Hindawi
Journal of Sensors
Volume 2022, Article ID 6199900, 13 pages
https://doi.org/10.1155/2022/6199900

Research Article

A Security Transmission and Early Warning Mechanism for Intelligent Sensing Information in Internet of Things

Li Qi,[1] Zetian Wang,[2] Di Zhang,[2] and Yunfa Li[2]

[1] *Intelligent Video Surveillance Engineering Technology Research Center, The Third Research Institute of Ministry of Public Security, Shanghai 200031, China*
[2] *School of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou 310018, China*

Correspondence should be addressed to Yunfa Li; yunfali@hdu.edu.cn

Received 12 August 2021; Accepted 29 December 2021; Published 24 January 2022

Academic Editor: Carlos Marques

Copyright © 2022 Li Qi et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

As the demand for intelligent services in the Internet of Things continues to increase, the amount of intelligent sensing information is also increasing, and the security of these information has gradually attracted attention. Owing to the openness and the dynamics of intelligent sensor devices, there are a lot of security issues which needed to be resolved for the corresponding intelligent sensing information. In order to protect the transmission security of intelligent sensing information, this paper proposes a security transmission and early warning mechanism for intelligent sensing information in the Internet of Things. In the security transmission and early waring mechanism, we first propose an encryption/decryption algorithm for intelligent sensing information. Then, we build a security transmission algorithm. On that basis, we propose an early warning algorithm of intelligent sensing information. At the end of this paper, we analyze the security of this mechanism and the results of the experiment in order to illustrate its effectiveness. The results show that our proposed security transmission and early warning mechanism are very effective in the Internet of Things.

1. Introduction

Recently, the technology of the Internet of Things (IoT) has developed rapidly. With the development of the technology, the applications of IoT are becoming more and more extensive and there are more and more types of intelligent sensor devices. In this situation, people also show great enthusiasm for the research of various sensors especially in the field of optical fiber sensors. For example, Wang et al. [1] presented some specific optimization design methods and priority design parameters of the classified sensors. In these methods, the relationship between the strain transfer coefficient and allowable testing error is established based on the strain transfer theory. And the proposed relationship is regarded as the optimal control equation to obtain the optimal value of sensors that satisfy the requirement of measurement precision. By considering the practical state of sensors and the testing accuracy, comprehensive and systematic analyses on optical fiber sensors are provided from the perspective of mechanical actions, which could scientifically instruct the application design and calibration test of industrialized optical fiber sensors. In order to improve the durability of the optical fiber sensor, Wang et al. [2] explore the interfacial debonding failure mechanism of embedded sensors based on the strain transfer analysis and provide theoretical basis for enhancing the interfacial bonding properties. In order to open new opportunities for applications in wavelength division multiplexing networks and also for microwave photonic applications, Min et al. [3] demonstrate a simple method to fabricate phase-shifted fiber Bragg gratings in polymer optical fibers using the phase mask technique. In the paper, a simple way is demonstrated to fabricate phase-shifted fiber Bragg grating in polymer optical fibers as a narrowband transmission filter for a variety of applications at telecom wavelengths. In addition, in order to explore a new generation of sensors with advantageous features such as lower cost, easy connectivity, higher degree of customization, and better performance, Leal-Junior et al. [4] present a review of the fiber specklegram sensor (FSS) technology. And the operation principle and main characteristics of specklegram are presented, and the applications of fiber specklegram sensors are thoroughly discussed in this paper.

A conclusion can be drawn that some great achievements have been made in the development and application of sensors from the above studies. It is these great achievements that promote the widespread application of sensors in the Internet of Things. However, some attacks, such as theft, tampering, and unauthorized access to intelligent sensing information, often happen in the recent years. These occurrences have some impact on the security and service of intelligent sensing information of the Internet of Things and bring some security risks and economic losses to users, enterprises, and countries. Due to this situation, a lot of famous companies and research institutes began extensive research on this series of problems and put forward a series of theories and methods. These researches can be simply listed in the succeeding paragraphs.

Kandi et al. [5] propose a novel versatile key management protocol for the Internet of Things. In the paper, the security and performance of the novel versatile key management protocol are analyzed. By using the novel versatile key management protocol, the forward and backward secrecy of sensing information can be ensured for group communication. Yi and Dong [6] propose an item-level access control framework for intersystem security in the Internet of Things. The aim is to solve the problem of mutual trust between different partners when companies are building IoT systems. Bruce et al. [7] firstly analyze the authentication and access control method used in the Internet of Things presented by Jing et al. By analyzing Jing et al.'s protocol, the authors find that the message exchange and the security assessment are not strong. In order to overcome this fault, Bruce et al. propose improvements to the protocol to fill the discovered weakness gaps.

Gusmeroli et al. [8] describe a capability which can be used to manage their own access control processes to services and information. The mechanism is based on the access control system of enterprises, or even individuals, which can support rights delegation and a more sophisticated access control customization. Aafaf et al. [9] introduce a new access control framework for the IoT environment. The framework is called "IntelligentOrBAC," which is based on the OrBAC model. The access control framework puts the context awareness concern in a first position and deals with the constrained resources environment complexity. To achieve these goals, a list of detailed IoT security requirements and needs is drawn up in order to establish the guidelines of the "IntelligentOrBAC."

Qinlong et al. [10] propose a secure and fine-grained data access control scheme with a ciphertext update and a computation outsourcing in fog computing for IoT. In the scheme, the sensitive data of the owner are first encrypted using attribute-based encryption with multiple policies and then outsourced to a cloud storage. Hence, the user whose attributes satisfy the access policy can decrypt the ciphertext. In fact, the computations for data owners to encrypt, end users to decrypt, reencrypt, and sign are irrelevant to the number of attributes in the policies. Logrippo [11] takes a fundamental approach to the security problem of data flow control. In the fundamental approach, any network of communicating entities can be seen as a partial order of equivalence classes of entities under reflexivity and transitivity assumptions.

Kendrick et al. [12] present a novel implementation of a multiagent system. By using the system, the Internet of Things networks can support the distributed processing of security events and can offload the computational cost of processing data from the Internet of Things devices. Yang et al. [13] firstly studied an algorithm redundancy design method for an industrial control network and discussed the importance of the algorithmic-level heterogeneous redundancy. Then, they proposed an improved majority voting algorithm. In order to show the higher accuracy and output efficiency of the improved majority voting algorithm, it is compared with the standard majority voting algorithm and the median voting algorithm. Ammar et al. [14] first describe the design and implementation of S$\mu\mu$V. Then, they highlight the formal verification of software architecture and characterize the remote attestation protocol. At last, they evaluate the S$\mu\mu$V implementation using an 8-bit AVR microcontroller that is widely used in IoT devices.

Siboni et al. [15] propose an innovative security testbed framework targeted at IoT devices. The authors propose the testbed framework to test all types of IoT devices, with different software/hardware configurations. At the end of the paper, advanced analysis processes based on machine learning algorithms are employed in order to monitor the overall operation of the IoT device under test. Kamals and Tariq [16] propose a light-weight protocol to secure the data and achieving data provenance for the multihop IoT network. In the protocol, the link fingerprints are matched at the server to compute the correlation coefficient. The higher the value of the correlation coefficient, the higher the percentage of the secured data transmissions. Lower value gives the detection of adversarial node in between a specific link.

