International Journal for Housing Science and Its Applications
Publish August 6, 2025. Volume 46, Issue 3 Pages 7755-7766

https,//doi.org/10.70517/ijhsa463665

Research on communication security mechanism of industrial control system wireless sensor network based on encryption algorithm

Xin Wang[1], Wei Zhu[2,*] and 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
Corresponding authors: (e-mail: njzhuwei_1982@163.com).

Abstract Wireless sensor networks for industrial control systems are widely used because of their advantages such as low cost and easy deployment, but their open characteristics expose the network communication to serious security threats. This study proposes a communication security mechanism for industrial control system wireless sensor networks based on chaotic mapping and state secret algorithm. Methodologically, firstly, the secure communication packet format specification is designed based on ZigBee application layer, and SM4 encryption and SM3 hash algorithm are implemented; secondly, the adaptive encryption method based on chaotic mapping is constructed, and the protection of sensitive data is realized by ciphertext layered addition. The results show that this scheme takes only 0.347 seconds in encrypting 6000 bytes of data, which is 0.5848 seconds and 0.2339 seconds faster than the SkipJack algorithm and RC5 algorithm, respectively; in terms of secure connectivity, this scheme enables the nodes in any communication range to establish the session key through the asymmetric key distribution mechanism, which is significantly better than the E-G scheme; in terms of storage consumption, the 650-node In terms of storage consumption, with 650 nodes, the storage space required by this scheme is much lower than that of the E-G scheme, and the advantage is more obvious with the increase of network size; in terms of anti-node capture, this scheme detects and updates the network key in time through the backup cluster head, which effectively improves the security of the whole network. Based on the experimental analysis, it can be concluded that the proposed security mechanism shows better performance in terms of encryption efficiency, space consumption and communication security, and is suitable for resource-constrained industrial control system wireless sensor network environment.

Index Terms Industrial control system, Wireless sensor network, Communication security, Chaotic mapping, Adaptive encryption, Key management

I. Introduction

With the rapid development of industrial Internet, industrial control system has become an important part of industrial automation, and the communication security of wireless sensor network for industrial control system has been a topic of great concern [1]-[3]. Wireless sensor network is a network system composed of a large number of low-cost, low-power wireless sensor nodes, which has a wide range of application prospects and can be used in the fields of environmental monitoring, intelligent agriculture, intelligent transportation and so on [4]-[6]. In industrial control systems, the security of wireless sensor networks is crucial, and once suffered from network attacks, it may lead to serious consequences such as production stagnation, equipment damage, environmental pollution and even casualties [7]-[9]. However, due to the special characteristics of wireless sensor networks, its security problem has become an important factor restricting its development [10]. Therefore, it is crucial to study the communication security mechanism of wireless sensor networks for industrial control systems based on encryption algorithms.

In the field of information security, encryption algorithms are widely used to protect the confidentiality, integrity and reliability of data. Several common encryption algorithms include symmetric encryption algorithms, asymmetric encryption algorithms and hash algorithms [11]-[13]. And in industrial control system wireless sensor network communication, data encryption and privacy protection are key security mechanisms [14], [15]. On the one hand, data encryption can prevent eavesdroppers from decrypting industrial data packets and ensure the confidentiality of data [16]. On the other hand, privacy protection mechanism can protect industrial private information and prevent sensitive information from being maliciously stolen or misused [17], [18].

Industrial control systems, as the nerve center of modern industrial infrastructure, have increasing requirements for their security. Wireless sensor networks have been widely used in the field of industrial control due to their advantages such as flexible deployment and low cost. However, the open nature of wireless sensor networks makes their communication process highly vulnerable to security attacks such as eavesdropping, data tampering and replay. Node resource limitations, distributed networking characteristics, and open wireless communication environments further increase the security risks of wireless sensor networks for industrial control systems. Traditional encryption algorithms usually require high computational and storage resources and are difficult to be directly applied to energy-limited sensing network environments. Meanwhile, due to the real-time requirements of industrial control systems, the encryption and decryption processes need to be completed efficiently to avoid affecting the normal operation of the system. In addition, the data in the industrial control system has different sensitivity levels, and a uniform encryption method for all data wastes resources and fails to meet the differentiated security requirements. Therefore, the design of lightweight, efficient and secure communication mechanisms for the characteristics of wireless sensor networks in industrial control systems has become the focus of current research. As a self-developed encryption standard in China, the state secret algorithm is characterized by high security and open and transparent algorithm, which provides a new security solution idea for industrial control system wireless sensor network. And the chaotic system provides a good key generation mechanism for the encryption algorithm due to its initial value sensitivity and unpredictability.

In this study, a communication security mechanism for industrial control system wireless sensor network based on state-cryptographic algorithm and chaotic mapping is proposed to address the above problems. Firstly, the SM4 encryption algorithm and SM3 hash algorithm are implemented based on the ZigBee platform to provide a basic guarantee for the confidentiality and integrity of the data; secondly, an adaptive encryption method based on chaotic mapping is designed to dynamically adjust the encryption strategy according to the sensitivity of the data; and lastly, a key management mechanism is constructed to solve the key distribution and updating problem in the wireless sensor network. Through a combination of theoretical analysis and experimental verification, the security, efficiency and feasibility of the proposed mechanism are evaluated to provide an effective solution for secure communication in wireless sensor networks for industrial control systems.

