The Application of National Security Algorithm in Wireless Networks for Industrial Automation Process Automation (WIA-PA) Network Data Security Transmission

Ganghua Bai

School of Economics and Management, Hebi Polytechnic, Hebi 458030, China
E-mail: liwanghui1114@126.com

Received 18 April 2024; Accepted 10 October 2024

Abstract

Industrial wireless communication technology is the key to promoting the development of factory intelligence and automation. However, wireless network data security has hindered the development of industrial intelligence. Therefore, to solve the security issues of industrial wireless networks, a network data secure transmission technology based on the national security algorithm is proposed based on industrial wireless network standard protocols. Firstly, to address the vulnerability of network node identity authentication to attacks, the national security algorithm is used to construct a node authentication model. Secondly, a data security transmission model is constructed based on the improved national security algorithm, which can securely transmit industrial wireless networks by encrypting network application layer data. In network node identity authentication, when the step size was 50, the identity authentication average accuracy of the research mode reached over 98.95%, which was better than other models. When the step size was 50, the average accuracy of identity authentication in the research model

Journal of Cyber Security and Mobility, Vol. 13_6, 1401–1424.
doi: 10.13052/jcsm2245-1439.1368

was over 98.95%, showing the best performance among similar models. In the attack test of illegal client C, when the interaction history data was within 500, the node identity authentication was higher than 99.56%. However, when the interaction history data exceeded 500, the overall performance of the research model was still the best. In the comparison of node code storage and content usage overhead, when the code quantity was 15000, the storage overhead of the research model was 87356 bytes, with more node code storage and lower memory usage. The overall performance of the research model is better. From this, the research method performs the best in both identity recognition accuracy and security in network data security. The research content will provide technical support for the security management and data transmission of industrial wireless technology.

Keywords: National security algorithm, hash encryption algorithm, identity authentication, WIA-PA, data security.

1 Introduction

Industrial wireless technology plays an important role in modern industrial automation, but it still faces many communication security issues. Industrial wireless networks require a large number of communication devices during deployment. The transmission and interaction of data information are highly susceptible to external interference [1]. In addition, special architectural features also mean that the integrity and security of information are difficult to effectively ensure [2]. Ensuring the effectiveness and security of communication data and avoiding sensitive data from being violated is currently a challenge in the application of industrial wireless technology. At present, China has developed a Wireless Networks for Industrial Automation Process Automation (WIA-PA). The WIA-PA network standard technology has low power consumption, high stability, and security, reaching the advanced level around the world. However, the WIA-PA network still faces network communication data security issues during use. Especially in cutting-edge manufacturing processes, if WIA-PA network communication data is hacked or tampered with, it will affect the safe operation of the entire factory. However, based on China's independently controllable WIA-PA network standard technology, there are still data security issues, such as external and internal malicious node attacks, and sending false information to the network. At present, common security technologies include encryption algorithms and key management, such as international block cipher algorithm, hash encryption algorithm, etc. However, these technologies still face difficulties in large-scale data transmission and identity access recognition, making data vulnerable to theft [3]. Therefore, to ensure the security of WIA-PA network data, a WIA-PA network data secure transmission technology based on the national security algorithm is proposed. The study uses Hash-based Message Authentication Code-SM3 (HMAC-SM3) and Information Security Technology-SM4 Block Cipher Algorithm (SM4) to rigorously encrypt communication node authentication. At the same time, an improved SM4 algorithm is used to encrypt end-to-end application layer data. There are two innovations. Firstly, it analyzes the node identity authentication end and adopts multiple key encryption to ensure the communication security at the network node end. Secondly, considering the security of data transmission at the application layer, authentication and encryption are performed at the application layer to ensure the integrity and validity of information. The research technology will provide important technical references for the deployment and information management of enterprises in industrial automation, thereby promoting the development of traditional industry towards intelligent manufacturing industries. (1) Therefore, in order to address the security issues of industrial wireless network data, this study proposes a network data security transmission technology that combines national encryption algorithms to meet the data security requirements of China's industrial wireless networks. (2) Secondly, the study aims to reconstruct the identity authentication model by combining national encryption algorithms and hash encryption algorithms to ensure the security of data transmission. (3) Finally, in order to address end-to-end data security issues, application layer data encryption is constructed to further improve the security and stability of data transmission, ensuring industrial network security.

2 Related Works

In modern industrial manufacturing, efficient and secure wireless communication technology is crucial for industrial development. Domestic and foreign scholars have conducted extensive research on the application of industrial WIA-PA wireless technology. Ji Z et al. designed a visualization management software for the WIA-PA network to improve its reliability. Firstly, the design requirements and functions of visual management software were analyzed. Then, the software was designed using the decoupled network topology layout algorithm. In addition, the heuristic algorithm was introduced to improve the tension exclusion model and enhance the network topology layout effect.

Experimental analysis was conducted on the research technology, which showed excellent performance in 100 devices [4]. Ademaj F et al. proposed a routing protocol technique to improve the latency of WIA-PA networks. The power consumption between wireless sensor and actuator nodes was analyzed, while minimizing end-to-end latency to achieve reliability. In addition, the study introduced a time-division multiple access scheme that improved energy efficiency by avoiding conflicts and reduces network latency and data round-trip time. Finally, the technology was applied to specific scenarios, which had good application effects [5]. Perwej Y et al. focused on the privacy and security of industrial WIA-PA networks. To improve the effectiveness of network data transmission and ensure the healthy development of the medical industry, the security of medical network data was explored. Data transmission security was systematically analyzed, taking into account the development needs and challenges of the medical industry. Related research was conducted to address the secure data transmission in communication networks [6].