Ullah et al. [17] propose a combined deep learning approach to detect the pirated software- and malware-infected files across the IoT network. In the approach, the TensorFlow deep neural network is first proposed to identify pirated software using source code plagiarism. Then, the tokenization and weighting feature methods are used to filter the noisy data and, further, to zoom the importance of each token in terms of source code plagiarism. At the same time, the deep learning approach is used to detect source code plagiarism. Lastly, the dataset is collected from Google Code Jam (GCJ) to investigate software piracy. Pechetti et al. [18] propose a novel scheme, channel-based mapping diversity. In the scheme, the inherent randomness of the wireless channel and multiple mappings is used which are available for an M-ary phase shift keying constellation in confusing an eavesdropper. Krishna and Lorenz [19] propose a novel approach of location, context, and social objectives using knowledge-based rules and conflict resolution for security (LOCSKS) in the Internet of Things. In the approach, the Bayesian decision theory is applied and the node behavior is analyzed, which is based on prior and posterior knowledge of the location, context, and social objectives in the Internet of Things. In order to ensure the location privacy and trust in the system, LOCSKS exclusive and economical keys are considered the context to service-type mapping and risk levels.

Bradbury et al. [20] present a novel formalization of a duty cycling protocol as a transformation process. Using derived transformation rules, they present the first duty cycling protocol for a Source Location Privacy awareness routing protocol for a local eavesdropping attacker. Jiang et al. [21] study an approach that applies independent random projection at each IoT object to obfuscate data and trains a deep neural network at the coordinator based on the projected data from the IoT objects. This approach introduces light computation overhead to the IoT objects and moves most workload to the coordinator that can have sufficient computing resources. With the proliferation of IoT cameras, it is possible to use crowdsourced videos to help find interested targets on demand. However, this may raise privacy concerns when owners of IoT cameras are provided with photos of the target. To address this problem, Khazbak et al. [22] design and implement TargetFinder, a privacy-preserving system for target search through IoT cameras. By exploiting homomorphic encryption techniques, the server can search for the target on encrypted information.

To sum up, although a series of security theories and methods have been proposed to maintain the security of the Internet of Things, these security theories and methods mainly focus on the key management, access control, testbed framework, privacy preserving, and so on. There is lack of the analysis method of the transmission state of intelligent sensing information. Moreover, there is also lack of a link information collection and the encryption synchronization mode of intelligent sensing information. All of these will impact on the security of the service security of intelligent sensing information.

In recent years, some attacks, such as theft, tampering, and unauthorized access to intelligent sensing information, often happen. The main factors that generated these attacks are as follows: (1) due to the influence of energy consumption and other factors, some intelligent sensor devices in IoT usually undergo dynamic changes (such as join or quit), and their intelligent sensing information and the corresponding transmission link will also undergo dynamic changes. Thus, the dynamic changes of intelligent sensor devices, intelligent sensing information, and transmission link will bring more opportunities and possibilities to the network intrusion of illegal users. (2) Due to the dynamic changes of intelligent sensor devices, the network management is complex and difficult. Thus, it makes it easier for illegal users to hack into networks. (3) Due to the limitations of wireless transmission, it makes it easier for illegal users to invade the intelligent sensing information.

These attacks have some impacts on the security and the reliability of service of intelligent sensing information in the Internet of Things. And they bring some security risks and economic losses to users, enterprises, and countries. However, the existing network security protection policies cannot be satisfied with the security requirements of intelligent sensing information at present. In this state, it has become an urgent problem for people which need to be resolved that how to protect the security of intelligent sensing information in the Internet of Things.

In order to overcome this problem, we will adopt a link information collection and the encryption synchronization mode of intelligent sensing information. That is, the source intelligent sensor device which transmits the intelligent sensing information is responsible for collecting the sensing information of all intelligent sensor devices in the link path and opening this information to all intelligent sensor devices in the link path. The intelligent sensor device transmitted in the middle only needs to authenticate the secret information and confirmation information sent by the previous intelligent sensor device and does not need to decrypt/encrypt the transmitted intelligent sensing information. Thus, it can effectively reduce the calculation cost of the intelligent sensor device in the intermediate transmission and reduce energy consumption by using the methods.

Based on the above methods, we propose a security transmission and early warning mechanism for intelligent sensing information in the Internet of Things. In this mechanism, we first build an encryption/decryption algorithm for intelligent sensing information. Then, we build a security transmission algorithm. On that basis, an early warning algorithm is constructed for the secure transmission of intelligent sensing information according to the actual requirement of the security transmission of intelligent sensing information.

The organization of this paper is as follows: Section 2 describes the security transmission and early warning mechanism for intelligent sensing information in the Internet of Things. The security of the security transmission and early warning mechanism is analyzed in Section 3. Section 4 describes a series of experiments and analyzes the results of experiments. The last section is Conclusions and Future Work.

2. Security Transmission and Early Warning Mechanism

This section will propose a security transmission and early warning mechanism for intelligent sensing information in the Internet of Things which is based on intelligent sensor devices. Figure 1 shows the architecture of intelligent sensor devices in the Internet of Things.

This section includes three stages to ensure the security of intelligent sensing information: (1) an encryption/decryption algorithm for intelligent sensing information, (2) the security transmission algorithm of intelligent sensing information, and (3) an early warning algorithm of abnormal conditions. Each stage is described as follows.

2.1. Encryption/Decryption Algorithm for Intelligent Sensing Information. The security transmission process of intelligent sensing information involves encryption/decryption, security transmission, and an early warning of abnormal conditions in the Internet of Things. At present, a number of scholars mainly use DES and AES as a representative

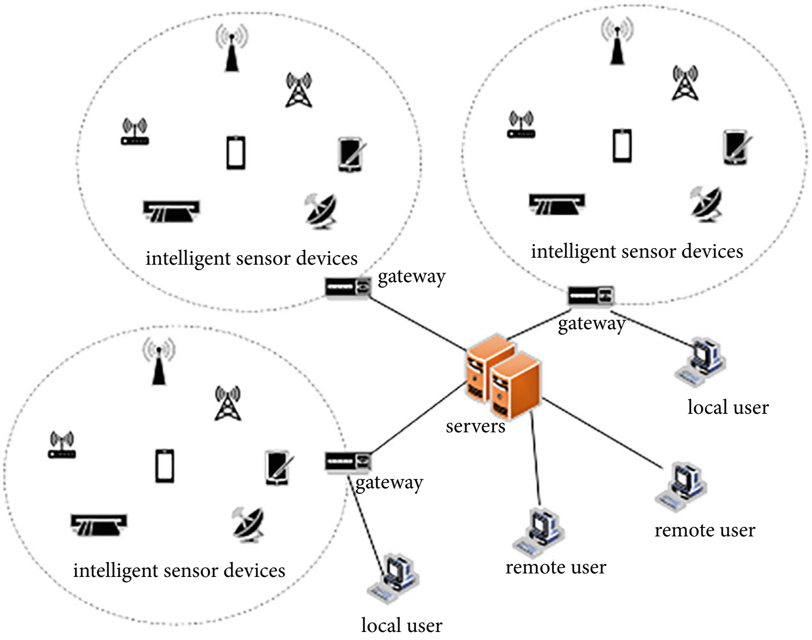
intelligent sensor devices
gateway
intelligent sensor devices
gateway
local user
servers
intelligent sensor devices
gateway
remote user
remote user
local user

