Research Article

An Efficient and Secure Session Key Management Scheme in Wireless Sensor Network

Gulzar Mehmood¹, **Muhammad Sohail Khan**², **Abdul Waheed**^{3,4}, **Mahdi Zareei**⁵,
Muhammad Fayaz⁶, **Tariq Sadad**⁷, **Nazri Kama**⁸, and **Azri Azmi**⁸

¹Department of Computer Science and Information Technology, University of Malakand, Chakdara 23021, Pakistan

²ISPaR (Institute of Social Policy and Research, Peshawar), Department of Computer Science, Bacha Khan University, Charsadda 24420, Pakistan

³Department of Information Technology, Hazara University, Mansehra 21120, Pakistan

⁴School of Electrical and Computer Engineering, Seoul National University, Seoul 08826, Republic of Korea

⁵Tecnologico de Monterrey, School of Engineering and Sciences, Monterrey 45201, Mexico

⁶Department of Computer Science, University of Central Asia, Naryn, Kyrgyzstan

⁷Department of Computer Science and Software Engineering, International Islamic University, Islamabad 44000, Pakistan

⁸Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Kuala Lumpur 54100, Malaysia

Correspondence should be addressed to Mahdi Zareei; m.zareei@ieee.org

Received 13 April 2021; Revised 1 June 2021; Accepted 4 June 2021; Published 14 June 2021

Academic Editor: Dimitri Volchenkov

Copyright © 2021 Gulzar Mehmood et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Wireless Sensor Network (WSN) is a particular network built from small sensor nodes. These sensor nodes have unique features. That is, it can sense and process data in WSN. WSN has tremendous applications in many fields. Despite the significance of WSN, this kind of network faced several issues. The biggest problems rising in WSN are energy consumption and security. Robust security development is needed to cope with WSN applications. For security purposes in WSN, cryptography techniques are very favorable. However, WSN has resource limitations, which is the main problem in applying any security scheme. Hence, if we are using the cryptography scheme in WSN, we must first guarantee that it must be energy-efficient. Thus, we proposed a secure hybrid session key management scheme for WSN. In this scheme, the major steps of public key cryptography are minimized, and much of the operations are based on symmetric key cryptography. This strategy extensively reduces the energy consumption of WSN and ensures optimum security. The proposed scheme is implemented, and their analysis is performed using different parameters with benchmark schemes. We concluded that the proposed scheme is energy-efficient and outperforms the available benchmark schemes. Furthermore, it provides an effective platform for secure key agreements and management in the WSN environment.

1. Introduction

The world economy is rapidly growing due to the rapid development in technology. In the market, new technologies are introduced every day which facilitates human being different and each new technology tries to advance human lives. That provides a new amazing way that human accomplishes their activities. Each field of life needs technological assistances technique for proficient performance. The

renowned areas where technical testing is conducted and has prodigious influences include wireless communication, educational process, sports activity monitoring, military surveillance industries automation, and healthcare structure [1, 2].

The well-known medium of information exchange is communication. Wireless communication is growing its application to a new broader domain. This new communication technology introduced a new way of

communication named the Wireless Sensor Network (WSN). WSN is the most growing technology and has numerous significant applications in several fields. This technology made the connection between objects easier. It provides robustness in communication due to which helpful information is shared between entities easily. WSN comprises a large number of sensor nodes. These sensor nodes are deployed in the targeted area for activity monitoring. That covers the specific territory where vital signs are collected from the target area. These tiny sensor nodes can sense, process, communicate, and aggregate the collected data. To avoid the issue of line of sight communication in this network, multihop communication is adopted. The main components of WSN include sensor nodes, a base station (BS), and an area under observation [3, 4]. WSN performed two essential tasks: monitoring and target tracking. Tracking applications of WSN contain tracking of different things like animal tracking in the forest or tracking the activities of humans [5, 6]. The small's nodes of WSN are deployed without human intervention.

Additionally, these nodes have the ability to self-organization because human intervention is sometimes not practicable. The small sensor nodes perform sensing, processing, and data transmission. The main components of a sensor node are the power unit, memory unit, and processor. The main issue with WSN is energy consumption because in a harsh environment, battery is not replaceable [7].

There are various research issues related to WSN. Some of the common problems in WSN are architecture of WSN, optimized energy-efficient methodology, effective topology, and effective security management. Security is a significantly rising research issue in WSN because of the sensitive data it deals with and monitors [8]. We need effective schemes that ensure security and energy efficiency. There are many attacks for which a robust security solution is required to secure WSN. However, the energy resource of WSN is typically minimum in amount. Consequently, the different security protocols are not directly applicable to overcome various security issues. The state-of-the-art security schemes need more resources. Planetary security and cryptographic schemes are basically for standard wire and ad hoc networks. Still, the foremost issue is that how we can use these protocols for the WSN platform. The optimum level of use of these protocols for security insurances is a challenging issue.

