Secure message transmission scheme in wireless sensor networks

Kameran Ali Ameen[1], Baban Ahmed Mahmood[2], Yalmaz Najmaldeen Taher[3]
[1,3]Department of Computer Science, Kirkuk University, Kirkuk, Iraq
[2]Department of Networks, Kirkuk University, Kirkuk, Iraq

Article Info

Article history:

Received Sep 29, 2020
Revised Feb 27, 2021
Accepted Mar 25, 2021

Keywords:

Cryptography
Key management
Security
Security attacks
WSN

ABSTRACT

Wireless sensor networks (WSNs) have been the subject of intensive research in the past few years and the backbone of most maximum present information technology. WSNs have been employed in various applications such as track monitoring battlegrounds in military fields and patients' medical requirements in the civilian field. The wireless sensor networks are always randomly distributed in an open area (hostile), pervasive environment, and open media channel. Thus, WSNs are vulnerable to several species of attacks. Moreover, messages may be easily intercepted or altered because the transmission is not secure, hence effective key management scheme is strongly needed to reduce the risks. Cryptography methods are a crucial aspect of WSNs to reach security goals. In this paper, we propose an efficient and secure message transmission scheme that combines the Knapsack algorithm with the Diffie-Hellmann process to encrypt messages. The results and analysis show that the proposed scheme is efficient and it achieves most of the security goals providing high privacy and security. It is also resilient against some of the well-known attacks.

Corresponding Author:

Baban Ahmed Mahmood
Department of Networks
Kirkuk University, Kirkuk, Iraq
Email: Baban.mahmoodjaf@gmail.com

1. INTRODUCTION

Recently, WSNs have become one of the interesting parts of the wireless network research field. WSNs generally consist of some nodes that are randomly distributed over a certain area [1], [2]. WSN is usually designed to have a base station, ordinary sensor nodes, and cluster heads (CHs). The sensors detect/sense some events and send data to the base station through the CHs [3], [4]. Since hierarchical nodes are deployed in an open area and unattended environments without physical protection making the nodes prone to several types of well-known attacks, thus, the main concern is how to build secure communications among nodes [5]. Management of key is a security aspect that has importance in cluster-based networks [6], [7]. Key management must ensure offering the requirement of security that includes integrity, confidentiality, and authentication of nodes by using cryptographic techniques to encrypt messages and authenticate the communication among nodes [8], [9]. This type of network is widely used in various scenarios, for example, environmental monitoring, military, commercials, healthcare, and agriculture [10], [11].

In this paper, we propose a secure message transmission scheme in wireless sensor networks (SMTS) that encrypts messages using a knapsack algorithm [12], [13] with the Diffie-Hellmann process. The proposed method adds a shared key that is created depending on the Diffie-Hellmann to secure message access and authenticates the nodes that communicate with each other using message authentication code

(MAC). The objective and motivation behind our paper is presented. Since wireless communication enters into various facets of our life, it cannot be excluded. The success of any technology mainly depends on whether the security issues are taken into consideration properly. This has made us study the security issues associated with WSN and present a novel technique that helps in sending data packets efficiently such that privacy is highly preserved.

The organization of the rest of the paper is depicted as follows. Section 2 presents the literature review. In section 3, discussion of the security issues and attacks in WSNs are presented. Describing the Diffie-Hellman key exchange and its advantages are given in section 4. Sections 5 and 6 present the network model and the proposed method successively. Implementation and Analysis of the proposed method are given in section 7. Section 8 concludes the paper.

2. LITERATURE REVIEW

The security requirement is a critical issue for network security. The network obligation ensures the delivery of messages among sensor nodes without alteration or modification. In this section, we will review some of the algorithms presented in the literature.

Jiang *et al.* [14] propose a distributed scheme for user authentication for WSNs that relies on the self-certified key cryptosystem (SCK). This SCK is then implemented using elliptic curve cryptography (ECC) to setup pair-wise keys for the sensor network. This scheme assumes there exist of a key distribution senter (KDC) which is in charge of secret information generation to construct pair-wise keys between users and nodes. In user authentication phase, when a user needs to join the network, he must obtain his own secret information (e.g. an identifier) from the KDC. Several researches in the literature proved that ECC is suitable in WSNs because of the discrete logarithm problem and small key sizes.

Diop *et al.* [15] propose an efficient and secure key management scheme for hierarchical wireless sensor network. This method presents a secure cluster formation operation which distributes the keys with each cluster head (CH) in the network to prevent the virulent nodes from joining the network, as a result sending fake messages is prevented. A lightweight scheme for user authentication that is adapted to WSNs is presented in [16]. This scheme allows establishing a session key without requiring an infrastructure. Participating members can be authenticated before gaining access to the WSN. This is because users are equipped with personal digital assistant. The security of the scheme depends on memorizing passwords which are secret keys.