In addition, with the increasingly serious communication security issues in recent years, strengthening communication data security is crucial. The national security algorithm has important application value in the field of communication data security. Jiang Y et al. conducted research on network data security. The communication data security issue has become increasingly severe. To solve the security issues of communication data transmission, a data privacy protection technology was proposed, which used the national security algorithm to authenticate and encrypt large data files. Then, the national security algorithm symmetric cryptography was used to encrypt genomic data. The experiment showed that this technology had good data privacy protection performance and met the requirements of data encryption [7]. In addition, Shao T et al. analyzed the side channel security of block cipher algorithms. To ensure the security of communication channels, a novel group symmetric encryption technology was proposed. This technology successfully reduced the algebraic order of the decomposed S-box from 7 to 2 by performing two tower field decompositions in a group symmetric cipher box, thereby improving the resistance of the scheme [8]. Xiangliang M A et al. used models such as recursive neural networks and multi-layer perceptrons to recover block cipher software and hardware information keys to improve the security of network transmission data. In addition, multiple algorithms were combined to recover the correct key of SM4 software. Through specific experimental testing, this technology had good data processing capabilities and application effects, which was also suitable for attack scenarios implemented through key encryption [9]. Finally, according to Wang R et al.'s research on communication data encryption technology, the conflict-based attack performed better in white box SM4 implementation than previously published attacks, while reducing known time complexity. This technology improved the practical application effect of white box cryptography and data encryption technology [10]. Larijani et al. conducted research on various intrusion techniques and combined them with improved teaching and learning optimization algorithms, improved JAYA algorithms, and support vector machines. Finally, the improved JAYA algorithm was used to optimize the parameters of the support vector machine. The improved method showed excellent performance compared with similar techniques and provided support for data security [11]. Abolfathi M et al. conducted research on current network privacy technologies in order to improve data security. A fingerprint total model for super learners based on machine learning and adversarial thinking principles was proposed in the research, which used multiple classification models for recognition and analysis to ensure data security. The results showed that this technology had good anti-attack capabilities, which was more accurate than similar technologies [12]. Dezfuli S M K P et al. conducted research on data information security in the context of assassination to analyze the characteristics of international control organizations. The normative transformation of concepts such as national sovereignty and exclusivity standards in international relations was indexed, thereby providing technical support for information security and military operations [13].

In summary, in recent years, industrial wireless communication technology has been widely applied and developed. The data security of industrial wireless communication technology has received widespread attention. Ensuring the effectiveness and security of communication data is crucial. Therefore, the above research has conducted in-depth research on privacy protection of network data and related encryption technologies. However, there is currently limited research on data security for industrial WIA-PA wireless technology. Therefore, the security of WIA-PA data transmission is analyzed. Based on advanced national security algorithms, secure industrial communication data transmission is achieved, providing important technical support for industrial intelligent manufacturing and communication data security.

The study consists of four chapters. The first section discusses the latest security technologies and data transmission technologies related to industrial networks. The second section analyzes and models industrial network data security technology based on national security algorithms. The third section verifies and analyzes the proposed technology, and compares its effectiveness with similar technologies. The last section summarizes and analyzes the entire technology.

3 Construction of Network Data Security Encryption Model Based on National Security Algorithm

This section analyzes the security transmission issues of WIA-PA network data. A node authentication model is constructed to address the node access security. At the same time, a data security transmission model is constructed to address the security of application layer data transmission.

3.1 Construction of Node Authentication Model Based on WIA-PA Network

In recent years, the transformation of information and communication technology has accelerated the development of traditional industrial manufacturing towards automation and intelligence. Among them, industrial wireless technology is the key to industrial intelligence construction, which needs to ensure that the network has efficient bandwidth and transmission stability, while meeting network security requirements. Therefore, based on industrial WIA-PA network security, a WIA-PA network data security transmission model is constructed to ensure the security of industrial wireless networks. The WIA-PA network model is shown in Figure 1.

According to Figure 1, the industrial WIA-PA network mainly includes handheld devices, network routers, gateways, field devices, and other devices. Among them, the research uses handheld devices to obtain node long addresses, and uses field devices to detect or collect relevant network data. The network router is responsible for finding a suitable path for the message to be “routed”, that is, forwarded to the appropriate direction. The gateway is responsible for data transmission and conversion, completing the industrial network data transmission. As an industrial open network, WIA-PA can be exploited by hackers to tamper with data and instructions without authorization, causing serious impacts on network security. Starting from network node identity authentication, a WIA-PA network node authentication model is constructed based on the national security algorithm HMAC-SM3 and SM4 to ensure the security of network node access. Compared with commonly used international block cipher algorithms, the research algorithm adopts rigorous

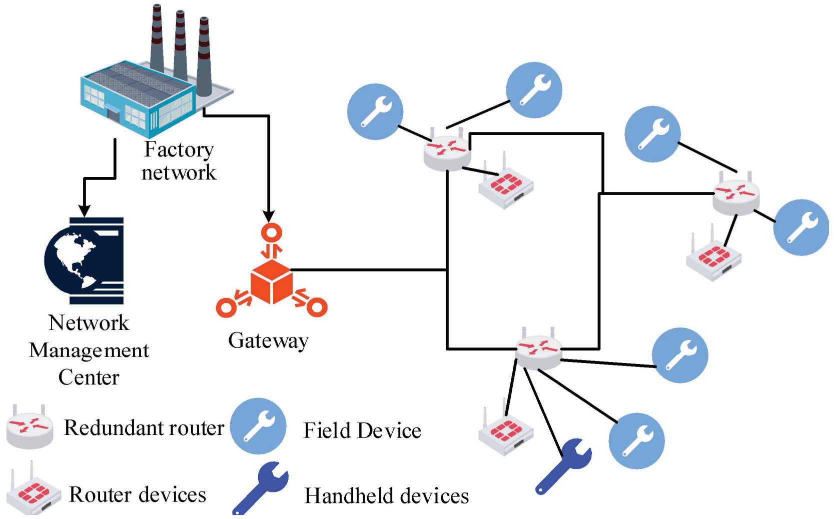


Figure 1 WIA-PA network structure diagram.

cryptographic principles and complex computational methods. It can resist various traditional and modern cryptographic attack methods and has higher security. At the same time, it is developed based on specific scenarios in China and has stronger adaptability. The entire network node authentication model construction process is shown in Figure 2.

Figure 2 shows the authentication process of security algorithms and hash encryption algorithms. Firstly, a handheld device is used to generate the key, followed by the SM4 encryption to generate the challenge frame. Next, the study uses HMAC-SM3 and hash encryption to calculate message codes for nodes, etc., and completes the identity authentication process through time and key. In the specific execution, system initialization needs to be completed in the offline state of the gateway first. In order to ensure that the offline initialization is attacked, this study uses a shared initial key between both parties to ensure data security. At the same time, even if the gateway is offline, it should be ensured that the communication between the handheld device and the gateway is encrypted. Finally, The integrity of critical data is verified mainly through national encryption algorithms to ensure offline security. After the WIA-PA network handheld device is connected to the network, the identity identification of all nodes is divided through the gateway. The set of node identity identifiers is shown in Equation (1).

$$N_{Node} = \{Node_1, Node_2, Node_3, \ldots, Node_i\} \quad 1 \leq i \leq n \tag{1}$$

