Journal of Combinatorial Mathematics
and Combinatorial Computing
www.combinatorialpress.com/jcmcc

Research on Secure Communication Mechanisms in Wireless Sensor Networks for Industrial Control Systems

Xin Wang[1], Wei Zhu[2,✉], Chun Chen[1]

[1] *Electrical Engineering Sanjiang University, Nanjing, Jiangsu, 210012, China*

[2] *Nanjing Cigarette Factory, China Tobacco Jiangsu Industrial Co., Ltd., Nanjing, Jiangsu, 210019, China*

ABSTRACT

In wireless sensor networks in industrial control systems, wireless communication security is challenged due to the broadcast nature of the wireless channel, where information is more easily eavesdropped by illegal nodes on the network. The article establishes a secure communication system based on ZigBee wireless communication technology applied to wireless sensor networks in industrial control systems. In order to improve the secure communication performance of wireless sensor networks, this paper combines the Merkle tree with the μTesla protocol to establish a key management scheme for wireless communication. Then from the node trust degree, the node two-way authentication mechanism for data transmission is constructed by combining the digital signature algorithm. For the effectiveness of the secure communication mechanism of wireless sensor networks, this paper carries out data analysis through performance testing. The key management scheme takes about 17.37 μs and 3.24 μs to add and revoke a key, respectively, and the local optimal value of user time consumption is 7.26 s when the connectivity frequency is 12 min and the revocation threshold is 60. The average value of the node bidirectional authentication mechanism can reach 96.17% for the accuracy of identifying the malicious nodes in the wireless sensor network, and the bit error rate is lower than 0.5 % for the communication transmission with the mesh topology. The bit error rate is less than 0.1%. The introduction of Merkle tree and digital signature algorithms into the construction of secure communication mechanisms in wireless sensor networks can significantly improve the data transmission security performance of industrial control systems.

Keywords: wireless sensor network; Merkle tree; digital signature; key management; secure communication mechanism

✉ Corresponding author.
E-mail address: njzhuwei_1982@163.com (W. Zhu).
Received 10 June 2024; Revised 25 August 2024; Accepted 20 January 2025; Published Online 16 April 2025.
DOI: 10.61091/jcmcc127b-069

1. Introduction

At the end of the 1990s, with the modern sensor equipment upgrades, the generation of a variety of wireless communication technologies and microelectromechanical systems technology, and other emerging technologies, which are interconnected and integrated with each other, the sensors are becoming more and more intelligent and smaller, along with the development of network technology, and then to the direction of networking [1-3]. A large number of miniature sensors are interconnected through the network to form a self-organizing network system - wireless sensor network, this kind of network can be in the collection of all the data information to be sensed within the network coverage area, and then through intelligent algorithms will be collected to process the data obtained, and finally the processed data will be saved in the network database, the user Finally, the processed data is stored in the network database, and users can access the database information to obtain the required information [4-7].

Industrial control automation technology is widely used in factory production lines, to increase production output, improve product quality and reduce energy consumption to provide important technical support, it is based on the principle of automatic control as the basic theoretical framework, combined with instrumentation technology, computer technology, etc., to realize real-time monitoring, real-time operation, real-time management of the whole process of production [8-11]. It mainly includes three major parts of industrial automation software, hardware and system [12].

The communication technology, coverage scale, and application areas used in wireless networks are different, so there exist a variety of classification methods [13]. According to the form of network organization, they can be classified as structured networks and self-organized networks [14]. Structured networks have a fixed communication infrastructure, are responsible for the access and authentication of wireless terminals, and provide network services, such as wireless cellular networks and wireless metropolitan area networks (WMAs), etc. Self-organized networks are organized according to a spontaneous form of networking, and there is no unified management mechanism, and nodes collaborate to provide services according to a distributed strategy, including mobile networks and sensor networks. In contrast, self-organized networks (especially sensor networks) face greater security and privacy risks due to the lack of network architecture and unified management mechanism support [15-18].

According to coverage, transmission rate and usage, wireless networks can be further categorized into, wireless wide area networks, wireless metropolitan area networks, wireless local area networks and wireless personal areas [19]. The basic security threats to wireless networks include information leakage, integrity breach, denial of service and illegal use [20]. These four basic security threats must be countered with appropriate security measures to achieve the four basic security goals of confidentiality, integrity, availability of information and legitimate use of resources [21-22].

Wireless networks have already brought us a lot of convenience in our life and work, and at the same time it also brings great challenges in information security. In order to solve the above challenges, institutions of higher education, research institutes and companies in various countries have invested a lot of human and material resources into the research of network security [23]. As a research hotspot and difficulty in today's information field, network security involves the intersection of several disciplines, including key management, secure routing, intrusion detection, and many other techniques need to be studied in depth [24]. Among them, privacy protection, secure reprogramming, user authentication, trust management, and network secure communication architecture are the most critical security techniques affecting the successful implementation of wireless networks and are the basis of many security operations [25].

Wireless sensor network is one of the hotspots in today's research, which is widely used in different industrial fields such as industrial production, environmental monitoring, etc. Its communication mechanism is the basis to ensure the safe and stable transmission of data. This paper is oriented to the

wireless sensor network architecture and energy transmission mode, combined with ZigBee technology to establish a secure communication system for wireless sensor networks. Based on the key list to establish Merkle tree, then combined with the μTesla protocol to build the data transmission key management scheme for wireless sensor networks. Based on the node behavioral trust degree, the node two-way authentication mechanism for secure communication is constructed by introducing digital signature algorithm. In order to verify the application effectiveness of the secure communication mechanism, performance tests are carried out from the perspectives of key management and node authentication, respectively.

2. Secure communication framework for wireless sensor networks

Industrial control system refers to the collection of personnel, hardware, strategy and software that play a role and influence on the safety, information security and reliable operation of industrial production process, including centralized control system, supervisory control and data acquisition system, programmable logic controller, remote measurement and control unit, and related information system such as human-machine interface. With the development of informatization and industrialization, industrial control systems are widely used in national defense and military industry, rail transportation, electric power grid, petrochemical industry, water conservancy and reservoirs, and other key industrial control industries related to the national economy and people's livelihood, due to its complexity and diversity, the secure communication of wireless sensor networks in industrial control systems is also faced with threats from various aspects.

2.1. Wireless Sensor Network Architecture and Transmission

2.1.1. Wireless Sensor Network Architecture. In a typical wireless sensor network (WSN), it usually includes sensor nodes, aggregation nodes, and task management nodes [26]. The wireless sensor network architecture is shown in Fig. 1. This kind of network, which is composed in a self-organized form, transmits data to the aggregation node through multi-hop relay, and finally connects to an external network, such as the Internet, UAV, or satellites to transfer the collected data in the whole monitoring area to the receiving node of the remote task for centralized management and information processing, while the user at the far-end can carry out the required configurations and management of the sensor network in the monitoring area through the corresponding management node The user can configure and manage the sensor network in the monitoring area through the corresponding management node at the remote end.

