilities at the FC are expressed as

$$\begin{aligned} P_f &= P\left(Z > \beta \mid H_0\right) = Q\left(\frac{\beta - E\left(Z|H_0|\right)}{\sqrt{\mathrm{var}\left(Z|H_0|\right)}}\right) = Q\left(\frac{\beta - \vec{w}^T\vec{\mu}_0}{\sqrt{\vec{w}^T\Phi_{H_0}\vec{w}}}\right), \\ P_d &= P\left(Z > \beta \mid H_1\right) = Q\left(\frac{\beta - E\left(Z|H_1|\right)}{\sqrt{\mathrm{var}\left(Z|H_1|\right)}}\right) = Q\left(\frac{\beta - \vec{w}^T\vec{\mu}_1}{\sqrt{\vec{w}^T\Phi_{H_1}\vec{w}}}\right), \\ \beta &= \left(\frac{\sqrt{w^T\Phi_{H_1}w}\,\mu_0^T\vec{w} + \sqrt{\vec{w}\Phi_{H_1}w}\,\mu_1^T w}{\sqrt{w^T\Phi_{H_0}w} + \sqrt{w^T\Phi_{H_1}w}}\right). \end{aligned} \tag{9}$$

Let us assume that $P_f = P_m$, where P_m is the miss detection probability and $P_f = 1 - P_d$, and therefore, the total error probability P_e is determined as

$$P_e = P_f + P_m = Q\left(\frac{\beta - \vec{w}^T\vec{\mu}_0}{\sqrt{\vec{w}^T\Phi_{H_0}\vec{w}}}\right) + Q\left(\frac{\vec{w}^T\vec{\mu}_1 - \beta}{\sqrt{\vec{w}^T\Phi_{H_1}\vec{w}}}\right). \tag{10}$$

In (10), it is noticeable that the error probability is highly dependent on the weighting coefficient vector $\vec{w}$. Therefore, the optimal threshold β needs to be determined for satisfying high detection, minimum false alarm, and low error probabilities, and then it is substituted into (10). In the proposed CSS scheme, the choice of $\vec{w}$ is performed such that $0 < w_i < 1$ and $\sqrt{\sum_{i=1}^{M} w_i^2} = 1$ in order to reduce the search space and computational complexity.

3.2. Proposed GA-Based SDF Scheme. The GA is a biological inspired method which is widely used for searching optimized solutions in various science and engineering problems. It is referred to the chromosomes as the strings of binary symbols encoding a candidate solution to the given problem [34, 38].

In our proposed GA-based SDF scheme, the GA tries to find an optimal set of weighted coefficient vectors for combining the sensing reports received from all cooperative

```
For n = 1 to Sensing Interval
    For i = 1 to M
        Energy reported by the i^th SU as Z_i
    End
  // Determine optimal threshold and weighting coefficient values
    Initialize randomly weights w as an N × M
    Normalize weights w.
    Calculate (Φ_{H_1}, Φ_{H_0}) based on Z_i.
    For k = 1 to N
        Investigate threshold against the k^th vector as β(k).
        Determine P_f(k) based on β(k) and w(k).
        Find P_d(k) based on β(k) and w(k).
        Estimate P_e(k).
    End
    Sort w in ascending order probabilities.
    The chromosomes at the top are selected as parents.
    Crossover (w)
    Mutate (w)
    // End i^th sensing
    Select the optimal β and w with minimum P_e
    For i = 1 to M
        Z'_i = w_i × Z_i // new energies against users
    End
    If Σ_{i=1}^{M} (Z'_i) > β
        G_B(i) = H_1
    Else
        G_B(i) = H_0
    End
End
```

Algorithm 1: Proposed GA-based SDF scheme.

users. In a random normalized set of coefficient vectors, a vector resulting in low error probability can be chosen as an optimal set of the vectors, and then, it is further utilized to make a global decision for SDF.

The proposed GA-based SDF scheme consists of the following five steps:

Step 1: initial population

N total number of chromosomes is considered at initial. The algorithm is initialized with an initial population of randomly generated N chromosomes that consist of M genes, i.e., $\vec{\mathbf{w}}_S = [\, w_1 \;\; w_2 \;\; \ldots \;\; w_M \,]^T, s \in 1, \ldots, N$, normalized in the range of 0 to 1.

Step 2: fitness of the particles

The suitability of each coefficient vector is determined by measuring their fitness scores: $P_e(\vec{w}_1)$, $P_e(\vec{w}_2), \ldots, P_e(\vec{w}_N)$. The population is sorted in the ascending order of their fitness measurements.

Step 3: crossover and mutation

The chromosomes with minimum error probability results from the top are selected as parent chromosomes. A crossover point is randomly selected in this work that changes the subsequences before and after the locus in the parents to form kid's reproduction. After then, a random mutation operation is performed for the selected weighting coefficient vector.

Step 4: new population

The fitness of the kid's population is determined as in step 2, and the results are sorted in the ascending order of their fitness. The crossover and mutation operations are performed for the newly established population.

Step 5: stopping criteria

The GA starts to repeat step 2 if the fitness functions (i.e., minimum P_e) are not achieved or if the number of iterations is not completed.

The implementable algorithm of the proposed GA-based SDF scheme is explained in detail in Algorithm 1, and the overall flowchart of the proposed scheme is shown in Figure 3.

4. Numerical Results and Analysis

In this section, we provide numerical results of the proposed GA-based SDF scheme in comparison with other conventional schemes. In our simulation environments, the number of SUs in the CRN is adjusted to 10 and 14 users. Among whole SUs, four users are selected as AY, AN, AO, and RO MUs, respectively. In the results, SNR values are varying from 30 dB to 0 dB. The sensing interval is set to 1 ms with 270 to 335 samples. The SUs are placed at different locations with varying SNRs and each of which senses the PU channel independently. A crossover point is randomly chosen in the

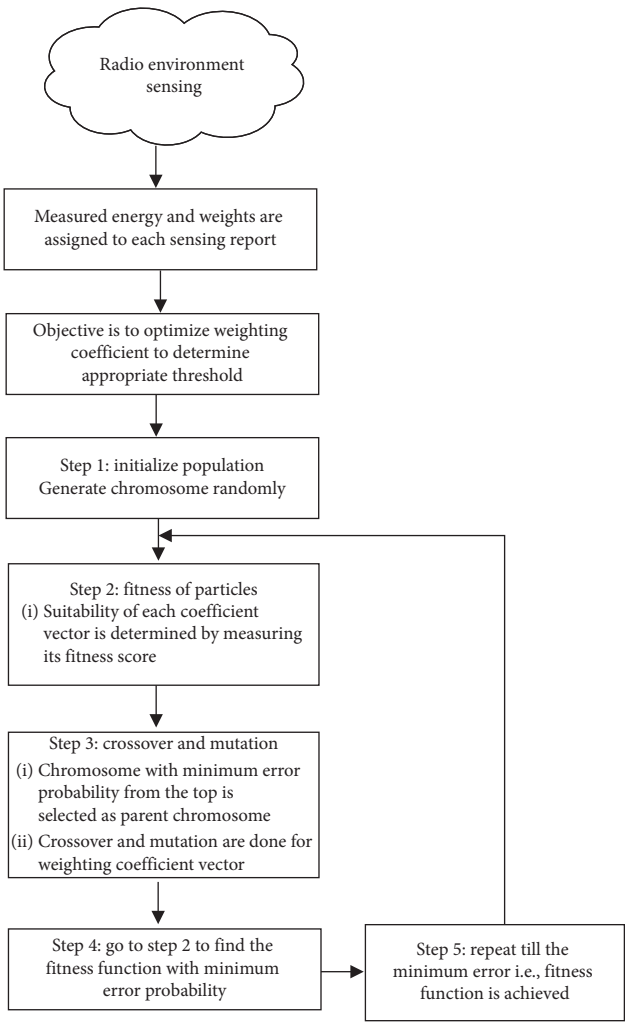


Figure 3: Flowchart of the proposed GA-based SDF scheme.

range of 1 to M. The proposed GA-based SDF scheme finds the optimum coefficient vector, which is further used to make a global decision for SDF at the FC.

The performance of the proposed GA-based SDF scheme is evaluated through simulations, and the results are compared with the conventional count-HDF, MGC-SDF, and KL-SDF schemes. We consider three different scenarios. In Scenario 1, we show the error probabilities for varying SNRs with fixed number of SUs. In Scenario 2, we discuss the error probabilities for varying number of SUs. Finally, in Scenario 3, we show the error probabilities for varying number of SUs with two fixed SNRs at −21.5 dB and −13.5 dB. The parameters for numerical results and analysis are summarized in Table 1.

4.1. Scenario 1. In the first scenario, we fix the number of SUs and sensing time, while SNR values are varying from −30 dB to 0 dB. The performance of the proposed GA-based SDF scheme is evaluated in terms of error probability. In Figure 4, we compare the proposed GA-based SDF scheme with count-HDF, MGC-SDF, and KL-SDF schemes when no MU exists in the network. It is obviously shown from

Table 1: Parameters for numerical results.

Parameter	Value
Total number of users	M
Malicious users	4
Number of genes in GA	M
Total number of GA chromosomes	$N = 30$
Random crossover	1 to M
GA iteration size	50
Count decision	$M/2$

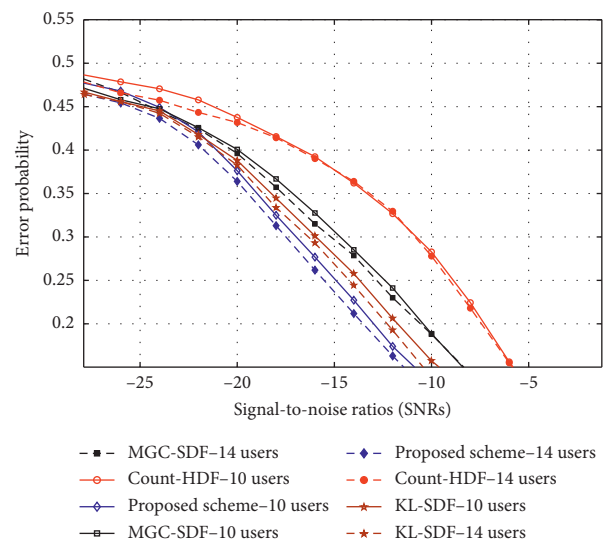


Figure 4: Error probability vs. SNR without MUs.

Figure 4 that the proposed GA-based SDF scheme outperforms the other schemes in terms of error probability. In Figure 5, the same parameters are considered to evaluate the proposed GA-based SDF scheme except that MUs at low SNR exist in the network. It can be observed that, with the existence of MUs in the network, the error probability of the proposed scheme is smaller to that of the other schemes. The other schemes are badly affected when there exist MUs in the network. Similarly, when there exist MUs at high SNR as in Figure 6, the performance of the other conventional schemes is highly affected, while the proposed GA-based SDF scheme is capable to mitigate the effect of MUs at the FC.

4.2. Scenario 2. In the second scenario, we consider fixed sensing time duration and SNR values (e.g., −21.5 dB and −13.5 dB) and varying number of SUs from 10 to 22. We evaluate the performance of the proposed GA-based SDF scheme, compared with other schemes, according to MU existence in the network: (i) no MU, (ii) MUs at low SNR, and (iii) MUs at high SNR. Figure 7 shows the error probability for varying number of SUs when no MU exists in the network. It is shown that the error probability decreases as the number of SUs increases. The reason is obvious that, with CSS, the detection probability increases, while the false alarm probability decreases, and thus, the error probability

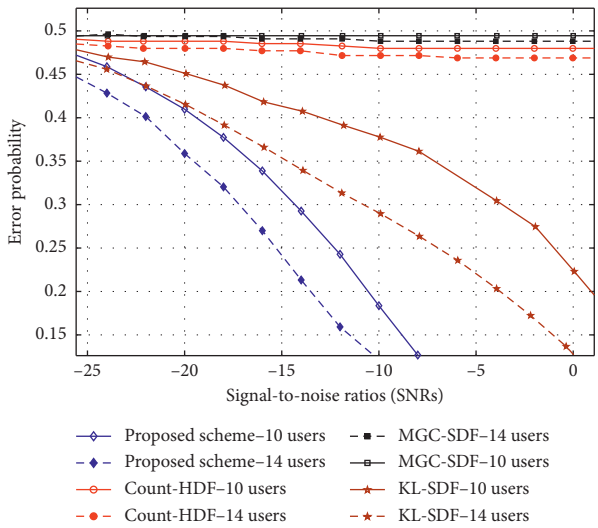


Figure 5: Error probability vs. SNR when MUs exist at low SNR.

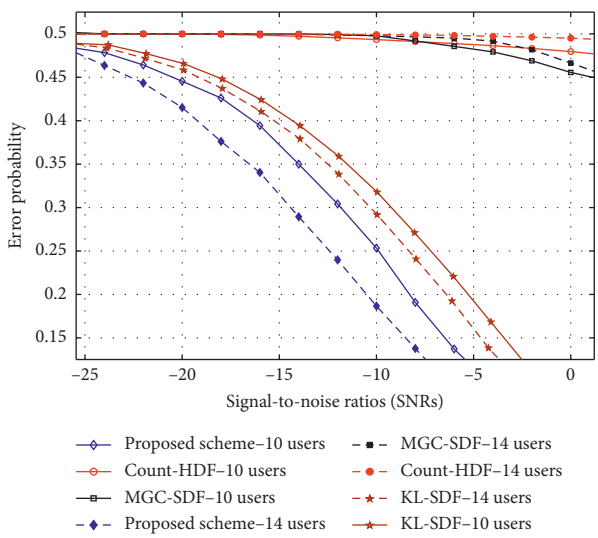


Figure 6: Error probability vs. SNR when MUs exist at high SNR.

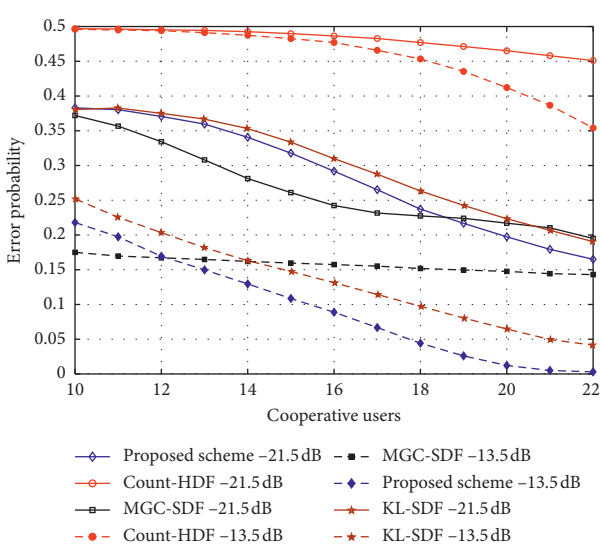


Figure 7: Error probability vs. number of SUs without MUs.

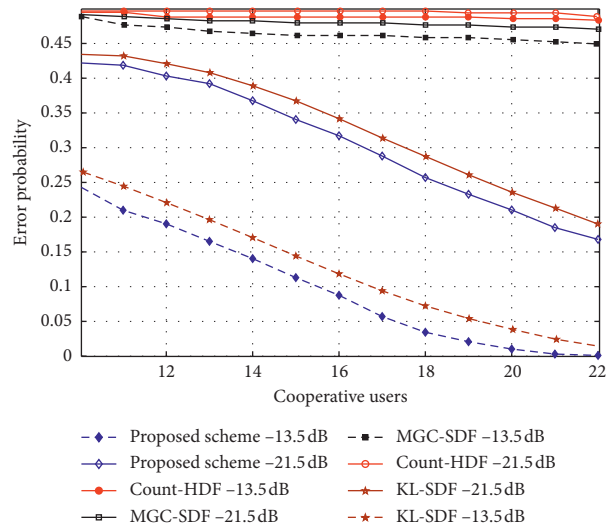


Figure 8: Error probability vs. number of SUs when MUs exist at low SNR.

can be consequently reduced. The error probability of the proposed GA-based SDF scheme is significantly reduced as the average SNR value varies from −21.5 dB to −13.5 dB. It always outperforms the conventional schemes in the whole SNR regions, while the conventional count-HDF and MGC-SDF schemes show very high error probabilities regardless of the SNR region.

Figure 8 shows the error probability for varying number of SUs when there exist MUs at lower SNR than normal SUs. In the figure, the error probabilities of the conventional count-HDF and MGC-SDF schemes do not quickly descend, different from the proposed GA-based SDF scheme. Similarly, Figure 9 shows the error probability when there exist MUs at higher SNR than normal SUs. We also consider two average SNR values of −21.5 dB and −13.5 dB. For the proposed GA-based SDF scheme, the error probability decreases more quickly compared with the conventional count-HDF, MGC-SDF, and KL-SDF schemes with increasing number of SUs.

4.3. Scenario 3. In the last scenario, the sensing time duration is varying from 270 to 335 when the number of SUs and SNR values are fixed. Figures 10–12 show the error probabilities of the proposed GA-based SDF scheme compared with the conventional schemes, when no MU exists, MUs exist at low SNR, and MUs exist at high SNR, respectively.

In Figure 10, it is shown that the proposed GA-based SDF scheme achieves the lowest error probability. The error probability is reduced further as average SNR increases from −21.5 dB to −13.5 dB. Basically, the error probabilities for all schemes are slightly reduced as the number of sensing samples increases. As shown in Figure 11, when MUs exist at low SNR, the conventional count-HDF and MGC-SDF schemes do not steeply reduce the error probability, while the proposed GA-based SDF and KL-SDF schemes still do it. A significant reduction in the error probability is presented when the average SNR is increased

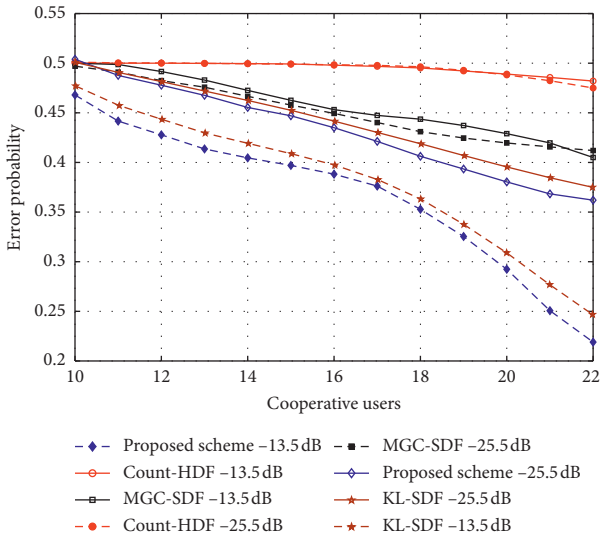


Figure 9: Error probability vs. number of SUs when MUs exist at high SNR.

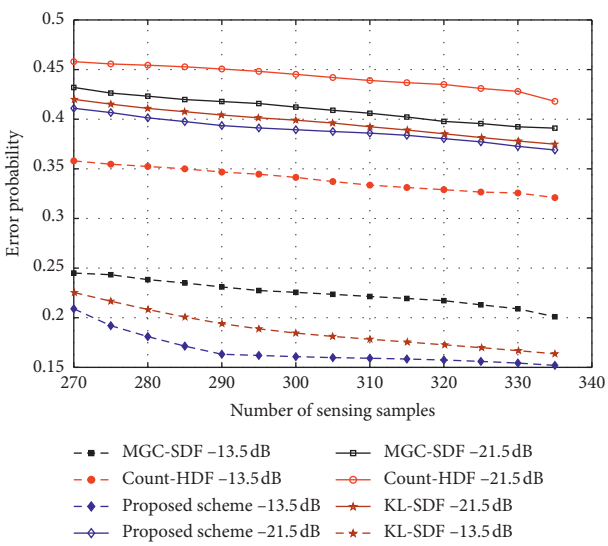


Figure 10: Error probability vs. number of sensing samples without MUs.

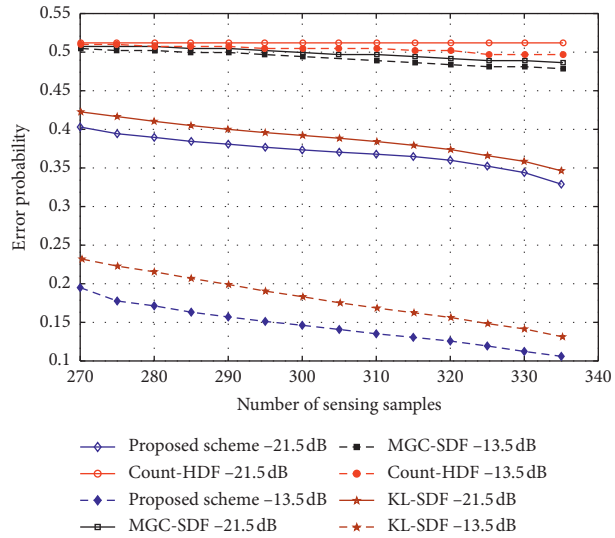


Figure 11: Error probability vs. number of sensing samples when MUs exist at low SNR.

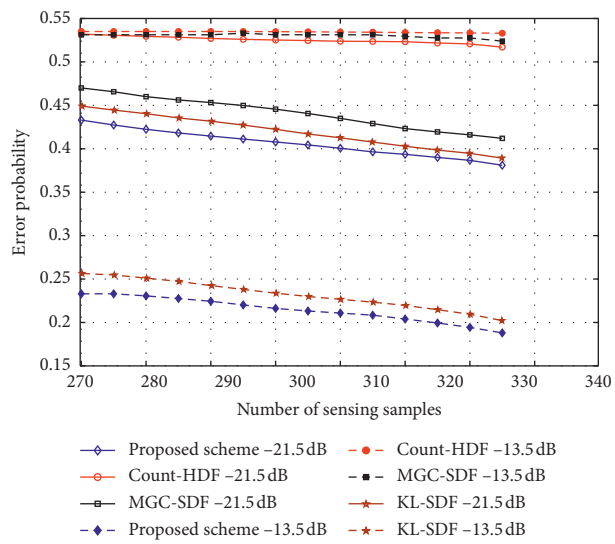


Figure 12: Error probability vs. number of sensing samples when MUs exist at high SNR.

from −21.5 dB to −13.5 dB. In this figure, it is shown that the count-HDF scheme achieves the worst error performance in the presence of MUs. In Figure 12, the sensing reports transmitted from MUs with high SNRs are collected. In the figure, as the average SNR is increased from −21.5 dB to −13.5 dB, the error probability of the conventional MGC-SDF scheme significantly degrades. However, since the proposed GA-based SDF scheme can mitigate the effect of MUs even at high SNR, it provides the best error performance and still has some performance gap with the conventional KL-SDF scheme, which achieves the best performance among the conventional schemes.

5. Conclusion

The integration of cognitive radio (CR) and Internet of Things (IoT) technologies seems to shift the future 5G and beyond wireless networks. The CR technology has the potential to efficiently utilize the spectrum via cooperative sensing. However, inaccurate sensing information caused by wireless fading effects and existence of malicious users (MUs) in the network can significantly affect the sensing performance. In this paper, we proposed a genetic algorithm (GA)-based soft decision fusion (SDF) scheme to determine the optimum coefficient vector for combining sensing reports collected from multiple secondary users (SUs). The weighting coefficient vector found by the proposed GA-based SDF scheme provides high detection, low false alarm, and low error probabilities. Through extensive simulations, the effectiveness of the proposed scheme was evaluated by considering number of SUs, average SNR, and sensing time duration. The results showed that the proposed GA-based SDF scheme significantly outperforms the conventional

count-HDF, MGC-SDF, KL-SDF schemes, even in the presence of MU in CR networks.

Data Availability

The data used to support the findings of this study are included within the article.

Disclosure

The work reported in this paper was conducted during the sabbatical year in Korea Polytechnic University in 2019.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This work was supported in part by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) Support Program (IITP-2019-2018-0-01426) supervised by the IITP (Institute for Information and Communication Technology Planning & Evaluation) and in part by the National Research Foundation (NRF) funded by the Korea government (MSIT) (no. 2019R1F1A1059125). Prof. J. Kim's work was conducted during the sabbatical year in Korea Polytechnic University in 2019.

References

[1] A. Agarwal, G. Misra, and K. Agarwal, "The 5th generation mobile networks-key concepts, network architecture and challenges," *American Journal of Electrical & Electronic Engineering*, vol. 3, no. 2, pp. 22–28, 2015.

[2] T. Q. Duong and N.-S. Vo, "Wireless communication and network for 5G and beyond," *Mobile Networks and Applications*, vol. 24, no. 2, pp. 443–446, 2019.

[3] B.-S. P. Lin, F. J. Lin, and L.-P. Tung, "The role of 5G mobile broadband in the development of IoT, big data, cloud and SDN," *Communications and Network*, vol. 8, no. 1, pp. 9–21, 2016.

[4] R. Chávez-Santiago, M. Szydełko, A. Kliks et al., "5G: the convergence of wireless communications," *Wireless Personal Communications*, vol. 83, no. 3, pp. 1617–1642, 2015.

[5] W. Ejaz, A. Anpalagan, M. A. Imran et al., "Internet of things (IoT) in 5G wireless communication," *IEEE Access*, vol. 4, pp. 10310–10314, 2016.

[6] K. Ashton, *That "Internet of Things": In the Real World, Things Matter More than Ideas*, Springer, Berlin, Germany, 2009.

[7] F. A. Awin, Y. M. Alginahi, E. A. Raheem, and K. Tepe, "Technical issues on cognitive radio based internet of things: a survey," *IEEE Access*, vol. 7, pp. 97887–97908, 2019.

[8] S. Chatterjee, R. Mukherjee, S. Ghosh, D. Gosh, S. Gosh, and A. Mukherjee, "Internet of things and cognitive radio- issues and challenges," in *Proceedings of the IEEE International Conference on Opto-Electronics and Applied Optics (Optronix)*, Kolkata, India, November 2017.

[9] A. A. Khan, M. H. Rehmani, and A. Rachedi, "When cognitive radio meets the Internet of things?" in *Proceedings of the IEEE International Wireless Communications & Computing Conference (IWCMC)*, Paphos, Cyprus, September 2016.

[10] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: a survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[11] Q. Wu, G. Ding, Y. Xu et al., "Cognitive Internet of things: a new paradigm beyond connection," *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 129–143, 2014.

[12] FCC, "Notice of proposed rule-making and order," Report No. 03-222, FCC, Washington, DC, USA, 2003.

[13] Y. Arjoune and N. Kaabouch, "A comprehensive survey on spectrum sensing in cognitive radio networks: recent advances, new challenges, and future research direction," *Sensors*, vol. 19, no. 1, p. 126, 2019.

[14] M. S. Khan, J. Kim, E. H. Lee, and S. M. Kim, "An efficient contention-window based reporting for internet of things features in cognitive radio networks," *Wireless Communications and Mobile Computing*, vol. 2019, Article ID 8475020, 9 pages, 2019.

[15] A. Ranjan, Anurag, and B. Singh, "Design and analysis of spectrum sensing in cognitive radio based on energy detection," in *Proceedings of the IEEE International Conference on Signal and Information Processing (IConSIP)*, Nanded, India, October 2016.

[16] I. Ilyas, S. Paul, A. Rahman, and R. K. Kundu, "Comparative evaluation of cyclo-stationary detection based cognitive spectrum sensing," in *Proceedings of the IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, New York, NY, USA, October 2016.

[17] I. F. Akilidz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: a survey," *Physical Communication*, vol. 4, no. 1, pp. 40–62, 2011.

[18] D. Cabric, S. M. Mishra, and R. W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in *Proceedings of the Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, USA, November 2004.

[19] R. Tandra and A. Sahai, "Fundamental limits on detection in low SNR under noise uncertainty," in *Proceedings of the International Conference on Wireless Networks, Communications and Mobile Computing*, Maui, HI, USA, June 2005.

[20] D.-J. Lee, "Adaptive random access for cooperative spectrum sensing in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 2, pp. 831–840, 2015.

[21] Y. He, S. Member, J. Xue, T. Ratnarajah, and S. Member, "On the performance of cooperative spectrum sensing in random cognitive radio networks," *IEEE Systems Journal*, vol. 99, pp. 1–12, 2016.

[22] D. B. Teguig, B. Scheers, and V. Le Nir, "Data fusion schemes for cooperative spectrum sensing in cognitive radio networks," in *Proceedings of the Military Communications and Information Systems Conference*, Canberra, Australia, October 2012.

[23] D. Hamza, S. Aissa, G. Aniba, S. Member, and G. Aniba, "Equal gain combining for cooperative spectrum sensing in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 13, no. 8, pp. 4334–4345, 2014.

[24] R. Biswas, J. Wu, and X. Du, "Mitigation of the spectrum sensing data falsifying attack in cognitive radio networks," in *Proceedings of the IEEE International Conference on Communication (ICC)*, Qingdao, China, May 2019.

[25] M. S. Khan and I. Koo, "Mitigation of adverse effect of malicious users by hausdorff distance in cognitive radio networks," *Journal of Information and Communication Convergence Engineering*, vol. 13, no. 2, pp. 74–80, 2015.

[26] V. V. Hiep and I. Koo, "A robust cooperative spectrum sensing based on kullback-leibler divergence," *IEICE Transaction on Communications*, vol. E95-B, no. 4, pp. 1286–1290, 2012.

[27] M. Jenani, "Network Security a challenge," *International Journal of Advanced Networking and Applications*, vol. 8, no. 5, pp. 120–123, 2017.

[28] I. S. Turbin, "Security threats in mobile cognitive radio networks," in *Proceedings of the IEEE East-West Design & Test Symposium (EWDTS)*, Kazan, Russia, September 2018.

[29] M. S. Khan, M. Jibran, I. Koo, S. M. Kim, and J. Kim, "A double adaptive approach to tackle malicious users in cognitive radio networks," *Wireless Communications and Mobile Computing*, vol. 2019, Article ID 2350964, 9 pages, 2019.

[30] I. Ngomane, M. Velempini, and S. V. Dlamini, "The detection of the spectrum sensing data falsification attack in cognitive radio ad hoc networks," in *Proceedings of the IEEE Information Communication Technology & Society (ICTAS)*, Durban, South Africa, May 2018.

[31] R. Wan, L. Ding, N. Xiong, and X. Zhou, "Mitigation strategy against spectrum sensing data falsification attack in cognitive radio sensor networks," *International Journal of Distributed Sensor Networks*, vol. 15, no. 9, 2019.

[32] H. A. B. Salmeh, S. Almajali, M. Ayyash, and H. Elgala, "Spectrum assignment in cognitive radio networks for Internet of things delay sensitive applications under jamming attack," *IEEE Internet of Things*, vol. 5, no. 3, pp. 1904–1913, 2018.

[33] S.-C. Lin, C.-Y. Wen, and W. A. Sethares, "Two-tier device based authentication protocol against PUEA attacks for IoT applications," *IEEE Transaction on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 33–47, 2018.

[34] U. Mehboob, J. Qadir, S. Ali, and A. Vasilakos, *Genetic Algorithms in Wireless Networking: Techniques, Applications, and Issues*, Springer, vol. 20, no. 6, Berlin, Germany, 2016.

[35] S. Bhattacharjee, P. Das, S. Mandal, and B. Sardar, "Optimization of probability of false alarm and probability of detection in cognitive radio networks using GA," in *Proceedings of the 2015 IEEE 2nd International Conference on Recent Trends in Information Systems (ReTIS)*, Kolkata, India, July 2015.

[36] M. Akbari and M. Ghanbarisabagh, "A novel evolutionary-based cooperative spectrum sensing mechanism for cognitive radio networks," *Wireless Personal Communications*, vol. 79, no. 2, pp. 1017–1030, 2014.

[37] M. Akbari, M. R. Manesh, A. A. El-Saleh, and M. Ismail, "Improved soft fusion-based cooperative spectrum sensing using particle swarm optimization," *IEICE Electronics Express*, vol. 9, no. 6, pp. 436–442, 2012.

[38] Z. Quan, S. Cui, and A. H. Sayed, "Optimal linear cooperation for spectrum sensing in cognitive radio network," *IEEE Journal of Selected Topics in Signal Processing*, vol. 2, no. 1, pp. 28–40, 2008.

Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 8416823, 18 pages
https://doi.org/10.1155/2020/8416823

Research Article

Privacy Preserving for Multiple Sensitive Attributes against Fingerprint Correlation Attack Satisfying *c*-Diversity

Razaullah Khan,[1] Xiaofeng Tao,[1] Adeel Anjum,[2] Haider Sajjad,[2] Saif ur Rehman Malik,[3] Abid Khan,[2] and Fatemeh Amiri[4]

[1]*National Engineering Laboratory for Mobile Network Technologies, Beijing University of Posts and Telecommunications, Beijing, China*
[2]*Department of Computer Science, COMSATS University Islamabad, 45550 Islamabad, Pakistan*
[3]*Cybernetica AS Estonia, Tallinn, Estonia*
[4]*Department of Computer Engineering, Hamedan University of Technology, Hamedan, Iran*

Correspondence should be addressed to Xiaofeng Tao; taoxf@bupt.edu.cn

Received 6 November 2019; Accepted 19 December 2019; Published 28 January 2020

Academic Editor: Ghufran Ahmed

Privacy preserving data publishing (PPDP) refers to the releasing of anonymized data for the purpose of research and analysis. A considerable amount of research work exists for the publication of data, having a single sensitive attribute. The practical scenarios in PPDP with multiple sensitive attributes (MSAs) have not yet attracted much attention of researchers. Although a recently proposed technique (p, k)-Angelization provided a novel solution, in this regard, where one-to-one correspondence between the buckets in the generalized table (GT) and the sensitive table (ST) has been used. However, we have investigated a possibility of privacy leakage through MSA correlation among linkable sensitive buckets and named it as "fingerprint correlation (fcorr) attack." Mitigating that in this paper, we propose an improved solution "(c, k)-anonymization" algorithm. The proposed solution thwarts the fcorr attack using some privacy measures and improves the one-to-one correspondence to one-to-many correspondence between the buckets in GT and ST which further reduces the privacy risk with increased utility in GT. We have formally modelled and analysed the attack and the proposed solution. Experiments on the real-world datasets prove the outperformance of the proposed solution as compared to its counterpart.

1. Introduction

Data generation and sharing have shown a drastic increase in the ongoing decade. The reason behind is obviously the growing sources of data due to huge research and smart revolution (smart grids, cities, devices, etc.). The utility of the shared/published data is utilized in research and analysis by the data researchers. The research and analysis may involve data mining, statistical data analysis, and other policy makings. In the context of health records, the data owners are the individuals to whom the data belong. The hospital that collects, manipulates, and shares that data is known as the data publisher. The data researchers may be a wide range of stakeholders (e.g., pharmaceuticals, government agencies, and survey organizations). The collected data contain private information (e.g., name, contact number, and social security number), partial identifiers (e.g., age, gender, zipcode, and country), and confidential or sensitive information (e.g., disease) about the data owners. Sharing such sensitive information is a privacy breach and legislatively wrong, if disclosed to unauthorized parties.

To ensure privacy of such information, most of the existing algorithms [1–6] in the literature deal exist with a single sensitive attribute only. However, a dataset may practically have multiple sensitive attributes (MSAs) [7–14]. For example, a hospital may publish data with more than one sensitive attribute, such as disease, symptom, and physician as shown in Table 1. The sensitive nature of healthcare records urges researchers to handle such scenarios and assure that the privacy of an individual may not be breached.

Table 1: Original data table T.

Personally identified attribute	Quasi-identifier attributes QIDs			Multiple sensitive attributes (MSAs)					
Name	Gender	Age	Zipcode	Cancer type	Cancer treatment	Physician	Diagnosis date	Symptom	Diagnostic method
p1 (Michael)	M	34	34548	Rectal	Surgery	Jack	7/8/19	Back pain	Chest X-ray
p2 (Lisa)	F	21	34607	Breast	Inhibitor therapy	Alan	17/8/19	Swelling	Ultrasound
p3 (Richard)	M	26	37506	Colon	Surgery	Daisy	22/11/19	Back pain	Blood test
p4 (Dave)	M	31	34549	Prostrate	Biologic therapy	Tom	29/08/19	Abdominal pain	Chest X-ray
p5 (Kate)	F	35	33753	Prostrate	Radiation	Frank	9/09/19	Testis swelling	Blood test
p6 (William)	M	38	43674	Liver	Ablation	Tom	5/08/19	Weight loss	CT scan
p7 (Robert)	M	27	35064	Rectal	Medication	Tom	12/08/19	Abdominal pain	CT scan
p8 (Olivia)	F	32	44662	Prostrate	Biologic therapy	Jack	21/09/19	Back pain	Blood test
p9 (Emily)	F	22	34548	Breast	Biologic therapy	Alan	13/09/19	Skin imitation	MRI test

In data publications, along with privacy, data utility is also a major concern so that researchers may perform research and analysis. Therefore, data should be anonymized in such a way that the research analysts may extract useful information. Balancing privacy and utility in privacy preserving data publishing (PPDP) is a NP-hard problem [15–20]. Therefore, the scenario in this paper is more challenging, as we consider the dimensionality in quasi-identifiers (QIs) as well as more than one sensitive attributes, i.e., MSAs.

