A Hybrid Key Management Scheme for Wireless Sensor Network

Yanyan Han[1,2], Yanru He[1(✉)], Peihe Liu[1], Xiaoxuan Yan[1], and Na Li[2]

[1] Beijing Electronic Science and Technology Institute, 7 Fufeng Road, Beijing, China
hyr63476984@163.com
[2] Xidian University, 2 Taibai South Road, Xi'an, Shaanxi, China

Abstract. With the rapid development of the Internet of things (IoT), the wireless sensor network (WSN) as the most fundamental layer of the network is widely applied to the IoT, and more researchers focus on the security of WSN. Intrusion Detection System (IDS) is an important element in the security of computer system and smart devices. In this paper, a key management scheme which designed for WSN and based on area management is proposed under the premise that the system has IDS, and the scheme divides network into a number of non-overlapping hexagonal areas. In our scheme, two different key management modes are used for inter-regional and intra-regional communication respectively, and the certificates and keys of gateway node and cluster-head node can be efficiently managed by introducing the security gateway. The scheme not only can reduce the complexity of computation and storage effectively, but also improve the communication security and network connectivity.

Keywords: WSN · Key management · Identity · Authentication

1 Introduction

In recent years, the Internet of things has been known as the third wave of information era, and the wireless sensor network has broad application prospects in military detection, target tracking, situational awareness and other fields due to their advantages of high redundancy, low power consumption, self-organization and rapid deployment [1]. However, WSN is different from other traditional network because of resource-constrained sensor nodes, all of these make it difficult to run efficiently in the high-strength encryption algorithm, and most of nodes are generally deployed in exposed environment, it is easy to be physically accessed by adversaries, the key information stored in nodes can also be stolen. The adversary attacks the whole network by forging, tampering and so on, then finally leads to the collapse of the whole network. So, the key management is an essence of WSN security, and it is the security basis to manage the key in a reasonable and order way. Therefore, we propose a hybrid key management scheme, which divides WSN into several non-overlapping hexagonal network areas. Meanwhile, the security gateway is introduced to distribute security certificates to cluster-head nodes and gateway node, then it manages both certificates and keys

B. Shen et al. (Eds.): FCS 2019, CCIS 1105, pp. 347–364, 2019.
https://doi.org/10.1007/978-981-15-0818-9_22

effectively. Our scheme supports the key revocation and update of nodes, and has the ability to resist a variety of attacks. On the condition of ensuring high key connectivity, it effectively reduces the communication, computing and storage complexity of nodes, it also improves the network security compared with other schemes.

The remainder of the paper is organized as follows: Sect. 2 discusses some of classic key management schemes in WSN. According to the drawbacks of existing schemes, a hybrid key management scheme is proposed based on the characteristics of clustering wireless sensor network in Sect. 3. Section 4 gives the performance analysis of the proposed scheme. Finally, we conclude the superiority of the proposed scheme.

2 Related Work

Wireless sensor network nodes are generally deployed in extreme conditions, so most of them has the limitation of power, computing capability and storage capacity. Therefore, due to the characteristics of WSN, traditional key management schemes cannot apply, but key pre-distribution is an effective solution. Key pre-distribution scheme refers to the distribution of keys at the time of node deployment, and it only needs simple negotiation between nodes to encrypt the sessions during the network is running [1, 2]. Now numerous key management schemes based on key pre-distribution are proposed for WSN.

The earliest random key pre-distribution scheme is given by Eschenauer and Gligor [3] as basic scheme where a key pool is established first and each sensor node then randomly selects one of the keys in the key pool as the keyring for that node. Assuming that a communication link is to be established between two neighbor nodes, they must share the same key of the key ring, and a part of key is randomly selected as the key pair in communication links. This scheme has the advantages of low computational complexity, low storage pressure of nodes, and strong adaptability in dynamic network. But network connectivity is not high, and the key is selected based on probability, so the security is low. Once the node is captured by adversaries, it will threaten to the security of the link. Subsequently, Chan et al. [4] proposed the q-composite scheme. Compared with E-G [3] scheme, it requires that the nodes share at least q keys to establish a secure communication link. This scheme enhances the network security by improving the q value, but the network connectivity is worse. At the same time, the security of WSN will decrease rapidly with the increasing number of captured nodes. In [5–7], a series of improvement schemes and methods are put forward to solve such problems as low key connectivity, limited scale of network, high communication and storage cost. However, any compromised node will directly affect the security of key information in the entire WSN, and the key connectivity has not been effectively improved in these key management mechanisms. In [8], Blom et al. proposed a matrix-based key management mechanism. This mechanism not only allows any two nodes to establish a secure connection but also effectively improves network connectivity. In terms of security, the mechanism can ensures the network absolute safety unless more than λ nodes are compromised. Then an efficient key establishment and update mechanism based on Blom scheme is given by Hussain et al. [9]. But the scheme fails to solve the problem of threshold value λ, which means the security of the key is still