Xinyang and Jidong [17] propose a secure efficient key management scheme in hierarchical wireless sensor networks. This scheme supports the establishment and updating of three kinds of keys as the following: first, a network key that all nodes share to encrypt messages and authenticate new nodes. Second, a group key that all nodes share in the same CH. Third, a pairwise key that a specific pair of nodes share in the network. This scheme is able to perform node revocation and addition in the network. The method depends on hierarchical structure which provides flexibility and scalability of the network.

A novel key management scheme which is based on the congruence property of modular arithmetic for heterogeneous WSNs is proposed in [18]. The network composes of many clusters wherein each CH is responsible of distributing key seeds to its member nodes. Then, each member uses the key seed to calculate the shared unique key with its CH and a group key that is shared in the same cluster with other nodes. The CH can keep forward secrecy via broadcasting a key update message. This method is based on ECC, therefore, it consumes more energy. However, the base station performs majority of the computations.

Gandino *et al.* [19] use a new key management scheme for WSNs which relies on public key cryptography (PKC) during key establishment. Each sensor node stores an authentication table wherein each row contains the information required to authenticate one node of the network. The authentication process ensures that only eligible nodes can join the WSN. This scheme uses PKC to protect the key establishment.

3. RESULTS AND DISCUSSION

Security requirement is a very essential aspect of protocols in WSNs. The goal of security requirements is to protect the data exchanges between nodes [20]. Also, there are several attacks presented in the literature that are needed to be considered. This section, in addition to the security requirements, presents some of the attacks presented in the literature. Some of the security requirements are presented below.

3.1. Security issues and goals

In this subsection, we present some of the security issues presented in the literature.

3.1.1. Authentication, integrity, and confidentiality

One of the main challenging aspects for WSNs is authentication which verifies the identity of the source because it is used in open areas and uses the public wireless channel. Therefore, the destination node needs to ensure those messages are authenticated by identifying the source. The aforementioned process prevents the admittance of the data transmitted by the attacker or the adversary nodes [21], [22].

To get reliable and secure communications in wireless network, the received data by the target node ought to be consistent with that sent by the originating node. The information in the packets is supposed to remain intact and not altered by intermediate nodes such that virulent activity should not corrupt the data [22]. The data collected by nodes in WSNs is sensitive. Secrecy of the data should be maintained. So the message content must be concealed from every node other than the receiver. Users that have proper authorizations are supposed to have access to the information; however, illegitimate users must be declined from accessing the data [22].

3.1.2. Data freshness and scalability

Data freshness ensures that no outdated messages are replayed by malicious nodes. This can be done by applying time stamps or random numbers during encryption to maintain data freshness [22]. The ability of supporting expansion of network is known as network scalability. It is also known as increasing number of nodes, such that network performance is not affected. Also, scalability should be supported by wireless sensor networks' routing protocols. These routing protocols are supposed to keep their performance while the network grows larger, hence a good routing protocol has to be scalable and adaptive to changes [23]-[25].

3.2. Different attacks on WSNs

In this subsection, we present some of the attacks presented in the literature.

3.2.1. Eavesdropping attack and Sybil attack

Broadcasting feature of channels in wireless sensor networks makes it easier for intruders with strong receivers to eavesdrop and intercept transmitted data. This interception can gain access to different information carried by the data packets such as location of the nodes, message identifiers, node identifiers, timestamps, and application specific information [26]. In Sybil attacks, malicious nodes illegitimately assign several identities to the other nodes in the sensor network. Significant risks are posed which may decrease fault-tolerance effectiveness significantly. Authentication and encryption methods can avoid this attack [26].

3.2.2. Man-in-middle attack and replay attack

An attacker in Man-in-Middle attack sits between the source and destination node and sniffs any data that is exchanged between them. This enables the attacker to impersonate the sender such that it can communicate with the receiver. It can also impersonate the receiver to reply to the sender [27]. Replay attack is a security violation wherein a malicious node purposely retransmits the data packets. This retransmission process is done continuously and repeatedly such that it exhausts the victim’s power supplies or buffers. As a result, it degrades the network’s performance [28].

3.2.3. Denial of service attack

This attack attempts to separate a node from a network and exhaust its resources by keeping it busy. It continuously sends fake messages in order to prevent benign network users from accessing resources or services to which they are entitled [28].

4. INTRODUCTION OF THE DIFFIE-HELLMAN KEY EXCHANGE AND ITS ADVANTAGES

The Diffie-Hellman (DH) key exchange permits two parties to get a shared key through a communication channel that is public. An attacker, eavesdropping at the messages sent by both sender and receiver, will not be able to define what the shared key is. This is useful because the shared secret key can be used such that a secret session key can be created and used with symmetric key cryptography like MAC or data encryption standard (DES) [29]. Excellent scalability, low-storage memory, and communication overhead that does not need trusted third party are advantages of DH. This makes DH work for entities that do not possess a secret key and have never met in advance with a trusted third party [30].

4.1. Advantages of DH

It is assumed that the eavesdropper that has access to the public values is not able to find the shared secret key, this assumption is called the Diffie-Hellman assumption which is somehow related to the discrete log assumption. Discrete log assumption states that given a generator g of ZP* with an element public key (PUB) of ZP* is infeasible to calculate x in such a way that $g^x \equiv$PUB of ZP* [30].

