Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 8548981, 14 pages
https://doi.org/10.1155/2021/8548981

*Research Article*

# Examination on Security Performance Analysis Model of Internet of Things Assigned Based on Composite Security Key

**Ying Sun and Lei Bai**

*Engineering Training Center, Beihua University, Jilin, 132000 Jilin, China*

Correspondence should be addressed to Lei Bai; bailei@beihua.edu.cn

Received 29 July 2021; Revised 31 August 2021; Accepted 9 September 2021; Published 18 October 2021

Academic Editor: Zhihan Lv

Rapid development of Internet of Things technology makes the Internet interact and communicate with objects in the real world. The diversity of Internet of Things' system architectures and the diversity of networks determine the complexity of their security issues. A key step in building an Internet of Things' security system is to build a model and evaluate threats of security. First, this paper studies the distribution of key security about mobile ad hoc networks and analyzed the characteristics of the scene. To promote the certification of the key exchange strategy of both sides, it supports key exchange between the core node and multiple nodes for existing problems that management scheme of random key preallocation is limited by the storage space of the node through combination of key matrix elements which has less information to generate a large number of keys, and each sensor node only needs to store related parameters and key matrix. It saves the memory space of node greatly. The results of simulation show that the program has a strong security; it can fight against the common attacks of wireless sensor networks, such as node forgery attacks, message replay attacks, and denial of service attacks. At the same time, it is superior to traditional solutions in terms of network connectivity and nondestructibility, which can apply clustered wireless sensor network massively.

## 1. Introduction

With the continuous advancement of network and communication technologies, information transmission is becoming more and more convenient, and the amount of data carried on the information network is increasing. Network communication has been immersed in all aspects of people's production and life which are increasingly dependent on the convenience of information exchange brought [1]. However, the use of information technology to provide fast information services must also be mainly due to the risk of information leakage caused by this process. How to ensure the security of information transmission has become one of the most important concerns in the development of the network [2]. As we all know, due to the diversity of network connection styles and the characteristics of network openness and popularity, coupled with the extensive distribution of network infrastructure, the loopholes and inherent defects of communication transmission protocols make the foundation of information security of the network very weak and easy to appear: illegal acquisition of data, transmission of stealing, and other network attacks. Especially in the military, finance, and politics, the consequences of information leakage are very serious; it is related to the victory of war, people's property and privacy, intellectual patents, trade secrets, and national security [3]. Especially in the "Prism Gate" incident that broke out in 2013, the contradiction between the protection and theft of information was even more prominent. Therefore, the confidentiality of information is straightforward for us, and an important task deserves people's attention and research [4].

For security in information transmission, the most effective way is to securely encrypt the information, and the key cannot be known by a third party. This gave birth to the discipline of cryptography [5, 6]. It has played a major role in the development of human society. The classic encryption technology is mainly divided into a symmetric key system and an asymmetric key system. The symmetric key requires that both parties can securely share the same key. The encryption and decryption algorithms are symmetrical. It is simple to calculate, but there are many vulnerabilities. If the key is eavesdropped by a third party, encryption will fail [7]. Although this problem can be solved by the "one time and one secret" technology. But this will make the keys all one-time, resulting in very low efficiency. And the process of key transmission is also inconvenient and will also form new security holes. This key system is not a classic public key system, and encryption and decryption use different keys [8]. Each user has a private key and a public key. The private key is private, and the public key is public and does not require confidentiality. The source end of the communication encrypts the plaintext with the public key of the sink and sends the encrypted ciphertext to the sink. The sink uses its own public key and its own private key to solve the plaintext from the ciphertext. From a mathematical point of view, the encryption and decryption of this system are similar to a single function [9]. One of its characteristics is that the original image cannot be obtained from the function value, and this depends on the complexity of mathematical calculation.

Cai et al. demonstrated entangled QKD and high-dimensional coding, where the high visibility Franson interferometer provides security against collective Gaussian attacks [10]. They achieved unprecedented critical capacity and throughput based on entangled QKD systems through the four main factors: Franson interferometry does not decrease with loss, error correction coding can tolerate high error rates, optimized time-energy entanglement generation, and efficient superconducting nanowire single-photon detector. The security key capacity yields 8.7 bits each. When optimized for throughput, they observed a security key rate of 2.7 Mbit/s (-1) after 20 km fiber transmission and 6.9 bits per photon coincidence [11]. Quantum key distribution (MDI QKD) independent of measurement equipment is an effective way to share secrets using untrusted measurement devices. However, in this promising protocol, assumptions about the characterization of the coding state are still necessary, which may lead to unnecessary complexity and potential vulnerabilities in actual implementation [12]. Chao et al. proposed the first principle verification experiment and the featureless coding source of MDI QKD by using the basic statistics of mismatch. In this demonstration, the encoding state only needs to be constrained in the two-dimensional Hilbert space, and the two remote parties (Alice and Bob) resist state preparation defects, even if they do not know the details of their encoding state [13]. Tsai and Lo use the identity-based signature scheme. In the proposed solution, the smart meter can anonymously access the service provided by the service provider using a private key during authentication without the help of a trusted anchor [14].

Firstly, this paper studies the key security distribution of mobile ad hoc networks and analyzes the characteristics of the scenarios to promote the authentication of the key exchange strategies. It supports key exchange between the core node and multiple nodes. Then, the validity of the strategy and its security proof in the presence of the opponent's environment are proposed. Finally, the strategy is verified by simulation. Aiming at the problem that the existing random key preallocation management scheme is limited by the storage space of the node, the scheme of this paper is based on the public key combination system on the elliptic curve to generate the key. A large number of keys are generated by a combination of key matrix elements with less information, and each sensor node only needs to store related parameters and key matrices. Significant savings are in node memory space. The simulation results show that the scheme has a strong security and can resist common attacks of wireless sensor networks. At the same time, it is superior to traditional solutions in terms of network connectivity and nondestructibility and can be applied to large-scale clustered wireless sensor networks.

## 2. Proposed Method

### *2.1. Internet of Things Security*

*2.1.1. Characteristics of the Internet of Things.* The Internet of Things technology has three technical features that can be tracked, monitored, and connected.

(1) Traceable features: At any time, as long as the object is connected to the Internet of Things, its precise location, and even its surroundings, can be tracked. For example, in the logistics industry, by using radio frequency identification technology, goods and vehicles in transit are marked with electronic tags, and tag information is read by fixed side readers of the roadside. Information is transmitted to the command center via the communications network to track the entire transportation process in real time. This can effectively prevent the loss of transported goods and ensure the safety of the transport process

(2) Monitorable features: The Internet of Things can use objects to monitor and manage people, for example, measurement of physiological parameters. The various conditions of the patient can be monitored and data transmitted to the destination node over the communication network

(3) Connectable features: The high integration of the Internet of Things and the mobile Internet further enables the control and compatibility of objects under the wireless network. For example, if a drinking driver uses a car key, the sensor is implanted in the car and its key nodes; the key monitors the alcohol content and sends a wireless signal to the car, so the car cannot start

*2.1.2. Threats to the Internet of Things.* As shown in Figure 1, security threats to the Internet of Things include the awareness layer, the access transport layer, and the business application layer. Due to the uncertainty of the network environment, the sensing node faces many threats, and the sensing node itself is used to monitor and control various sensing devices. The nodes monitor various detection objects to provide data information transmitted by the sensing device to monitor the operation of the network system. These smart sensor nodes are exposed to attackers and are