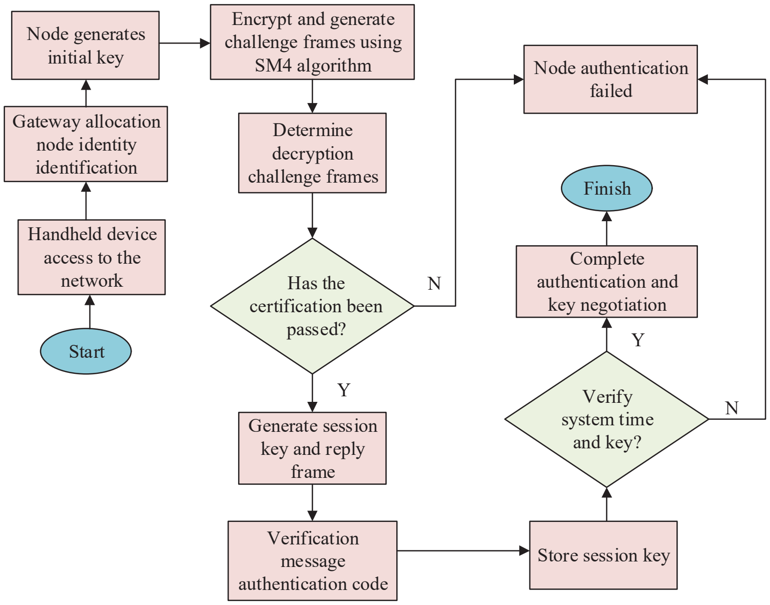

Node generates initial key
Encrypt and generate challenge frames using SM4 algorithm
Node authentication failed
Gateway allocation node identity identification
Determine decryption challenge frames
Finish
Handheld device access to the network
Has the certification been passed?
N
Complete authentication and key negotiation
Start
Y
Y
Verify system time and key?
N
Generate session key and reply frame
Verification message authentication code
Store session key

Figure 2 Network node authentication model flowchart.

In Equation (1), $Node_i$ identifies the identity of the i-th node. n identifies the deployment volume of nodes. Before the node enters the network, a handheld device is used to obtain the 64-bit node long address for WIA-PA networks. An initial key KJ_i shared by both parties is created at the node. The KJ_i information is written to the network node under the handheld device. Then, an isolation strategy is used to deploy the gateway and nodes, thereby preventing hackers from stealing $Node_i$ information and initial key KJ_i from the WIA-PA node and gateway. The above operation initializes the system [14]. In the authentication process of WIA-PA network nodes, the node obtains a random number R_i through a random generator. In the authentication process of WIA-PA network nodes, nodes obtain random numbers through a random generator. The main function of the random generator is to ensure the uniqueness of identity data in node identity recognition. It randomly generates unique identity recognition information for each node. The random generator is generated by the network system random generator module. The national security algorithm SM4 is used to encrypt the random number R_i and $Node_i$ identification and obtain a challenge frame, as shown in Equation (2).

$$C_i = SM4_{KJ_i}(Node_i||R_i) \tag{2}$$

In Equation (2), C_i represents the challenge frame. Next, the national security algorithm HMAC-SM3 calculates the message code for the random number R_i, $Node_i$ identifier, and system timestamp T_1, as shown in Equation (3).

$$TAG = HMAC - SM3_{KJ_i}(Node_i \| R_i \| T_1) \tag{3}$$

In the calculation of message codes, the HMAC-SM3 algorithm also uses the initial key KJ_i. Based on this, the identity request message is obtained, as shown in Equation (4).

$$Q_{TAG} = C_i \| TAG \| T_1 \tag{4}$$

The calculated Q_{TAG} is sent to the system gateway. When the system receives the identity authentication message Q_{TAG} transmitted by the WIA-PA node, the current state time T_G is obtained and verified, as shown in Equation (5).

$$|T_G - T_1| \leq \Delta T \tag{5}$$

In Equation (5), ΔT represents the maximum data transmission delay of the current system. If the verification does not meet the system requirements, it indicates that the node identity authentication has failed. If the verification is successful, the gateway will decrypt the challenge frame C_i and obtain the system node security information. Whether the $Node_i$ information in the node is reasonable is determined. If the verification is reasonable, the corresponding security parameters are stored, as shown in Equation (6).

$$N_i = R_i' \tag{6}$$

In Equation (6), N_i represents the safety parameter of authentication R_i. Next, the national security algorithm SM3 is used to calculate the summary value, as shown in Equation (7).

$$TAG' = HMAC - SM3_{KJ_i}(Node_i \| R_i' \| T_1) \tag{7}$$

When the requirement $TAG' = TAG$ is met, it indicates that the node has passed security authentication. Otherwise, the network authentication request for the node fails. After confirming the information of the WIA-PA network nodes, the system gateway randomly generates a random number r_i again. The random number r_i at this moment is stored by the system as a security parameter n_i. Next, parameters n_i and N_i are used as keys to obtain the input summary value $HMAC - SM3_{KJ_i}(N_i \,\|\, n_i)$ of HMAC-SM3. The last 16 bytes of the summary value are selected as the data transmission key Ks. SM4 is used to obtain the response frame, as shown in Equation (8) [15].

$$E = SM4_{K\ Ji}(R_i' \| K_s \| r_i) \tag{8}$$

According to Equation (8), the new random number R_i', random number r_i, and key K_s are obtained. The HMAC-SM3 is used again to obtain the message authentication code, as shown in Equation (9).

$$MAC = HMAC - SM3_{KJ_i}(R_i' \| K_s \| r_i) \tag{9}$$

After obtaining the message authentication code, the key generates a response message and transmits the information to the node. After obtaining the authentication, the current time T_g of the system is obtained. Based on the response message information, weather the verification message authentication code MAC is consistent with the message authentication code MAC' generated by the HMAC-SM3 is verified. If it is the same, the response message passes the verification. After the response message is passed, the node randomly generates a new random number r_i' through the key T_2. The confirmation message is obtained through SM4 encryption, as shown in Equation (10).

$$Ack = SM4_{K_S}(r_i') \tag{10}$$

The received confirmation message is transmitted to the gateway and a new system current time T_2 is obtained. When $|T_2 - T_g| \leq \Delta T$ satisfies, it indicates successful key verification. When $r_i' = r_i$ satisfies, the entire WIA-PA network completes node security authentication. Based on the above method, the identity authentication is set up between the WIA-PA node and the gateway. When the key between the two is authenticated, the WIA-PA node can prove its Internet security.