5. THE NETWORK MODEL

In the proposed scheme, the network structure is considered to be hierarchical as shown in Figure 1. The network consists of BS and two different types of sensor nodes which are cluster head CHi and sensor nodes (L_i). The sensor nodes are member nodes that are equipped with an amount of resources lower than that of the CHs. We make the following assumptions:

a. BS is considered trustworthy and it performs at its highest capabilities in terms of computing power, energy, and storage capacity that are assumed. It can directly connect to all sensor nodes in the network.
b. BS registers all nodes and saves a table of node ID, when a node joins the network, BS updates this table.
c. All the sensor nodes in the network are static.
d. CHs are in charge of data transfer, coordination, and nodes' management in the cluster which is reached by one hop to the BS.
e. The sensor nodes L_i can be reached by one or multi hops to the CH and they collect information about the surrounding location and transmit it to the CHs.
f. Each CH is equipped with a global positioning system (GPS).
g. Enemy requires at least T time capture to compromise any node.
h. Each message that is exchanged has a timestamp called "T" which guarantees the information freshness.

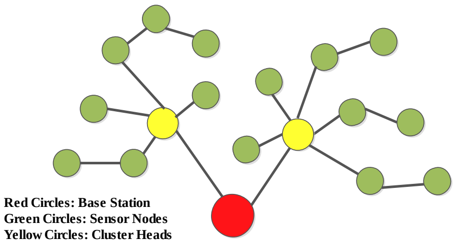

Red Circles: Base Station
Green Circles: Sensor Nodes
Yellow Circles: Cluster Heads

Figure 1. The network model

6. THE PROPOSED SCHEME

The proposed scheme, presented in this section, is divided into seven phases: (i) Initialization; (ii) Node distribution; (iii) Cluster forming; (iv) Creating shared key; (v) Secure data transmission; (vi) Node removal; (vii) Updating shared key. In the following subsections, a description of each phase is presented in detail.

6.1. Initialization

In the initialization phase, the BS is responsible of generating the public key and private key needed for all nodes, CHs, and itself. All CHs are provided with tamper-resistant hardware. An adversary cannot get the keys even if it captures a CH. Thus, all CHs can use the same public key and private key (PUB_{CH}, PRV_{CH}). This process is depicted below, and the notations' descriptions that are used in the proposed scheme are shown in Table 1.

Table 1. The parameters of the simulation

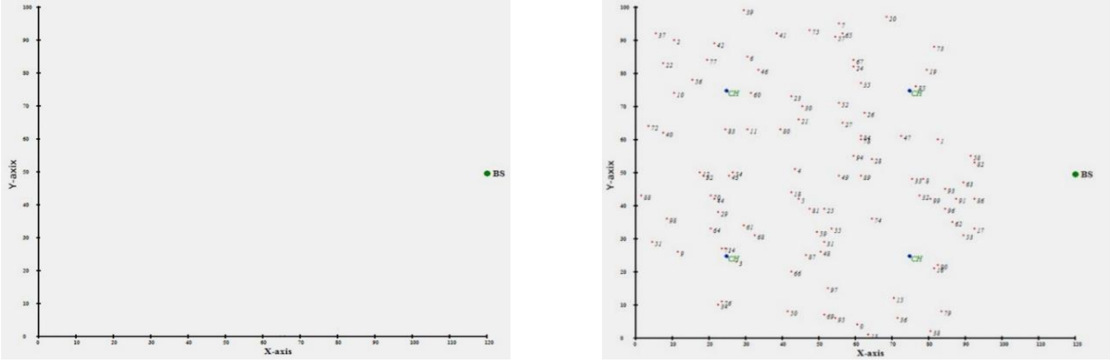
Notation	Description
L_i	Low sensor node
CH_i	Cluster Head
IDL_i	Identification number of node
$IDCH_i$	Identification Cluster Head
ID_{BS}	Identification Base Station
MAC	Message Authentication Code
M_S	Message to transmit
SK_{AB}	Shared Key between node A and B
PRV_{CH} ,PUB_{CH}	Private and Public keys of CH_i
PRV_{BS}, PUB_{BS}	Private and Public keys of BS
||	Concatenation Operator
PRV_{Li}, PUB_{Li}	Private Key of Li and Public Key of L_i
T	Time Stamp

- BS assigns an identity (ID) to itself and each sensor node and the CH.
- BS, CH, and each sensor node are pre-loaded with algorithms 1 and 2 that are shown later in this section.
- BS is preloaded with the public key of each cluster head (PUB_{CH}) and its own public and private keys (PUB_{BS}, PRV_{BS}).

- Each CH is preloaded with the private key, generator number, and prime number, a cyclic subgroup of large order, public key of base station (PUB_{BS}) and the public key of all L_i.
- Each sensor L_i is preloaded with its private key (PRV_{Li}), generator number, and a cyclic subgroup of large order, prime number, and the public key of each CH (PUB_{CH}).