The main motivation of this research work is that WSN monitors different activities; most of them are very sensitive. Therefore, we need a robust security scheme for these activities. In the paper, we use a cryptographic technique to protect sensitive applications for different applications. However, robust security algorithms need much recourse, such as adequate memory, bandwidth, and energy resources. Therefore, it is challenging to apply any robust cryptographic algorithm in a resource constraint WSN that reduces the resources' capabilities [9]. Furthermore, trust management between sensor nodes with crucial management in a dynamic environment performs packet delivery and average delay. Moreover, the privacy of data is efficiently protected [10].

WSN security can be ensured in several ways. Among all, cryptography is the most powerful technique to ensure the security of the system. Key management is the heart of any cryptography technique. Key management is accomplished in two broad methods that are symmetric key and asymmetric key cryptography. Symmetric key cryptography has its advantages. However, asymmetric key cryptography has the benefits of scalability and better security. Apart from their edges, both types have their shortcomings, such as the symmetric key cryptography scheme has not guaranteed the complete security of WSN [11, 12]. To sidestep these problems in this paper, a new hybrid key management scheme has been proposed. The proposed system provides better security for the WSN environment. Adding to this, it consumes less amount of energy of the network with minimum delay. This approach is very efficient and beneficial, which can be adopted in various frameworks. The key advantage of the proposed scheme is that if a particular sensor node has been compromised or if any hacker recognizes some value of the session key, they could not forecast the upcoming anticipated session key values. The novelty of the proposed scheme is that the proposed scheme used public key cryptography at an optimum level due to which limited resources of WSN are utilized for a longer time.

The remaining paper is organized as follows: In Section 2, a comprehensive survey of related work is presented. Section 3 presents the model of the proposed scheme. In Section 4, the detailed simulation analysis of the proposed scheme is given. Lastly, in Section 5, the conclusion of the proposed work and future directions are given.

2. Literature Survey

In this section, a detailed survey of the most relevant research work has been presented. Mainly, that literature includes those schemes which have a significant concern with the proposed scheme. Various important algorithms for key management in WSN are reviewed critically. After a comprehensive review, several research flaws are pointed out in the given literature. Based on the shortcoming highlighted in the literature survey, a new efficient key agreement scheme has been proposed. Some of the notable schemes and protocols are presented below.

Tang et al. [13] proposed a group key agreement scheme based on elliptic curve cryptography in WSN. The proposed protocol provides implicit verification of sensor nodes. The key contributions of the proposed protocol are low communication and computation cost. However, the proposed work's main issue is that each node is involved in complex security operations. Thus, the overall computation cost is extraordinary and affects the overall performance of the scheme. Zhang et al. [14] proposed a unique group key agreement protocol in the WSN scenario. The proposed technique accomplishes session key management in an efficient very.

Moreover, the proposed scheme prescribes various passive/active attacks inside the network and guarantees forward and backward secrecy. Additionally, in the given scenario, restoring the key computation is challenging. Due

to this reason, it is difficult for any hacker to get secret key information. However, the main issue in this work is that the clustering method utilized many resources of the WSN.

Nagalgaonkar Pramod and Ranjit Sharnappa [15] proposed a protocol using round optimization and authentication Group Key Agreement (GKA). The proposed protocol certifies the group key agreement in WSN. Furthermore, the total number of rounds in the scheme is minimized. Thus, the computation cost decreases significantly. The network computing complexity is also improved. However, the GKA protocol adds computation overhead inside the network. Likewise, Abi-Char et al. [16] proposed a scheme for secure key management in WSN. The proposed method used Elliptic Curve Cryptography for key management. The proposed work ensures authentication and secure key management. Moreover, protection is given against various kinds of security attacks. The proposed scheme uses a new method based on the discrete logarithmic problem that offers greater security.

Meingast et al. and Singelee et al. [17, 18] proposed schemes that handled group session keys among sensor nodes and their server. The base of the proposed work is well-known symmetric key encryption AES. From the comprehensive reviews of the proposed work, it is clear that these schemes are very efficient in cost and security. However, the main issue in these schemes AES decryption is performed at the base station (BS). Hence, appropriate authentication of the sensor nodes is challenging in a given WSN environment. Ertual and Lu [19, 20] proposed schemes based on ECC cryptography and the Alike algorithm for the IoT platform. Threshold cryptography is an energy-efficient mechanism that is used for energy optimization. That consumes minimum energy and provides trust between the sensor nodes. Also, ECC-based cryptography is an excellent key management algorithm. In this paper, performances are evaluated of the RSA and ECC-based algorithms. The output results attested that the ECC-based algorithm gives paramount results to the RSA-based algorithm. However, still using RSA for the same algorithm in the IoT domain utilized various network resources.