An adversary or an attacker is a person who tries to breach the data privacy using different types of background knowledge (bk) about the MSA dataset. The bk includes the fact that certain pattern of values in published data is more likely to be observed than other values. For example, this knowledge can be fingerprint correlation (fcorr) knowledge, QI knowledge (qik) [10], or nonmembership knowledge (nmk) [21, 22]. MSA values in a table that belongs to a specific individual form a fingerprint. The fcorr between two k-anonymous [1] groups can increase an adversary knowledge. The qik is the personally identifiable information (PII) [21] for an adversary to uniquely identify an individual, and according to nmk, an individual cannot be linked to a specific sensitive value (SV). The (p, k)-Angelization [22] is a strong privacy algorithm for MSAs, where p represents the different sensitivity level of categorical SAs and k implies the k-anonymous QIs. The (p, k)-Angelization algorithm shown in Tables 2 and 3 are obtained from the original microdata in Table 1. The authors in [22] overcame the problem of the nmk attack but still privacy could be breached with fcorr named as the fcorr attack. The fcorr attack is comparatively considered as a strong privacy attack. If the adversary is intended to disclose privacy of almost every individual, the fcorr attack iteratively can breach the privacy of the whole dataset. The privacy breach scenario is explained in Section 1.1 in detail.

1.1. Motivation. The (p, k)-Angelization [22] algorithm directly adopts the single SA approach named as angelization [23] to implement privacy for MSAs. This approach invalidates the (p, k)-Angelization for the fcorr attack. The privacy breach scenario I explains the invalidation for [22] in detail. The complexity, lack of utility, and privacy breaches in SLOMS [24] and SLAMSA [25] techniques have already been invalidated by the (p, k)-Angelization. Although [22] is an efficient solution for utility improvement, the intruder can easily breach the privacy for a record using the bk and his intelligence. Our work has been motivated by the following limitations in the (p, k)-Angelization algorithm:

Table 2: Generalized table (GT) from the (p, k)-Angelization.

Gender	Age	Zipcode	Batch ID
Person Person	22–26	34548–37506	1
Person Person Person	31–38	34549–44662	2
Person Person	21–34	34548–34607	3
Person Person	27–35	33753–35064	4

(i) Privacy breach scenario I. For example, an adversary (i.e., David) intends to identify p2 (Lisa) information in Table 1. Since they both live in a neighbourhood, age, gender, and Zipcode are known (21, F, and 34607). Using QIs, David identifies her presence in group 3 of the generalized table (GT), i.e., Table 2, and through the batch ID, the sensitive batch table (SBT), i.e., Table 3, in group 3 can be accessed. For the (p, k)-Angelization, physician is a maximum weighted attribute (see Section 5.2). The maximum weighted attribute implies high dependency that has high privacy risk. An attack on it can easily breach privacy. So the intruder starts the attack from the physician attribute. It is an iterative process that leads to the record identification of the target

Table 3: Sensitive batch table (SBT) from the (p, k)-Angelization.

Physician	Cancer type	Cancer treatment	Diagnosis method	Symptom	Diagnosis date	Batch ID
Daisy, Alan	Colon, Breast	Surgery, Biologic therapy	Blood test, MRI test	Back pain, Skin irritation	22/11/19, 13/09/19	1
Tom, Jack	Prostrate, Liver	Ablation, Biologic therapy	CT scan, Chest X-ray, Blood test	Weight loss, Abdominal pain, Back pain	5/08/19, 21/09/19, 29/08/19	2
Alan, Jack	Rectal, Breast	Inhibitor therapy, Surgery	Chest X-ray, Ultrasound,	Back pain, Swelling	7/8/19, 17/8/19	3
Tom, Frank	Prostrate, Rectal	Radiation, Medication	Blood test, CT scan	Testis swelling, Abdominal pain	12/08/19, 9/09/19	4

individual and can identify the complete records in data table T. Since the (p, k)-Angelization blindly follows the angelization [23] mechanism, correlating the MSAs in different buckets may result in single SA values against each SA. This is a column-wise vertical correlation between two SA fingerprint buckets (SAFBs) in SBT that has common physicians and other SA values. The intruder takes intersection of SAFB 3 with groups having common physicians and proceeds iteratively until p2 is identified. So, he takes intersection between SAFB 3 and SAFB 2 because of the common physician Jack, between SAFB 2 and SAFB 4 because of Tom, and then between SAFB 3 and SAFB 1 because of Alan. Table 4 depicts the identified SVs and hence the disclosed individuals. Although the intruder was interested to identify only p2, the privacy of p1 and p4 was also breached during the process, which implies that this process iteratively can breach the individuals in the complete dataset.

The intruder uses Table 3 (SBT) and on each step stores the values in Table 4 and finally identifies all the sensitive information related to p2. In Table 4, the values against each physician attribute are the values obtained by taking intersection between two SAFBs in Table 3 linked through common physician's names. In Table 3, Jack is common between SAFB 3 and SAFB 2, so whatever value David gets from intersection, he adds against Jack in Table 1. First, chest X-ray is common in the diagnostics method. The leftover value ultrasound for sure belongs to Alan. While in group 3, both the remaining diagnosis values cannot be assigned to Tom, as Tom may have only one value, so the intruder is not sure at this stage. In the symptoms attribute, back pain is common and is stored against Jack. Here, another symptom value "*swelling*" is definitely for Alan because there is neither physician nor symptom. Since any further intersection for cancer treatment and cancer type does not produce any value, the process is forwarded to SAFB 2 and SAFB 4 because of Tom. Similarly, for the diagnostic method, Tom had CT scan and Blood test and no value for Frank. Although there is one value for Frank, the intruder can refine this while taking Frank intersection with other SAFBs that are not in the current sample dataset. In the symptom column, abdominal pain for Tom and the lifted value in SAFB 4 is testis swelling for Frank. The weight loss and back pain symptoms in SAFB 2 cannot be assigned to either Tom or Jack because the intruder has no enough information about this yet. For cancer treatment, there is no common value while for the cancer type *prostrate* is assigned to Tom. The last intersection process is between SAFB 1 and SAFB 3. Although there is no common value for the diagnostic method and the values in SAFB 3 are only related to rays, the intruder is intelligent enough that he can easily assign MRI test to Alan. This may not be the exact value, but can help to guess or identify the record. For symptom although we already have swelling for Alan, taking back pain for Alan which is already assigned to Jack and the only two values in this cell do not suit to the intruder knowledge. For cancer treatment, the common value is surgery and for the cancer type breast is the only attribute value. In SAFB 3, the leftover values are Rectal for Jack and in SAFB 1 and colon for Daisy. At the end, as the intruder also knows that p2 is a female, her attribute values {breast cancer, swelling, and ultrasound/MRI} can easily identify p2. The weighted sensitive attributes values disclosed against the linkable ($\mathscr{L}$) SA identifies the patient p2 record. Table 4 shows that during the process, the details about patient p1 and p4 are also identified. Some of the information regarding Frank and Daisy is incomplete or incorrect due to the fact that no further intersection with any other group is possible since the current data are sample data. This process iteratively executes and can also identify the remaining patients MSAs values.

(ii) Need for bucketization. Deeply analysing the (p, k)-Angelization, it is observed that all the features of angelization [16] were not well utilized. Tables 2 (GT) and 3 (SBT) by the (p, k)-angelization have one-to-one correspondence/linking between the two tables using the bucket id (BID). Due to the one-to-one correspondence, both tables are not considered as independent while the purpose of angelization was to publish both tables independently. Applying SA diversity may affect the utility in GT. Similarly, increasing the dimensionality in QIs in GT also decreases the utility. The adversary after finding a presence of an individual in a bucket in GT can easily move from GT to the exact group in SBT, where the $\mathscr{L}$ fingerprint buckets may help in isolating the sensitive values. In fact, splitting the table into GT and SBT in the (p, k)-angelization is useless.

In our proposed (c, k)-anonymization algorithm, the bucketization approach is adopted, which separates the QIs and SAs into two separate tables: generalized table (GT) and sensitive table (ST), independently. Both tables are respectively linked through BID.

GT consists of k-anonymous QIs generalized buckets (GBs), and an adversary cannot get additional information about an individual's privacy. The ST is a bucket table with

Table 4: Privacy breach in the (p, k)-Angelization.

Physician	Diagnosis method	Symptoms	Cancer treatment	Cancer type	Privacy breached
Jack	Chest X-ray (intersection between bucket 2 and 3)	Back pain (intersection between bucket 2 and 3)	—	Rectal (lifted after Alan got the breast)	p1
Alan	Ultrasound (after Jack got the chest X-ray between bucket 2 and 3) MRI test (from general knowledge of rays type treatment since in bucket 3 only ray-type methods exist)	Swelling (lifted symptom after Jack got the back pain from intersection between bucket 2 and 3) Back pain (temporary)	Surgery (wrong, but not very important)	Breast (intersection between bucket 1 and 3)	p2
Tom	CT scan, blood test (intersection between bucket 2 and 4)	Abdominal pain (intersection between bucket 2 and 4)	—	Prostrate (intersection between bucket 2 and 4)	p4
Frank	—	Testis swelling	—	—	—
Daisy	—	—	—	Colon (after Alan got the breast)	—

Table 5: (c, k)-anonymization generalized table (GT).

Name	Gender	Age	Zipcode	Bucket ID
p2 (Lisa)	F	[21–27] (21)	[34548–37506] (34607)	1
p9 (Emily)	F	[21–27] (22)	[34548–37506] (34548)	1
p3 (Richard)	M	[21–27] (26)	[34548–37506] (37506)	2
p7 (Robert)	M	[21–27] (27)	[34548–37506] (35064)	3
p8 (Olivia)	*	[32–38] (32)	[43674–44662] (44662)	1
p6 (William)	*	[32–38] (38)	[43674–44662] (43674)	2
p4 (Dave)	*	[31–35] (31)	[33753–34549] (34549)	3
p1 (Michael)	*	[31–35] (34)	[33753–34549] (34548)	1
p5 (Kate)	*	[31–35] (35)	[33753–34549] (33753)	3

MSAs in the bucketized form named as sensitive attributes fingerprint buckets (SAFBs). Anatomy [26] and Angel [23] are examples of bucketization for preserving privacy; however, they are applicable to single sensitive attributes. In this work, we use the bucketization for MSAs that can prevent different types of adversary's attack, e.g., fcorr attack. Tables 5 and 6 are the GT and ST produced by the proposed (c, k)-anonymization algorithm. In the proposed approach, better privacy has been achieved with minimum utility loss. It is also not necessary that the publisher should always publish the data with all their QIs attributes known as marginal publication. Marginal publication is to publish the GT with few QI attributes instead of all QI attributes, along with ST. The idea of marginal publication was introduced in [23]. The bucketization has the minimum information loss because of the independent publishing of the GT and ST. In both these tables, the connection is not between the buckets, instead it is between the records in generalized buckets and sensitive buckets.

1.2. Contributions. We propose an efficient solution (c, k)-anonymization for privacy preservation in MSAs. In (p, k)-angelization [22], privacy can be breached under the fcorr attack (explained in Section 1.1). The tables published by the proposed (c, k)-anonymization are depicted in Tables 5 and 6. The "Name" attribute in Table 5 is not published while publishing the data. The proposed approach also prevents against the adversary nmk and qik. The main contributions are as follows:

(i) We propose an improvement of (p, k)-angelization, named as the (c, k)-anonymizaiton algorithm, for MSAs privacy. The proposed solution prevents against fcorr attack. For reducing the privacy risk, the real (i.e., one to one) linking between GT and ST is transformed to one-to-many (i.e., real and likely) linking.

(ii) We formally model and investigate the invalidation of (p, k)-angelization for the fcorr attack and correctness of the proposed (c, k)-anonymization algorithm.

(iii) Based on the above points, the experimental results prove that our proposed approach provides better privacy and utility as compared to its counterpart.

2. Related Work

In this section, we broadly categorize the data privacy models in order to define boundaries of the proposed work in the available literature.

2.1. Data Privacy Models and Methods. Privacy models can be categorized as (i) syntactic (i.e., partition), or (ii) semantic (i.e., randomized). The syntactic approach achieves privacy in two levels: clustering data and privacy framework. The k-anonymity

Table 6: (c, k)-anonymization sensitive table (ST).

Physician	Cancer type	Cancer treatment	Diagnosis method	Symptom	Diagnosis date	Bucket ID
Jack, Alan	Rectal, breast, prostrate	Surgery, inhibitor therapy, biologic therapy	Chest X-ray, ultrasound, blood test, MRI test	Back pain, swelling, skin imitation	7/8/19, 17/8/19, 21/09/19, 13/09/19	1
Daisy, Tom	Colon, liver	Surgery, ablation	Blood test, CT scan	Back pain, weight loss	22/11/19, 5/08/19	2
Tom, Frank	Prostrate, rectal	Biologic therapy, radiation, medication	Chest X-ray, blood test, CT scan	Abdominal pain, testis swelling	29/08/19, 9/09/19, 12/08/19	3

[1] and then its extension l-diversity [3] and then the t-closeness [4] are the examples of syntactic data privacy models, in which the final set of groups are called equivalence classes (ECs). In the semantic approach, the original values are noised in a random way. ϵ-differential privacy [27] is an example of the semantic data model. The researchers have proposed both the syntactic and semantic privacy models for different types of data, e.g., single sensitive attribute [3, 4, 6], or MSAs [7–9], or 1 : m (i.e., one individual having many records) [28] microdata. For preserving the privacy, the algorithms in privacy models practice different approaches. These approaches can be categorized to (i) generalization [1–5, 13–15] (i.e., greedily convert the more specialized values to less specialized values), (ii) anatomy [25, 26] (i.e., partition the QI and S attributes), and (iii) microaggregation [29, 30] (i.e., dataset is partitioned into clusters where QI values of records are replaced with the mean of value). The proposed work in this paper considers the syntactic data privacy, using generalization and anatomy for MSAs.

2.2. Syntactic Anonymization Literature for Multiple Sensitive Attributes. A plethora of research contributions related to MSAs privacy [7–14, 16–18, 22, 24, 25, 31–38] exists. A recent work, anatomization with slicing [25] is an effective technique for MSAs. Although it does not generalize the QIs attributes, it enhances utility but publishes many tables, which makes the solution more complex. To prevent against proximity breach, the authors in [7] have adopted multi-sensitive bucketization (MSB) technique using clustering. However, it is applicable to numerical data only. The (α, l) model [8] for a single sensitive attribute satisfies the privacy requirements for MSAs. The authors in [31] prevent the negative and positive disclosure of associating between MSAs. In [33], rating of MSAs was proposed that fulfils the privacy requirements. However, the inherent relationship between the SAs can cause association rule attack. An adversary can use related bk to breach the privacy. The authors in [32] prevented the data from association attack and removed the weakness of the rating algorithm. In [37, 38], the authors perform vertical partitioning (i.e., anatomy) and implement decomposition and decomposition plus, respectively, to achieve l-diversity for MSAs. Decomposition plus [38] optimizes the noise value selection in [37] and keeps it closer to the original. The possibility of skewness and similarity attacks in [4, 39] was eliminated by the p^+ sensitive t-closeness model [40]. It combines the good features from p-sensitive k-anonymity [39] and t-closeness [4] approaches.

ANGELMS (anatomy with generalization for MSA) [34] vertically partitions the dataset into the QIs table and several SAs tables satisfying the k-anonymity [1] and l-diversity [3] principles, but still it can be attacked with similarity, skewness, and sensitivity attacks. In [16, 18], the KC Slice for dynamic data publishing of MSAs integrates the features of KC-privacy and slicing techniques. The authors have presented the method for a single release, and no studies for multiple releases are available to prove the dynamic claim. In [35, 36], MSAs were handled for achieving privacy but the l-diversity [3] principle was directly adopted that caused huge information loss. The nmk attack was prevented in [41] but still caused high information loss due to the grouping conditions over the data and vulnerability to the background join attack.

The proposed work categorizes the sensitivity of MSAs as top secret, secret, less secret, and nonsecret. c-diverse fingerprint buckets are created that contain records from different categories. The QI values of the created fingerprint buckets are bottom-up generalized through k-anonymity [1].

3. Preliminaries

Let table $T = \{\mathrm{EI}, \mathrm{QI}, S\}$ (as shown in Table 1) is the private data form for a publisher to publish. Let there be t tuples in T, and each tuple represents an individual or record respondent i. The components for tuple $t \in T$ are explicit identifier attributes (also called identifying attribute) $\mathrm{EI} = \{A_1^{ei}, A_2^{ei}, A_3^{ei}, \ldots, A_h^{ei}\}$, quasi identifier attributes (also called partial identifiers) $\mathrm{QI} = \{A_1^{qi}, A_2^{qi}, A_3^{qi}, \ldots, A_d^{qi}\}$, and sensitive information attributes $S = \{A_1^s, A_2^s, A_3^s, \ldots, A_m^s\}$. QIs are the partial identifiers or personally identifiably information (PII) that can identify an individual i if linked with external data, e.g., voting or census data. Data privacy is all about protecting the sensitive information, which are the confidential and private information belonging to an individual. In this work, we consider a challenging scenario of more than one sensitive attributes for a single individual named as multiple sensitive attributes (MSAs). Notations used in the paper are shown in Table 7.

Definition 1 (MSA fingerprint [22]). The MSAs values in table T that belongs to a specific individual form a fingerprint known as MSA fingerprint.

Definition 2 (sensitive attribute fingerprint bucket (SAFB)). A sensitive attribute partitioning of the microdata T consists of a list of SAFB: $\mathrm{FB}_1, \mathrm{FB}_2, \ldots, \mathrm{FB}_m$ according to the following conditions:

Table 7: Summary of notations used.

Symbol	Description
T	Original microdata
T^*	Anonymized form of T
A_i^{ei}	Explicit identifiers in T
A_i^{qi}	Quasi-identifiers in T
A_i^s	Sensitive information in T
GT	Generalized table
ST	Sensitive table
BID	Bucket identifier
ED	External dataset
GB	Generalized bucket
SAFB	Sensitive attribute fingerprint bucket
EC	Equivalence class
HLPN	High-level petri nets
ctg$T$	Category table for SAs
nmk	Nonmembership knowledge
fcorr	Fingerprint correlation knowledge
$\varnothing$	Null or zero
χ	External factor
w_i	Weight of dependent A_i^s
ξ_{w_i}	Maximum weighted attributes
ζ_{w_i}	Minimum weighted attributes
C	Category level (diversity) of SAs in Ctg$T$
$\mathscr{L}$	Linkability or linking between SAFBs
c_ℓ	Linkability control factor
k	k-anonymous level
δ	Single maximum weighted attribute after χ

(i) Each FB consists of two columns BID and MSA values.

(ii) $\cup_{i=1}^{m}\mathrm{FB}_i = \mathrm{ST}$, and for any $i \neq j$, $\mathrm{FB}_i \cap \mathrm{FB}_j = \varnothing$ or >1 among linkable ($\mathscr{L}$) buckets through maximum weighted sensitive attributes (δ) (see Section 5).

(iii) Each SAFB, FB_i $(1 \leq i \leq m)$ fulfils c-diversity from the category table (Table 8). The subscript i of FB_i is the BID of bucket FB_i.

Definition 3 (generalized bucket (GB)). A generalized bucket partitioning from an EC of the microdata T consists of buckets $B_1^{qi}, B_2^{qi}, B_3^{qi}, \ldots, B_n^{qi}$ such that

(i) Each B_i^{qi} is the set of tuples only with QI attributes of T and BID from FB

(ii) $\cup_{i=1}^{n} B_i^{qi} = \mathrm{GT}$, and for any $i \neq j$, $B_i^{qi} \cap B_j^{qi} = \varnothing$

(iii) Each generalized bucket B_i^{qi} $(1 \leq i \leq n)$ fulfils k-anonymity principle

3.1. Adversarial Model. In literature, an adversary is the attacker, who intends to breach the privacy and has different types of knowledge known as bk. Data correlation is an important type of adversary knowledge that breaches the privacy. The data correlation can be attribute correlation that exists among two or more attributes, e.g., [42], or row correlation between two or more rows, e.g., [43]. This paper is related to row correlation and more specifically FB correlation. This work focuses on reducing the threat exposed by FB correlation linked through the high-weighted SA value. Each FB contains few fingerprints that belong to k individuals in a specific GB inside GT. The adversary uniquely identifies an individual from the fingerprint correlation knowledge which has direct correspondence with the QI values.

Definition 4 (nonmembership knowledge (nmk) [22]). If an adversary knows that an individual i in GB cannot be linked to a specific SV in FB it is known as nmk.

Definition 5 (fingerprint correlation knowledge (fcorr)). The MSA values obtained from correlating two linkable FBs, i.e., $\mathrm{FB}_i \cap \mathrm{FB}_j$, can be assigned to a specific individual.

Based on the available information, we consider the adversary's bk consists of bk = {GT, ST, ED, nmk, qik, fcorr}, where

(i) GT (generalized table) $= \left\{A_1^{qi}, A_2^{qi}, A_3^{qi}, \ldots, A_d^{qi}, \mathrm{BID}\right\}$

(ii) ST (sensitive table) $= \{A_1^s, A_2^s, A_3^s, \ldots, A_m^s, \mathrm{BID}\}$

(iii) Any external dataset $\mathrm{ED} = \{\mathrm{ED}_1, \mathrm{ED}_1, \ldots, \mathrm{ED}_d,\}$ available publically

The adversary applies the bk on available anonymized data to perform an attack and to breach an individual's privacy.

Definition 6 (fingerprint correlation (fcorr) attack). The adversary with known QIs values and fcorr is able to perform fcorr attack by deducing single SVs from the intersection of FBs that are linked via δ. The fcorr attack can be

(i) Partial (pfcorr) attack: few of the SAs from fingerprints in two or more FBs may produce unique SVs

(ii) Full (ffcorr) attack: all of the SAs from fingerprints in two or more FBs may produce unique SVs

For an adversary, the ffcorr attack has no doubt to uniquely identify an individual while with the pfcorr attack can identify a record respondent if the resulted sensitive information belongs to the above minimum weighted attributes (ζ_{w_i}) (see 5.1 algorithm). The ζ_{w_i} attributes do no contribute in an individual record identification.

Definition 7 (high-level petri-nets (HLPNs) [44]). A petri-net is used as a model to examine the control of information in a system. HLPN formally analyses the system with mathematical properties. A HLPN is a 7-tuple $N = \{P, T, F, \varphi, R_n, L, \text{ and } M_0\}$, where P is a set of places represented by circles, T is a set of transitions represented by rectangular boxes such that $P \cup T \neq \varnothing$ and $P \cap T = \varnothing$, F is the flow relations such that $F \subseteq (P \times T) \cup (P \cup T)$, L are the labels on F, φ maps places to types., R_n represents the rules for transitions, and M_0 is the initial marking. In short, L, φ, and R_n represent the static semantic, whereas P, T, and F depict the dynamic structure.

Table 8: Category table from original microdata table T.

Category ID	Physician	Cancer type	Cancer treatment	Diagnosis method	Symptom	Diagnosis date	Sensitivity level
One	Daisy, Frank	Colon, prostrate	Surgery, radiation	Blood test	Back pain, testis swelling	22/11/19, 9/09/19	Top secret
Two	Jack	Rectal, prostrate	Surgery, biologic therapy	Chest X-ray, blood test	Back pain	7/8/19, 21/09/19	Secret
Three	Alan	Breast	Inhibitor therapy, biologic therapy	Ultrasound, MRI test	Swelling, skin irritation	17/8/19, 5/08/19, 12/08/19	Less secret
Four	Tom	Prostrate, liver, rectal	Biologic therapy, ablation, surgery	Chest X-ray, CT-scan	Weight loss, abdominal pain	29/08/19, 5/08/19, 12/08/19	Nonsecret

4. Critical Review for (p, k)-Angelization with fcorr Attack Identification Using Formal Modelling and Analysis

Definition 8 ((p, k)-Angelization [22]). A pair of bucket partitioning $= \{B_1, B_2, B_3, \ldots, B_n\}$ and batch partitioning $= \{C_1, C_2, C_3, \ldots, C_n\}$ of table T produces two tables GT and SBT such that

(i) GT consists of QI attributes with batch id (BID) belonging to table T. The QI values from t records are k-anonymously grouped and linked with SBT via BID.

(ii) SBT consists of (SA, BID), where BID is i $(1 \leq i \leq m)$ and SA are the MSA from table T.

(iii) Batch partitioning satisfies (p, k)-anonymity [16] where every bucket has records from p categories and have k-tuples to prevent against linking attack while the group partitioning satisfies (p, k)-anonymity [23].

The following reasons explains the invalidation for (p, k)-angelization [22].

(i) The invalidation of the existing (p, k)-angelization is due to the fcorr that causes fcorr attack (as shown in Table 4). Although the records from p categories are k indistinguishable on MSAs fingerprint, they are uniquely distinguishable because of unique SAFB values obtained from linkable buckets. So, Lemma 2 in [22] is incorrect. Its corrected form is given in Lemma 1 (Section 5).

(ii) Invalidation of theorem 2 in [15]: the adversary can correlate the sensitive information from qik. Scenario I explains the fcorr attack that extracts unique sensitive information using QI values.

Now, we formally model the (p, k)-angelization algorithm to check its invalidation with respect to the fcorr attack. The (p, k)-angelization algorithm is depicted with HLPN and formally analysed with its mathematical properties. The purpose of using HLPNs is to depict (i) the interconnection of the model components and processes, (ii) a clear flow of data among the processes, and (iii) the in depth inside about how the process of information takes place, in order to isolate the flaw in (p, k)-angelization. Figure 1 depicts HLPNs for (p, k)-angelization. The variable types and mapping of data types on places are shown in Tables 9 and 10, respectively. The adversarial model in Figure 1 comprises of three entities: end user, trusted data sanitizer, and adversary. The initial transition is referred to as input transition that contains the raw data (e.g., patient's EHRs) collected from a health organization. The trusted data sanitizer anonymizes the data using the (p, k)-angelization algorithm and produces GT (Table 2) and SBT (Table 3) tables. The produced tables are ready to be published which are exploited by the adversary through the fcorr attack in Table 4.

Rule 1 checks the existence of the number of dependent SAs with respect to another SA. Rule 2 counts the dependent attributes and selects the maximum weighted attributes. However, if there exists more than one in the weight set, then an external factor ε is added to one of them, based on some external facts. The weight set is sorted in descending to select the maximum weight as in rule 3 and 4. Based on weight calculation and MSAs in T, the category table is formed in rule 5.

Rule 1: $R(\text{Chk Dep}) = \forall i2 \in x2, i3 \in x3 \mid i3\ [1] := \text{Dep}\ (i2[2]_u, i2[2]_v)_{\forall i2[2]_u, i2[2]_v \in x2 \mid u \neq v}$

$\wedge x3' := x3 \cup \{(i3[1])\}$

Rule 2: $R(\text{Wt} - \text{Cal}) = \forall i4 \in x4, \quad i5 \in x5 \mid i5[1] := \text{calcWt}(|i4[1]|)$

$\wedge \max(i5[1]) \wedge \text{same}(i5[1]) > 1 \longrightarrow i5[1] + \varepsilon$

$\wedge i5' := x5 \cup \{(i5[1])\}$

Rule 3: $R(\text{SortData}) = \forall i6 \in x6, \quad i7 \in x7 \mid i7[1] := \text{wtSort}\ (|i6[1]|)$

$\wedge i7' := x7 \cup \{(i7[1])\}$

Rule 4: $R(\text{MaxWt}) = \forall i8 \in x8, \quad i9 \in x9 \mid i9[1] := \max \text{Wt}\ (i8[1]) \wedge$

$\wedge i9' := x9 \cup \{(i9[1])\}$

Rule 5: $R(\text{Categorize}) = \forall i10 \in x10, \quad i11 \in x11 \mid i11[1] := i10[1] \wedge i11[2] := i1[2]$

$\wedge i11' := x11 \cup \{(i11[1], i11[2])\}$

The problem arises from rule 6 onward. The (p, k)-angelization [22] blindly follows the basic angelization [23] mechanism. According to rule 6, the data in table T based on the category table (Table 8) use angelization to create GT and SBT. In [23], the $\mathscr{L}$ between two SA buckets

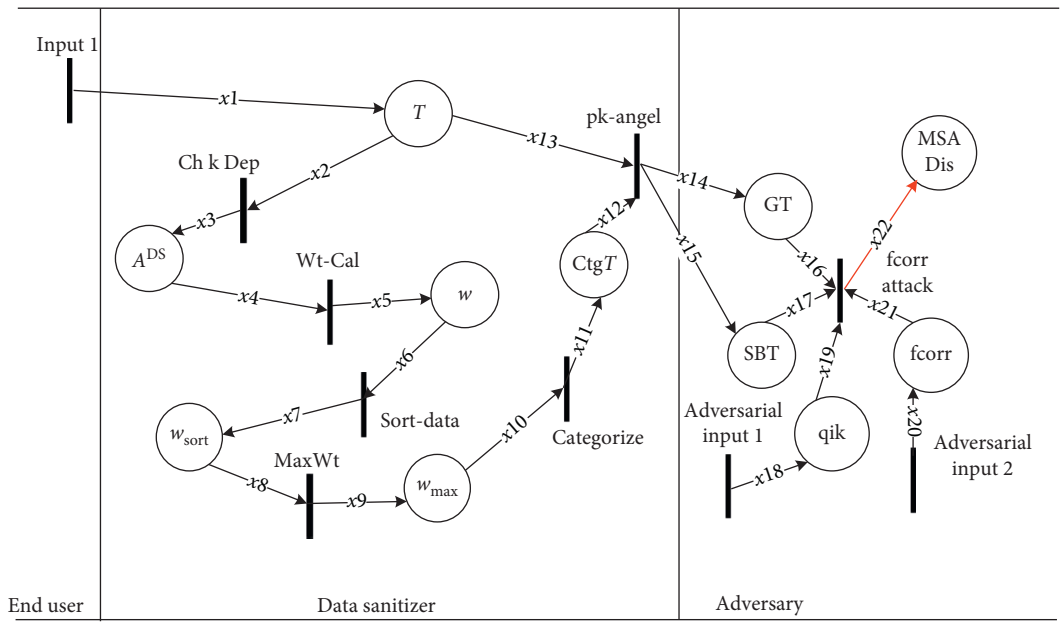


Figure 1: HLPN for (p, k)-angelization.

Table 9: Types used in HLPN for the (p, k)-angelization.

Types	Descriptions
T	Place holding integer and string type data
PID	An integer identifying patient id
A^{DS}	A set consists of dependent sensitive attributes
w	An integer defines final calculated weights of A^{DS}
w_{sort}	Set containing sorted weight of SA in descending
w_{max}	Maximum weight after adding external factor χ
C	Category Id for MSA
BID	Batch id used to connect GT and SBT
QI	Quasi-identifier for ith end user.
MSF	Multiple sensitive fingerprint values for ith end user

Table 10: Mapping of data types on places.

Places	Mapping
$\varphi\ (T)$	$\mathbb{P}\ (\mathrm{QI} \times \mathrm{MSF} \times \mathrm{PID})$
$\varphi\ (A^{DS})$	$\mathbb{P}\ (A^{DS})$
$\varphi\ (w)$	$\mathbb{P}\ (w)$
$\varphi\,(w_{sort})$	$\mathbb{P}\,(w_{sort})$
$\varphi\,(w_{max})$	$\mathbb{P}\,(w_{max})$
$\varphi\,(\mathrm{Ctg}T)$	$\mathbb{P}\ (C \times \mathrm{MSF})$
$\varphi\,(\mathrm{GT})$	$\mathbb{P}\ (\mathrm{QI} \times \mathrm{BID})$
$\varphi\,(\mathrm{SBT})$	$\mathbb{P}\ (\mathrm{MSF} \times \mathrm{BID})$
$\varphi\,(\mathrm{qik})$	$\mathbb{P}\ (\mathrm{QI} \times \mathrm{BID})$
$\varphi\,(\mathrm{fcorr})$	$\mathbb{P}\ (\mathrm{MSF} \times \mathrm{BID})$
$\varphi\,(\mathrm{MSA\ Dis})$	$\mathbb{P}\ (\mathrm{QI} \times \mathrm{MSF} \times \mathrm{PID})$

does not exist because of single SA. While handling the MSAs, the basic angelization is not applicable without proper measures. Rule 7 shows the fcorr attack that breaches the privacy of an individual. In 7, the known QI values in a specific GB in GT have exactly a single-correspondent FB in SBT for applying the fcorr attack to disclose unique values from the MSAs $\mathscr{L}$ FBs.

Rule 6: $R\,(\mathrm{pk-Angel}) = \forall i12 \in x12,\ i13 \in x13, i14 \in x14, i\ 15 \in x15|$

$i14\,[1] \coloneqq \mathrm{angel}\,(\{i12\,[1]\}, \{i13\,[1], i13\,[2], i13\,[3]\})$ $\wedge i14\,[2] \coloneqq \mathrm{bucketID}\,(i12\,[1])$

$\wedge i14' \coloneqq x14 \cup \{(i14\,[1], i14\,[2])\}$

$i15\,[1] \coloneqq \mathrm{angel}\,(\{i12\,[1]\}, \{i13\,[1], i13\,[2], i13\,[3]\}) \wedge$ $i15\,[2] \coloneqq \mathrm{bucketID}\,(i12\,[1])$

$\wedge i15' \coloneqq x15 \cup \{(i15\,[1], i15\,[2])\}$

Rule 7: $R\,(\mathrm{fcorr\ Attack}) = \forall i16 \in x16,\ \ i17 \in x17, i19 \in x\ 19, i21 \in x21, i22 \in x22|$

$\mathrm{qik}i16\,[1], i\,[19\,[1]) \longrightarrow i22\,[1] \coloneqq i13\,[1] \wedge$

$\mathrm{fcorrDis}\,(i17\,[1] i_{\forall i17[1]_{\mathscr{L}} \in i}, i21\,[1]) \longrightarrow i22\,[2] \coloneqq$ $i13\,[2] \wedge\ i22\,[3] \coloneqq i13\,[3]$

5. Proposed (c, k)-Anonymization for Multiple Sensitive Attributes

Although the (p, k)-Angelization model is a state-of-the-art approach for MSAs, especially for the categorization of sensitive values. But the ST still lacks in privacy because of blindly using the same angelization [23] approach for MSAs. It leads to fcorr attack, i.e., ffcorr attack or pfcorr attack. We name the improved form of (p, k)-angelization as (c, k)-anonymization for MSAs and is describe as follows:

Definition 9 ((c, k)-anonymization). A pair of generalized bucket partitioning $= \{B_1^{qi}, B_2^{qi}, B_3^{qi}, \ldots, B_n^{qi}\}$ and sensitive attribute fingerprint bucket partitioning $= \{\mathrm{FB}_1, \mathrm{FB}_2, \ldots, \mathrm{FB}_m\}$ of table T produces two tables GT and ST such that

(i) GT consists of QI attributes buckets B_i^{qi} $(1 \le i \le n)$ with bucket id (BID) belonging to table T. The QI values belonging to t records are k-anonymously

grouped and linked with corresponding sensitive buckets in ST via BID. And $\cup_{i=1}^{n} B_i^{qi} = \text{GT}$, and for any $i \neq j$, $B_i^{qi} \cap B_j^{qi} = \varnothing$.

(ii) ST consists of (FB_i and BID), where BID is i ($1 \leq i \leq n$) and FB are the MSAs in buckets from table T. And $\cup_{i=1}^{m} \text{FB}_i = \text{ST}$, for any $i \neq j$, and $\text{FB}_i \cap \text{FB}_j = \varnothing$ or > 1 among linkable ($\mathscr{L}$) buckets through maximum weighted sensitive attributes (δ).