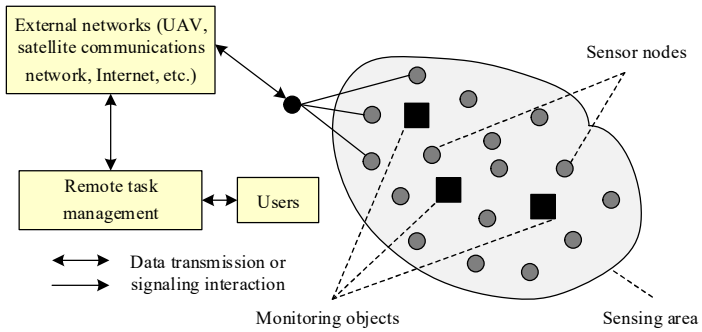


Fig. 1. Wireless sensor network architecture

Wireless sensor nodes are generally composed of four parts: sensor module, processor module, wireless communication module and energy supply module. The sensor module is responsible for the collection of information and data conversion in the monitoring area. The processor module is the brain of the entire node, responsible for controlling the entire sensor node data storage and processing

of its own collected data as well as data sent by other nodes. Wireless communication module is responsible for wireless communication with other sensor nodes, exchange control information and send and receive collected data. The energy supply module provides energy for the sensor nodes to run, usually powered by miniature batteries.

In sensor networks, the vast majority of sensor nodes are usually a miniature embedded system with relatively weak computational, storage and communication capabilities, powered by batteries carrying limited energy. In terms of functional roles, each sensor node has a dual function. Both with the traditional network terminal and router functions, on the one hand, can be near the region of the information collection and data processing, but also shoulder the other nodes of the network forwarded to the data management, storage, fusion and forwarding and other tasks.

2.1.2. Network Energy Transfer Model. Depending on the distance between the wireless sensors, between the wireless sensors and the base station, and between the receiver and the transmitter, the energy consumption of the wireless communication of the sensor nodes in the network will be chosen to use both the free-space propagation model and the multipath fading model. If the distance between the receiver and the transmitter is less than a certain threshold value d_0, the free space model will be used for energy consumption; if the distance between the receiver and the transmitter is greater than a certain threshold value, the multipath fading model will be used for energy consumption. In this way, the energy consumed by this wireless channel if it sends a 1 Byte data message to a receiving device that is separated by a distance of d is:

$$\begin{aligned} E_{Tx}(l,d) &= E_{Tx-elec}(l) + E_{Tx-amp}(l,d) \\ &= \begin{cases} lE_{elec} + l\varepsilon_{fs}d^2 & d < d_0 \\ lE_{elec} + l\varepsilon_{amp}d^4 & d \geq d_0 \end{cases} \end{aligned} \tag{1}$$

The energy consumed to receive 1Byte of information is:

$$E_{R_x}(l) = E_{R_x}ed_0 \Rightarrow lE \tag{2}$$

Where $E_{Tx}(l,d)$ represents the energy consumption at the transmitter side, $E_{Rx}(l)$ represents the energy consumption at the receiver side, E_{elec} represents the energy consumed by the transmitter circuit, ε_{fs} and ε_{omp} represent the amplifier coefficients, while d_0 is the critical distance.

The borrowing point aggregates m 1Byte messages and the energy consumed is:

$$E_{DA} = mlE_t \tag{3}$$

Where, E_{da} represents the energy consumed to aggregate a unit bit of data.

So when $d > d_0$, $E_1' > E_2'$, i.e., the energy consumed in a single hop is greater than the energy consumed in multiple hops.

So when the transmission distance is greater than the critical value d_0, the multi-hop approach is more efficient in utilizing the energy in the wireless sensing network and prolongs the survival life of the network.

2.2. Secure Communications Program for Wireless Sensor Networks

2.2.1. ZigBee wireless communication technology. Zigbee is a short-range, low-power wireless communication technology for Internet of Things (IoT) and Machine-to-Machine (M2M) applications. It is an open standard, developed by the IEEE, based on the IEEE 802.15.4 standard, and uses low-power RF technology for low-speed, low-bandwidth data transmission. Its network can be formed into a network that supports point-to-point, star, tree and mesh topologies, as well as broadcast and multicast communication methods, with self-organization, self-healing and self-adaptation

characteristics, which can realize the IoT applications in the fields of smart home, smart city, smart transportation, smart healthcare and so on [27].

The Zigbee protocol stack consists of two main parts, the application support sublayer (APS) and the network layer (NWK). They are responsible for processing application layer data and network layer data respectively.APS is an optional protocol layer which provides an interface between the high level application and the underlying network layer.The APS layer processes Application Data Units (ADUs) and passes them to the network layer. It also provides identification and control of devices in the Zigbee network, such as support for security and connectivity.NWK is the core part of the Zigbee protocol stack, which handles network discovery, routing, and data transfer. It uses the Network Layer Protocol (NLP) to control the network topology and routing tables while supporting multiple routing protocols, including those based on centralized routing, distributed routing, and hybrid routing.

In addition, the Zigbee protocol stack includes physical (PHY) and MAC layers, which are responsible for wireless communication and medium access control. The physical layer handles the physical medium and wireless signals, while the MAC layer handles the frame format, transmission and reception of frames, and management of the network topology. Together, these two layers provide Zigbee networks with low power, low latency, and highly reliable communication characteristics.

2.2.2. ZigBee-based secure communication. In order to realize the secure communication of wireless sensor network in industrial control system, this paper proposes the secure communication architecture of wireless sensor network based on ZigBee technology, and its specific framework is shown in Figure 2 [28]. Among them, the ZigBee network consists of ZigBee terminal devices, ZigBee router, and ZigBee coordinator, the temperature and humidity data are collected on the sensors on the ZigBee terminal devices and then the data are aggregated to the ZigBee coordinator, and the coordinator transmits the data to the server through the serial port. Mobile terminals and PCs can access the server through the Internet so as to read the environmental data collected by the ZigBee terminal devices, and they can also give control commands to the ZigBee network through the mobile terminals and PCs, such as replacing the encryption and hash algorithms, and reading the battery status of the ZigBee terminal devices, and so on.

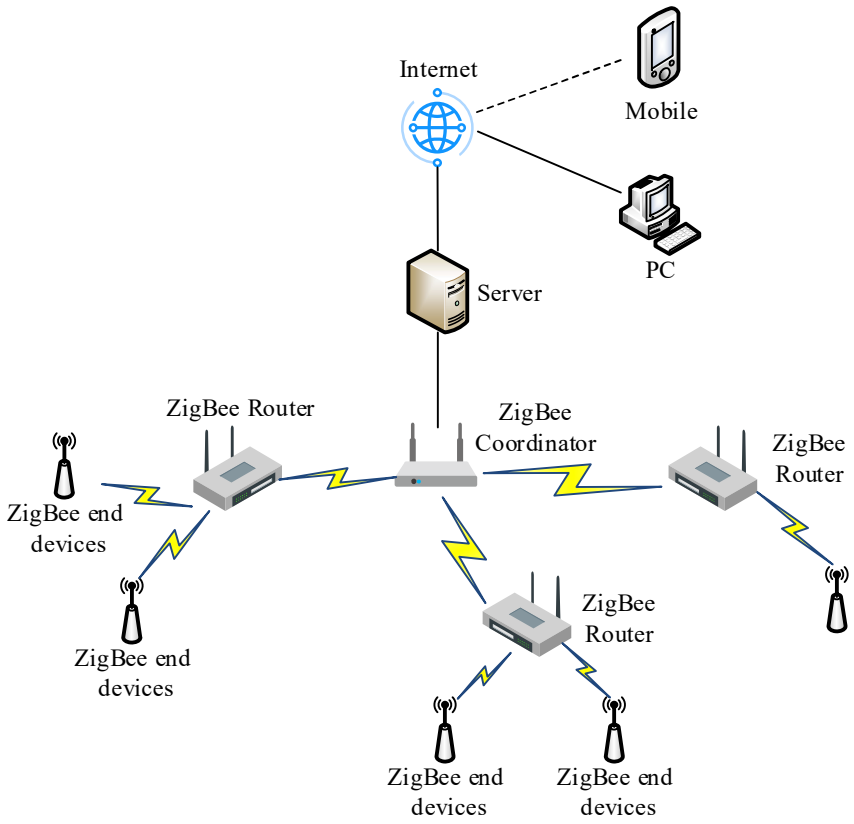


Fig. 2. The security communication framework based on Zigbee

The process from sensor collected data to data processing transmission and data reception unpacking is:

1) The ZigBee end device reads the sensor data collected by the sensor.