6.2. Node distribution

An array of sensor nodes' IDs is generated by the BS in the network. Then, 100 nodes are distributed uniformly at random in the area of size (100×100) m^2 [17, 18] as shown in Figure 2. The sensor nodes depend on their locations to obtain confidentially, communication and mutually authenticating each other.

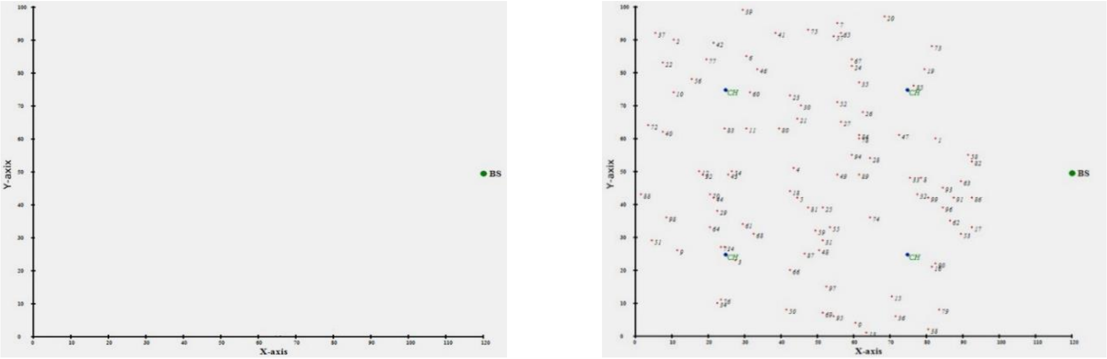


(a) (b)

Figure 2. Node distribution phase, (a) The BS setup, (b) Random node distribution

6.3. Cluster forming

The clustering method is one of the main methods such that the lifetime of a sensor network is extended by reducing energy consumption. Scalability and life time can also be increased by clustering [12]. This phase starts after sensor deployment in the area where some of the nodes are selected as CH randomly whereas other nodes select their leaders based on some other parameters such as the strongest signal received from a CH [7], [31]. Between member nodes and the CH in the network, the communication is either single hop or multi-hop and the CHs communicate to the BS by single hop as shown in Figure 3. In order to reduce the energy consumption of a CH, new nodes are select as CH after certain interval of time [32]. Among sensors, energy consumption can be averaged by routing CHs [33], [34].



(a) (b)

Figure 3. Formation of cluster head, (a) Nodes select CH, (b) CH contacts with BS

6.4. Creating the shared key

The DH process allows two nodes to jointly generate a shared key by directly exchanging messages with each other over an insecure communication channel [15], [19], [21]. Diffie-Hellman key exchange or key agreement does not include a third party to form a shared key between two nodes. This feature noticeably reduces the communication overhead. DH is a reliable algorithm in terms of consuming energy and overhead of communication of WSN. Here, they are using Diffie-Hellman key exchange algorithm to establish a shared key between the CH and nodes in its cluster or among nodes in the same cluster. This shared key is used by all the nodes and the CH combines the shared key with the result of the knapsack algorithm when nodes tend to send messages.

6.5. Secure data transmission

To make the data transfer secure, the message must be encrypted by the sending node when sending it to the destination. This prevents unauthorized access to the data being sent [1]. Data transmission in the hierarchical model includes two distinct parts. First, member nodes send data to their CH directly or via multi-hop technique. Second, the CHs send the data to the BS by one hop because CHs have higher resources when compared with other nodes. This phase consist of two procedures, which are described below.

6.5.1. Message encryption

Message encryption applies after cluster formation phase. Suppose that node L_A wants to send a message "A" to node L_B in the same CH. Applying this process is done as follows:

- Initiate the connection with L_A and L_B.
- Both L_A and L_B have private keys PRV_A and PRV_B consequently.
- Both nodes L_A and L_B generate public keys as in (1) and (2) consequently, then they exchange their public keys through a secure channel.

$$PUB_A = \; g^{PRV_A}\, mod\; p \qquad (1)$$

$$PUB_B = \; g^{PRV_B}\, mod\; p \qquad (2)$$

- Next, L_A and L_B compute the shared key (SK_{AB}) depending on Diffie-Hellman key exchange as shown in (3) and (4) consequently.

$$SK_{AB} = \; PUB_B^{PRV_A}\, mod\; p \qquad (3)$$

$$SK_{AB} = \; PUB_A^{PRV_B}\, mod\; p \qquad (4)$$

- M_i=convert the original message (M) to corresponding American Standard Code for Information Interchange (ASCII) values.
- Compute M_K as according to algorithm 1.
- Then, compute the cipher message as $C_m = M_K + SK_{AB}$.
- L_A concatenates C_m, ID_A, ID_B, and MAC (M||T) altogether where MAC includes the timestamp T and M is the message to be sent.
- The message transfer is performed as follows:
- $M_S \rightarrow [C_m \,||\, IDL_A \,||\, IDL_B \,||\, MAC\,(M||T)]$ where M_S is the encrypted message to be sent.

