Hindawi
Security and Communication Networks
Volume 2022, Article ID 1059997, 9 pages
https://doi.org/10.1155/2022/1059997

Research Article

A CFL-Based Key Management Scheme for Routing-Driven Internet of Things

Jiuru Wang, Chongran Sun, Haifeng Wang, Bin Zhao, and Ping Gong

School of Information Science and Engineering, Linyi University, Linyi, Shandong 276005, China

Correspondence should be addressed to Bin Zhao; jnzhaobin@163.com

Received 7 January 2022; Revised 10 March 2022; Accepted 22 March 2022; Published 26 April 2022

Academic Editor: Zheng Yang

This study is aimed at the authentication problem between the node's public key and the node in the sensor network of the Internet of Things(IoT). As well as the sensor node key distribution needs to verify trusted nodes, resulting in a lot of storage and computational overhead problems. A routing-driven key management scheme for the IoT based on identification certificate authentication system is proposed. The scheme takes the identification key pair of the node as the verification key to verify the random key pair generated by the node to ensure that the whole process does not need the intervention of a trusted third party; random key pairs are generated by nodes independently to ensure that each sensor node has different keys. When a node is broken, it will not cause damage to other nodes. At the same time, the shared key is only established for adjacent sensor nodes that communicate with each other to ensure the security and lightweight storage overhead of the sensor nodes. The experimental analysis shows that the scheme can provide better security, can effectively reduce sensor nodes' storage space and energy consumption, and has higher advantages in safety and performance.

1. Introduction

The mobile IoT is an important part of the new infrastructure. Promoting the innovative development of the mobile IoT will help accelerate the digital transformation of traditional industries and further support the construction of manufacturing power and network power. Applying the technology of the Internet of Things to the construction of smart cities will help improve the urban structure and enhance the city's comprehensive service level [1]. The essential thing for building a smart city is the sensor network (HSN), composed of different types of sensor nodes as the sensing layer of the IoT. Ensuring safe communication between sensor nodes is a priority issue for the IoT [2]. Therefore, key management aiming to provide secure and reliable communication is the most critical and essential content of IoT security research [3]. The research on key management based on wireless sensor networks has achieved many results in traditional networks. However, due to the limited resources of IoT nodes, lack of infrastructure support, and the vulnerability of deployment environments, many existing research results (Such as PKI/CA technology) cannot be directly applied [4].

In recent years, the proposed key management scheme has been mainly based on the public key cryptosystem authentication method. Its core solution lets each node share a key with its neighboring nodes to achieve secure communication [5]. Choi et al. [6] proposed an encryption strategy based on geographic location information that only relies on node location information. The strategy does not need to know the specific deployment information of the node and considers the attack situation inside and outside the node but does not consider the problem of node identity authentication, resulting in poor security. Zhang et al. [7] and others proposed a lightweight asymmetric group key agreement protocol between clusters, which established a secure and efficient group communication channel for sensor nodes between clusters. Elhoseny [8] et al. proposed a key management scheme of elliptic curve cryptography algorithm and homomorphic encryption algorithm based on asymmetric public key cryptosystem, which reduced the cost of communication, memory, and energy. Alappatt and

Prathap [9] mixed Diffie-Hellman key exchange and Elliptic Curve Cryptography (ECC) methods so that each cluster head in the cluster keeps the public key of its corresponding member node and only acts as a router. Mesmoudi et al. [10] proposed a dynamic key management scheme for HSN to ensure the scalability and flexibility of the network.

From the above key management scheme analysis, it can be seen that in the public key cryptosystem, the binding between the public key and the node is mainly based on certificate authentication and identity authentication. However, there are still some defects in these two authentication methods: the node public key (PK) has nothing to do with the node identification in certificate authentication; it needs to be proved by a trusted third party [11]. In identity authentication, the node key is entirely generated by the Key Management Center (KMC), and the node has no complete control over its private key (SK). Furthermore, in the HSN network, to ensure the connectivity of the whole IoT, each node needs to store a sizeable key pool, resulting in colossal storage and computing pressure. Especially when the sensor network is connected to other external networks (including the Internet), it is easy to be attacked by external networks. Once the attacker obtains the information of the key pool from the captured node, the entire network's security may collapse.

This paper aims at the defects of the public key authentication way of sensor nodes in the existing key management schemes and the fragile security and limited resources of sensor nodes in IoT networks. Combined with the identification-based certificate authentication scheme CFL (C, F, and L are the first letters of the last name of three inventors, Chen Huaping, Fan Xiubin, and Lv Shuwang), a route-driven key management scheme based on CFL is analyzed and constructed. The scheme only establishes the shared key for the adjacent sensor nodes that may communicate with each other and uses the CFL authentication system to select the shared key. The identification key pair of the node is used as the verification key pair to verify the random key pair generated by the node. At the same time, the random key pair makes each sensor node have different keys. When a node is broken, it will not cause damage to other nodes. The whole process does not need the intervention of a trusted third party to ensure the security and lightweight storage overhead of the sensor node. An efficient and trusted scheme is proposed to solve the security problems of authentication and communication of node and public key binding in the IoT.