2) The ZigBee end device node processes the data according to the predefined encryption algorithm. If the data does not take any security measures, the packet Payload field is sensor data plaintext at this time. If the data packet takes security transmission measures, the corresponding encryption and hash algorithms are used to securely process the data to be transmitted to obtain the ciphertext and hash value, and the hash value is the result of hashing the plaintext of the data to be transmitted.

3) ZigBee end device nodes group packets and send them according to the secure communication packet format.

4) The ZigBee coordinator receives the wireless sensing packet from the terminal and parses the data according to the contents of the data header. If the values of the encryption and hash fields are not zero, the corresponding decryption algorithm is used to decrypt the data and check whether the data has been tampered with by recalculating the plaintext hash value. The packet unpacking operation can also be placed on the backend of the server, where the coordinator only acts as a data forwarder.

3. Secure Communication Mechanisms for Wireless Sensor Networks

With the deepening of research and the development of related hardware technology, wireless sensor networks have been deployed more and more in practical applications and gradually penetrated into data-sensitive fields such as military detection and resource protection. The security of wireless sensor networks is an important guarantee for the implementation of these applications, which enables wireless sensor networks to exclude the interference of attackers, interact with users normally, and provide data basis for correct decision-making. However, because the nodes in wireless sensor networks are limited by energy, storage space, computing power and their own security, it makes

ensuring the security of wireless sensor networks a great challenge. How to develop an efficient secure communication mechanism based on the characteristics of wireless sensor networks has become a current research hotspot.

3.1. Merkle Tree Based Key Management

3.1.1. Merkle trees. Merkle tree is a fully binary tree with nodes consisting of Hash values. Where the leaf node value is the Hash value containing the data and the intermediate node value is computed from the Hash values of its two child nodes as parameters [29]. For effective and secure communication in wireless sensor networks, this paper establishes the basic reactor Merkle tree and sensor Merkle tree based on existing research. The details are as follows:

1) Reactor Merkle Tree. Construct N leaf node $L_1 \cdots L_N$, each leaf node corresponds to a reactor in the wireless sensing reaction network. The Hash value Φ of each leaf node contains the identity id and public key of that reactor. After building the leaf nodes, build the whole reactor Merkle tree from leaf to root, counting the node values:

$$\Phi\left(L_i\right) = Hash\left(id_i, pk_i\right) fori = 1, \cdots, N \tag{4}$$

The intermediate node values are denoted as:

$$\Phi(V) = Hash\left(\Phi\left(V_{left}\right) \| \Phi\left(V_{right}\right)\right) \tag{5}$$

2) Sensor Merkle Tree. In addition to the leaf nodes containing information about the identity, deployment location and public key of this sensor node, the sensor Merkle tree is built in the same way, where the leaf node values can be expressed as:

$$\Phi\left(L_i\right) = Hash\left(id_i \oplus loc_i, pk_i\right) \; for \; i = 1, \ldots, M \tag{6}$$

The intermediate node values can be expressed as:

$$\Phi(V) = Hash\left(\Phi\left(V_{left}\right) \| \Phi\left(V_{right}\right)\right) \tag{7}$$

3) Merkle tree public key authentication process. Let Alice's public key be pk, L is Alice's corresponding leaf node in the Merkle tree, λ is the path from leaf node L to the root node. H is the length of λ, which is the Merkle tree height. For each node $v \in \lambda$ on the path, Alice sends Φ (v's sibling) and their public key pk to Bob, we use $\lambda_1, \lambda_2 \ldots . \lambda_H$ to denote these Φ values and call these Φ values evidence. To authenticate Alice's public key pk (let Alice's identity be id and her location be loc), Bob computes the Hash $\left(loc \oplus loc, pk\right)$ and then reconstructs the Merkle tree R' using this Hash value and the evidence $\lambda_1, \lambda_2 \ldots . \lambda_H$ by setting the Hash value of the root of R' to be $\Phi\left(R'\right)$. Bob will trust that the pk public key is Alice's public key only if $\Phi\left(R'\right) = \Phi(R)$.

3.1.2 Merkle tree construction. In order to enhance the performance of secure communication in wireless sensor networks, this paper constructs a Merkle tree structure based on a key list based on blockchain technology.The Merkle tree is used to summarize all the keys in a block, and at the same time generates a digital fingerprint of the entire key list, and provides an efficient way of verifying whether a certain key exists in a block.

Generating a complete Merkle tree involves recursively hashing the hash values, with each non-leaf node having two child nodes that are hashed together based on the 256-bit hash values of the two child nodes in series. In order to resist the length extension attack against SHA256 hash function, double hashing algorithm is used in Merkle tree, so the time complexity of building a Merkle tree can be expressed as:

$$O(n) = N \log_2\left(N\right) \tag{8}$$

Each block keeps a table corresponding to file information and file key, and is sorted by file information. When N file information with a file key is inserted into a leaf node of the Merkle tree, up to $\log_2(N)$ calculations are performed to determine whether the block contains the file key. Then:

$$O(n) = \log_2(N) \tag{9}$$

The Merkle tree is constructed from the bottom up, the leaf nodes hold the file information cipher hash and the file key cipher, the file information cipher hash serves as the unique identifier of the file in the blockchain. The file key ciphertext is the ciphertext state of the file encryption key.

The hash values of the leaf nodes in the Merkle tree are generated using the following algorithm, if the file information cipher hash $(FICH)$ and the file key cipher (FR) have been obtained as:

$$H = SHA256\left(SHA256\left(FICH + FR\right)\right) \tag{10}$$

The hash value of a non-leaf node in a Merkle tree is generated using the hash value of two child nodes, and if there is only one child node, that child node is copied.

Merkle tree in some specific cases there will be a non-leaf node with only one child node, calculate the hash value of that non-leaf node using the hash value of the child node twice. Then:

$$H_{1+1} = SHA256\left(SHA256\left(H_1 + H_1\right)\right) \tag{11}$$

After the above process, the Merkle tree will finally generate only a 256-bit root hash value $\left(H_{1+2+\ldots+n}\right)$ to be stored in the Block Header and participate in the calculation of the nonce value in the Block Header.

$$\begin{aligned} &SHA256\left(SHA256\left(PreviousBlockHash + BlockHeader + H_{l+2+\ldots+n} + nonce\right)\right) \\ &<= target \end{aligned} \tag{12}$$

In key storage, it is very common for a single block to have an amount of thousands of keys, and summarizing any number of keys with the above method will produce a hash value of just 256 bits as the Merkle root hash value to participate in the calculation of the nonce value of the block. And according to the characteristics of the Merkle tree, once a key is tampered with, the hash value of its parent node as well as that of the parent node's parent node will change, and an avalanche effect occurs.

3.1.3. Key management authentication program. Based on the result of Merkle tree construction based on key list, and combined with the existing μTesla protocol, this paper proposes a secure communication key management scheme applied to wireless sensor network, which mainly ensures the effective distribution of node parameters in the sensor network, solves the initialization problem of node parameters, and realizes the secure communication of wireless sensor network. Its specific steps are as follows:

1) All nodes request like gateway node, and the gateway node sends all node information under this gateway to the server.