restricted to the threshold value λ. Deployment based key pre-distribution is presented by Du et al [10]. The design of the scheme is to implement a simple security connection and improve the network connectivity, simultaneously reduce the storage and computing requirements of nodes. But it cannot meet the expansion of the network, and the location information cannot be accurately obtained due to node position errors. Blundo et al. [11] gives a scheme based on polynomials, using the symmetry of polynomials to generate session keys between nodes. In this scheme, the communication cost of key establishment is reduced, and the storage cost of sensor nodes is reduced to ensure the expansion capacity of network to some extent. When the compromised nodes are less than t, the network is absolutely safe. However, with the increase of t, the storage overhead and computational complexity of nodes also increase sharply, which will shorten the network life to a certain extent, even result in a poor distributed management in the network. The LEAP scheme is given by Zhu et al. [12] which provides a beautiful idea for the application of key management for dynamically clustering, it can support multiple communication mode of WSN and a strong anti-destroying ability. Besides, any compromised nodes will not affect the others, and the scheme also provides authentication function, can resist the wormhole attack and so on. But the master key of the whole network will be saved by all nodes. Once the master key compromised, the network will be crashed. In addition, the scheme cannot support the nodes added and cannot adapt to the dynamic of network. Group key management schemes based on logical routing tree is proposed in [13] and [14]. The ultimate purpose of these schemes is to complete the establishment of group key to ensure multicast communication security, and reduce the cost in WSN. The existing key management schemes are unable to meet all requirements related to security, storage, computation and communication of WSN. Thus, a key management scheme is needed to improve the network connectivity, key management efficiency and communication security on the premise of ensuring low computing and storage costs.

3 The Proposed Scheme

According to the shortcomings of existing solutions, this paper proposes a hybrid key management scheme based on the assumption that the system has intrusion detection function, combined with the characteristics of clustering wireless sensor network. And this section details the working of the proposed scheme. The symbols and their meanings are listed in Table 1.

Intrusion Detection System (IDS) is an important element in the security of computer systems and smart devices, it can detect malicious actions and respond. There are various forms of responses, and the most common of which is to create an alert announcing an enemy invasion. However, intrusion detection system is not responsible for resisting intrusion [15], and its main functions are as follows: monitor device or user behavior, find and respond to suspicious activities, and report them to the administrator.

In contrast to common sensor nodes, the cluster-head node has stronger computing power, more sufficient energy and storage. Therefore, our scheme is based on the structure of clustering type and adopts the area management model divided network

Table 1. Symbols and their meanings

Symbol	Meaning
C_i	Regular hexagon grid area
K	Key space
m_{ij}	Node
$ID_{m_{ij}}$	Identifier of node
K_m	Space of shared key
$K_{m_{ij}m_{ik}}$	Session key
L_i	List of compromise node
Mes_{UK}	Key update message
h_i	Cluster-head node
GWN	Update message sent by the gateway node
*C*er	Security certificate
CA	Certificate Authority
rand	Random number generated by requester and responder
rand*	The random number decrypted by using private key of requester
rand**	The random number decrypted by using private key of responder

into non-overlapping hexagonal areas. The model is given in Fig. 1, and particularly, the non-overlapping hexagonal area is the leak-free area coverage model with the least repetition, which can guarantee the high connectivity of the network, and the specific proof can be known in [16]. Each area has a cluster-head node and several common sensor nodes. At the same time, the scheme includes both inter-area and intra-area key management schemes. The node in the area generates the core key by using the Blom matrix, and the session key of Inter-area is established by cluster-head node. The security gateway distributes security certificates to the cluster-head node and gateway node, and takes responsible for the certificate and key management between them.

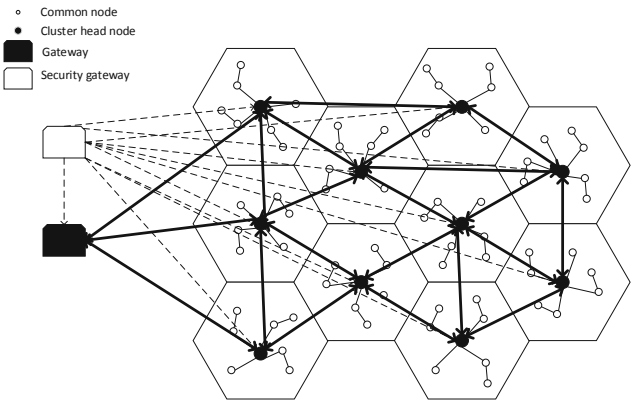

Fig. 1. The clustering type WSN architecture based on area management

In this structure, each hexagonal network area has a cluster-head node and the same number of common nodes. The security gateway as the root CA, distributes and manages the certificates for the cluster-head nodes and gateway node.

3.1 The Inter-area Key Management Scheme

Compared with the common sensor nodes, the cluster-head node owns more computation and communication capabilities, as well as more sufficient energy and storage. Thus, the cluster-head node is selected in our scheme as the communication bridge, and the session key between areas is established by the cluster-head node in each area. Security gateway is introduced as root CA in the scheme, and used for certificating and managing gateway node and cluster-head nodes. Nevertheless, if gateway communicate with cluster-head nodes, the security gateway does not participate. The security gateway is mainly composed of five parts, including main control board, security management module, key agreement module, identity authentication module and encryption and decryption module. The main control module is the control center which manages key and certificate of both the cluster-head and gateway nodes, the key agreement module and the identity authentication module are used to the key agreement and identity authentication between nodes, and the secret key is generated in the encryption and decryption module. According to whether the gateway node is connected to the IP network and send data to the cloud platform, the working mode is divided into online or offline mode. In the online mode, the gateway node manages the key and certificate of the nodes in WSN. While the gateway node and cluster-head nodes are managed by the security gateway with certificate and key management in the offline mode. Figure 2 shows the diagram of security gateway, and the structure of cluster-head node is shown in Fig. 3. Where the arrows in the two figures represent the relationships and data flow interactions between the important components of the nodes.