2. Preliminaries

2.1. Identity-Based Certificate Authentication System CFL. CFL is a new identification-based authentication system, which combines certificate authentication and identity authentication. The CFL certification system was first introduced in 2011 and approved by the National Password Administration in 2016 [12, 13]. This scheme combines Public Key Infrastructure (PKI) and Identity-based Cryptography (IBC) authentication schemes to overcome the shortcomings of the existing authentication schemes, making this algorithm a self-authentication authentication algorithm. It achieves centralized key management and guarantees the user's ownership of the random private key. It can meet the security needs of users in public networks to protect their privacy.

The basic key pair of this scheme consists of an identity key pair and random key pair. User ID generates identity key pair as certificate signature and verification key pair and provides certificate signature and verification for user-generated random key pair. A certificate authentication system with a self-certification function is formed, and the whole verification process does not require the intervention of trusted third parties. The specific steps shown in Figure 1 include the following:

(1) User

① Generate real identity ID and generate a random set of public and private key pairs (RAPK, RASK) according to the selected working password algorithm.

② Submit the user identity ID and the self-generated random public key RAPK to the Key Management Center (KMC). The KMC is a credit endorsement that certifies that the ID and signature are generated by a trusted institution.

(2) Key Management Center (KMC)

③ KMC reviews the submitted identification ID to ensure its authenticity and uniqueness

④ Generate an identification key pair (IDPK, IDSK) according to the submitted information

⑤ Use IDSK as the key to sign the certificate with RAPK as the core content and issue the signed certificate to the user

(3) Public side

⑥ Use IDPK as the public key of the verification algorithm to verify the signed certificate. If the verification is correct, the certificate is passed; otherwise, it is not passed.

2.2. Route-Driven Key Management Scheme. In addition to many ordinary sensor nodes (L-Sensors), there are also some special wireless communication devices (H-Sensors) with strong storage and computing power. HSN uses the many-to-one communication mode in the IoT to divide the sensor nodes into several clusters through a clustering algorithm. Each cluster contains a high-energy node and multiple ordinary nodes (shown in Figure 2). Among them, the high-energy node, also known as the cluster head, is responsible for controlling the normal operation of a cluster [14]. The *L* sensing node is responsible for collecting information from the surrounding environment and sending the collected information to the H sensing node through multihop communication [15]. Each sensor node transmits the data to the cluster head node in the cluster. After data fusion, the cluster head node uses multihop communication to send the data to the sink node (sink).

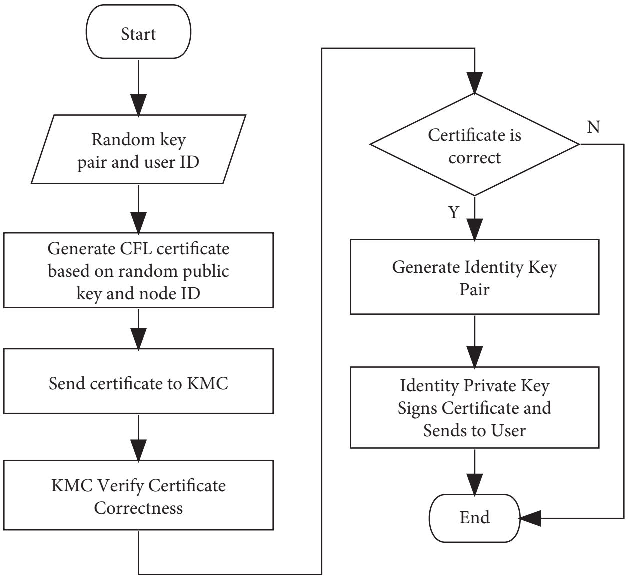
Start
Random key pair and user ID
Generate CFL certificate based on random public key and node ID
Send certificate to KMC
KMC Verify Certificate Correctness
Certificate is correct
N
Y
Generate Identity Key Pair
Identity Private Key Signs Certificate and Sends to User
End

Figure 1: Authentication steps based on CFL.