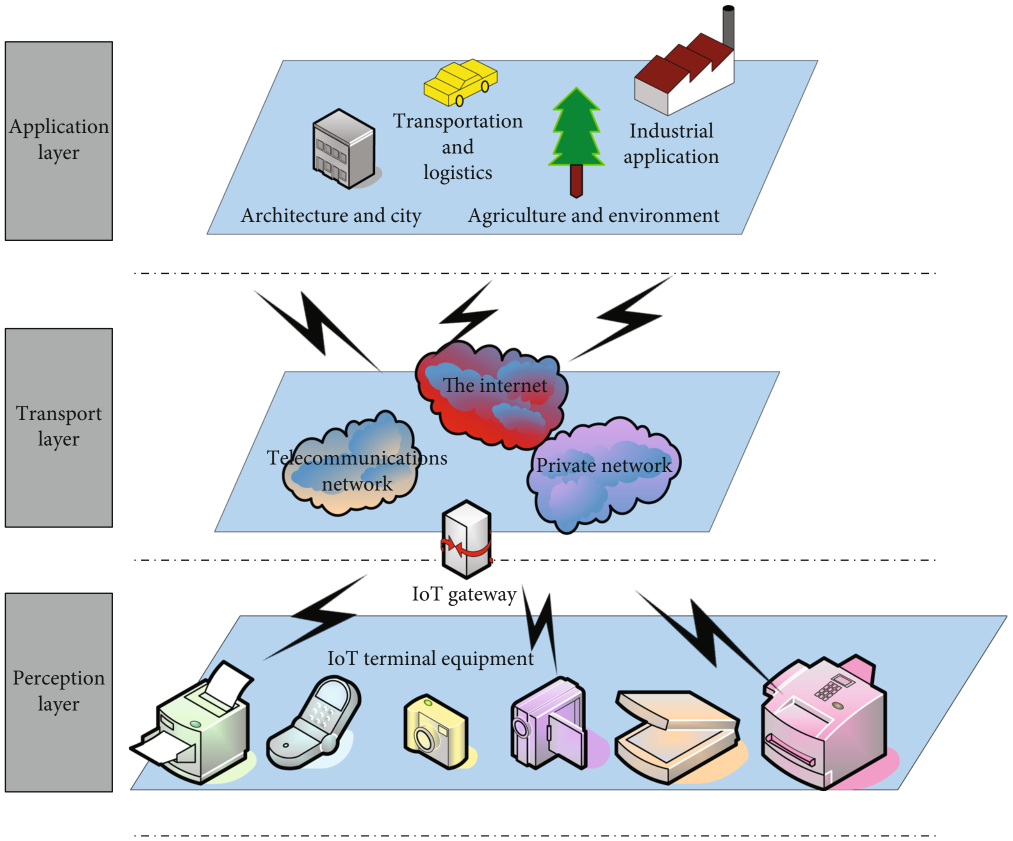

Figure 1: Threats to the Internet of Things.

the most vulnerable. Therefore, compared with traditional IP networks, all monitoring measures and security countermeasures not only face more complex network environments but also have higher real-time requirements.

The main threats to the Internet of Things are as follows:

(1) Security and privacy: Radio frequency identification technology is widely used in IoT systems. RFID tags can be embedded in any object, such as people's life and production supplies. However, the owner of these items may not understand the situation and cause the owner of the object to be scanned, located, and tracked at will

(2) Forgery attacks: Sensor devices and electronic tags are exposed to attackers compared to traditional IP networks. At the same time, part of the access transport network is a wireless network. Therefore, the forged node attacks faced by these aspects of the network threaten the security of the sensor nodes to a large extent, thus affecting the security of the entire Internet of Things

(3) Malicious code attacks: Malicious code can find many breakthroughs that can be attacked in the access transport layer and the sensing layer. As far as an attacker enters the network, it is easy to spread the virus through the transmission network. It has a strong concealment and is harder to defend against wired networks. For example, malicious code like worms itself does not require parasitic files

(4) A denial of service attack is a familiar attack method, and the probability of a connection between the sensing layer and the access transport layer is very large. Since the number of sensor nodes in the Internet of Things is huge, and most of them exist in the form of clusters, when information is transmitted in the network, a large number of sensing node information transmission and forwarding requests will cause network congestion and denial of service attacks

(5) Information security: Perceptual nodes usually have the characteristics of a single function and low information processing capability. Therefore, it is impossible for the sensory node to have high-intensity safety precautions. At the same time, due to the diversity of sensor nodes, the collected data and transmitted information will not have a uniform format. Therefore, it is difficult to provide a unified security protection strategy and security architecture

(6) In addition to the security threats faced by traditional wired networks, the Internet of Things access transport layer and business application layer also have certain security risks. In addition, due to inconsistent data, the format of the Internet of Things collection at the sensor layer is not standardized. The

data information of different types of sensor nodes is unimaginable and is multisource heterogeneous data. Therefore, the security issues of the access layer and the business application layer are more complicated

### 2.2. Key Security Assignment Problem

*2.2.1. Analysis of the Problem of Subkey Security Allocation.* Many key management strategies do not provide a corresponding solution for the secure allocation of subkeys and only emphasize that the subkeys should be securely distributed to each node. The scene diagram we need is shown in Figure 2. There is an adversary in the figure. The adversary can implement attack methods such as man-in-the-middle attacks, tampering with messages, and stealing packet contents. At the same time, we believe that the core node and the ordinary node cannot be directly connected, but communicate with each other through multiple hops.

So, in this scenario, the strategy we are required to use must meet the following security requirements:

(1) The adversary cannot crack the subkeys that the core node distributes to each node

(2) The node can identify the identity of the core node and can prevent man-in-the-middle attacks

(3) The node can verify the integrity of the communication message with the core node and prevent the enemy from tampering with the communication information

(4) The core node can authenticate the node identity

*2.2.2. Group Key Exchange Strategy Based on Discrete Logarithm.* It can be seen from Figure 1 that in this scenario, if the core node wants to distribute the subkeys securely to each node, then it is necessary to establish a secure communication mechanism with each node, so this article can be utilized under this requirement. The Diffie-Hellman key exchange algorithm solves this problem, but notices that the DH key exchange process is a two-party key exchange process. In this paper, the core node is a common node, which is a core node and multiple common nodes. In the process of constructing a key, so if the DH key exchange algorithm is directly applied to the scenario directly, the core node needs to perform a key exchange with each common node in the network. Therefore, if the DH key exchange algorithm is directly applied to the scenario, it will cause some waste in message overhead and time overhead. In addition, there are opponents in the scenario that can implement man-in-the-middle attacks, and the weakness of the DH key exchange algorithm is that there is no authentication measure, so the DH algorithm needs to be improved to adapt to the current scenario environment. Based on the above two shortcomings, we consider using a group key exchange strategy with authentication in this scenario. The method used in this paper is extended from the two-party authentication key exchange strategy to the group key exchange. The related symbols and comments involved are shown in Table 1.

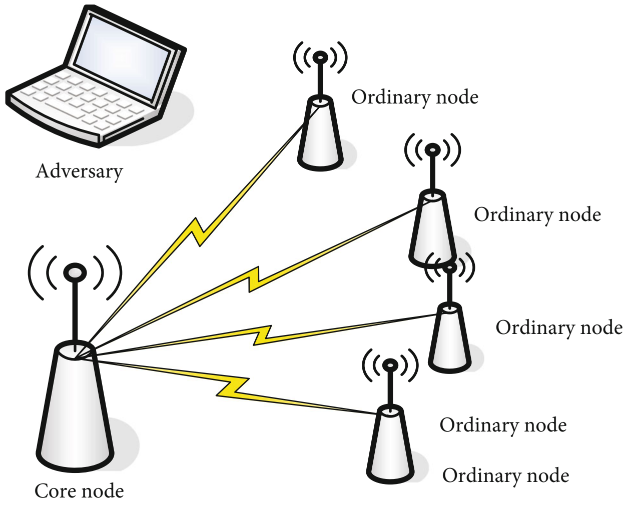

FIGURE 2: Scene diagram.

*2.3. Key Distribution Technology.* As shown in Figure 3, it is the flow chart of the key distribution technology. First, carry out the system initialization configuration, configure the RKL server, KMS system, encryption machine, IP assignment, and port number of the CA system, and configure the encryption method, key validity period, etc. Then, the hardware encryption module is initialized, and finally, RKL key distribution management is performed.