Eldefrawy et al. [21] proposed a key agreement scheme for the WSN platform. The proposed work session key is established between sensor nodes and the gateway (GW) for a specific time. Whenever alteration or any fault occurs in the network, the session key is redeveloped for a particular session of time. Thus forward secrecy is ensured. Besides, the proposed scheme offers implicit authentication of the nodes in WSN. It ensures that no other nodes are involved in WSN specific sessions; e.g., S_i does not know the expected secret session key. The proposed scheme can be scalable and offer protection against any error in the network. However, the main issues in this work are high communication and computation costs. Wu and Stinson [22] proposed an algorithm for secure message communication named Multipath Key Establishment (MPKE). That capture active attacks and gives a safeguard against many severe attacks in communication in WSN. The main benefit of the proposed research work is the secure and reliable transmission of information. For secure session key agreement, Reed-

Solomon codes have been used where each round is accomplished using the protocol for Perfectly Secure Message Transmission (PSMT). The limitation in this research work is that the key agreement steps are not clearly elaborated. Thus, not effective and energy-efficient for resource constraint WSNs.

Mehmood et al. [12] propose a scheme for session key agreement with rekeying in WBANs for healthcare applications. This scheme's main contribution is tested in heterogeneous WSN applications, which can be tested for homogeneous WSN for better results. However, if the proposed scheme is validated using a mathematical model, it will be given a robust model. Ali et al. [23] proposed a Diffie-Hellman-based cryptography scheme for WSN. The modified Diffie-Hellman approach is used for secure and efficient key generation, which prevents man-in-the-middle attacks. This approach is analyzed in terms of the security operation, key generation, and computation time for various data packets and efficient results. However, the proposed scheme has high data response time or computation time.

Some latest exciting research schemes have been proposed in other related fields for security and privacy preservation. This research work used cryptographic techniques, most especially the ECC (Elliptic Curve Cryptography) technique, because it has low computation complexity for cryptographic operations. Moreover, the energy consumption and communication costs of these schemes are very low [24–30]. The comprehensive review of the related research work proposed by authors is studied and analyzed in this section for efficient key management in WSN. From the critical study of the research work, it has been concluded that asymmetric cryptography algorithms are highly appropriate for vital data communication security. However, asymmetric cryptography algorithms can also be used for the security of essential operations. In major steps, heavy operations are viable and necessary for strong security preservation. Similarly, symmetric key algorithms have been widely used. However, symmetric key management algorithms are not so much capable of protecting against many attacks. However, the main issue with public key cryptographic algorithms is that we cannot adopt them directly for resource constraint WSN. Nevertheless, we can use them professionally at a different phase, where heavy processes are reduced significantly.

3. The Proposed Model

In this section, the proposed scheme's model is elaborated, and phase-wise descriptions are given in the WSN environment. The proposed scheme uses a clustering approach for efficient network management. Moreover, Cluster Head (CH) is responsible for the major decision within the network. All the details of the different phases of the proposed scheme are explained in subsections. Some of the common assumptions are elaborated below:

- (i) In the proposed scheme, the symmetric and asymmetric cryptography-based hybrid model is used

- (ii) Major operations are minimized; thus, it should be energy-efficient
- (iii) The network lifetime is increased due to the efficient management of our scheme
- (iv) The proposed model is significantly scalable
- (v) The proposed scheme ensures adequate security

3.1. Proposed Scheme. In this section, a novel hybrid key establishment scheme for WSN is presented. The proposed scheme's main benefit achieved less computation cost because most of the operations involve being light-weighted operations that require less energy. In contrast, some processes involve asymmetric cryptography operations involved among Cluster Head (CH) and the Base Station (BS) that needed more power resources. The proposed method is beneficial and highly secure for WSN critical environments. In the WSN scenario, the Base Station (BS) has no resource constraint, so highly complex operations are performed in BS.

In comparison, miner processing is performed on the sensor nodes. Furthermore, in the proposed scheme, we construct ten sensor nodes cluster, and there is a maximum of three clusters. After that, a CH is dynamically selected for each cluster according to LEACH [31]. The sensor nodes communicate with the CH in a cluster, and the CH then further corresponds to the send data to the BS. The BS is the source of secure link establishment within the network. In WSN, the unique identification of each sensor is kept secret. Thus, the proposed scheme ensures secret key management in WSN. That consists of four phases elaborated in the subsequent section: key preloading phase, CH selection phase, session key establishment phase, and rekeying phase.