Figure 1: The architecture of intelligent sensor devices in the Internet of Things.

symmetric information encryption technology and RSA as a representative asymmetric information encryption technology to collect and transmit sensing information. In the processes of using these encryption algorithms, the intelligent sensing information which appears in plaintext is encrypted by bit operation. Thus, if the number of iterations increases, the efficiency of encryption will decrease with the increase of the plaintext of sensing information. In order to effectively solve this problem and avoid the damage caused by information leakage to the intelligent sensing equipment, the intelligent sensing information required to be transmitted by the intelligent sensor devices will be first divided according to the size of the constraint time. Then, according to the basic principles of chaos algorithms, the operation methods of Lorenz chaotic algorithm [23] and Wien chaotic algorithm [24] are mixed to process the block information accordingly, so as to improve the randomness of chaotic sequence. Since the information block will produce a certain offset in the process of chaotic algorithm, and the same information block may have a different offset after a different chaotic algorithm, we construct a coupling equation to couple them in order to increase the coupling of different chaotic maps.

In addition, in order to improve the security of the ciphertext, we construct a jamming sequence to conduct secondary jamming on the ciphertext of the secret information. On this basis, the chaotic sequence corresponding to each plaintext block is organically combined with the plaintext and generated sequential key stream. Finally, the ciphertext is obtained by bitwise *XOR* operation between the sequence of the key and the plaintext. In the process of decryption, the same method as the encryption method will be used and the key stream will be used to decrypt the received ciphertext.

Suppose that the intelligent sensing information that the intelligent sensor device needs to transmit during the time slot T is *SM(T)*, and $L(SM(T))$ represents the size of the intelligent sensing information *SM(T)*, p_i is the segmentation parameter of the i*th* block of the intelligent sensing information SM(T) ($0 < p_i \leq 1, 1 \leq i \leq n, \sum_{i=1}^{n} p_i = 1$), then the segmentation information of the i*th* block of intelligent sensing information SM(T) can be expressed as: $DM(T)_i = \lfloor p_i * SM(T) \rfloor$, its size can be expressed as $L(DM(T)_i) = \lfloor p_i * L(SM(T)) \rfloor$. From this, we can get the following conclusions:

$$
\begin{gathered}
DM(T)_i \cap DM(T)_j = \varnothing, \text{where, } i \neq j, 1 \leq i \leq n, 1 \leq j \leq n, \\
SM(T) = \sum_{i=1}^{n} DM(T)_i, \\
\sum_{i=1}^{n} p_i = 1, \text{ where, } 0 < p_i \leq 1, 1 \leq i \leq n.
\end{gathered} \tag{1}
$$

Therefore, the specific block algorithm is described as follows:

(Step 1) The intelligent sensor device determines the intelligent sensing information SM(T) and the size of the intelligent sensing information *L(SM(T))* according to its processing ability, which need to be transmitted during the time slot T.

(Step 2) The intelligent sensor device determines the segmentation parameter p_i of each block in its intelligent sensing information SM(T) according to its own communication ability (where $0 < p_i \leq 1, 1 \leq i \leq n, \sum_{i=1}^{n} p_i = 1$).

(Step 3) The intelligent sensor device computes each information block $DM(T)_i = p_i * SM(T)$ and its size $L(DM(T)_i) = p_i * L(SM(T))$ according to its segmentation parameter p_i.

(Step 4) The intelligent sensor device divides intelligent sensing information SM(T) according to the following calculation formula

$$\begin{cases} DM(T)_i \cap DM(T)_j = \varnothing \text{where, i} \neq j, 1 \leq i \leq n, 1 \leq j \leq n \\ SM(T) = \sum_{i=1}^{n} DM(T)_i \, DM(T)_i \neq \varnothing, 1 \leq i \leq n \end{cases}. \tag{2}$$

(Step 5) The intelligent sensor device judges whether the intelligent sensing information SM (T) is divided or not. If so, go to step 6; otherwise, go to step 3.

(Step 6) End.

According to the basic principle of chaotic algorithm, Lorenz chaotic algorithm is first applied to process the intelligent sensing information block $DM(T)_i (1 \leq i \leq n)$. Then, the corresponding initial iteration sequence $\pi_L = (\pi_L^1(DM(T)_i), \pi_L^2(DM(T)_i), \pi_L^3(DM(T)_i))$ is obtained, abbreviated as $\pi_L = (\pi_L^1, \pi_L^2, \pi_L^3)$. Then, Wien chaotic algorithm is used to process the intelligent sensing information block $DM(T)_i (1 \leq i \leq n)$ and get the corresponding initial iteration sequence $\pi_W = (\pi_W^1(DM(T)_i), \pi_W^2(DM(T)_i), \pi_W^3(DM(T)_i))$, abbreviated as $\pi_W = (\pi_W^1, \pi_W^2, \pi_W^3)$. In the following step, the two initial iterative sequences are mixed to get the result $\pi = \pi_L \otimes \pi_W = (\pi_L^1, \pi_L^2, \pi_L^3, \pi_W^1, \pi_W^2, \pi_W^3)$. In order to effectively improve the randomness of the mixed chaotic sequence and eliminate the cross-correlation between the mixed chaotic sequence, the following *XOR* operation ("⊕" is the *XOR* operator) is performed on the mixed chaotic sequence:

$$\begin{aligned} \pi_W^1 &= \pi_L^1 \oplus \pi_W^1, \\ \pi_W^2 &= \pi_L^2 \oplus \pi_W^2, \\ \pi_W^3 &= \pi_L^3 \oplus \pi_W^3. \end{aligned} \tag{3}$$

Thus, a new chaotic sequence is obtained: $\pi_{new} = (\pi_L^1, \pi_L^2, \pi_L^3, \pi_W^1, \pi_W^2, \pi_W^3)$.

We use M_0 to denote the initial iteration number of Lorenz chaotic algorithm, N_0 to denote the initial iteration number of Wien chaotic algorithm, and φ_i to denote the offset of the first byte of the plaintext block.

The actual iteration number M_K of the intelligent sensing information block $DM(T)_i$ in Lorenz chaotic algorithm can be obtained by using the equation $M_K = (\varphi_i/n) + M_0$. And the actual iteration number N_E of the intelligent sensing information block $DM(T)_i$ in Wien chaotic algorithm can be obtained by using the equation $N_E = (\varphi_i/n) + N_0$.

Therefore, all new hybrid chaotic iterative sequences and the number of hybrid chaotic iterative sequences can be obtained. If we assume π^*_{new} is the set of all new hybrid chaotic iterative sequences, then the following equation can be obtained:

$$\pi^*_{new} = \{\pi_{new} \mid (\pi_L^1(M_k), \pi_L^2(M_k), \pi_L^3(M_k), \pi_W^1(N_e), \pi_W^2(N_e), \pi_W^3(N_e))\}, \tag{4}$$

where $1 \leq k \leq K$, $1 \leq e \leq E$.