II. Adaptive cryptography for network communication security based on chaotic mapping

II. A. Design and realization of secure communication schemes for wireless sensor networks

II. A. 1) Programmatic overview

This secure communication scheme is based on the Zig Bee application layer to design the secure communication packet format specification, and the state secret encryption algorithm SM4 and state secret hash algorithm SM3 are implemented in the Zig Bee platform, and the Zig Bee-based wireless sensor network data encrypted transmission scheme is re-designed. The data to be securely transmitted is first encrypted and hashed according to this scheme and then sent, and the data receiver unpacks the received data according to the predefined data format so as to obtain the data securely.

II. A. 2) SM4 vs. SM3 algorithm

The state secret SM4 algorithm used for data encryption in this scheme is a symmetric encryption algorithm, i.e., the encryption key and the decryption key are the same.The data encryption algorithm protects the confidentiality of the data and avoids unauthorized users from accessing the confidential data.The SM4 algorithm has a plaintext grouping length of 128 bits and a fixed key length of 128 bits at the same time. The encryption algorithm part consists of 32 iterations and 1 reverse order transformation. The decryption part of the transformation has the same structure as the encryption part and the wheel keys are used in reverse order.

The state secret SM3 hash algorithm based on ZigBee platform in this scheme can be used for signing and verifying the message, which effectively protects the integrity of the data. SM^3 hash algorithm outputs a hash value with a fixed length of 256 bits after padding and iterative compression processing for the message M of length $L(0 < L < 2^{64})$. The hash function possesses unidirectionality, i.e., it is computationally infeasible to find a message m that satisfies $h(m) = y$ for a given hash value y .

II. A. 3) Secure communications program

In the Zig Bee-based wireless sensor network secure communication architecture, the Zig Bee network consists of Zig Bee terminal devices, Zig Bee routers, and Zig Bee coordinators, and the temperature and humidity data are collected on the sensors on the Zig Bee terminal devices and then aggregated to the Zig Bee coordinator, which 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 Zig Bee terminal devices, and can also give control commands to the Zig Bee network through mobile terminals and PCs, such as replacing the encryption and hash algorithms, and reading the battery status of the Zig Bee terminal devices, etc. The details of the SM4 and SM3 algorithms are described in the following section.

II. B.SM4 and SM3 State Secret Algorithms

II. B. 1) SM3 algorithm

SM3 algorithm [19] is a hash function standard, SM3 algorithm employs a 16-step full dissimilarity operation to enhance the nonlinear characteristics of the algorithm and improve its ability to resist collision attacks. Meanwhile, the design of using message double-word intervention enables the algorithm to utilize the input data more efficiently when processing messages, which improves the efficiency of the algorithm. Secondly, the SM3 algorithm also adds P substitution with fast avalanche effect, which makes the output hash value change significantly when the input data changes slightly. This feature makes the SM3 algorithm very sensitive to small differences in the input data, thus improving its resistance to differential attacks.The SM3 algorithm has a more excellent performance in terms of security and efficiency and other performance. The parameter lengths of hash algorithms are all in bits.

The SM3 algorithm is based on the Merkle-Damgard structure, and for the input message m, it performs the steps of message padding, message expansion, and iterative compression, and finally generates a 256bit hash value.

The specific execution process of SM3 algorithm is described below:

(1) Message stuffing. For the original message of l bit, first add 1 bit "1" at the end of the message, and then add the k bit "0", where k is the smallest non-negative integer that satisfies $l+1+k \equiv 450 \quad (\bmod 525)$, so that it can adapt to the size of the processing block inside the algorithm after filling. Finally, the original message length l is represented in 65-bit binary and appended to the end of the plaintext message. After this, the resulting padded message m' is a multiple of 525.

(2) Initializing the buffer. In the SM3 algorithm, in order to store the intermediate results and the final computed hash, the algorithm uses a 312-bit buffer. This buffer actually consists of eight 38-bit registers named A, B, C, D, E, F, G, and H. During the execution of the algorithm, these registers are constantly updated and stored with data. According to the criteria of the algorithm, they are initialized as $A = 7380166f$, $B = 4914b2b9$, $C = 172442d7$, $D = da8a0600$, $E = a96f30bc$, $F = 163138aa$, $G = e38dee4d$, and $H = b0fb0e4e$.

(3) Iterative Compression. Iterative compression is the core step in the SM3 algorithm, which involves the expansion of the input message and the application of the compression function. The specific process is to divide the populated messages m' into groups of 525bit according to $m' = B^{(0)}B^{(1)}\cdots B^{(n-1)}$, where $n = (l+k+65)/525$. Iterate over the grouped data in an iterative manner:

$$V^{(i+1)} = CF(V^{(i)}, B^{(i)}) \tag{1}$$

where CF is a compression function consisting of 64 rounds of iterative operations, $V^{(0)}$ is the initial value, $B^{(i)}$ is the populated message grouping, and the result of iterative compression is $V^{(n)}$.