Moreover, the proposed scheme consists of three clusters named C1, C2, and C3. Each cluster consists of fifteen nodes. The BS retains the planetary of resources. Therefore, BS is responsible for creating a routing Path-Table from those sensor nodes that are involved in WSN topology. The BS provides links to an exterior environment. Then, the collected data are analyzed in other tires and communicated further to the BS.

3.2. Abbreviations and Notations. Table 1 demonstrates some of the notations used for the proposed scheme. Q is the set of a large prime number. Small " b " is the complex number, and D_{bs} is the distance to the BS. D_{si} is the sensor private key D_{si} sensor public key, and R_{si} is the random number generated by a sensor node S_{si} . Similarly, E_k is encryption with the session key, and D_k is decryption with the session key, and so on.

3.3. Proposed Scheme Steps. The proposed scheme consists of four phases, as mentioned above, elaborated in detail in this section. 1st phase is key preloading, in which all the nodes involved in the network load their keys. Then in the 2nd phase, the CH section is accomplished. The 3rd phase is the crucial phase of this scheme in which secure session key

TABLE 1: Abbreviations and notations.

Notation	Description
Q	Q is the large prime number set ($q \geq 2512$)
b	b is the complex number ($b \geq 2512$)
D_{bs}	Base station (BS) private key
P_{bs}	Base station (BS) public key
D_{si}	Sensor node S_i private key
P_{si}	Sensor node S_i public key
R_{si}	Random number generated by a node S_i
PS_k	Presession key
S_k	Session key generated
R_{ch}	Randomly selected number by each CH
R_{bs}	Random set number of the BS
E_k	Encryption with key k
D	Decryption with key k

establishment is performed. Lastly, if any error occurs or the network changes, then rekeying operation has been performed.

3.3.1. Keys Preloading. The first phase of the proposed scheme is the key preloading. In this phase, each sensor S_i is loaded with a public and private key. BS is loaded with the public key of every sensor node present in WSN. Similarly, BS is also loaded with its public and private keys pairs. Table 2 displays the keys loaded to all sensor nodes participating in the WSN environment.

3.3.2. Cluster Head Selection. In the CH selection phase, all clusters select CH for themselves. Thus, for this purpose, the LEACH protocol is used according to the work of [12, 32]. CH is responsible for the key management of sensor nodes involved in a cluster. CH is dynamically changed whenever updates occur in the network. CH is selected accordingly, and we have no concern here for the detail of how CH is selected. However, CH is responsible for the majority of communication with BS. Thus, CH works as a gateway between sensor nodes and BS.

3.3.3. Session Key Establishment Phase. Session key establishment is the important phase of the proposed scheme. We developed the proposed scheme stepwise, and their visual representation is given in Figure 1. Session keys are generated according to the steps taken in this phase. Algorithm 1 presents the actions of the session key establishment. Following are the algorithmic steps taken for session key establishment in WSN.

3.4. Session Key Establishment Algorithm. The algorithm for the session key establishment is described below in detail. The most common notation used in this algorithm is CH, PS_k , S_k , D_{pv} , r_{bs} , and S_i . The rest of the steps are demonstrated as follows:

- (1) CH generates a unique random number rni. Furthermore, it is considered as a presession key, i.e., PS_k

TABLE 2: Preloading of keys.

Base station	Sensors S_i
d_{bs}, P_{bs}, S_{si}	P_{bs}, d_{si}, P_{si}

- (2) CH then encrypts PS_k along with its calculated hash value using the public key of the BS P_{bs} .
- (3) When BS receives this data, it decrypts them with having their private key d_{bs} , i.e. $(PS_k \| h(PS_k))$; here, the integrity of PS_k is also checked.
- (4) BS after this generates a session key as $S_k = PS_k \text{ XOR } r_{bs}$.
- (5) BS then encrypts this session key (S_k) and the hash of that session key $h(S_k)$ using the PS_k and sending that information to each CH involved in WSN.
- (6) The CH Ch_i decrypts the collected information, i.e., the generated session key using presession key PS_k , and the integrity of the session key has been checked.
- (7) After receiving that session key information, CH Ch_i encrypts session key S_k combines it with a hash of session key $h(S_k)$ and sends them to all sensor nodes S_i in the WSN.
- (8) The sensor node S_i decrypts the received information and recovers them by symmetric decryption with key D_{pv} so that the session key for the whole network is communicated securely.