The security of the cryptosystem relies on the security of the key, so key management is very important. Any cryptosystem, whether it is a key system or a public key system, must be running to efficiently generate, distribute, use, and destroy keys. This creates a cyclical problem in a certain sense. In order to communicate securely over an insecure channel, the user must first exchange the key (key information); if there is no alternative to the existing nonsecure channel, the security is exchanged securely. The key information basically represents the same security issue as the next secure communication. The biggest obstacle to implementing a symmetric encryption scheme is that any communicating party must preestablish a shared key, which is typically achieved by additional secure channel communications, such as messenger services. Key management becomes a challenge as the size of the system or the number of entities using the system grows. Modern cryptography has developed an alternative technology solution for system users to exchange critical information through central agencies. This assumes that each user must establish some kind of secure communication with the central authority. The biggest weakness of the solution is that the central authority understands the keys of all users and becomes a bottleneck for security. An attractive solution to this type of key management challenge is to establish or assign symmetric keys using asymmetric cryptography. The key management problem of the public key system is relatively simple because the key information exchanged between users or between the user

Table 1: Necessary notes.

| | |
|---|---|
| $S$ | String |
| $\|\|S\|\|$ | String length |
| $S_1\|\|S_2$ | $S_1$ and $S_2$ stitching |
| $\oplus$ | XOR symbol |
| $1^k$ | A string of length $k$ |
| $I(i_1, i_2, i_3 \cdots) \longrightarrow (o_1, o_2, o_3 \cdots)$ | Map from $i_1 \sim i_n$ to $o_1 \sim o_n$ |
| $c$ | Cipher text |
| $H$ | Generator of prime order group |
| $P$ | Prime field |

and the central authority is public. In addition, the way to replace the unsecure channel is also simpler; for example, a physical mail system is sufficient, especially in the case of transmitting redundant information over an unsecure channel. Thus, even if the communication party has never performed secure communication in advance, communication can be performed safely. This asymmetric technique is a so-called asymmetric key establishment scheme.

One of the main applications of public key cryptosystems is the public distribution of keys. The essence of this approach is very simple, just think of the shared key as a special form of message. Assuming that the system has completed the distribution and distribution of the user's public key, the user can encrypt and sign the symmetric key with the public key system to establish the key as needed. This uses public key cryptography to reduce key distribution issues to resolve the problem of binding user IDs and their public keys. The latter is relatively simple and does not require the transmission of confidential information. This means that users can generate their own private/public key pairs without exposing them to anyone. However, it is critical that the user's public key must be properly verified. Since only integrity and verifiability are considered, users can register their public keys over unsecured channels. In large networks, this may require a hierarchically distributed authentication center system and requires a trust delivery mechanism to protect. For example, the central verification center can verify the second level of authentication authorization, and then, the second level authority can verify the user's public key information. Other levels can also be added. Such users can be authenticated through a verification chain. For example, if a user registers with a local verification authority and the local verification authority may belong to the organization, the user's organization ID can be used to verify the user's public key. If the local verification authority can communicate securely with the central verification authority, the user's public key can be passed to the central verification authority for publication. Assuming that the user's public key can be verified and published, two users can use the other party's public key to establish a shared key to encrypt the information without seeking a secure channel.

*2.3.1. RSA Key Transmission Technology.* If attacker $C$ intercepts $y_A$ and sends$y_c = g^{xC}$ mod $P$ to $B$, $B$ will also think that he is receiving $y_A$, and $B$ will unconsciously establish a key with $C$. In other words, the public key cryptosystem used supports confidentiality and does not support authentication. This hopes that a system that provides confidentiality can add authentication services. RSA is such a cryptosystem. RSA-based symmetric key transmission technology can effectively guarantee confidentiality and provide authentication services. The American National Standard ANSI X9.44 is a draft key transmission standard based on the RSA algorithm. The standard defines a mechanism for symmetric key management using reversible public key cryptography, while addressing the security requirements and other considerations for key management in conjunction with a public key infrastructure (digital signature in PKI). The technology specified in this standard is intended to securely establish and securely transmit symmetric keys.

The output of the key generation process is as follows:

(1) A public key for verification

(2) A private key for signature

Although each signature private key output is optional, sufficient information must be retained to regenerate the private signature index $d$ to generate the signature.

(3) Audit information (optional)

Key transmission is a mechanism in which one party (sender) generates a random symmetric key and transmits a symmetric key encrypted with the public key of the other party (receiver). Key transmission uses reversible public key cryptography, including the following steps:

(1) Symmetric key generation

(2) Symmetric key encryption

(3) Symmetric key recovery

Key negotiation is a mechanism in which both parties actively participate in the establishment of a random symmetric key without requiring any party to actually exchange the symmetric key. Key negotiation uses reversible public key cryptography, including the following steps:

(1) The generation of symmetric key elements

(2) Encryption of symmetric key elements

(3) Recovery of symmetric key elements

(4) Derivation of symmetric keys

*2.3.2. Elliptic Curve Key Agreement and Transmission Protocol.* There are two common preconditions for implementing ANSI X9.63: all entities involved in using these schemes must obtain a trusted copy of the elliptic curve parameters used, and each entity must obtain a static public key for each of the other entities, a true copy of it. The latter is a binding between an entity and its static public key, which can be implemented by a certification authority.

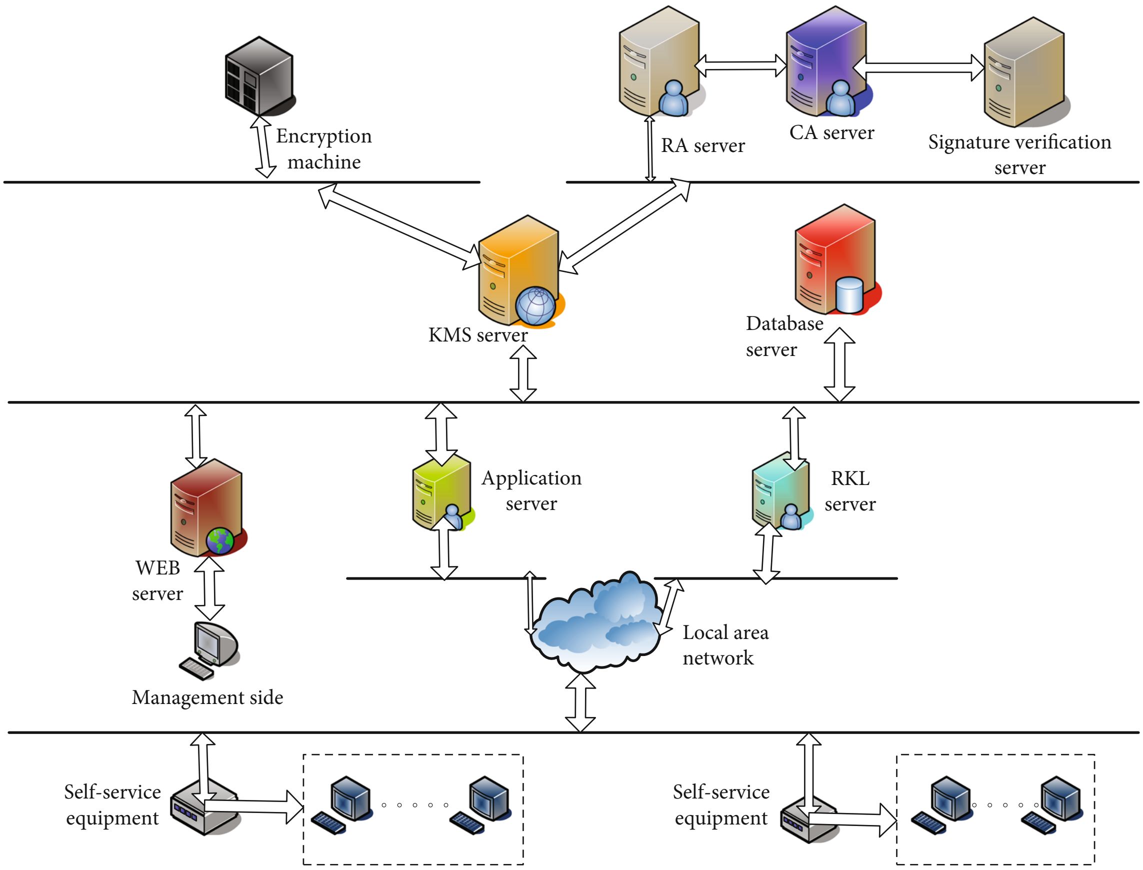

Figure 3: Remote key distribution technology.