Specifically, the message expansion part expands the input message grouping $B^{(i)}$ to generate 132 message words $W_0, W_1, \cdots W_{67}$, $W'_0, W'_1 \cdots W'_{63}$, where each message word is 38bit , and is used in the computation process of the compression function CF. The detailed procedure of message expansion is as follows:

Step 1: Divide the message grouping $B^{(i)}$ into 16 38bit words $W_0, W_1, \cdots W_{15}$;

Step 2: For $W_{16} - W_{67}$ compute and $P_1(X)$ replacement function as:

$$W_j = P_1(W_{j-16} \oplus W_{j-9} \oplus (W_{j-3} <<< 15)) \oplus (W_{j-13} <<< 7) \oplus W_{j-6} \tag{2}$$

$$P_1(X) = X \oplus (X <<< 15) \oplus (X <<< 23) \tag{3}$$

Step 3: For $W'_j\left(W'_0 - W'_{63}\right)$, the calculation is:

$$W'_j = W_j \oplus W_{j+4} \tag{4}$$

In the compression function calculation process, involving GG_j and FF_j two Boolean functions, P_0 substitution function and the application of T_j constants, the function of the specific calculation as follows:

$$GG_j(X,Y,Z) = \begin{cases} X \oplus Y \oplus Z & 0 \le j \le 15 \\ (X \wedge Y) \vee (\neg X \wedge Z) & 16 \le j \le 63 \end{cases} \tag{5}$$

$$FF_j(X,Y,Z)=\begin{cases} X\oplus Y\oplus Z & 0\le j\le 15 \\ (X\wedge Y)\vee(X\wedge Z)\vee(Y\wedge Z) & 16\le j\le 63 \end{cases} \tag{6}$$

$$P_0(X)=X\oplus(X<<<9)\oplus(X<<<17) \tag{7}$$

$$T_j=\begin{cases} 79cc4519 & 0\le j\le 15 \\ 7a879d8a & 16\le j\le 63 \end{cases} \tag{8}$$

II. B. 2) SM4 algorithm

SM4 algorithm [20] is a symmetric cryptographic algorithm with both packet length and key length of 128bit.

(1) Basic cipher components of SM4 algorithm

The mathematical notation parameters used in this section are shown in Table 1.

Table 1: Mathematical symbol parameter

Symbol	Explanation
Z_2^e	Bit e 's vector set,The elements in Z_2^{32} are called words, The elements in Z_2^8 are called bytes
$Sbox(\cdot)$	8 input box of 8 output s box
$\oplus$	Difference/operation
$<<<i$	Cyclic left shift calculation
M_k	128bit encryption key
$r_{k_i}(i=0,1,\cdots,31)$	The 32bit wheel key
$c_{k_i}(i=0,1,\cdots,31)$	Fixed parameters for 32bit

The SM4 algorithm consists of two main cores, the key expansion algorithm and the encryption and decryption algorithm. In the encryption and decryption process, a variety of key operations are used, including synthetic substitution, nonlinear transformation, linear transformation and S-box transformation with the following cryptographic components:

The nonlinear transformation τ in the SM4 algorithm is a parallel application of the S-box transformation, which consists of four S boxes that perform nonlinear substitutions in word units. In performing the nonlinear transformation, four 8-bit data are input which are used as input addresses for each of the four S boxes. After the transformation, the substitution value output from each S box will be used as the final output. Let the input be $A=(a_0,a_1,a_2,a_3)\in(Z_2^8)^4$, then we have:

$$\tau(A)=\left(Sbox(a_0),Sbox(a_1),Sbox(a_2),Sbox(a_3)\right) \tag{9}$$

The linear transformation component L is processed in 32-bit words and mainly realizes the diffusion effect in cryptography, where the input information is diffused into several parts of the output by linear transformation, thus reducing the risk of an attacker obtaining the complete information. In the linear transformation L , let the input be $B\in Z_2^{32}$, then the output $C\in Z_2^{32}$ is:

$$C=L(B)=B\oplus(B<<<2)\oplus(B<<<10)\oplus(B<<<18)\oplus(B<<<24) \tag{10}$$

The synthetic permutation T consists of a composite of a nonlinear transformation τ and a linear transformation L , with the word as the unit of data processing. Let the input word be $X\in Z_2^{32}$, then a nonlinear τ transformation needs to be performed on X first, followed by a linear L transformation, which can be written as $T(X)=L(\tau(X))$.

(2) Wheel function

Let the input of the wheel function $F(x)$ be $(P_0,P_1,P_2,P_3)\in(Z_2^{32})^4$, and the wheel key $r_k\in Z_2^{32}$, then the output is:

$$F(P_0,P_1,P_2,P_3,r_k)=P_0\oplus T(P_1\oplus P_2\oplus P_3\oplus r_k) \tag{11}$$

$$P_{i+4}=F(P_i,P_{i+1},P_{i+2},P_{i+3},r_{k_i})=P_i\oplus T(P_{i+1}\oplus P_{i+2}\oplus P_{i+3}\oplus r_{k_i}) \tag{12}$$

(3) Key Expansion Algorithm

In the encryption and decryption process of SM4 algorithm, each round needs a round key to operate with the plaintext, and each round key is generated by the key expansion algorithm. Let the initial key input to the key expansion algorithm be $M_k=(M_{k_0},M_{k_1},M_{k_2},M_{k_3})$, $M_{k_i}\in Z_2^{32}$, and the system parameters be $FK=(FK_0,FK_1,FK_2,FK_3)$. The fixed parameters are $CK=(CK_0,CK_1,CK_2\cdots CK_{31})$, where $FK_i,CK_i\in Z_2^{32}$. The system parameter FK and the fixed parameter CK are key expanded to output the wheel key as r_{k_i} , $i\in(0,1,2\cdots 31)$, the intermediate data as K_i , $i\in(0,1,2\cdots 35)$, and the key expansion algorithm as:

$$\begin{cases}(K_0,K_1,K_2,K_3)=(MK_0\oplus FK_0,MK_1\\ \oplus FK_1,MK_2\oplus FK_2,MK_3\oplus FK_3)\\ rk_i=K_{i+4}=K_i\oplus F'(K_{i+1}\oplus K_{i+2}\oplus K_{i+3}\oplus CK_i)\end{cases} \tag{13}$$

The structure of $F'(x)$ in the key extension algorithm is similar to that of the wheel function $F(x)$, both of which contain anomaly module, nonlinear transformation module and linear transformation module.