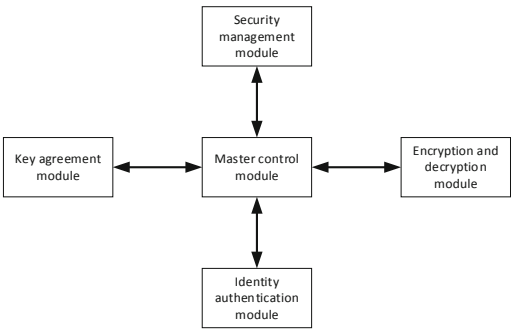

Fig. 2. The structure of security gateway node

In the offline mode, the security gateway selects gateway node and cluster-head nodes to establish the safety management network. The security gateway updates the certificates and the root CA public key of gateway node and cluster-head nodes for authentication. The session key is required in the step of key agreement before updating,

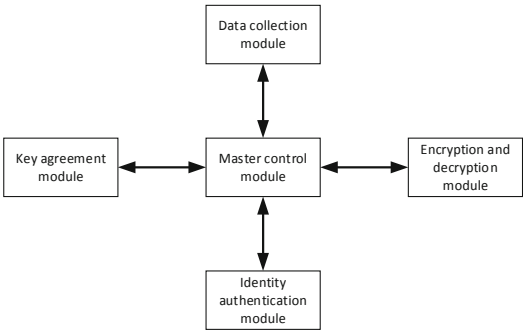

Fig. 3. The structure of cluster-head node

and the certificates of gateway and all cluster-head nodes must be updated after get the new public key. The process of inter-area security communication is as follows:

Step.1 Gateway and cluster-head nodes start identity authentication and key agreement to obtain session key;
Step.2 The gateway gets the cluster-head nodes information by ciphertext transmission;
Step.3 The cluster-head nodes in each area transmit data with ciphertext.

Safety binding is required for cluster-head nodes before deploying the network in each area. The flowchart of cluster-head nodes bound by security gateway is shown in Fig. 4.

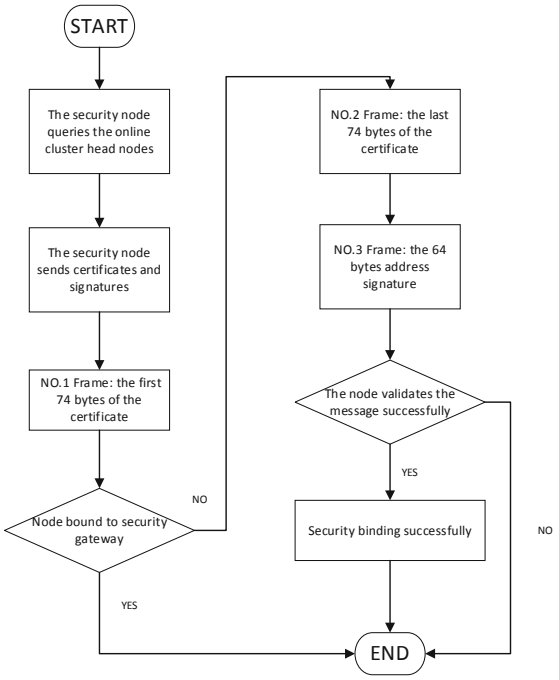

Fig. 4. The cluster-head node safety bound by the security gateway

In the scheme, the length of the data for security binding commands is 212 bytes. One of the 148 bytes are the security gateway certificate or gateway certificate and the rest of 64 bytes are the signature. The security gateway transmits the data as three frames. The first frame is the first 74 bytes of the certificate, containing the information whether the node is bound or not. After receiving the first frame, the cluster-head node will respond a secure bound message to the security gateway. The data of second frame is the remaining 74 bytes of the certificate. In the third frame, the 32-bytes address of the security gateway that sent the binding command is signed as a 64 bytes value. Then the cluster-head node will respond the data frame by frame, which is the secure binding command sent by the security gateway. After the first frame is sent, the remaining two frames are stopped immediately. Then the cluster-head node validates the first frame to verify whether the node has been bound or not. If the binding is done, it is the time to send the address information to security gateway and end the conversation. Otherwise, security gateway will continue to send the second frame, and the cluster-head node will receive and store the second frame data. Then, the security gateway continues to send the address signature information of the third frame, and the cluster-head node will call for the certificate from the security module to assure whether the message is sent by the security gateway. After passing the verification, the address of the cluster-head node is sent to the security gateway to complete the binding. If the binding is failed, it will return a 16-bit-all-zero message. After that, the identity authentication and key agreement between the gateway node and the cluster-head node should be carried out. Both gateway node and cluster-head node can initiate a request for confidential communication. For convenience, the party initiating the communication is called Requester A, and another party is called Responder B. The communication interaction process is shown in Fig. 5.

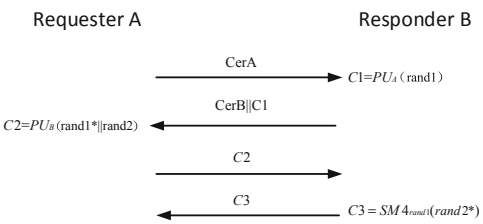

Fig. 5. Authentication and key agreement of the Inter-area

The detailed process of communication is as follows:

(1) Requester A reads its certificate *Cer*A and sends it to Responder B.
(2) Responder B reads the root public key, then uses the key to verify the certificate *Cer*A sent by Requester A, and gets the public key PU_A of Requester A. Then, Responder B generates the random number rand1, and the SM2 algorithm is used to encrypt rand1 to get C1. The encryption key is the public key of the requester PU_A. Finally, the certificate *Cer*B of responder is transmitted along with C1 to the Requester A.