If we assume MN is the number of hybrid chaotic iterative sequences, then MN can be calculated out by using the following equation: $MN = M_K * N_E$.

For any mixed chaotic iteration sequence $\pi_{new} = (\pi_L^1(M_j), \pi_L^2(M_j), \pi_L^3(M_j), \pi_W^1(N_j), \pi_W^2(N_j), \pi_W^3(N_j))$, $1 \leq j \leq MN$ of the mixed chaotic iterative sequence set π^*_{new}, in order to guarantee the high reliability and the randomness of the iterative sequence, we use $\pi_S = (\pi_L^1(M_j), \pi_L^2(M_j), \pi_L^3(M_j), \pi_W^1(N_j))$ to denote the initial sequence before information encryption, $\pi_D = (\pi_W^2(N_j), \pi_W^3(N_j))$ to denote the interference sequence before information encryption. On this basis, Wien chaotic algorithm and 2D Logistic chaotic algorithm [25] are used to generate the key sequence required by the intelligent sensing information block $DM(T)_i$ for encryption, namely, $\pi_{SK} = (\pi_{sk}^1, \pi_{sk}^2, \pi_{sk}^3, \pi_{sk}^4)$. In order to maintain the security and reliability of the key sequence in the transmission process, the XOR operation is performed as follows:

$$\begin{aligned} \pi_{sk}^3 &= \pi_{sk}^1 \oplus \pi_{sk}^3, \\ \pi_{sk}^4 &= \pi_{sk}^2 \oplus \pi_{sk}^4. \end{aligned} \tag{5}$$

Therefore, a new key sequence can be obtained, namely, $\pi_{SK}^{new} = (\pi_{sk}^1, \pi_{sk}^2, \pi_{sk}^3, \pi_{sk}^4)$.

In order to carry out the XOR operation between the key sequence and the plaintext sequence of intelligent sensing information, it is necessary to carry out decimal point shift and modulus operation on the elements in the new key sequence. The calculation equation can be described as follows:

$$\begin{gathered} \pi_{sk}^i = \pi_{sk}^i * 10^9 - \lfloor \pi_{sk}^i \rfloor * 10^9 \; (\text{where } i = 1, 2, 3, 4), \\ \pi_L^i(M_j) = \pi_L^i(M_j) * 10^9 - \lfloor \pi_L^i(M_j) \rfloor * 10^9 \; (\text{where } i = 1, 2, 3), \\ \pi_W^i(N_j) = \pi_W^i(N_j) * 10^9 - \lfloor \pi_W^i(N_j) \rfloor * 10^9 (\text{where } i = 2, 3). \end{gathered} \tag{6}$$

In order to ensure the requirement of encryption, the intelligent sensing information block $DM(T)_i$ is divided into plaintext code stream according to 4 bytes (the last part is supplemented with 0), and its corresponding *ASCII* code is used. On this basis, the corresponding encryption process is carried out; that is, the plaintext in the plaintext stream and the key in the new key sequence are *XOR* operated once to get the initial ciphertext. Then, the interference sequence is used to *XOR* the initial ciphertext again to get the final ciphertext of the initial ciphertext. The calculation formula is as follows:

$$\begin{aligned} C\left(DM(T)_i\right)_{4l+1} &= \mathrm{ASCII}\left(DM(T)_i\right)_{4l+1} \oplus \pi_{sk}^{1}(l+1) \oplus \pi_{W}^{2}\left(N_j\right)(l+1), \\ C\left(DM(T)_i\right)_{4l+2} &= \mathrm{ASCII}\left(DM(T)_i\right)_{4l+2} \oplus \pi_{sk}^{2}(l+1) \oplus \pi_{W}^{3}\left(N_j\right)(l+1), \\ C\left(DM(T)_i\right)_{4l+3} &= \mathrm{ASCII}\left(DM(T)_i\right)_{4l+3} \oplus \pi_{sk}^{3}(l+1) \oplus \pi_{W}^{2}\left(N_j\right)(l+1), \\ C\left(DM(T)_i\right)_{4l+4} &= \mathrm{ASCII}\left(DM(T)_i\right)_{4l+4} \oplus \pi_{sk}^{4}(l+1) \oplus \pi_{W}^{3}\left(N_j\right)(l+1). \end{aligned} \tag{7}$$

In the above calculation formula, $l+1$ is used to denote the iteration number of the encryption processes.

When an adjacent intelligent sensor device or a legitimate user receives the encrypted intelligent sensing information, the same steps similar to the encryption method are used to decrypt the received cipher text by using the key stream.

2.2. Security Transmission Algorithm of Intelligent Sensing Information. In the Internet of Things, a large number of intelligent sensor devices need to transmit their sensing information to remote servers through a complex network. Due to the openness, dynamics and versatility of the Internet of Things, deception and eavesdropping usually occur between different intelligent sensor devices, in order to prevent unauthorized users and other illegal users from accessing and stealing intelligent sensing information and protecting intelligent sensing information security, a security transmission algorithm of intelligent sensing information is specially proposed.

The basic idea of the security transmission algorithm of intelligent sensing information is as follows: first, the intelligent sensor device determines the intelligent sensing information to be transmitted. Then, it determines the transmission range of the intelligent sensing information and ensures the number of end points (the ultimate receiver of intelligent sensing information, which is the end point) within the range that can transmit information. On this basis, mutual authentication between the intelligent sensor device and other intelligent sensor devices or other communication devices is carried out. When the authentication is legal, the intelligent sensor device uses the encryption/decryption algorithm of the intelligent sensing information proposed in the previous section to encrypt it. The information receiver decrypts the information after receiving the intelligent sensor device information. When the authentication is illegal, the intelligent sensor device rejects to transmit the intelligent sensing information.

The specific security transmission algorithm of intelligent sensing information is described as follows:

(Step 1) The intelligent sensor device *A* determines the intelligent sensing information *SM(T)* to be transmitted during the time slot *T*, and constructs the transmission information table file *TITF(T)*.

(Step 2) The intelligent sensor device *A* determines the transmission range of its device and determines the number of intelligent sensor devices within the range that can transmit sensor information to each other *n*.

(Step 3) The intelligent sensor device A numbers the intelligent sensor devices located within the transmission range of the device that can transmit sensor information to each other *num* ($num = 1, 2, 3, \ldots, m$), and constructs the transmission link table file *TLTA(T)*.

(Step 4) The intelligent sensor device A uses our proposed block algorithm to obtain information block $DM(T)_i$ ($i = 1, 2, 3, \ldots, n$) for the intelligent sensing information *SM(T)* that needs to be transmitted.

(Step 5) The intelligent sensor device *A* randomly generates an integer *R*, and calculates $(DM(T)_i \cup TITF(T)) * num - R$ for each intelligent sensor device *num* that will transmit sensing information, so that $m_{num} = (DM(T)_i \cup TITF(T)) * num - R$.