(iii) Generalized bucket partitioning satisfies definition 3 and sensitive bucket partitioning satisfies definition 2 based on the category table Ctg$T$ (Table 8). Every generalized bucket has k-tuples to prevent against linking attack. The sensitive partitioning has c-diverse records from c categories in Ctg$T$ such that

(a) for strict approach, fulfil equation (4)
(b) for relax approach, fulfil equation (5)

Lemma 1 (uncertainty in $\mathscr{L}$ SAFBs). *If for T having the MSAs dataset, the anonymized form T' satisfies (c, k)-anonymization, then T' satisfies (c, k)-diversity for MSA fingerprints.*

Proof. Let sbp be the random sensitive bucket partitioning in T'. There must be at least t tuples from c categories in sbp such that ($\text{sbp}_a \cap \text{sbp}_b > 0$ or 1, $\text{a} \neq \text{b}$) or the fcorr $\leq \zeta_{w_j} \forall\, \text{sbp}_{\mathscr{L}}$, where ζ_{w_j} are the minimum weighted SAs having the lowest dependency (see algorithm 5.1). So the c categorized records are indistinguishable on the MSA fingerprint by k records. Thus, sbp satisfies the definition of (c, k)-diversity and uncertainty in $\mathscr{L}$ SAFBs is maximized. □

5.1. Privacy Risk: Feasibility of the Proposed Work. The presence attack and fcorr attack are the two possible attacks that breach the privacy of GT and ST, respectively. The adversary can breach an individual's privacy by linking the obtained sensitive information with the QI values and with the bk. Every QI record has a corresponding SA fingerprint in a specific FB, as depicted in Tables 2 and 3. The (p, k)-angelization has the one-to-one real linking through BID. The real linking has high privacy leakage and 100% chances of presence attack. Another type of linking can be the likely linking between GT and ST where all BID linking are not real. Relating the real and likely linking, the privacy risk for an individual is defined as $\text{PriRisk}(t) = (r/n)$, where r are the real linking and n are the total number of likely linking. The likely linking for a specific size of EC varies, and it depends on the QI values in GT that have linking with certain FBs. For preventing privacy leakage $\text{PriRisk}(t) \leq (1/l)$, where l represents the l-diversity [3]. Every FB has c-diverse fingerprints that correspond to at least k individuals. In our proposed (c, k)-anonymization, for $c = 1$, implies $l = 2$; for $c = 2$, implies $l \leq 4$; for $c = 3$, implies $l \leq 6$, and so on.

Consider the privacy risk for the given Tables 5 and 6 processed by proposed (c, k)-anonymization. In GT Table 5, for $c = 2$, there are three different sizes of ECs that have varying l-diversity (ranging $2 \leq l \leq 4$) in ST Table 2. For EC size 4, $r = 4$ and $n = 4 \times 4 + 4 \times 2 + 4 \times 3 = 42$; so, $\text{PriRisk}(t) = (r/n) = (4/42) \leq (1/4) \Longrightarrow 0.09 \leq 0.25$, which is a very low privacy risk. Similarly, for EC size 2, $r = 2$ and $n = 2 \times 4 + 2 \times 2 = 12$; so, $\text{PriRisk}(t) = (2/12) \leq (1/2) \Longrightarrow 0.16 \leq 0.5$. For the last EC size 3, $r = 3$ and $n = 3 \times 3 + 3 \times 4 = 21$; so, $\text{PriRisk}(t) = (3/21) \leq (1/3) \Longrightarrow 0.14 \leq 0.3$. Even in case when in an EC, the minimum distance QI values link to a single FB in ST, for example, when EC size is 2, then $r = 2$ and $n = 2 \times 2 = 4$ so $\text{PriRisk}(t) = (2/4) \leq (1/2) \Longrightarrow 0.5 \leq 0.5$, and the probability of privacy disclosure is the diversity in the FB. In certain cases, the higher utility in QI values may further increase the likely linking which will more reduce the privacy risk. This proves that the proposed approach has very low privacy risk for the presence attack and data disclosure.

5.2. (c, k)-Anonymization Algorithm. The objective of the proposed (c, k)-anonymization algorithm is to provide a sustainable privacy for MSAs. The algorithm gets a microdata table T (Table 1) as input and produces two anonymized tables, i.e., GT (Table 5) and ST (Table 6).

The proposed Algorithm 1 performs two major functionalities: categorizing the MSAs based on calculated weights and creating secure FBs for the whole dataset. For SA categorization, the algorithm calculates weights for all the MSAs in the dataset to get to know the dependency of SAs. The dependency shows the sensitivity level of the SAs. These weights are sorted in the descending order to get categorized MSAs. The weights calculation for MSAs creates the category table (Ctg$T$) that helps to create l-diverse (c-diverse with respect to category) FBs. The FBs must satisfy equations (4) and (5) in order to prevent fcorr attack. Therefore, if some of the FBs are not according to equations (4) or (5) they are refined to fulfil. The purpose to refine is because the input data may be of different nature and may contain SVs that may not be grouped initially. The complete algorithm (Algorithm 1) and its working are explained in the following:

Sensitive attributes weight calculation. In Algorithm 1, a calling function wtCalc( ), shown in Function 1, calculates weights for all the MSAs from Table 1. There are six different types of SAs, and each has its own level of sensitivity or sensitivity weights. Let $W = \{w_1, w_2, \ldots, w_n\}$ is the set of weights for each SA such that s_1 has weight w_1, s_2 has weight w_2, and so on. SA weights are the dependency on all other SAs. Similar to [22] the weight is calculated in the following equation:

$$w_i = \sum_{u=1}^{m} \text{Dep}(s_u, s_v)_{\forall v \in S \wedge u \neq v}, \tag{1}$$

where m are the total number of attributes dependent on attribute s_u. The dependency of an SA is determined by the total range of attributes identifying the SAs. The for loop in the beginning calculates the sensitivity for s_u with all other SAs, i.e., s_v. This determines the sensitivity level for all the SAs. To calculate the weights (second for loop), cardinality checking is performed of all dependent attributes. Calculated weights for the SAs that exist in microdata are shown in Table 11.

```
Input:
T: Microdata table = {ID, QI, S}
χ: External Factor
Output:
GData: Generalized Table-GT
SAFB: Sensitive Table-ST
Procedure CK − ANONYMIZATION (T)
SAFB = { }, GData = { }
w_i = wtCalc (w, D, s, h)
∀ξ_{w_j} = (max (w_i))_{∀w_i∈W}
∀ζ_{w_j} = (min (w_i))_{∀w_i∈W}
∀w_j ∈ ξ_{w_j} . w_j = w_j + χ (w_j)
   v = Sort (w_j)
   δ = (max (v))
CtgT = Categorize (δ, MSA)
FB = CreateFB (CtgT, T)
while FB ≠ { }
   if FB_k satisfy equation (4) then
      SAFB = SAFB ∪ FB_k
   else
      SAFB RefineFB ( )
   end if
end while
GData = Generalization (T, SAFB, k)
return GData, SAFB
```

Algorithm 1: (c, k) − anonymization.

```
Input:
   s: sensitive attribute (SA)
   w: weight for a SA
   Dep: SA dependency
   h: height of dependency (no. of dependent SAs)
Output: list of weights for all SA, i.e., w_i
for each s_u and s_v
      Dep (s_u, s_v)_{∀u ≠ v}
end for
for check all dependent SAs
      w_i = |Dep (s_u, s_v)|_{∀v∈Dep (s_u,s_v)}
end for
return w_i
end function
```

Function 1: Function wtCalc $(w_i$, Dep, s, and $h)$.

Table 11: MSAs weight calculation.

Sensitive attributes	Identified by	Dependency	Weightage
$s1$: cancer type	$s2$, $s3$, $s6$	3	3
$s2$: cancer treatment	$s1$	1	1
$s3$: physician	$s1$, $s2$, $s6$	3	3
$s4$: diagnostic date	—	0	0
$s5$: symptoms	—	0	0
$s6$: diagnostic method	s1	1	1

Maximum weighted sensitive attributes selection. From the calculated dependencies through Function 1, maximum weighted attributes ξ_{w_j} are selected. Maximum weights mean high dependency leads to high disclosure risk. So attributes set with ξ_{w_j} needs maximum protection. Although there are very rare chances, the problem arises if there exists more than one SAs having the same ξ_{w_j}. Then, an external factor χ is added to select only one maximum weighted attribute. The algorithm adds an external factor χ, i.e., $w_j + \chi(w_j)$ to each attribute in set ξ_{w_j}, and the weights w_i are then sorted in the descending order to get one single maximum weighted SA (δ) (can be seen in Algorithm 1).

Categorizing sensitive attributes. Attribute occurring in the first location of the set w_j is selected as δ. The descending order of calculated weights for MSA is categorized through the categorize() function as top secret, secret, less secret, and nonsecret, in Table 8. From weight calculations, although disease and physician have equal weights, we select physician as the maximum weighted SA (δ) because of some other external factors χ. For example, physician information may be publically available on the Internet.

Creating FBs. FBs consist of MSAs with the BIDs column at the time of anonymization. Function 2, function CreateFB( ), shows the whole process for creating c-diverse FBs. Create FBs mainly based on Ctg$T$ (as shown in Table 8). Let $A^s = \{A_1^s, A_2^s, \ldots, A_m^s\}$ and N are the total number of records in the microdata table T. To create a 2-anonymous 2-diverse FB, i.e,. $k = 2$, $l = 2$ (i.e., $c = 1$), for example, r_u and r_v are two different records in T such that $r_u \in \text{ctg}_x$ and $r_v \in \text{ctg}_y$, where $\text{ctg}_x \neq \text{ctg}_y$ and $\text{ctg}_i \in \text{Ctg}T$. The union of these two different records from different sensitive categories creates an FB, as shown in the following equation:

$$\text{FB}_k = \left(r_u \in \text{ctg}_x\right) \cup \left(r_v \in \text{ctg}_y\right), \tag{2}$$

where $u \neq v$ and $x \neq y$. Selecting records from different categories to create an FB is to implement the l-diversity principle in the form of c-diversity in our case. Privacy in data is all about creating an EC that prevents an intruder to breach any of its sensitive contents. Unlike [22], we focus on creating an FB that satisfies c-diversity and prevents against any attack from the adversary, e.g., fcorr attack. The fcorr attack is prevented by taking two measures: (i) minimizing the likability or linking ($\mathscr{L}$) between two FBs and (ii) uncorrelating the records or maximizing the uncertainty between the $\mathscr{L}$ FBs (explained in Refine FB).

Patients records (i.e., SVs) are high in number as compared to the physician attribute and both can normally be correlated or linked with one another. This $\mathscr{L}$ provides a reason for an attack. Therefore, to minimize the $\mathscr{L}$, we use the linkability control factor ($\mathscr{c}_f$), ($1 \leq \mathscr{c}_f \leq$ max count for specific δ). $\mathscr{c}_f$ minimizes the repetition of the same δ value in different FBs. The table (Table 6) published by the proposed algorithm has $\mathscr{c}_f = 2$, which means that a maximum of two records for a single physician can exist in an FB. This brings the existing δ values to minimum FBs and $\mathscr{L}$ is reduced. So, the chances of the fcorr attack on possible FB are ultimately reduced (Table 3 has 3 $\mathscr{L}$ FBs while Table 6 has only 1 $\mathscr{L}$ FB). The high value for $\mathscr{c}_f$ further reduces $\mathscr{L}$

```
Input:
  FB = {FB_1, FB_2, FB_3, ..., FB_FB}, all FBs in the
  whole dataset T
  r: source record to create FB, it can be r_u or r_v, u ≠ v
  N: no. of records in the actual dataset T
  c_ℓ: linkability control factor
  k: k-anonymity level (minimum FB size)
  ctg_x: any category of SA in category Table 8
  ctg_y: any category of SA in category Table 8
Output: FB having list of FB_k with k-anonymous records
in each
FB = { } FB_k = {}
while N ≠ ∅
  if N < 2k then
    FB_k = N
    FB = FB ∪ FB_k
  else
    r_ux = (∀r_{u·δ_same} ∈ ctg_x) ≤ c_ℓ
    //if e.g. c_ℓ = 2, will select max 2
    //records having same physician
    r_vy = distinct (∀r_{v·δ_same} ∈ ctg_y) ≤ c_ℓ,
    //where u ≠ v and x ≠ y
    FB_k = {r_ux}
    FB_k = {FB_k ∪ {r_vy}}
    FB = FB ∪ FB_k
    N = N\FB_k
  end if
end while
return FB
end function
```

Function 2: *Function* CreateFB (r_u, r_v, N, c_ℓ, FB, FB_k, ctg_x, ctg_y).

but increases information loss, so a balance should be maintained between c_ℓ and utility preservation.

Refining FBs. FBs are refined through the function Refine FB( ), as depicted in Function 3. The fcorr attack between any two $\mathscr{L}$ FBs can breach the privacy. The purpose is to completely avoid the correlation. A percentage of record that discloses from intersection between $\mathscr{L}$ FBs can be associated to a specific individual. For example, any percentage of record obtained from equation (3) that results in a single value for each SA correlation is a privacy breach and is not acceptable, especially for high weighted attributes.

$$\mathrm{FB}_i \cap \mathrm{FB}_j = \left\{A^s_{1i} \cap A^s_{1j},\ A^s_{2i} \cap A^s_{2j}, \ldots, A^s_{mi} \cap A^s_{mj}\right\}, \qquad (3)$$

where $i \neq j$ and i, j are $\mathscr{L}$ via δ. The high percentage disclosure infers a high intruder confidence for privacy breach and vice versa. The decreasing order of w_i is the decrease in probability of privacy breach, among the n $\mathscr{L}$ FBs. The measure to prevent against the fcorr attack is no or minimum data expose from intersection. The refining process in Function 3 for FBs works under two approaches, i.e., strict and relax. Strict approach is given in the following equation:

$$\mathrm{FB}_{\mathrm{i}}^{w_i-\delta} \cap \left\{\mathrm{FB}^{w_i-\delta}\Big|_j^n\right\} = 0 \text{ or} > 1, \quad \forall A^s, \qquad (4)$$

```
Input:
FB = {FB_1, FB_2, ..., FB_n}: a set of FB that are linked
via the same δ
k: minimum k-anonymity level
Output: set of refined FB = {FB_1, FB_2, ..., FB_n},
linked via same δ.
while FB ≠ { }
  [if FB_k satisfies equation (4) then // Strict ECs or
OR if FB_k satisfies equation (5) then] // Relax ECs
    SAFB = SAFB ∪ FB_i
  else
    SAFB = SAFB ∪ {FB_i = {FB_i ∪ r_v1 ∈ FB_j}}∧
    SAFB = SAFB ∪ {FB_n = {FB_n ∪ r_v2 ∈ FB_j}} // where
      //(r_v1 & r_v2) ∈ FB_j, merge the FBs, FB_j dissolved
  end if
end while
return SAFB
```

Function 3: *Function* RefineFB( ).

where $i \neq j$ and FBs are $\mathscr{L}$ through δ, i.e., $\delta_{\mathrm{FB}_i} = \delta_{\mathrm{FB}_j}$, for example, they are $\mathscr{L}$ through the physician and n are the total number of FBs where the same physician exists. The intersection in this case ensures that fcorr should be zero or have more than one SVs in common to create uncertainty for single SA.

In case of the worst dataset, there may be some of the records that do not fit in any FB via the strict approach. A relax strategy is adopted with no breach in privacy. The percentage of record exposure from fcorr is minimized to an acceptable value. In the worst case scenario, the proposed (c, k)-anonymization maintains fcorr $\leq \zeta_{w_j}$, $\forall \mathrm{FB}_{\mathscr{L}}$ where ζ_{w_j} are the minimum weighted attributes that have no dependency. Relax strategy is given in the following equation:

$$\mathrm{FB}_i^{w_i-\left(\zeta_{w_i}\cup\delta\right)} \cap \left\{\mathrm{FB}^{w_i-\left(\zeta_{w_i}\cup\delta\right)}\Big|_j^n\right\} = 0 \text{ or} > 1, \quad \forall A^s, \qquad (5)$$

where $i \neq j$ and FBs are $\mathscr{L}$ through δ, i.e.,$\delta_{\mathrm{EC}_i} = \delta_{\mathrm{FB}_j}$, for example, they are $\mathscr{L}$ through physician and n are the total number of FBs where the same physician exists. According to equation (5), only fcorr $\leq \zeta_{w_j}$, $\forall \mathrm{FB}_{\mathscr{L}}$ is acceptable which is a percentage of information leakage but not a privacy breach because of not dependent attributes and hence impossible for an intruder to link with other SA or QI of a specific patient record. The working of RefineFB() function for equation (5) is the same as it is for equation (4).

Generalization. Function 4 deals with QI attributes with BIDs that correspond to unique FBs in ST. Initially, the records are sorted by QIs. Then, every individual record is generalized to achieve k-anonymous EC. For generalizing the tuple $t \in N$, the t QI $= \{x_1, x_2, \ldots, x_n\}$ is generalized to $\mathrm{QI}' = ([y_1 - z_1], [y_2 - z_2], \ldots, [y_n - z_n])$, where $y_i \leq x_i \leq z_i$ and y_i, z_i are the close boundaries for x_i. The Generalization() function in Function 4 shows the generalization process.

```
Input:
T: QI attributes from original microdata T
k: k anonymity level
BID: Bucket identifier from SAFBs
Output: GData
GData = { }
N = |T| //BID is received from SAFBs
sort N w.r.t QIs
  while N ≠ ∅
    if N < 2k then
      GData = N
    else
      GData = GData ∪ gen(N) // using BID
  each GB has mostly both real and likely linking
    end if
  end while
  return GData
  end function
```

Function 4: *Function* Generalization (T, SAFB, k).

5.3. Formal Modelling and Analysis for Proposed (c, k)-Anonymization Algorithm. In this section, we do formal modelling of the proposed (c, k)-anonymization algorithm to analyse and formally validate against adversary's background knowledge, i.e., fcorr attack. We have used HLPN (Definition 7) to model the proposed system. The HLPN provides the mathematical representation to analyse the behaviour of the proposed system. For a system representation in HLPN, first, the data types associated with the P (Places) are defined and then the set of rules for HLPN are defined. Figure 2 represents the HLPN for the proposed (c, k)-anonymization algorithm. Tables 12 and 13 show the data types and mapping of data types on places that are described which are involved in the proposed algorithm HLPN.

The algorithm begins from weight calculation as in [22] to create the Ctg$T$ table (Table 8). So, the transitions in rules 1, 2, 3, 4, and 5 are the same for the proposed (c, k)-anonymization algorithm. The main goal is to nullify rule 7 and to create such FBs that prevent against fcorr attack. In rule 8, the FBs are created. The function createFB() takes T (i.e., $\mathbb{P}$ (QI × MSF × PID)), and based on category id C the categorized MSA are accommodated into different c-diverse FBs.

Rule 8 $R(\text{Crt}-\text{FB}) = \forall i12 \in x12, i13 \in x13, i14 \in x\ 14|$

$i14[1] \coloneqq \text{createFB}(\{i13[1]\}, \{i12[1], i12[2], i12[3]\})$
$\wedge i14[2] \coloneqq \text{bucketID}(i13[2])$

$\wedge i14' \coloneqq x14 \cup \{(i14[1], i14[2])\}$

In the next step, the created FBs in 8 are evaluated to prevent fcorr attack. Rule 9 gets an input of equations (4) and (5) to verify the nonexistence of fcorr knowledge between different $\mathscr{L}$ FBs. All those FBs that satisfy either of the equation are stored at place SAFB via rule 10, while other SAFBs are forwarded for refinement to satisfy the equations as shown in rule 11.

Rule 9: $R(\text{Chk}-\text{Eqs}) = \forall i15 \in x15, i17 \in x17, i18\ \in x18|$

satisfy equation $(i17[1]i_{\forall i17[1]_{\mathscr{L}} \in i}) = i15[1] \longrightarrow$
$i18[1] \coloneqq \text{TRUE} \wedge i18' \coloneqq x18 \cup \{(i18[1])\}$

$\vee$satisfy equation $(\text{i}17[1]j_{\forall i17[1]_{\mathscr{L}} \in j}) \neq i15[1] \longrightarrow i18[1]$
$\coloneqq \text{FALSE} \wedge i18' \coloneqq x18 \cup \{(i18[1])\}$

Rule 10: $R(\text{Pick FB}) = \forall i19 \in x19, i20 \in x20, i21\ \in x21|$

$i20 = \text{TRUE} \longrightarrow i21[1] \coloneqq \text{storeAll}(i19[1]k_{\forall i19}$
$[1] \in k) \wedge i21[2] \coloneqq i19\ [2]$

$\wedge i21' \coloneqq x21 \cup \{(i21[1], i21[2])\}$

Rule 11: $R(\text{Call RFB}) = \forall i22 \in x22, i23 \in x23, i24\ \in x24|$

$i22 = \text{FALSE} \longrightarrow\ i24[1] \coloneqq \text{storeAll}(i23[1]j_{\forall i23[1] \in j}) \wedge$
$i24[2] \coloneqq i23[2]$

$\wedge i24' \coloneqq x24 \cup \{(i24[1], i24[2])\}$

The minimum requirement to prevent from the fcorr attack is to at least satisfy equation (5). In rule 12, such requirements are fulfilled via function RefineFB() for all the FALSE FBs from rule 9 and are stored at place SAFBr. Rule 13 just combines all the secured FBs from places SAFB and SAFBr to create one ST that can prevent from any bk attack, e.g., fcorr attack.

Rule 12: $R(\text{Crt RFB}) = \forall i25 \in x25, i26 \in x26|$

$i26[1] \coloneqq \text{refineFB}(i25[1]k_{\forall i25[1] \in k}) \wedge i26[2] \coloneqq i25$
$[2] \wedge i26' \coloneqq x26 \cup \{(i26[1], i26[2])\}$

Rule 13: $R(\text{Crt ST}) = \forall i27 \in x27, i28 \in x28, i29\ \in x29|$

$i29[1] \coloneqq \text{combine}(i27[1], i28[1]) \wedge i29[2] \coloneqq$
$\text{combine}(i27[2], i28[2])$

$\wedge i29' \coloneqq x29 \cup \{(i29[1], i29[2])\}$

The generalization of the QIs in T with respect to the sensitivity categorization and the BID obtained from ST (rule 13) is performed in rule 14. The created GT and ST tables via rules 13 and 14, respectively, can thwart against an adversary's presence and fcorr attacks and are ready to publish. Rule 15 shows the adversary's zero gain after attack.

Rule 14: $R(\text{Gen}) = \forall i30 \in x30, i31 \in x31, i32 \in x32,$
$i33 \in x33|$

$i33[1] \coloneqq \text{generalize}(\{i31[1]\}, \{i30[1]\})$
$\wedge i33[2] \coloneqq i32[2]$

$\wedge i33' \coloneqq x33 \cup \{(i33[1], i33[2])\}$

In rule 15, the adversary's bk, i.e., fcorr, consists of QI, MSA, and PID. To apply the fcorr attack, the adversary compares the SVs in bk with published tables MSA buckets and with the corresponding QIs to get a matching MSAs that belong to a specific PID as in the original table T. However, the adversary fails to do so and the union of the bk yields an empty set, which shows that the bk could not identify a specific individual record.

Rule 15: $R(\text{fcorr Attack}) = \forall i34 \in x34, i35 \in x35, i37 \in$
$x37, i38 \in x38|$

$\text{fcorrDis}(i34[1], i35[1]) \longrightarrow (\{i34[1], i35[1]\} \cup$
$i37[2]) \neq i12[2] \wedge i12[3]$

$(i38[1] \cup i38[2]) = \varnothing$

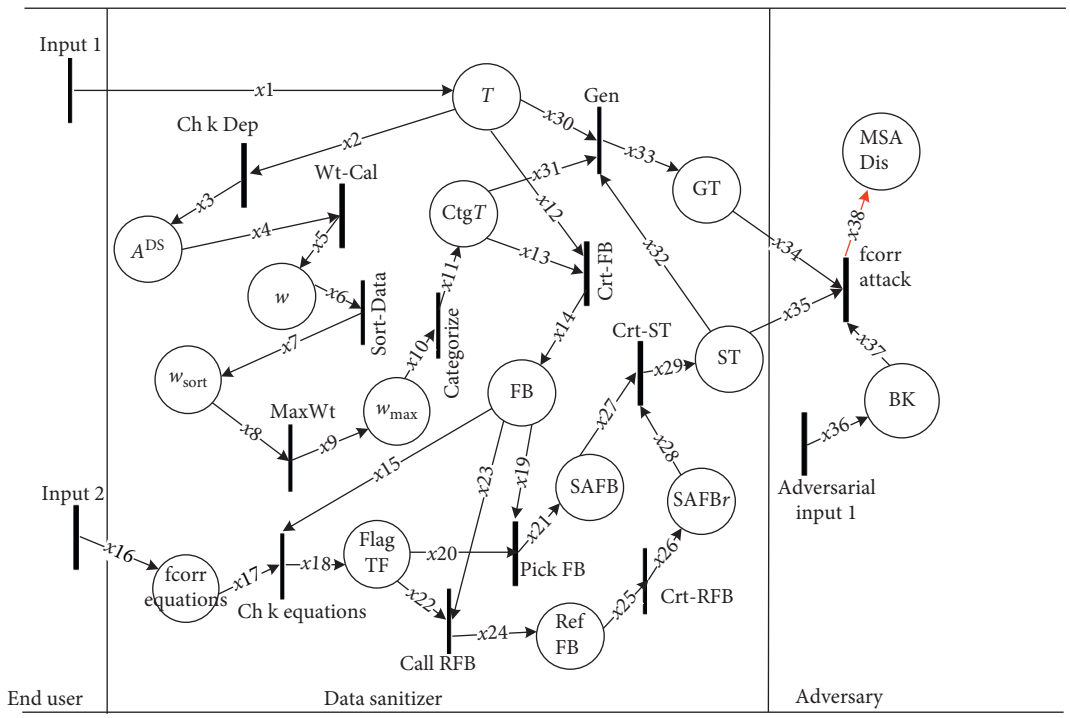


Figure 2: HLPN for the (c, k)-anonymization algorithm.

Table 12: Types used in HLPN for (c, k)-anonymization.

Types	Descriptions
T	Place holding integer and string type data
PID	An integer identifying patient id
A^{DS}	A set consists of dependent sensitive attributes
W	An integer defines final calculated weights of A^{DS}
w_{sort}	An integer set containing sorted weight of SA in descending
w_{max}	Maximum weight after adding external factor χ
C	Category id for MSA
BID	Bucket id used to connect GT and SBT
QI	An integer and string type quasi-identifiers for i^{th} end user
MSF	Multiple sensitive fingerprint string values for i^{th} end user
MSF_I	Initial MSF string values in a bucket for i^{th} end user
MSF_N	Not correlated MSF string values in a bucket for i^{th} end user
MSF_C	Correlated MSF string values in a bucket for i^{th} end user
MSF_R	Refined MSF string values in a bucket for i^{th} end user

Table 13: Mapping of data types on places.

Places	Mapping
φ (T)	$\mathbb{P}$ $(QI \times MSF \times PID)$
φ (A^{DS})	$\mathbb{P}$ (A^{DS})
φ (w)	$\mathbb{P}$ (w)
$\varphi(w_{sort})$	$\mathbb{P}(w_{sort})$
$\varphi(w_{max})$	$\mathbb{P}(w_{max})$
$\varphi(CtgT)$	$\mathbb{P}$ $(C \times MSF)$
$\varphi(FB)$	$\mathbb{P}$ $MSF_I \times BID)$
$\varphi(FlagTF)$	$\mathbb{P}(condition)$
$\varphi(SAFB)$	$\mathbb{P}$ $(MSF_N \times BID)$
$\varphi(RefFB)$	$\mathbb{P}$ $(MSF_C \times BID)$
$\varphi(SAFBr)$	$\mathbb{P}$ $(MSF_R \times BID)$
$\varphi(GT)$	$\mathbb{P}$ $(QI \times BID)$
$\varphi(ST)$	$\mathbb{P}$ $(MSF \times BID)$
$\varphi(BK)$	$\mathbb{P}$ $(QI \times MSF_C \times PID)$
$\varphi(MSA\ Dis)$	$\mathbb{P}$ $(QI \times MSF \times PID)$

6. Experimental Analysis

In this section, we evaluate our proposed anonymization algorithm (c, k)-anonymization to compare the performance with (p, k)-Angelization. Both the algorithms are implemented in JAVA language on a machine having Windows 10 operating system with 4 GB RAM and Intel Core i5 2.39 GHz processor. The values plotted for the (p, k)-angelization algorithm have been obtained from the algorithm's program code executed on the same machine. The dataset obtained from the Cleveland Clinic Foundation Heart disease is available at https://archive.ics.uci.edu/ml/ datasets/Heart-+Disease. This dataset consists of 75 attributes. The experiments are performed on two QI attributes: age and gender and 12 sensitive attributes. These attributes are enough to evaluate the performance of the proposed algorithm. Table 14 shows the QIs and SAs used in the experiment with attribute description and number of distinct values in each domain.

Different general purpose posteriori measures for utility and privacy loss [9, 15, 18, 22] are available for generalization-based algorithms. In these approaches, the publisher does not know about the recipient analysing method. The

Table 14: Attributes used in the experiments.

S. no	Attributes		Description	No. of distinct values
1	QI	Age	Age in years (range values)	48
2		Gender	Male or female	2
3	MSA	Cp	Chest pain type (typ, atyp, non, asymp)	4
4		Trestbps	Resting blood pressure	49
5		Chol	Serum cholesterol	148
6		Smoke	Yes or no	2
7		Cigs	Cigarettes per day	24
8		Fbs	Fasting blood sugar (true or false)	2
9		Famhist	Family history of coronary artery disease	2
10		Restecg	Resting electrocardiographic results	3
11		Thalach	Maximum heart rate achieved	90
12		Thalrest	Resting heart rate	61
13		Cmo	Month of cardiac cath	12
14		Cyr	Year of cardiac cath	4

publisher only evaluates the similarity between the original and anonymized data. The lower values in utility loss and privacy loss reflect the effectiveness of the developed algorithm. We measure the utility loss using the normalized certainty penalty (NCP) [22], query accuracy [22], and privacy loss by calculating the vulnerable records. Also, both algorithms execution time are analysed and a discussion is provided at the end.

6.1. Utility Loss. For utility loss measure, we analyse our algorithm using the following techniques.

6.1.1. Normalized Certainty Penalty. NCP measures accuracy loss in the anonymized release. Let $T = \{Q_1, Q_1, \ldots, Q_q\}$ are QI. The information loss for a single QI attribute is $\mathrm{NCP}_{QI_i}(t) = (z_i - y)_i / |QI_i|$, where $y_i \le x_i \le z_i$, x_i is the actual QI value from T, and $|\mathrm{QI}_i|$ is the domain range on QI_i, i.e., max $\{t.\mathrm{QI}_i\}$–min $\{t.\mathrm{QI}_i\}$. The total weighted certainty penalty for the whole table is the sum of all attributes in a tuple, and then NCP obtained from all tuples is added as shown in the following equation:

$$\mathrm{NCP}(T^*) = \sum_{t \in T^*} \sum_{i=1}^{q} w_i \cdot \mathrm{NCP}_{Q_i}(t), \tag{6}$$

where $\mathrm{NCP}(t) = \sum_{i=1}^{q} w_i \cdot \mathrm{NCP}_{Q_i}(t)$ represents penalty for a tuple, w_i are weights associated to attributes, and T^* is the final anonymized release. Figure 3 shows the percentage value for NCP for varying values of k-anonymity, keeping fixed number of attributes (e.g., MSA = 6) for analysing (c, k)-anonymization and (p, k)-anonymization algorithms. The penalty, i.e., NCP% value for (p, k)-angelization continuously increases while increasing the k-anonymity because the k groups have the one-to-one correspondence with FBs in ST. This means high diversity in FBs may further effect the utility in GT. So, the splitting of table T (Table 1) into GT (Table 2) and ST (Table 3) has no benefit at all. The attributes in each table are still dependent on each other. While the proposed (c, k)-anonymization has one-to-many correspondence between ST and GT where the GB creates closer k-anonymous groups for the same

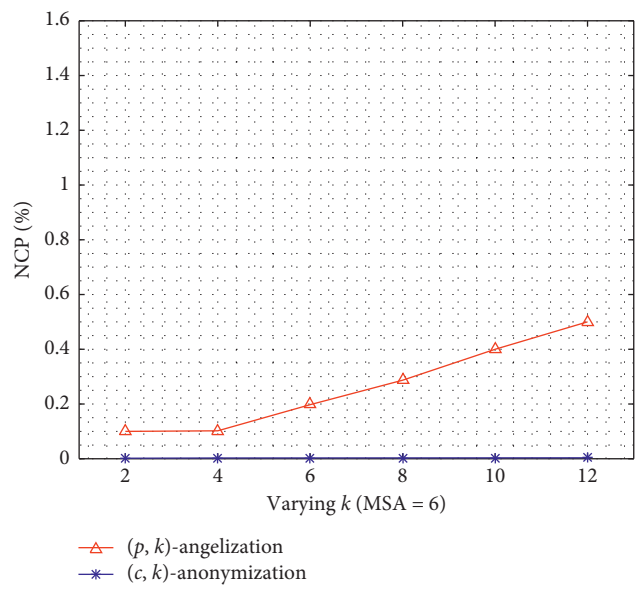


Figure 3: Normalized certainty penalty.

k size class. The comparatively less generalized QIs have lower utility loss and have almost zero loss.

6.1.2. Query Accuracy or Precision of Data Analysis Queries. The purpose of anonymized data is to extract useful statistics and contribute in decision-making. Such utility of the anonymized release is measured through aggregate query answering. Consider the following type of aggregate query:

$$\begin{aligned} &\text{Select COUNT}(*) \text{ from } T^* \text{ where } A_1^{QI} \in \text{Domain} \\ &\left(A_1^{QI}\right) \text{ AND } \ldots \text{ AND } A_q^{QI} \in \text{Domain}\left(A_q^{QI}\right). \end{aligned} \tag{7}$$

Published table T^* has q as $A^{QI}s$, i.e., $A_i^{QI}, A_2^{QI}, \ldots, A_q^{QI}$. The domain (A_i^{QI}) size depends on query selectivity (θ) which indicates the expected number of record selection. The selectivity $\theta = |r_Q|/|T|$, where $|T|$ is the total number of records in the dataset and $|r_Q|$ indicates the number of records obtained from query (Q). To measure the precision

loss, the query error in equation (8) analyses the error between the COUNT queries executed on the published and original datasets.

$$\text{Query error} = \frac{|\text{count (generalized)} - \text{count (original)}|}{\text{count (original)}}. \tag{8}$$

Calculating the query error is a common matrix to measure the utility of the anonymized release. We compare the utility of the (p, k)-angelization and (c, k)-anonymization by generating 1000 random queries and averaging their query errors. Figure 4 depicts the query error for (p, k)-angelization and (c, k)-anonymization comparatively. In Figure 4(a), the comparative increase in the query error for varying k size is because of the new record insertions that increase the generalization range. While the proposed (c, k)-anonymization shows a comparative low error rate because of comparative decrease in QI generalization. The selectivity, i.e., θ graph in Figure 4(b), depicts that for high selectivity, more number of records are selected. So, the difference to calculate the query error via equation (8) will automatically decrease.

6.2. Privacy Loss. Identification of individual record respondents from an anonymized release is directly proportional to the privacy loss. Therefore, the privacy loss is measured with respect to the number of single record identifications that are obtained from the intersection of $\mathscr{L}$ FBs, considered as vulnerable records. We analyse the privacy loss with varying value of k and MSA. Figure 5 shows the results obtained from the experiments for the (p, k)-angelization and (c, k)-anonymization algorithms. In Figure 5(a), for (p, k)-angelization, the number of vulnerable records increases with increase in k size because there are more number of records that have single SV obtained from the intersection among $\mathscr{L}$ FBs. Similarly, in Figure 5(b), with increasing the MSAs, the chances of getting a single SV against each SA increases and hence the number of vulnerable records increases for (p, k)-angelization. While in both cases, i.e., Figures 5(a) and 5(b), the proposed (c, k)-anonymization has no such single SV from the intersection in $\mathscr{L}$ FBs because of satisfying equations (4) and (5). Therefore, there exists no vulnerable records in the proposed (c, k)-anonymization algorithm.

6.3. Execution Time Analysis. The execution time for the proposed (c, k)-anonymization is high as compared to the (p, k)-angelization. This is because of the privacy requirements to satisfy equations (4) and (5). Although the categorization and record selection are almost the same in both algorithms, however, to satisfy equations (4) and (5) is time consuming and may need further time to merge records between $\mathscr{L}$ FBs. Therefore, at the cost of improved privacy, the execution time increases. In Figure 6, with the increase in number of MSAs, the proposed (c, k)-anonymization algorithm execution time comparatively increases because of satisfying privacy equations for all the available attributes; however, the algorithm execution time is still small and acceptable.