(3) After receiving the message, Requester A uses the root public key to verify the certificate *CerB* sent by responder B and get the public key of responder B PU_B. Then, using its private key to decrypt the received information C1, get rand1∗, and generate random number rand2. After that, the public key PU_B is used as the encryption key and the SM2 algorithm is used to encrypt rand1∗ and rand2 to get C2. Finally, C2 is sent to Responder B.
(4) After receiving the message C2 sent by Requestor A, Responder B decrypts it with its own private key and gets rand1∗∗ and rand2∗. And then determine whether rand1∗∗ and rand1 are equal. If not, end the session. Otherwise, use rand1 as the encryption key and use SM4 algorithm to encrypt rand2∗ to get C3. Finally, C3 is sent to Requestor A.
(5) Firstly, the Requestor A uses rand1∗ as the decryption key to get rand2∗∗ after receiving the information C3. Then, if rand2∗ and rand2 are equal, the authentication is successful and rand1 is used as the encryption key. Otherwise, authentication fails and the session ends.

Above all, the authentication and key agreement mode between cluster-head node and security gateway can effectively realize the authentication and ensure the security of identity information during the process of communication.

3.2 The Intra-area Key Management Scheme

In the intra-area key management scheme, cluster-head node and common node are not distinguished. The session keys between the nodes use the Blom matrix to generate the core keys, and this scheme gives a different key space for each area, then allocates the key of each node according to the node's ID and other deployment information.

(1) Key pre-distribution phase

In the initialization stage, the server first constructs a $(t+1) \times N$ Vandermonde matrix in the finite field GF(q). And t is the security threshold of the shared key, if t or more sensor nodes are compromised in the network, the WSN is not secure. Take Area C_i as an example, there are m nodes in C_i, and each node has a unique ID, where Area G_i represents the Vandermonde matrix of C_i then we can get matrix G_i as follows:

$$G_i = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ (ID_{m_{i1}})^1 & (ID_{m_{i2}})^1 & \cdots & (ID_{m_{iN}})^1 \\ (ID_{m_{i1}})^2 & (ID_{m_{i2}})^2 & \cdots & (ID_{m_{iN}})^2 \\ \vdots & \vdots & \ddots & \vdots \\ (ID_{m_{i1}})^t & (ID_{m_{i2}})^t & \cdots & (ID_{m_{iN}})^t \end{bmatrix} \tag{1}$$

Then, the server randomly generates a $(t+1) \times (t+1)$ symmetric secret matrix D_i in the finite field GF(q), and the Blom matrix A_i of the area can be obtained:

$$A_i = (D_i \cdot G_i)^T \tag{2}$$

The Key Space is the matrix $K = A \cdot G$, and it is represented by K_i as follows:

$$\begin{aligned} K_i &= A_i \quad \cdot \quad G_i \\ &= (D_i \quad \cdot \quad G)_i^T \quad . \quad G_i \\ &= G_i^T \quad . \quad D_i \quad . \quad G_i \\ &= (A_i \quad . \quad G)_i^T \\ &= K_i^T \end{aligned} \tag{3}$$

Then, taking m_{ij} as an example, any node in Area C_i only need to store the $\mathrm{row}_j(A_i)$ of matrix A_i, and the identifier of node $ID_{m_{ij}}$ in advance.

(2) Key establishment phase

The key information stored by all nodes in the regular hexagon grid area comes from the matrix G_i and A_i. Node m_{ij} and node m_{ik} in C_i store information $\left\{\mathrm{ID}_{m_{\mathrm{ij}}}, \mathrm{row}_j(A_i)\right\}$ and $\{\mathrm{ID}_{m_{\mathrm{ik}}}, \mathrm{row}_k(A_i)\}$ according to the key pre-distribution respectively, the space of shared key between node m_{ij} and m_{ik} is $K_m = (A_m \cdot G_i)$.

Firstly, node m_{ij} and node m_{ik} exchange their node identification information ID with each other. Then the node m_{ij} is computed by using $ID_{m_{ik}}$:

$$\begin{cases} col_k = & [1 & (ID_{m_{ik}})^1 & (ID_{m_{ik}})^2 & \cdots & (ID_{m_{ik}})^t]^T \\ K_{m_{ij}m_{ik}} = & \left[row_j(A_i)\right] & \times & [col_k(G_i)] & & \end{cases} \tag{4}$$

Then we can get the session key $K_{m_{ij}m_{ik}}$ between node m_{ij} and m_{ik} from symmetry:

$$K_{m_{ij}m_{ik}} = K_{m_{ik}m_{ij}}, \tag{5}$$

(3) The key updates and revocation

When the gateway node detects that a node has been compromised by an adversary in the WSN, the system can revoke the session key established. Intrusion detection as an active defense technology can prevent internal and external attacks [15], which has become a strong security premise for WSN. The premise of our scheme is that the system has intrusion detection function [17, 18], and the system sends the list of compromised nodes to the gateway node for key update. The process of key update and revocation is shown in Fig. 6.