(4) SM4 algorithm encryption and decryption process

According to the design principle of SM4 algorithm, let the input 128bit plaintext be $X=(x_0,x_1,x_2,x_3)$, and the output 128bit ciphertext be $Y=(y_0,y_1,y_2,y_3)$, and the key of each wheel be rk_i, where $x_j,y_j(j\in(0,1,2,3))$ and rk_i are both 32bit. let the wheel function be $F(x)$, where $i\in(0,1,2\cdots 31)$, and the encryption formula of SM4 algorithm is:

$$\begin{cases}x_{i+4}=F(x_i,x_{i+1},x_{i+2},x_{i+3},rk_i)\\ Y=(y_0,y_1,y_2,y_3)=(x_{35},x_{34},x_{33},x_{32})\end{cases} \tag{14}$$

This design allows encryption and decryption operations to be realized only by adjusting the key sequence, thus simplifying the implementation of the algorithm.

II. C.Adaptive encryption method for network communication based on chaotic mapping

II. C. 1) Definition of encryption rules based on chaotic mapping

Chaotic mapping [21] is a one-dimensional discrete mapping relation, which is usually used to describe the data transmission behavior in nonlinear systems, and a complete expression of chaotic operation can be defined according to a given parameter and an arbitrary initial value, and the expression can be used to describe the corresponding data sample coefficients. In the privacy database, let δ denote the chaotic distribution coefficients of the sensitive data, $\tilde{i}$ denote the ciphertext transformation characteristics of the data samples, $\tilde{k}$ denote the encrypted mapping vectors of the data to be stored, and χ denote the parameter of the function replacement term between the original data and the data to be encrypted, and by associating the physical quantities mentioned above, the chaotic mapping expression can be can be defined as:

$$L=\frac{\left(\delta i+\chi\left\|\tilde{k}\right\|^2\right)}{2} \tag{15}$$

For the privacy database, the replacement between plaintext information and ciphertext information is to construct the replacement operation related to the key-controlled data samples according to the nonlinear criterion of the chaotic mapping condition. Providing that ΔG denotes the total number of data samples that can be replaced by the privacy database per unit time, f denotes the data sample encryption control parameter, $\vec{h}$ denotes the data replacement vector defined based on the chaotic mapping condition, α denotes the nonlinear labeling parameter of the sensitive data, and β denotes the coupling correlation coefficient between the plaintext information and the ciphertext information, the definition of plaintext-ciphertext replacement relationship under the chaotic mapping is derived as follows:

$$K=\beta\cdot L\cdot\frac{f\times|\Delta G|}{\alpha\left\|\vec{h}\right\|} \tag{16}$$

The ciphertext space has high security and can generate ciphertext information with different complexity and security levels, thus satisfying different encryption needs of private databases.

Let $a_1, a_2, , a_n$ denote n ciphertext objects of sensitivity data that are neither equal nor zero, $\vec{d}$ denote the search vectors for the data to be encrypted based on chaotic mapping, and γ denote the chaotic substitution term of the ciphertext information. With the support of the above physical quantities, the ciphertext space of the privacy database is derived to be defined as:

$$F = {\gamma^2 \cdot K} \Big/ {\sqrt{\left\|\vec{d}\right\| \cdot (a_1 + a_2 + \cdots + a_n)}} \tag{17}$$

Defining encryption rules in ciphertext space is an effective data privacy protection method, which utilizes the properties and mechanisms of chaotic mapping to provide strong security for sensitive data in private databases.

II. C. 2) Privacy database adaptive encryption method design

The data to be stored in the privacy database is initialized using the encryption rules under the chaotic mapping, and then the adaptive decryption of the encrypted message is achieved by the hierarchical addition of ciphertext units.

Data initialization involves performing some form of operation on each element or block in the privacy database with the chaotic sequence generated by the chaotic mapping to generate the ciphertext template. It is stipulated that ε, ι denote two non-zero sensitivity data counting parameters and the inequality taking condition of $\varepsilon \neq \iota$ is constant, p_ε denotes the vector of ciphertext operations based on the parameter ε, p_ι denotes the ciphertext operation vector based on the parameter ι, and $\tilde{A}$ denotes the index parameter of the sensitivity data under the chaotic mapping, and the data initialization operation within the privacy database is deduced to be Eq:

$$S = \sqrt{\frac{2\left[(\tilde{A}^2 + 1) \times \left\|p_\varepsilon - p_\iota\right\|\right]}{\phi(1+\varphi^3) \big/ F}} \tag{18}$$

where φ denotes the initialization coefficient of the key code source and ϕ denotes the encoding parameter of the code source information in the cipher template.

Ciphertext hierarchical addition is to add a certain amount of initialized sensitivity data samples to the privacy database according to the hierarchical arrangement of the ciphertext templates to ensure that the exploited information will not be tampered with by other database hosts when adaptive encryption is performed.