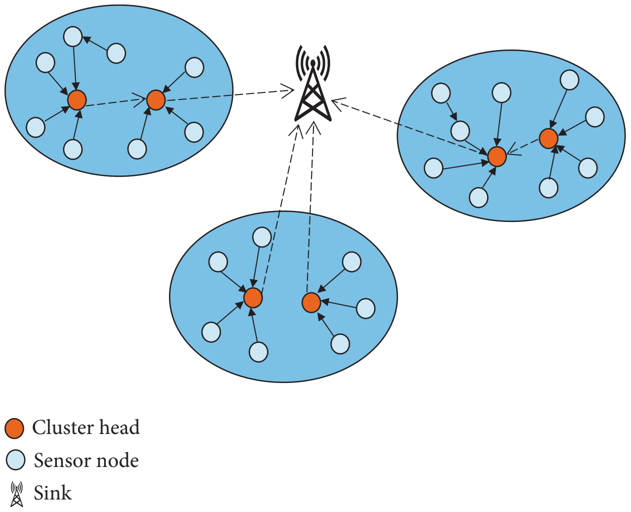

Figure 2: Heterogeneous IoT structure.

In reality, sensor nodes of many-to-one traffic mode only communicate with a small number of adjacent nodes on the transmission path [16], which means nodes do not need to communicate with all neighbors. Therefore, the route-driven key management scheme [17] only sets the shared key for each sensor node and the first adjacent node in the path where its data reaches the receiving node; it is unnecessary to establish the shared key for each neighbor sensor node. When the sensor node sends a packet to the cluster head, the packet will be forwarded by other sensor nodes in the cluster. The intracluster routing scheme determines the node through which the packet needs to pass from the sensor node to its cluster head by making all sensor nodes form a minimum spanning tree (MST) or shortest path tree (SPT) with the cluster head as the root. In order to construct the routing structure, the cluster headfirst needs to obtain the location information of each sensor node. Then the cluster head uses a centralized algorithm to construct the spanning tree according to the relative location of each sensor node. After the routing information is determined, the cluster head uses one or more broadcasts to propagate the routing structure (parent-child relationship) to all sensor nodes.

After the routing structure is determined, the cluster head encrypts the shared key (Symmetric Cipher) between the parent and child nodes through the elliptic curve algorithm (ECC). It sends the key information to the corresponding node. After receiving the message, the node decrypts it to obtain the shared key between itself and its neighbor nodes. It uses the shared key to establish secure communication between adjacent nodes. Each sensor node communicates with only a small part of its neighboring nodes in this scheme, which greatly reduces the communication and computing overhead of key settings. At the same time, the symmetric cryptographic algorithm is used as the shared key between adjacent nodes, which reduces the storage requirements of each sensor node. But correspondingly, because nodes are deployed in dangerous environments, the security of node information cannot be guaranteed.

3. CFL-Based Routing-Driven Key Management Scheme

In this section, a key management scheme for HSN is proposed. The scheme uses the CFL authentication system and many to one communication mode in the HSN network, called route-driven IoT key management scheme based on CFL.

3.1. Scenario Assumptions. In order to focus the research on the algorithm design of route driven key management scheme based on CFL, the paper makes the following assumptions:

(1) The L-sensor and H-sensor nodes are evenly and randomly distributed in the network.

(2) The network is a two-dimensional plane. After the sensor nodes are deployed, an efficient clustering algorithm is used in HSN to form a cluster [18]. Each L-sensor node selects the closest H-sensor node as the cluster head (unless there are obstacles between them). After the cluster is formed, the HSN is divided into multiple clusters, in which the H-sensor node acts as the cluster head to form the backbone of the HSN network.

(3) Each H-sensor node can communicate directly with adjacent H-sensor nodes (if not, the H-sensor node relays through the L-sensor node [19]).

(4) Each L-sensor and H-sensor node has a unique node ID and knows its location.

3.2. Routing Structure of HSN. When the hierarchical network architecture in HSN is formed, the routing in HSN includes two stages:

(1) Intracluster routing: each L-sensor node sends the collected data to its cluster head (H-sensor node)

(2) Intercluster routing: each cluster head integrates the data from multiple L-sensor nodes and sends the data to the receiving node through the network backbone

When the L-sensor node sends a packet to its cluster, the packet will be forwarded by other L-sensor nodes in the cluster. The routing structure in the cluster determines the node through which the packet passes when the L-sensor node transmits the packet to its cluster head. The basic idea of establishing the routing structure in the cluster is to make all l sensing nodes in the cluster form a tree with the cluster head as the root.

In this model, adjacent sensor nodes in the same cluster generate the same data structure (all packets generated by adjacent sensor nodes are k-bit), which is shown in the literature [20]:

(1) The MST consumes the least total energy in the cluster when the intermediate node performs a complete data fusion (i.e., two k-bit packets that become one k-bit packet) during data forwarding.

(2) If there are no data fusion in the cluster, the shortest path tree (SPT) consumes the least total energy.

(3) For partial data fusion, finding the tree with the least total energy consumption is an NP-complete problem. Therefore, MST is used to construct the routing structure in this paper.