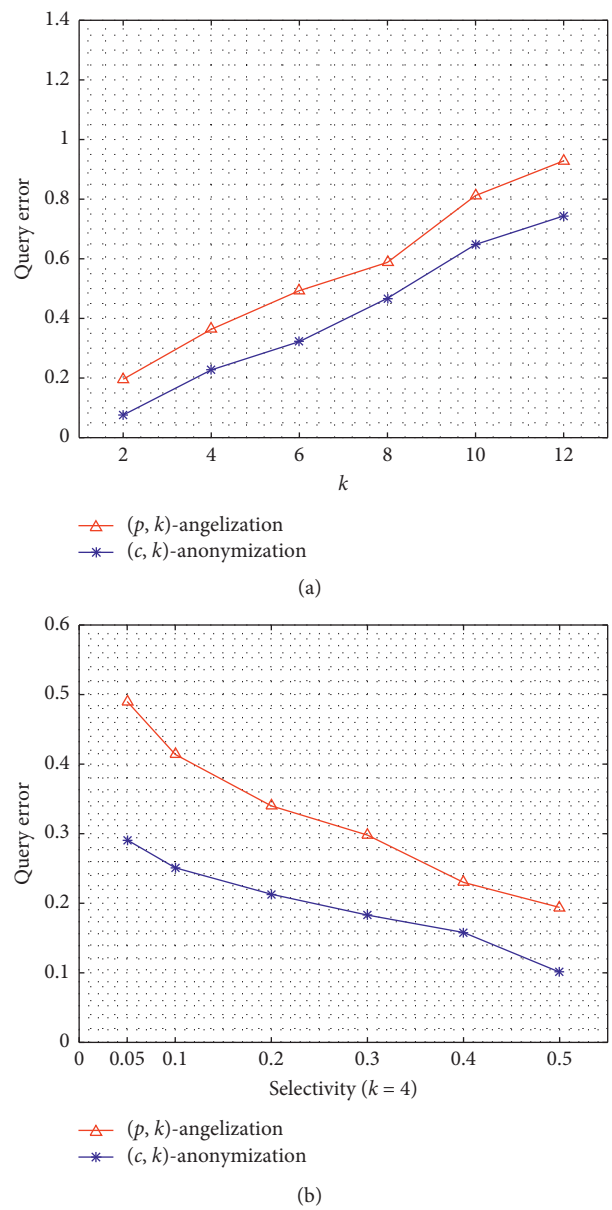


Figure 4: (a) Query error w.r.t varying k size; (b) query error w.r.t varying selectivity.

6.4. Discussion. The proposed algorithm has been analysed through utility loss and privacy loss metrics. The main goal of the algorithm is to prevent attribute disclosures using some background knowledge. The algorithm achieves this goal. The main priority of the algorithm is to prevent from the fcorr attack. For this purpose, the algorithm creates a classification strategy in the form of Ctg$T$ to have c-diverse records in each FB and to prevent attribute disclosures. In the defensive position, the algorithm focuses on reducing the $\mathscr{L}$ between FBs using $\mathscr{c}_f$ in order to reduce the number of possible attacks. In the next phase, we enforce each FB for

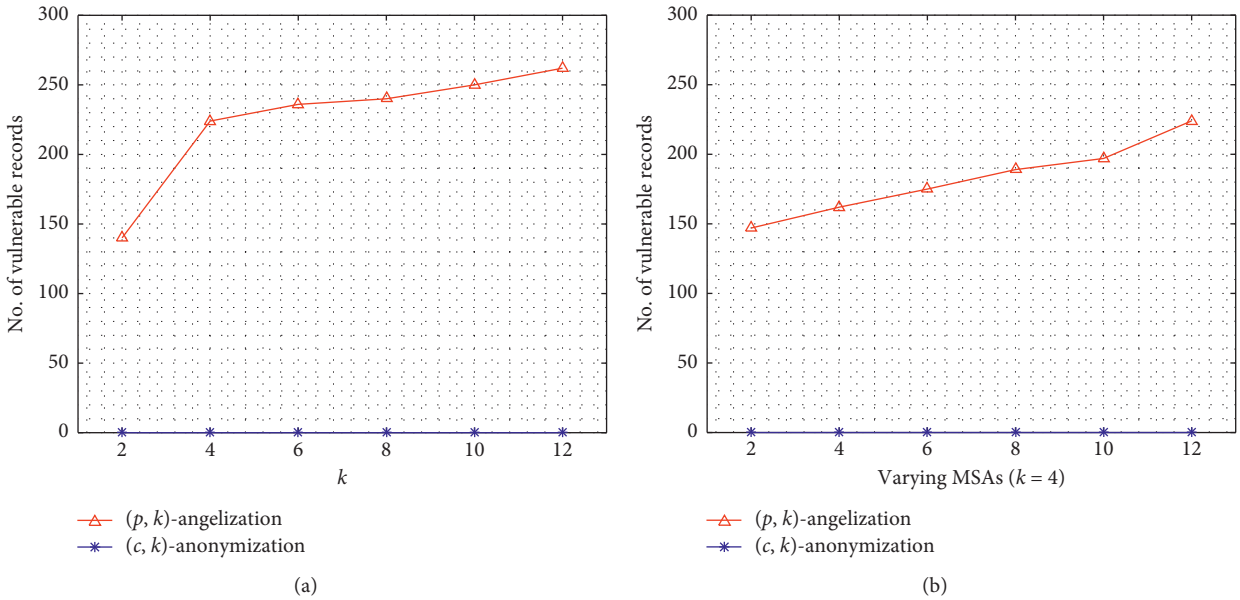


Figure 5: Privacy loss (a) with varying k size and (b) with varying MSA.

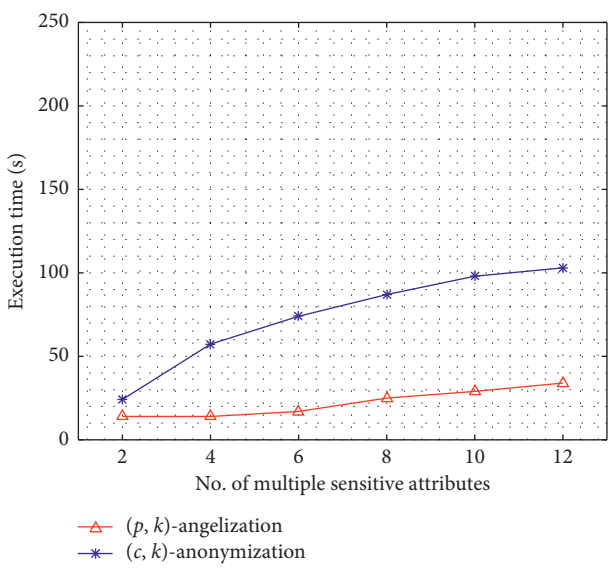


Figure 6: Algorithm execution time.

the fulfilment of equation (4) and in the worst case equation (5) which completely avoids the risks of fcorr attack. Partitioning of attributes based on weights and enforcement for conditions reduces the privacy loss, and creating closest k-anonymous QI class also results in low information loss. The evaluation parameters for privacy and utility proved that there is a minimum disclosure risk and information loss for the proposed (c, k)-anonymization algorithm.

7. Conclusion

In this paper, privacy for MSAs of healthcare data has been addressed. Irrespective of adopting any predefined methodology for our proposed approach similar to (p, k)-angelization, we proposed a novel algorithm, (c, k)-anonymization for privacy and utility improvement in MSAs. The proposed algorithm consists of two major steps. First, it categorizes the MSAs based on calculated weights. Second, FBs are created and refined iteratively to implement privacy. To categorize the MSAs, the weight calculation is done as in [22]. The privacy risk is reduced by implementing one-to-many linking which disassociate the buckets in GT and ST. The one-to-many linking not only reduces the probability of adversary's attacks but also improves the utility in GT. The major step in privacy implementation is to reduce the correlation between $\mathscr{L}$ FBs by satisfying equations (4) and (5). Such measures prevent the main cause of privacy breach, i.e., correlation between SAs. It makes the adversary unable to disclose the privacy of an intended individual. The experiment's results show that both with respect to utility and privacy the proposed (c, k)-anonymization algorithm performs well as compared to the (p, k)-Angelization algorithm.

Preserving the same privacy, this work can be extended to 1 : M microdata [28]. Another challenging future work can be combining 1 : M with MSA in a dynamic data publishing [6, 16] scenario. To the best of our knowledge, for the later scenario, there exists no available literature.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (61932005, 61601051, and 61941105), Beijing Municipal Science and Technology Project (Z181100003218005), and 111 Project of China B16006.

References

[1] 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.

[2] F. Song, T. Ma, Y. Tian, and M. Al-Rodhaan, "A new method of privacy protection: random *k*-anonymous," *IEEE Access*, vol. 7, pp. 75434–75445, 2019.

[3] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "*l*-diversity: privacy beyond *k*-anonymity," *ACM Transactions on Knowledge Discovery from Data*, vol. 1, no. 1, pp. 1–52, 2007.

[4] N. Li, T. Li, and S. Venkatasubramanian, "*t*-closeness: privacy beyond *k*-anonymity and *l*-diversity," in *Proceedings of the 2007 IEEE 23rd International Conference on Data Engineering*, pp. 106–115, Istanbul, Turkey, April 2007.

[5] J. Wang, K. Du, X. Luo, and X. Li, "Two privacy-preserving approaches for data publishing with identity reservation," *Knowledge and Information Systems*, vol. 60, no. 2, pp. 1039–1080, 2019.

[6] X. Xiao and Y. Tao, "*m*-invariance: towards privacy preserving re-publication of dynamic datasets," in *Proceedings of the ACM SIGMOD International Conference on Management of Data*, pp. 689–700, Beijing, China, 2007.

[7] Q. Liu, H. Shen, and Y. Sang, "Privacy-preserving data publishing for multiple numerical sensitive attributes," *Tsinghua Science and Technology*, vol. 20, no. 3, pp. 246–254, 2015.

[8] L. Zhang, J. Xuan, R. Si, and R. Wang, "An improved algorithm of individuation *k*-anonymity for multiple sensitive attributes," *Wireless Personal Communications*, vol. 95, no. 3, pp. 2003–2020, 2017.

[9] R. Wang, Y. Zhu, T.-S. Chen, and C.-C. Chang, "Privacy-preserving algorithms for multiple sensitive attributes satisfying *t*-closeness," *Journal of Computer Science and Technology*, vol. 33, no. 6, pp. 1231–1242, 2018.

[10] L. E. E. Yong Ju and L. E. E. Kyung Ho, "Re-identification of medical records by optimum quasi-identifiers," in *Proceedings of the 19th International Conference on Advanced Communication Technology (ICACT)*, pp. 428–435, Bongpyeong, South Korea, 2017.

[11] N. Maheshwarkar, K. Pathak, and N. S. Choudhari, "*k*-anonymity model for multiple sensitive attributes," *International Journal of Computer Applications—IJCA*, vol. 10, pp. 51–56, 2012.

[12] T. S. Gal, Z. Chen, and A. Gangopadhyay, "A privacy protection model for patient data with multiple sensitive attributes," *International Journal of Information Security and Privacy*, vol. 2, no. 3, 2008.

[13] M. Guo, Z. Liu, and H.-B. Wang, "Personalized privacy preserving approaches for multiple sensitive attributes in data publishing," *DEStech Transactions on Engineering and Technology Research*, no. ssme-ist, 2016.

[14] P. Usha, R. Shriram, and S. Sathishkumar, "Multiple sensitive attributes based privacy preserving data mining using *k*-anonymity," *International Journal of Scientific and Engineering Research*, vol. 5, no. 4, pp. 122–126, 2014.

[15] F. Amiri, N. Yazdani, A. Shakery, and A. H. Chinaei, "Hierarchical anonymization algorithms against background knowledge attack in data releasing," *Knowledge-Based Systems*, vol. 101, pp. 71–89, 2016.

[16] S. A. Onashoga, B. A. Bamiro, A. T. Akinwale, and J. A. Oguntuase, "A dynamic privacy preserving data publishing technique for multi sensitive attributes," *Information Security Journal: A Global Perspective*, vol. 26, no. 3, pp. 121–135, 2017.

[17] K. Ashoka and B. Poornima, "Enhanced utility in preserving privacy for multiple heterogeneous sensitive attributes using correlation and personal sensitivity flags," in *Proceedings of the 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 970–976, Karnataka, India, September 2017.

[18] N. V. S. Lakshmipathi Raju, M. N. Seetaramanath, and P. Srinivasa Rao, "A novel dynamic KCi-slice publishing prototype for retaining privacy and utility of multiple sensitive attributes," *International Journal of Information Technology and Computer Science*, vol. 11, no. 4, pp. 18–32, 2019.

[19] Y. Xu, T. Ma, M. Tang, and W. Tian, "A survey of privacy preserving data publishing using generalization and suppression," *Applied Mathematics & Information Sciences*, vol. 8, no. 3, pp. 1103–1116, 2014.

[20] B. C. M. Fung, K. Wang, R. Chen, and P. S. Yu, "Privacy-preserving data publishing: a survey of recent developments," *ACM Computing Surveys (CSUR)*, vol. 42, no. 4, pp. 1–53, 2010.

[21] A. Majeed, F. Ullah, and S. Lee, "Vulnerability-and diversity-aware anonymization of personally identifiable information for improving user privacy and utility of publishing data," *Sensors*, vol. 17, no. 5, pp. 1–23, 2017.

[22] A. Anjum, N. Ahmad, S. U. R. Malik, S. Zubair, and B. Shahzad, "An efficient approach for publishing microdata for multiple sensitive attributes," *The Journal of Supercomputing*, vol. 74, no. 10, pp. 5127–5155, 2018.

[23] Y. Tao, H. Chen, X. Xiao, S. Zhou, and D. Zhang, "Angel: enhancing the utility of generalization for privacy preserving publication," *IEEE Transactions on Knowledge and Data Engineering*, vol. 21, no. 7, pp. 1073–1087, 2009.

[24] J. Han, F. Luo, J. Lu, and H. Peng, "SLOMS: a privacy preserving data publishing method for multiple sensitive attributes microdata," *Journal of Software*, vol. 8, no. 12, pp. 3096–3104, 2013.

[25] V. S. Susan and T. Christopher, "Anatomisation with slicing: a new privacy preservation approach for multiple sensitive attributes," *SpringerPlus*, vol. 5, no. 1, pp. 964–984, 2016.

[26] X. Xiao and Y. Tao, "Anatomy: simple and effective privacy preservation," in *Proceedings of the 32nd International Conference on Very Large Data Bases VLDB Endowment*, pp. 139–150, Seoul, South Korea, September 2006.

[27] J. Domingo-Ferrer and J. Soria-Comas, "From *t*-closeness to differential privacy and vice versa in data anonymization," *Knowledge-Based Systems*, vol. 74, pp. 151–158, 2015.

[28] Q. Gonga, J. Luoa, M. Yang, W. Ni, and X.-B. Li, "Anonymizing 1 : M microdata with high utility," *Knowledge-Based Systems*, vol. 115, pp. 15–26, 2016.

[29] Y. Shi, Z. Zhang, H. C. Chao, and B. Shen, "Data privacy protection based on micro aggregation with dynamic sensitive attribute updating," *Sensors (Basel)*, vol. 18, no. 7, p. 2307, 2018.

[30] J. Domingo-Ferrer and J. Soria-Comas, "Steered microaggregation: a unified primitive for anonymization of data sets and data streams," in *Proceedings of the 2017 IEEE*

International Conference on Data Mining Workshops, pp. 995–1002, New Orleans, LA, USA, November 2017.

[31] Z. Li and X. Ye, "Privacy protection on multiple sensitive attributes," in *Proceedings of the International Conference on Information and Communications Security*, pp. 141–152, Zhengzhou, China, December 2007.

[32] T. Yi and M. Shi, "Privacy protection method for multiple sensitive attributes based on strong rule," *Mathematical Problems in Engineering*, vol. 2015, Article ID 464731, 14 pages, 2015.

[33] J. Liu, J. Luo, and J. Z. Huang, "Rating: privacy preservation for multiple attributes with different sensitivity requirements," in *Proceedings of the 2011 IEEE 11th International Conference on Data Mining Workshops (ICDMW) IEEE*, pp. 666–673, Vancouver, Canada, December 2011.

[34] F. Luo, J. Han, J. Lu, and H. Peng, "ANGELMS: a privacy preserving data publishing framework for microdata with multiple sensitive attributes," in *Proceedings of the International Conference on Information Science and Technology (ICIST)*, pp. 393–398, IEEE, Yangzhou, China, 2013.

[35] X.-C. Yang, Y.-Z. Wang, B. Wang, and G. Yu, "Privacy preserving approaches for multiple sensitive attributes in data publishing," *Chinese Journal of Computers*, vol. 31, no. 4, pp. 574–587, 2008.

[36] Y. Jing and W. Bo, "Personalized *l*-diversity algorithm for multiple sensitive attributes based on minimum selected degree first," *Journal of Computer Research and Development (China)*, vol. 49, no. 12, pp. 2603–2610, 2012.

[37] Y. Ye, Y. Liu, and D. Lv, "Decomposition: privacy preservation for multiple sensitive attributes," in *Database Systems for Advanced Applications, Lecture Notes in Computer Science*, vol. 5463, pp. 486–490, Springer, Berlin, Germany, 2009.

[38] D. Das and D. K. Bhattacharyya, "Decomposition$^+$: improving *l*-diversity for multiple sensitive attributes," in *Proceedings of the International Conference on Computer Science and Information Technology*, pp. 403–412, Bangalore, India, 2012.

[39] T. M. Truta and B. Vinay, "Privacy protection: p-sensitive k-anonymity property," in *Proceedings 22nd International Conference on Data Engineering Workshops*, p. 94, IEEE, Atlanta, Georgia, April 2006.

[40] C. N. Sowmyarani and G. N. Srinivasan, "A robust privacy preserving model for data publishing," in *Proceedings of the International Conference on Computer Communication and Informatics (ICCCI)*, pp. 1–6, IEEE, Coimbatore, India, 2015.

[41] A. Abdalaal, M. E. Nergiz, and Y. Saygin, "Privacy-preserving publishing of opinion polls," *Computers & Security*, vol. 37, pp. 143–154, 2013.

[42] B. Al Bouna, C. Clifton, and Q. Malluhi, "Efficient sanitization of unsafe data correlations," in *Proceedings of the Workshops of the EDBT/ICDT 2015 Joint Conference*, pp. 278–285, Brussels, Belgium, March 2015.

[43] H. Wang and R. Liu, "Hiding outliers into crowd: privacy-preserving data publishing with outliers," *Data & Knowledge Engineering*, vol. 100, pp. 94–115, 2015.

[44] S. U. R. Malik, S. U. Khan, and S. K. Srinivasan, "Modeling and analysis of state-of-the-art VM-based cloud management platforms," *IEEE Transactions on Cloud Computing*, vol. 1, no. 1, p. 1, 2013.

Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 7845107, 11 pages
https://doi.org/10.1155/2020/7845107

Research Article

Secure Green-Oriented Multiuser Scheduling for Wireless-Powered Internet of Things

Xiaohui Shang,[1,2] Hao Yin,[2] Aijun Liu,[1] Mu Li,[1,2] Yida Wang,[1] and Yong Wang[1]

[1]*College of Communications Engineering, Army Engineering University of PLA, Nanjing 210007, China*
[2]*Institute of Systems Engineering, AMS, Beijing 100039, China*

Correspondence should be addressed to Xiaohui Shang; shangxiaohui1214@126.com

Received 20 June 2019; Revised 7 August 2019; Accepted 30 August 2019; Published 7 January 2020

Guest Editor: Hasan Ali Khattak

In this paper, we consider the secure green-oriented multiuser scheduling for the wireless-powered Internet of Things (IoT) scenario, in which multiple source sensors communicate with a controller assisted by an intermediate sensor with the existence of a passive tapping device. Due to the limited energy, all sensors must acquire energy from external power beacons (PBs). Specifically, for the security improvement, we introduce two multiuser scheduling schemes possessing the optimal PB chosen by the relay, i.e., the best source sensor is scheduled in a random way (BSR), while the best source sensor is decided by the best PB (BSBP). Furthermore, for every scheme, we derive the analytical expressions for the secrecy outage probability (SOP) and investigate the secure energy efficiency (SEE) optimization problem with constricted transmission power in PBs. Simulation results reveal that the BSBP scheme provides better secrecy performance, and elevating the PBs quantity or reducing both the ratio of distance from PBs to source users and the total communication distance to some extent is helpful for improving SEE. In addition, the time-switching factor shows an important effect upon secrecy performance of the considered system.

1. Introduction

As the key architecture of the fifth generation (5G) mobile communication system, the Internet of Things (IoT) has attracted more and more attention [1]. The primary driving thought for the prospective IoT has relation with smart sensors, and wireless sensor networks (WSNs) have been observed as key enablers of IoT applications recently, where multiple sensor nodes are caused by instant or periodic data acquisition in multiple environments [2]. However, among various types of IoT sensors, most of the objects are resource-constrained, battery-powered, and characterized by both of the low energy and poor computation capacity, resulting in the one of the biggest barrier impeding generalization of IoT in the future which is the limitation of energy [3]. Meanwhile, the rapid development of IoT will give rise to the massive deployment of sensor nodes and a vast amount of information exchange, making it unfeasible to flexibly recharge and control the power-constricted devices. Due to the rising power costs, green-oriented methods have inevitably become the dominating design consideration in the IoT system. Fortunately, far-field wireless energy transfer (WET), which enables wireless devices to acquire energy from the broadcast signals for their operation and information exchange, has considered as an appealing method to provide consistent and stable energy to power-constrained users of IoT, particularly when traditional energy harvesting (EH) techniques from reproducible energy sources are inapplicable [4]. Such a new communication type is known as wireless-powered communication (WPC), where the wireless users of IoT are powered through surrounding electromagnetic signals, which is likely to be dedicated wireless transmitters utilized to charge wireless terminals. As such, it can completely eliminate the burden of battery renewal and/or recharging, avoid the interruption caused by the running out of power, and provide networks with theoretically perpetual lifespans [5].

Generally, a basic hurdle of wireless transmission upon the basis of WPC rest with the fast attenuation of radio frequency (RF) signals with distance changing. Moreover,

energy amount acquired at wireless-powered devices is fairly restricted, which limits the coverage severely and has become a bottleneck for the widespread application of WPC. Consequently, the design of energy-efficient transmission is of great significance for transforming the green concept into future wireless-powered IoT. Although the harvested energy from RF signals appears to be inefficient and the WPC-based wireless communication seems to be not widely available at the current stage, practical applications for power-constrained devices of IoT have already been investigated, and more feasible applications will be implemented in the near future [6–8]. Until now, a lot of research efforts have also been devoted to explore the advantages of WPC in most applications of IoT since it could be easily combined with wireless terminals [9–13]. Specifically, typical wireless-powered communication networks (WPCN) were investigated in [9], where introduction of a dynamic time division multiple access (TDMA) protocol was performed for a multiuser WPCN, and the best time allocation for the downlink WPC and the uplink wireless information transmission (WIT) had been analyzed. Until now, the studies on WPCN have been extended to various communication systems. In particular, a joint wireless power transfer (WPT) and relay selection method were proposed for WPCN in [10], where the source and relays utilize the time-switching-based RF-EH method to acquire energy from a power beacon (PB) with multiple antennas. Differently, secrecy performance discussion of EH wireless sensor networks was examined in [11], where the authors proposed an optimization method, in which a wireless-powered friendly jammer was utilized for improving the secrecy performance of the considered model. Furthermore, the authors in [12] analyzed the secrecy performance of the EH sensor system and proposed a best-relay-and-best-jammer protocol for enhancing the secrecy of a system with the source user and multiple sensor relays harvesting energy from diverse PBs. Recently, inspired by abovementioned works, a secure energy-efficient transmission design for wireless-powered IoT possessing various PBs was investigated in [13], where the authors introduce different relay selection schemes possessing the optimal PB under the selection of the single source and solve the optimization problem of secure energy efficiency (SEE). It is worth mentioning that above works mostly focused on the secrecy performance improvement contributed by relay selection, while ignored the practical scenario with multiusers, which can be considered as the typical application of IoT.

1.1. Related Works. Remarkably, in an effort to reduce the complexity and the costs of resource-constricted wireless-powered IoT, the multiuser scheduling has drawn wide attention due to the significant potential performance improvement [14–19]. Particularly, the authors in [14] explore the largest energy efficiency for multiuser WPCN by joint power control and time allocation while taking account of the initial battery energy level of all the users. Furthermore, the authors in [15] applied the notion of proportional fair scheduling to WPCN and overcome the doubly near fair problem by an opportunistic scheme. Meanwhile, in a multiuser system, the authors in [16] consider multiuser scheduling criteria taking into account cochannel interference in a multicell environment and propose an adaptive scheduling scheme. Then, in a WPCN-based multi-input multioutput (MU-MIMO) multiuser system, [17] proposes a zero-forcing-based transmission method by a downlink energy beamformer to optimize the related parameters. Afterwards, the authors in [18] concentrate on an MIMO-WPCN, in which a dedicated multiantenna PB transfers RF energy to some starve users, and then these users send required information to the destination. And, last but not the least, [19] focuses on the cumulative transmission framework of multiuser scheduling in full-duplex wireless-powered IoT system and designs a novel throughput-oriented scheduling strategy, which models the dynamic charging and discharging procedures for all the devices in IoT as a finite-state Markov chain.

On the contrary, the broadcast characteristics of wireless transmission make the WPT and WIT more vulnerable to malicious attacks, turning secure transmission into a burdensome task [20]. Typically, the upper layer cryptographic techniques are explored for securing the privacy information against intercepting in traditional wireless transmissions [21]. However, conventional cryptographic technology is limited in wireless-powered IoT because of the requirements of high hardware complicacy and massive energy [22]. Furthermore, an eavesdropper (Eve) possessing unlimited computing capacity is likely to make such technology compromised [23]. Fortunately, physical layer security (PLS), as a promising approach to make sure the safety of wireless communication, has been a high-effectiveness supplement to current solutions. As far as wireless PLS is concerned, the fundamental thought is to utilize the features of wireless channels for transmitting information in a reliable manner from the source to the intended receiver and to make sure the privacy of the information, to put in different way, not to be intercepted or eavesdropped [24]. Currently, PLS has been broadly deployed for ensuring security of future wireless networks [25, 26] because it can provide the security of new network architectures such as the IoT. In recent years, some literatures have explored secure communications in multiuser-scheduling-aided WPCN [27, 28]. Specifically, [27] investigates the secrecy performance of dual-hop multiuser relay system by exploiting the maximal ratio transmission (MRT) scheme and proposes a threshold-based multiuser scheduling method. On the contrary, the authors in [28] consider a multiantenna wireless network, in which the base station and the users have been given with multiple antennas. However, it is worth noting that few works have considered the SEE in wireless-powered IoT scenario.

1.2. Paper Contributions and Organization. Enlightened by the aforementioned observations, this paper focuses on the secrecy performance analysis of a typical wireless-powered IoT, in which multiple source sensors that perform monitoring or operating tasks in a localized group and an

intermediate node performs as relay are powered by multiple dedicated PBs. Furthermore, we propose two multiuser scheduling schemes and compare their secrecy performance for providing the secure energy-efficient transmissions. The main contributions of our work are listed as follows:

(i) We explore the PLS in the wireless-powered IoT and propose two green-oriented multiuser scheduling schemes, in which the optimal PB is decided by the relay; meanwhile, the best source is scheduled in a random way (BSR) or chosen by the best PB (BSBP), respectively.

(ii) For the two proposed schemes, we obtain the closed-form expressions of the secrecy outage probability (SOP) and solve the SEE optimization problem with constrained transmission power in PB by resorting to the searching method. Compared with the BSR scheme characterized by lower complexity and simpler application, the BSBP scheme can make full use of the power transfer links contributed by diverse PBs and present the better secrecy performance.

(iii) Simulation results demonstrate that increasing the number of PBs is favorable to improve the SEE of the studied scenario. Meanwhile, decreasing both the ratio of distance from PBs to the sources and the total communication distance to some extent is advantageous for SEE. Additionally, the time-switching factor has an important effect upon the secrecy performance of the considered system, which is worth designing and optimizing carefully.

The remaining part of this paper is summarized as follows. Section 2 provides details concerning the system model, the process of WPT, signal analysis, and two proposed multiuser scheduling schemes. Section 3 derives the exact SOP of BSR and BSBP schemes, respectively. Then, in Section 4, the SEE optimization research is given. The simulation results are presented in Section 5. Eventually, conclusions of this paper are drawn in Section 6.

2. System and Channel Model

The system model, the process of WPT, signal analysis, and two multiuser scheduling strategies are presented in this section.

2.1. System Model. Consider a dual-hop multiuser uplink WPCN for the IoT application as illustrated in Figure 1, where multiple source users S_n, $n \in \mathcal{M} = \{1, \ldots, N\}$ communicate with the controller D aided by the decode-and-forward (DF) relay, and are overheard by the passive Eve E. Considering the constricted coverage of sensors, we assume the direct $S_n \longrightarrow D$ link is not available [10]. Meanwhile, owing to the limitation of energy in the IoT system, S_n and R have to gain energy by WPT from a selected P_m, $m \in \mathcal{M} = \{1, \ldots, M\}$ to support data transmission. And, the controller is powered by on-grid power. Apart from that, considering the size and cost limitations, it is assumed that, in each sensor, the destination D and the Eve E are single-antenna and half-duplex devices [12]. It is worth highlighting that the above configurations have numerous practical applications, such as in IoT, where the multiple source sensors upload information via a certain sensor (performs as relay) that is limited to a single antenna due to size limitations and cost.

Furthermore, we consider that each link will be affected by Rayleigh fading. Thus, the power gains of the channel are subject to exponential distribution with parameter λ_{XY}, where $X \in \{P_m, S_n, R\}$ and $Y \in \{S_n, R, E, D\}$. Meanwhile, the additive white Gaussian noise (AWGN) at R and D has zero mean and variance N_0. Compared with the full channel state information (CSI) assumption in [12, 27], where perfect CSI is considered in order to investigate the performance bound, we consider only the statistic CSI can be acquired, which is more practical due to the weak computation ability and small memory of sensors. The specific estimation method for obtaining CSI is shown in [29]. In practice, when the eavesdropper is a member of the network and wants to interpret information that is not passed on to him, the partial CSI of the wiretap link is available.

In order to facilitate mathematical modeling, the channel coefficients of the $P_m \longrightarrow S_n$, $P_m \longrightarrow R$, $S_n \longrightarrow R$, $S_n \longrightarrow E$, $R \longrightarrow E$, and $R \longrightarrow D$ transmission channels are represented by $h_{P_m S_n}$, $h_{P_m R}$, $h_{S_n R}$, $h_{S_n E}$, h_{RE}, and h_{RD}, respectively, which are independent and distributed in an identical manner (i.i.d.) from one block to next. Meanwhile, the distances of the $P_m \longrightarrow S_n$, $P_m \longrightarrow R$, $S_n \longrightarrow R$, $S_n \longrightarrow E$, $R \longrightarrow E$, and $R \longrightarrow D$ transmission links are represented by $d_{P_m S_n}$, $d_{P_m R}$, $d_{S_n R}$, $d_{S_n E}$, d_{RE}, and d_{RD}, respectively. Furthermore, it is assumed that the multiple PBs and multiple source users are close in proximity, i.e., a certain clustering protocol in place. This assumption is generally used in the WPCN [12], which brings about the equivalent mean channel power gains of the channels $P_m \longrightarrow S_n$, $P_m \longrightarrow R$, $S_n \longrightarrow R$, and $S_n \longrightarrow E$, respectively. For convenience, we define $\lambda_{P_m S_n} = \lambda_{PS}$, $\lambda_{P_m R} = \lambda_{PR}$, $\lambda_{S_n R} = \lambda_{SR}$, and $\lambda_{S_n E} = \lambda_{SE}$ for any $m \in \mathcal{M}$ and $n \in \mathcal{N}$.

2.2. Wireless Power Transfer. In the WPT process, the receiver adopts the EH model based on rectangular antenna structure. For the rectangular antenna, the received signal can be converted into a direct current (DC) signal by a rectifier consisting of a passive low-pass filter (LPF) and a Schottky diode [30]. Then, it is considered that the harvested energy by all users at the stage of WPT is entirely used to transmit message in WIT, which is known as the harvest-use (HU) mode as in [31]. This consideration is practical for devices of IoT because they are limited by the size and cost, which leads to the smaller batteries. As for the relaying strategy, the time-switching-based receiver (TSR) protocol is applied in the data transmission, thanks to its high throughput compared with power splitting-based receiver (PSR) protocol [32]. In particular, the duration between two successive data transmission is defined as a transfer time slot T, αT denotes the time of WPT, and $(1-\alpha)T$ represents the duration of WIT as

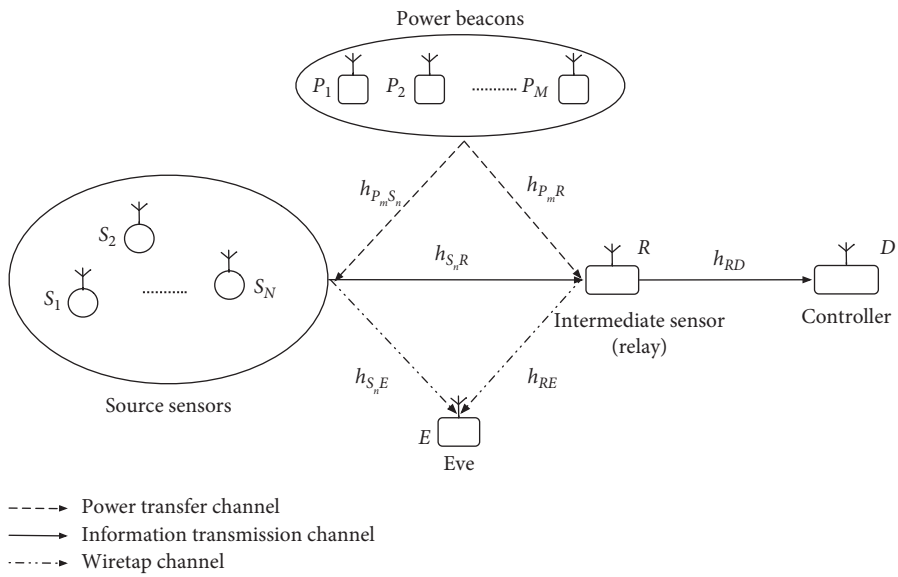


Figure 1: System model.

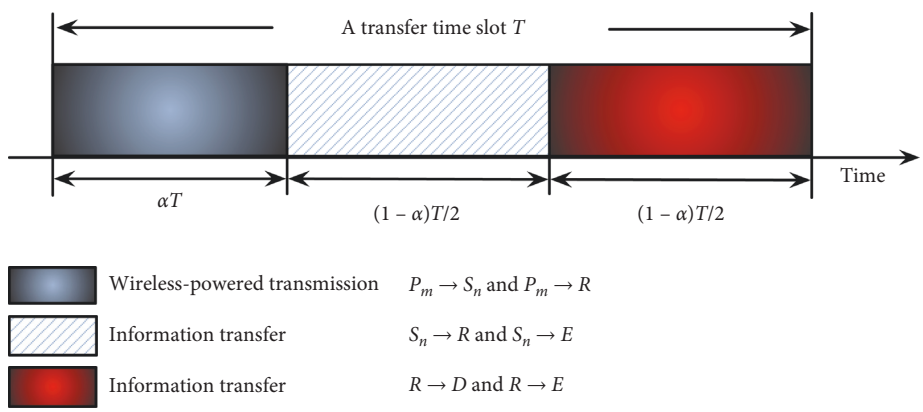


Figure 2: Time-switching relaying strategy. The communication time slot T is applied for WPT and WIT, where αT is applied for harvesting energy from the chosen PB; meanwhile, the rest time $(1-\alpha)T$ is provided to send the data from the source user to the controller D.

illustrated in Figure 2, where $\alpha \in (0,1)$ is the time-switching coefficient. Based on the dual-hop communication, the time window of WIT is divided into two parts, i.e., $(1-\alpha)T/2$ is for $S_n \longrightarrow R$ and the remaining $(1-\alpha)\ T/2$ is provided for $R \longrightarrow D$.