3.2 Data Security Transmission Model Based on SM4-CRT

In WIA-PA network security management, Internet identity authentication is established between network nodes and gateways. In addition, secure encryption is applied at both the sending and receiving ends of the data to ensure the integrity and security of the application layer data in the WIA-PA network [16]. In this regard, the next research focuses on the application layer data encryption of WIA-PA networks, which utilizes gateways and nodes to obtain shared keys, and uses algorithms such as SM4 to achieve end-to-end data security authentication. Among them, the WIA-PA application layer security package format and control field format are shown in Table 1.

Table 1 Application layer security package format and control field format

Data Link Security Header	Parameter	Application Control Package Field Format	Parameter
Package control	1 byte	Position: 0–1	Package type
Serial number	1 byte	Position: 2	Security
Package length	1 byte	Position: 3	Confirm
Data link payload	Parameter	Position: 4–5	Transmission mode
Safety control	1 byte	Position: 6–7	Hold
Load	Variable length	–	–
Application layer authentication code Ministry of Internal affairs and Communications (MIC)	0/4 bytes	–	–

According to Table 1, the session layer key Ks and the application layer payload together form the authentication code MIC. According to the control field, setting the field to 1 results in a secure operation. Different control fields implement different security measures to ensure data transmission security. Based on the shared key Ks obtained through bidirectional authentication between the gateway and nodes, the sender constructs a security header according to the system security mechanism. The SM4 algorithm encryption process and the Cipher Block Chaining-Message Authentication Code (CBC-MAC) achieves secure communication data processing, ensuring data integrity and security while reducing node consumption [17]. In data integrity analysis, the first step is to construct an application layer authentication data string $B_0\|B_1\|\cdots\|B_t$. Then, it is used as an input value for the SM4 encryption process.

Firstly, the identification byte $Flag$ of the authentication data block B_0 is constructed, which includes the Reserved byte of 0. In the research, the application layer serves as an additional part of the authentication data. The additional field Adata is set to 1 [18]. Meanwhile, for the two 3-bit identification fields M' and L'. The value of M' is determined by the output authentication field length M, as shown in Equation (11).

$$M' = (M - 2)/2 \tag{11}$$

For L', it is mainly determined by the plain-text data length byte L, with the value of $L - 1$. Based on the identification byte $Flag$ and the key authentication process parameters N_i and n_i, a 13 bytes $Nonce = N_i \,\|\, n_i$ can be obtained. A 128-bit length authentication data block B_0 can be constructed,

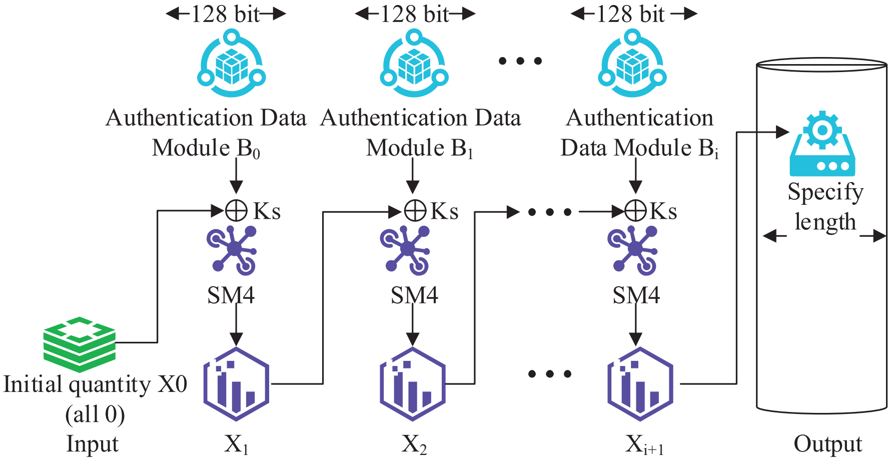

128 bit
128 bit
128 bit
Authentication Data Module B0
Authentication Data Module B1
Authentication Data Module Bi
Ks
Ks
Ks
SM4
SM4
SM4
Initial quantity X0 (all 0)
Input
X1
X2
Xi+1
Specify length
Output

Figure 3 Complete calculation process of CBC-MAC data.

expressed as Equation (12).

$$B_0 = Flag\|Nonce\|len(m) \tag{12}$$

In Equation (12), $len(m)$ represents the plain-text effective byte length value. A 128-bit authentication data string $B_1\|\cdots\|B_t$ can be constructed using plain-text data strings and additional authentication data strings. The data block B_1 consists of additional authentication data a and the additional authentication data length $len(a)$. The plain-text data string B_{a+1} is composed of plain-text data m and plain-text data length $len(m)$ [19]. In the system, the payload of the WIA-PA application layer is plain-text data m. To ensure that the length of m is 128-bit, 0 is added at the end. After constructing the authentication data string $B_0\|B_1\|\cdots\|B_t$, the SM4 algorithm is used for complete CBC-MAC data calculation, as shown in Figure 3.

According to the process in Figure 3, the 128-bit initial vector block X_0 is 0, namely $X_0 = 0^{128}$. The SM4 encryption process is completed using the XOR result of key Ks and authentications X_0 and B_0. The input vector is obtained, as shown in Equation (13).

$$X_{i+1} = SM4(Ks, X_i \oplus B_i) i = 0, \ldots, t \tag{13}$$

In Equation (13), $\oplus$ represents the exclusive OR symbol. The final cipher-text block $X_1\|\cdots\|X_{t+1}$ and message verification code MIC are obtained

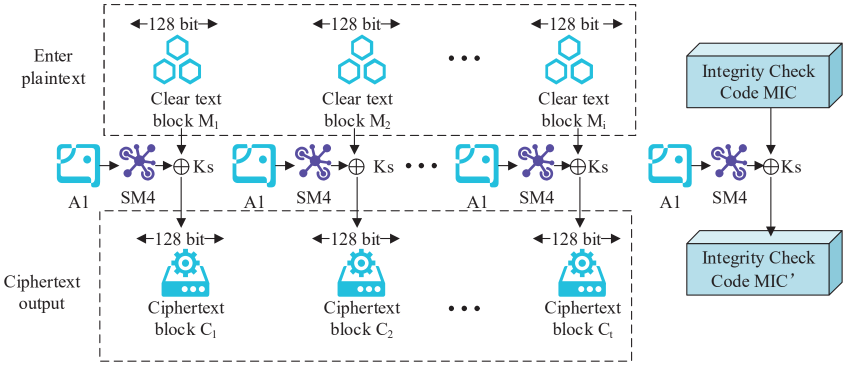


Figure 4 SM4 CCM * data security encryption process.