*2.4. Wireless Sensor Network Key Management Scheme.* Key management is the core of any secure communication scheme, and various schemes have been proposed. In order to facilitate the research work, the following summarizes and analyzes the existing key management schemes and classifies them as shown in Figure 4.

*2.4.1. Q-Composite Random Key Preallocation Scheme.* After the node obtains all the shared key information of the neighbor node, if there are more than $q$ shared keys between the nodes, assuming $t(t \geq q)$, the session key $K$ for communication between the two nodes is obtained by the following equation:

$$K = \text{hash}(k_1 \| k_2 \| \cdots \| k_t). \tag{1}$$

If each node selects $m$ keys from the key pool, the probability of having $q$ shared keys between the nodes is as follows:

$$p(i) = \frac{C^{i}_{|S|} C^{2(m-i)}_{|S|-i} C^{m-i}_{2(m-i)}}{C^{m}_{|S|} C^{m}_{|S|}}. \tag{2}$$

Use $p_c$ to indicate the probability that there are at least $q$ shared keys between any nodes. The formula is as follows:

$$P_c = 1 - \sum_{i=1}^{q-1} p(i). \tag{3}$$

When $x$ nodes are captured in the network, the probability of a key leak in the key pool is $1 - ((1-m)/|S|)^x$. The Internet describes, exchanges, and stores information through HyperText Markup Language (HTML), while the Internet of Things describes, exchanges, and stores information through physical markup language EPC. Assuming that the number of shared keys between two nodes is $i$, the probability that the communication keys of the secure links of the two nodes are captured is$(1 - ((1-m)/|S|)^x)^i$. If the communication link of two uncaptured nodes is to be attacked, then the probability $P$ of the link being destroyed is as follows:

$$P = \sum_{i=q}^{m} \left(1 - \left(1 - \frac{m}{|S|}\right)^x\right)^i \frac{p(i)}{P_c}. \tag{4}$$

The solution enhances network security by increasing the $q$ value. When a small number of nodes are captured, the impact on the network is greatly reduced, and there is some anticapture. However, when the number of captured nodes rises to a certain amount, the security is not as good as the $E$ -$G$ scheme, and the scalability is also limited. The Internet of Things provides a new development opportunity for

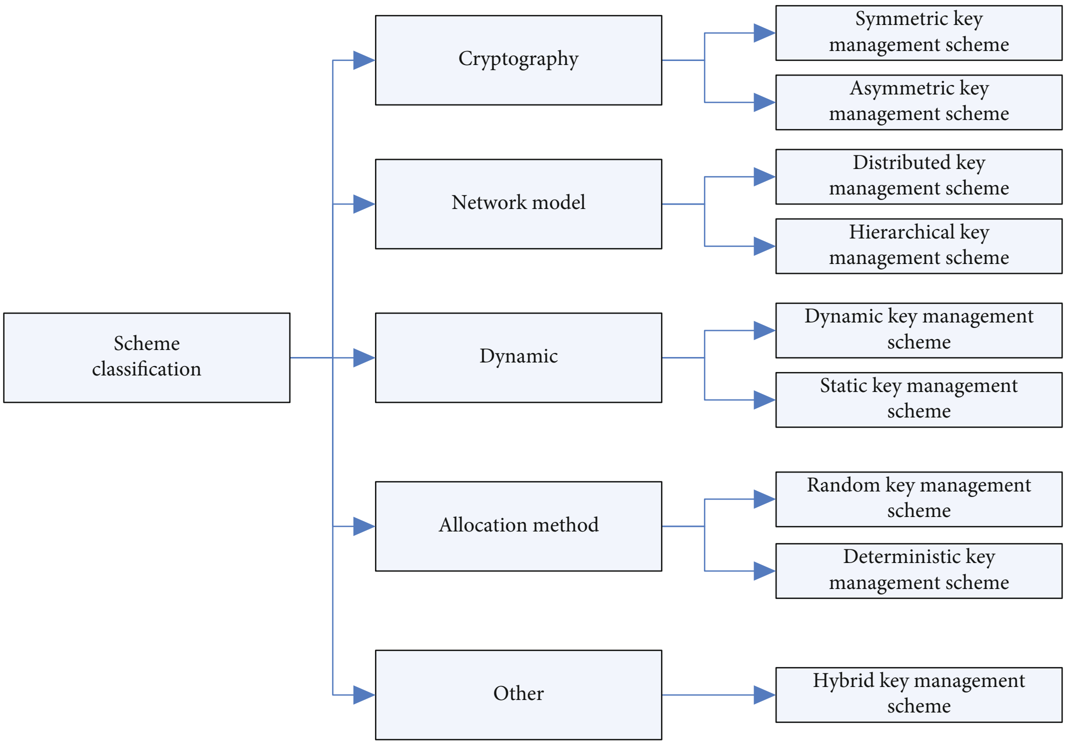
Scheme classification
Cryptography
Network model
Dynamic
Allocation method
Other
Symmetric key management scheme
Asymmetric key management scheme
Distributed key management scheme
Hierarchical key management scheme
Dynamic key management scheme
Static key management scheme
Random key management scheme
Deterministic key management scheme
Hybrid key management scheme

Figure 4: Classification of key management scheme.

technology. It applies a new generation of information technology to all walks of life. Based on the Internet, it realizes the integration of human society and the physical world and realizes real-time management and control of objects, so as to greatly improve the utilization of resources.

*2.4.2. Polynomial-Based Key Preallocation Scheme.* Compared with the random key preallocation scheme, such a scheme has a security threshold to improve the antiattack capability. The core idea steps are as follows:

(1) The trusted key service center randomly generates a binary polynomial on the finite field GF ($q$) as shown in the following equation:

$$f(x, y) = \sum_{i=0,j=0}^{t} a_{ij} x^i y^j (\mathrm{mod}\ q), \tag{5}$$

where $q$ is a large prime number and $1 \leq a_{ij} \leq q-1$.

(2) The Key Service Center assigns a unique identifier $\mathrm{ID}_i$ to each node $i$ and prestores a component $f(\mathrm{ID}_i, y)$

(3) If the node $i$ and the node $j$ are to establish a secure communication link, the shared key existing between the two nodes is as follows:

$$K_{i,j} = f\left(\mathrm{ID}_i, \mathrm{ID}_j\right) = f\left(\mathrm{ID}_j, \mathrm{ID}_i\right). \tag{6}$$

*2.4.3. Dynamic Clustering Wireless Sensor Network Key Management Scheme*

(1) Operations on elliptic curves

Assuming that two points $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$ on the elliptic curve $E$ are known, the third point $P_3(x_3, y_3)$ on the curve is obtained according to the following calculation rule so that the$P_3 = P_1 + P_2$ is satisfied.

If the two points coincide; that is, $P_1 = P_2 = P$, the slope $\lambda$ of the straight line is first obtained, and the intersection of the straight line and the curve is the point $-P_3$, and the coordinates of the $P_3$ can be obtained by the point $P_3$ and the $-P_3$ being symmetric about the $x$-axis.