Suppose that the compromise node list is $L_i = \left(m_{i1}, m_{i2,} \cdots, m_{ik}\right)$ in the regular hexagon grid area, and the steps of update are as follows:

A. In the finite field, the gateway node randomly generates a new $(t+1) \times (t+1)$ secret matrix, then it can be obtained from the regular hexagon grid area C_i:

$$\begin{cases} A_i^* = (D_i \cdot G_i)^T \\ Sum_i = A_i + A_i^* \end{cases} \tag{6}$$

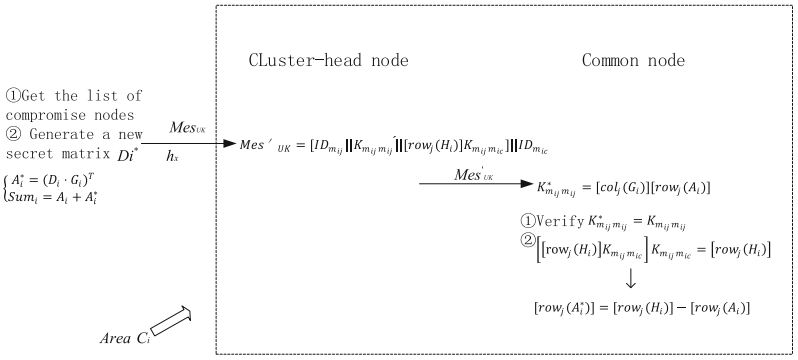

Fig. 6. The key update and revocation process

B. Set up an n-dimensional row vector R_i. If node m_{ij} is in list L_i, then $R_i[j] = 0$, otherwise, $R_i[j] = 1$.
C. Create a matrix $H_i = \mathrm{Sum}_i \cdot R_i$.
D. The gateway node sends the update key message to the cluster-head node h_i of C_i. Assuming that the message passes in the middle cluster-head node h_x, then:

$$\begin{cases} K_{m_{ij}m_{ij}} = [col(G_i)] \cdot [row(A_i)] \\ Mes_{UK} = [ID_{m_{ij}} || K_{m_{ij}m_{ij}} || [row_j(H_i)] | 1 \le j \le n] K_{h_x h_i} || GWN \end{cases} \tag{7}$$

And GWN means that the message is sent by the gateway node, and later nodes can use $K_{m_{ij}m_{ij}}$ to verify the correctness of the message. $K_{h_i h_x}$ represents the encryption of $[ID_{m_{ij}} || K_{m_{ij}m_{ij}} || [row_j(H_i)] | 1 \le j \le n]$, after the cluster-head node h_i receives the message, we uses the stored shared key $K_{h_i h_x}$ to decrypt the message and gets $[ID_{m_{ij}} || K_{m_{ij}m_{ij}} || [row_j(H_i)] | 1 \le j \le n]$.

Then, the cluster-head node h_i in C_i sends the key update message Mes_{UK} to all legitimate common nodes based on the node identifier in the area:

$$\begin{aligned} &h_i(m_{ic}) \rightarrow m_{ij}: \\ &Mes'_{UK} = [ID_{m_{ij}} || K'_{m_{ij}m_{ij}} || [row_j(H_i)] K_{m_{ij}m_{ic}}] || ID_{m_{ic}} \end{aligned} \tag{8}$$

When the common node receives the key update message, it will calculate according to its stored information:

$$K^*_{m_{ij}m_{ij}} = [col_j(G_i)][row_j(A_i)] \tag{9}$$

Then to judge $K^*_{m_{ij}m_{ij}} = K_{m_{ij}m_{ij}}$, if not equal that we can make sure the message is not from the gateway and discard it. Otherwise, the key is updated.

$$\left[\left[\mathrm{row}_j(H_i)\right]K_{m_{ij}m_{ic}}\right]K_{m_{ij}m_{ic}} = \left[row_j(H_i)\right]$$

$$\left[row_j\left(A_i^*\right)\right]=\left[row_j(H_i)\right]-\left[row_j(A_i)\right] \tag{10}$$

Finally, we can get new key information $row_j\left(A_i^*\right)$. For compromised nodes, because of the $\mathrm{row}_j(H_i)$ is 0, key updates cannot be performed, and the later data communication and other operations cannot be carried out. By judging the key information, the node can receive the message of the gateway node in time, then update the key and communicate.

3.3 The Application of Proposed Scheme

Our scheme divides the network into hexagonal sub-areas with full coverage, so it mainly applied to the perception layer with cellular architecture in the Internet of Things. The prominent advantage of our scheme is and realize the central key management and authentication through cluster-head nodes in each area, so as to simplify the communication process and reduce the cost. At the same time, the security gateway is introduced to enhance the ability of anti-attacking. The performance analysis and comparison are described specifically in Sect. 4.

The application process of the scheme is shown as follows: Firstly, in the offline mode, the security gateway starts to bind and identify cluster-head nodes and gateway nodes, so as to realize certificate and key management. Secondly, in the online mode, the security gateway stops working. If we do intra-area communication, cluster-head nodes as same as other common nodes start key agreement to obtain communication keys and, then complete secret communications. If we do inter-area communication, the gateway will set up a secure network with each cluster-head node, then obtain the communication key through identification, and complete the secret communication. Especially, the security gateway usually works in the offline mode. Once the gateway node is attacked, the security gateway will start the emergency response and work in the online mode temporarily instead of the gateway. Moreover, the introduction of security gateway enhances the system's anti-attacking with the acceptable overhead.