2) The server assigns parameters to each node, and the parameter format is consistent with the μTesla protocol, and the parameters are:

$$Para_i = K_0 \left| T_s \right| T_{\text{int}} \left| \delta \right. \tag{13}$$

Where K_0 represents the initial key on the key chain, T_s represents the starting synchronization time, T_{int} represents the validity period of a key, and δ represents the number of intervals for delayed key release.

3) The server generates a Merkle tree with the parameters of each node as leaf nodes and sends the root of the tree to each receiving node.

4) The server returns to the node parameter certificates through the gateway node, which include the parameters of this node and the authentication path to the root of the Merkle tree.
5) When a node wants to transmit, each transmitting node first sends a message packet carrying a parameter certificate $Para_{certi}$ to all the receiving nodes with which it communicates to verify its identity.
6) The receiving node receives the parameter certificate sent to it by the sending node, uses the hash function to calculate the authentication path, and compares the calculated tree root value with the locally stored tree root value M, and if they are the same, it means that the parameter is correct.

The authentication passes. After the authentication is passed the receiving node records the broadcast parameters of all the broadcast nodes, the broadcast parameters are used to authenticate the packets broadcast by the broadcast nodes, after that the receiving node authenticates the packets and the communication between the receiving node and the broadcast node is the same as in the μTesla protocol.

3.2. Two-way authentication of nodes based on digital signatures

3.2.1. Trust in node behavior. Node trust degree is the degree of subjective trust that a node has in a particular behavior of another node. Generally, there exist three degrees of node trust, namely direct trust, indirect trust and combined trust. Direct trust degree refers to the subjective trust of a node directly to another node, indirect trust degree refers to the need of a trusted third party to get mutual trust between two nodes, and combined trust degree refers to the combined effect of direct and indirect trust degrees to get mutual trust between two nodes. The related parameters are defined as follows:

$IDT_{ij}(t)$ denotes the indirect trust obtained by node i evaluating node j up to t moments, $P_i(t)$ is the number of positive behaviors of node j during node i record t time, $N_{ij}(t)$ is the number of negative behaviors of node j during node i record t time. α is the security action coefficient, which is non-negative, $F_i(t)$ indicates the frequency of interaction between node i and node j up to the t moment, and a node can reduce the number of interactions of malicious nodes and achieve a high level of trust only if it receives multiple favorable comments.

In the calculation of node trustworthiness, to prevent selfish nodes from masquerading as normal nodes, the time is divided into N time slice, each of size T_1 and total time $T = N * T_1$.

The direct trust degree is calculated as:

$$DT_{ij}(t) = \begin{cases} \dfrac{\sum P_{ij}(t)}{\sum P_{ij}(t) + \alpha \times \sum N_{ij}(t)} F_{ij}(t) & i \neq j \\ 0 & i = j \end{cases} \tag{14}$$

Suppose $\{K_1, K_2, K_3, \cdots, K_N\}$ is a neighbor node of node i and a neighbor node of node j.
1) At the moment t, superimpose the direct trust of node i to node k_x with the following formula:

$$DT(t) = \sum_{x=1}^{N} DT_{j_x}(t) \tag{15}$$

2) The indirect trust of node i to node j at moment t, Eq:

$$IDT_{ij}(t) = \frac{\sum_{x=1}^{N} DT_{ik_x}(t) \cdot \omega(k_x)}{DT} \tag{16}$$

Among them, the recommendation trustworthiness of node k_x is $\omega(k_x)$, which is used to prove that the relevant information of the recommended node is accurate and true.

3) β_{DT} is the direct trust weight, β_{DDT} is the indirect trust weight, and the comprehensive trust degree of node j is calculated as follows:

$$T_{\Phi}(t) = \beta_{DT} \times DT(t) + \beta_{DDT} \times IDT_{ij}(t) \tag{17}$$

4) Set the initial trust threshold of the system to 0.5, if the node's combined trust is less than this value, the node is not trustworthy, otherwise it is trustworthy.

3.2.2. Node Bidirectional Authentication Algorithm. In order to improve the secure communication performance of wireless sensor networks, digital signatures are used to accomplish two-way authentication between trusted nodes. By using digital signature algorithms and public key cryptography, it is ensured that the communication between the nodes is secure and reliable and prevents threats such as man-in-the-middle attacks and information tampering [30]. The use of digital signatures effectively enhances the confidentiality, integrity and trustworthiness of network communication. Digital signatures are based on bilinear mapping and the process of applying them to two-way authentication of WSN nodes is as follows:

Suppose a trusted node i is prejoined to a cluster j after the above authentication, and a unique ID_i is assigned to it when the base station performs the registration operation and transmits the ID_j of the cluster head node of the cluster to the node as a way of assigning the node a unique private key $S_e k_i = vG(ID_i \| x_i)$, where x_i is the solution to the equations owned by the node i.

Node i chooses a random number $n \in Z_c$ and unfolds a digital signature, viz:

$$\begin{cases} \zeta_i = WS_i + nD \\ \zeta_i' = e(D, D)^n \end{cases} \tag{18}$$

Where ζ_i, ζ_i' are used to denote the 1st and 2nd digital signatures generated by node i respectively, D denotes the generating element, Z_c represents the modulo c integer multiplicative group, and e denotes the bilinear mapping function.

When nodes implement information exchange, node i sends itself ID_i, signature pair $\{\zeta_i, \zeta'_i\}$, and the timestamp t_g at the time of sending the digital signature together in a package to the cluster head node j, and the cluster head node j unfolds the digital signature authentication, viz:

$$e(\zeta_i, D) e\left(G\left(ID_i \| x_i\right), -D_{pub}\right) \zeta_i' \tag{19}$$

Where G represents the hash function and D_{pub} represents the whole system public key, if the above equation satisfies the equality condition, then it means that node i passes the authentication and becomes a real legitimate node. Node i passes the authentication and finds its symmetric key as:

$$K_{i-j} = e\left(WSe_i, G\left(ID_j \| x_j\right)\right) \tag{20}$$

Where K_{i-} expresses the symmetric key generated by node i to communicate with cluster head node j, cluster head node j uses its own private key $Sek_i = vG\left(ID_j \| x_j\right)$ to derive its symmetric key as:

$$K_{j-i} = e\left(G\left(ID_i \| x_x\right), WSek_j\right) \tag{21}$$

Where K_{j-i} represents the symmetric key generated by the cluster head node j to communicate with the node i, which is utilized K_{j-i} to generate the signature $\varepsilon = g\left(K_{j-i}\right)$ and sent to the legitimate node i to unfold the verification. The verification formula is $g\left(K_{i-j}\right)\varsigma$, where g represents the hash function $\{0,1\} \to Z_c$. If the formula satisfies the condition of equality, the cluster head node j is proved to be legitimate.

This completes the two-way authentication of node i and cluster head node j, at this time the wireless sensor network is also known as a high-security network structure, but also produces the corresponding symmetric key for information exchange.

4. Performance testing and analysis of secure communication mechanisms

Advances in sensor technology, microelectronics technology, network technology and wireless communication technology have promoted the generation and development of wireless sensor networks. Wireless sensor networks are capable of accomplishing target monitoring and tracking tasks in complex environments, and have been widely used in many industrial control fields in military and civilian applications, playing an increasingly important role. However, the sensor nodes in wireless sensor networks are easily affected by the external environment, thus affecting their safe communication performance, how to build a safe communication mechanism for wireless sensor networks in industrial control systems is a problem that must be solved to ensure that wireless sensor networks can be widely used.