If $P_1 \neq P_2$, the $P_1$ and $P_2$ are first connected and extended by a straight line, and the straight line and the elliptic curve are intersected at the point $-P_3$. When the point addition operation is performed, the slope $\lambda$ of the straight line is calculated to obtain the coordinates of the $P_3$.

To summarize the above two cases, the coordinates of the point $P_3$ are calculated as follows:

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 (\mathrm{mod}\ p), \\ y_3 &= \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\ p). \end{aligned} \tag{7}$$

The formula for calculating the slope $\lambda$ is shown in the following equation:

$$\lambda = \begin{cases} \dfrac{3x_1^2 + a}{2y_1}, & P_1 = P_2, \\ \dfrac{y_2 - y_1}{x_2 - x_1}, & P_1 \neq P_2. \end{cases} \tag{8}$$

(2) Public key combination technique on elliptic curve

In the large prime field, a part of the large prime numbers are randomly selected as $\mathrm{sk}_{ij}$, and the large prime numbers form the private key matrix $S_{\mathrm{sk}}$, which are as follows:

$$S_{\mathrm{sk}} = \begin{pmatrix} \mathrm{sk}_{11} & \mathrm{sk}_{12} & \cdots & \mathrm{sk}_{1n} \\ \mathrm{sk}_{21} & \mathrm{sk}_{22} & \cdots & \mathrm{sk}_{2n} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \mathrm{sk}_{m1} & \mathrm{sk}_{m2} & \cdots & \mathrm{sk}_{mn} \end{pmatrix}. \tag{9}$$

The elements of the public key matrix are composed of points mapped by the private key matrix onto the elliptic curve. The relationship between the elements of the public-private key matrix can be expressed as Equation (10), and the public key matrix is obtained by Equation (11) as follows:

$$\mathrm{sk}_{ij}G = \left(x_{ij}, y_{ij}\right), (1 \leq i \leq m, 1 \leq j \leq n), \tag{10}$$

$$S_{\mathrm{pk}} = \begin{pmatrix} \mathrm{sk}_{11}G & \mathrm{sk}_{12}G & \cdots & \mathrm{sk}_{1n}G \\ \mathrm{sk}_{21}G & \mathrm{sk}_{22}G & \cdots & \mathrm{sk}_{2n}G \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \mathrm{sk}_{m1}G & \mathrm{sk}_{m2}G & \cdots & \mathrm{sk}_{mn}G \end{pmatrix} = \begin{pmatrix} (x_{11}, y_{11}) & (x_{12}, y_{12}) & \cdots & (x_{1n}, y_{1n}) \\ (x_{21}, y_{21}) & (x_{22}, y_{22}) & \cdots & (x_{2n}, y_{2n}) \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ (x_{m1}, y_{m1}) & (x_{m2}, y_{m2}) & \cdots & (x_{mn}, y_{mn}) \end{pmatrix}. \tag{11}$$

Let the mapping value corresponding to the mapping value of a certain identifier under $n$ hash functions be $(a_1, a_2, \cdots, a_m)$, and the column coordinate is $(b_1, b_2, \cdots, b_n)$, and then, the private key SK and the public key PK can be calculated according to the following equations:

$$\mathrm{SK} = \left(\mathrm{sk}_{(a_1,b_1)} + \mathrm{sk}_{(a_2,b_2)} + \cdots + \mathrm{sk}_{(a_m,b_n)}\right) \bmod q, \tag{12}$$

$$\begin{aligned} \mathrm{PK} &= \left(x_{(a_1,b_1)}, y_{(a_1,b_1)}\right) + \left(x_{(a_2,b_2)}, y_{(a_2,b_2)}\right) + \cdots + \left(x_{(a_m,b_n)}, y_{(a_m,b_n)}\right) \\ &= \mathrm{sk}_{(a_1,b_1)}G + \mathrm{sk}_{(a_2,b_2)}G + \cdots + \mathrm{sk}_{(a_m,a_n)}G = \mathrm{SK} \cdot G. \end{aligned} \tag{13}$$

The points PK and SK form a public-private key pair of the elliptic curve $E\,(a, b, G, p, q)$.

(3) The fast calculation algorithm of NORX algorithm $H$ function linear approximation-related function

The underlying function $H(x, y)$ of the NORX algorithm is defined as follows:

$$H(x, y) = x \oplus y \oplus ((x \wedge y) << 1). \tag{14}$$

Assuming that the input mask of the $H$ function is $\alpha, \beta$ and the output mask is $\lambda$, the calculation formula for the correlation coefficient of the $H$ function linear approximation is as follows:

$$\rho = \rho_H((\alpha, \beta) \longrightarrow \lambda) = \frac{1}{2^{2n}} \sum_{x \in Z_2^n} \sum_{y \in Z_2^n} (-1)^{\alpha x \oplus \beta y \oplus \lambda H(x,y)}. \tag{15}$$

Expand the formula in brackets to the following:

$$\alpha x \oplus \beta y \oplus \lambda H(x, y), \tag{16}$$

$$\alpha x \oplus \beta y \oplus \lambda (x \oplus y \oplus ((x \wedge y) << 1)), \tag{17}$$

$$(\alpha \oplus \lambda) x \oplus (\beta \oplus \lambda) y \oplus y((x \wedge y) << 1). \tag{18}$$

In order to simplify the calculation, convert the $H$ function to a simplified $H$ function:

$$H'(x, y) = (x \wedge y) < < 1. \tag{19}$$

That is to ask

$$p(\alpha x \oplus \beta y \oplus \lambda((x \wedge y) << 1) = 0), \tag{20}$$

due to

$$\alpha x \oplus \beta y \oplus \lambda((x \wedge y) << 1), \tag{21}$$

$$\alpha_{m-1} x_{m-1} \oplus \beta_{m-1} y_{m-1} \overset{m-2}{\underset{j=0}{\oplus}} \left(\alpha_j x_j \oplus \beta_j y_j \oplus \lambda_{j+1} \left(x_j \wedge y_j\right)\right). \tag{22}$$

May wish to agree on $\lambda_m = 0$ and remember

$$M_j = \alpha_j x_j \oplus \beta_j y_j \oplus \lambda_{j+1} \left(x_j \wedge y_j\right). \tag{23}$$

Observing the above formula, we can see that

$$M_j, 0 \leq j \leq m - 1. \tag{24}$$

The two are independent of each other, and the formula can be calculated using the stacking lemma.

## 3. Experiments

*3.1. Simulation Experiment Design.* As shown in Table 2, it is the experimental environment required for the simulation experiment. This simulation experiment fully simulates the security performance test of the Internet of Things under the composite key.

Table 2: The environment required for the experiment.

| Experiment supplies | Configuration |
|---|---|
| Hardware | Intel® Core™ i5-4590 CPU, clocked at 3.30 GHz, memory 12 G |
| Software platform | VMware Workstation 9, Ubuntu 16.04, Fabric1.0 |
| Environment configuration | Go1.8 Linux/amd64, Docker |

As shown in Table 3, it is the user account information of the blockchain network. Each user has a one-to-one correspondence with the administrator account information, which facilitates the security performance test.

As shown in Table 4, the various numbering formats are used to explain the format applications in each type of numbering, so that the administrator can clearly understand what each format represents.

As shown in Table 5, it is the data index information of the user 1001. The data in the table is the unique identifying information of the user, and the user's security problem can be found through the user's authority.

As shown in Table 6, it is the data index information of user 1002, which records the user's data number, data path, data summary, data time stamp, and data authority content. In addition, there are restrictions from multiple networks and sensor nodes, communication interfaces, bandwidth, storage, and energy, which also restrict the development of the Internet of Things.

As shown in Table 7, it is the data index information of user 1003, which is similar to Table 4 and Table 5 and records various data of the user.