In order to build MST, each L-sensor node sends location information to the cluster header H and then constructs a routing structure based on the relative location of each L-sensor node. When the MST construction is complete, the cluster header uses broadcasting to send the tree structure (parent-child relationship between L-sensor nodes) to all L-sensor nodes. It is important to note that broadcasts from cluster headers need to be authenticated [21] to avoid malicious broadcasts by attackers that can disrupt the dissemination of routing information. Authentication of broadcasting identity will be discussed in the next section.

Because L-sensor nodes are small, easily captured, unreliable devices, and may time out and fail [22], MST or SPT algorithms will find multiple parent nodes for each L-sensor node when determining the routing structure. A parent node acts as the primary parent node, while other parent nodes act as the standby parent node. When the primary parent node fails, the L-sensor node uses the standby parent node for routing without crashing the entire communication network due to a failure of one node. Once the routing structure is determined, each L-sensor node only needs to establish a shared key with its parent and child nodes.

3.3. Key Distribution. In this section, we describe a shared key distribution scheme between adjacent sensor nodes based on CFL. The basic cryptographic algorithms for random key pairs can choose exponential product public-key cryptography, elliptic curve cryptography ECC, or RSA algorithms. In this section, only SM2- and SM3-based key management schemes are introduced, and the process is described as follows:

(1) The L-sensor node generates a set of random keys (RASK, RAPK) based on a previously selected working password algorithm.

(2) After the cluster head selection is completed, the L-sensor node u (Lu) sends the random public key RAPK_u and node information identification ID_u to the cluster head, which is designated as $\mathrm{ID}_1 = \mathrm{RAPK}_u \| \mathrm{ID}_u$. At the same time, since the location of the cluster head is known to all common sensor nodes in the cluster during cluster formation, the greedy geographic routing protocol [23] ensures that the information is forwarded to the cluster head.

(3) When the cluster head receives the information from the L-node, it calculates $h = H(\mathrm{ID}_i) = \{h_0,\ h_1,\ \ldots,\ h_{t-1}\}$, h_i: $\{i = 0,1,\ \ldots,\ t-1\}$ to get the control information h from the input of the control function. Where H uses the password hash function SM3, the output is $N = 256$ bits, and $N = st$ is set, s is the key length and meets $s \,|\, N$. The cluster head calculates the multilinear control function according to h as follows:

$$f_h(SKB) = f_h(sk0, sk1, \ldots, sk2s - 1 = \mathrm{IDSK}). \tag{1}$$

Generate node identity private key($IDSK$). SKB is the private key base, and the generation method is as follows: make m the period of base point P in SM2, cluster head randomly selects $sk_i \in Zm = Z/mZ$, $i = 0,1,\ldots,t2s - 1$, and the two are not equal to each other to get the private key base:

$$\mathrm{SKB} = \left(sk0, sk1, \ldots sk_{t2s-1}\right). \tag{2}$$

(4) The cluster head constructs an MST based on the location information of the L node and centralized MST algorithm to get the L_v of the parent node of L_u. Then use the signature algorithm SIGN, with IDSK as the key, to sign the contents of the certificate, which is recorded as $\mathrm{sign}_u = \mathrm{SIGN}_{\mathrm{IDSK}}(\mathrm{ID}_u \|$ $\mathrm{RAPK}_u \| v$ (parent node of u)$\|$ RAP K_v, send the signed certificate sign_u to L_u.

(5) After obtaining the certificate sign_u, L_u inputs ID_1 into the cryptographic hash function SM3 to obtain the control information h input by the multilinear control function. According to h and the public key generator, it is transformed by the following multilinear function:

$$f_h(\mathrm{ID}, \mathrm{PBK}) = f_h\left(pk_0, pk_1, \ldots, pk_{t2s-1}\right) = \mathrm{IDPK}. \tag{3}$$

PKB is the public key generator, PKB=(pk_0, pk_1,. . .,pk_{t2s-1}), and $pk_i = sk_i \cdot P \bmod E$, gets the public key base. Generate the identity public key IDPK_u, and use IDPK_u as the public key of the verification algorithm to verify the signed certificate.

(6) After the verification is correct, the certificate is passed. L_u uses the public key $RAP\ K_v$ of the parent node L_v to communicate with L_v.

The pseudo-code of key distribution algorithm is shown in Algorithms 1–3.

3.4. Key Revocation

3.4.1. Cluster Member Revocation. When the L-sensor node in the cluster is destroyed, it is necessary to revoke all keys about the L-sensor node and update the routing structure about the node. When the cluster head node detects that the node is damaged, the cluster head node determines according to the position of the damaged node in the routing structure:

(1) When the node to be revoked is a leaf node, only one revocation information needs to be sent to its parent node

(2) When the node to be revoked is the parent node, and its child node has a standby parent node, send the revocation information to the parent node and child node of the damaged node, and use the standby parent node for communication in the next communication

(3) When the node to be revoked is the parent node, and its child node has no standby parent node, the cluster head needs to re-establish the route for the child node of the damaged node and pass the revocation information and the new routing structure to the child node

The revocation message contains the key list to be revoked (symmetric key for communication between nodes). The key list is signed with the identification private key IDSK(expressed as sign), and the sign is appended to the key list. Each L-sensor node has a separate identification public–private key pair. Therefore, when the L-sensor node receives the revocation message, it verifies the digital signature through the identification public key IDPK to check the integrity and authenticity of the message. It can effectively prevent the opponent from sending false revocation messages.