(Step 6) The intelligent sensor device *A* randomly generates a new random integer r_i, and uses the encryption/decryption algorithm of the intelligent sensing information proposed in the previous section to encrypt $m_{num} \| r_i$ to obtain $E(m_{num} \| r_i)$.

(Step 7) The intelligent sensor device *A* sends the encrypted information $E(m_{num} \| r_i)$ to the intelligent sensor device *num* according to *num*.

(Step 8) The intelligent sensor device *num* receives the encrypted information $E(m_{num} \| r_i)$ sent by the intelligent sensor device *A*.

(Step 9) After the intelligent sensor device *num* receives the encrypted information $E(m_{num} \| r_i)$ sent by the intelligent sensor device A, it randomly selects a secret message m_s (e.g., identity information) and compares it with the received confirmation message ACK_{num} performs string operation to get $m_s \| ACK_{num}$.

(Step 10) The intelligent sensor device *num* uses the encryption/decryption algorithm proposed in the previous section to encrypt $m_s \| ACK_{num}$ to obtain $E(m_s \| ACK_{num})$.

(Step 11) The intelligent sensor device *num* transmits $E(m_s \| ACK_{num})$ to the intelligent sensor device *A*.

(Step 12) After the intelligent sensor device *A* receives $E(m_s \| ACK_{num})$ it uses the encryption/decryption algorithm of intelligent sensing information proposed in the previous section to decrypt $E(m_s \| ACK_{num})$ to get $m_s \| ACK_{num}$.

(Step 13) The intelligent sensor device A performs identity authentication and confirmation message authentication on the intelligent sensor device num according to $m_s\|ACK_{num}$. If the authentication is passed, the intelligent sensor device A will randomly select a secret information m_A (e.g., identity information), and perform a string operation with the received confirmation message ACK_A to obtain $m_A\|ACK_A$; if the authentication fails, the intelligent sensor device A will disconnect the communication with the intelligent sensor device num, go to Step 20.

(Step 14) The intelligent sensor device A uses the encryption/decryption algorithm proposed in the previous section to encrypt $m_A\|ACK_A$ to obtain $E(m_A\|ACK_A)$.

(Step 15) The intelligent sensor device A sends the encrypted information $E(m_A\|ACK_A)$ to the intelligent sensor device num according to m_s $\|ACK_{num}$.

(Step 16) The intelligent sensor device num receives the encrypted information $E(m_A\|ACK_A)$ sent by the intelligent sensor device A.

(Step 17) After the intelligent sensor device num receives the encrypted information $E(m_A\|$ $ACK_A)$ sent by the intelligent sensor device A, it uses the encryption/decryption algorithm of the intelligent sensing information proposed in the previous section to decrypt E $(m_A\|ACK_A)$ and get $m_A\|ACK_A$.

(Step 18) The intelligent sensor device num performs identity authentication and confirmation message authentication on the intelligent sensor device A according to $m_A\|ACK_A$. If the authentication is passed, the intelligent sensor device num will use the intelligent sensing information encryption/decryption algorithm proposed in the previous section to decrypt $E(m_{num}\|r_i)$ to obtain $m_{num}\|r_i$. if the authentication fails, disconnect and communication of intelligent sensor device A, go to Step 20.

(Step 19) The intelligent sensor device num calculates out m_{num} and r_i according to the decrypted $m_{num}\|r_i$, thereby ensures the intelligent sensing information $DM(T)_i$ and the transmission information table file *TITF(T)*.

(Step 20) End.

2.3. Early Warning Algorithm of Intelligent Sensing Information. In the Internet of Things, intelligent sensor devices encrypt the intelligent sensing information that needs to be transmitted, which can improve the security of intelligent sensing information transmission. However, for the intelligent sensor devices in the intermediate transmission, if the decryption and encryption are frequently performed, the calculation cost is too high and the energy consumption is too large. In order to overcome this problem, we will adopt the link information collection and the encryption synchronization mode of intelligent sensing information. That is, the source intelligent sensor device which transmits the intelligent sensing information is responsible for collecting the sensing information of all intelligent sensor devices in the link path and opening this information to all intelligent sensor devices in the link path. The intelligent sensor device transmitted in the middle only needs to authenticate the secret information and the confirmation information sent by the previous intelligent sensor device, and does not need to decrypt/encrypt the transmitted intelligent sensing information. This method can effectively reduce the calculation cost and the energy consumption of the intelligent sensor device in the intermediate transmission.

Although the link information collection and the encryption synchronization mode of the intelligent sensing information can effectively reduce the calculation cost and the energy consumption of intelligent sensor devices in the intermediate transmission, it also increases the security risk of intelligent sensor devices and intelligent sensing information transmission. To avoid this risk from harming the security of intelligent sensing information, we propose an early warning algorithm for the security transmission of intelligent sensing information.

The basic idea of the early warning algorithm for the security transmission of intelligent sensing information is that the intelligent sensor device first judges whether it is an intermediate transmission node of the intelligent sensing information block $DM(T)_i$ $(i = 1, 2, 3, \ldots, n)$ according to the transmitted link table file *TLTA(T)*. If yes, the intelligent sensor device receives the encrypted intelligent sensing information and the transmission information table file *TITF(T)*. Then, it uses the intelligent sensing information encryption/decryption algorithm proposed in this paper to decrypt the received intelligent sensing information and the transmission information table file *TITF(T)*, respectively. On this basis, statistical analysis is performed by the intelligent sensor device based on the received intelligent sensing information according to the decrypted intelligent sensing information and the transmission information table file *TITF(T)*. If the received intelligent sensing information *ISI_A* exceeds the upper limit $ISI\_A_{\max}$, allowed by the system, a warning message will be generated. it indicates that the intelligent sensing information may have been attacked by the network during the link transmission process, and illegal data has entered in disguise, and the stream key needs to be updated. If the received intelligent sensing information *ISI_A* is lower than the lower limit $ISI\_A_{\min}$, allowed by the system, a warning message is generated. It indicates that the intelligent sensing information may have been stolen by hackers during the link transmission process, causing the legal data to be lost, and the stream key needs to be updated again. If the received intelligent sensing information is within the range allowed by the system, no warning is required.

The specific early warning algorithm for the security transmission of intelligent sensing information is described as follows:

(Step 1) The intelligent sensor device B receives the link table files $TLTA(T)$ and $E(m_{num}\|r_i)$ transmitted from the adjacent intelligent sensor device A.

(Step 2) The intelligent sensor device B judges whether the encrypted information $E(m_{num}\|r_i)$ and the link table file $TLTA(T)$ have been transmitted, if they have been transmitted, go to Step 3; otherwise, go to Step 1.

(Step 3) According to the transmitted link table file $TLTA(T)$, the intelligent sensor device B judges whether it is an intermediate transmission node of the intelligent sensing information block $DM(T)_i$ (i=1, 2, 3, …, n). If yes, go to Step 4; if not, go to Step 6.

(Step 4) The intelligent sensor device B uses a security transmission algorithm of intelligent sensing information to transmit the encrypted information $E(m_{num}\|r_i)$ to the next adjacent intelligent sensor device C according to the link table file $TLTA(T)$.

(Step 5) The intelligent sensor device B judges whether the encrypted information $E(m_{num}\|r_i)$ has been transmitted. If yes, go to Step 12; if not, go to Step 4.