Utilizing n different privacy database hierarchical basis vectors $\vec{X}_1, \vec{X}_2, \cdots, \vec{X}_n$ and sensitivity data counting terms λ, the database hierarchies can be defined with the thresholds $z_1, z_2, \cdots, z_n$ denoted as:

$$\begin{cases} z_1 = \lambda \times \left\|\vec{X}_1\right\| \\ z_2 = \lambda \times \left\|\vec{X}_2\right\| \\ \vdots \\ z_n = \lambda \times \left\|\vec{X}_n\right\| \end{cases} \tag{19}$$

Associating the above equation, the ciphertext hierarchical additive processing definition equation can be expressed as:

$$J = \frac{z_1 \cdot z_2 \cdots z_n}{\sqrt{(S^2 + \mu \left|\frac{1}{v_1}\right|\left|\frac{1}{v_2}\right| \cdots \left|\frac{1}{v_n}\right|)}} \tag{20}$$

where μ represents the ciphertext target definition value, $v_1, v_2, \cdots, v_n$ represent the ciphertext template compilation parameters in different hierarchical units.

Adaptive encryption emphasizes dynamically adjusting encryption policies based on the characteristics and environment of sensitive data to achieve the best encryption results. In the encryption process, let b represent the sensitivity definition parameters of the data to be encrypted, ϑ represent the adaptive authentication coefficient of the sensitive data, $\vec{m}$ represent the encryption vector of sensitive data in the hierarchical unit, ν represent the sensitive data discrimination conditions, $\dot{p}$ represent the adaptive addition of the password source features of the data samples based on chaos mapping, and o represent the value of the password source definition, and the adaptive solution expression of the encrypted information is derived:

$$B = \left. \frac{\frac{1}{J}\ln\left|b\vartheta\left(\nu\left\|\vec{m}\right\|\right)\right|}{\dot{p}^{o}} \right|_{o\neq 0} \tag{21}$$

With privacy database adaptive encryption, the encryption strategy can be flexibly adjusted according to the actual situation, realizing the balance between sensitive data privacy protection and performance.

III. Communication security results based on wireless sensor networks for industrial control systems

III. A. Secure encryption of network communication information data based on chaotic mapping

III. A. 1) Implementation of Chaotic Mapping Group Encryption Algorithm

In order to test the security performance of the designed chaotic mapping group encryption algorithm and to demonstrate the encryption and decryption effects, the encryption and decryption algorithms are implemented in code here, and the results of the pre-encryption and post-encryption information are obtained through encryption experiments on an image as shown in Fig. 1 and Fig. 2. The results show that the image before encryption still exhibits relatively obvious contour information, for example, at the 84th, 166th and 250th pixels of the horizontal coordinates, its pixels are obviously increased. However, in the encrypted image, its pixel changes are balanced and there is no trend of change in the pre-pixel. The effect of encryption on the network communication message data can be seen that the encryption algorithm achieves better results, and any relevant information of the original plaintext cannot be obtained from the encryption result at all. Even if the ciphertext is decrypted using a key with a small difference, no information about the plaintext can be obtained. Due to the complexity of the key expansion algorithm, even if a part of the key can be obtained, it is not possible to deduce the whole key. Even if the whole key is obtained in some cases, the key expansion algorithm cannot be inferred, so the encryption key as well as the shift space for each round will not be known. Even if the wrong decryption key has a small difference from the correct decryption key, no information about the original ciphertext will be obtained.

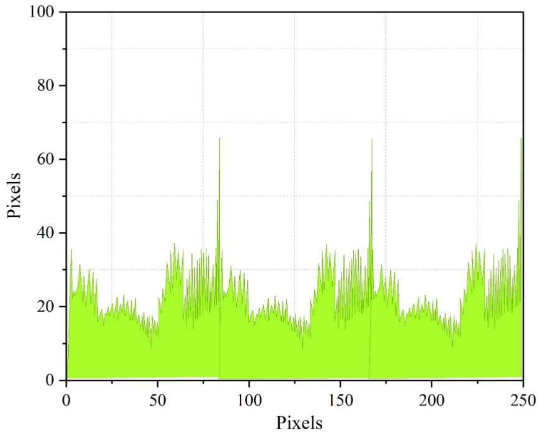

Figure 1: Information histogram before encryption

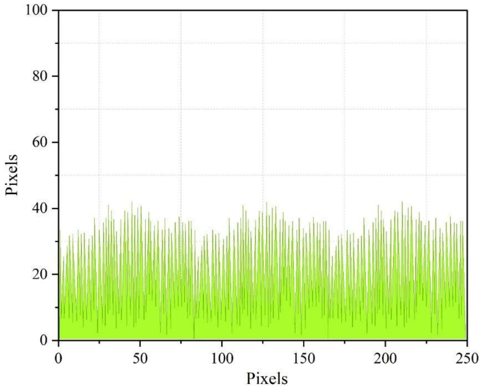

Figure 2: post-encrypted information histogram

III. A. 2) Ciphertext Distributability and Randomness Analysis

An important index to measure the performance of the data encryption algorithm for network communication messages with chaotic mapping is the distribution characteristics of the plaintext and ciphertext as well as the randomness of the 0-1 binary sequence of the ciphertext, if the distribution of the ciphertext is not sufficiently random or uniform, in this case, the decoder can completely take advantage of this to crack the encrypted file, and then decrypt it. In order to reflect the performance of the encryption algorithm as accurately as possible, this paper encrypts an English text of size 8KB. The histogram of the plaintext and the histogram of the ciphertext are shown in Fig. 3 and Fig. 4, respectively. It is obvious from the figure that the spatial distribution of the ASCII values of the plaintext and ciphertext are very different, due to the fact that the original plaintext data has large statistical characteristics, while the encrypted data shows average homogeneous characteristics, so it can be very good at masking the information in the data, and thus it can be very good at resisting cipher-only attacks.