through SM4 encryption operation. MIC is obtained by truncating M bytes from the leftmost side of the cipher-text block X_{i+1} [20]. After completing the data integrity analysis, the next step is to conduct a data security analysis. Firstly, the vector block A_i is constructed. A_i is used as the input value for application layer data encryption. Its construction identifier byte is $Flag$. By identifying byte $Flag$ and the key authentication process parameters N_i and n_i, 13 bytes $Nonce = N_i \| n_i$ can be obtained. At the same time, the calculator $Counter_i$ with 2 bytes can be obtained [21]. The calculation of vector block A_i is shown in Equation (14) [22].

$$A_i = Flag\|Nonce\|Counter_i, i = 0, 1, 2, \ldots, i < len(m) \tag{14}$$

The effective plain-text data m and the plain-text data length $len(m)$ are used to construct the plain-text data string $M_1|\cdots|M_i$. The plain-text data m is used as the application layer payload, ensuring that the data block is 128-bit by adding 0 at the end [23]. Next, the SM4 algorithm is used to perform CountTeR mode (CTR) calculations on $M_1|\cdots|M_i$ [24]. The entire data security encryption calculation process is shown in Figure 4.

According to Figure 4, a 128-bit grouping vector block is constructed using A_i. The key and SM4 algorithm are used to encrypt Ks. The plain-text block and the key result are XOR computed to obtain the cipher-text block, as shown in Equation (15).

$$C_i = SM4(Ks, A_i) \oplus M_i, i = 1, \ldots, t \tag{15}$$

According to the MIC obtained from data integrity calculation, the same data is securely encrypted. The encrypted MIC' is shown in Equation (16).

$$MIC' = SM4(Ks, A_0) \oplus MIC \tag{16}$$

The encrypted MIC' can effectively prevent verification messages from being intercepted or tampered with by hackers, thereby ensuring the security of the authentication code MIC [25]. Finally, based on the SM4-CRT, secure cipher-text blocks are output to achieve secure transmission of WIA-PA application layer data.

4 Algorithm Performance Testing

To verify the application effectiveness of the proposed WIA-PA network data security transmission technology, experimental testing is conducted on the Windows 11 64-bit platform. The simulation analysis is completed on the Visual Studio 2018 platform. Meanwhile. During the experiment, the SmartRF Packet sniffer tool is used to visually monitor the network WIA-PA communication protocol. Based on this tool, data content such as WIA-PA network beacon frames, data frames, and confirmation frames are obtained. The communication data parameters for the experimental section are shown in Table 1.

During the experiment, the widely used Advanced Encryption Standard (AES) algorithm and Triple DES (3DES) are introduced for experimental comparison. The 3DES data encryption algorithm only supports 56-bit key encryption and decryption, which does not meet the node authentication requirements in the study. Therefore, only the research model and AES model to compare the accuracy of identity authentication, as shown in Figure 5.

Figure 5 shows the results of the WIA-PA network node identity authentication test. The interaction step size refers to the number of times information is exchanged between nodes during the authentication process. The longer interaction steps indicate that the authentication process is more complex and time-consuming, and the communication overhead is also higher. Four types of clients are selected for node identity authentication in the experiment, namely legitimate client, illegal client a, illegal client b, and illegal client c. 1000 different lengths of interaction history data are generated between

Table 2 Communication data for the experimental section

Data Type	Numerical Value	Data Size (GB)
Text data	14852	18.2
Video data	23542	52.6
Image data	75643	48.6
Table data	15682	16.2

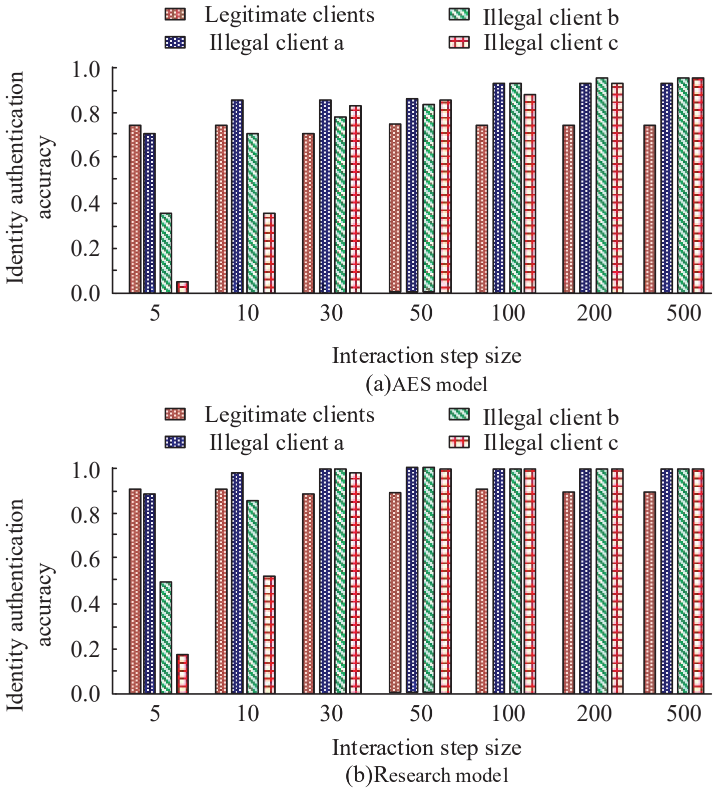


Figure 5 Identity authentication accuracy testing results.

four types of clients and WIA-PA network servers. Figures 5(a) and 5(b) respectively show the identity authentication results of the AES model and the research model. According to the results, as the step size increased, the accuracy of node identity authentication in both models significantly improved. When the step size reached 50, the average accuracy of identity authentication in the research model was over 98.95%, while the AES model was only 84.65%. Furthermore, further analysis revealed that after reaching a step size of 50, the three types of illegal clients were almost unable to obtain authentication in both models. The increase in step size does not affect the authentication effect of legitimate clients. Based on this result, the research technology of industrial wireless network authentication process has significant advantages. Compared with the AES model, the research model has higher accuracy and stronger security in the identity authentication process,