Then, we consider the scenario that a particular PB is activated, while other PBs remain silent in order to reduce the computational complexity and energy consumption, because PB selection is an green-oriented WPT scheme [12]. To be more specific, the PB with the best link for the $P_m \longrightarrow R$ channel is chosen to implement WPT for S_n and R. The index of certain PB can be expressed as

$$m^* = \arg\max_{m \in \mathscr{M}} \left\{ \left| h_{P_m R} \right|^2 \right\}, \tag{1}$$

where $|h_{P_m R}|^2$ is power gain of the link from the selected P_m to R. Furthermore, the harvested energy at S_n and R can be expressed as follows [33]:

$$\begin{aligned} E_{S_n} &= \eta P_B \alpha T \frac{\left| h_{P_{m^*} S_n} \right|^2}{d^{\theta}_{P_{m^*} S_n}} = \eta P_B \alpha T \gamma_{P_{m^*} S_n}, \\ E_R &= \eta P_B \alpha T \frac{\left| h_{P_{m^*} R} \right|^2}{d^{\theta}_{P_{m^*} R}} = \eta P_B \alpha T \gamma_{P_{m^*} R}, \end{aligned} \tag{2}$$

where $10\% < \eta < 80\%$ denotes the EH efficiency factor, which is mainly determined by the EH circuitry and frequencies (e.g., 15 MHz–2.5 GHz) [34]; P_B represents the transmit power of the PBs; θ is the path loss exponent; $|h_{P_{m^*} S_n}|^2$ and $|h_{P_{m^*} R}|^2$ are power gains of the channels from the selected P_m to S_n and R, respectively; $\gamma_{P_{m^*} S_n} = |h_{P_{m^*} S_n}|^2 / d^{\theta}_{P_{m^*} S_n}$ and $\gamma_{P_{m^*} R} = |h_{P_{m^*} R}|^2 / d^{\theta}_{P_{m^*} R}$. Note that we neglect the harvested energy from the noise since the source users and the relay sensor are passive, and their received noise powers are much smaller than the received powers contributed by the PBs [35].

Lemma 1. *If X_k, $k \in \mathcal{K} = \{1, \ldots, K\}$, is the random variable subject to the exponential i.i.d, the probability density function (PDF) and the cumulative distribution function (CDF) of $X = \max_{k\in\mathcal{K}}\{X_k\}$ can be expressed by*

$$f_X(x) = K\lambda_X e^{-\lambda_X x}\left(1 - e^{-\lambda_X x}\right)^{K-1}, \tag{3}$$

$$F_X(x) = \left(1 - e^{-\lambda_X x}\right)^{K}, \tag{4}$$

in which x denotes the independent variable, and $1/\lambda_X$ is the average channel gain.

According to Lemma 1, the PDF of $\gamma_{P_{m^*}R}$ can be derived as

$$f_{\gamma_{P_{m^*}R}}(x) = M\lambda_{PR} e^{-x\lambda_{PR}}\left(1 - e^{-x\lambda_{PR}}\right)^{M-1}, \tag{5}$$

where $1/\lambda_{PR} = E[|h_{P_{m^*}R}|^2]/d^{\theta}_{P_{m^*}R} = E[\gamma_{P_{m^*}R}]$ and $E[\cdot]$ is an expectation operator.

Assuming that the channel fading factors are still unchanged within a transfer time slot, the transmit power of S_n and R are represented as follows [36]:

$$P_{S_n} = \frac{E_{S_n}}{(1-\alpha)T/2} = \frac{2\eta P_B \gamma_{P_{m^*}S_n}\alpha}{1-\alpha}, \tag{6}$$

$$P_R = \frac{E_R}{(1-\alpha)T/2} = \frac{2\eta P_B \gamma_{P_{m^*}R}\alpha}{1-\alpha}. \tag{7}$$

From (6) and (7), it is assumed that the SNRs at R and E in the first hop are denoted as γ_{SR} and γ_{SE}, while the SNRs at D and E in the latter hop are represented as γ_{RD} and γ_{RE}. And the SNRs can be given as

$$\begin{aligned}\gamma_{SR} &= \frac{P_{S_n}\left|h_{S_{n^*}R}\right|^2}{N_0 d^{\theta}_{S_{n^*}R}} \\ &= \frac{2\eta\alpha P_B \gamma_{P_{m^*}S_{n^*}}\left|h_{S_{n^*}R}\right|^2}{N_0(1-\alpha)d^{\theta}_{S_{n^*}R}} \\ &= \gamma_B \xi \gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}R},\end{aligned} \tag{8}$$

where n^* is the index of the chosen source sensor (i.e., scheduled user), $\gamma_B = P_B/N_0$, $\xi = 2\eta\alpha/1-\alpha$, and $\chi_{S_{n^*}R} = |h_{S_{n^*}R}|^2/d^{\theta}_{S_{n^*}R}$. Comparably, γ_{SE}, γ_{RD}, and γ_{RE} are given as

$$\begin{aligned}\gamma_{SE} &= \gamma_E \xi \gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}E}, \\ \gamma_{RD} &= \gamma_B \xi \gamma_{P_{m^*}R}\chi_{RD}, \\ \gamma_{RE} &= \gamma_E \xi \gamma_{P_{m^*}R}\chi_{RE},\end{aligned} \tag{9}$$

where $\gamma_E = P_B/N_E$, N_E denotes the variance of AWGN at E, and $\chi_{S_{n^*}E} = |h_{S_{n^*}E}|^2/d^{\theta}_{S_{n^*}E}$, $\chi_{RD} = |h_{RD}|^2/d^{\theta}_{RD}$, and $\chi_{RE} = |h_{RE}|^2/d^{\theta}_{RE}$.

2.3. Multiuser Scheduling Scheme. Then, when the best PB is determined, we pay attention to the two multiuser scheduling schemes, one is a straightforward scheme with the lower complexity, in which the best source is scheduled randomly from multiple users (BSR), and another is a joint PB and source user selection scheme, in which the best source is chosen by the optimal PB (BSBP).

2.3.1. The BSR Scheme. For reduction of the complexity and costs of considered networks, the source user is scheduled randomly among the candidates in the BSR scheme. It is worth noting that $\gamma_{P_{m^*}S_n}$, χ_{S_nR}, χ_{S_nE}, χ_{RD}, and χ_{RE} are exponentially distributed with parameters $1/\lambda_{PS}$, $1/\lambda_{SR}$, $1/\lambda_{SE}$, $1/\lambda_{RD}$, and $1/\lambda_{RE}$, respectively.

Remark 1. The BSR scheme is applicable for the delay-sensitive and resource-constricted scenarios owing to its lower complexity of computation. However, the BSR scheme fails to have the diversity gain contributed by diverse users, which hinders the secrecy improvement of communication systems.

2.3.2. The BSBP Scheme. Aiming to obtain the diversity gain, the best user is chosen from the perspective of P_{m^*} in this scheme. Specifically, based on the CSI of the $P_{m^*} \longrightarrow S_n$ channels, the index of the scheduled source n^* can be drawn as

$$n^* = \arg\max_{n\in\mathcal{N}}\left(\left|h_{P_{m^*}S_n}\right|^2\right). \tag{10}$$

Therefore, $\chi_{S_{n^*}R}$, $\chi_{S_{n^*}E}$, χ_{RD}, and χ_{RE} are exponentially distributed with parameters $1/\lambda_{SR}$, $1/\lambda_{SE}$, $1/\lambda_{RD}$, and $1/\lambda_{RE}$, respectively, while the PDF of $\gamma_{P_{m^*}S_{n^*}}$ can be drawn according to Lemma 1:

$$f_{\gamma_{P_{m^*}S_{n^*}}}(x) = N\lambda_{PS} e^{-x\lambda_{PS}}\left(1 - e^{-x\lambda_{PS}}\right)^{N-1}, \tag{11}$$

where $1/\lambda_{PS} = E[|h_{P_{m^*}S_{n^*}}|^2]/d^{\theta}_{P_{m^*}S_{n^*}} = E[\gamma_{P_{m^*}S_{n^*}}]$.

Remark 2. According to the (10) and (11), we find that the BSBP scheme is able to obtain the diversity gain contributed by multiple users. Note that this scheme schedules the source user, taking into account the selection of PB adequately. As a result, this scheme can decline the interruption probability of information communication for source sensors in an effective way, which is beneficial to energy-limited IoT applications.

3. Secrecy Outage Probability Analysis

In the system, we consider that S_n and R use the different codebooks to improve secrecy performance. In line with [37], the secrecy capacity of the scenario can be indicated as

$$C_s = \min\left(C_{s1}, C_{s2}\right), \tag{12}$$

where C_{s1} and C_{s2} denote the achievable secrecy capacity of the dual-hop, respectively, which is presented to be

$$C_{s1} = \varepsilon\left[\log_2\left(\frac{1+\gamma_{SR}}{1+\gamma_{SE}}\right)\right]^+,$$
$$C_{s2} = \varepsilon\left[\log_2\left(\frac{1+\gamma_{RD}}{1+\gamma_{RE}}\right)\right]^+, \tag{13}$$

where the reason why the factor $\varepsilon = (1-\alpha)/2$ is that, the communication time of every hop is $(1-\alpha)T/2$ during a transmission slot, $[x]^+ = \max(x, 0)$. Therefore, the secrecy capacity C_s can be updated as

$$C_s = \varepsilon\left[\log_2 \min\left(\frac{1+\gamma_B\xi\gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}R}}{1+\gamma_E\xi\gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}E}}, \frac{1+\gamma_B\xi\gamma_{P_{m^*}R}\chi_{RD}}{1+\gamma_E\xi\gamma_{P_{m^*}R}\chi_{RE}}\right)\right]. \tag{14}$$

Regarding evaluation of the secrecy performance, the SOP is used as the figure of merit, which is regarded as an important indicator of PLS generally. From the perspective of information theory, the transmission incurs secrecy outage if C_s is less than a predetermined secrecy rate threshold R_{th}. Specifically, the SOP of every scheme $P_{\text{sop}}^{(\text{sch})}$ can be shown as

$$P_{\text{sop}}^{(\text{sch})} = \Pr\left(C_s^{(\text{sch})} < R_{\text{th}}\right) = \Pr\left(\gamma_{\text{sec}}^{(\text{sch})} < \beta\right), \tag{15}$$

where sch $\in \{\text{BSR}, \text{BSBP}\}$, $C_s^{(\text{sch})}$ is the secrecy capacity of each scheme, and $\Pr\{\cdot\}$ is the probability.

$$\gamma_{\text{sec}}^{(\text{sch})} = \min\left(\frac{1+\gamma_B\xi\gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}R}}{1+\gamma_E\xi\gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}E}}, \frac{1+\gamma_B\xi\gamma_{P_{m^*}R}\chi_{RD}}{1+\gamma_E\xi\gamma_{P_{m^*}R}\chi_{RE}}\right),$$
$$\beta = 2^{R_{\text{th}}/\varepsilon}. \tag{16}$$

3.1. Derivation for the BSR Scheme. According to the BSR scheme, each source user of the system has the same opportunity to participate in the transmission. Therefore, the exact SOP of the BSR scheme should be formulated as

$$P_{\text{sop}}^{(\text{BSR})} = \frac{1}{N}\sum_{n=1}^{N} P_{sop,S_nR} = 1 - \sum_{m=1}^{M}\binom{M}{m}(-1)^{m+1} \times \frac{4\gamma_B(\beta-1)\lambda_{SE}\lambda_{RE}\sqrt{m\lambda_{PS}\lambda_{PR}\lambda_{SR}\lambda_{RD}}}{\xi(\gamma_B\lambda_{SE}+\beta\gamma_E\lambda_{SR})(\gamma_B\lambda_{RE}+\beta\gamma_E\lambda_{RD})}$$
$$\times K_1\left(2\sqrt{\frac{m\lambda_{PR}\lambda_{RD}(\beta-1)}{\gamma_B\xi}}\right) \times K_1\left(2\sqrt{\frac{\lambda_{SR}\lambda_{PS}(\beta-1)}{\gamma_B\xi}}\right), \tag{17}$$

where P_{sop,S_nR} is the SOP when the source user S_n is decided and $K_1(\cdot)$ represents the modified Bessel function of the second kind [38].

Proof. See Appendix A. □

3.2. Derivation for the BSBP Scheme. Furthermore, according to (16), the closed-form expression of SOP for BSBP scheme is calculated as

$$P_{\text{sop}}^{(\text{BSBP})} = 1 - \sum_{n=1}^{N}\sum_{m=1}^{M}\binom{N}{n}\binom{M}{m}(-1)^{m+n} \times \frac{4\gamma_B(\beta-1)\lambda_{SE}\lambda_{RE}\sqrt{mn\lambda_{PS}\lambda_{PR}\lambda_{SR}\lambda_{RD}}}{\xi(\gamma_B\lambda_{SE}+\beta\gamma_E\lambda_{SR})(\gamma_B\lambda_{RE}+\beta\gamma_E\lambda_{RD})}$$
$$\times K_1\left(2\sqrt{\frac{m\lambda_{PR}\lambda_{RD}(\beta-1)}{\gamma_B\xi}}\right) \times K_1\left(2\sqrt{\frac{n\lambda_{SR}\lambda_{PS}(\beta-1)}{\gamma_B\xi}}\right). \tag{18}$$

Proof. See Appendix B. □

4. Secure Energy Efficiency Maximization

Generally, security improvement comes at the expense of more energy consumption frequently. With regard to energy-limited IoT applications, recklessly pursuing secrecy improvement has a negative effect on the performance of networks. Consequently, it is of great significance to make sure the safe communication in the application of IoT with low energy cost. From the above, the SEE is utilized as the proper metric for evaluation of the secrecy performance [39]. Mathematically, the SEE of above discussed schemes can be given as

$$\eta_s^{(\text{sch})} = \frac{R_{\text{th}}\left(1 - P_{\text{sop}}^{(\text{sch})}\right)}{P_{\text{total}}}, \tag{19}$$

where $\eta_s^{(\text{sch})}$ denotes the SEE of each scheme, $P_{\text{total}} = \kappa P_B + P_c$ represents the total power cost at PBs, κ denotes the power factor, and P_c and P_B stand for the fixed power and transmit power at PBs, respectively. Consider that the

harvested energy by the sensors is fully used for data transmission, while the power consumption of the circuity is ignored.

To find the best transmit power of PBs and the time-switching factor, the SEE maximization problem can be considered as

$$\begin{aligned} \max_{P_B,\alpha} \quad & \eta_s^{(\mathrm{sch})} = \frac{R_{\mathrm{th}}\left(1 - P_{\mathrm{sop}}^{(\mathrm{sch})}\right)}{P_{\mathrm{total}}} \\ \text{s.t.} \quad & 0 < P_B \le P_{\max} \\ & 0 < \alpha < 1, \end{aligned} \tag{20}$$

where $P_{\max}$ denotes the maximum transmit power of PBs. Obviously, the solving process of the exact expressions for P_B and α is rather tedious. Instead, by using the searching method, the optimal P_B and α can be derived on the basis of simulation and numerical analysis. It ought to be highlighted that equation (20) is of more practical importance to the IoT scenarios.

5. Numerical Results and Discussion

In this section, some numerical outcomes are provided for validation of the abovementioned secrecy analysis and for discussion of the joint effect of corresponding parameters upon the secrecy performance of the two proposed multiuser scheduling schemes. Consistent with [40], the simulation is conducted on a linear topology, in which the multiuser sensors in a localized group as well as multiple PBs, relay R, and controller D are arranged horizontally. Unless otherwise stated, we use the following parameters in accordance with [10] throughout this section. In particular, we set $\gamma_E = 20$ dB, the predetermined secrecy rate $R_{\mathrm{th}} = 0.2$ bits/s/Hz, the energy conversion efficiency $\eta = 0.6$, the distances are set to $d_{RD} = d_{SE} = d_{RE} = 3$ m, $d_{BS} = (1/2)d_{SR}$, and $d_{BR} = d_{SR} - d_{BS}$. Moreover, we set the number of the users $N = 3$, the power coefficient $\kappa = 2.63$, the path loss exponent $\theta = 2$, and $P_c = 112.2$ mW. It is obvious that the theoretical results agree exactly with the simulation results, which validates the correctness of our derivations. It is worth noting that all the numerical results in this section come from the simulation environment of MATLAB, which are all true experimental results. Combining the parameter setting in the article with the program code, all the results can be reproduced.

Figure 3 describes the SOP of the proposed multiuser scheduling schemes versus γ_B for different M with $\alpha = 0.5$, $N = 3$. Overall, it can be seen in this figure that the proposed BSBP scheme can achieve better secrecy performance than the BSR scheme in the whole range of γ_B with different M, which indicates that the BSBP scheme is more effective to improve the secrecy performance of the considered system. Furthermore, the number of PBs contributes to the improvement of SOP. This is attributed to the fact that more PBs are able to provide larger diversity gain for improving SOP.

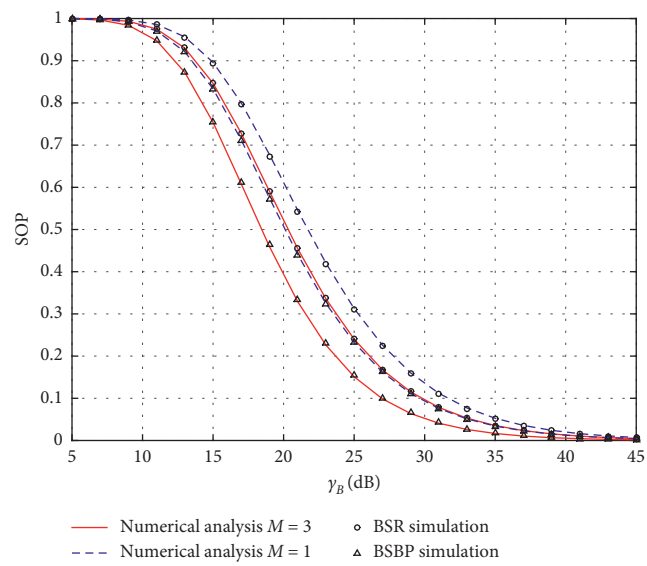


Figure 3: Effect of γ_B and M upon the secrecy outage probability with $\alpha = 0.5$ and $N = 3$.

Figure 4 shows the SEE of the system with BSR/BSBP scheme versus γ_B for different M with $\alpha = 0.5$ and $N = 3$. It is illustrated in this figure that the function of SEE and γ_B is unimodal function. The reason is that increasing γ_B brings about the improvement of SEE in low energy consumption, but it has a negative impact on the SEE in high energy consumption. Furthermore, as expected, the SEE of BSBP scheme outperforms that of the BSR scheme in the whole region, which demonstrates the advantage of BSBP in improving the secrecy performance. In addition, by increasing the number of PBs, the better security can be achieved, which can be understood through the following discussion. Furthermore, Figure 5 depicts the SEE of two multiuser scheduling strategies versus α with $N = 3$ and $\gamma_B = 20$ dB in consideration of various M. Obviously, the function of SEE and α is also unimodal function. This is due to the fact that when α is small, the harvested energy is commonly insufficient for the operation of multiple source sensors and relay sensor, while if α is large excessively, the duration of information communication will be restricted seriously, which will result in high transmission interruption probability. On the contrary, similar to Figure 4, the BSBP scheme always provides the best SEE performance with varying α and M, which validates the advantage of proposed BSBP scheme again.

Figure 6 presents the SEE of the two proposed strategies versus d_{PS} and M with $\alpha = 0.5$ and $\gamma_B = 20$ dB. It can be observed that when the group of PBs is closer to multiple source users and the number of PBs is much more relative, the two proposed strategies achieve the best efficiency. Meanwhile, the BSBP scheme is more effective when M is larger, which can be explained as the abovementioned discussion.

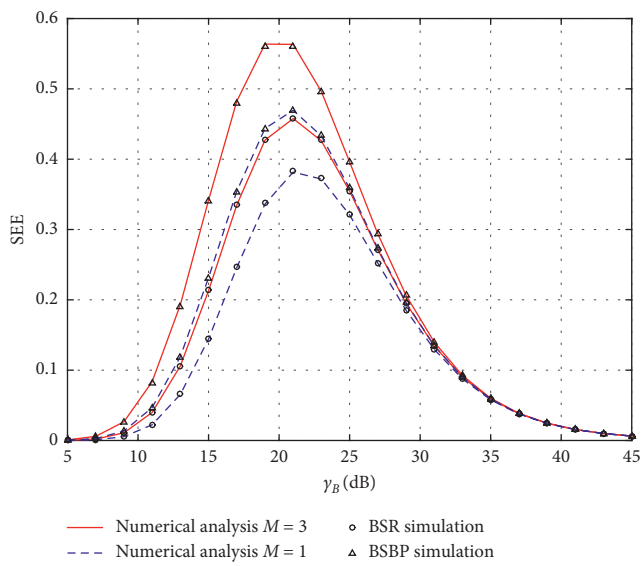


Figure 4: Effect of γ_B and M upon the secrecy energy efficiency with $\alpha = 0.5$ and $N = 3$.

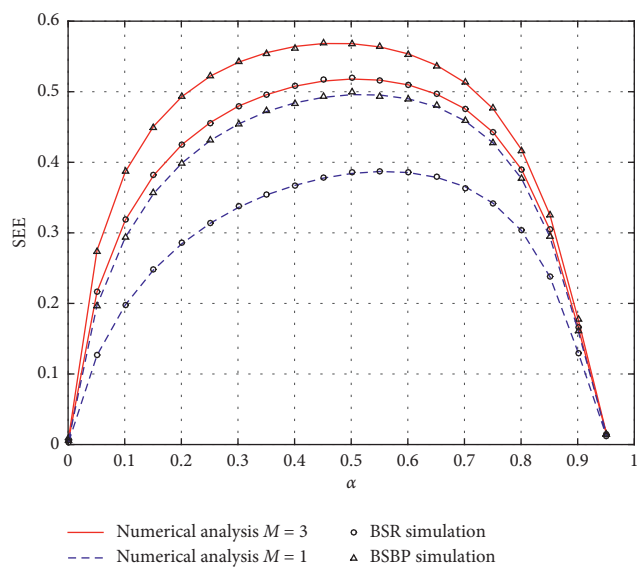


Figure 5: Effect of α and M upon the secrecy energy efficiency with $N = 3$ and $\gamma_B = 20$ dB.

Figure 7 plots the impact of d_{SD} and d_{PS} on the optimization of SEE by the searching method with BSR/BSBP scheme for $\gamma_B = 20$ dB. As shown clearly in the figure, the proposed multiuser scheduling schemes are more effective when d_{SD} and d_{PS} are smaller. As a matter of fact, the condition makes it possible for the sensors to acquire plenty of energy more readily, of which effect is equivalent to increasing P_B or expand α.

6. Conclusion

In this paper, the secrecy performance analysis of wireless-powered IoT possessing diverse PBs has been investigated. Specifically, the two green-oriented multiuser scheduling schemes to promote the secrecy performance of the networks are proposed. For each scheme, the analytical closed-form expression of SOP is obtained, while the optimization problem of SEE is solved by resorting to the searching method. To shed light on future applications of wireless-powered IoT, simulation results are presented to demonstrate the accuracy of our analysis, and the secrecy performance of the two proposed schemes is discussed, subject to various important parameters of the system.

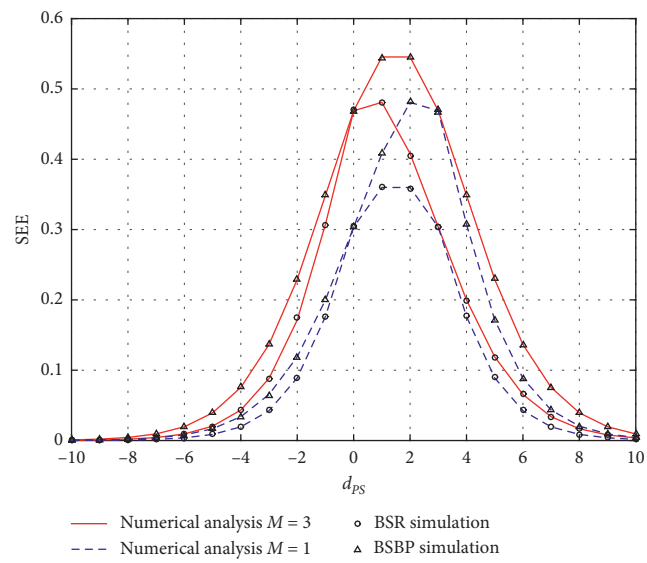


Figure 6: Effect of d_{PS} and M upon the secrecy energy efficiency with $\alpha = 0.5$ and $\gamma_B = 20$ dB.

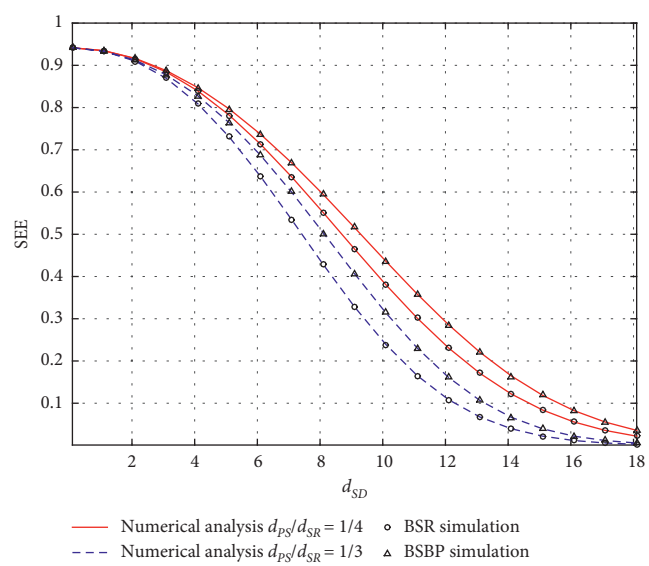


Figure 7: Effect of d_{SD} and d_{PS} upon the secrecy energy efficiency with $\gamma_B = 20$ dB.

Appendix

A. Proof of Formula (17)

According to (16), $\gamma_{\text{sec}}^{(\text{BSR})}$ is given by

$$\gamma_{\text{sec}}^{(\text{BSR})} = \min\left(\frac{1+\gamma_B\xi\gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}R}}{1+\gamma_E\xi\gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}E}}, \frac{1+\gamma_B\xi\gamma_{P_{m^*}R}\chi_{RD}}{1+\gamma_E\xi\gamma_{P_{m^*}R}\chi_{RE}}\right)$$
$$= \min\left(\gamma_{\text{sec}\,1}^{(\text{BSR})}, \gamma_{\text{sec}\,2}^{(\text{BSR})}\right). \tag{A.1}$$

Then, in line with (15) and (16), we have

$$P_{\text{sop}}^{(\text{BSR})} = P_{\text{sop},S_nR} = \Pr\left(\gamma_{\text{sec}}^{(\text{BSR})} < \beta\right) = F_{\gamma_{\text{sec}}^{(\text{BSR})}}(\beta), \tag{A.2}$$

where $F_{\gamma_{\text{sec}}^{(\text{BSR})}}(\beta)$ is the CDF of $\gamma_{\text{sec}}^{(\text{BSR})}$, which can be given with the help of (A.1) by

$$\begin{aligned} F_{\gamma_{\text{sec}}^{(\text{BSR})}}(\beta) &= \Pr\left\{\gamma_{\text{sec}}^{(\text{BSR})} < \beta\right\} \\ &= \Pr\left\{\min\left(\gamma_{\text{sec}\,1}^{(\text{BSR})}, \gamma_{\text{sec}\,2}^{(\text{BSR})}\right) < \beta\right\} \\ &= 1 - \Pr\left\{\gamma_{\text{sec}\,1}^{(\text{BSR})} > \beta\right\}\Pr\left\{\gamma_{\text{sec}\,2}^{(\text{BSR})} > \beta\right\} \\ &= 1 - \left[1 - \Pr\left\{\gamma_{\text{sec}\,1}^{(\text{BSR})} < \beta\right\}\right] \times \left[1 - \Pr\left\{\gamma_{\text{sec}\,2}^{(\text{BSR})} < \beta\right\}\right]. \end{aligned} \tag{A.3}$$

Furthermore, $\Pr\left\{\gamma_{\text{sec}\,1}^{(\text{BSR})} < \beta\right\}$ and $\Pr\left\{\gamma_{\text{sec}\,2}^{(\text{BSR})} < \beta\right\}$ can be derived aided by the Eq. (3.351.3) in [38], and the expression is listed as follows:

$$\begin{aligned} \Pr\left\{\gamma_{\text{sec}1}^{(\text{BSR})} < \beta\right\} &= \Pr\left\{\frac{1+\gamma_B\xi\gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}R}}{1+\gamma_E\xi\gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}E}} < \beta\right\} \\ &= \int_0^\infty\int_0^\infty F_{\chi_{S_{n^*}R}}\left[\frac{\beta(1+\gamma_E\xi xy)-1}{\gamma_B\xi x}\right] \\ &\quad \times f_{\gamma_{P_{m^*}S_{n^*}}}(x) f_{\chi_{S_{n^*}E}}(y)\mathrm{d}x\,\mathrm{d}y \\ &= 1 - \frac{\gamma_B\lambda_{PS}\lambda_{SE}}{\lambda_{SE}\gamma_B + \beta\gamma_E\lambda_{SR}} \times 2\sqrt{\frac{\lambda_{SR}(\beta-1)}{\gamma_B\xi\lambda_{PS}}}K_1 \\ &\quad \cdot \left(2\sqrt{\frac{\lambda_{SR}\lambda_{PS}(\beta-1)}{\gamma_B\xi}}\right), \end{aligned} \tag{A.4}$$

$$\begin{aligned} \Pr\left\{\gamma_{\text{sec}2}^{(\text{BSR})} < \beta\right\} &= \Pr\left\{\frac{1+\gamma_B\xi\gamma_{P_{m^*}R}\chi_{RD}}{1+\gamma_E\xi\gamma_{P_{m^*}R}\chi_{RE}} < \beta\right\} \\ &= \int_0^\infty\int_0^\infty F_{\chi_{RD}}\left[\frac{\beta(1+\gamma_E\xi xy)-1}{\gamma_B\xi x}\right] \\ &\quad \times f_{\gamma_{P_{m^*}R}}(x) f_{\chi_{RE}}(y)\mathrm{d}x\,\mathrm{d}y \\ &= 1 - \sum_{m=1}^{M}\binom{M}{m}(-1)^{m+1}\frac{m\gamma_B\lambda_{PR}\lambda_{RE}}{\lambda_{RE}\gamma_B + \beta\gamma_E\lambda_{RD}} \\ &\quad \times 2\sqrt{\frac{\lambda_{RD}(\beta-1)}{m\gamma_B\xi\lambda_{PR}}}K_1\left(2\sqrt{\frac{m\lambda_{PR}\lambda_{RD}(\beta-1)}{\gamma_B\xi}}\right). \end{aligned} \tag{A.5}$$

Finally, by substituting (A.4) and (A.5) into (A.3) and performing some mathematical manipulations, (17) can be derived.

B. Proof of Formula (18)

Similar with $\gamma_{\text{sec}}^{(\text{BSR})}$ in (A.1), $\gamma_{\text{sec}}^{(\text{BSBP})}$ can be shown as

$$\gamma_{\text{sec}}^{(\text{BSBP})} = \min\left(\frac{1+\gamma_B\xi\gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}R}}{1+\gamma_E\xi\gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}E}}, \frac{1+\gamma_B\xi\gamma_{P_{m^*}R}\chi_{RD}}{1+\gamma_E\xi\gamma_{P_{m^*}R}\chi_{RE}}\right)$$
$$= \min\left(\gamma_{\text{sec}1}^{(\text{BSBP})}, \gamma_{\text{sec}2}^{(\text{BSBP})}\right). \tag{B.1}$$

Meanwhile, according to (15) and (16), we find

$$P_{\text{sop}}^{(\text{BSBP})} = \Pr\left(\gamma_{\text{sec}}^{(\text{BSBP})} < \beta\right) = F_{\gamma_{\text{sec}}^{(\text{BSBP})}}(\beta), \tag{B.2}$$

where $F_{\gamma_{\text{sec}}^{(\text{BSBP})}}(\beta)$ is the CDF of $\gamma_{\text{sec}}^{(\text{BSBP})}$, and it can be expressed with the help of (A.1) as

$$\begin{aligned} F_{\gamma_{\text{sec}}^{(\text{BSBP})}}(\beta) &= \Pr\left\{\gamma_{\text{sec}}^{(\text{BSBP})} < \beta\right\} \\ &= \Pr\left\{\min\left(\gamma_{\text{sec}\,1}^{(\text{BSBP})}, \gamma_{\text{sec}2}^{(\text{BSBP})}\right) < \beta\right\} \\ &= 1 - \Pr\left\{\gamma_{\text{sec}\,1}^{(\text{BSBP})} > \beta\right\}\Pr\left\{\gamma_{\text{sec}\,2}^{(\text{BSBP})} > \beta\right\} \\ &= 1 - \left[1 - \Pr\left\{\gamma_{\text{sec}\,1}^{(\text{BSBP})} < \beta\right\}\right] \times \left[1 - \Pr\left\{\gamma_{\text{sec}\,2}^{(\text{BSBP})} < \beta\right\}\right]. \end{aligned} \tag{B.3}$$

After that, $\Pr\left\{\gamma_{\text{sec}\,1}^{(\text{BSBP})} < \beta\right\}$ and $\Pr\left\{\gamma_{\text{sec}\,2}^{(\text{BSBP})} < \beta\right\}$ can be obtained using the Eq. (3.351.3) in [38] and the expression listed below:

$$\begin{aligned} \Pr\left\{\gamma_{\text{sec}\,1}^{(\text{BSBP})} < \beta\right\} &= \Pr\left\{\frac{1+\gamma_B\xi\gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}R}}{1+\gamma_E\xi\gamma_{P_{m^*}S_{n^*}}\chi_{S_{n^*}E}} < \beta\right\} \\ &= \int_0^\infty\int_0^\infty F_{\chi_{S_{n^*}R}}\left[\frac{\beta(1+\gamma_E\xi xy)-1}{\gamma_B\xi x}\right] \\ &\quad \times f_{\gamma_{P_{m^*}S_{n^*}}}(x) f_{\chi_{S_{n^*}E}}(y)\mathrm{d}x\,\mathrm{d}y \\ &= 1 - \sum_{n=1}^{N}\binom{N}{n}(-1)^{n+1}\frac{n\gamma_B\lambda_{PS}\lambda_{SE}}{\lambda_{SE}\gamma_B + \beta\gamma_E\lambda_{SR}} \\ &\quad \times 2\sqrt{\frac{\lambda_{SR}(\beta-1)}{n\gamma_B\xi\lambda_{PS}}}K_1\left(2\sqrt{\frac{n\lambda_{SR}\lambda_{PS}(\beta-1)}{\gamma_B\xi}}\right), \end{aligned} \tag{B.4}$$

$$\begin{aligned}\Pr\left\{\gamma_{\sec 2}^{(\mathrm{BSBP})}<\beta\right\} &= \Pr\left\{\frac{1+\gamma_B\xi\gamma_{P_{m^*}R}\chi_{RD}}{1+\gamma_E\xi\gamma_{P_{m^*}R}\chi_{RE}}<\beta\right\}\\ &= \int_0^\infty\int_0^\infty F_{\chi_{RD}}\left[\frac{\beta(1+\gamma_E\xi xy)-1}{\gamma_B\xi x}\right]\\ &\quad\times f_{\gamma_{P_{m^*}R}}(x)f_{\chi_{RE}}(y)\mathrm{d}x\,\mathrm{d}y\\ &= 1-\sum_{m=1}^{M}\binom{M}{m}(-1)^{m+1}\frac{m\gamma_B\lambda_{PR}\lambda_{RE}}{\lambda_{RE}\gamma_B+\beta\gamma_E\lambda_{RD}}\\ &\quad\times 2\sqrt{\frac{\lambda_{RD}(\beta-1)}{m\gamma_B\xi\lambda_{PR}}}K_1\left(2\sqrt{\frac{m\lambda_{PR}\lambda_{RD}(\beta-1)}{\gamma_B\xi}}\right).\end{aligned} \tag{B.5}$$

Finally, by substituting (B.4) and (B.5) into (B.3) and performing some mathematical manipulations, (18) can be derived.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant numbers 61501508 and 61671476.