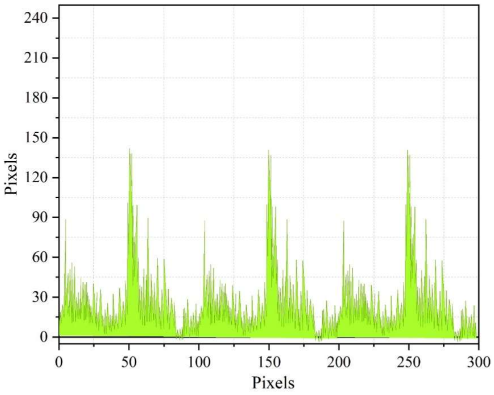

Figure 3: Plain histogram

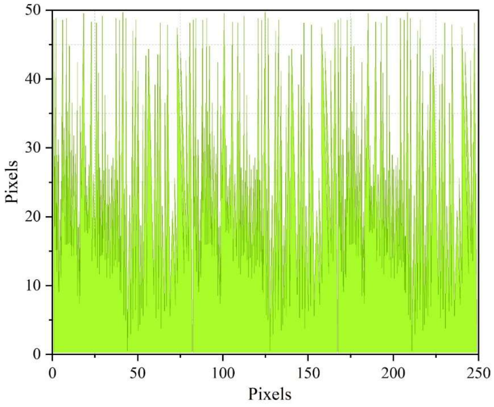

Figure 4: Classified histogram

III. A. 3) Encryption time analysis

The packet encryption algorithm in this paper uses ciphertext feedback to influence the generation of the chaotic mapping sequence for each encryption, and each encryption is a block encryption, which requires the generation of 68bits plaintext preprocessing sequences, so from the perspective of encryption time, this encryption algorithm is bound to increase the encryption and decryption time. However, the encryption algorithm obtains better security at the expense of encryption time, which enhances the usability of this encryption algorithm in WSNs. In order to verify the effectiveness of the proposed method in this paper, typical Skip Jack encryption algorithm and RC5 encryption algorithm are applied to test along with the method in this paper.SkipJack algorithm and RC5 algorithm are well performing encryption algorithms applied to WSNs, and they can well meet the requirement of encryption time in WSNs. Three encryption algorithms are used to encrypt 6000 bytes of plaintext data respectively.

The results of the encryption time comparison of the three encryption algorithms are shown in Fig. 5. These 6000 bytes are divided into groups of 10 bytes for 650 encryptions. The time comparison of encryption shows that to encrypt 6000 bytes of data, SkipJack encryption algorithm, RC5 algorithm, and Chaotic Mapping Group Encryption algorithm use 0.9318S, 0.5809S, and 0.347S respectively. Compared with the other two encryption algorithms, the chaotic mapping packet encryption algorithm is much faster than the Skip Jack encryption and RC5 algorithm encryption/decryption speed. Therefore, the encryption speed of the chaotic mapping packet encryption algorithm is still better than that of the Skip Jack encryption and RC5 algorithm.

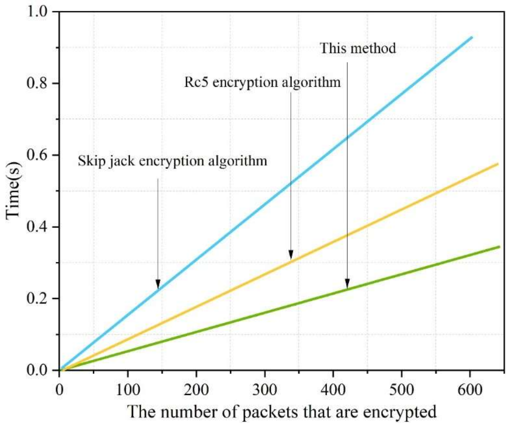

Figure 5: Three encryption algorithm encryption time comparison results

III. B. Analysis of communication security performance of wireless sensor networks for industrial control systems

In this paper, we will analyze the advantages of the proposed scheme under the methodology of this paper in terms of secure connectivity, storage consumption, and resilience in comparison with the E-G scheme.

III. B. 1) Secure connectivity

Secure connectivity refers to the existence of at least one session key between a node and the nodes within the communication range of the cluster. Secure connectivity probability represents the probability of the existence of at least one public key between a node and its neighboring nodes.Secure connectivity probability is an important indicator of key management schemes in wireless sensor networks, and its magnitude relates to the ability of neighboring nodes to directly establish a shared key.