3.4.2. Cluster Member Revocation. Like cluster members, cluster heads are also hostile and need to be adjusted when they are captured or damaged. When the base station detects that the cluster head is captured or damaged, it queries all the node information in the cluster based on the identity of the cluster. It broadcasts the updated information to all the nodes in the cluster. After receiving the updated information, the cluster members delete the existing key pairs and query the nearest cluster head information except for the original cluster head, apply to join the cluster, redistribute the key, and form the IoT network with the new cluster head.

4. Experiment and Analysis

4.1. Safety Analysis

Theorem 1. *CFL is a computationally difficult and provable security scheme.*

Prove. The working private key of the CFL system user and the signature private key generation meta-set of the CFL Certificate Generation Center are independent of each other. Only the random public key of the L node and the signature verification public key generation meta-set of the H node are published in the key work phase. Therefore, in theory, the attacker's attack on the original set of the signature private key generated by the certificate generation center and the working private key of the CFL user is transformed into a corresponding mathematical problem.

Theorem 2. *If the adversary breaks through a cluster member and obtains the random private key and signature public key of the node, it does not affect the private key of other cluster members and the private key generation meta set of the cluster head.*

Prove. Probability Turing Machine TM (M, $\sum$) given polynomial time, where M is signature information, E is a signature random variable, and M, $\sum$ is independent of each other, (M, $\sum$) induces random variable (H, M, $\sum$), where H is a Hash function; then,

$$\forall h, \sigma, \Pr((H(M), \Sigma) = (h, \sigma)) = \frac{1}{2^{2n}}. \qquad (4)$$

In the CFL certification system, $\forall h$ makes

$$\Pr((H(M), \Sigma) = (h, \sigma)) = \begin{cases} \frac{1}{2^n}, & Sign_{CFL}(h) = \sigma \\ 0\ , & else \end{cases}, \left|\Pr((H(M), \Sigma) = (h, \sigma)) - \Pr\left((H(M), \Sigma') = (h, \sigma)\right)\right| \leq \frac{1}{2^n}. \qquad (5)$$

So in polynomial time,

$$\sum_{|(h,\sigma)| < n^c} \left|\Pr((H(M), \Sigma) = (h, \sigma)) - \Pr\left((H(M), \Sigma') = (h, \sigma)\right| \leq \frac{n^c}{2^n}. \qquad (6)$$

```
IF L-Node $U$ applies for registration THEN
    Upload $U$ identity information
    IF Authentication pass THEN
        $RAPK_u$, $PASK_u \leftarrow$ Generate
        $\mathrm{ID}_u \leftarrow$ Node ID
        $\mathrm{ID}_1 \leftarrow \mathrm{RAPK}_u||\mathrm{ID}_u$
        H-Node $H \leftarrow \mathrm{ID}_1$
    END IF
END IF
```

Algorithm 1: Node operation algorithm.

```
MST $\leftarrow$Generate
//Generate MST according to node location information
$L_v \leftarrow$ Generate
//Generate parent node of Lu according to MST
IDSK $\leftarrow f_h$ (SKB)
//SKB $= (sk_0, sk_1, \ldots, sk_{t2s-1})$; $h = H(\mathrm{ID}_i) = \{h_0, h_1, \ldots, h_{t-1}\}$
$\mathrm{sign}_u \leftarrow \mathrm{SIGN}_{\mathrm{IDSK}}(\mathrm{ID}_u||$ $\mathrm{RAPK}_u||(v($parent node of $u)||\mathrm{RAP}\ K_v)$
$\mathrm{L}_u \leftarrow \mathrm{sign}_u$
```

Algorithm 2: Cluster head operation algorithm.

```
IDPK $\leftarrow f_h$ (ID, PBK) //PKB $= (pk_0, pk_1, \ldots, pk_{t2s-1})$, $pk_i = sk_i\ P \bmod E$
IF $\mathrm{VERIFY}_{\mathrm{IDPK}}$ $(\mathrm{sign}_u) =$ TRUE
    $L_u$ and $L_v$ use $\mathrm{RAPK}_v$ to communicate
ELSE
    Abandon $\mathrm{sign}_u$
End IF
```

Algorithm 3: Node operation algorithm.