(Step 6) The intelligent sensor device B uses our proposed encryption/decryption algorithm for intelligent sensing information to decrypt $E(m_{num}\|r_i)$.

(Step 7) The intelligent sensor device B judges whether the encrypted information $E(m_{num}\|r_i)$ has been decrypted, if not, go to Step 6; if the decryption is completed, go to Step 8.

(Step 8) The intelligent sensor device B performs statistical analysis based on the decrypted intelligent sensing information. If $ISI\_A > ISI\_A_{\max}$ or $ISI\_A < ISI\_A_{\min}$ is established, it will alarm, and transmit the alarm information to the adjacent intelligent sensor device A, then go to Step 9; if the inequality is not established, then the intelligent sensor device B shows "success," go to Step 12.

(Step 9) The intelligent sensor device A receives alarm information, updates the stream key according to the alarm information, and sends the stream key to adjacent the intelligent sensor device B through a secret channel.

(Step 10) The intelligent sensor device B receives the stream key sent by the intelligent sensor device A, and updates the stream key.

(Step 11) After the intelligent sensor device B has updated the stream key, go to Step 1.

(Step 12) End.

3. Security Analysis

3.1. The Encryption/Decryption Algorithm of This Intelligent Sensing Information Can Effectively Resist Sliding Attacks. In the encryption/decryption algorithm of the intelligent sensing information, the intelligent sensing information to be transmitted by the intelligent sensor device is first divided into blocks, which can intercept the direct physical contact between the information modules and become independent individuals each other. The information module is not leaked out through comparative analysis, and the attack point of the sliding attack is broken down and cracked at the root cause. In addition, in the process of generating the key stream, Lorenz chaotic algorithm and Wien chaotic algorithm are used to generate the initial value and interference value. And the chaotic sequence corresponding to each plaintext block is organically combined with the plaintext to generate the key stream. Thereby, the leakage and the theft of the key can be avoided and the collision of different key pairs is intercepted. Moreover, the means and methods of sliding attacks are broken. All of these can improve the security of intelligent sensing information protection.

3.2. The Encryption/Decryption Algorithm of This Intelligent Sensing Information Can Effectively Resist Replay Attacks. In the encryption/decryption algorithm of intelligent sensing information, Lorenz chaotic map and Wien chaotic map are used to generate initial values and interference values, and the chaotic sequence corresponding to each plaintext block is organically combined with the plaintext to generate a key stream, so that the keys used for each information block are not the same. Even if the attacker intercepts and records the data from the intelligent sensor device A to the adjacent intelligent sensor device B at a certain moment (stream, block), the attacker still cannot intercept the data at the next moment (stream, block) from the stolen data because the key is constantly changing and different data streams and different data blocks correspond to different keys. Therefore, this intelligent sensing information encryption/decryption algorithm can effectively resist replay attacks.

3.3. The Secure Transmission Algorithm of Intelligent Sensing Information Can Effectively Prevent the Access of Unauthorized Users and Other Illegal Users. In the secure transmission algorithm of intelligent sensing information, the intelligent sensing information is first divided into blocks and encrypted in term of the form of a plaintext stream by the sent intelligent sensor device. In the entire transmission processes, the intelligent sensing information appears in term of the form of ciphertext. At the same time, the mutual authentication between the sending intelligent sensor device and the receiving intelligent sensor device will be performed before the ciphertext is transmitted. Therefore, this method can effectively prevent the access of unauthorized users and other illegal users and protect the security of intelligent sensing information transmission.

3.4. The Security Transmission Algorithm of This Intelligent Sensing Information Has High Security Performance. In the process of transmission and reception of intelligent sensing information, the effectiveness of security protection of intelligent sensing information is often affected by the anti-attack properties of the encryption/decryption algorithm and the secure transmission algorithm of intelligent sensing information. However, in the encryption/decryption mechanism using the stream key the attack resistance is usually directly related to the number of subkeys. In our proposed secure transmission algorithm of intelligent sensing information, the source intelligent sensor device can decide whether to authorize and transmit according to the warning message of the adjacent intelligent sensor device. Thereby, it can reduce the error calculation and the transmission of key stream. Moreover, it can also reduce the calculation complexity of the subkey. All of these can enhance the integrity and the security of intelligent sensing information transmission.

3.5. The Secure Transmission Algorithm of Intelligent Sensing Information Can Effectively Protect Its Integrity during the Transmission Process. In the transmission process of intelligent sensing information, the intelligent sensor devices usually adopt encryption/decryption algorithms to protect intelligent sensing information. Therefore, a certain amount of additional overhead is generated for the intelligent sensor devices because of using the encryption/decryption algorithms. And the loss of information may be caused for the intelligent sensor devices. All of these has a certain impact on the efficiency of information transmission. Of course, different encryption/decryption algorithms have different additional costs for their intelligent sensor devices. Thus, the corresponding transmission efficiency of intelligent sensing information may be also different each other.

In our proposed secure transmission algorithm of intelligent sensing information, the intelligent sensing information that needs to be transmitted by the intelligent sensor is divided into blocks, which can reduce the transmission time of each information block and enhance the difficulty for illegal users to aggregate intelligent sensor information. Thus, the possibility of information block from being stolen or modified will be reduced. Moreover, it is more difficult for illegal users to steal information since each information block uses a different key. Therefore, the secure transmission algorithm of the intelligent sensing information can effectively protect the integrity of intelligent sensing information during the transmission process.

4. Experiments and Results Analysis

In this section, we first introduce the experiments and the composition of experimental components. Then, we describe a series of experiments. At last, we analyze the experiment results. The specific process can be described as follows.

4.1. Experiments. In our experiments, we construct two different transmission modes of intelligent video sensing information transmission, respectively. One is not to use any secure transmission mechanism, and the other is to use our proposed security transmission and early warning mechanism for intelligent sensing information in the intelligent video monitor and the server of the Internet of Things.

These intelligent video monitors mainly include video image sensor module, timing control module, signal processing module, power management module, communication transmission module and so on. The video image sensor module has the function of static electronic shutter and the adjustable function of the integration time, and can continuously monitor the fixed area for a long time. The video image sensor module integrates analog signal processing circuit, I^2C bus control interface, exposure/white balance control, video timing generation circuit, digital conversion circuit, row selection, column selection and amplification, photosensitive unit array, and so on. The timing control module is mainly used to set the working mode of the video image sensor module and control its exposure and readout. The main function of the signal processing module is to encode for the image datums which are outputted by the video image sensor and transmit these encoded image datums to the communication transmission module. The power management module provides the required working voltage for all components of the whole board. Although there is a separate communication transmission module in the two transmission modes, they aren't the same.

In the first transmission mode, the communication transmission module only contains communication functions. The main reason is that it only includes some transmission protocols and does not to use any secure transmission mechanism. In the second transmission mode, the communication transmission module contains not only the communication functions but also the encryption/decryption function and the information detection function. The main reason is that it includes not only some transmission protocols but also our proposed security transmission and early warning mechanism for intelligent sensing information. Therefore, in the second transmission mechanism, the intelligent video sensor device can not only perceive the image, but also safely transmit and warn for the perceived image information. The architecture of intelligent video monitor in different transmission mode is, respectively, shown as Figures 2 and 3.