6.5.2. Message decryption

Message decryption is applied at the destination node L_B. To decrypt the ciphered message in order to recover original message M, the following process is applied:

- The receiver L_B divides the cipher message M_S into four parts.
- The receiver now verifies the received message from the ID of the sender and destination by the table of ID it has. If the result verification is unsuccessful, then the message will be rejected. Otherwise the next step is applied in which the message is saved.
- Compute $M_k = C_m - SK_{AB}$.
- Algorithm 2 is applied on the M_k to find message M_{new}.
- The destination verifies M_{new} by calculating the MAC if $M_{new} = M_{received}$ then it saves M_{new}; otherwise it rejects the M_{new}. Finally, accepting the message, the destination sends back an ACK to the sender.

Algorithm 1 (Compute M_K)

```
Initialization
n is an integer number, b is a binary bit.
Create series of vectors ($X_i$), where ($X_i$ = 1, $n_1$, $n_2$, $n_3$… $n_m$ ) (1 ≤ i ≤  m) and m
is the length of the binary bit string.
$M_i$ is represented as a text message in its binary form as: $M_i$ = $b_1$, $b_2$, $b_3$…, $b_m$ (1
≤ i ≤  m).
$M_i$ is represented as a text message in its binary form as: $M_i$ = $b_1$, $b_2$, $b_3$…, $b_m$ (1
≤ i ≤  m).

Compute a cumulative sum Mi according to the following Equation:
```

$$M_K = \sum_{i=1}^{m} X_i \ M_i$$

```
7. In the final signed message version, the value of $M_i$ is replaced by its
   equivalent $M_K$.
8. End.
```

Algorithm 2 (Recovery M_{new})

```
1. Initialization
2. n is an integer number, $M_K$ is an encrypted message.
3. Checking the destination.
  3.1 If, $M_K - n^m > 0$ then X binary bits of value 1 are assigned at the $(m)^{th}$ point.
      The current value is $M_K = M_K - n_m$.
  3.2 Else, $M_K - n_m < 0$ then a 0 bit is assigned and the $M_K$ remains unchanged.
  3.3 End if
4. Destination continues to calculate subtract operation $n_m$-1 from the current $M_K$
   depending upon whether it is > 0 or < 0, assign 1 or 0 at the relevant bit point.
   Subtraction operation continues until the $X_i$ series is exhausted.
5. Recover the binary bit pattern of $M_K$.
6. Then convert the binary bits to integer number $M_i$ which is an ASCII value.
7. Convert ASCII values to correspond the text $M_{new}$.
8. Save $M_{new}$.
9. End.
```

6.6. Removing nodes

The nodes can be easily captured and become compromised because they are deployed in an unattended environment, so they must be removed from the network. We assume that compromised nodes can be disclosed by the detection system that is used in the network, which is, after the network detects the compromised nodes and inform the CH about it. Then the cluster head broadcasts a message containing the IDs of the compromised nodes after being encrypted using the shared key. When a node receives a revocation message, first, it verifies the message's reliability that is sent by CH. Second, the node checks whether it is in communication with the node that is being compromised. If so, the node withdraws the keys that are shared with the compromised node and removes the ID from it.

6.7. Updating the shared key

To increase the efficiency of the proposed scheme and to decrease the danger of attacks, it is necessary to update the shared key. Hence the shared key of all the nodes are periodically updated. The shared key is only valid for a limited time that is less than the required time which is predicted for compromising a node. This time period depends on the environment of the network. After that time period, the BS selects a new integer modular and broadcasts it to the entire network. Every node, as well as the CHs is supposed to receive the message.

7. IMPLEMENTATION AND ANALYSIS OF THE PROPOSED METHOD

The proposed scheme is simulated on a PC with an Intel(R) Core(TM) i3-2328M CPU @ 2.20GHz 2.20 GHz processer, A memory (RAM) of 8.00 GB, a 64-bit operating system Windows 10 Ultimate using C# programming language. The performance analysis of our proposed scheme is calculated based on different aspects including security requirement and security attacks, and then a comparison is made with the other schemes.

7.1. Security requirements analysis

7.1.1. Authentication and integrity

Authentication is available in this proposal because each node has a unique ID which is assigned by the BS as well as the use of MAC to achieve authentication in the secure data transmission phase. The integrity of the message is guaranteed by the verification procedure through calculating the MAC. The nodes send the messages by encrypting it using knapsack, then combine it with a shared key. The verification process fails if the message changed through the transmission. Hence, the receiving node is able to make a decision about whether a message has been infringed upon which it decides to accept or reject the message.

7.1.2. Scalability, confidentiality, and data freshness

The proposed scheme is fully scalable and secure because it is first based on the knapsack problem to encrypt message then it depends on the shared key. Moreover, the hierarchical topology optimizes resource consumption and confirms the scalability of the communication process. All the messages are encrypted using the knapsack algorithm in the proposed scheme. In the traditional cryptographies, the original message should be sent with the encrypted message when two nodes exchange the message. In this proposed scheme, only one message is sent after encryption. After provisioning confidentiality and integrity is assured, the freshness of all the messages is supposed to be provided. Informally, data freshness proposes that the data is recent such that stale data are not sent. In this proposed scheme, since share key between nodes are updated over time and a timestamp is added to every encrypted message sent. Subsequently, we guarantee the freshness of messages exchanged in the network.