Let the set of nodes be U; if $\forall u_1, u_2 \in U$, and $u_1 \neq u_2$,

$$P\left(\mathrm{RASK}_{u_1} = \mathrm{RASK}_{u_2}\right) < \varepsilon. \tag{7}$$

The node private key satisfies one-node-one-secret if $\varepsilon \longrightarrow 0$.

Thus, when SM2 and SM3 satisfy random predictors, the CFL certification system based on SM2 and SM3 satisfies statistical zero-knowledge. The random keys of the cluster members and the signature verification cipher algorithm of the cluster head satisfy "one-node-one-secret" in use [24]. When an attacker gets the key pair information of a node, the adversary can get the key length s of the node to guess the keys of other nodes with a guess space of 2^s. Only when an attacker obtains the signature private key of $t2^s$ nodes can the private key generation meta set of the cluster head node be obtained. However, the cost of obtaining a token private key from a token public key is enormous, and the difficulty of obtaining $t2^s$ token private keys is not calculable under current computing conditions.

Theorem 3. *In this scheme, the adversary cannot break the entire key system by intercepting the cluster head.*

Prove. If the adversary captures a cluster head, the base station can detect and broadcast the revocation message of the cluster head. All cluster members of the original cluster head delete the random key and flag key pairs used for communication within the existing cluster, find the closest H node except the original cluster head and apply to become a member within the cluster. The routing structure and node key of the original cluster head are invalid. When a cluster member joins a new cluster, his leaf node key is modified, so the adversary cannot obtain the communication key of the newly joined cluster.

The three theorems in this section prove that the key leakage of a single node in the system does not affect the security of other nodes and the whole system. It shows that the scheme has high antinode acquisition ability and security and ensures the security of cluster heads and cluster members in the adversary environment.

4.2. Performance Analysis. Because most sensor nodes have limited resources, in addition to security, the storage requirements, connectivity, computation, and energy consumption of the key management algorithm are important

Table 1: Algorithm complexity analysis.

Protocol	Storage space	Connectivity	Tate pairing	Length of message sent	Length of message received
[7]	$(M+4)N+5M$	1	5	$4\|G_1\|$	$(N+4)\|G_1\|$
[17]	$(M+2)N+3M$	1	2	$2\|G_1\|$	$3\|G_1\|$
Ours	$M*N+3N$	1	1	$3\|G_1\|$	$4\|G_1\|$

Storage space indicates the capacity required by the sensor to store keys. Connectivity represents the connection efficiency of sensors in different protocols. Tate pairing refers to bilinear pairing during key generation.

indicators to measure the performance of the protocol [5]. This paper compares the key management scheme used in wireless sensor networks with this scheme. Table 1 lists the comparison results between this scheme and the comparable key management scheme in terms of storage requirements, computational complexity, and connectivity.

Assume that the number of H-sensors and L-sensors in observation area is M and N, respectively. Typically, we have $M << N$. In the CFL-based key management protocol for the IoT, the H-sensors store the node information certificates $\mathrm{ID}_L = \mathrm{RAPK}_L \| \mathrm{ID}_L$ of all nodes in the cluster (including the random public key RAPK_L and the node information identification ID_L), the L-sensors store the self-generated random private key RASK_L and the identification public key IDPK_L and the random key RAP K_v of the parent node required to communicate with neighbor nodes, so the storage requirements for this solution are

$$M*N+3N. \tag{8}$$

In the ECC-based key management scheme [17], H-sensors need to preload the public keys of all L-sensors, a pair of their public and private keys, and a deployment key K_H; L-sensors need to preload its private key and H's public key, so the total number of keys preloaded by ECC-based key management scheme is

$$M*(N+3)+2N=(M+2)N+3M. \tag{9}$$

In scheme [7], H-sensors need to store intercluster Federation key, node information (session key identity, partner identity, group session key pair), and intracluster node information. In contrast, L-sensors only need to store their node information. The required storage space is

$$5M+MN+4N=(M+4)N+5M. \tag{10}$$

Figure 3 shows that the schema [7] requires the highest storage space. Scheme [17] requires very close storage space with the same number of nodes, but its key generation still needs the key management center, and the node does not have full control over the private key.

From the energy consumption of the protocol, this paper quantifies the total energy consumed by the key management scheme to the sum of the calculation and communication consumption of the group members in the negotiation process, which is general. According to the data provided in [25], the energy consumption of a 133 MHz "Strong ARM" microprocessor for computing and communication is shown in Table 2:

Since the security of the 160-bit ECC encryption algorithm is comparable to that of 1024-bit RSA and DSA encryption algorithm [26], it is assumed that the single information quantity of key management algorithm based on elliptic curve encryption scheme is $|G_1| = 160$ bit. Then the total energy consumption analysis is shown in Figure 4. The total energy consumption of the scheme [7] increases rapidly with the increase of the number of nodes; The scheme in this paper has a significant advantage over the scheme [17] in terms of total energy consumption.