The server mainly includes communication security management module, monitoring management module, host management module, user management module, network management module, intelligent video monitor management module, permission management module, service management module, storage management module, task management module, log management module, Information statistics management, etc. At the same time, in the first transmission mode, the communication transmission module of the server only contains communication function. The main reason is that it only includes some transmission protocols and does not to use any secure transmission mechanism. In the second transmission mode, the communication transmission module contains not only the

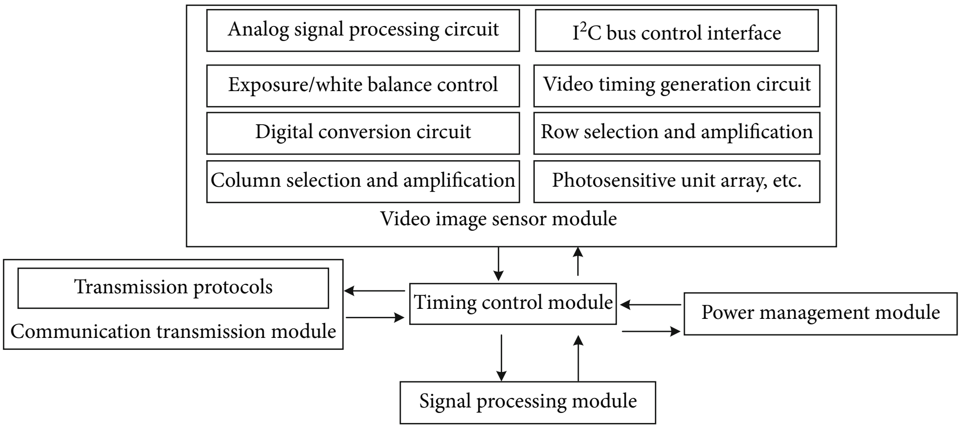
Analog signal processing circuit
I^{2}C bus control interface
Exposure/white balance control
Video timing generation circuit
Digital conversion circuit
Row selection and amplification
Column selection and amplification
Photosensitive unit array, etc.
Video image sensor module
Transmission protocols
Communication transmission module
Timing control module
Power management module
Signal processing module

Figure 2: The architecture of an intelligent video monitor in the first transmission mode.

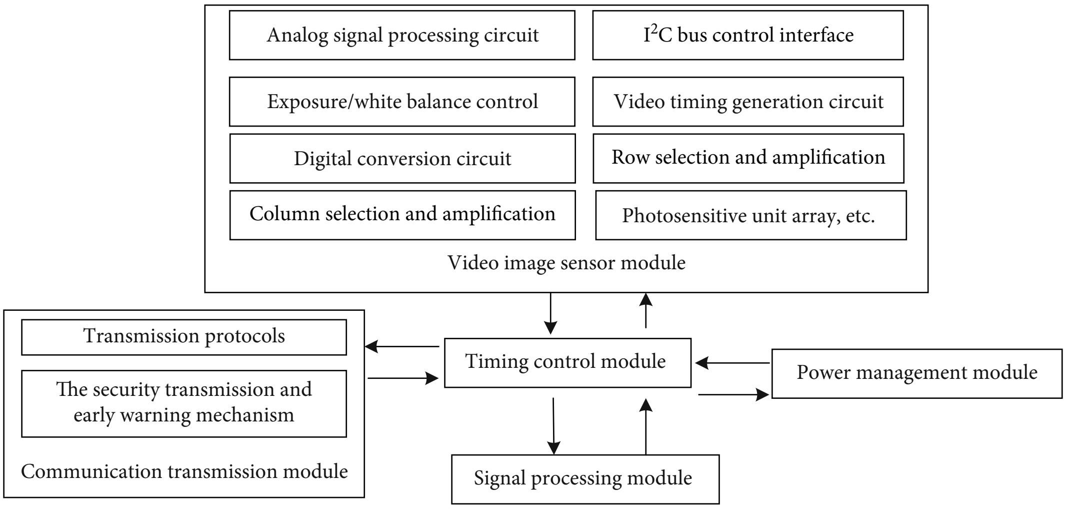
Analog signal processing circuit
I^{2}C bus control interface
Exposure/white balance control
Video timing generation circuit
Digital conversion circuit
Row selection and amplification
Column selection and amplification
Photosensitive unit array, etc.
Video image sensor module
Transmission protocols
The security transmission and early warning mechanism
Communication transmission module
Timing control module
Power management module
Signal processing module

Figure 3: The architecture of an intelligent video monitor in the second transmission mode.

communication functions but also the encryption/decryption function and the information detection function. The main reason is that it includes not only some transmission protocols but also our proposed security transmission and early warning mechanism for intelligent sensing information. The architecture of server in different transmission mode is, respectively, shown as Figures 4 and 5.

In the two different transmission modes, the server is composed of 8-node machines, each node machine contains 16 Intel Xeon CPU cores, 32G memory, 1.6 TB disk, and the operating system is simultaneous interpreting Linux 2.6.18. Node machines are connected together by network cables with a speed of 100Mbps. In the intelligent video monitor, the maximum response time (s) is set to 1.5 s, the maximum waiting time is 15 s, and the wireless area communication range (m) is 40 m.

In the experiments, the false detection rate of intelligent video sensing information and the loss rate of packet are, respectively, tested and compared. Moreover, in the two different communication modes, the corresponding intelligent video monitor faces the same external environment, such as temperature, humidity and weather.

4.2. Results Analysis

4.2.1. The False Detection Ratio of Intelligent Video Sensing Information. Figure 6 gives the situation of the false detection ratio of intelligent video sensing information with the number of intelligent video sensing information in the two different transmission mode, respectively. It can be seen from the figure that when the amount of video sensing information is the same, the false detection ratio of intelligent video sensing information is lower than that in the second transmission mode. The main reason for this situation is that our proposed security transmission and early warning mechanism is used in the second transmission mode. In the security transmission and early warning mechanism, we use our proposed encryption/decryption algorithm of intelligent sensing information, secure transmission algorithm of intelligent sensing information and early warning algorithm of intelligent sensing information. By using the encryption/decryption algorithm of intelligent sensing information and the secure transmission algorithm of intelligent sensing information, the secure transmission and the authentication of intelligent video sensing information are

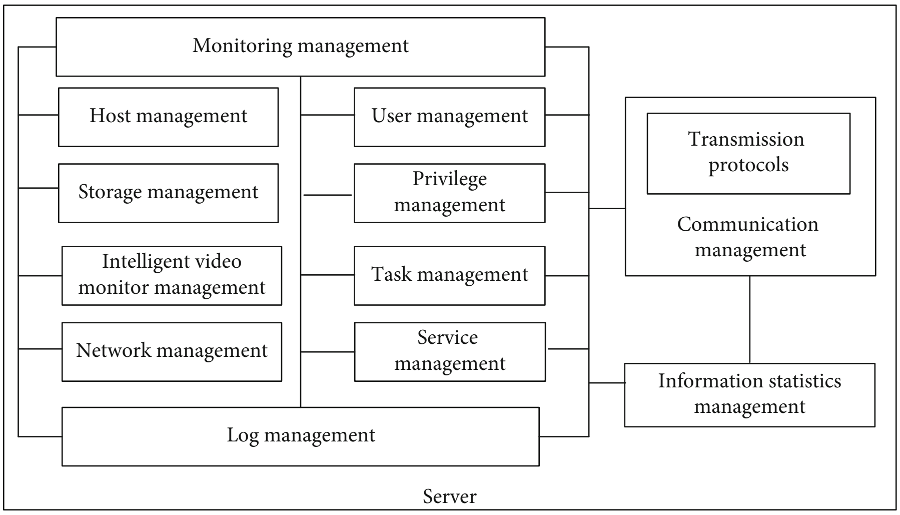

Figure 4: The architecture of a server in the first transmission mode.