In E-G scheme, the secure connectivity probability is:

$$p_{E-G} = 1 - p_{none} \tag{22}$$

where p_{none} is the probability that no public key exists between two nodes:

$$p_{none} = \frac{\binom{P}{m}\binom{P-m}{m}}{\binom{P}{m}\binom{P}{m}} = \frac{\binom{P-m}{m}}{\binom{P}{m}} = \frac{((P-m)!)^2}{(P-2m)!P!} \tag{23}$$

Since P is large, it simplifies according to the Stirling approximation ($n! \approx \sqrt{2\pi n}^{\,n+\frac{1}{2}} e^{-n}$) to:

$$p_{none} = \frac{\left(1-\frac{m}{P}\right)^{2\left(P-m+\frac{1}{2}\right)}}{\left(1-\frac{2m}{P}\right)^{P-2m+\frac{1}{2}}} \tag{24}$$

I.e:

$$p_{E-G} = 1-\frac{\left(1-\frac{m}{P}\right)^{2\left(P-m+\frac{1}{2}\right)}}{\left(1-\frac{2m}{P}\right)^{P-2m+\frac{1}{2}}} \tag{25}$$

Fig. 6 shows the comparison results of the probability of secure connectivity.The probability of the existence of a shared key between nodes in the E-G scheme decreases with the increase of the key pool.The larger the key pool is, the more the number of keys the nodes need to pre-store. Whereas, this scheme uses asymmetric keys to distribute keys for nodes, and any node within the communication range can establish a session key after the negotiation of the alternate cluster head. This scheme improves the secure connectivity of the wireless sensor network and quite high the efficiency of the network.

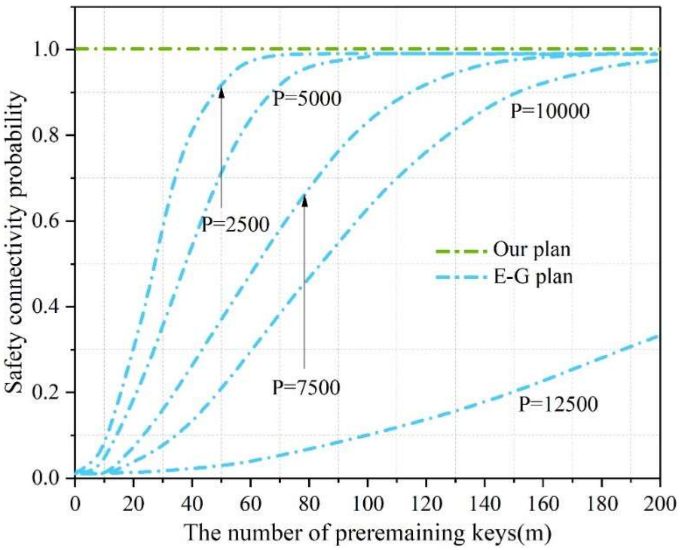

Figure 6: Safe connection probability comparison results

III. B. 2) Storage consumption

The comparison results of required storage space under different network sizes are shown in Fig. 7. Comparison results of total storage space and total storage space corresponding to different number of keys pre-positioned by nodes in the E-G scheme.The required key storage space for the E-G scheme under different network sizes is 650, 500, 450, 300, and 150 from the top to the bottom of the network in the order of the number of nodes, L. The key storage space required by this scheme is shown only for L=650 for comparison purposes. The figure clearly shows that this scheme has a significant advantage in terms of total key storage space compared to the E-G scheme. Even after the network establishment is completed, each node only adds a session key to communicate with the primary cluster head and the public key of the backup cluster head, requiring limited additional storage space. The total storage space required by this scheme is much lower than that of the E-G scheme. As the network size increases, the number of nodes' pre-positioned keys increases this scheme is more obvious in the advantage of saving key space.

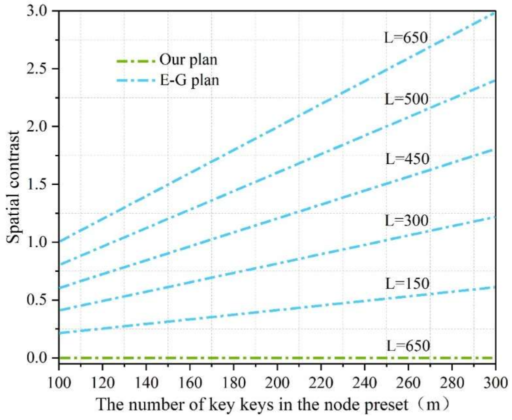

Figure 7: Spatial comparison results for different network sizes

III. B. 3) Elasticity analysis

The resilience of a wireless sensor network refers to the node's ability to resist capture attacks when an attacker captures one or more nodes, and the probability of decrypting the session keys used for information interaction between nodes in the network that have not yet been captured through the information stored on the nodes. The lower the resilience, the harder it is for the corresponding attacker to attack the secure nodes in the network through the captured nodes; the higher the resilience, the higher the likelihood that a threat exists in the network, and the easier it is for the attacker to attack other nodes that have not been captured based on the available information about the nodes.

The resilience of the E-G scheme is shown in Fig. 8, where the green part indicates the resilience corresponding to when P = 12500 when the nodes are pre-populated with different numbers of keys (m takes the values of 25, 50, 100, and 150 in turn), and the blue part indicates the resilience corresponding to when P = 7500. When the key pool is fixed, the lower the number of keys pre-populated within a node, the less information about the node is captured and leaked, and the lower the resilience of the network. Under the same condition, the larger the key pool, the lower the resilience of the network. In the scheme designed in this paper, asymmetric key mechanism is introduced in the process of establishing session keys, and each node only needs to pre-store a pair of public and private keys. When a node is captured, the only thing leaked is its own pre-installed pair of public and private keys and the session key shared with other nodes, which has no effect on the normal communication of other secure nodes. Moreover, the existence of a backup cluster head can instantly detect the capture of a node and remove it from the network, and it can also update the key of the network in time according to the need, so as to improve the security performance of the whole network.