During the simulation experiment, the blockchain network starts 6 nodes, including 1 sorting node, 1 management node, and 4 peer nodes, and deploys the chain code on two of the peer nodes. The four peer nodes belong to the same management domain, each two peers form an organization, and the two organizations share a channel. Set a node in each organization as an anchor node. The communication between the organizations is completed through the anchor node, and the nodes can access each other through the domain name.

*3.2. The Basic Structure of the Model.* Because the Petri net model of the wireless communication process of the Internet of Things system is difficult to abstract, this paper uses state diagrams and sequence diagrams to represent the data transmission process in the system. A state diagram is a description of the dynamic behavior of an entity based on an event response. A sequence diagram is an entity in which an entity reacts to different events based on the current state and describes how to send and receive messages between objects. A dynamic collaborative process between multiple objects is displayed to visually describe the static characteristics and dynamic behavior of the IoT system. The sequence diagram describes the state diagram in more detail.

The elements in the state diagram and the sequence diagram correspond one-to-one with the Petri net model elements. Figure 5 depicts the process of converting an IoT wireless communication process analysis graph to a Petri net model.

Table 3: Blockchain network user account information.

| User ID | User password | Network operation authority |
|---|---|---|
| 0001 | 111111 | 1111 |
| 1001 | 123456 | 0110 |
| 1002 | abcdef | 0110 |
| 1003 | abc123 | 0110 |

Table 4: Various numbering formats.

| Name | Format |
|---|---|
| Merchant ID | C + number, such as C01 |
| Equipment name | Device + number, such as Device01 |
| Device ID | D + user ID + business ID + device ID, such as D10010101 |

The basic ideas for extracting Petri net model diagrams from the analysis diagram are as follows:

(1) Use the object-oriented method to establish the model ontology of the two graphs, respectively, that is, the concept and the clear specification. Analyze the relationship between the structure and components of the Internet of Things and give a text description and description

(2) Integrate two ontology, find out the mapping relationship between them, and generate a unified integrated ontology

(3) According to the generated integrated ontology, complete the mapping relationship between the graphic elements, complete the extraction and transformation of the model, and make the knowledge sharing between the two possibilities

The construction of model ontology is the first step of mutual transformation. In order to facilitate the subsequent ontology mapping process, the ontology structure should be unified and simplified as much as possible to improve the transformation speed and accuracy of the model.

*3.3. Threat Assessment Process.* The evaluation algorithm is based on the extended attack tree model of the Internet of Things system, analyzes the tree topology of the model, and extracts the topology of the attack process. Think of each component node in the structure as a threat factor, and the analysis can take advantage of the probability of each threat factor and combine the resulting threat factor weights. Calculate threat risk values and analyze threat attack capabilities and losses. The security threat risk assessment method based on the attack path map mainly follows the following process:

Table 5: Data index information of user 1001.

| Data number | Data path | Data summary | Data timestamp | Data permission | |
|---|---|---|---|---|---|
| | | | | Access ID | Access permission |
| 1 | /1001/C01/Device01/D10010101 | d8b991e1c1cc4119a298862abbeb8d6c | 201801120934 | 0001 | 1110 |
| | | | | 1002 | 1001 |
| | | | | 1003 | 1001 |

Table 6: Data index information of user 1002.

| Data number | Data path | Data summary | Data timestamp | Data permission | |
|---|---|---|---|---|---|
| | | | | Access ID | Access permission |
| 1 | /1001/C01/Device01/D10020201 | e3936483daecf98c7638eba3f67bb5c3 | 201801140941 | 0001 | 1110 |
| | | | | 1001 | 1010 |
| | | | | 1003 | 1001 |

Table 7: Data index information of user 1003.

| Data number | Data path | Data summary | Data timestamp | Data permission | |
|---|---|---|---|---|---|
| | | | | Access ID | Access permission |
| 1 | /1001/C01/Device01/D10030101 | 990826221c9f89770e1a42e820ed1c6e | 201801221541 | 0001 | 1110 |
| | | | | 1001 | 1010 |
| | | | | 1002 | 0000 |

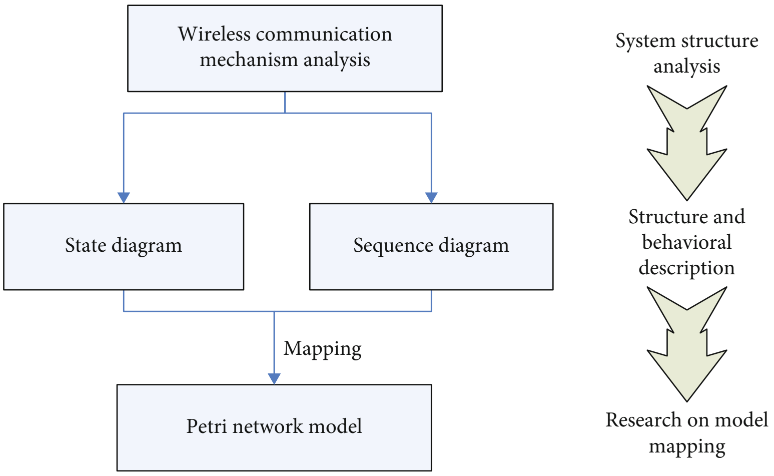
Wireless communication mechanism analysis
State diagram
Sequence diagram
Mapping
Petri network model
System structure analysis
Structure and behavioral description
Research on model mapping

Figure 5: Modeling method framework.

(1) A comprehensive calculation function for determining the threat risk of each threat factor and attack path

(2) Attack path map extraction. Combine the tailored extended attack tree to obtain the attack path map of the system, view and analyze the utilization relationship between the threat factors, and use the depth-first traversal algorithm to search the implementation path of a certain threat factor to find the complex attack hidden in the system. Path and set the attack path. Again, this method can also find all paths where the threat factor enters the system within the boundary

(3) Threat factor reliability availability calculation. The topology analysis of the attack path graph, the series-parallel relationship between the subsystems, and the possibility of using the target threat factor are obtained. In the same way, the availability (reliability) of the entire path can be derived

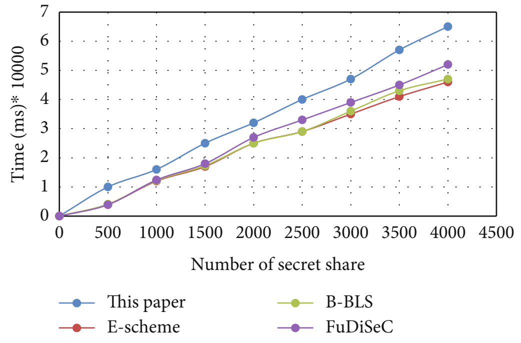

FIGURE 6: Split key generation time simulation.

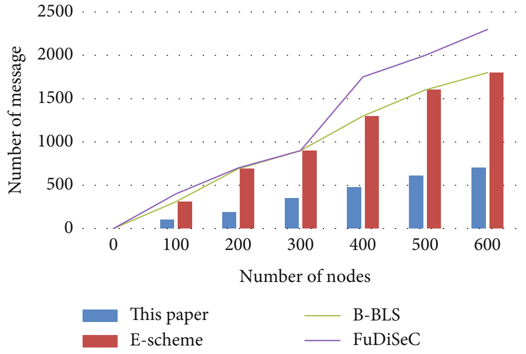

FIGURE 7: Subkey distribution message overhead.

(4) Threat risk assessment. Divide the level of each threat factor and use the concept of the correlation function instead of the manual allocation method to calculate the weight of each threat factor in the same level of threat factor. The risk factor or the entire path of the threat is calculated based on the comprehensive calculation function to assess the risk level for in-depth analysis and evaluation of system security threats

## 4. Discussion

### 4.1. Time Efficiency Analysis

*4.1.1. Split Key Generation Time.* For the subkey generation time, we compare our strategy with several other strategies. Here, we do not consider the delay of transmission between nodes. The simulation result is shown in Figure 6. From the time of split key generation, we can see from the simulation graph that our strategy has a longer and longer generation time with the number of nodes our strategy has a certain gap between the generation time of the key and other strategies, but they are all within an acceptable range.