4.1. Communication key management authentication

4.1.1. Key management performance. The experiments in this section illustrate that the scheme meets the design goals of high efficiency and smaller space occupation by showing the time overhead of the key management scheme based on the combination of Merkle tree and μTesla protocol in adding and revoking a single key under different key number scales and comparing it with the traditional static and dynamic MHT tree and CAT based schemes. In this context, the scale of the number of keys is set to 2n, $n \in [1,15]$, respectively.Meanwhile, the hash function in the paper is selected as SHA256 and the symmetric encryption algorithm is AES256 algorithm. Fig. 3 shows the comparison results of key addition time overhead of different key management schemes.

Since the insertion of a leaf node containing a new key in the MHT requires updating the hash values of the relevant nodes in each layer up to the root node from the bottom up. Therefore, the number of layers of the MHT becomes progressively larger as the key size becomes larger, while the number of times the hash function needs to be computed is the same as the number of layers of the MHT. In CAT scheme, as the left leaf node keeps the key hash value while the right leaf node keeps the key chameleon hash value. Therefore the number of CAT layers is more than the number of MHT layers for the same number of keys. In the key management scheme designed in this paper, the number of times the hash function is calculated is related to the insertion path of the key. Since the Merkle tree has extension nodes and branch nodes with 16 children, the number of nodes that the key passes through when it is inserted into the Merkle tree is greatly reduced compared to the number of layers of MHT and CAT. The experimental results show that the key management scheme designed in this paper takes a more stable time to add a new key, which is about 17.37 μs, under different key number scales. And when n>9, the elapsed time to add a key for the MHT tree-based scheme increases gradually. For example, when n=9, the elapsed time of dynamic and static MHT is 22.03μs and 21.54μs, respectively. The dynamic and static MHTs reach 34.59 μs and 38.31 μs, respectively, when n = 15. Meanwhile, the time consumption grows from 24.02 μs to 41.11 μs under the CAT scheme. Therefore, the Merkle tree designed in this paper combined with μTesla protocol possesses better key addition computational overhead time, and the time consumed by Merkle tree to add a single key is independent of the key size, while the efficiency of the remaining schemes decreases with the increase of keys.

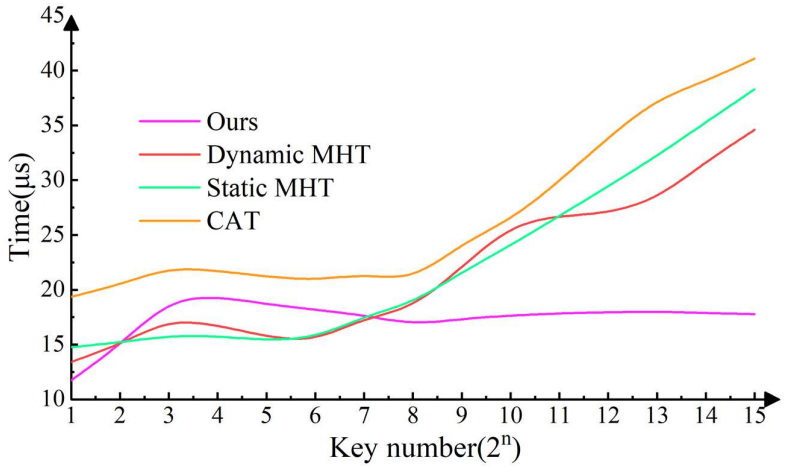


Fig. 3. The key new time cost comparison results

Similarly, in order to maintain the balance of the binary tree, revoking a key in MHT and CAT is done by updating the value of the leaf node where the key is located to the hash value of the joint revocation flag of the original key and recalculating the hash value layer by layer up to the root node. In contrast, the scheme in this paper only needs to delete the leaf node corresponding to the key directly according to the search path and update the hash value of all nodes on the path to complete the key revocation. Fig. 4 shows the comparison results of key revocation time overhead of different key management schemes.

Under different key number sizes, the method in this paper takes about 3.24 μs to revoke a key, and when n = 5, the dynamic and static MHTs take 11.65 μs and 17.26 μs, respectively, and CAT takes 17.35 μs. When n = 15, the dynamic and static MHTs take 37.51 μs, 39. 41 μs, respectively, and CAT takes 40.43 μs. Similar to the key addition efficiency, the key revocation efficiency of the key management scheme designed in this paper remains more stable when the key size becomes larger, while the other schemes gradually decrease.

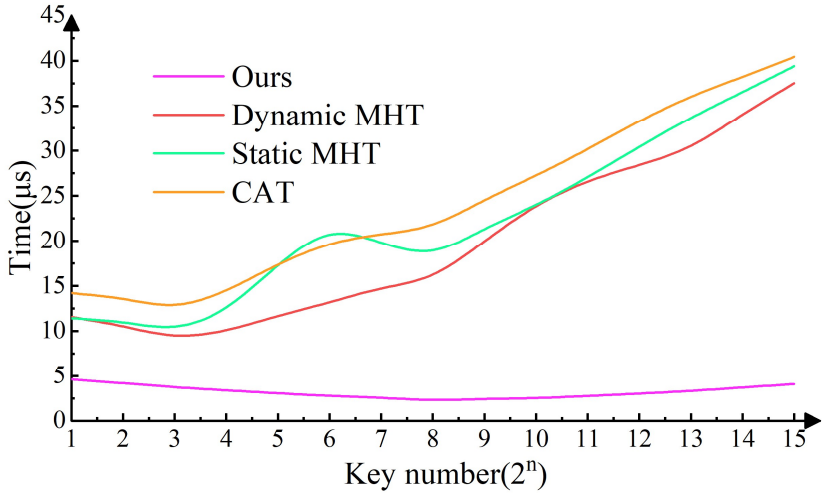


Fig. 4. The key revocation time cost comparison

When performing key verification, MHT and CAT need to generate the verification path based on the position of the leaf node where the key is located, and comparing the hash value of the new root node computed based on the path with the value stored in the TPM. In contrast, the scheme in this paper has the characteristics of a dictionary tree, so it can directly search for the corresponding leaf nodes based on the search path of the key, and recalculate the hash values of all nodes on the path to the root

node, and compare them with the root node in the TPM to determine whether the key is valid or not. Overall, the key management scheme for wireless sensor networks based on Merkle tree combined with μTesla protocol in this paper is not affected by the key size and has better key management efficiency.

4.1.2. Network influences. In the process of key update, the network quality is an important factor that affects the key update time, so the network factor is added in the experiment to test the key management scheme designed in this paper and analyze the usability of the algorithm. Before the message sending at the cluster head, the connectivity status of the sensing node is firstly detected, and when it is connected, the message is sent directly, otherwise the revocation algorithm for that sensing node is automatically executed. In the experiment, two threshold triggers are added, i.e., connectivity frequency trigger as well as undo threshold trigger. The Connectivity Frequency (CF) is the time interval for connectivity test, in which one connectivity test is performed in each time interval. The revocation threshold trigger is the upper limit of the number of consecutive disconnections, and when the number of consecutive disconnections reaches a certain value, the sensing node revocation algorithm is executed. The time consumption of the user under the influence of network factors is shown in Fig. 5.

As can be seen from the table, when the connectivity frequency is increased from 0.5min to 60min, the user's time consumption is decreasing, and its time consumption decreases gradually with the increase of the revocation threshold. Based on the consideration of revocation threshold and connectivity frequency, it can be seen that when the connectivity frequency is 12min and the revocation threshold is equal to 60, the local optimal value of the user's time consumption can be obtained as 7.26s, and at this time, the number of key operations performed by the user is relatively small. Therefore, the key management scheme for secure communication in wireless sensor networks based on Merkle tree combined with μTesla protocol in this paper can effectively reduce the time consumption brought by different network environment factors and provide a reliable encryption mechanism to ensure secure communication in wireless sensor networks.