Supplementary Materials

The supplementary materials mainly include three folders. First of all, the folder named "Additional materials," which contains some pictures, is provided to illustrate the authenticity and reproducibility of our experimental results. It is worth noting that the above results are derived from the experimental environment of MATLAB and can be obtained by appropriately adjusting the simulation program that is given later. Then, the folder "Code" gives some simulation programs, on the basis of which we can reproduce our research results. Specific procedures and related instructions can be found in the simulation program. Furthermore, the *M* file in the folder "code", named WPCCN6_SEE_gammaB, is the main program. Based on the main program, by changing the different performance indicators, i.e., SOP or SEE required, Figures 3 and 4 in our manuscript can be derived. Meanwhile, other *M* files in the folder "code" are the callable programs. On the contrary, the files named "WPCCN_fig0.fig" and "WPCCN_fig1.fig" in the folder "code" are the numerical results of the simulation experiment, which had been given in our paper, i.e., Figures 3 and 4. Finally, the folder named "ReadMe" is a document explaining the simulation program, which can also be seen as a simple explanation of the supplementary material. It is worth noting that all the numerical results in our paper come from the simulation environment of MATLAB, which all are true experimental results. The specific experimental parameters are given in Section 5. Combining the parameter setting in the article with the program code, all the results can be reproduced. All program codes in the folder "code" are our original, which are refused to forward to others. If anyone has any questions, please contact us via email. The mailbox address is shangxiaohui1214@126.com. (*Supplementary Materials*)

References

[1] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5G networks for the internet of things: communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2018.

[2] F. Jameel, S. Wyne, and I. Krikidis, "Secrecy outage for wireless sensor networks," *IEEE Communications Letters*, vol. 21, no. 7, pp. 1565–1568, 2017.

[3] A. S. M. Z. Kausar, A. W. Reza, M. U. Saleh, and H. Ramiah, "Energizing wireless sensor networks by energy harvesting systems: scopes, challenges and approaches," *Renewable & Sustainable Energy Reviews*, vol. 38, pp. 973–989, 2014.

[4] Z. Hadzi-Velkov, I. Nikoloska, G. K. Karagiannidis, and T. Q. Duong, "Wireless networks with energy harvesting and power transfer: joint power and time allocation," *IEEE Signal Processing Letters*, vol. 23, no. 1, pp. 50–54, 2015.

[5] H. Chen, C. Zhai, Y. Li, and B. Vucetic, "Cooperative strategies for wireless-powered communications: an overview," *IEEE Wireless Communications*, vol. 25, no. 4, pp. 1–8, 2018.

[6] Y.-J. Kim, H. S. Bhamra, J. Joseph, and P. P. Irazoqui, "An ultra-low-power RF energy-harvesting transceiver for multiple-node sensor application," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 62, no. 11, pp. 1028–1032, 2015.

[7] J. Bito, R. Bahr, J. G. Hester, S. A. Nauroze, A. Georgiadis, and M. M. Tentzeris, "A novel solar and electromagnetic energy harvesting system with a 3-D printed package for energy efficient internet-of-things wireless sensors," *IEEE Transactions on Microwave Theory and Techniques*, vol. 65, no. 5, pp. 1831–1842, 2017.

[8] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: a contemporary survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 757–789, 2015.

[9] H. Ju and R. Zhang, "Throughput maximization in wireless powered communication networks," *IEEE Transactions on Wireless Communications*, vol. 13, no. 1, pp. 418–428, 2014.

[10] N.-P. Nguyen, T. Q. Duong, H. Q. Ngo, Z. Hadzi-Velkov, and L. Shu, "Secure 5G wireless communications: a joint relay selection and wireless power transfer approach," *IEEE Access*, vol. 4, pp. 3349–3359, 2016.

[11] V. N. Vo, T. G. Nguyen, C. So-In, and D.-B. Ha, "Secrecy performance analysis of energy harvesting wireless sensor networks with a friendly jammer," *IEEE Access*, vol. 5, pp. 25196–25206, 2017.

[12] V. N. Vo, T. G. Nguyen, C. So-In, Z. A. Baig, and S. Sanguanpong, "Secrecy outage performance analysis for energy harvesting sensor networks with a jammer using relay selection strategy," *IEEE Access*, vol. 6, pp. 23406–23419, 2018.

[13] Y. Wang, W. Yang, X. Shang, J. Hu, Y. Huang, and Y. Cai, "Energy-efficient secure transmission for wireless powered

internet of things with multiple power beacons," *IEEE Access*, vol. 6, pp. 75086–75098, 2018.

[14] Q. Wu, M. Tao, D. W. Ng, W. Chen, and R. Schober, "Energy-efficient transmission for wireless powered multiuser communication networks," in *Proceedings of the 2015 IEEE International Conference on Communications (ICC)*, pp. 154–159, London, UK, June 2015.

[15] Z. Hadzi-Velkov, I. Nikoloska, H. Chingoska, and N. Zlatanov, "Proportional fair scheduling in wireless networks with RF energy harvesting and processing cost," *IEEE Communications Letters*, vol. 20, no. 10, pp. 2107–2110, 2016.

[16] I. Bang, S. M. Kim, and D. K. Sung, "Adaptive multiuser scheduling for simultaneous wireless information and power transfer in a multicell environment," *IEEE Transactions on Wireless Communications*, vol. 16, no. 11, pp. 7460–7474, 2017.

[17] J. Choi, C. Song, and J. Joung, "Wireless powered information transfer based on zero-forcing for multiuser MIMO systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 8561–8570, 2018.

[18] H. Lee, H. Kin, K.-J. Lee, and I. Lee, "Asynchronous designs for multiuser MIMO wireless powered communication networks," *IEEE Systems Journal*, vol. 13, no. 3, pp. 1–11, 2018.

[19] D. Zhai, H. Chen, Z. Lin, Y. Li, and B. Vucetic, "Accumulate then transmit: multiuser scheduling in full-duplex wireless-powered IoT systems," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2753–2767, 2018.

[20] L. Fan, N. Yang, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Exploiting direct links for physical layer security in multiuser multirelay networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 3856–3867, 2016.

[21] F. Gandino, B. Montrucchio, and M. Rebaudengo, "Key management for static wireless sensor networks with node adding," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1133–1143, 2014.

[22] Y. Zou, J. Zhu, X. Wang, and V. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network*, vol. 29, no. 1, pp. 42–48, 2015.

[23] Y. Zou and G. Wang, "Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 2, pp. 780–787, 2016.

[24] M. Bloch and J. Barros, *Physical-layer Security: From Information Theory to Security Engineering*, Cambridge University Press, Cambridge, UK, 2011.

[25] L. Wang, K. J. Kim, T. Q. Duong, M. Elkashlan, and H. V. Poor, "Security enhancement of cooperative single carrier systems," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, pp. 90–103, 2015.

[26] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: state of the art and beyond," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 32–39, 2015.

[27] M. Yang, D. Guo, Y. Huang, T. Q. Duong, and B. Zhang, "Secure multiuser scheduling in downlink dual-hop regenerative relay networks over Nakagami-m fading channels," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8009–8024, 2016.

[28] M. Yang, D. Guo, Y. Huang, T. Q. Duong, and B. Zhang, "Physical layer security with threshold-based multiuser scheduling in multi-antenna wireless networks," *IEEE Transactions on Communications*, vol. 64, no. 12, pp. 5189–5202, 2016.

[29] G. Wang, Q. Liu, R. He, F. Gao, and C. Tellambura, "Acquisition of channel state information in heterogeneous cloud radio access networks: challenges and research directions," *IEEE Wireless Communications*, vol. 22, no. 3, pp. 100–107, 2015.

[30] T. Paing, J. Shin, R. Zane, and Z. Popovic, "Resistor emulation approach to low-power RF energy harvesting," *IEEE Transactions on Power Electronics*, vol. 23, no. 3, pp. 1494–1501, 2008.

[31] Z. Chen, L. Hadley, Z. Ding, and X. Dai, "Improving secrecy performance of a wirelessly powered network," *IEEE Transactions on Communications*, vol. 65, no. 11, pp. 4996–5008, 2017.

[32] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Transactions on Wireless Communications*, vol. 12, no. 7, pp. 3622–3636, 2013.

[33] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: architecture design and rate-energy tradeoff," *IEEE Transactions on Communications*, vol. 61, no. 11, pp. 4754–4767, 2013.

[34] N. Shinohara, *Wireless Power Transfer via Radiowaves*, Wiley, Hoboken, NJ, USA, 2014.

[35] X. Kang, Y.-C. Liang, and J. Yang, "Riding on the primary: a new spectrum sharing paradigm for wireless-powered IoT devices," *IEEE Transactions on Wireless Communications*, vol. 17, no. 9, pp. 6335–6347, 2018.

[36] T. M. Hoang, T. Q. Duong, N.-S. Vo, and C. Kundu, "Physical layer security in cooperative energy harvesting networks with a friendly jammer," *IEEE Wireless Communications Letters*, vol. 6, no. 2, pp. 174–177, 2017.

[37] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 3000–3015, 2012.

[38] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, Academic Press, Cambridge, MA, USA, 7th edition, 2007.

[39] J. Farhat, G. Brante, R. D. Souza, and J. L. Rebelatto, "Energy efficiency of repetition coding and parallel coding relaying under partial secrecy regime," *IEEE Access*, vol. 4, pp. 7275–7288, 2016.

[40] W. Liu, X. Zhou, S. Durrani, and P. Popovski, "Secure communication with a wireless-powered friendly jammer," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 401–415, 2016.

Hindawi
Wireless Communications and Mobile Computing
Volume 2019, Article ID 8391307, 8 pages
https://doi.org/10.1155/2019/8391307

Research Article

Design and Implementation of Directional Sensors for Privacy-Ensured Device-Free Target Localization in Indoor Environment

Ata ur Rehman,[1] Zeeshan Ellahi,[2] Asif Iqbal,[3] Farman Ullah,[1] Ahmed Ali,[1] and Kyung Sup Kwak[3]

[1]*Department of Electrical and Computer Engineering, COMSATS University Islamabad, Attock, Pakistan*
[2]*National Institute of Electronics, Islamabad, Pakistan*
[3]*Department of Information and Communication Engineering, Inha University, Incheon 22212, Republic of Korea*

Correspondence should be addressed to Kyung Sup Kwak; kskwak@inha.ac.kr

Received 1 August 2019; Revised 5 November 2019; Accepted 18 November 2019; Published 27 December 2019

Guest Editor: Sarmadullah Khan

This paper presents two radio frequency (RF) sensors with different directivities designed and tested for device-free localization (DFL) in an indoor environment. Mostly, in smart homes and smart offices, peoples may be irritated by wearing the device on them all the time. As compared with device-based localization, the proposed sensors can localize both cooperative and non-cooperative targets (intruders and guests etc.) without privacy leakages. Both sensors are tested to detect the change in received signal strength (ΔRSS) due to the presence of an obstacle. RF sensors, i.e., antennas are designed to operate in the ISM band of 2.4–2.5 GHz. Experimental results show that the sensor with higher directivity provides better ΔRSS that helps in improved accuracy to detect a device-free target.

1. Introduction

Accurate indoor localization of objects and people is among the most researched areas nowadays for many applications such as indoor navigation, location-based services, and advertisements [1–3]. One of the significant challenges in indoor localization is the use of device or tag by the target to be localized, such as RFID tags and smartphones [4–7]. Device-based localization is not suitable in case of non-cooperative targets (passive targets) such as intruders and guests. Mostly, in smart homes [8] and smart offices, people may be irritated by wearing the device on them all the time. Tag-based localization is highly prone to the leakage of privacy and personal information, e.g., a person's daily routine [9–12]. Many techniques have been proposed for the localization of non-cooperative targets such as thermal infrared sensors, pressure sensors, sound source, light sensors, electric field, ultrasonic sensors, and radio frequency- (RF-) based localization schemes [13–15].

In pressure sensor-based localization, pressure sensors are installed beneath the floor. This is a traditional way of passive localization. Position identification is made by sensing pressure on the floor [16–18]. Different systems are proposed in this regard. One of them is a load cell system that uses load sensors for user localization, and larger size tiles are used to reduce the number of sensors [19]. There is a tradeoff between system complexity and the number of targets detected simultaneously versus the size of the tile used. Another approach is the use of a pixelated surface (mat), which uses sensors made of binary switches. These sensors are costly to be used in larger areas. Magic carpet [20] and electromechanical film (EMFi) are commercially available systems, but their installation is complicated. Alternatively, the Z-tile system [21] and smart carpet [22] are easily scalable and commercially available solutions. Overall the installation of a pressure sensors system is complicated and laborious and needs modification of the floor, which is sometimes not feasible in already constructed buildings.

Another way to localize a device-free target is to use infrared sensors [23]. The wavelength of infrared light ranges from 750 nm to 1 mm. This wavelength corresponds to temperature radiated by the objects having temperatures between 0 and 70°C [24]. An infrared camera uses a microbolometer detector, which is used to create a thermal image for localization [25]. Many devices use the microbolometer detector, but these are very expensive. Other detectors such as quantum detectors and Golay cell [26, 27] are inefficient in the home environment. Alternatively, pyroelectric and thermopile detectors are affordable as they detect a change in heat and generate an electric signal [28]. In thermal infrared sensing metals, lamps and heater disrupt the image and make difficulties for the identification of persons or objects. So, the quantity and placing of the sensors are critical considerations to increase the performance. Multitarget tracking is another issue in thermal infrared sensing, although many techniques and algorithms are being developed [29].

The localization of sound sources is categorized in active and passive sources. Active sources send a signal and detect the presence of the user by the reflected signal as in sonar, while passive sources only detect the sound signal generated by the target [30]. Microphones are used as a sensor in sound sources localization. Generally, an array of microphones is used to measure the time difference of arrival (TDOA) to calculate the position of a target. Accuracy is increased by placing many sensors and using triangulation and keeping the same frequency characteristic of all sensors [31]. Main algorithms for sound source localization are TDOA [32], steered beamforming [33], and high-resolution spectral estimation [34]. There are many drawbacks of sound source localization, as it gives false detection due to echo, noise, and sound from other sources [35].

Ultrasound localization is based on the travel time of waves from one position to another position. Time difference of arrival (TDOA) and time of flight (TOF) are two methods used for ultrasound-based positioning. The TDOA-based technique uses two transmitters and a receiver and calculates the difference for locating the target; however, this method is sensitive to noise. While in the TOF method, time to travel from the transmitter to the receiver is calculated for localization [36]. In [37], ultrasound localization is done by calculating TOF of receive wave reflected off person's head. The complexity of the system increases sharply by increasing the region of interest. Synchronization and multipath are other challenges in an indoor environment.

Electric field positioning is based on the principle that the human body conducts low-frequency signals [38]. Mainly two modes are proposed for localization, i.e., human shunt and human transmitter. In the human shunt mode, the potential difference (ΔV) between transmitter and receiver electrodes generate a displacement current, that flows from transmitter to receiver, and when a person enters in the vicinity of an electric field, displacement current decreases due to shunt of the electric field to ground, which helps in locating a person. In the human transmitter method, the human body acts as an electric field transmitter as a person moves toward the receiver, electrode displacement current increases, which helps to locate a person. Some practical solutions are tile track [39], electric field resonance coupling [40], and electric sensors with intelligence (ELSI) system [41]. These systems are inexpensive, but installation is expensive and complex.

Light sensors detect a change in the level of light to estimate the position of the target. AOA-based measurements are used as a sensing parameter. AOA from different sensors is used to estimate the location of the target through the intersection of directional lines. However, these sensors work only in the presence of light, which is not feasible to use in all environments [42], for example, at night.

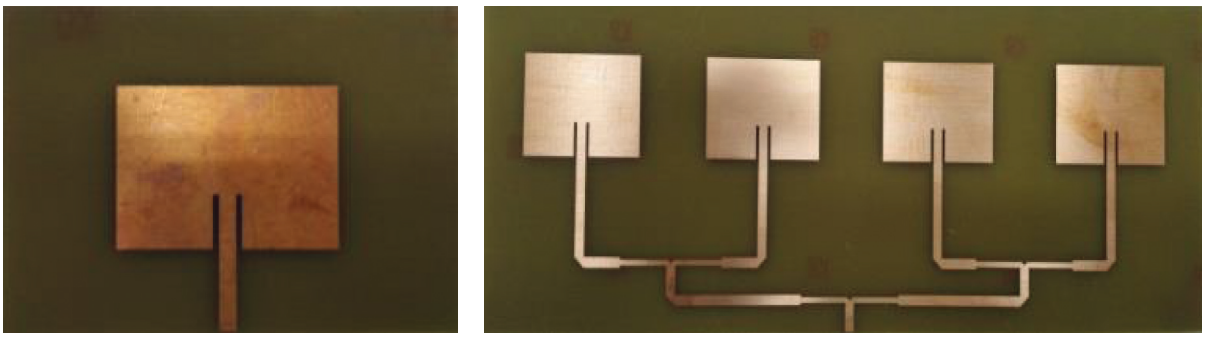
The device-free localization (DFL) techniques pose some challenges such as environmental dependency, installation complexity, and resizing. However, RF-based localization caters to these challenges and shows effective results. RF-based passive localization using Wi-Fi infrastructure detects the change in RSS, but this change is insignificant due to the omnidirectional pattern of the Wi-Fi antenna. RF-based DFL works on the principle that obstacles affect the strength of radio signals. Saeed et al. [14] presented a system using Wi-Fi access point as a transmitter and laptop as the receiver to detect human presence. This system needs a human presence profile for calibration during the initial installation. The system deployment on a large-scale area increases the calibration overheads. These systems are not accurate and often produce false alarm [43–45]. The antenna radiation pattern is very important while implementing the localization system, as it affects the RSS value according to its radiation pattern.

Directional antennas have been used for estimating the angle of arrival (AOA) to localize the active target (target bearing a tag) [46–48]. However, to the best of our knowledge, directional antennas have not been used for DFL. To overcome the limitations of DFL systems based on antennas with poor directivity, we proposed a localization system based on antennas with higher directivity.

2. Methodology

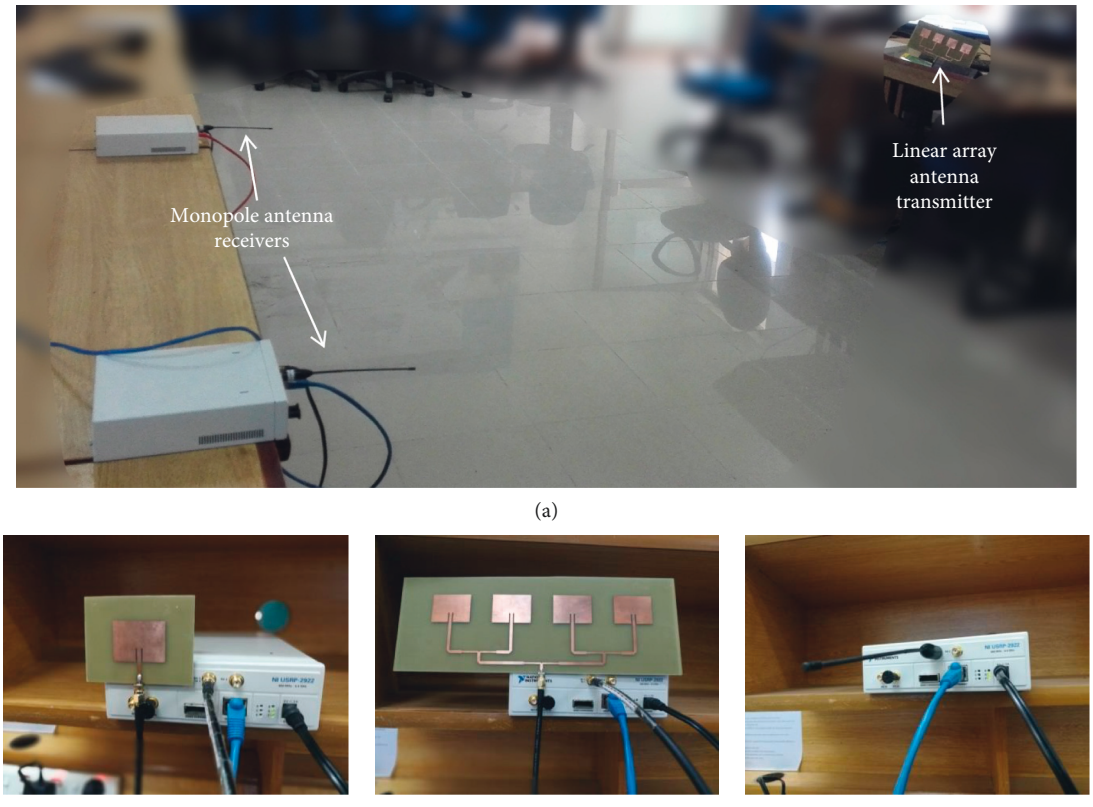
Directional antennas incorporate AOA measurements with RSS-based measurements, which help to detect the target with more accuracy. We have designed a microstrip patch antenna and a linear array of patch antennas at 2.45 GHz. These antennas are used as RF sensors to test for DFL. An experiment is carried out to detect the change in RSS first using a sensor with lower directivity and then a sensor with higher directivity. These antennas are used in transmitting mode, while two monopole antennas are used as receivers. We have measured the RSS values from two different angles at receivers with and without target (human).

2.1. Sensor Design. The simulations and optimization of proposed RF sensors were done through finite integration technique-based CST microwave studio 2014. A low cost and easily available FR4 substrate was used with the relative permittivity of 4.4 and a dielectric loss of 0.02, while the thickness of the substrate is 1.6 mm. Two-sided copper



(a) (b)

Figure 1: Fabricated antennas: (a) single microstrip antenna and (b) linear array of microstrip antennas.



(a)

(b) (c) (d)

Figure 2: (a) Localization experiment environment. (b) Single microstrip antenna attached with USRP. (c) Linear array of microstrip antennas attached with USRP. (d) Monopole antenna attached with USRP.

cladding is used for the radiating patch (top) and ground (bottom) of the substrate. For practical realization and to demonstrate the proposed designs experimentally prototypes of both the designs are fabricated. A standard technique for designing the printed circuit board (PCB) called wet etching is used for fabrication of proposed RF sensor designs. The fabricated prototypes are shown in Figure 1.

2.2. Localization Experiment. Figure 2 shows the experimental setup used to test the effect of the directivity of the designed RF sensors at 2.45 GHz for target localization. To perform localization experiments, we have used National Instrument USRP (Universal Software Radio Peripheral) kits as transceivers. Fabricated antennas are used as transmitters, and two monopole antennas are used as receivers, which are placed at 0° and 20°. First, the localization experiment is carried out by using the single patch antenna as a transmitter and then the linear array antenna as a transmitter. In this experiment, we have measured the RSS at both receivers when no target is present. Then, the RSS is measured again in the presence of the target (human). To verify the effect of antenna directivity on RSS, we have measured the RSS by placing the target at 0° and then at 20°.

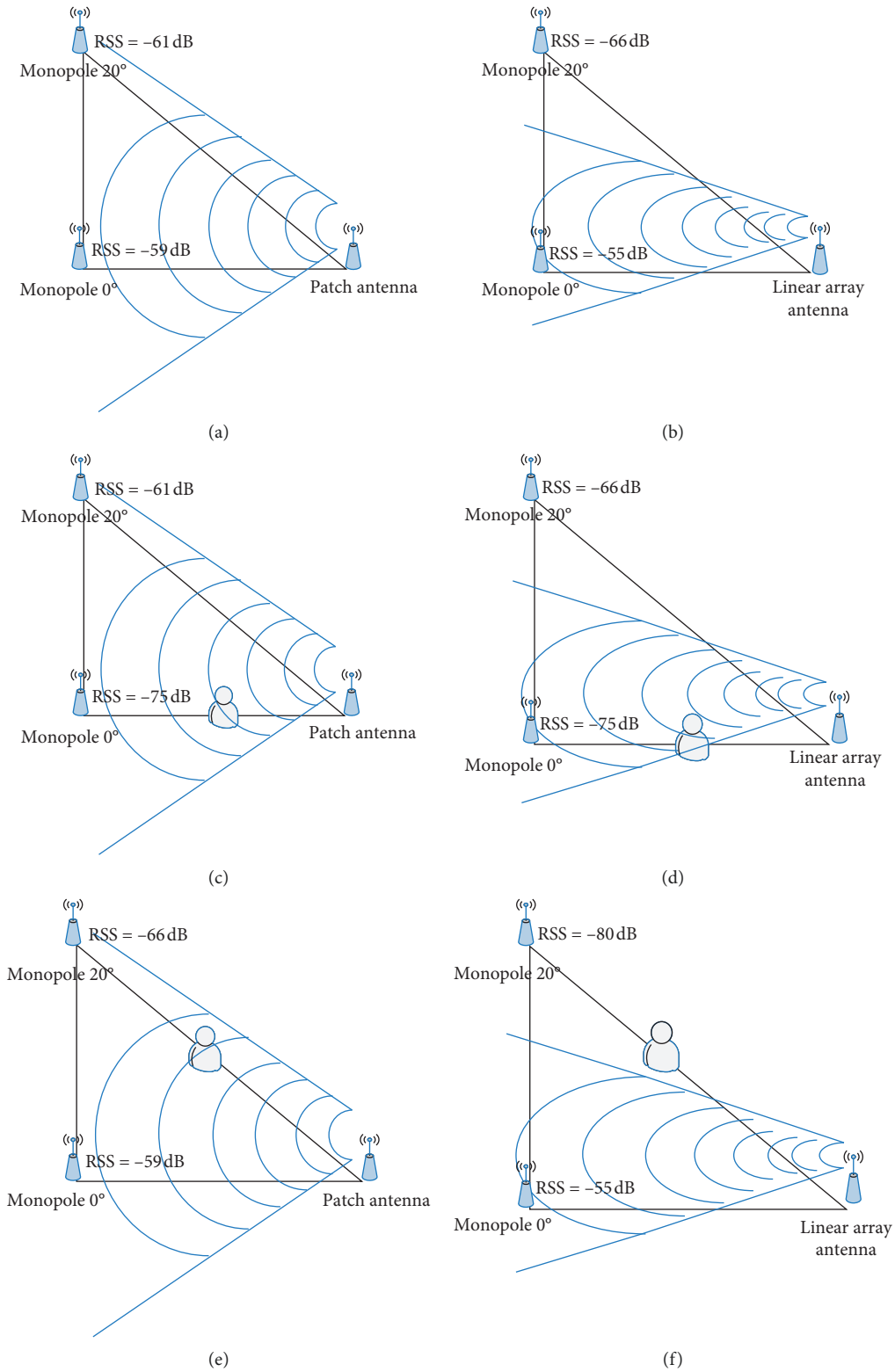


Figure 3: Localization experiment scenarios: (a) patch antenna without target; (b) linear array antenna without target; (c) single patch with target at 0°; (d) linear array with target at 0°; (e) single patch with target at 20°; (f) linear array with target at 20°.

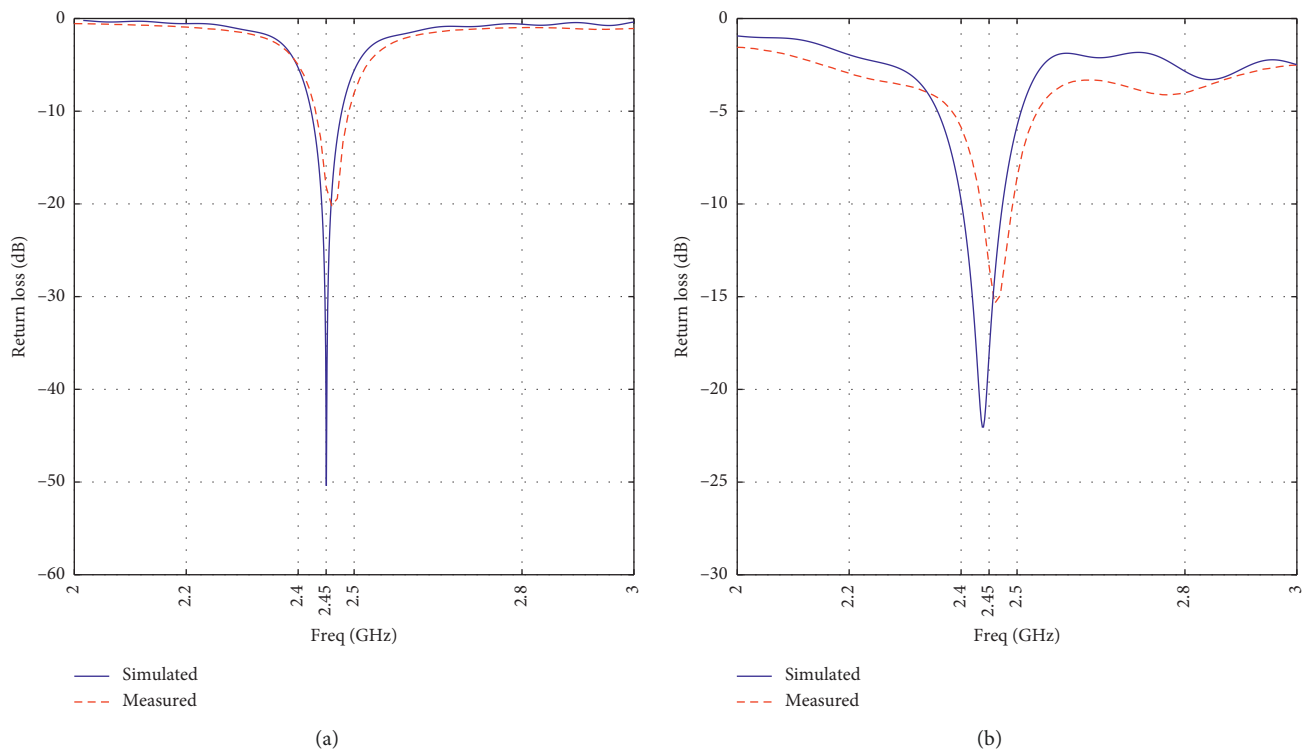


Figure 4: Simulated and measured return loss: (a) single microstrip antenna and (b) linear array of microstrip antennas.

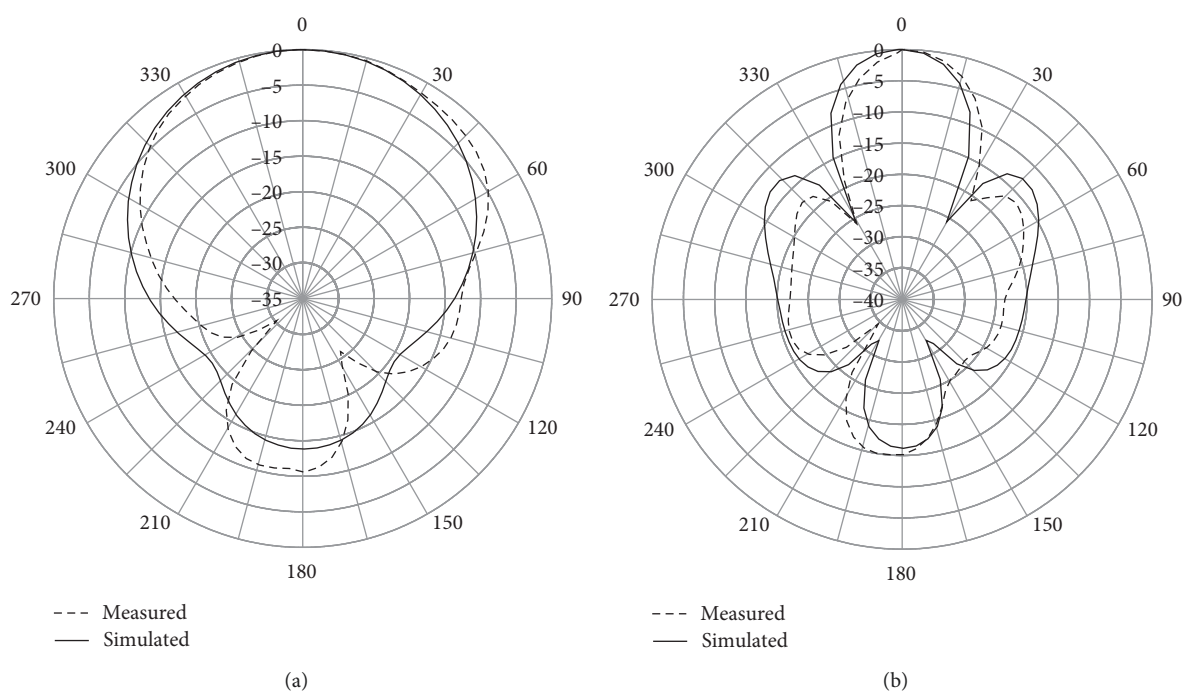


Figure 5: Simulated and measured radiation patterns: (a) sensor with lower directivity and (b) sensor with higher directivity.

RSS is measured at both receivers with monopole antennas in six scenarios as follows:

(1) The single patch antenna as the transmitter without a target

(2) The single patch antenna as the transmitter with the target (human) at 0°

(3) The single patch antenna as the transmitter with the target (human) at 20°

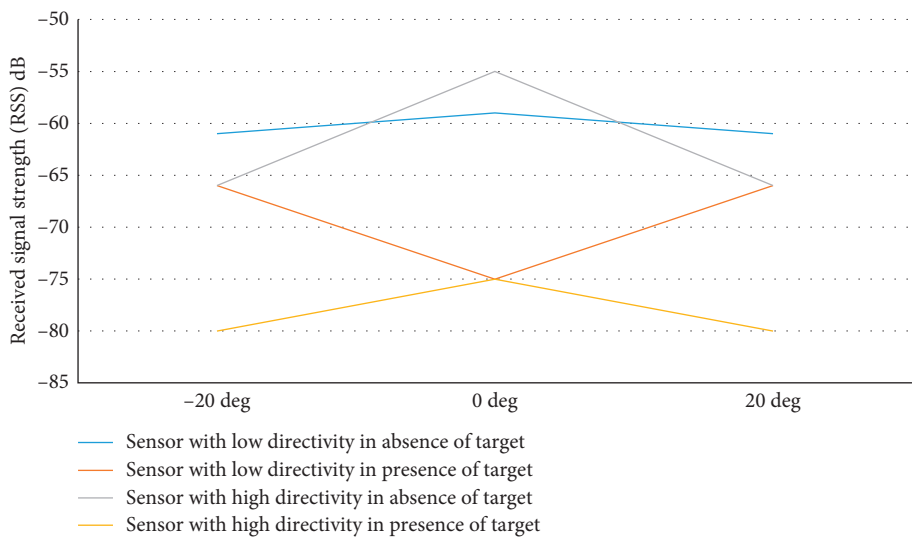


Figure 6: Measured RSS values for localization experiment scenarios.

Table 1: Comparison of change in received signal strength for all measurements.

Antenna type	Scenario	In the absence of target	In the presence of target	|ΔRSS|
Single patch antenna	RSS at 0° (dB)	−59	−75	16
	RSS at 20° (dB)	−61	−66	5
Linear array antenna	RSS at 0° (dB)	−55	−75	20
	RSS at 20° (dB)	−66	−80	14

(4) The linear array as transmitter without any target

(5) The linear array as transmitter with the target (human) at 0°

(6) The linear array as transmitter with the target (human) at 20°

These six scenarios are pictorially represented in Figure 3.

3. Results

The RF sensors were simulated in CST, and the fabricated sensors were tested for return loss using VNA, and the radiation pattern measurements were done in an anechoic chamber.

In order to carry out the RSS measurements, a single frequency signal is enough, and covering the entire ISM band is not necessary. The only requirement is that the antennas should resonate in the ISM license-free band. Return losses of the simulated and the fabricated patch antenna and linear array antenna are shown in Figure 4. Both antennas resonate in the desired frequency band (2.4–2.5 GHz), and the simulated and fabricated return losses of both the designs are in close agreement. The slight shift of the resonance is due to the fabrication and measurement losses.

Both the simulated and measured radiation patterns of the patch antenna and the linear array antenna are shown in Figures 5(a) and 5(b), respectively. From the comparison of Figures 5(a) and 5(b), it is evident that the linear array antenna is more directive than the single element patch antenna. Moreover, the simulated and fabricated radiation patterns of both the antennas are in close agreement.

These sensors were used to carry out the localization experiment for performance evaluation. Figure 6 shows that in the case of the sensor with lower directivity at 0° with respect to broadside the RSS values drops from −59 dB to −75 dB resulting a |ΔRSS| = 16 dB as compared with a drop in RSS for sensor of higher directivity from −55 dB–75 dB resulting a |ΔRSS| = 20 dB that is improved by 4 dB. At the angles of ±20° with respect to broadside for the sensor with lower directivity the RSS values drops from −61 dB to −66 dB resulting in a |ΔRSS| = 5 dB as compared with a drop in RSS for the sensor of higher directivity from −66 dB–80 dB resulting in a |ΔRSS| = 14 dB that is improved by 9 dB. These results are summarized in Table 1.