7.2. Security attacks analysis

7.2.1. Replay attack, man-in-middle attack, and Sybil attack

Our proposal scheme is able to resist replay attack because the message sent contains the timestamp T which specifies the moment when the message was sent. This determines the difference in time which detects any attack in the replay phase. This scheme can endure man-in-middle attack even if an adversary intercepts the message transmitted between two nodes. No useful information about the shared key is revealed during a successful run. If an adversary intercepts g, it cannot compute share key as PUB_A and PUB_B rely on the PRV_A and PRV_B. To break this scheme, adversary needs to compute PRV_A given g and $g^{PRV}{}_A$, which is assumed hard. Using a fake ID, the Sybil attack sends messages to the nodes in the network. Since this process is unsuccessful because the receiver checks the ID of the sender before decrypting the message using MAC.

7.2.2. Eavesdropping attack and stolen ID attack

The proposed scheme is able to resist eavesdropping attack because the contents of the message are a sequence of bits such that the original message is not sent. Moreover, the algorithm used in this proposed scheme makes the output not understandable because it is not repeated. Denial of Service attack tries to separate a node from a network and exhaust its resources by keeping it busy by sending fake messages. This process is only possible if the adversary is able to access the network and become its authentic member or through stealing the IDs of the nodes. Here this would not work because the adversary needs to know the shared key to encrypt the message after applying knapsack algorithm. Table 2 shows the comparison of the proposed method with other schemes in terms of security issues. Figure 4 shows the time it takes a node to send a packet from one node to another node (hop) for the purpose of message encryption and decryption.

Table 2. Comparison of the proposed scheme with respect to security requirements

Issues	Cryptographic method	Authentication	Confidentiality	Integrity	Scalability	Data freshness
Proposed method	DH and Knapsack Algorithm	✓	✓	✓	✓	✓
[16]	Encryption and XOR	✓	✕	✓	✓	✓
[21]	ECDSA	✓	✕	✕	✓	✕
[35]	ECC	✓	✕	✓	✕	✕

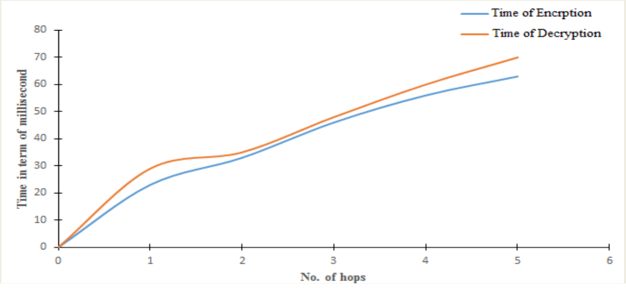


Figure 4. Time consumption in each hop

8. CONCLUSION

In the applications of WSNs, data gathered by sensor nodes or CH is sensitive and important making providing proper data protection a must. Therefore, cryptography methods are necessary in order to maintain data integrity, confidentiality, and authenticity. In this paper, we proposed a method, SMTS, based on the DH key exchange such that it establishes a shared key to be used between a CH and nodes in a specific cluster or BS. The shared key is combined with the output of the knapsack algorithm when nodes tend to send messages. SMTS provides a periodical update of the shared key for all the nodes to avoid nodes from being captured and to ensure that only valid nodes send messages. Hence, it provides a continuous authentication of nodes in the network. The analyses show that our method is efficient achieves most of the security goals.

Moreover, compared to other algorithms, it has an acceptable performance in terms of security issues and resistance against known attacks.

REFERENCES

[1] K. Viji, T. S. Perumal, R. S. Prakash, and M. V. Ananthkumar, “An improved three-layer low-energy adaptive clustering hierarchy for wireless sensor networks,” *International Journal of Innovative Science and Research Technology*, vol. 2, no. 5, pp. 797-803, 2017, doi: 10.1109/JIOT.2016.2530682.

[2] A. Rani and S. Kumar, "A survey of security in wireless sensor networks," *2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT)*, 2017, pp. 1-5, doi: 10.1109/CIACT.2017.7977334.

[3] E. Elgenaidi, T. Newe, E. O’Connell, D. Toal, and G. Dooly, “Secure and efficient key coordination algorithm for line topology network maintenance for use in maritime wireless sensor networks,” *Sensors*, vol. 19, no. 12, p. 2204, 2016, doi: 10.3390/s16122204.

[4] R. Rab, S. A. D. Sagar, N. Sakib, A. Haque, M. Islam, and A. Rahman, “Improved self-pruning for broadcasting in ad hoc wireless networks,” *Wireless Sensor Network*, vol. 9, no. 2, pp. 73-86, 2017, doi: 10.4236/wsn.2017.92004.