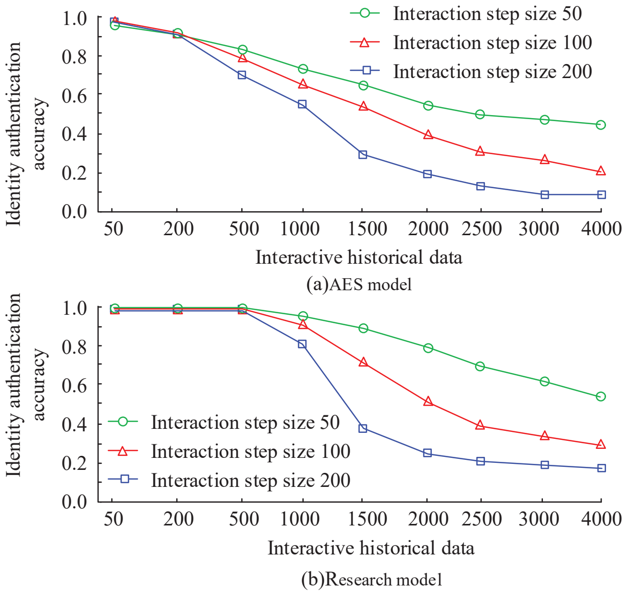


Figure 6 Illegal client c attack testing.

which is of great significance for network node identity security recognition. In addition, at lower interaction step sizes, illegal client c exhibits strong aggressiveness in both models, resulting in lower authentication. Therefore, the aggressiveness of illegal client c is tested, as shown in Figure 6.

Figures 6(a) and 6(b) show the testing results of the AES model and the research model, respectively. According to the result, as the amount of historical interaction data increased, it actually enhanced the aggressiveness of the model. When the interaction history data were within 500, the research model had excellent defense ability, with an identity authentication accuracy of over 99.56%. The AES model only had a high defense capability within the range of 50 interaction historical data. The identity authentication significantly decreased after 200 interaction historical data. Furthermore, further analysis revealed that both models had better attack defense ability when the interaction step size was 50. However, compared with the AES model, the attack and defense performance of the research model improved by 21.35%, indicating better attack defense performance. From the test results, illegal clients in industrial wireless networks have a significant impact on the security of network data, especially with an increase in historical interaction data. The attacks on identity authentication process data will also increase,

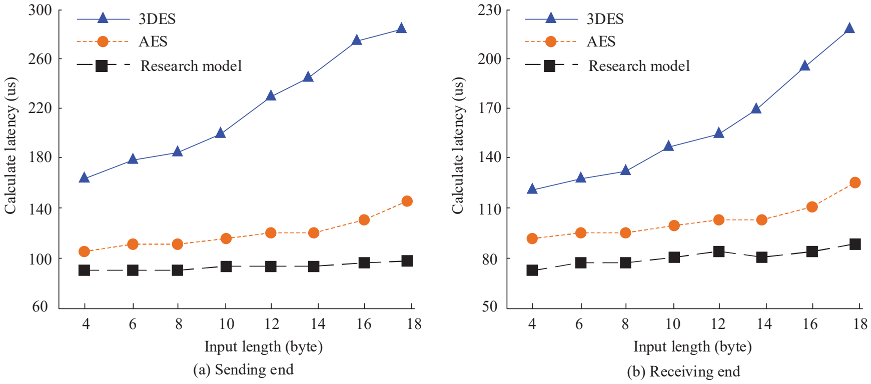


Figure 7 Comparison of network data communication delay performance.

further increasing the data security risks of industrial networks. However, in actual testing, the overall impact of the research model is significantly lower compared with the AES model. The comprehensive anti-attack performance of the research model is better. Therefore, when industrial networks are attacked, the research model has higher security. Next, the end-to-end communication latency is compared, as shown in Figure 7.

Figure 7(a) shows the comparison results of data transmission delay at the sending end. From the results, as the data length increased, the data calculation delay of the model continued to expand. When the input length was 18 bytes, the delay of 3DES, AES, and research model was 289.5 μs, 145.6 μs and 98.6 μs, respectively. The 3DES model had the highest delay and the research model has the lowest delay. Figure 7(b) shows the comparison results of data transmission delay at the receiving end. The research model still had the lowest latency, while the overall latency of the 3DES model was relatively high. When the input length was 16 bytes, the delay of 3DES, AES, and research model was 206.5 μs, 106.5 μs and 90.2 μs, respectively. Overall, the national security algorithm has been optimized and designed for the Chinese industrial network scenario. In addition, the SM4 algorithm uses a 128-bit key, which is equivalent to AES-128. Compared with 3DES (which uses three 56-bit or 168-bit keys), it is simpler and more efficient in key management, significantly reducing overhead and improving communication efficiency. The research model has the lowest network communication delay and better data transmission performance. In addition, the data transmission energy consumption of different models is compared, as shown in Figure 8.

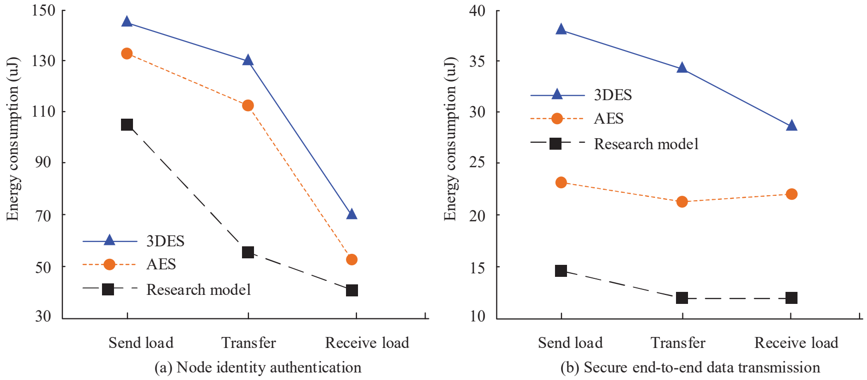
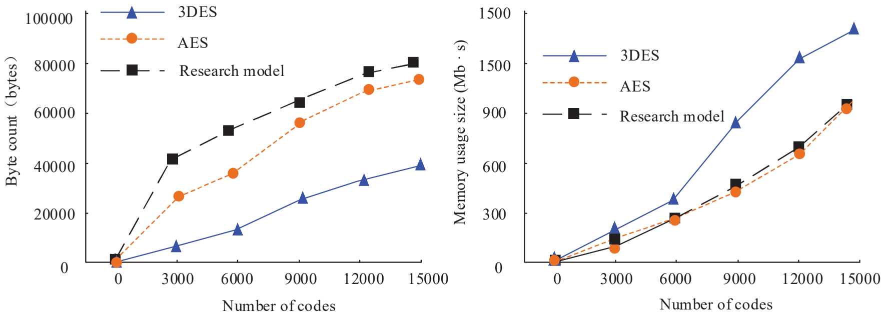


Figure 8 Comparison of end-to-end communication energy consumption.