4. Discussion

In the localization experiment, we have proved that by using directive sensors, we can detect a significant change in RSS. The accuracy of localization depends on the change in RSS due to the target. As the target comes in the range of the system, we detect the change in RSS at all receivers. The change in RSS using sensors with low directivity is almost the same when the link is interrupted. If the change is the same at all receivers, we cannot locate the target with certainty. For this purpose, the improvement in this value is required. This can be done if we use sensors with higher directivities, as their transmit power is only significant at the

receiver, which is placed in its line of sight. Therefore, in the localization experiment, we have compared the change in RSS by using a high-directive antenna (sensor with higher directivity) and a relatively low-directive antenna (sensor with low directivity). We have got very prominent localization results, which endorse our proposed solution.

5. Conclusion

In this paper, the potential application of directional sensors for device-free indoor localization has been proposed. Patch antenna and linear array antenna were designed and tested in an indoor environment for device-free target localization. The results show that the change in RSS is more significant for sensors with higher directivity making them a better candidate for localization systems developed to localize device-free targets in indoor environments.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This work was supported by the National Research Foundation of Korea-Grant funded by the Korean Government (Ministry of Science and ICT) (no. NRF-2017R1A2B2012337).

References

[1] A. Yassin, Y. Nasser, M. Awad et al., "Recent advances in indoor localization: a survey on theoretical approaches and applications," *In IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1327–1346, 2016.

[2] I. Ashraf, S. Hur, and Y. Park, "mPILOT-magnetic field strength based pedestrian indoor localization," *Sensors*, vol. 18, no. 7, p. 2283, 2018.

[3] R. Xi, D. Liu, M. Hou, Y. Li, and J. Li, "Using acoustic signal and image to achieve accurate indoor localization," *Sensors*, vol. 18, no. 8, p. 2566, 2018.

[4] C. Luo, L. Cheng, M. C. Chan, Y. Gu, J. Li, and Z. Ming, "Pallas: self-bootstrapping fine-grained passive indoor localization using WiFi monitors," *IEEE Transactions on Mobile Computing*, vol. 16, no. 2, pp. 466–481, 2017.

[5] J. Huang, X. Yu, Y. Wang, and X. Xiao, "An integrated wireless wearable sensor system for posture recognition and indoor localization," *Sensors*, vol. 16, no. 11, p. 1825, 2016.

[6] F. Seco and A. R. Jiménez, "Smartphone-based cooperative indoor localization with RFID technology," *Sensors*, vol. 18, no. 1, p. 266, 2018.

[7] J.-H. Bang, Y.-S. Jeong, C.-H. Kim, S. Li, B.-C. Ahn, and S.-G. Choi, "Dual-loop near-field antenna for RFID label printer applications," *Electronics Letters*, vol. 52, no. 25, pp. 2029-2030, 2016.

[8] A. Iqbal, F. Ullah, H. Anwar et al., "Interoperable Internet-of-Things platform for smart home system using Web-of-Objects and cloud," *Sustainable Cities and Society*, vol. 38, pp. 636–646, 2018.

[9] J. Zhang, X. Zheng, Z. Tang et al., "Privacy leakage in mobile sensing: your unlock passwords can be leaked through wireless hotspot functionality," *Mobile Information Systems*, vol. 2016, Article ID 8793025, 14 pages, 2016.

[10] F. Zafari, A. Gkelias, and K. K. Leung, "A survey of indoor localization systems and technologies," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2568–2599, 2019.

[11] A. Majeed, F. Ullah, and S. Lee, "Vulnerability- and diversity-aware anonymization of personally identifiable information for improving user privacy and utility of publishing data," *Sensors*, vol. 17, no. 5, p. 1059, 2017.

[12] S. Zhong, H. Zhong, X. Huang et al., "Connecting physical-world to cyber-world: security and privacy issues in pervasive sensing," in *Security and Privacy for Next-Generation Wireless Networks*, pp. 49–63, Springer, Cham, Switzerland, 2019.

[13] T Kivimäki, T Vuorela, P. Peltola, and J. Vanhala, "A review on device-free passive indoor positioning methods," *International Journal of Smart Home*, vol. 8, no. 1, pp. 71–94, 2014.

[14] A. Saeed, A. E. Kosba, and M. Youssef, "Ichnaea: a low-overhead robust WLAN device-free passive localization system," *IEEE Journal of Selected Topics in Signal Processing*, vol. 8, no. 1, pp. 5–15, 2014.

[15] S. H. Yang, S. K. Han, and E. M. Jeong, "Indoor positioning based on received optical power difference by angle of arrival," *Electronics Letters*, vol. 50, no. 1, pp. 49–51, 2014.

[16] L. Middleton, A. A. Buss, A. Bazin, and M. S. Nixon, "A floor sensor system for gait recognition," in *Proceedings of the 4th IEEE Workshop Automatic Identification Advanced Technologies*, pp. 171–176, Buffalo, NY, USA, October 2005.

[17] R. J. Orr and G. D. Abowd, "The smart floor: a mechanism for natural user identification and tracking," in *Proceedings of the CHI'00 Extended Abstracts on Human Factors in Computing Systems*, pp. 275-276, The Hague, Netherlands, April 2000.

[18] S. Pirttikangas, J. Suutala, J. Riekki, and J. Röning, "Footstep identification from pressure signals using hidden markov models," in *Proceedings of the Finnish Signal Processing Symposium*, pp. 124–128, Tampere, Finland, May 2003.

[19] A. Schmidt, M. Strohbach, K. Van Laerhoven, A. Friday, and H. W. Gellersen, "Context acquisition based on load sensing," in *Proceedings of the UbiComp 2002: Ubiquitous Computing*, pp. 161–192, Göteborg, Sweden, September 2002.

[20] J. Paradiso, C. Abler, K. Hsiao, and M. Reynolds, "The magic carpet: physical sensing for immersive environments," in *Proceedings of the CHI'97 Extended Abstracts Human Factors Computing Systems Looking to the Future*, pp. 277-278, Atlanta, GA, USA, March 1997.

[21] B. Richardson, K. Leydon, M. Fernstrom, and J. A. Paradiso, "Z-tiles: building blocks for modular, pressure sensing floorspaces," in *Proceedings of the CHI'04 Extended Abstracts Human Factors Computing Systems*, pp. 1529–1532, 2004.

[22] D. Savio and T. Ludwig, "Smart carpet: a footstep tracking interface," in *Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)*, pp. 754–760, Niagara Falls, Canada, May 2007.

[23] D. Yang, B. Xu, K. Rao, and W. Sheng, "Passive infrared (PIR)-based indoor position tracking for smart homes using accessibility maps and a-star algorithm," *Sensors*, vol. 18, no. 2, p. 332, 2018.

[24] D. Hauschildt and N. Kirchhof, "Advances in thermal infrared localization: challenges and solutions," in *Proceedings of the 2010 International Conference on Indoor Positioning and*

Indoor Navigation, pp. 1–8, Zurich, Switzerland, September 2010.

[25] E. M. Tapia, S. S. Intille, L. Lopez, and K. Larson, "The design of a portable kit of wireless sensors for naturalistic data collection," *Lecture Notes in Computer Science*, Springer, vol. 3968, pp. 117–134, Berlin, Germany, 2006.

[26] J. Kemper and H. Linde, "Challenges of passive infrared indoor localization," in *Proceedings of the 5th Workshop Positioning, Navigation and Communication*, pp. 63–70, Hannover, Germany, March 2008.

[27] D. Denison, M. Knotts, H. Hayden, S. Young, and V. Tsukruk, "Influence of micro-Golay cell cavity diameter on millimeter-wave detection sensitivity," in *Proceedings of the 2011 International Conference on Infrared, Millimeter, and Terahertz Waves*, pp. 1-2, Houston, TX, USA, October 2011.

[28] J. L. Honorato, I. Spiniak, and M. Torres-Torriti, "Human detection using thermopiles," in *Proceedings of the 2008 IEEE Latin American Robotic Symposium*, pp. 151–157, Natal, Brazil, October 2008.

[29] Q. Sun, F. Hu, and Q. Hao, "Context awareness emergence for distributed binary pyroelectric sensors," in *Proceedings of the 2010 IEEE Conference on Multisensor Fusion and Integration*, pp. 5–7, Salt Lake City, UT, USA, September 2010.

[30] J. M. R. Bian and G. D. Abowd, "Sound source localization in domestic environment," Tech. Rep., GVU Center, Atlanta, GA, USA, 2004.

[31] M. Mandlik, Z. Nemec, and R. Dolecek, "Real-time sound source localization," in *Proceedings of the 2012 13th International Radar Symposium*, pp. 322–325, Warsaw, Poland, May 2012.

[32] M. S. Brandstein, *A framework for speech source localization using sensor arrays*, Ph.D. dissertation, Brown University, Providence, RI, USA, 1995.

[33] J. M. Valin, F. Michaud, B. Hadjou, and J. Rouat, "Localization of simultaneous moving sound sources for mobile robot using a frequency-domain steered beamformer approach," in *Proceedings of the IEEE International Conference on Robotics and Automation*, pp. 1033–1038, New Orleans, LA, USA, April 2004.

[34] J. Benesty, "Adaptive eigenvalue decomposition algorithm for passive acoustic source localization," *The Journal of the Acoustical Society of America*, vol. 107, no. 1, pp. 384–391, 2000.

[35] X. Bian, G. Abowd, and J. Rehg, "Using sound source localization in a home environment," in *Pervasive Computing. Lecture Notes in Computer Science*, H. Gellersen, R. Want, and A. Schmidt, Eds., pp. 19–36, Springer, Berlin, Germany, 2005.

[36] S. Holm and C. C. Nilsen, "Robust ultrasonic indoor positioning using transmitter arrays," in *Proceedings of the 2010 International Conference on Indoor Positioning and Indoor Navigation*, pp. 1–5, Zurich, Switzerland, September 2010.

[37] Y. Nishida, T. Hori, S. Murakami, and H. Mizoguchi, "Minimally privacy-violative system for locating human by ultrasonic radar embedded on ceiling," in *Proceedings of the 2004 IEEE International Conference on Systems, Man and Cybernetics*, vol. 2, pp. 1549–1554, The Hague, Netherlands, October 2004.

[38] T. G. Zimmerman, J. R. Smith, J. A. Paradiso, D. Allport, and N. Gershenfeld, "Applying electric field sensing to human-computer interfaces," in *Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 280–287, Austin, TX, USA, May 1995.

[39] M. Valtonen, J. Mäentausta, and J. Vanhala, "Tiletrack: capacitive human tracking using floor tiles," in *Proceedings of the 2009 IEEE International Conference on Pervasive Computing and Communications*, pp. 31–40, Galveston, TX, USA, March 2009.

[40] S. Nakamura, S. Ajisaka, K. Takiguchi, A. Hirose, and H. Hashimoto, "Electric-field resonance coupling between human and transmitter for human position estimation system," in *Proceedings of the International Conference on Control, Automation and Systems*, pp. 109–114, Gyeonggi-do, South Korea, October 2010.

[41] A. Ropponen, M. Linnavuo, and R. Sepponen, "LF indoor location and identification system," *International Journal on Smart Sensing and Intelligent Systems*, vol. 2, no. 1, pp. 94–117, 2009.

[42] X. Mao, S. Tang, J. Wang, and X. Y. Li, "iLight: device-free passive tracking using wireless sensor networks," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3785–3792, 2013.

[43] L. Chen, K. Yang, and X. Wang, "Robust cooperative Wi-Fi fingerprint-based indoor localization," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 1406–1417, 2016.

[44] Z. Liu, F. Bien, and Y. Kim, "Indoor positioning and life detection by using asynchronous multiple frequency shift keying radar," *Electronics Letters*, vol. 51, no. 22, pp. 1817–1819, 2015.

[45] J. Wilson and N. Patwari, "Radio tomographic imaging with wireless networks," *IEEE Transactions on Mobile Computing*, vol. 9, no. 5, pp. 621–632, 2010.

[46] M. I. Jais, P. Ehkan, R. B. Ahmad, I. Ismail, T. Sabapathy, and M. Jusoh, "Review of angle of arrival (AOA) estimations through received signal strength indication (RSSI) for wireless sensors network (WSN)," in *Proceedings of the International Conference on Computer, Communications, and Control Technology (I4CT)*, pp. 354–359, Kuching, Malaysia, August 2015.

[47] M. Rzymowski, P. Woznica, and L. Kulas, "Single-anchor indoor localization using ESPAR antenna," *IEEE Antennas and Wireless Propagation Letters*, vol. 15, no. 1, pp. 1183–1186, 2016.

[48] C. C. Cruz, J. R. Costa, and C. A. Fernandes, "Hybrid UHF/UWB antenna for passive indoor identification and localization systems," *IEEE Transactions on Antennas and Propagation*, vol. 61, no. 1, pp. 354–361, 2013.

Hindawi
Wireless Communications and Mobile Computing
Volume 2019, Article ID 4582391, 14 pages
https://doi.org/10.1155/2019/4582391

Research Article

Policy-Based Security Management System for 5G Heterogeneous Networks

Hani Alquhayz,[1] Nasser Alalwan,[2] Ahmed Ibrahim Alzahrani,[2] Ali H. Al-Bayatti,[3] and Mhd Saeed Sharif[4]

[1]*Department of Computer Science and Information, College of Science in Zulfi, Majmaah University, Al-Majmaah 11952, Saudi Arabia*
[2]*Department of Computer Science, Community College, King Saud University, Riyadh 11437, Saudi Arabia*
[3]*School of Computer Science and Informatics, De Montfort University, Leicester LE1 9BH, UK*
[4]*School of Architecture, Computing and Engineering, UEL, University Way, Dockland Campus, London E16 2RD, UK*

Correspondence should be addressed to Ahmed Ibrahim Alzahrani; ahmed@ksu.edu.sa and Ali H. Al-Bayatti; aalbay00@gmail.com

Received 13 August 2019; Accepted 23 October 2019; Published 14 November 2019

Guest Editor: Hasan Ali Khattak

Advances in mobile phone technology and the growth of associated networks have been phenomenal over the last decade. Therefore, they have been the focus of much academic research, driven by commercial and end-user demands for increasingly faster technology. The most recent generation of mobile network technology is the fifth generation (5G). 5G networks are expected to launch across the world by 2020 and to work with existing 3G and 4G technologies to provide extreme speed despite being limited to wireless technologies. An alternative network, Y-Communication (Y-Comm), proposes to integrate the current wired and wireless networks, attempting to achieve the main service requirements of 5G by converging the existing networks and providing an improved service anywhere at any time. Quality of service (QoS), vertical handover, and security are some of the technical concerns resulting from this heterogeneity. In addition, it is believed that the Y-Comm convergence will have a greater influence on security than was the case with the previous long-term evolution (LTE) 4G networks and with future 5G networks. The purpose of this research is to satisfy the security recommendations for 5G mobile networks. This research provides a policy-based security management system, ensuring that end-user devices cannot be used as weapons or tools of attack, for example, IP spoofing and man-in-the-middle (MITM) attacks. The results are promising, with a low disconnection rate of less than 4% and 7%. This shows the system to be robust and reliable.

1. Introduction

5G is the fifth-generation cellular network technology, and the International Telecommunication Union (ITU) has designated the International Mobile Telecommunications-Advanced (IMT-Advanced) standard as the global standard for 5G wireless communications. The ITU Radiocommunication Sector (ITU-R) has specified that 5G must [1]

(i) Provide features such as high mobility
(ii) Be ultrareliable and have ultralow latency (1 ms)
(iii) Have a high peak data rate of 10–20 GB

Many 5G providers are attempting to build systems that satisfy these requirements, particularly high speed, but these lack convergence between wireless and wired networks. However, Y-Communication (Y-Comm) architecture, developed at Cambridge University, allows for heterogeneous networking. It consists of a fast core network and a slower peripheral network [2].

Our system includes optical networks and peripheral networks and uses wireless technologies such as 5G [3], which is the main component of the core network. The current security weaknesses in 4G have been investigated thoroughly in [4–6]. However, to date, there are no real

security provisions for 5G heterogeneous mobile networks. Y-Comm includes a security solution that uses a multilayer security system, but research has demonstrated that several security threats could result in service interruption and the expropriation of data.

The research has further demonstrated that current and new perceived threats to security are intrinsic to 5G technology [7]. ETH Zurich, the University of Lorraine/INRIA, and the University of Dundee found that criminals will be able to intercept 5G communications and steal data due to multiple security gaps. According to a press release issued by the group, this is in part because "security goals are underspecified" and there is a "lack of precision" [8]. Therefore, the security specifications of 5G heterogeneous networks can be classified into two levels; the first is associated with mobile equipment and the second with operator networks. Moreover, a number of mobile equipment security specifications need to be considered, such as guaranteeing a device's integrity, privacy, and confidentiality; ensuring controlled access to data; and preventing the mobile equipment from being stolen or compromised, and the data from then being compromised or used as a tool for aggression. Authentication and authorisation on the interface between the network and the operator have been the main focus of security research carried out on 5G heterogeneous networks.

There is a critical commercial need to create a comprehensive security management system for 5G heterogeneous networks, and we have therefore developed

(i) A policy-based security management system that identifies whether a mobile device has been used as an attacking tool in the Y-Comm environment. This follows ITU-T recommendation M.3400 to deal with security violations in the network.

(ii) A novel intelligent agent (IA) mechanism to detect malicious behaviour in an end-user device.

(iii) A self-managed cell for the Y-Comm network to interact with managed objects. The self-managed cell is represented as a policy feedback loop, which is triggered by the end-user device.

The rest of this paper is structured as follows. Section 2 contains background information about the security problems related to 5G heterogeneous networks, ITU-T recommendations, and policy-based systems. Section 3 presents the critical analysis of related work. Section 4 clarifies the Y-Comm framework. In Section 5, we illustrate the results, and in Section 6, we show the testing performance. Our conclusions will also be presented in Section 7.

2. Background

The following section will discuss all related aspects of this paper, starting with 5G networks and ending with Ponder2 (the second version of Ponder).

2.1. 5G Networks. Information and communication applied sciences have sparked innovations worldwide. The ever-growing ability to instantly transfer and process facts is transforming society in many ways, including online shopping, social interactions, media distribution, e-learning and m-learning, and audio and video communication. Industry and business have been based primarily on technological advancements. In attempting to satisfy increasing user requirements, it is becoming extremely difficult to ignore what is required in next-generation wireless communications [9].

Next-generation 5G wireless communications face a challenge in achieving very high data rates, low latency, an increase in base station capacity, and improved QoS in comparison to current 4G in attempting to satisfy increasing user requirement (LTE) networks.

Major industries, researchers, and vendors have determined the key requirements of the next-generation 5G systems, which are as follows:

(i) Up to 10 Gbps data rates in realistic networks (10a 10-fold increase compared with an LTE network) [7]

(ii) High bandwidth in unit areas compared with 4G [10]

(iii) A massive number of subscribers to connected devices in order to realise the imaginative and prescient Internet of things (IoT) [11]

(iv) 1 ms round trip latency—roughly 10 times less than LTE's 10 ms round trip time;

(v) Wide coverage ("anytime anywhere" connectivity)—5G wireless networks should provide almost 100% coverage

(vi) Reduction in power consumption by almost 90%

With the abovementioned requirements, wireless industries, as well as academia and research companies, have started cooperating regarding the one-of-a-kind aspects of the 5G wireless structure. In 5G, virtually all communication spectrums can be used more efficiently and can be categorised as vertical and horizontal sharing. Vertical sharing refers to spectrum sharing between users of different priority (e.g., primary and secondary), that is, unequal rights of spectrum access. Horizontal sharing is sharing between systems that have the same priorities; namely, different users have equal access rights. If the users in the spectrum adopt the same technology, it is called homogenous horizontal sharing; otherwise, it is called heterogeneous horizontal sharing [12].

2.2. Y-Comm Architecture. A group of researchers from the Networking Research Group at Middlesex University, the Computer Laboratory at Cambridge University, Samsung Research and Deutsche Telekom, introduced the Y-Comm framework. The objective of this framework is to address new challenges in heterogeneous networks. There are challenges in many areas, including the network, device, and application levels. The framework maintains a layered approach and performs as a reference model, as in the Open Systems Interconnection (OSI) reference model [13]. In this study, we propose a security management system for the Y-Comm framework.

Given that different operators will own the future heterogeneous networks, new network operators will be able to join the core network. However, this raises the issue of interoperability between these different operators. ITU-T addresses this issue, recommending a central management entity that works as a regulatory authority with the power to enforce policies in the network and implement service and network-level agreements to control the entire network. Y-Comm follows this concept by proposing a core endpoint to work as an administrative entity to control the peripheral networks [14]. Our proposed policy-based system enforces policies in the Y-Comm architecture using this administrative entity.

Figure 1 shows the structure of the Y-Comm network, which contains the core endpoint at the top and the peripheral networks at the bottom. The peripheral networks provide the service to the end users via access routers (ARs). The middle level contains domains, with each one representing a network operator. The most important components in this research are the central A3C server (CA3C) and the AR. Other components address other issues in the network, such as QoS and handover. The CA3C server is the central authentication, authorisation, accounting, and cost system; it also contains the service-level agreements (SLAs) and network-level agreements (NLAs). SLAs specify the terms on which the clients use the service, and NLAs specify the terms on which the clients access the networks [14]. The AR is the link between the network provider and the end-user device, and it is responsible for enforcing admission control decisions. Additionally, the AR acts as the authenticator for network users after receiving permission from the CA3C server in the core endpoint.

2.3. Analysis of Y-Comm and 5G Networks. Owing to its open nature, the 5G infrastructure can be accessed from a range of external connection points through peer operators, the Internet, and third-party technologies. All these represent security vulnerabilities in the system, and, because service providers use the same core network infrastructure, if a single provider is under threat, this would affect the whole network infrastructure [4]. To overcome such threats, the Y-Comm research group has developed a security system, although the solutions are not comprehensive. Aiash et al. focused their research on the security difficulties found in 4G systems. Their approach to resolving these difficulties involved applying existing security techniques to 4G networks, as they discovered that existing and new security threats were intrinsic only to 4G technology. They examined the idea of applying the authentication and key agreement (AKA) of 3G to a 4G communication framework using standard X.805. By doing this, they were able to analyse the AKA protocol in 4G networks. They consequently discovered a significant number of threats to the network's security [5]. Moreover, Park et al. discovered that because 5G is an IP-based and heterogeneous network, a variety of security threats exist that have the potential to interrupt service and allow data to be expropriated. In addition, they investigated and suggested solutions for a number of ongoing open problems that need to be solved [4].

In a traditional network, security is achieved by not allowing threats to access network entities. However, in a 5G open-architecture network, this is ineffectual because the attackers attempt to discover security vulnerabilities in the operating system, network protocols, and applications, and by exploiting them, they can develop malware that attacks and abuses the network. The new architecture identifies possible threats within a 5G network system, including IP address spoofing, user ID theft, theft of service (ToS), denial of service (DoS), and intrusion attacks. Due to the open architecture and IP-based environment, 5G heterogeneous networks are subject to new security threats and inherit existing threats from the Internet. Given that the network infrastructure was the property of the service providers and access to other network equipment was prohibited, these threats were never present in 3G and 4G networks. In addition, there is an increase in security threats because of the diversity of end-user devices and security levels [15]. Experience relating to Internet protection indicates that protection needs to incorporate data and entities, which suggests that the 5G network should preserve both the entities and infrastructure [4].

An additional security problem arises in mobile communications when an end-user device is disconnected from the network for any reason, for example, if the device has run out of battery. Moving from disconnected to connected status on a mobile device provides an opportunity for an attacker to simulate a mobile device or a mobile support station [3]. The emergence of root kits, malware capable of modifying operating system codes and data for malicious reasons, has made it even more important to protect end-user devices. According to McAfee, the use of root kits has increased by 600% over the last few years [16] and the majority of malware seems to target Android operating systems [17]. Furthermore, new end-user devices are becoming sources of DoS attacks, viruses, and worms, with smart phones becoming attractive targets. As a result, there is an increasing number of harmful social implications that must be addressed. Y-Comm and Hockey have proposed some security solutions for heterogeneous mobile networks. However, these solutions do not consider the security of end-user devices, which are the source of numerous security weaknesses, and do not meet the security standards of 5G systems.

2.4. Policy Overview. This paper details a policy-based system to cover the vulnerabilities in security systems for heterogeneous networks. The convergence between wired and wireless technologies in 5G heterogeneous networks and the diversity of network technologies make managing these networks complex. The intricacies involved have encouraged researchers to find an appropriate network management technique. Policy-based management systems have become promising solutions for controlling such networks. There are various motivations for the recent interest in creating a

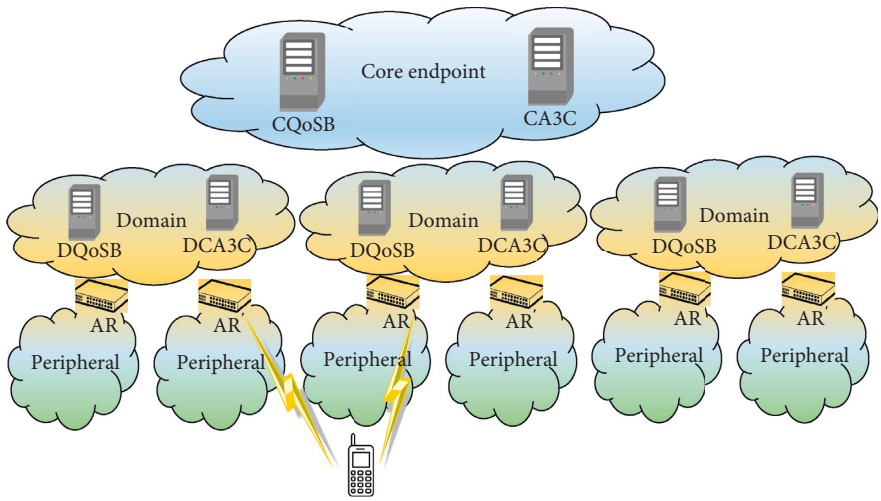


Figure 1: The core endpoint structure with the attached networks.

policy-based management system, for example, those in [18–23]:

(i) It supports the dynamic change of behaviour of the system without the need to halt. This feature suits heterogeneous network services, which should be available at all times without sudden stops or reconfiguration.

(ii) It requires less human effort to administer the network. This is an attractive characteristic when managing large-scale networks with diverse network technologies, such as 5G heterogeneous networks. Therefore, it is important to produce a policy-based system that can also be cost effective for the end user as well.

(iii) It defines the behaviour of large-scale networks or distributed systems. With a significant increase in the number of network users, the number of applications and services required by end users has grown and there is a need to define the rules of using such services and to control the relationship between different network entities. Therefore, it is a difficult task to build a management system. A policy-based management system can help to define policy rules and to enforce them.

(iv) It provides better security. Many network resources are joined in the core network, and protecting these resources from abuse is crucial. Authorised users could abuse these resources if they misuse their network privileges.

The following types of policies are used in this study.

2.4.1. Authorisation Polices. Authorisation policies specify what activities a user can (or cannot) engage in the system. Positive authorisation policies include policies that allow users access. Negative authorisation policies prohibit users from performing actions involving objects in the system [19]. Note that the use of positive and negative authorisation policies may cause conflicts. However, the policy specification language used in this study helps resolve such conflicts. We describe these conflicts and explain how to deal with them in the subsequent sections.

2.4.2. Obligation Policies. Obligation policies specify what the subject in the system must do, if a particular event occurs. Thus, predefined events trigger the security policies to execute actions. This is the basis of event condition action (ECA) rules [19]. Obligation policies have numerous applications, particularly for dealing with security violations. When a security violation occurs, a set of actions is performed to protect the network. In this study, we used such policies to deal with a predefined security violation. The set of actions is based on ITU-T recommendations, which are explained in Section 2.7. The policy specification language used in this study is Ponder2 [20], which helps the obligation policies to work in heterogeneous networks.

2.5. Policy System Selection. The variety of features policy systems such as, Ponder, PDL, XACML, LaSCO, Tower, and Ponder2 influenced the choice of an appropriate system for the working environment in this paper. The features and drawbacks of each policy were considered to determine their suitability to be part of a security management system for 5G heterogeneous networks. Although these policy systems support the main policy types needed for security management purposes, they mainly aimed to manage large distributed systems and networks, as in the case of Ponder and PDL, which are unsuitable for small devices. Ponder2 differs from PDL and Ponder in that it is more flexible and extensible, which suits environments that contain a variety of network technologies and operating systems. In addition, Ponder2 includes PonderTalk, a high-level configuration language, which ensures that the developer of a policy system does not need to know low-level details of various devices. This makes Ponder2 an ideal choice for environments that contain a range of small devices and different network technologies.

2.6. Ponder2. The Ponder2 policy system is appropriate for many environments and applications. It supports flexibility and extensibility, and provides interactivity that allows users to engage with the managed system. The most important feature of Ponder2 is being able to function with various software and hardware components and a wide range of environments, such as local area networks (LANs), wide area networks (WANs), and distributed systems [20].

According to [24], Ponder2 is implemented as a self-managed cell (SMC). An SMC is any hardware or software component capable of performing the required functions autonomously. SMCs have a self-management feature and consist of an administrative domain in the managed system. Ponder2 implements the policy-based system by considering every part in the managed system as a managed object. Managed objects can be anything, including sensors, switches, routers, and end-user devices. The concept of managed objects gives Ponder2 the seamless ability to maintain the various parts of the managed system and to utilise these components for management purposes.

Ponder2 supports both authorisation and obligation policies. Furthermore, an event type in Ponder2 is considered a managed object. An event type specifies the template to represent an event. An event is an instance of an event type and a managed object. The managed object sends a message depending on a timer or the detection of something. Moreover, Ponder2 follows the concept of domains. Domains in Ponder2 are managed objects that consist of other managed objects. The main purpose of domains is to maintain policies in an easier manner, particularly for large-scale systems. This is another capability of Ponder2 that makes it suitable for heterogeneous networks [20].

Ponder2 is a promising policy system, and it has proven to have multiple applications. It has been used in various projects at numerous institutions [22, 24] and has been implemented on different devices, including mobile phones, body sensors, and robots. The research projects in which Ponder2 has been implemented include e-health systems consisting of on-body wireless sensors [24] and self-management frameworks for unmanned autonomous vehicles [25].

2.7. International Telecommunication Union. The ITU-R offers guidelines on how to deal with certain malicious events and the actions that should be taken to protect networks. The ITU-R clearly explains that security management should follow a set of procedures after an attack occurs. We specified policies in this security management system based on these recommendations. Therefore, we focus on the ITU Telecommunication Standardisation Sector (ITU-T) recommendation M.3400 in this section.

M.3400 belongs to the telecommunications management network (TMN) group of recommendations; it provides a list of security management specifications for the TMN management function and states that security management cannot be disconnected from any telecommunication network but must be considered part of TMN management. There are groups of function sets in security management, namely, prevention, detection, containment, and recovery and security administration. We followed the specifications of security management throughout the process of designing and developing our system, and, as noted, there are several function sets. However, in our work, we investigated and utilised those best suited to achieving our security specification requirements.

We consider accessing a user's information more harmful in a Y-Comm network. Stealing user identities is becoming more of a threat in current and future mobile networks due to increased user activity on these networks. In their research study that was part of a Microsoft project investigating smart phone security, Guo et al. [26] explained about that stealing the identities of smart phone users. The danger lies in an attacker behaving like a normal user on the network after stealing the identity of a legitimate user and possibly harming the network resources. This highlights the need for a security solution as part of the network; to detect such malicious behaviour and take action to protect the network resources. In another study, [27] investigated the security of smart phones and concluded that some malicious behaviour damages not only the device itself but also network components. This situation can worsen when the attacker takes full control of the end-user device, thus generating a need for a solution incorporated into network security systems. We believe the increase of user privileges on the network due to the increasing requirements of applications increases the risk to the network associated with identity theft. An attacker who steals a user's identity may also attempt other attacks using this identity.

3. Related Work

In this section, we review the security requirements of 5G networks. Although we attempted to meet security requirements that have not been clearly met in Y-Comm security systems, the proposed security management system is extendable to achieve additional security goals. A number of techniques have been developed in 4G and 5G systems to improve data rates, including multiple-input multiple-output (MIMO) technology [28], full duplex technology [29], adaptive beamforming [28], sectorisation antennas [30], and increased capacity, latency, and QoS. Other techniques have been developed in association with the new radio access network (RAN) [30].

Regarding 5G security systems, Zheng et al. [31] explain that failing to consider devices' security in the early stage will increase the security vulnerability of 5G networks. They introduced five security requirements. Firstly, the integrity of the hardware and software of the mobile device should be protected; secondly, the security system should control access to the data stored on the mobile device. Thirdly, the integrity and confidentiality of the data stored or transported to the network operator should be protected. Fourthly, the security system should protect the users' privacy and identity. Fifthly, the security system should prevent a mobile device from being abused and used as an attack tool. The final requirement is important due to users' increased privileges in terms of network resources. In our proposed

security system, this requirement has been investigated and met. The security requirements of network operators are explained in detail in [31], and we address these requirements in the discussion of Y-Comm security systems in Section 2.1 and Section 2.2.

Different policy-based system use different mechanisms to manage the network and to provide a secure environment. However, as indicated below, the vulnerability of some related work indicates that the Y-Comm heterogeneous environment requires an improved approach.

In [32], a policy-based system is used to automatically manage security policies in a network. The system was designed and developed to reduce human involvement in network management. The system attempts to maintain security as the network changes, and it reconfigures the network if necessary. This is achieved by building an automatic management system to help the system administrators enforce policies because of the high number of changes in the network configurations and the rapid growth of network elements. Such growth makes managing the network difficult. The main component in their system is a policy engine that validates the policies and generates new configuration settings for network elements when policies are violated. However, there is a security challenge in this approach, namely, how to prevent an illegal user from gaining access to the network after the network is reconfigured. This technique is not efficient for an environment such as a Y-Comm network. As explained previously, new service providers can join the core network in Y-Comm, which makes it difficult to install a management console for each network administered. Moreover, installing more components will increase the cost of providing the services, which contradicts the security requirements of 5G networks.

In [33], authors presented a real-time transformation of authorities and dynamic aggregation between dispatched entities, which also engages with a cloud-based invocation, automatically leveraging wide levels of self-management between acting entities. However, the xml-based open standard is helping multiple actors to specify their intentions in a static objective way. Yet, the work is not reflecting clearly on critical attacks such as distributed denial-of-service (DDoS).

Lapiotis et al. [34] extended this approach and proposed a security management system focused on wireless network security issues. They presented a policy-based system architecture that includes a central policy engine, wireless domain policy managers, and local monitors. Their main motivation was the widespread use of wireless LAN, which comes with a significant increase in security risks related to malicious attacks. The researchers assumed that malicious attacks could be initiated by internal network users as well as external attackers. The system proposed by Lapiotis et al. [34] provides features such as protecting the network from new security threats without relying on the latest security mechanisms. However, one question that arises is whether the detection of abnormal traffic is sufficient in considering the demand for a highly open network. Because of the great demand in highly open heterogeneous networks to provide satisfactory services, including high-speed connections anywhere and at any time, their security management system is not suitable for heterogeneous networks. One of the limitations is that they do not indicate what kind of security policies have been enforced nor do they explain the formal validation of policies. This study follows the concept of the policy engine as the brain of the system but with numerous modifications. Furthermore, separating the policy specification from enforcement makes it more dynamic and efficient in an environment such as a Y-Comm network that contains a multilayered security service.

In [35], the authors have proposed a security management system based on an IP address supported by a spatiotemporal role-based access control (STRBAC) model. They divide a network into policy zones to improve the efficiency of policy enforcement. They addressed the numerous changes in dynamic, volatile wireless environments, including the increase in malicious attacks and the diversity of network elements. The introduction of policy zones to represent the location in their model and the role permission given to the end user to access network resources are based on these zones. Figure 2 shows the conceptual framework of the security management system based on policy zones.

The framework consists of six main components: the home agent, the foreign agent, the central authentication and role server, the local role servers, the global policy server, and the distributed wireless policy zone controllers. The local policy server is responsible for enforcing the policy in zones. However, the need for a server in each zone increases the cost and complexity of managing large and diverse networks. Additionally, the concept of dividing the network into policy zones is inefficient because legal network users access the network remotely from outside the controlled policy zones. Moreover, this approach is not scalable for wide networks or for when the current network converges with other networks. They assume that the mobile IP is always specific to a host and does not change from one location to another. This is not applicable when the network is composed of both wired and wireless technologies, such as in Y-Comm network.