[5] K. Malav, D. Gupta, and V. Quintin, “An energy alert tree based routing (EATR) in Zigbee wireless sensor network for well-organized multimedia broadcast,” *Int. J. of Innov. Sci. and Research Tech.*, vol. 1, no. 3, pp. 26-29, 2017.

[6] Z. Fei, B. Li, S. Yang, C. Xing, H. Chen and L. Hanzo, "A Survey of Multi-Objective Optimization in Wireless Sensor Networks: Metrics, Algorithms, and Open Problems," in *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 550-586, Firstquarter 2017, doi: 10.1109/COMST.2016.2610578.

[7] S. B. Kamble and V. V. Jog, "Efficient key management for dynamic wireless sensor network," *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, 2017, pp. 583-586, doi: 10.1109/RTEICT.2017.8256663.

[8] E. Yuan, L. Wang, S. Cheng, N. Ao, and Q. Guo, “A key management scheme based on pairing-free identity based digital signature algorithm for heterogeneous wireless sensor networks,” *Sensors*, vol. 20, no. 6, p. 1543, 2020, doi: 10.3390/s20061543.

[9] B. Kim and J. Song, “Energy-efficient and secure mobile node reauthentication scheme for mobile wireless sensor networks,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1-6, 2019, doi: 10.1186/s13638-019-1470-9.

[10] M. S. BenSaleh, R. Saida, Y. H. Kacem, and M. Abid, “Wireless sensor network design methodologies: A survey,” *Journal of Sensors*, vol. 2020, pp. 1-13, 2020, doi: 10.1155/2020/9592836.

[11] B. A. Mahmood, A. Ibrahim and D. Manivannan, "Hybrid On-demand greedy routing protocol with backtracking for Mobile Ad-Hoc Networks," *2016 9th IFIP Wireless and Mobile Networking Conference (WMNC)*, 2016, pp. 110-116, doi: 10.1109/WMNC.2016.7543977.

[12] S. Parvin, S. Han, Z. U. Rehman, A. Al Faruque, and F. K. Hussain, “A new identity-based group signature scheme based on Knapsack ECC,” *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IEEE*, Palermo, Italy, pp. 73-80, 2012, doi: S. Parvin, S. Han, Z. U. Rehman, A. Al Faruque and F. K. Hussain, "A New Identity-Based Group Signature Scheme Based on Knapsack ECC," *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, 2012, pp. 73-80, doi: 10.1109/IMIS.2012.88.

[13] R. R. Ramasamy, M. A. Prabakar, M. I. Devi, and M. Suguna, “Knapsack based ECC encryption and decryption,” *International Journal of Network Security*, vol. 9, no. 3, pp. 218-226, 2009.

[14] C. Jiang, B. Li and H. Xu, "An Efficient Scheme for User Authentication in Wireless Sensor Networks," *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)*, 2007, pp. 438-442, doi: 10.1109/AINAW.2007.80.

[15] X. Zhang and J. Wang, "An efficient key management scheme in hierarchical wireless sensor networks," *2015 International Conference on Computing, Communication and Security (ICCCS)*, 2015, pp. 1-7, doi: 10.1109/CCCS.2015.7374122.

[16] O. Cheikhrouhou, A. Koubâa, M. Boujelben and M. Abid, "A lightweight user authentication scheme for Wireless Sensor Networks," *ACS/IEEE International Conference on Computer Systems and Applications - AICCSA 2010*, 2010, pp. 1-7, doi: 10.1109/AICCSA.2010.5586995.

[17] X. Zhang and J. Wang, "An efficient key management scheme in hierarchical wireless sensor networks," *2015 International Conference on Computing, Communication and Security (ICCCS)*, 2015, pp. 1-7, doi: 10.1109/CCCS.2015.7374122.

[18] J. Zhang, Q. Cui and X. Liu, "An Efficient Key Management Scheme for Wireless Sensor Networks in Hostile Environments," *2009 International Conference on Multimedia Information Networking and Security*, 2009, pp. 417-420, doi: 10.1109/MINES.2009.157.

[19] F. Gandino, C. Celozzi, and M. Rebaudengo, “A key management scheme for mobile wireless sensor networks,” *Applied Sciences*, vol. 7, no. 5, pp. 1-18, 2017, doi: 10.3390/app7050490.

[20] A. R. Al-Breiki1, H. S. Jassim, B. T. Sharef, and Z. T. Sharef, “Review of wireless sensor networks: challenges and threats,” *International Journal of Innovative Science and Research Technology*, vol. 3, no. 2, pp. 980-984, 2018.

[21] W. -h. Wang, Y. -l. Cui and T. -m. Chen, "Design and implementation of an ECDSA-based identity authentication protocol on WSN," *2009 3rd IEEE International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications*, 2009, pp. 1202-1205, doi: 10.1109/MAPE.2009.5355821.

[22] P. Sinha, V. K. Jha, A. K. Rai and B. Bhushan, "Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey," *2017 International Conference on Signal Processing and Communication (ICSPC)*, 2017, pp. 288-293, doi: 10.1109/CSPC.2017.8305855.