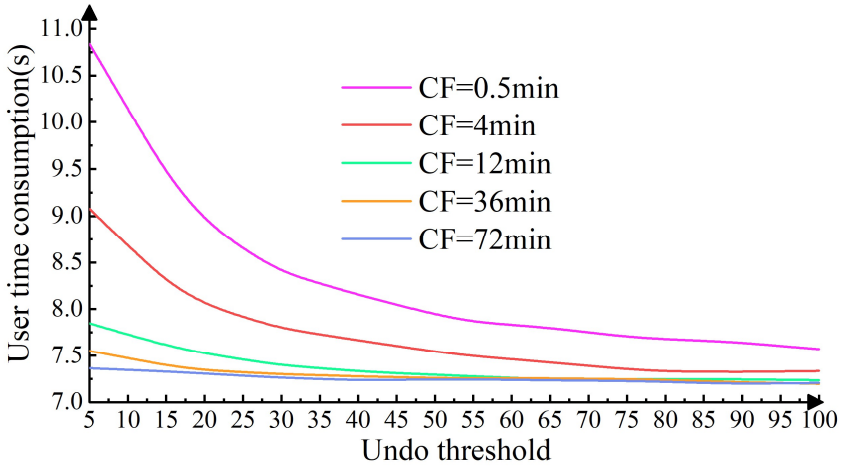


Fig. 5. Time consumption under different network environment

4.2. Node Bidirectional Authentication Analysis

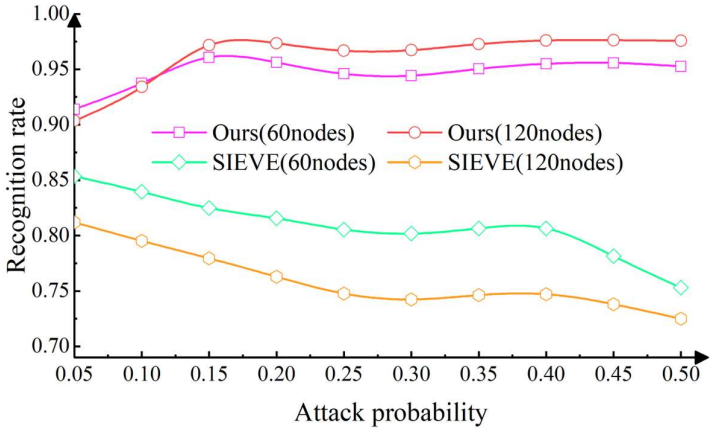
4.2.1. Malicious node identification. In this paper, we propose a two-way authentication mechanism for nodes that combines trust and digital signatures with the aim of better identifying trusting nodes, while those with lower trust are judged as malicious nodes. Based on this, this subsection uses recognition rate and false detection rate as evaluation metrics as a way to assess the accuracy of the node two-way authentication mechanism in recognizing malicious nodes.

The node identification accuracy of the mechanism is evaluated by comparing the node two-way authentication mechanism proposed in this paper with SIEVE technique in terms of recognition rate and false detection rate under a specific attack probability. Here the attack probability is defined as the ratio of the number of malicious nodes to the total number of sensor nodes in the network. In the experiment the attack probability is set to be 0.05 to 0.5 and then the recognition rate and false detection rate of the algorithm are recorded in two cases, which means the total number of sensor nodes in the wireless sensor network is set to be 60 and 120, respectively.In these two cases, the variation of the recognition rate and the false detection rate of the node bi-directional authentication mechanism proposed in this paper with the SIEVE technique with respect to the attack probability is shown in Fig. 6. Where Fig. 6(a)~(b) shows the variation of recognition rate and false detection rate with attack probability, respectively.

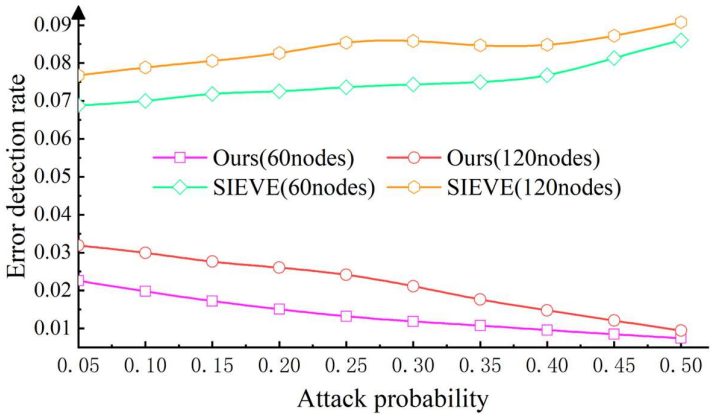
The increase in attack probability means that more malicious nodes are captured in the network to launch attacks on the wireless sensor network. From Fig. 6(a), it can be found that as the attack probability grows, the recognition rate of the node bi-directional cognition mechanism proposed in this paper varies less, and its recognition rate basically stays at a high level (the minimum value is 90.36%). When the total number of sensor nodes is 60, the recognition rate of the node two-way authentication mechanism under various attack probabilities maintains above 91% with an average of 94.72%, while when the total number of sensor nodes is 120, the recognition rate under various attack probabilities maintains above 90% with an average of 96.17%. However, the recognition rate of SIEVE technique is lower than the recognition rate of node two-way authentication mechanism and decreases approximately with the increase in attack probability. When the total number of sensor nodes is 60, the highest recognition rate of SIEVE is 85.35% and the average recognition rate is 80.87%, while when the total number of sensor nodes is 120, the highest recognition rate of SIEVE is 81.19% and the average recognition rate is 75.96%.Even the highest recognition rate of the SIEVE technique is 5.01 percentage points lower than the lowest recognition rate of the algorithm proposed in this paper.

From Fig. 6(b), it can be found that the misdetection rate of the node bi-directional cognition mechanism proposed in this paper basically maintains at a low level as the probability of attack increases, with an average misdetection rate of 1.36% and 2.15% for 60 and 120 sensor nodes, respectively. However, the misdetection rate of SIEVE technique is higher than the misdetection rate of the node two-way authentication mechanism, and the misdetection rate increases approximately with the increase of the attack probability, and the misdetection rates of 60 and 120 sensor nodes are 7.51% and 8.37% on average, respectively.The misdetection rate of SIEVE technique is at least 3.49 times of the misdetection rate of the algorithm proposed in this paper.

Through the above analysis, it can be found that compared with SIEVE technology the two-way node authentication mechanism proposed in this paper has a higher accuracy in identifying malicious nodes from the trust degree of node behaviors, that is to say, the node two-way authentication mechanism proposed in this paper is able to more accurately identify malicious nodes in the wireless sensor network. This is mainly because the node two-way authentication mechanism is based on the node behavior trust, combined with the digital signature algorithm to assess the node behavior, and the third party node with a larger weight of trust to carry out the assessment work, which leads to a more efficient identification of nodes in the network.



(a) Recognition rate and attack probability



(b) Error detection rate and attack probability

Fig. 6. The recognition rate and the error rate vary with the probability of attack

4.2.2. Communication security verification. Since high information entropy represents higher randomness and unpredictability and is commonly used for node authentication security analysis, this paper adopts information entropy to analyze the characteristics of the hash function. Let the hash value of a node A consists of three random variables, assuming that the distribution of these hash values is uniform (i.e., the probability of each hash value is equal), and the hash values of different nodes are independent of each other. The greater the information entropy of the node hash value, the higher the uncertainty and randomness of the hash value, thus increasing the security of the hash function. The effectiveness of the method of this paper is verified by the comparison of information entropy between the node two-way authentication mechanism and the authentication methods of MPCAuth, Multi-level Authentication Encryption System (MAES), and the improved CoPA protocol. The comparison results of different methods are shown in Fig. 7.