The detail of the algorithm is elaborated and visualized in Figure 1, where communication for session key establishment takes place between sensor nodes, CH and BS. The same procedure and algorithm are also adopted for rekeying phase.

3.5. Rekeying Phase. The operations in rekeying phase are similar to the session key establishment phase. However, the only variation is that for rekeying phase, each CH generates a new random number such as rch . The BS is exceptional and has no link to the earlier random generation generated by CH and BS. Thus, the new generated random number is considered as the new presession key PS_k' . The detailed rekeying algorithm is the same as the session key establishment; therefore, it is not mentioned here due to limited space. However, the pseudocode for rekeying step is presented in Algorithm 2.

The proposed energy-efficient session key establishment scheme can be used for numerous applications of WSNs. Likewise, it can be efficiently adopted in the emerging framework, i.e., smart grade, cloud computing, and IoT.

4. Simulation and Analysis

This section presents the detailed simulation and evaluation of the proposed scheme concerning the relevant system. The simulations are performed in the Omnet++ Castalia simulator. Castalia is a simulation platform suitable for low-power networks such as WSNs and WBANs. Omnet++

simulator is based on C/C++ and contains a sufficient library supporting different functions, i.e., hash function generation and calculating random numbers. Omnet++ simulator has two interfaces; one is used to construct a different structure called module interface. We assume a first-order radio model for energy consumption and communication in the proposed WSN scenario.

In comparison, the other module is used for code development. The important configuration for WSN topology construction is made, consisting of different nodes, i.e., BS, CH, communication. After the necessary background, the simulations are performed in the proposed layout and get a text console. These results are then analyzed and compared with Eldefrawy et al. [21].

All the sensor nodes are homogeneous. The proposed topology comprises of $50 \times 50 \text{ m}^2$ area where 30 nodes are randomly deployed. These sensor nodes are divided into three clusters. In the proposed scenario of the network, three types of nodes exist. Sensor nodes, a small tiny device that performed sensing and communication, are the most secure point and possess rich resources. CH is the type of sensor device that has somehow additional skill than the normal sensor node. Table 3 demonstrates the simulation parameters for the proposed scheme.

4.1. Results Analysis. The results obtained from the simulation are analyzed and evaluated. The proposed session key establishment scheme's output results have been compared with Eldefrawy et al. [21], the most relevant research work. From the simulation and resulting data, which are visualized and compared with the state of the art, the proposed scheme is the best fit in the critical WSN scenario. The resultant graph shows that the presented scheme results are efficient in terms of different parameters. The experiments are performed using several parameters such as communication cost, communication overhead, and network delay. For the experiment, ten nodes are considered in the first round, 20 sensor nodes are considered in the second attempt, and 30 nodes are considering in the 3rd attempt to check their strength and adaptability.

4.2. Bits Exchanges for Session Key Establishment. Bit ratio significantly affects the performance of the WSN and due to which possible fault or congestion arises, due to which real-time communication is affected. The number of bit interchanges for the proposed scheme and Eldefrawy et al. [21] is measured. It is clear from Table 4 that exceeded bits' exchange is happening in the Eldefrawy scheme, which causes greater communication costs of the given WSN scenario. However, the proposed scheme encounters fewer bits during communication, as shown in the table below, during the session key establishment operation. The lower ratio of bit exchanges in the proposed scheme ensures reliable and secure data delivery. Moreover, less energy cost is utilized of WSN. Thus a trusted environment is generated within the network.

FIGURE 1: Scenario of the proposed scheme.

- (1) Start
- (2) Cluster Head $\Rightarrow$ Base Station
- (3) GW $D_{d_{bs}}(PS_k || h(PS_k))$
- (4) Base Station $\Rightarrow$ Cluster Head
- (5) BS $\rightarrow$ CH_i $E_{PS_k}(S_k || h(S_k))$ i.e. $S_k = PS_k = PS_k \text{ XOR } r_{bs}$
- (6) CH_i $D_{PS_k}(S_k || h(S_k))$
- (7) CH_i $\rightarrow$ S_i $E_{P_v}(S_k || h(S_k))$
- (8) S_i $D_{P_v}(S_k || h(S_k))$
- (9) End

ALGORITHM 1: Session key establishment.