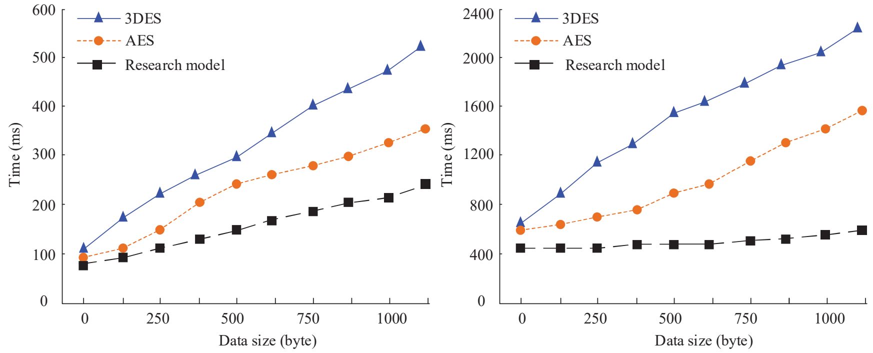
Figure 8(a) shows the energy consumption during the node identity authentication process. The system energy consumption was highest during the data transmission load stage. The energy consumption of 3DES was 147.2 μJ, AES was 137.6 μJ, and the research model was 107.5 μJ. During the load receiving phase, the energy consumption of 3DES, AES, and the research model was 71.5 μJ, 58.6 μJ and 41.2 μJ, respectively. The research model had lower energy consumption. Figure 8 shows the energy consumption during end-to-end data secure transmission. From the data results, the 3DES model had the highest overall energy consumption. The data transmission energy consumption during the sending, transferring, and receiving loads was 38.6 μJ, 34.9 μJ and 29.8 μJ, respectively. The research model had the lowest energy consumption. The energy consumption during sending, transferring, and receiving loads was 15.2 μJ, 12.5 μJ and 12.6 μJ, respectively. Overall, the proposed algorithm is optimized in terms of key length, number of encryption rounds, etc., resulting in a significant reduction in encryption overhead. In addition, the national encryption algorithm adopts a round key generation method, which further reduces the computational load and exhibits excellent energy consumption performance. The research model for node identity authentication and communication data transmission has excellent energy consumption performance. Next, the Keil C51 software is used to compile the system protocol stack in the experiment. The obtained storage space and system running memory usage overhead are shown in Figure 9.

Figure 9(a) shows the code storage overhead of WIA-PA gateway nodes. From the results, as the number of codes increased, the storage overhead



(a) Code storage overhead (b) Code occupancy cost

Figure 9 Code storage and memory usage overhead results.



(a) Encryption performance (b) Decryption performance

Figure 10 Comparison of encryption and decryption performance.

continued to expand. When the code quantity was 15,000, the storage capacity of 3DES, AES, and research model was 39936 bytes, 78235 bytes, and 87356 bytes, respectively. The storage quantity of research model was higher. Figure 9(b) shows the results of node code occupancy cost. The overall memory usage of the 3DES model was high. The memory usage cost of the research model was similar to the AES model. Under the same storage cost, the memory cost of the research model was lower, and the overall effect was better. Finally, the encryption and decryption performance of different models are compared, with a maximum plain-text size of 1250 bytes and a key length of 128-bit, as shown in Figure 10.

Figures 10(a) and 10(b) show the comparison results of encryption and decryption performance, respectively. According to the curve results, as the data increased, both the encryption and decryption time of the model

Table 3 Attack testing of illegal client c under large-scale data

Historical Interaction Data	3DES	AES	Research Model
500	0.901	0.94	0.995
1000	0.854	0.901	0.975
2000	0.804	0.886	0.954
3000	0.764	0.834	0.935
4000	0.545	0.645	0.815
5000	0.535	0.597	0.756
6000	0.521	0.564	0.684
7000	0.514	0.526	0.675
8000	0.510	0.519	0.654

continued to increase. The encryption stage took less time compared with the decryption stage. In encryption, when the data size was 1000 bytes, the time consumption for 3DES, AES, and research model was 498.6 ms, 335.5 ms, and 224.5 ms, respectively. In terms of decryption time, for the same data size of 1000 bytes, 3DES, AES, and research model took 2318.3 ms, 1568.6 ms, and 523.6 ms, respectively. The research model has excellent performance in both encryption and decryption processes, with the shortest encryption and decryption time. In addition, a larger scale industrial wireless network is selected for technical deployment to test the application effectiveness of the research model. Among them, in larger scale industrial wireless networks, there are 75265 text data with a size of 102.2G. There are 89234 video resources with a size of 325.2G. The image data have 235562, with a size of 286.2G. The table data has 65845 entries, with a size of 210.3G. Next, the exchange step size is set to 100. The effectiveness of identifying illegal client c attacks under large-scale historical interaction data is compared. The test is shown in Table 3.

According to the results in Table 3, when the historical interaction data were low, the aggressiveness of illegal client c was weak. When the historical interaction data were 500, the identity authentication accuracy for all three models was above 0.90. As the historical interaction data increased, the total number of illegal clients gradually increased, resulting in a decrease in identity authentication for all three models. However, overall, the research model had stronger defense against external attacks. For example, when the historical interaction data were 2000, the identity authentication accuracy of the research model was 0.954. When the historical interaction data were 3000, the identity authentication accuracy was 0.935, which was significantly better than similar technologies. This indicates that this technology also has excellent performance effects in larger industrial wireless network deployments.