4 Performance Analysis of the Proposed Scheme

4.1 Security

4.1.1 Security of Compromised Node

In the scheme, if anyone wants to attack a key space successfully, he must gain $\mathbf{t}+1$ nodes in that area. If the total number of nodes does not exceed $\mathbf{t}+1$, the network is absolutely safe. In addition, when the gateway node finds that the sensor node is compromised, it will send the update message to the node in that area. After other common nodes receive the message of key update, it obtains the new key information through calculation. However, the operation of key update cannot be completed for the compromised node. Therefore, our scheme shows the probability of key leakage through any compromised node is 0 in the hexagon area.

Inter-area communication is conducted by cluster-head nodes. We introduce a security gateway as the root CA to accomplish certificate and key management for gateway nodes and cluster-head nodes. Even if the gateway node and the cluster-head node are controlled by the attacker, the important information such as the communication key and the pairing key will not be disclosed. At the same time, bidirectional authentication performed firstly in communication, and a new session key is created each time which can effectively prevent malicious nodes, and establish trust between the nodes. Therefore, even if the previous session key is captured, the attacker cannot get other session keys. In inter-area communication, the scheme chooses the three-way authentication based on certificate, so it can resist replay attack. Figure 7 shows the ratio of the number of compromised nodes to the number of links affected.

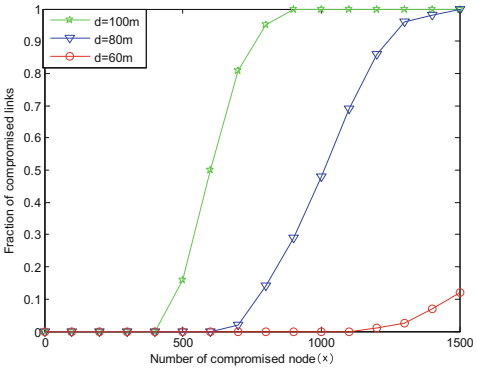

Fig. 7. The ratio of the number of compromised nodes to the number of links affected

Assuming that the number of compromised nodes is x, and the probability of the key space information contained in each node is expressed as $p = \mu/\omega$, Then the expression of probability that the number of compromised nodes and the corresponding key space are all broken by the attacker is as follows:

$$P = \sum_{i=t+1}^{x} C_x^i p^i (1-p)^{x-i} \tag{11}$$

Among them, d represents the side length of the regular hexagon area. It can be concluded that with the expansion of area and the same number of compromised nodes, the proportion of affected communication links will increase accordingly. That is, the more compromised nodes are concentrated in an area, the more vulnerable the area is to an attacker.

4.1.2 Random Attack Security Analysis

Random attack means that the adversary attacks the network without knowing the node distribution and key management scheme. For a better comparison with the existing solutions, the deployment densities of the nodes should be the same. Figure 8 shows the comparison of the scheme's ability to resist random attacks with E-G [3] scheme

and q-composite [4] scheme. It can be concluded from the experimental results that our scheme has better anti-random attack ability, and when the number of nodes acquired by the adversary is equal, the influence of the communication link suffered takes up the smallest proportion.

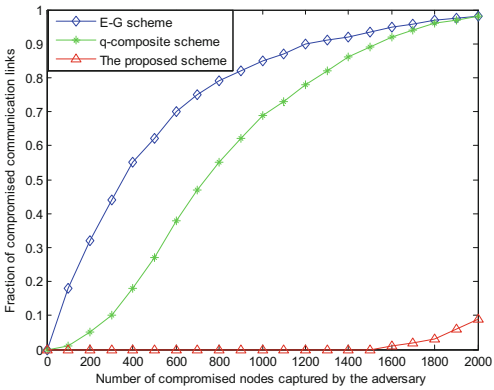

Fig. 8. Comparison of anti-random attack schemes

(1) Resist physical capture attacks

In the inter-area communication, the scheme introduces a security gateway as the root CA which is the key distribution center, and manage the certificate and key for the gateway node and cluster-head node. Even if those critical nodes, like the gateway node and the cluster-head nodes, are captured and controlled by the adversary, the group communication key, broadcast key, pairing key and other important information will not be revealed. When communicating inside the area, take area C_i as an example, the node m_{ij} only needs to store the $\text{row}_j(A_i)$ and $ID_{m_{ij}}$. Even if the node is captured and controlled by the attacker, the group key and other important information will not be leaked. Therefore, our scheme can resist physical capture attack no matter it is inter-area or intra-area communication.

(2) Resist eavesdropping attack

In each authentication process of inter-area communication, the cluster-head node and gateway node will generate a new session key randomly, so the new generated key is different from the previously generated. Even if the previous session key is captured, the adversary cannot get other session keys. In the process of intra-area communication authentication, when the gateway node detects that a compromised node, the system can revoke the established session key. But all of above are under the premise of the system has intrusion detection function [17, 18], and the system sends the list of compromised nodes to the gateway node for key update. In conclusion, the scheme can prevent eavesdropping effectively.

(3) Resist replay attack

The authentication process of inter-area communication adopts the three-way authentication based on digital certificate. Since the random number is generated randomly, the third party cannot know it, so when verifying the signature sent by the other party, it can determine whether the message has been modified in the session by comparing the generated random number is equal to itself. After the gateway node of the intra-area finds that the sensor node is compromised, it will send the update message to other nodes in the area. After other nodes receive the key update message, it updates the new key by calculating. Therefore, the adversary cannot conduct a replay attack to the WSN through the compromised node and the scheme can resist replay attack.