- (1) Start
- (2) Cluster Head $\Rightarrow$ Base Station
- (3) CH $\rightarrow$ BS $E_{P_{bs}}(PS'_k || h(PS'_k))$, i.e., $PS'_k = r'_{ch}$
- (4) BS $D_{d_{bs}}(PS'_k || h(PS'_k))$
- (5) Base Station $\Rightarrow$ Cluster Head
- (6) BS $\rightarrow$ CH_i $E_{PS'_k}(S'_k || h(S'_k))$, i.e., $S_k = PS'_k \text{ XOR } r'_{bs}$
- (7) CH $D_{PS'_k}(S'_k || h(S'_k))$
- (8) CH_i $\rightarrow$ S_i $E_{P_v}(S'_k || h(S'_k))$
- (9) S_i $D_{PS}(S'_k || h(S'_k))$
- (10) End

ALGORITHM 2: Rekeying phase.

4.3. Power Consumption. The fundamental attention in the proposed scheme's performance evaluation is on the sensor node's energy consumption. We analyze that how much resources are consumed before and after applying the proposed security algorithm. In the simulation, we initially

take specific constant energy for all sensor nodes. Then the same operation is repeated for a different number of sensor nodes, and results are obtained. The results are then compared for evaluation of the scheme using different parameters.

TABLE 3: Simulation parameter for the proposed scheme.

Parameter	Values
Simulation area	(50 × 50) meter square
Number of nodes	30
Cluster radius	r 50 m
Sensing radius	rs 40 m
The initial energy of the network	1500 μ J
Packet size	40 Bytes
The threshold for receiver Power	-95 dBm
Agent tracer	On

TABLE 4: Number of bits exchange.

Number of nodes	Existing scheme (Kbytes/sec)	Proposed scheme (Kbytes/sec)
10	8.71	3.45
20	17.73	6.36
30	26.95	8.92

4.3.1. Communication Cost. The communication cost is evaluated considering ten nodes, twenty nodes, and thirty nodes respectfully, as shown in Figure 2. The simulation results show that the proposed scheme gives better results than Eldefrawy et al. [21]. The number of major operations has been reduced in the proposed scheme; i.e., the only major operation is involved in session key establishment. That major is accomplished, and the communication takes place between CH and BS. All the remaining operations are slight in the proposed WSN scenario. Figure 2 demonstrates the communication cost of both schemes for session key establishment in WSN. It is clear from the resultant graph that the proposed scheme has better results (less amount of communication cost).

4.3.2. Communication Overhead. WSN has minimal bandwidth, so the core issue related to WSN is decreasing unnecessary communication, which optimized energy consumption. Due to light-weighted operations, the communication cost is minimized significantly. Thus, less communication overhead is encountered. In the three rounds of the simulations, different results are obtained. The results obtained are visualized as shown in Figure 3. This indicates that the proposed scheme transmits fewer number bits during the key establishment phase. Therefore, less amount of overhead is generated in the network.

4.3.3. Computation Cost. Computation is the activity performed by WSN nodes, which is the most technical task. In the proposed session, key establishment phase computation for key generation is the most complex operation. In which the most complex activities are involved. Such actions are squaring and multiplication. In the analysis, we have to consider the QoS parameters; the computation is done in such a way to preserve the privacy of the individual nodes and QoS of data during communication in a critical WSN environment. For session key establishment, two types of

FIGURE 2: Communication cost.

FIGURE 3: Communication overhead.

costs are countable, i.e., the individual computation cost of each sensor node and the cost of communication of each CH for the whole cluster with BS. The simulation results of the proposed scheme with the state-of-the-art comparison are shown in Figure 4.

4.4. Key Establishment Delay. Delay is a critical aspect to be considered for the proposed scheme evaluation. We reduce the number of major operations for session key establishment like asymmetric operations. The only major operation involves CH and BS. All other nodes are in the communication range of CH and belong to that cluster. Therefore, the communication of sensor nodes with their CH is based on symmetric (minor operation). Thus, key establishment delay is minimized significantly. As shown in Figure 5, the proposed scheme's time is less than the stat-of-the-art due to lightweight operations.

4.5. Security Analysis. In this section of the proposed research work, the theoretical security analysis is carried out. It is imperative to analyze the security importance of the proposed scheme. We emphasized that the proposed system is secure as we know that security and privacy preservation in critical WSN are highly essential. In every cryptography scheme, the primary thing is the secret key, which is the

FIGURE 4: Computation cost.

FIGURE 5: Key establishment delay.

heart of any security scheme, which needs to be securely distributed. That is, whenever a new sensor node joins the network, first their integrity and confidentiality will be checked. After that, for different activity different session keys are generated for secure data exchange.

The proposed scheme ensures forward and backward secrecy in the WSN environment. That is because the unique random number has no link with previous randomly generated numbers. R_{si} in each iteration must be unique. The advantage of the proposed scheme is that if a specific node is compromised or if any hacker recognizes some value of the session key, they could not foresee the future expected session key values. Because the session key is generated using a random number, which is unique in every attempt [33].