From the figure, it can be seen that the information entropy of the node two-way authentication mechanism proposed in this paper is significantly larger than that of the authentication methods of the other three algorithms, and its mean value is 62.69%, 111.45%, and 150.43% higher than that of the improved CoPA protocol, the Multi-Level Authentication Encryption System (MAES), and MPCAuth, respectively. This is due to the fact that although the node two-way authentication mechanism set up in this paper is relatively lightweight in terms of calculating hashes for individual nodes, due to the fact that each device ID is unique. And the structure of digital signature splices and uploads multiple lightweight hashed unique IDs layer by layer to the root node, thus greatly increasing the randomness of the root node. While the other three methods do not realize the combined authentication of multiple nodes and only authenticate each node individually, with lower randomness. Therefore, this fully

verifies the security of the node two-way authentication mechanism based on node trust degree and digital signature proposed in this paper, which can fully ensure the secure communication of wireless sensor networks in industrial control systems.

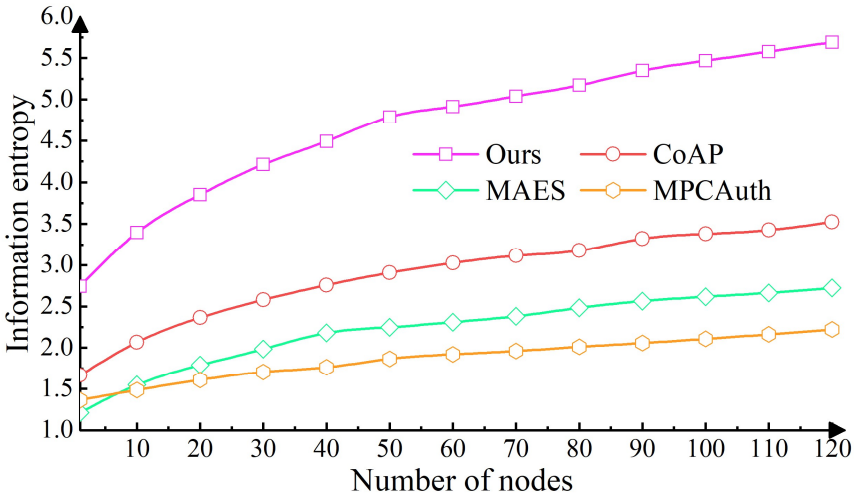
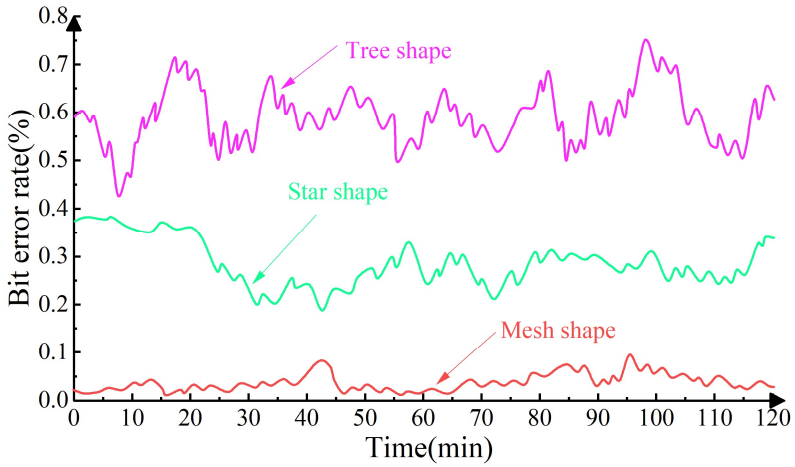


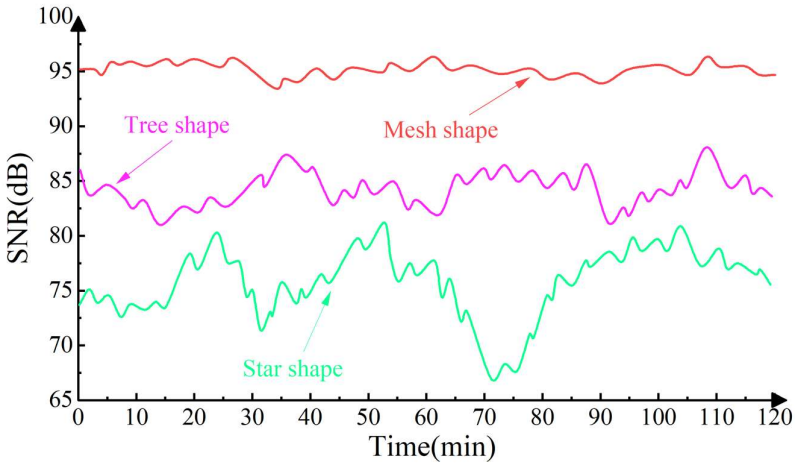
Fig. 7. Comparison results of different methods

4.2.3. Sensor Node Testing. Based on the key management scheme and node two-way authentication mechanism designed in this paper, it is applied to the secure communication of wireless sensor networks in industrial control systems. Since the wireless sensor network contains three topologies: tree, star and mesh, the performance of sensor nodes under the three topologies is tested based on the two schemes to further enhance the secure communication capability of the wireless sensor network. In the sensor node test, this paper selects the bit error rate and signal-to-noise ratio as the test basis, the bit error rate is a measure of the data accuracy of data transmission in a certain period of time, the smaller the bit error rate is, the better the performance of the sensor network node. The signal-to-noise ratio is an index used to measure the proportion of noise, the larger the signal-to-noise ratio is, the smaller the signal noise is. The test results of sensor nodes in different topologies are shown in Fig. 8, where Fig. 8(a)~(b) shows the results of bit BER and SNR, respectively.

In the monitoring results of the bit error rate of the sensor node state shown in Fig. 8(a), when the topology of the sensor is tree-type, its bit error rate fluctuates in the range of 0.42% to 0.76%, when the topology of the sensor is star-type, the bit error rate obtained from this experiment is about 0.18%-0.39%, and when the sensor node's topology is mesh-type, its bit error rate is lower than 0.1%. Comparing the three sets of data, it can be seen that the sensor BER of the mesh-type structure is much smaller than the other two sensor topologies. In the signal-to-noise ratio test, the signal-to-noise ratios of the three types of sensor node topologies are all greater than 65.3 dB, with the lowest signal-to-noise ratios in the star structure of about 65.3 to 82.5 dB, the signal-to-noise ratios in the tree structure of between 81.6 and 85.7 dB, and the signal-to-noise ratios in the mesh structure of 93.4 to 96.7 dB. it can be seen from the above data that the bit error rate of all three types of sensor node topologies with the The bit error rate is less than 0.8%, and its signal-to-noise ratio is at least 65.3dB, which shows that the secure communication mechanism of the wireless sensor network designed in this paper can help to improve the security of data transmission. And when the sensor nodes choose the network structure, its communication effect is better than the other two topologies.