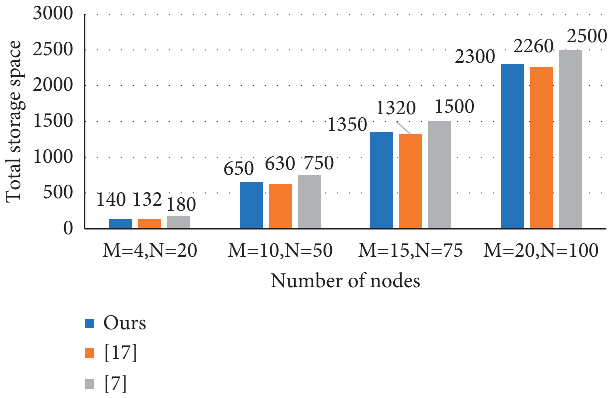

Figure 3: The relationship between node number and total storage demand.

Table 2: Energy cost for computation and communication.

Type of communication	Energy cost/mJ
Computation cost of tate pairing	47.0
Communication cost for sending 1bit	0.66×10^{-3}
Communication cost for receiving 1bit	0.31×10^{-3}

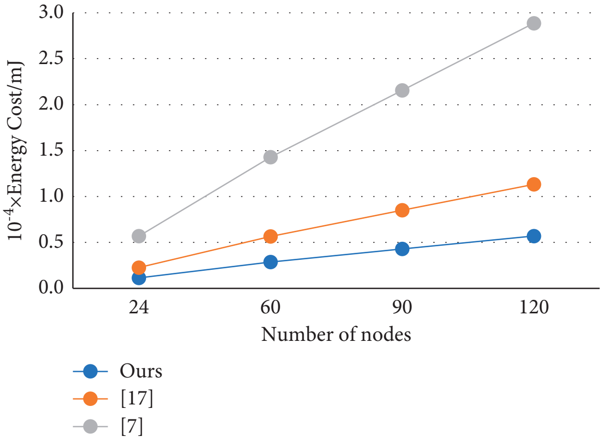

Figure 4: Total energy consumption.

Moreover, this scheme has fewer storage requirements, greater flexibility, and higher security.

5. Conclusions and Future Work

This paper combines identity-based certificate authentication system CFL with heterogeneous sensor networks. It proposes a new routing-driven key management scheme based on CFL to solve the problems faced by current heterogeneous IoT key management. It effectively solves the authentication and communication between the nodes and public keys of the IoT. At the same time, third-party services are not required to participate in the key establishment process. Key information will not be leaked during the key transfer process to ensure the security of the key transfer. The final result analysis shows that this scheme has obvious advantages in security, storage requirements, connectivity, and energy consumption and is more suitable for low-configuration wireless IoT networks. The next step is to further research and realize its key management application in decentralized [27] (such as blockchain) IoT application scenarios.

Data Availability

The data used to support the results of this study, including algorithms and proofs, are included in this paper and can also be obtained from the corresponding authors upon request.

Conflicts of Interest

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

Acknowledgments

This work was partially funded by the Key Research and Development Program of Shandong Province (2019GNC106027 and 2019JZZY010134) and the Natural Science Foundation of Shandong Province (ZR2020MF058 and ZR2020MF029).

References

[1] General Office of Ministry of Industry and Information Technology, “Notice of the general office of the ministry of industry and information technology on deepening the all-round development of mobile Internet of things [EB/OL],” 2020, http://www.gov.cn/zhengce/zhengceku/2020-05/08/content_5509672.htm, in Chinese.

[2] W. Li, D. Wang, and P. Wang, “Insider attacks on multi factor authentication protocol in wireless sensor networks,” *Journal of Software*, vol. 30, no. 08, pp. 2375–2391, 2019, in Chinese.

[3] A. Irshad, S. A. Chaudhry, Q. Xie et al., “An enhanced and provably secure chaotic map-based authenticated key agreement in multi-server architecture,” *Arabian Journal for Science and Engineering*, vol. 43, no. 2, pp. 811–828, 2018.

[4] A. Karrothu and J. Norman, “Group and hierarchical key management for secure communications in Internet of Things,” *International Journal of Communication Systems*, vol. 33, no. 13, p. e3859, 2020.

[5] A. K. Gautam and R. Kumar, “A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks,” *SN Applied Sciences*, vol. 3, no. 1, pp. 1–27, 2021.

[6] J. Choi, J. Bang, L. H. Kim, M. Ahn, and T. Kwon, “Location-based key management strong against insider threats in wireless sensor networks,” *IEEE Systems Journal*, vol. 11, no. 99, pp. 494–502, 2017.