Moreover, the integrity of any node is checked by calculating the hash value of each step. The calculated hash values are checked and compared with received value. If both give the same result, then we considered that integrity had been ensured. This further substantiates that someone in the middle of communication has not amended the information. If the amendment is done in the information, we can easily trace it using the proposed scheme. Likewise, the

Random number is generated randomly at each iteration. If an attacker attempts any modifications in the value of integrity, integrity will not be compromised due to the Random Oracle Model property.

5. Conclusion and Future Work

Security is the core concern in WSN because it mainly deals with critical data in many applications. Many researchers worked out to guarantee the security of WSN. We know that WSN security is mostly certainly exposed by various attackers. Hence, security is the primary requisite in this kind of network. For the security of WSN, the cryptographic technique is the most efficient and applicable way to protect and manage data. Several solutions have been proposed for wired and wireless networks. However, these schemes cannot apply directly to WSN platform because of the different configurations. The more robust cryptography protocols such as RSA and ECC need exceptional communication and computation costs and other key establishment requirements. The key distribution in the cryptography scheme is a very tough task. That requires an optimized technology that is energy-efficient and ensures proper security. Thus, in this paper, we proposed a light-weighted scheme and provided the secure session key establishment in the WSN environment. Computation and communication costs are minimized by reducing the major operations. The majority of the process is symmetric-based cryptography between sensor nodes and CH. Thus, the energy consumption is significantly minimized in the given scenario of WSN.

Additionally, the security requirements of the proposed scheme have been minimized considerably. In case an attacker wishes to access any particular environment, they have to face the security barrier. Furthermore, the developed scheme is also scalable and adaptable in a dynamic situation.

In the future, we aim to involve most of the recent relevant security schemes in the research domain of WSN and IoT applications. Their resultant analysis can be demonstrated concerning the state of the art. Moreover, the proposed scheme can further have analyzed using a mathematical model. This system can be tested using different new parameters, and its effectiveness will be checked for the security of WSN and other related domains.

Data Availability

All the relevant data are available in this manuscript.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This research work was partially supported by the Tecnológico de Monterrey, School of Engineering and Sciences, Zapopan 45201, Mexico, and the Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Kuala Lumpur 54100, Malaysia.