[23] R. Priyadarshi, B. Gupta, and A. Anurag, "Deployment techniques in wireless sensor networks: a survey, classification, challenges, and future research issues," *The Journal of Supercomputing, Springer*, pp. 1- 41, 2020, doi: 10.1007/s11227-020-03166-5.

[24] B. A. Mahmood and D. Manivannan, "Position based and hybrid routing protocols for mobile Ad Hoc networks: A survey," *Wireless Personal Communications*, vol. 83, no. 2, pp.1009-1033, 2015, doi: 10.1007/s11277-015-2437-8.

[25] B. A. Mahmood, A. Ibrahim, and D. Manivannan, "A secure source routing protocol to prevent hidden-channel attacks," *2016 IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, New York, USA, pp. 1-7, 2016, doi: 10.1109/WiMOB.2016.7763267.

[26] V. E. Ekong and U. O. Ekong, "A survey of security vulnerabilities in wireless sensor networks," *Nigerian Journal of Technology*, vol. 35, no. 2, pp. 392-397, 2016, doi: 10.4314/njt.v35i2.21.

[27] S. Gupta, H. K. Verma, and A. L. Sangal, "Security attacks & prerequisite for wireless sensor networks," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 2, no. 5, pp. 558-566, 2013.

[28] M. D. Shah, S. N. Gala and N. M. Shekokar, "Lightweight authentication protocol used in Wireless Sensor Network," *2014 International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA)*, 2014, pp. 138-143, doi: 10.1109/CSCITA.2014.6839249.

[29] J. F. Raymond and A. Stiglic, "Security issues in the Diffie-Hellman key agreement protocol," *IEEE Transactions on Information Theory*, vol. 22, pp. 1-17, 2000.

[30] N. Ghanmy, L. C. Fourati, and L. Kamoun, "Elliptic curve cryptography for WSN and SPA attacks method for energy evaluation," *Journal of Networks*, vol. 9, no. 11, pp. 2943-2950, 2014, doi: 10.4304/jnw.9.11.2943-2950.

[31] E. Alnawafa and I. Marghescu, "New energy efficient multi-hop routing techniques for wireless sensor networks: static and dynamic techniques," *Sensors*, vol. 18, no. 6, p. 1863, 2018, doi: https://doi.org/10.3390/s18061863.

[32] H. Rhim, K. Tamine, R. Abassi, D. Sauveron, and S. Guemara, "A multi-hop graph-based approach for an energy-efficient routing protocol in wireless sensor networks," *Human-centric Computing and Information Sciences*, vol. 8, no. 1, pp. 1-21, 2018, doi: https://doi.org/10.1186/s13673-018-0153-6.

[33] J. Sumathi and R. L. Velusamy, "A review on distributed cluster based routing approaches in mobile wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-15, 2020, doi: https://doi.org/10.1007/s12652-020-02088-7.

[34] T. A. Alghamdi, "Energy efficient protocol in wireless sensor network: optimized cluster head selection model," *Telecommunication Systems*, pp. 1-15, 2020, doi: https://doi.org/10.1007/s11235-020-00659-9.

[35] R. Maharana and P. M. Khilar, "An improved authentication protocol for hierarchical wireless sensor networks using ECC," *International Journal of Computer Applications*, vol. 67, no. 22, pp. 23-30, 2013, doi: 10.5120/11528-7352.

BIOGRAPHIES OF AUTHORS

Kameran A. Ameen is currently instructor at University of Kirkuk, Kirkuk, Iraq. He received a B.Sc. degree in Computer Science from Kirkuk University/ College of Science, Kirkuk, Iraq in 2008 and an M.Sc degree in Information Technology from Cankaya University, Ankara, Turkey in 2015. He published his research in the following areas: Computer Networks, Security in Wireless Sensors Network, Authentication in Wireless Sensors Networks, Attacks in Wireless Sensors network and Encryption/Decryption.

Dr. Baban A. Mahmood is currently the head of Networks department at College of Computer Science and Information Technology-University of Kirkuk, Kirkuk, Iraq. He received his B.Sc, degree in Computer and Software engineering from University of Al-Mustansryah, Baghdad, Iraq, in 2003 and an M.Sc., degree in Computer Science from University of Sulaimaniya, Kurdistan, Iraq, in 2009. He also received an M.Sc., degree in Computer Science and PhD degree in Computer Science from University of Kentucky, Lexington, Kentucky, USA in 2015 and 2016 respectively. He published his research work in the following areas: routing in wormhole networks, routing in ad hoc networks, security of source routing protocols in MANET.

Yalmaz N. Taher is currently instructor at University of Kirkuk, Kirkuk, Iraq. He received a B.Sc. in Computer Science from Kirkuk University/ College of Science, Kirkuk, Iraq in 2006 and an M.Sc in Mathematics and Computer Science from Cankaya University, Ankara, Turkey in 2015. He published his research in the following areas: Database, Data mining and Cloud Computing.