[7] Q. Zhang, Y. Gan, R. Wang, Z. Jiamin, and T. Yu’an, “Asymmetric group key agreement protocol between clusters,” *Journal of Computer Research and Development*, vol. 55, no. 12, pp. 2651–2663, 2018, in Chinese.

[8] M. Elhoseny, H. Elminir, A. Riad, and X. Yuan, “A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption,” *Journal of King Saud University - Computer and Information Sciences*, vol. 28, no. 3, pp. 262–275, 2016.

[9] V. Alappatt and P. M. J. Prathap, “Hybrid cryptographic algorithm based key management scheme in MANET,” *Materials Today Proceedings*, 2020, In Press.

[10] S. Mesmoudi, B. Benadda, and A. Mesmoudi, Skwn, Smart and dynamic key management scheme for wireless sensor networks,” *Communication Systems*, vol. 32, pp. 1–23, 2019.

[11] Q. Zhang, X. Hu, W. Liu, and W. Jianghong, “An improved three-party password verification meta-authentication key exchange protocol,” *Journal of Software*, vol. 31, no. 10, pp. 3238–3250, 2020.

[12] H. Chen, X. fan, and S. Lu, *Identity-based Certification Scheme CFL*, CN102957536A, Beijing, 2013, in Chinese.

[13] State Password Administration, “Notice on approval of CFL authentication system based on SM2 and SM3 [EB/OL] ,” 2016, https://sca.gov.cn/sca/xxgk/2016-03/21/content_1002812.html, in Chinese.

[14] H. Chan, P. Adrian, and D. Song, “Random key predistribution schemes for sensor networks,” *2003 Symposium on Security and Privacy*, IEEE, 2003.

[15] A. Chanda, P. Sadhukhan, and N. Mukherjee, “Key management for hierarchical wireless sensor networks: a robust scheme,” *EAI Endorsed Transactions on Internet of Things*, vol. 6, no. 23, 2020.

[16] P. Li and L. Zhu, “A multi-conditional proxy broadcast Re-encryption scheme for sensor networks,” *Computers, Materials & Continua*, vol. 65, no. 3, pp. 2079–2090, 2020.

[17] X. Du, Y. Xiao, S. Ci, M. Guizani, and H. Chen, “A routing-driven key management scheme for heterogeneous sensor networks,” in *Proceedings of the 2007 IEEE International Conference on Communications*, pp. 3407–3412, IEEE, Glasgow, UK, June 2007.

[18] Z. Kuang, J. Wu, and J. Li, “Ring KNN algorithm based on clustering,” *Computer engineering and Science*, vol. 41, no. 05, pp. 804–812, 2019, in Chinese.

[19] X. Wang, H. Wu, D. Liu, D. Ye, and Z. Yang, “A global key management method for hierarchical wireless sensor networks,” *International Core Journal of Engineering*, vol. 6, no. 7, pp. 327–333, 2020.

[20] D. Nageswari, R. Maheswar, and G. R. Kanagachidambaresan, “Performance analysis of cluster based homogeneous sensor network using energy efficient N-policy (EENP) model,” *Cluster Computing*, vol. 22, no. 5, pp. 12243–12250, 2019.

[21] C. Wang, D. Wang, G. Xu, and D. He, “Efficient privacy-preserving user authentication scheme with forward secrecy

for industry 4.0," *Science China Information Sciences*, vol. 65, no. 1, 2022.

[22] C. Esposito, M. Ficco, A. Castiglione, F. Palmieri, and A. D. Santis, "Distributed group key management for event notification confidentiality among sensors," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 3, pp. 566–580, 2018.

[23] Q. Xian and Y. Long, "An enhanced greedy perimeter stateless routing algorithm for wireless sensor network," in *Proceedings of the 2016 IEEE international conference of online analysis and computing science (ICOACS)*, pp. 181–184, IEEE, Chongqing, China, May 2016.

[24] C. Du, J. Liu, and X. fan, "CFL satisfies statistical zero-knowledge," *Research on Information Security*, vol. 2, no. 007, pp. 621–627, 2016, in Chinese.

[25] Q. Zhang, R. Wang, and Y. Tan, "Identity-based verifiable asymmetric group key agreement protocol," *Journal of Computer Research and Development*, vol. 51, no. 8, pp. 1727–1738, 2014.

[26] L. I. Zengpeng, V. Sharma, M. A. Chunguang, G. E. Chunpeng, and S. U. S. I. L. O. Willy, "Ciphertext-policy attribute-based proxy re-encryption via constrained PRFs," *Science China(Information Sciences)*, vol. 64, no. 06, pp. 242-243, 2021.

[27] C. Qu, M. Tao, J. Zhang, X. Hong, and R. Yuan, "Blockchain based credibility verification method for IoT entities," *Security and Communication Networks*, vol. 2018, pp. 1–11, 2018.