References

- [1] G. Simon, M. Maróti, Á. Lédeczi et al., "Sensor network-based countersniper system," in *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pp. 1–12, Baltimore, MD, USA, November 2004.
- [2] M. Castillo-Effer, D. H. Quintela, W. Moreno, R. Jordan, and W. Westhoff, "Wireless sensor networks for flash-flood alerting," in *Proceedings of the Fifth IEEE International Caracas Conference on Devices, Circuits and Systems*, 2004, pp. 142–146, Punta Cana, Dominican Republic, November 2004.
- [3] S. Zhang and H. Zhang, "A review of wireless sensor networks and its applications," in *Proceedings of the 2012 IEEE International Conference on Automation and Logistics*, pp. 386–389, Zhengzhou, China, August 2012.
- [4] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, 2008.
- [5] IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1, IEEE Std 802.16e-2005 and IEEE Std 802.16-2004/Cor 1-2005 (Amendment and Corrigendum to IEEE Std 802.16-2004), 2006.
- [6] L. Yu, N. Wang, W. Zhang, and C. Zheng, "GROUP: a grid-clustering routing protocol for wireless sensor networks," in *Proceedings of the 2006 International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1–5, Vancouver, Canada, July 2006.
- [7] M. Elshrkawey, S. M. Elsherif, and M. Elsayed Wahed, "An enhancement approach for reducing the energy consumption in wireless sensor networks," *Journal of King Saud University-Computer and Information Sciences*, vol. 30, no. 2, pp. 259–267, 2018.
- [8] T. Wang, J. Zeng, Y. Lai et al., "Data collection from WSNs to the cloud based on mobile Fog elements," *Future Generation Computer Systems*, vol. 105, pp. 864–872, 2020.
- [9] E. Golden Julie and Y. Harold Robinson, "Security and privacy issues in wireless sensor networks," in *IoT and Analytics for Agriculture*, pp. 187–210, Studies in Big Data, Springer, Singapore, 2020.
- [10] D. Wu, S. Si, S. Wu, and R. Wang, "Dynamic trust relationships aware data privacy protection in mobile crowd-sensing," *IEEE Internet of Things Journal*, vol. 5, pp. 2958–2970, 2017.
- [11] M. N. Khan, A. Rao, and S. Camtepe, "Lightweight cryptographic protocols for IoT constrained devices: a survey," *IEEE Internet of Things Journal*, vol. 8, 2020.
- [12] G. Mehmood, M. Z. Khan, H. U. Rahman, and S. Abbas, "An efficient and secure session key establishment scheme for health-care applications in wireless body area networks," *Journal of Engineering and Applied Sciences*, vol. 37, 2018.
- [13] H. Tang, L. Zhu, and Z. Zhang, "A novel authenticated group key agreement protocol based on elliptic curve Diffie-Hellman," in *Proceedings of the 2008 4th International Conference on Wireless Communications*, pp. 1–4, Dalian, China, October 2008.
- [14] Z. Zhang, C. Jiang, and J. Deng, "A novel group key agreement protocol for wireless sensor networks," in *Proceedings of the 2010 International Conference on Measuring Technology and Mechatronics Automation*, pp. 230–233, Changsha, China, March 2010.
- [15] D. B. Nagalgaonkar Pramod and G. Ranjit Sharnappa, "Review on fault detection and recovery in WSN," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5, 2015.
- [16] P. E. Abi-Char, A. Mhamed, and B. El-Hassan, "A secure authenticated key agreement protocol based on elliptic curve cryptography," in *Proceedings of the Third International Symposium on Information Assurance and Security*, pp. 89–94, Manchester, UK, August 2007.
- [17] M. Meingast, T. Roosta, and S. Sastry, "Security and privacy issues with health care information technology," in *Proceedings of the 2006 International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 5453–5458, Montreal, Canada, June 2006.
- [18] D. Singelée, B. Latré, B. Braem et al., "A secure low-delay protocol for wireless body area networks," *Adhoc & Sensor Wireless Networks*, vol. 9, 2010.
- [19] L. Ertaul and W. Lu, *ECC Based Threshold Cryptography for Secure Data Forwarding and Secure Key Exchange*, University of Waterloo, Waterloo, Canada, 2005.
- [20] L. Ertaul, P. Chudinov, and B. Morales, "IoT security: authenticated lightweight key exchange (ALIKE)," in *Proceedings of the International Conference on Wireless Networks (ICWN)*, pp. 45–50, Rome, Italy, July 2019.
- [21] M. H. Eldefrawy, M. K. Khan, and K. Alghathbar, "A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography," in *Proceedings of the 2010 International Conference on Anti-Counterfeiting*, pp. 1–6, Hoboken, NJ, USA, March 2010.
- [22] J. Wu and D. R. Stinson, "Three improved algorithms for multipath key establishment in sensor networks using protocols for secure message transmission," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, pp. 929–937, 2010.
- [23] S. Ali, A. Humaria, M. S. Ramzan et al., "An efficient cryptographic technique using modified Diffie-Hellman in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 16, 2020.
- [24] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, "Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 9, pp. 4957–4968, 2019.
- [25] D. He, M. Ma, S. Zeadally, N. Kumar, and K. Liang, "Certificateless public key authenticated encryption with keyword search for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, pp. 3618–3627, 2017.
- [26] A. Dua, N. Kumar, A. K. Das, and W. Susilo, "Secure message communication protocol among vehicles in smart city," *IEEE Transactions on Vehicular Technology*, vol. 67, pp. 4359–4373, 2017.
- [27] S. Tyagi and N. Kumar, "A systematic review on clustering and routing techniques based upon LEACH protocol for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 36, no. 2, pp. 623–645, 2013.
- [28] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, vol. 11, pp. 2590–2601, 2016.
- [29] M. S. Yousefpoor and H. Barati, "Dynamic key management algorithms in wireless sensor networks: a survey," *Computer Communications*, vol. 134, pp. 52–69, 2019.
- [30] M. S. Yousefpoor and H. Barati, "DSKMS: a dynamic smart key management system based on fuzzy logic in wireless

- sensor networks,” *Wireless Networks*, vol. 26, no. 4, pp. 2515–2535, 2020.
- [31] Q. Ren and G. Yao, “An energy-efficient cluster head selection scheme for energy-harvesting wireless sensor networks,” *Sensors*, vol. 20, p. 187, 2020.
- [32] G. Mehmood, M. Z. Khan, A. Waheed, M. Zareei, and E. M. Mohamed, “A trust-based energy-efficient and reliable communication scheme (Trust-Based ERCS) for remote patient monitoring in wireless body area networks,” *IEEE Access*, vol. 8, pp. 2169–3536, 2020.
- [33] C. Chunka, S. Banerjee, and R. S. Goswami, “An efficient user authentication and session key agreement in wireless sensor network using smart card,” *Wireless Personal Communications*, vol. 117, 2021.