(a) Bit error rate



(b) SNR

Fig. 8. Performance testing of sensor node state

5. Conclusion

Based on ZigBee wireless communication technology, the article constructs a secure communication architecture system of wireless sensor network in industrial control system, and introduces the key management scheme of Merkle tree and the two-way authentication mechanism of nodes with digital signature to ensure its communication security performance. Based on the effectiveness of the secure communication mechanism to carry out verification analysis, specifically as follows:

1) The key management scheme based on Merkle tree and μTesla protocol takes a more stable time to add and revoke a key under different key number scales, with values of about 17.37 μs and 3.24 μs, which is a higher performance than the comparison method. And when the connectivity frequency is 12 min and the revocation threshold is 60, the local optimal value of user time consumption is 7.26 s. Therefore, the key management scheme for secure communication in wireless sensor networks constructed by combining the Merkle tree and the μTesla protocol can improve the efficiency of encrypted data transmission and ensure the security of industrial data transmission.

2) The node trust degree combined with digital signature algorithm is used to construct the node two-way authentication mechanism for data communication, and its mean accuracy of recognizing malicious nodes in wireless sensor networks is up to 96.17%. The bit error rate is lower than 0.1%

and the signal-to-noise ratio is between 93.4 and 96.7dB when the communication is transmitted in a mesh topology.

In conclusion, the secure communication architecture of wireless sensor network based on ZigBee technology in this paper can ensure the secure transmission of data in industrial control system, and the key management scheme and node bidirectional cognitive mechanism can help to improve the communication security performance of wireless sensor network.

References

[1] Majid, M., Habib, S., Javed, A. R., Rizwan, M., Srivastava, G., Gadekallu, T. R., & Lin, J. C. W. (2022). Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. Sensors, 22(6), 2087.

[2] Ramotsoela, D., Abu-Mahfouz, A., & Hancke, G. (2018). A survey of anomaly detection in industrial wireless sensor networks with critical water system infrastructure as a case study. Sensors, 18(8), 2491.

[3] Hu, Y., Yang, A., Li, H., Sun, Y., & Sun, L. (2018). A survey of intrusion detection on industrial control systems. International Journal of Distributed Sensor Networks, 14(8), 1550147718794615.

[4] Park, P., Ergen, S. C., Fischione, C., Lu, C., & Johansson, K. H. (2017). Wireless network design for control systems: A survey. IEEE Communications Surveys & Tutorials, 20(2), 978-1013.

[5] Lăzăroiu, G., Andronie, M., Iatagan, M., Geamănu, M., Ştefănescu, R., & Dijmărescu, I. (2022). Deep learning-assisted smart process planning, robotic wireless sensor networks, and geospatial big data management algorithms in the internet of manufacturing things. ISPRS International Journal of Geo-Information, 11(5), 277.

[6] Bhushan, B., & Sahoo, G. (2020). Requirements, protocols, and security challenges in wireless sensor networks: An industrial perspective. Handbook of computer networks and cyber security: principles and paradigms, 683-713.

[7] Kobo, H. I., Abu-Mahfouz, A. M., & Hancke, G. P. (2017). A survey on software-defined wireless sensor networks: Challenges and design requirements. IEEE access, 5, 1872-1899.

[8] Li, X., Li, D., Wan, J., Vasilakos, A. V., Lai, C. F., & Wang, S. (2017). A review of industrial wireless networks in the context of Industry 4.0. Wireless networks, 23, 23-41.

[9] Aalsalem, M. Y., Khan, W. Z., Gharibi, W., Khan, M. K., & Arshad, Q. (2018). Wireless Sensor Networks in oil and gas industry: Recent advances, taxonomy, requirements, and open challenges. Journal of network and computer applications, 113, 87-97.

[10] Raza, M., Aslam, N., Le-Minh, H., Hussain, S., Cao, Y., & Khan, N. M. (2017). A critical analysis of research potential, challenges, and future directives in industrial wireless sensor networks. IEEE Communications Surveys & Tutorials, 20(1), 39-95.

[11] Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. computers & security, 89, 101677.

[12] Aponte-Luis, J., Gómez-Galán, J. A., Gómez-Bravo, F., Sánchez-Raya, M., Alcina-Espigado, J., & Teixido-Rovira, P. M. (2018). An efficient wireless sensor network for industrial monitoring and control. Sensors, 18(1), 182.

[13] Osanaiye, O., Alfa, A. S., & Hancke, G. P. (2018). A statistical approach to detect jamming attacks in wireless sensor networks. Sensors, 18(6), 1691.

[14] Bhushan, B., & Sahoo, G. (2018). Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks. Wireless Personal Communications, 98, 2037-2077.

[15] Modieginyane, K. M., Letswamotse, B. B., Malekian, R., & Abu-Mahfouz, A. M. (2018). Software defined wireless sensor networks application opportunities for efficient network management: A survey. Computers & Electrical Engineering, 66, 274-287.

[16] Kandris, D., Nakas, C., Vomvas, D., & Koulouras, G. (2020). Applications of wireless sensor networks: an up-to-date survey. Applied system innovation, 3(1), 14.

[17] Gulati, K., Boddu, R. S. K., Kapila, D., Bangare, S. L., Chandnani, N., & Saravanan, G. (2022). A review paper on wireless sensor network techniques in Internet of Things (IoT). Materials Today: Proceedings, 51, 161-165.

[18] Ramson, S. J., & Moni, D. J. (2017, February). Applications of wireless sensor networks—A survey. In 2017 international conference on innovations in electrical, electronics, instrumentation and media technology (ICEEIMT) (pp. 325-329). IEEE.

[19] Jiang, Q., Zeadally, S., Ma, J., & He, D. (2017). Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. Ieee Access, 5, 3376-3392.

[20] Gope, P., Das, A. K., Kumar, N., & Cheng, Y. (2019). Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks. IEEE transactions on industrial informatics, 15(9), 4957-4968.

[21] Deebak, B. D., & Al-Turjman, F. (2020). A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks. Ad Hoc Networks, 97, 102022.

[22] Dua, A., Kumar, N., Das, A. K., & Susilo, W. (2017). Secure message communication protocol among vehicles in smart city. IEEE Transactions on Vehicular Technology, 67(5), 4359-4373.

[23] Kocakulak, M., & Butun, I. (2017, January). An overview of Wireless Sensor Networks towards internet of things. In 2017 IEEE 7th annual computing and communication workshop and conference (CCWC) (pp. 1-6). Ieee.

[24] Cao, B., Zhao, J., Gu, Y., Fan, S., & Yang, P. (2019). Security-aware industrial wireless sensor network deployment optimization. IEEE transactions on industrial informatics, 16(8), 5309-5316.

[25] Srinivas, J., Mukhopadhyay, S., & Mishra, D. (2017). Secure and efficient user authentication scheme for multi-gateway wireless sensor networks. Ad Hoc Networks, 54, 147-169.

[26] V Ranjith,C Yaashuwanth,K Prathibanandhi & T Jayasankar. (2024). Energy Efficient and Reliable High Quality Video Transmission Architecture for Wireless Sensor Networks. Tehnički vjesnik(3),973-981.

[27] Leilei Deng,Lifeng Sun,Yunjia Liu,Yuanbin Zhang & Xian Zhang. (2024). Study on smart grid fault detection based on ZigBee and MapX technologies. Measurement113859-.

[28] Padma Bhukya & Babu Erukala Suresh. (2023). Efficient Secure Communication in Zigbee Network Using the DNA Sequence Encryption Technique. Life (Basel, Switzerland)(5).

[29] Oleksandr Kuznetsov,Dzianis Kanonik,Alex Rusnak,Anton Yezhov,Oleksandr Domin & Kateryna Kuznetsova. (2024). Adaptive Merkle trees for enhanced blockchain scalability. Internet of Things101315-101315.

[30] Nishchal Soni. (2024). Letter to the editor: “Edwards curve digital signature algorithm for video integrity verification on blockchain framework”. Science & Justice(5),581-582.