5 Conclusion

To solve the data security in industrial wireless technology communication, a data security transmission technology based on WIA-PA network was proposed. Firstly, considering the vulnerability of WIA-PA network nodes to hacker attacks, the national security SM4 algorithm and HMAC-SM3 algorithm were used to encrypt the authentication between nodes and gateways, ensuring the security of node authentication through the uniqueness of the key. To ensure the effectiveness of network data transmission, a network data security transmission model was constructed based on the SM4 algorithm. The SM4 algorithm was used to authenticate and encrypt network application layer data to ensure the security of data transmission. The node identity authentication effects of different models were compared. When the step size reached 50, the average accuracy of identity authentication was over 98.95%, while the AES model was only 84.65%. According to the attack defense ability of different models under illegal client c, the model had excellent attack defense performance when the interaction history data were within 500, with a node authentication accuracy of over 99.56%, which was better than the AES model. In the comparison of data transmission delay at the sending end, when the input length was 18 bytes, the research model delay was 98.6 μs, while 3DES and AES were 289.5 μs and 145.6 μs, respectively. The overall performance of the research model was better. In addition, the data energy consumption during communication transmission and reception, as well as the node storage and memory usage overhead, were compared. The research model showed excellent performance. Although research technology has excellent application effects in the field of industrial Internet of Things security, in wireless networks with dynamic and mobile nodes, the frequent joining and leaving of nodes, constant changes in location, and frequent changes in network topology pose significant challenges to data transmission security. In the future, authentication and encryption mechanisms suitable for dynamic and mobile node environments can be developed, such as location-based authentication, dynamic key management, etc. In addition, in order to improve the overall security of industrial networks, network security technology can be integrated into the system to further enhance network system security.

References

[1] Shen T, Guo F, Wu C K, Jing CQ. An information transmission scheme based on secure QR code in IoT. International Journal of Wireless and Mobile Computing, 2023, 25(1): 47–57.

[2] Singh A K, Alshehri M, Bhushan S, et al. Secure and energy efficient data transmission model for WSN. Intelligent Automation & Soft Computing, 2021, 27(3): 761–769.

[3] Singh A K, Alshehri M, Bhushan S, Kumar M. Secure and energy efficient data transmission model for WSN. Intelligent Automation & Soft Computing, 2021, 27(3): 761–769.

[4] Ji Z. Engineering operation management technology based on network automation configuration visualization. International Journal of System Assurance Engineering and Management, 2021, 12(4): 765–775.

[5] Ademaj F, Bernhard H P. Quality-of-service-based minimal latency routing for wireless networks. IEEE Transactions on Industrial Informatics, 2021, 18(3): 1811–1822.

[6] Perwej Y, Akhtar N, Kulshrestha N, Rao AN. A Methodical Analysis of Medical Internet of Things (MIoT) Security and Privacy in Current and Future Trends. Journal of Emerging Technologies and Innovative Research, 2022, 9(1): 346–371.

[7] Jiang Y, Shang T, Liu J. SM algorithms-based encryption scheme for large genomic data files. Digital Communications and Networks, 2021, 7(4): 543–550.

[8] Shao T, Wei B, Ou Y, Wei, Y, Wu X. New Second-order Threshold Implementation of Sm4 Block Cipher. Journal of Electronic Testing, 2023, 39(4): 435–445.

[9] Xiangliang M A, Bing L I, Hong W, Di W. Non-profiled Deep-Learning-Based Power Analysis of the SM4 and DES Algorithms. Chinese Journal of Electronics, 2021, 30(3): 500–507.

[10] Wang R, Guo H, Lu J, Liu J W. Cryptanalysis of a white-box SM4 implementation based on collision attack. IET Information Security, 2022, 16(1): 18–27.

[11] Larijani A, Dehghani F. An efficient optimization approach for designing machine models based on combined algorithm. FinTech, 2023, 3(1): 40–54.

[12] Abolfathi M, Inturi S, Banaei-Kashani F, Jafarian JH. Toward enhancing web privacy on HTTPS traffic: A novel SuperLearner attack model and

an efficient defense approach with adversarial examples. Computers & Security, 2024, 139(82): 103–173.

[13] Dezfuli S M K P. Targeted killings and the erosion of international norm against assassination[J]. Defense & Security Analysis, 2023, 39(2): 191–206.

[14] Li T, Zhang J, Obaidat M S, Lin Y. Energy-efficient and secure communication toward UAV networks. IEEE Internet of Things Journal, 2021, 9(12): 10061–10076.

[15] Gupta M, Gupta K K, Shukla P K. Session key based fast, secure and lightweight image encryption algorithm. Multimedia Tools and Applications, 2021, 80(7): 10391–10416.

[16] Marzog H A, Mohsin M J, Therib M A. Chaotic systems with pseudorandom number generate to protect the transmitted data of wireless network. Indonesian Journal of Electrical Engineering and Computer Science, 2021, 21(3): 1602–1610.

[17] Zhang, Y., Xu, X., and Shi, Y. (2024). Construction and Analysis of Network Cloud Security Situation Awareness System Based on DBN-DE Algorithm. Journal of Cyber Security and Mobility, 13(03), 439–460. https://doi.org/10.13052/jcsm2245-1439.1335.

[18] Sathya S S, Umadevi K. RETRACTED ARTICLE: An optimized distributed secure routing protocol using dynamic rate aware classified key for improving network security in wireless sensor network. Journal of Ambient Intelligence and Humanized Computing, 2021, 12(7): 7165–7171.

[19] Ismael H M. Authentication and encryption drone communication by using HIGHT lightweight algorithm. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 2021, 12(11): 5891–5908.

[20] Jayapandian N. Cloud Dynamic Scheduling for Multimedia Data Encryption using Tabu Search Algorithm. Wireless Personal Communications, 2021, 120(3): 2427–2447.

[21] Gheisari M, Hamidpour H, Liu Y, Saedi P, Raza A, Jalili A, Rokhsati H, Amin R. Data Mining Techniques for Web Mining: A Survey. Artificial Intelligence and Applications, 2023, 1(1): 3–10.

[22] Groumpos P P. A Critical Historic Overview of Artificial Intelligence: Issues, Challenges, Opportunities, and Threats. Artificial Intelligence and Applications. 2023, 1(4): 197–213.

[23] Bordel B, Alcarria R, Robles T. Lightweight encryption for short-range wireless biometric authentication systems in Industry 4.0. Integrated Computer-Aided Engineering, 2022, 29(2): 153–173.

[24] Sikora, L. S., Lysa, N. K., Tsikalo, Y. I. and Fedevych, O. Y. (2023) "System-Information and Cognitive Technologies of Man-Made Infrastructure Cyber Security", Journal of Cyber Security and Mobility, 12(03), pp. 389–414.

[25] Kumar, S., Kumar, D. and Lamkuche, H. S. (2021) "TPA Auditing to Enhance the Privacy and Security in Cloud Systems", Journal of Cyber Security and Mobility, 10(3), pp. 537–568.

Biography

Ganghua Bai obtained a physics education degree from Henan Institute of Education in Henan Province, China (2012). At present, he is currently teaching computer related majors in Hebi Polytechnic, with the title of associate professor. He has been teaching for more than 20 years, and has published more than 10 papers, 3 works and 3 patents. His areas of interest include computer science and technology, and information security.