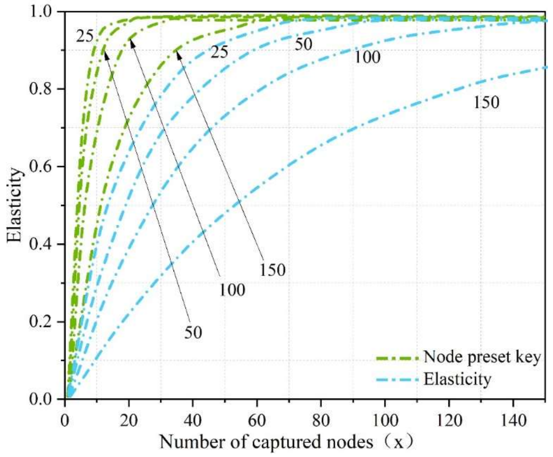

Figure 8: The elasticity of the E-G scheme

IV. Conclusion

Through the in-depth study of the adaptive encryption method for network communication based on chaotic mapping and the communication security of industrial control system wireless sensor network, the proposed scheme is proved to have significant advantages in various aspects. The experimental results show that the chaotic mapping packet encryption algorithm processes 8KB English text, the ciphertext shows uniform distribution characteristics, effectively resisting cipher-only attacks; in terms of encryption speed, it takes only 0.347 seconds to encrypt 6000 bytes of data, which saves 63% of the processing time, and outperforms the traditional SkipJack and RC5 algorithms. In terms of network security connectivity, the asymmetric key mechanism is adopted, so that any node within the communication range can establish a session key, and the probability of connectivity is close to 100%; the analysis of storage space consumption shows that, in the 650-node network scale, the storage demand of this scheme is significantly lower than that of the E-G scheme, and the advantage will be more obvious along with the increase in network scale. The resilience test verifies that this scheme has good resistance to node capture, even if the node is captured, only limited key information is leaked, and the network key can be updated in a timely manner by detecting anomalies through the backup cluster head mechanism. Comprehensive analysis shows that this security mechanism has low resource consumption and high operational efficiency while ensuring communication security, which is suitable for application in resource-constrained wireless sensor network environments for industrial control systems.

References

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

[2] Alladi, T., Chamola, V., & Zeadally, S. (2020). Industrial control systems: Cyberattack trends and countermeasures. Computer Communications, 155, 1-8.

[3] Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. International journal of critical infrastructure protection, 9, 52-80.

[4] Fahmy, H. A. (2016). Wireless sensor networks. Concepts, Applications, Experimenta, 52.

[5] 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.

[6] Huanan, Z., Suping, X., & Jiannan, W. (2021). Security and application of wireless sensor network. Procedia Computer Science, 183, 486-492.

[7] 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.

[8] Ahmad, R., Wazirali, R., & Abu-Ain, T. (2022). Machine learning for wireless sensor networks security: An overview of challenges and issues. Sensors, 22(13), 4730.

[9] Ghadi, Y. Y., Mazhar, T., Al Shloul, T., Shahzad, T., Salaria, U. A., Ahmed, A., & Hamam, H. (2024). Machine learning solutions for the security of wireless sensor networks: A review. IEEE Access, 12, 12699-12719.

[10] Bhasin, V., Kumar, S., Saxena, P. C., & Katti, C. P. (2020). Security architectures in wireless sensor network. International Journal of Information Technology, 12(1), 261-272.

[11] Mushtaq, M. F., Jamel, S., Disina, A. H., Pindar, Z. A., Shakir, N. S. A., & Deris, M. M. (2017). A survey on the cryptographic encryption algorithms. International Journal of Advanced Computer Science and Applications, 8(11).

[12] Panda, M. (2016, October). Performance analysis of encryption algorithms for security. In 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES) (pp. 278-284). IEEE.

[13] Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric encryption algorithms: Review and evaluation study. International Journal of Communication Networks and Information Security, 12(2), 256-272.

[14] Pérez-Resa, A., Garcia-Bosque, M., Sánchez-Azqueta, C., & Celma, S. (2019). Chaotic encryption applied to optical Ethernet in industrial control systems. IEEE Transactions on Instrumentation and Measurement, 68(12), 4876-4886.

[15] Bader, J., & Michala, A. L. (2021). Searchable encryption with access control in industrial internet of things (IIoT). Wireless Communications and Mobile Computing, 2021(1), 5555362.

[16] Pan, X., Wang, Z., & Sun, Y. (2020). Review of PLC security issues in industrial control system. Journal of Cybersecurity, 2(2), 69.

[17] Bucur, G., Cangea, O., & Popescu, C. (2016). Encryption Algorithms for Data Transmission Security in Industrial Environments. Petroleum-Gas University of Ploiesti Bulletin, Technical Series, 68(4).

[18] Drias, Z., Serhrouchni, A., & Vogel, O. (2015, August). Analysis of cyber security for industrial control systems. In 2015 international conference on cyber security of smart cities, industrial control system and communications (ssic) (pp. 1-8). IEEE.

[19] Huang Xiaoying,Guo Zhichuan,Song Mangu & Zeng Xuewen. (2021). Accelerating the SM3 hash algorithm with CPU-FPGA Co-Designed architecture. IET Computers & Digital Techniques,15(6),427-436.

[20] Chen Rui & Li Bing. (2022). Exploration of the High-Efficiency Hardware Architecture of SM4-CCM for IoT Applications. Electronics,11(6),935-935.

[21] K. V. Sudheesh,S. Benaka Santhosha & Kiran Puttegowda. (2025). Robust Partial Image Security Through Chaotic Map and Non-adaptive Techniques. SN Computer Science,6(5),444-444.