In [36], the authors have detailed the security challenges (i.e., end-to-end security, tenant isolation, virtualised security, and security management) faced by 5G networks, particularly multitenant NFV/SDN-enabled 5G access networks. They have proposed a security architecture as an extension to the ETSI VNFV architecture consisting of three main components—a policy-based security management system, service monitoring and analytics systems, and VSFs to achieve the desired security functionality. The security policy manager is in charge of providing best action recommendations by taking events triggered by the service monitoring and analytics (SMA) function as input. The SMA component within the orchestration layer is responsible for performing metrics and notifications acquisition from (i) the NFVI resources, (ii) the VNFs/VSFs, and (iii) the physical infrastructure. A virtualised intrusion detection system (vIDS) or virtualised intrusion prevention system (vIPS) supported by monitoring and analytics is proposed as a security service for different 5G network services to mitigate various attacks, such as DoS. However, the cross-layer security management in 5G is not addressed.

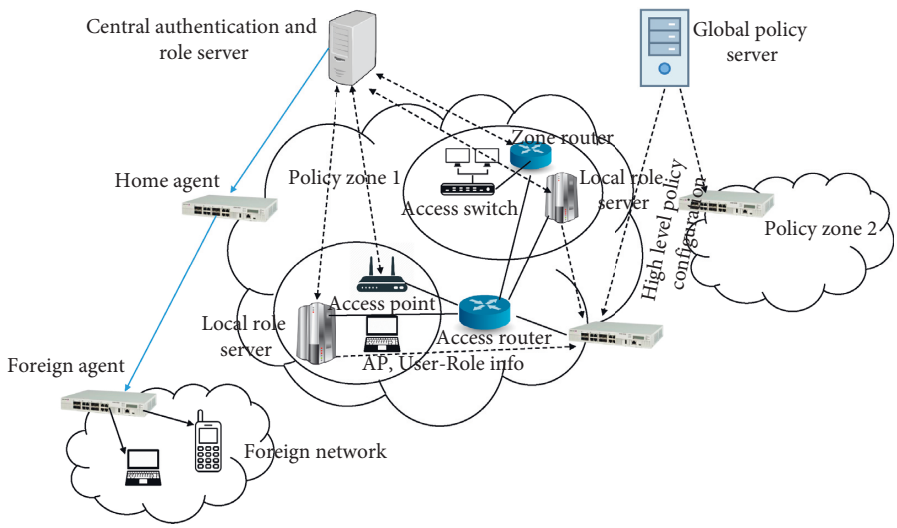


Figure 2: Wireless security management systems [35].

In [37], the authors have presented an automated SLA-driven security management framework (SEVM) for 5G networks and have implemented security services across multiple layers in 5G networks. This enables interaction between cloud service providers and tenants to detect attacks and noncompliance with security-related SLAs. Each cloud service provider has its own SEVM entity with monitoring, correlation, and remediation capabilities. Data are transferred between cloud service providers and tenants to implement security mechanisms against cyberattacks, including DDoS attacks. Events, logs, and correlated data may be exchanged in both directions based on corresponding security SLAs. The SEVM considers the interference between performance and security management and enables cloud service providers to deploy and configure security functions (e.g., firewalls and intrusion prevention systems) under strong performance requirements during the setting up of a service. The SEVM is used to automatically adjust security controls for services during runtime without violating the performance requirements of IoT applications in 5G ecosystems. For control and visibility, SEVM provides security functions (SFs) as a service to tenants, such as verticals, aimed at monitoring VMs and virtual network functions (VNFs) in slices and at correlating all relevant event and log data to detect attacks and anomalies. The SEVM monitors hyphenate SLAs from all tenants, such as security-related key performance indicators (KPIs), aimed at mitigating SLA violations before the tenants are affected.

In [15, 31, 38], the authors have investigated 5G networks and concluded that any future mobile network should meet the essential security requirements. These requirements may share characteristics of other fields in the network or distributed systems. Based on the above, we propose a security management policy-based system featuring mobile ID in the SLA stored in the core server. We enforce policing by using the current network resources without the need for more network equipment. Our system will meet the essential security requirements to provide a secure environment for users and the network, as we prove in the subsequent sections.

4. Framework Overview

As shown in Figure 3, we propose a management layer based on the ITU-T M.3400 recommendation for Y-Comm architecture. The management layer works as a security management system that is able to detect and contain predefined security violations in the network and prevent them from propagating and harming the entire network. Some detection function sets that met our requirements are as follows:

(i) The customer security alarm function set, defined as a set that supports access to a security alarm that indicates security attacks on its portion of the network and supports the detection of security violations in the network

(ii) The investigation of the ToS function set, defined as a set that supports the investigation of customers and internal users whose usage patterns indicate possible fraud or ToS and that helps recognise attacks on mobile equipment

(iii) The software intrusion audit function set, defined as a set that helps check for signs of software intrusion in the network and helps detect whether there has been a violation of the network or the mobile equipment

The M.3400 recommendations include containment and recovery function sets. One example is the exception report action function set, which supports actions to limit security breaches and provides some mechanisms. Another example is the ToS action function set, which helps limit security breaches by removing users' access privileges. We built our policies on these function sets and defined the procedures to follow if a security violation occurs. The procedures for dealing with security violations in terms of policy-based systems are explained further in the following sections.

The security requirements of 5G networks, which are explained in Section 2.3, state that the end-user device should be protected from abuse and the security system

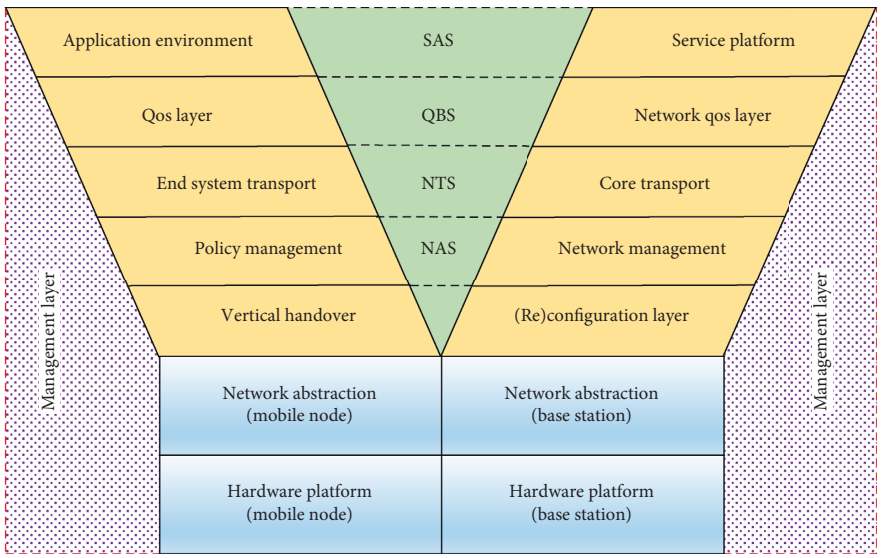


Figure 3: The complete Y-Comm architecture.

should prevent a mobile device that is under attack from being used as an attack tool. This requirement has not been satisfied in the Y-Comm architecture and needs to be addressed, as explained in Section 2.4. The opportunity to attack the network through an end-user device lies in stealing a user's network privileges. These privileges include access to sensitive data, and stealing such data triggers the security management system. The justification of considering this sensitive data is provided in Section 4.2. To detect such a security violation, we propose an intelligent agent (IA) in the end-user device. A full explanation of IA functions is given in subsequent sections.

4.1. Management Layer. The management layer is located vertically along the layers of the Y-Comm architecture. The proposed management layer, shown in Figure 3, is a policy-based system able to interact with the main components of Y-Comm. The management layer is composed of the security management system.

4.2. Security Management System. The main goal of the Security Management System is to detect attacks on the end-user device and to prevent the end-user device being used as an attacking tool. The main components of the system are the IA, security engine (SE), security administrator and security database, as illustrated in Figure 4.

The IA is located in the end-user device that works with the SE to trigger warnings when a security violation occurs. The IA has been designed to follow ITU-T recommendation M.3400. The recommendation suggests that the security management system should monitor internal users in case of ToS, as this theft can be committed with the aim of using the end-user device to attack the network resource. Thus, this important function set meets a key security requirement of 5G heterogeneous networks, which is to protect the network by preventing a legal end-user device from becoming an attack tool.

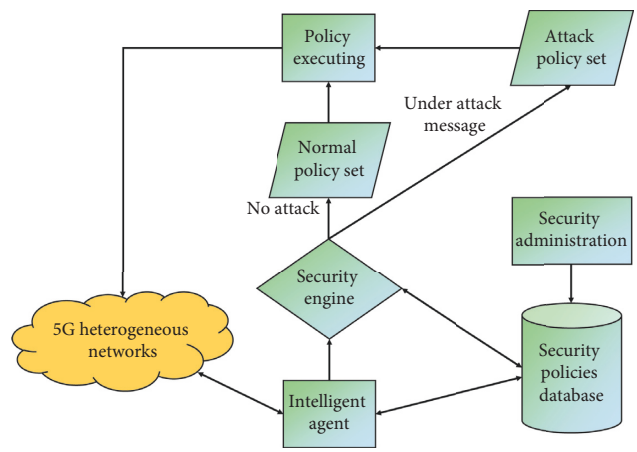


Figure 4: The proposed security management system.

The IA has four main functions:

(i) It collects related information in the end-user device based on the SE's management policies

(ii) It analyses this information and determines whether a malicious event occurred

(iii) It prepares a report and saves changes between previous and collected information

(iv) It sends the report to the SE to make a decision and apply the appropriate policy

The SE obtains information from the IA and makes a decision based on this information. This information can trigger the SE to apply the predefined security policies. In addition, the SE stores this information in the security database for future use. The SE chooses to apply the appropriate policy based on various factors: the type of attack, the type of end-user device, possible vulnerabilities in the same node, and existing records in the database. A significant threat occurs when an attacker attempts to access device configuration files to steal a user's privileges and

attack the network. Such a dangerous attack can harm the network. When the IA detects an attack, the IA warns the SE, which decides to isolate the end-user device. The isolation is based on the exception report action function set, which is part of the ITU-T recommendation, as explained in Section 2.7. The exception report action states that the security management system should limit the security breach using security mechanisms, for example, isolation. This action is taken by interacting with two main components in the Y-Comm architecture, the CA3C server and the related access router. The NLA is stored on the CA3C server, and when the SE removes a user's access privilege, the user cannot move to or access other network providers in the network. However, the user remains connected to the current service provider; therefore, the SE needs to interact with the access router to deny access and isolate the malicious device.

We designed the proposed architecture to contain a security administrator (SA) but have not implemented the SA, and we only explain its function and design factors. We believe that the SA should be automated for several reasons. First, changes in the network topology that mimic human capabilities cannot match the rapid movements in network management. Second, the functioning environment of Y-Comm is designed to allow new networks to join and other networks to extend rapidly [14]. Third, the SA needs to be automated to prevent any malicious attacks after these changes. Dynamic polices are more efficient and responsive to changes, as static policies are known to be limited [34].

4.3. Security Management Case Studies. This section describes how the system components interact in the case of a normal and a malicious event. With a normal event, no security violation or malicious behaviour occurs in the network or end-user device. Therefore, the SE does not need to take any action. However, when a security violation takes place, the IA sends a report to the SE, and the SE keeps a record in the database and executes the appropriate policy, as illustrated in Figure 5.

An end-user device is connected to the 5G heterogeneous Y-Comm network and is able to access network applications and resources; these sensitive privileges are stored as configuration files. Usually, attackers attempt to access these files with the aim of using the end-user device as a cybercrime tool. This kind of attack has occurred previously on GSM and LTE networks [26], and there is a high probability that it will happen on the 5G heterogeneous network. Such an attack will have a devastating effect due to users' increased network privileges and the openness and heterogeneity of the proposed network, as explained in Section 2.3. Our system will provide end-user devices with an IA to detect malicious behaviour and send a message to the SE that contains a mobile equipment identifier (MEID), as well as the attack type, date, and time. The SE applies and enforces the appropriate policies, in this case removing the users' access by modifying the NLA and sending a report to the current domain, which disconnects the end-user device, thus stopping the designated services. The enforcement of policies takes place at two policy-enforcement points, as discussed in Section 4.5. After the enforcement of the policies, the SE maintains a record in the database.

4.4. Policy Enforcement Points. The nature of Y-Comm architecture, based on integrating wired and wireless networks, has increased the difficulty of applying a new approach to this architecture. The security management system used in a wired network does not suit wireless networks because of the host's dynamic topology and mobility. Furthermore, the open nature of Y-Comm means that new network providers can join the core network, which leads to the need for systems that can deal with these new providers at any time. Therefore, the system we propose creates managed objects to deal with components introduced by the new network providers to enforce policies easily. These managed objects allow components to interact with the brain of the system (the SE), regardless of their configuration details. We chose Ponder2 as a tool to implement this system because it allows the creation of managed objects, which makes managing network resources an achievable task regardless of dealing with low-level equipment specifications. In addition, to support deployment of the system, the system creates adaptors using Ponder2. Adaptors in Ponder2 support deployment by allowing interaction between the heterogeneous components and the other managed objects in the system.

The Ponder2 authorisation framework (PAF) provides a way to enforce authorisation policies that can protect both the subject and the target [19] and that support negative and positive authorisation policies. However, this may introduce policy conflict, as discussed in Section 4.6. Figure 6 shows that two policy enforcement points (PEPs) are enforced in the Y-Comm architecture. The proposed security management system enforces PEP1 in the core endpoint and specifically in CA3C, which contains the NLAs. The NLAs contain the users' terms of access to the network services. Therefore, our system interacts with NLAs as managed objects to enforce the policy governing the removal of users' access to the network. This policy enforcement occurs after a security violation is detected that may harm the entire network. The end-user device needs to contact the access router, which obtains permission from the CA3C server in the core endpoint before connecting to the network. However, when removing a user's access to the CA3C server, the end-user device remains connected to the peripheral network. Therefore, another PEP is required. The second PEP is in the access router to stop providing the connection to the end-user device.

4.5. Policy Feedback Loop in the Security Management System. In this section, we discuss the application of a policy feedback loop as part of an SMC. When events trigger the proposed security management system, it analyses these events and applies the appropriate ECA obligation policy. As an extension of the obligation policy, the authorisation policy is forced back on the components of Y-Comm. This loop of interaction between Y-Comm components and the security management system is known as a policy feedback loop.

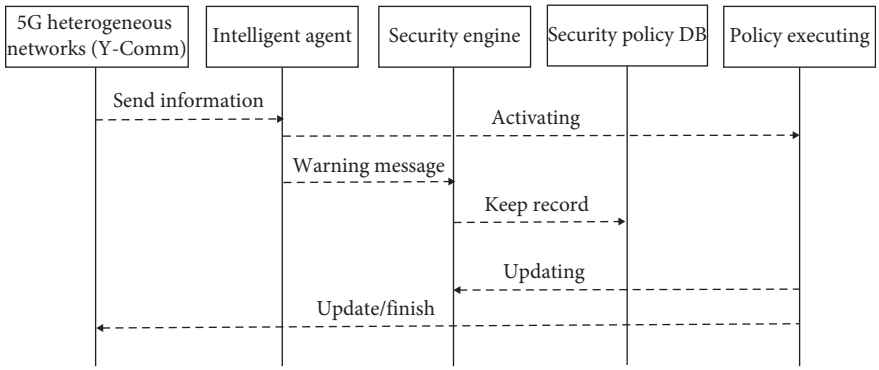


Figure 5: Sequence diagram of security management system (no security violation).

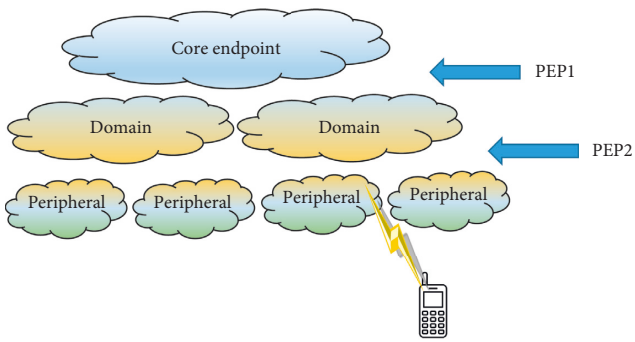


Figure 6: The policy enforcement point in the security management system.

Figure 7 shows the policy feedback loop. It illustrates the cycle of interactions between the Y-Comm network components and the proposed security management system. The Y-Comm components are managed objects, and the first managed object is the end-user device that generated events. Events are transmitted to the SE through the event bus. When the SE receives an event, it determines what decision should be taken based on the event. When the event is malicious, the system takes action based on the obligation policies. The second half of the loop is to enforce authorisation polices on managed objects in the Y-Comm network. The authorisation policies enforce two PEPs on two managed objects, the AR and CA3C. This loop represents the SMC in the system.

4.6. Resolution of Policy Conflict. Policy conflict is a common issue in policy-based systems, but Ponder2 contains features that resolve this issue when it arises in the network. Policy conflicts arise due to errors or conflicting requirements introduced by administrators. Moreover, they occur when two authorisation policies are in conflict with each other, for example, when one permits an activity and another forbids the same activity. Additionally, conflicts occur when diverse management functions apply different policies to objects in the system. Ponder2 provides a strategy for resolving policy conflict by dynamically determining which policy takes precedence. In terms of this strategy, when conflict arises between two policies, the more specific policy takes precedence. Thus, when policy $p1$ for a domain conflicts with policy $p2$ for a subdomain, $p2$ takes precedence. In the Y-Comm structure, if a conflict arises between a policy for a domain, the proposed security management system's policies are specific to a defined end-user device. For example, if a security violation takes place in the end-user device x, the IA detects and reports this violation. The SE then enforces the appropriates policy px. The policy px takes precedence because it is more specific than other polices applied to domains. The example shown in Figure 5 illustrates that the policy px conflicts with policy pa. However, the proposed security management system resolves this conflict using features of Ponder2. Therefore, in this case px takes precedence. This feature in Ponder2 is useful in the proposed security management system and meets the security requirements of 5G heterogeneous networks. Hence, this conflict resolution strategy works during runtime, which makes it more dynamic.

4.7. Specifications of the Security Management System. The approach to the proposed Security Management System is policy-based, and the system acts on two kinds of policies–obligation policies and authorisation policies. Obligation policies are specified in ECA format; thus, policies are specified to respond to events related to security violations. When an event occurs and the condition is true, action is taken to apply the appropriate policy. This integrates the security management system with the Y-Comm network. Moreover, we created managed objects for all the components needed in Y-Comm to ensure interoperability with the proposed system. Similarly, we created the components of the proposed architecture as managed objects to ensure interoperability and the achievement of the systems goals. These managed objects are the EUD, DB, AR, NLA, and the warning managed object.

Algorithm 1 explains how to create an ECA policy and how the security management system interacts with managed objects. In line (1), the system creates the ECA policy to check whether there is a security violation detected by the IA and received as an event. Then, the system receives event line (2), which contains the attributes of the attack type, EUD ID, date, and time. The condition in Ponder2 is expressed as in lines (3) and (4). The system checks whether the condition is satisfied and then activates the policy. When the ECA policy

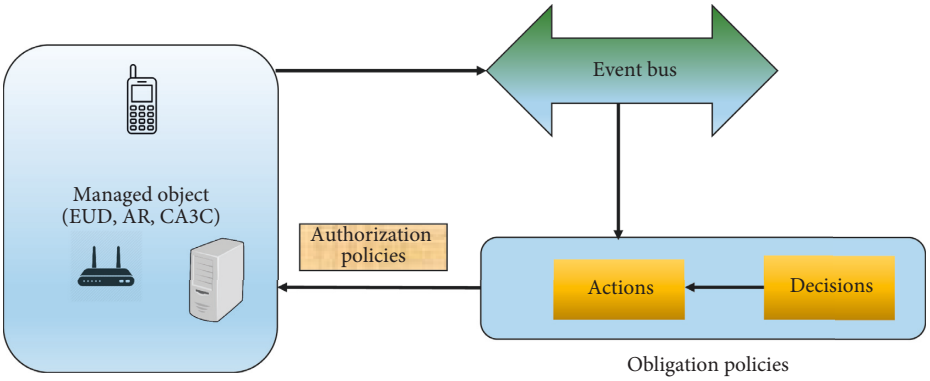


Figure 7: Security management system policy feedback loop.

(1) $Policy \longleftarrow (event, condition, attackType)$
(2) $event \longleftarrow eudValue$
(3) $condition \longleftarrow [: eudID : AttackType : Date : Time]$
(4) $attackType \longleftarrow$ "ConfigAccess"
(5) $print :$ "Checking End User Device"
(6) $Policyaction \longleftarrow (Record, Remove\ Access, Stop\ Access, Warning, ConfigureAccess)$
(7) $Record \longleftarrow (eudID, Attack\ Type, Date, Time)$
(8) $Remove\ Access \longleftarrow eudID$
(9) $Stop\ Access \longleftarrow eudID$
(10) $Set\ Warning \longleftarrow true; show$
(11) $Configure\ Access \longleftarrow Policy$
(12) $Activate\ Policy\ :\ true$

Algorithm 1: ECA policy in the security management system.

is activated, the actions include four main steps. Firstly, the system keeps a record in the database and sends the four attributes to the DB managed object. Secondly, it interacts with the NLA managed objects and executes the function of revoking the user's access. In addition, it sends the EUD ID to the NLA managed object, as shown in line (7). Thirdly, the system interacts with the AR managed object to activate the function stop access, which means stop providing the service to this EUD, and sends the EUD ID. Fourthly, the system warns the system administrator of the event through the warning managed object, as shown in line (9).

Algorithm 2 illustrates the creation of an event received from the EUD managed object. The system loads the events in the event bus to interoperate with the ECA policy. The system creates the event template first and then defines the attributes of the event, as indicated in line (1), before readying the template for loading. This step is necessary to allow the ECA policy to invoke the attributes of events and check their values when an event occurs. These two algorithms show how the system employs the features of Ponder2 to deal with Y-Comm components.

5. Results

After the event generator produces random cases to test the system's ability to respond to malicious acts, the system responds to these events and enforces the required policy. The core aspect of the system is how these managed objects interoperate to achieve the security requirements. Figure 8 shows a snapshot of the system after it responds to a malicious event.

Figure 8 shows that the system performed the main steps after detecting the malicious event. It activated the policy to deny the user access and kept a record containing all details of the event. The system captures details of malicious events to allow the analysis of these events and the extension of the system. The system creates an output file to store the details of malicious events that occur in the network, as illustrated in Table 1.

As shown in Table 1, the output file contains details of the date, time and type of attack. In addition, it contains the ID of the targeted EUD in case the need arises to collect further information from the IA in the future.

6. Testing Performance

We simulate our security management system with a focus on two kind of attacks, IP spoofing and MITM attacks, which target data and control channels in 5G networks.

The system was simulated using a Mininet emulator for both attacks. As part of the setup, we considered both light and dense configuration. Light configuration with 80 nodes and dense configuration with 400 nodes, also, as a measure

(1) $template \longleftarrow (eudID, attackType, attack\,Date, attackTime)$
(2) $maliciousEvent \longleftarrow template$

Algorithm 2: Event template of the security management system.

Figure 8: Snapshot of the security management system after detecting a malicious event.

Table 1: Snapshot of security management system after detecting a malicious event.

EUD ID	Attack type	Data	Time
458X87T88	CONFIGACS	07/07/2019	12:24
359R87598	CONFIGACS	07/07/2019	13:43
287Q9R54Y	CONFIGACS	07/07/2019	14:14
E95T1X4W6	IPSPOOF	07/07/2019	14:54
93Q1C4E4L	CONFIGACS	08/07/2019	08:21
87W4C27YU	IPSPOOF	08/07/2019	10:05
97GKI3213	IPSPOOF	09/07/2019	10:06
96QAZ123D	CONFIGACS	09/07/2019	11:31
2DQ76XZ51	CONFIGACS	09/07/2019	13:19

of performance, the disconnect rate will be the deciding indicator. This is derived as follows:

$$r = \frac{\mathrm{no}_{\mathrm{ds}}}{100}, \tag{1}$$

where $\mathrm{no}_{\mathrm{ds}}$ is the disconnect rate in the simulation environment. As part of the scenario, the attacker will be able to eavesdropping on the communication channel. When authentication is granted, the attacker can launch their own attacks targeting two adjacent nodes from their own device. To test various scenarios, 0 to 400 attacks were carried out and the disconnect rate was examined to test the feasibility of our system. As shown in Figure 9, the simulation results highlight that the system is robust against IP spoofing attacks. Even when the number of attacks increased to 500, the system showed proper resistance and managed to keep the disconnect rate fairly low.

As shown in Figure 10, similar to the IP spoofing, the simulation results highlight that MITM attacks are lower than 4%, showing a good level of response to such threats. In terms of performance, we can confidently state that the system fulfils the main security needs, such as availability and reliability.

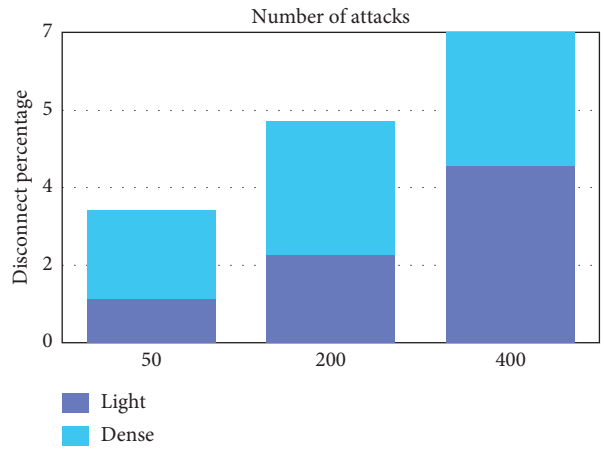


Figure 9: Performance under IP spoofing.

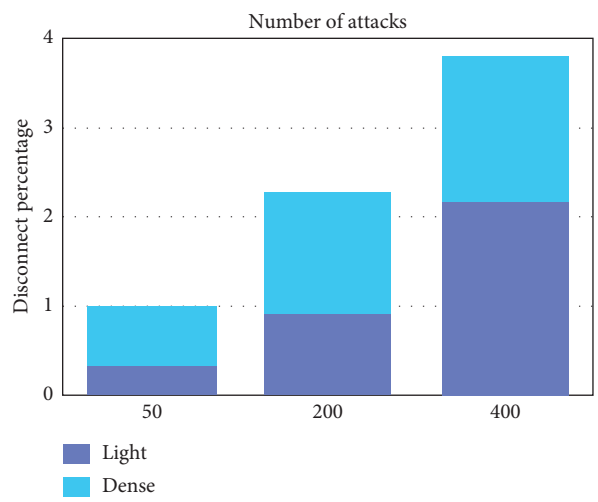


Figure 10: Performance under MITM.

7. Conclusion and Future Work

In this paper, we present an ITU-T-based Y-Comm security management network with 5G capabilities that integrates current wired and wireless networks. The main responsibility is to deliver QoS, vertical handover and heterogeneity without any major interruption of services. The results clearly demonstrate that the proposed security management system can satisfy security needs in the Y-Comm context. The deployment of the proposed system is possible with managed objects built for all components of Y-Comm using Ponder2. In addition, the system was tested against attacks, for instance, IP spoofing and MITM. The results are promising, with a low disconnection rate of less than 4% and 7%. This indicates the system is robust and reliable. The future aim is to compute

wrapping codes for components of the Y-Comm network, so they are able to interpret PonderTalk messages and complete tasks for security management purposes to propose a mechanism that gives isolated end-user devices their privileges back.

Data Availability

All data are available upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was funded by the Deanship of Scientific Research at King Saud University with grant number RG-1438-062.

References

[1] ITU, *ITU Towards "IMT for 2020 and Beyond"*, 2018, https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx.

[2] G. E. Mapp, F. Shaikh, D. Cottingham, J. Crowcroft, and J. Baliosian, "Y-Comm: a global architecture for heterogeneous networking," in *Proceedings of the 3rd International Conference on Wireless Internet; ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering): ICST*, pp. 22:1–22:5, Brussels, Belgium, 2007.

[3] T. Hardjono and J. Seberry, "Information security issues in mobile computing," in *Proceedings of the IFIP TC11 Eleventh International Conference on Information Security, IFIP/Sec '95*, pp. 143–151, Springer, Boston, MA, USA, 1995.

[4] Y. Park and T. Park, "A survey of security threats on 4G networks," in *Proceedings of the IEEE Globecom Workshops*, pp. 1–6, Washington, DC, USA, November 2007.

[5] M. Aiash, G. Mapp, A. Lasebae, and R. Phan, "Providing security in 4G systems: unveiling the challenges," in *Proceedings of the Sixth Advanced International Conference on Telecommunications*, pp. 439–444, Barcelona, Spain, May 2010.

[6] H. Alquhayz, A. Al-Bayatti, and A. Platt, "Security management system for 4G heterogeneous networks," in *Proceedings of the World Congress on Engineering, WCE*, vol. 2, pp. 52–55, London, UK, July 2012.

[7] J. G. Andrews, S. Buzzi, W. Choi et al., "What will 5G Be?," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1065–1082, 2014.

[8] P. Nelson, *5G and 6G Wireless Technologies Have Security Issues*, Network World, Boston, MA, USA, 2018, https://www.idginsiderpro.com/article/3315626/5g-and-6g-wireless-technologies-have-security-issues.html.

[9] A. Hammoodi, L. Audah, and M. A. Taher, "Green coexistence for 5G waveform candidates: a review," *IEEE Access*, vol. 7, pp. 10103–10126, 2019.

[10] S. Chen and J. Zhao, "The requirements, challenges, and technologies for 5G of terrestrial mobile telecommunication," *IEEE Communications Magazine*, vol. 52, pp. 36–43, 2014.

[11] N. Tariq, M. Asim, F. Al-Obeidat et al., "The security of big data in fog-enabled IoT applications including blockchain: a survey," *Sensors*, vol. 19, 2019.

[12] T. Alexander, W. Mazurczyk, A. Mishra, and A. Perotti, "Mobile communications and networks," *IEEE Communications Magazine*, vol. 57, no. 4, p. 94, 2019.

[13] G. Mapp, F. Shaikh, M. Aiash, R. P. Vanni, M. Augusto, and E. Moreira, "Exploring efficient imperative handover mechanisms for heterogeneous wireless networks," in *Proceedings of the International Conference on Network-Based Information Systems*, pp. 286–291, Indianapolis, IN, USA, August 2009.

[14] M. Aiash, G. Mapp, A. Lasebae, R. Phan, and J. Loo, "A formally verified AKA protocol for vertical handover in heterogeneous environments using Casper/FDR," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, p. 57, 2012.

[15] N. Seddigh, B. Nandy, R. Makkar, and J. F. Beaumont, "Security advances and challenges in 4G wireless networks," in *Proceedings of the Eighth International Conference on Privacy, Security and Trust*, pp. 62–71, Ottawa, Canada, August 2010.

[16] J. Bickford, R. O'Hare, A. Baliga, V. Ganapathy, and L. Iftode, "Rootkits on smart phones: attacks, implications and opportunities," in *Proceedings of the Eleventh Workshop on Mobile Computing Systems Applications*, pp. 49–54, New York, NY, USA, 2010.

[17] T. Greene, "McAfee: Android is sole target of new mobile malware in Q3," in *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications*, New York, NY, USA, 2011.

[18] J. Strassner, "Chapter 4-policy operation in a PBNM system," in *Policy-Based Network Management, the Morgan Kaufmann Series in Networking*, J. Strassner, Ed., Morgan Kaufmann, Burlington, VT, USA, 2004.

[19] K. Twidle, N. Dulay, E. Lupu, and M. Sloman, "Ponder2: a policy system for autonomous pervasive environments," in *Proceedings of the Fifth International Conference on Autonomic and Autonomous Systems*, pp. 330–335, Valencia, Spain, April 2009.

[20] J. Zhou, Q. Shen, and Y. Xu, "Research and improvement of Ponder2 policy language," in *Proceedings of the 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE)*, vol. 2, pp. 455–458, Zhangjiajie, China, May 2012.

[21] R. Neisse, P. D. Costa, M. Wegdam, and M. Sinderen, "An information model and architecture for context-aware management domains," in *Proceedings of the IEEE Workshop on Policies for Distributed Systems and Networks*, pp. 162–169, Palisades, NY, USA, June 2008.

[22] H. Zhao, J. Lobo, and S. M. Bellovin, "An algebra for integration and analysis of Ponder2 policies," in *Proceedings of the IEEE Workshop on Policies for Distributed Systems and Networks*, pp. 74–77, Palisades, NY, USA, June 2008.

[23] M. Asim, A. Yautsiukhin, A. D. Brucker, T. Baker, Q. Shi, and B. Lempereur, "Security policy monitoring of BPMN-based service compositions," *Journal of Software: Evolution and Process*, vol. 30, no. 9, Article ID e1944, 2018.

[24] E. Lupu, N. Dulay, M. Sloman et al., "AMUSE: autonomic management of ubiquitous e-Health systems," *Concurrency and Computation: Practice and Experience*, vol. 20, no. 3, pp. 277–295, 2008.

[25] E. Asmare and M. Sloman, "Self-management framework for unmanned autonomous vehicles," in *Proceedings of the 1st International Conference on Autonomous Infrastructure, Management and Security: Inter-Domain Management*,

pp. 164–167, Springer-Verlag, Berlin, Heidelberg, Germany, 2007.

[26] C. Guo, J. Helen, and W. Z. Wang, *Smart-Phone Attacks and Defenses, HotNeT III*, 2004.

[27] S. Töyssy and M. Helenius, "About malicious software in smartphones," *Journal in Computer Virology*, vol. 2, no. 2, pp. 109–119, 2006.

[28] F. W. Vook, A. Ghosh, and T. A. Thomas, "MIMO and beamforming solutions for 5G technology," in *Proceedings of the IEEE MTT-S International Microwave Symposium (IMS2014)*, pp. 1–4, Tampa, FL, USA, June 2014.

[29] S. Goyal, P. Liu, S. S. Panwar, R. A. Difazio, R. Yang, and E. Bala, "Full duplex cellular systems: will doubling interference prevent doubling capacity?," *IEEE Communications Magazine*, vol. 53, no. 5, pp. 121–127, 2015.

[30] H. Kim, I. Jung, Y. Park, W. Chung, S. Choi, and D. Hong, "Time spread-windowed OFDM for spectral efficiency improvement," *IEEE Wireless Communications Letters*, vol. 7, no. 5, pp. 696–699, 2018.

[31] Y. Zheng, D. He, W. Yu, and X. Tang, "Trusted computing-based security architecture for 4G mobile networks," in *Proceedings of the Sixth International Conference on Parallel and Distributed Computing Applications and Technologies (PDCAT'05)*, pp. 251–255, Dalian, China, December 2005.

[32] J. Burns, A. Cheng, P. Gurung et al., "Automatic management of network security policy," in *Proceedings of the DARPA Information Survivability Conference and Exposition II. DISCEX'01*, vol. 2, pp. 12–26, Anaheim, CA, USA, June 2001.

[33] Y. Karam, T. Baker, and A. Taleb-Bendiab, "Security support for intention driven elastic cloud computing," in *Proceedings of the Sixth UKSim/AMSS European Symposium on Computer Modeling and Simulation*, pp. 67–73, Malta, November 2012.

[34] G. Lapiotis, S. Das, and F. Anjum, "A policy-based approach to wireless LAN security management," in *Proceedings of the Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks*, pp. 181–189, Athens, Greece, September 2005.

[35] S. Maity, P. Bera, and S. K. Ghosh, "A mobile IP based WLAN security management framework with reconfigurable hardware acceleration," in *Proceedings of the 3rd International Conference on Security of Information and Networks*, pp. 218–223, New York, NY, USA, 2010.

[36] M. S. Siddiqui, E. Escalona, E. Trouva et al., "Policy based virtualised security architecture for SDN/NFV enabled 5G access networks," in *Proceedings of the IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, pp. 44–49, Palo Alto, CA, USA, November 2016.

[37] I. Adam and J. Ping, "Framework for security event management in 5G," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pp. 51: 1–51:7, New York, NY, USA, 2018.

[38] K. H. Y. uk Yu Hui, "Challenges in the migration to 4G mobile systems," *IEEE Communications Magazine*, vol. 41, pp. 54–59, 2003.