(4) Resist fake node attacks

In the proposed scheme, both sides of any communication are bidirectional authenticated before the session key is generated in the inter-region communication. The asymmetric key system is used between the gateway node and the cluster-head node. Both sides of the communication use the public key for encryption, and the private key is used for decryption, which has strong security. For the cluster-type network, key management adopted in this scheme, it is most vulnerable to the cluster-head fake attack of the adversary, and the adversary obtains the node identifier of the cluster-head node after compromise the common node, and then fake as the cluster-head node to broadcast the information to other common nodes. This scheme has the function of intrusion detection, which can detect any compromised node, and once it detected, the it will update the key immediately. When the cluster-head node communicates with the common node, it will first verify whether the key update message is from the gateway node, and if so, the key update operation will be completed. Otherwise, the session ends. In the inter-area communication, if there is a compromised node, the gateway will take the action of key update, and the compromised node cannot complete an update and obtain the communication key. Therefore, the scheme can resist node fake attack.

4.2 Connectivity Analysis

For the inter-area communication established by cluster-head nodes, a security gateway is introduced as the root CA to manage the certificate and key of both gateway node and cluster-head nodes. Before the cluster-head nodes communicate, bidirectional authentication and key agreement should be complete. Therefore, secure sessions can be established between any cluster-heads node, and the connectivity is 1. For the nodes in the intra-area, any node can establish the session key by exchanging the node identifier ID with the neighboring node, so as to achieve the secure communication. Therefore, a secure session can be established between any node in the area for so the connectivity is also 1.

Therefore, the network connectivity of our scheme is always 1. The comparison figure of the network connectivity between the proposed scheme and E-G [3] scheme and q-composite [4] scheme is shown in Fig. 9.

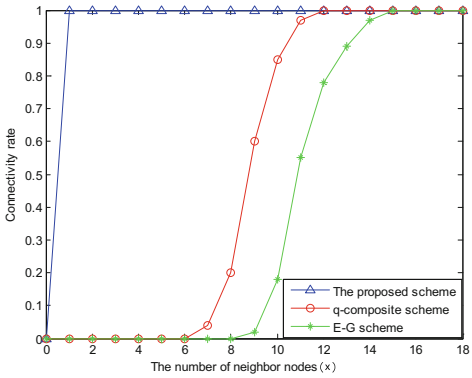

Fig. 9. Comparison of the network connectivity

As it can be seen from Fig. 9, in our scheme, as long as the number of neighbor nodes is not zero, the network connectivity rate is 100%. For E-G [3] scheme, the network connectivity rate can reach 100% only when the number reaches 14 or more. While the q-composite [4] scheme has the worse one, and the number must reach 16 or more, so that the network connectivity rate can reach 100%.

4.3 Performance Analysis of Storage

Common nodes in the intra-area only need to exchange their identifier IDs with each other, and the session key can be established without key agreement. In addition, common nodes need to store only the column of information corresponding to the public matrix G and the row of information corresponding to the Blom matrix A. The required space of single node to store key information is: $k = (t+1) * \mu + t + 1$. At the same time, because there is not the same key space between each regular hexagon grid region, it can contribute to isolation, so it avoids a lot of unnecessary communication consumption. The relationship between the number of key spaces and the number of areas required is shown in Table 2.

Table 2. Total required of key space

Total required number of keys	2	3	4	5	6
The number of areas	2	14	20	12	126

The cluster-head node has fewer neighboring nodes, so it can reduce the communication cost of key establishment. At the same time, most of the energy in WSN is used for communication, so the reduction of communication overhead can reduce the lifetime of WSN. The scheme is compared with E-G scheme [3], q-composite scheme [4] and LEAP scheme [12] in terms of computational, communication and storage complexities. The comparison results are shown in Table 3.

Table 3. Performance comparison of key management schemes

	Storage complexity	Computation complexity	Communication complexity
E-G scheme [3]	$O(k)$	$O(k)$	$O(2)$
q-composite scheme [4]	$O(m)$	$O(m)$	$O(2)$
LEAP scheme [12]	$O(d+l)$	$O(d^2/N)$	$O(\log N)$
The proposed scheme	$O(2)$	$O(2)$	$O(2)$

As shown in Table 3, the storage cost, computing cost and communication cost of our scheme are greatly reduced compared with others.

5 Conclusion

WSN as the perception layer is the lowest layer of the standard three-layer architecture of the Internet of things. The WSN nodes are often deployed in extreme conditions with limited resource. Therefore, traditional key management is not suitable for WSN. The hybrid key management scheme proposed in this paper is based on the premise that the system has intrusion detection function. It introduces security gateway to manage the key and certificate of gateway node and cluster-head nodes, so as to effectively prevent the key information leakage. In our scheme, the network is divided into non-overlapping hexagonal network regions with a cluster-head node and a number of common sensor nodes. In the inter-area, the communication overhead is reduced and the security of communication is improved by key agreement and bidirectional authentication between cluster-head nodes. In the intra-area, the key pre-distribution of identifiers is exchanged between nodes, which greatly reduces the computing cost, thus achieving high efficiency of key management. Compared with other classical schemes, the results are shown the higher security and efficiency of key management, as well as the better network connectivity.