*4.1.2. Key Distribution Message Overhead.* For the subkey message overhead, the strategy of this paper is also compared with other key management strategies. Here, we consider the message that needs to be sent when the subkey is generated. The simulation results are shown in Figure 7. From the perspective of subkey distribution message overhead, the strategy of this paper has the same linearity as other strategies in terms of message overhead, and it increases linearly with the increase of the number of nodes. It can be seen from the simulation graph that the strategy of this paper is in the node. As the number increases, the increase in message overhead is slower than other strategies.

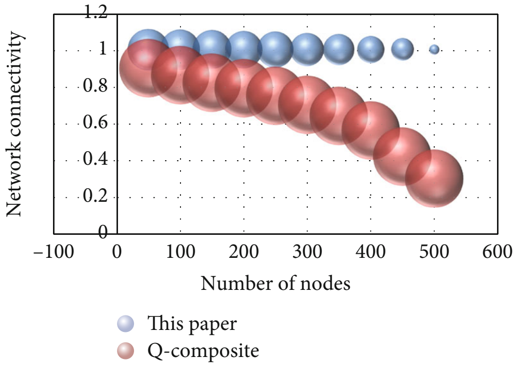

FIGURE 8: Network connectivity as a function of the number of nodes.

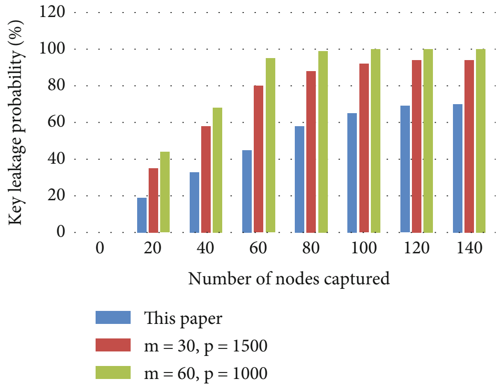

FIGURE 9: Key leakage probability as a function of the number of nodes being captured.

### 4.2. Performance Analysis

*4.2.1. Connectivity Analysis.* Adaptability to the key pool size: Set the key pool $S$ to be a variable, the network size is $N = 100$, the key chain is $m = 10$, and $q$ is taken as 3, 5, and 7, respectively. The simulation results are shown in Figure 8. As the key pool increases, the connectivity of the $q$-composite scheme gradually decreases, and the connectivity of the former is still significantly lower than the other two schemes. The latter is under the same conditions. The larger the $q$, the better the connectivity rate. The connectivity of the scheme designed in this paper is always 1, and it is not affected by the size of the key pool.

In classic random key preallocation scheme, in order to ensure network connectivity, nodes must prestore a large number of keys. The basic condition is that the nodes can communicate securely. The two nodes have shared keys in the prestored key ring. The probability of sharing a key is

Table 8: Protocol security comparison table.

| Safety requirements | PUF | Song | NTRU | ZMAP |
|---|---|---|---|---|
| Prevent label information leakage | √ | √ | √ | √ |
| Antitag tracking | √ | √ | √ | √ |
| Antieavesdropping attacks | √ | √ | √ | √ |
| Man-in-the-middle attack prevention | ○ | ○ | √ | √ |
| Antireplay attack | √ | × | × | √ |
| Prevent denial of service (DoS) | ○ | ○ | ○ | ○ |
| Resistance to insider attacks | × | × | × | √ |
| Multisystem interconnection environment application | × | × | × | √ |

Note: √ means to provide, × means not to provide, and ○ means to provide conditionally.

Table 9: Protocol performance comparison table.

| Program | PUF | Song | NTRU | ZMAP |
|---|---|---|---|---|
| Encryption type | Hardware circuit | Hash function | Asymmetric encryption algorithm | Zero-knowledge proof |
| Time complexity | $O(1)$ | $O(1)$ | $O(n^2)$ | $O(n)$ |
| Space complexity | $O(1)$ | $O(n)$ | $O(n)$ | $O(n)$ |
| Safety balance | Static | Static | Static | Dynamic |

directly affected by the size of the key pool in the scheme and the size of the prestored key ring. In this paper, nodes between different clusters can establish connections through the routing of cluster heads. Any node in the communication range can establish session keys and authenticate each other. Compared with the $Q$-composite scheme with random preallocated keys, this scheme has a great advantage in connectivity, which improves the security connectivity and working efficiency of the sensor network.

*4.2.2. Invulnerability.* Since the design of the scheme is based on the multilayer multicluster network structure, if the member nodes in a cluster are captured, only the security of the cluster is threatened, and the operation of the system is not affected by $\tau$. When a node is captured, since the scheme uses a secret sharing mechanism, the key can be recovered by a polynomial to ensure the security of the cluster key. In addition, when the number of captured objects approaches or exceeds $\tau$, the scheme also establishes a dynamic update mechanism of the key, which greatly increases the difficulty of attack. Therefore, the nodes in this scheme have better anticapture. Figure 7 is a comparison of the theoretical invulnerability of the scheme and the $E$-$G$ scheme in this paper. It can be seen that the $E$-$G$ scheme has better invulnerability when the number of keys in the key pool is large and the prestored key ring is small. However, any node in this solution is captured or lost without affecting the communication of other nodes, and the antidestructive performance is good. The results of Figure 9 are shown as follows.

*4.3. Security Analysis of the Internet of Things.* In order to more intuitively show the advantages and disadvantages between the ZMAP protocol and the three typical protocols mentioned above, the list is now compared, and now we compare the security and protocol performance between them. The security is mainly compared with the protocol pair. Common RFID attacks and the ability to meet the security requirements of the new Internet of Things and the performance of the protocol are mainly compared with the time complexity and spatial replication of the protocol.

As shown in Table 8, the protocol security comparison table, it can be seen that the ZMAP protocol can provide various security features, followed by the PUF protocol, which provides the second most security, and other protocols have lower security. Wireless communication network is an essential infrastructure for the development of the Internet of Things. The signals generated by electronic labels installed on animals, plants, and articles can be transmitted through wireless communication network anytime and anywhere.

As shown in Table 9, it is a protocol performance comparison table. The ZMAP performance encryption type is zero-knowledge proof. The time complexity is the same as the space complexity, both $O(n)$, and NTRU has the highest time complexity.

As shown in Table 10, it is the recognition accuracy of indoor test samples. 300 sets of indoor environmental factor test samples were collected for interference factor experiments. Among them, 298 samples were correctly checked and only contained 2 error checks, and the recognition accuracy reached 99.33%.

As shown in Table 11, it is the recognition accuracy of outdoor test samples. Among them, there are 299 samples that are correctly checked, and only one sample is wrongly checked, and the recognition accuracy reaches 99.67%. It can be seen that the recognition accuracy of the test samples is more than 99% whether it is indoor or outdoor.

TABLE 10: Recognition accuracy of indoor test samples.

| Number of indoor test samples | Positive inspection (a) | False detection (a) | Recognition accuracy |
|---|---|---|---|
| 300 | 298 | 2 | 99.33% |

TABLE 11: Recognition accuracy of outdoor test samples.

| Number of outdoor test samples | Positive inspection (a) | False detection (a) | Recognition accuracy |
|---|---|---|---|
| 300 | 299 | 1 | 99.67% |

TABLE 12: Recognition speed of indoor test samples.

| Number of indoor test samples | Execution time (ms) | Execution speed (milliseconds/a) |
|---|---|---|
| 300 | 1.968 | 0.0066 |

TABLE 13: Recognition speed of outdoor test samples.

| Number of outdoor test samples | Execution time (ms) | Execution speed (milliseconds/a) |
|---|---|---|
| 300 | 1.949 | 0.0065 |

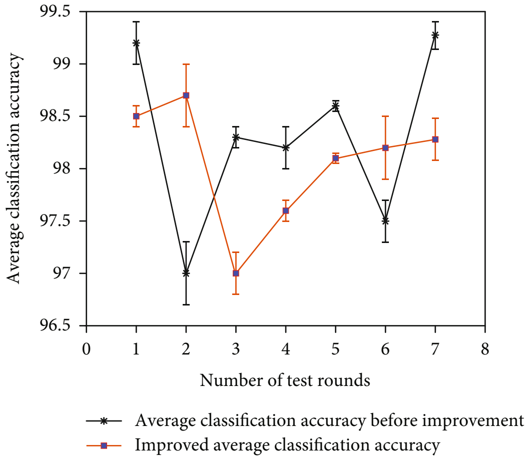

FIGURE 10: Comparison of classification accuracy.