References

1. Yu, B., Zhou, W., Bin, Y., et al.: ZigBee model for detection and suppression of same-frequency attacks. J. Electron. Inf. Technol. **37**(9), 2211–2217 (2015)
2. Lotfallahtabrizi, P., Morgan, Y.: A novel host intrusion detection system using neural network. In: Computing and Communication Workshop and Conference, pp. 124–130. IEEE (2018)
3. Eschenauer, L., Gligor, V.D.: A key-management scheme for distributed sensor networks. In: ACM Conference on Computer and Communications Security, pp. 41–47 (2002)
4. Chan, H., Perrig, A., Song, D.: Random key predistribution schemes for sensor networks. In: Proceedings of 2003 Symposium on Security and Privacy, pp. 197–213. IEEE (2003)

5. Du, W., Deng, J., Han, Y.S., et al.: A key management scheme for wireless sensor networks using deployment knowledge. In: IEEE INFOCOM 2004: Twenty-Third Annual Joint Conference of the IEEE Computer and Communications Societies, Hongkong, pp. 586–597. IEEE (2004)
6. Huang, D., Mehta, M., van de Liefvoort, A., et al.: Modeling pairwise key establishment for random key predistribution in large-scale sensor networks. IEEE/ACM Trans. Netw. **15**(5), 1204–1215 (2007)
7. Wang, H., Yang, J., Wang, P., Tu, P.: Efficient pairwise key establishment scheme based on random pre-distribution keys in WSN. In: Taniar, D., Gervasi, O., Murgante, B., Pardede, E., Apduhan, Bernady O. (eds.) ICCSA 2010. LNCS, vol. 6018, pp. 291–304. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-12179-1_26
8. Blom, R.: An optimal class of symmetric key generation systems. In: Beth, T., Cot, N., Ingemarsson, I. (eds.) EUROCRYPT 1984. LNCS, vol. 209, pp. 335–338. Springer, Heidelberg (1985). https://doi.org/10.1007/3-540-39757-4_22
9. Hussain, A.W., Ibrahem, M.K.: An efficient pairwise and group key management scheme for wireless sensor network. Int. J. Enhanc. Res. Sci. Technol. Eng. **1**(4), 25–31 (2015)
10. Du, W., Deng, J., Han, Y.S., et al.: A pairwise key predistribution scheme for wireless sensor networks. ACM Trans. Inf. Syst. Secur. (TISSEC) **8**(2), 228–258 (2005)
11. Blundo, C., Santis, A.D., Herzberg, A.: Perfectly-secure key distribution for dynamic conferences. Inf. Computat. **146**(1), 1–23 (1998)
12. Zhu, S., Setia, S., Jajodia, S.: LEAP: efficient security mechanisms for large-scale distributed sensor networks. In: ACM Conference on Computer and Communications Security, Dallas, USA, pp. 62–72. ACM (2003)
13. Jiang, R., Luo, J., Wang, X.: HRKT: a hierarchical route key tree based group key management for wireless sensor networks. KSII Trans. Internet Inf. Syst. **7**(7), 2042–2060 (2013)
14. Jiang, R., Luo, J., Wang, X.: A logic-route key tree based group key management scheme for wireless sensor networks. In: 2013 IEEE/CIC International Conference on Communications in China (ICCC), Xi'an, pp. 686–691. IEEE Computer Society (2013)
15. Du, Y., Zhang, Y., Li, M., et al.: Optimization method of intrusion detection sample data based on improved FastICA algorithm. J. Commun. **37**(1), 42–48 (2016)
16. Zhao, S., Zhang, Z.: Research on regular hexagon node coverage model of wireless sensor network. Comput. Eng. **36**(20), 113–115+118 (2010)
17. Manikandan, G., Sakthi, U.: A comprehensive survey on various key management schemes in WSN. In: 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, pp. 378–383 (2018)
18. Gautam, A.K., Kumar, R.: A comparative study of recently proposed key management schemes in wireless sensor network. In: 2018 International Conference on Computing, Power and Communication Technologies (GUCON), Greater Noida, Uttar Pradesh, India, pp. 512–517 (2018)
19. Bechkit, W., Challal, Y., Bouabdallah, A.: A highly scalable key pre-distribution scheme for wireless sensor networks. IEEE Trans. Wirel. Commun. **12**(2), 948–959 (2013)
20. Chakavarika, T.T., Chaurasia, B.K., Gupta, S.K.: Performance evaluation of a polynomial based key management scheme in wireless sensor networks. In: 2016 International Conference on Communication and Signal Processing (ICCSP), Melmaruvathur, pp. 2114–2118 (2016)
21. Kamble, S.B., Jog, V.V.: Efficient key management for dynamic wireless sensor network. In: 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology (RTEICT), Bangalore, pp. 583–586 (2017)

22. Ahlawat, P., Dave, M.: An improved hybrid key management scheme for wireless sensor networks. In: 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), Waknaghat, pp. 253–258 (2016)
23. Msolli, A., Ameur, H.: A new secure key management scheme for wireless sensor network. In: 2017 International Conference on Control, Automation and Diagnosis (ICCAD), Hammamet, pp. 254–257 (2017)
24. Prema, S., Pramod, T.C.: Key establishment scheme for intra and inter cluster communication in WSN. In: 2018 Second International Conference on Computing Methodologies and Communication (ICCMC), Erode, pp. 942–944 (2018)
25. Patel, J.S., Chavda, V.M.: Security vulnerability and robust security requirements using key management in sensor network. Int. J. Grid Distrib. Comput. **7**(3), 23–28 (2014)