As shown in Table 12, it is the recognition speed of indoor test samples. The speed of the SVM classifier in this experiment can reach the microsecond level when applied to scene recognition, and the execution speed is 0.0066 milliseconds/unit.

As shown in Table 13, it is the recognition speed of outdoor test samples. The execution time of 300 test samples is 1.949 ms, and the execution speed is 0.0065 ms/piece. It can be seen that the scene recognition speed is extremely fast, so it will not affect the efficiency of the authentication process of the experiment in this paper.

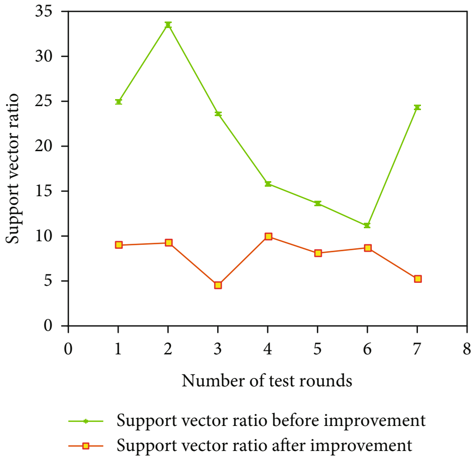

FIGURE 11: Comparison of the proportion of support vectors.

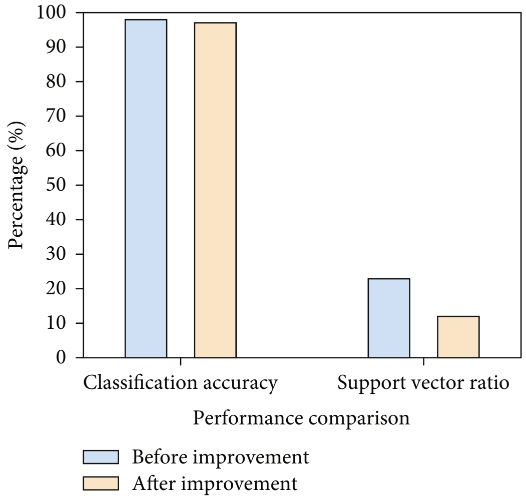

FIGURE 12: Histogram of classification accuracy and support vector ratio.

*4.4. Classification Performance Analysis of the Classifier.* As shown in Figure 10, for the comparison of experimental classification accuracy, it can be seen that the improved average classification accuracy is generally less than that before classification, and there is a slight decrease. At the same time, large-scale exposure of data will be vulnerable due to malicious attacks. Security factor is an important issue affecting the development of Internet of Things.

As shown in Figure 11, it is a comparison chart of the proportion of support vectors. This figure intuitively shows that the proportion of support vectors after the improvement is greatly reduced by more than twice the proportion of support vectors before the improvement.

As shown in Figure 12, by analyzing the experimental results, the improved PSO-SVM algorithm achieves better results in classification accuracy and support vector ratio.

While the classification accuracy is almost lost, the support vector ratio is reduced by 2-3 compared to before the improvement, thus greatly improving the generalization ability of the classifier.

## 5. Conclusions

(1) The key distribution protocol is the basis of sensor network security. Sensor network flexibility, fault tolerance, high sensing performance, no basic settings, low cost, high flexibility, fast layout, and other characteristics determine its wide range of applications. Based on the characteristics of sensor networks, the performance indicators of key distribution protocols are proposed. Analyze its premises, performance, load, application, and a brief description of some possible improvements and research directions

(2) Analyze the network structure and security requirements of the wireless sensor network. The key security is low for the traditional key management scheme. In the key negotiation process, the asymmetric key system is used between the cluster head and the base station. Authentication and cluster key management based on the threshold secret sharing mechanism in the common layer, which improves the key management flexibility while ensuring key security

(3) In-depth study of several key basic problems of efficient implementation of elliptic curve public key cryptosystem, design and implementation of efficient elliptic curve and random basis point efficient algorithm with high operational efficiency and high randomness, and the author's proposed various elliptic curve public key cryptosystem schemes

## Data Availability

This article does not cover data research. No data were used to support this study.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This study was supported by the project Research and Application of High Precision Control Strategy for 3D Printer (Project number: JJKH20180339KJ).

## References

[1] R. Valivarthi, I. Lucio-Martinez, P. Chan, A. Rubenok, C. John, and D. Korchinski, "Measurement-device-independent quantum key distribution: from idea towards application," *Journal of Modern Optics*, vol. 62, no. 14, pp. 1141–1150, 2015.

[2] L.-J. Wang, L.-K. Chen, L. Ju, M.-L. Xu, Y. Zhao, and K. Chen, "Experimental multiplexing of quantum key distribution with classical optical communication," *Applied Physics Letters*, vol. 106, no. 8, pp. 081108–081179, 2015.

[3] Y.-H. Li, Y. Cao, H. Dai, J. Lin, Z. Zhang, and W. Chen, "Experimental round-robin differential phase-shift quantum key distribution," *Physical Review A*, vol. 93, no. 3, 2016.

[4] C. Ma, W. D. Sacher, Z. Tang, J. C. Mikkelsen, Y. Yang, and F. Xu, "Silicon photonic transmitter for polarization-encoded quantum key distribution," *Optica*, vol. 3, no. 11, 2016.

[5] D. Lin, D. Huang, P. Huang, J. Peng, and G. Zeng, "High performance reconciliation for continuous-variable quantum key distribution with LDPC code," *International Journal of Quantum Information*, vol. 13, no. 2, p. 1550010, 2015.

[6] J. Jogenfors, A. M. Elhassan, J. Ahrens, M. Bourennane, and J. Larsson, "Hacking the Bell test using classical light in energy-time entanglement–based quantum key distribution," *Science Advances*, vol. 1, no. 11, p. e1500793, 2015.

[7] X. Zheng and Z. Cai, "Privacy-preserved data sharing towards multiple parties in industrial IoTs," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 968–979, 2020.

[8] D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," *Scientific Reports*, vol. 6, no. 1, 2016.

[9] Z. Tang, K. Wei, O. Bedroya, L. Qian, and H.-K. Lo, "Experimental measurement-device-independent quantum key distribution with imperfect sources," *Physical Review A*, vol. 93, no. 4, 2016.

[10] Z. Cai, Z. Xiong, H. Xu, P. Wang, and Y. Pan, "Generative adversarial networks," *ACM Computing Surveys*, vol. 54, no. 6, pp. 1–38, 2021.

[11] T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, and A. E. Lita, "Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding," *New Journal of Physics*, vol. 17, no. 2, 2015.

[12] M. Jahanbakht, X. Wei, L. Hanzo, and M. R. Azghadi, "Internet of underwater things and big marine data analytics—a comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 904–956, 2021.

[13] W. Chao, W. Shuang, Y. Zhen-Qiang, C. Wei, L. Hong-Wei, and Z. Chun-Mei, "Experimental measurement-device-independent quantum key distribution with uncharacterized encoding," *Optics Letters*, vol. 41, no. 23, 2016.

[14] J. L. Tsai and N. W. Lo, "Secure anonymous key distribution scheme for smart grid," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 906–914, 2016.