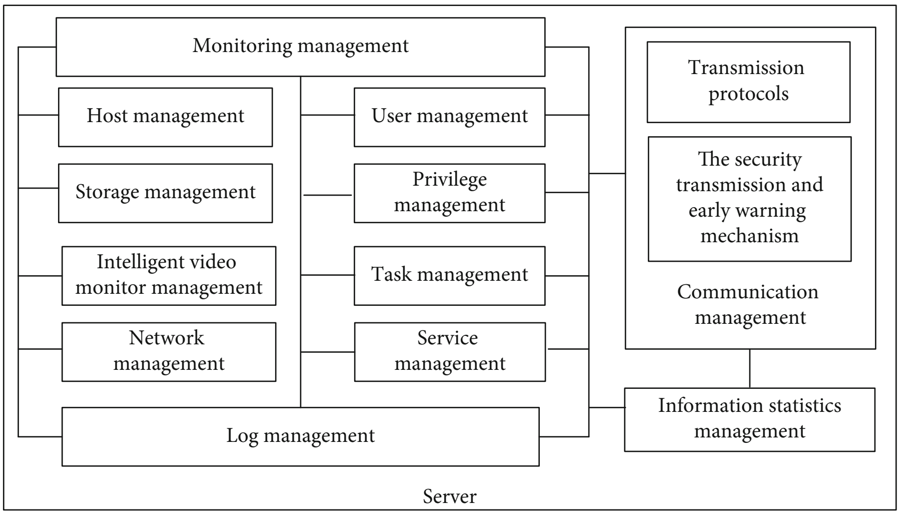

Figure 5: The architecture of a server in the second transmission mode.

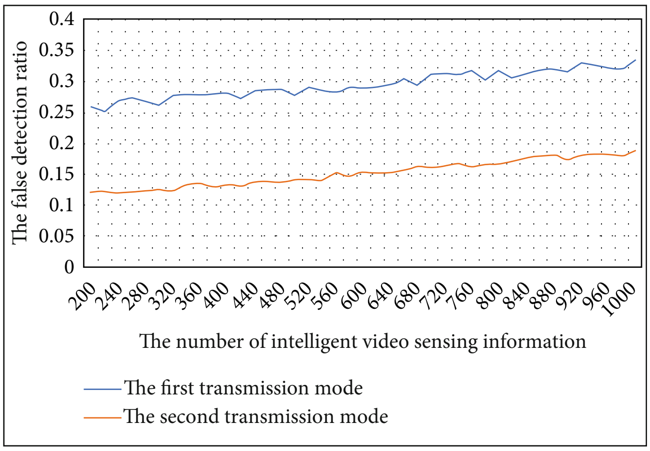

Figure 6: The false detection ratio of an intelligent video sensing information with the number of intelligent video sensing information in the two different transmission modes.

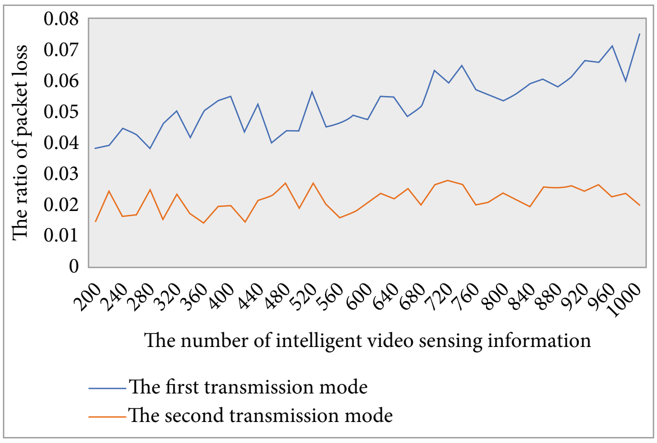

Figure 7: The ratio of packet loss with the number of intelligent video sensing information in the two different transmission modes.

ensured, and the interference and the blocking of other information are reduced. Moreover, the early warning algorithm of intelligent sensing information can realize the security early warning of intelligent video sensing information, which is conducive to the system to take a series of security measures, further reduce the interference and the blocking of other information, and reduce the probability of information false detection in the system.

4.2.2. The Ratio of Packet Loss. Figure 7 shows the ratio of packet loss with the number of intelligent video sensing information in the two different transmission mode.

From the figure, we can see that the ratio of packet loss in the first transmission mode is lower than that in the second transmission mode. The main reason for this situation is that our proposed encryption/decryption algorithm of intelligent sensing information, the secure transmission algorithm of intelligent sensing information and the early warning algorithm of intelligent sensing information are used in the second transmission mode. By using these algorithms and methods, the legitimate intelligent video sensing information can be protected from some deception or some improper accesses. All of these can improve the success rate of the target video monitor collection, transmission, accessing the packet. At the same time, these methods and algorithms can prevent illegal video monitors from cheating or sending false video sensing information. All of these can help each legitimate intelligent video monitor to correctly transmit authenticated message packets, so as to minimize packet loss and reduce the ratio of packet loss.

5. Conclusions and Future Work

Based on potential security threats, this paper proposes a method to improve the security of intelligent sensing information. The method mainly includes three phases, namely, the encryption/decryption phase of intelligent sensing information, the secure transmission algorithm phase of intelligent sensing information, and the early warning phase of intelligent sensing information. At each phase, we explained the specific steps of the algorithm in detail. In addition, this paper uses this method to analyze the security of common attack forms and confirm the security of the algorithm. At the end of this paper, we describe a series of experiments and analyze the experiment results. These results show that our proposed security transmission and early warning mechanism is very effective in the Internet of Things.

This paper only proposes secure encryption algorithm and does not involve blockchain or machine learning to enhance the security of the Internet of Things. In addition, different encryption/decryption algorithms have different additional costs for their intelligent sensor devices, and their transmission efficiency is also different. The algorithm may be affected by many factors, and under some conditions, the efficiency of the algorithm may be affected. In future work, we will continue to optimize the encryption algorithm to better adapt to the environment of the Internet of Things and further consider the security of the Internet of Things under 5G references.

Data Availability

The data used to support the findings of this study are included in the article.

Conflicts of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

The work was supported by the National Key R&D Program of China and by the Key Lab of Information Network Security, Ministry of Public Security.

References

[1] H. Wang, L. Jiang, and P. Xiang, "Priority design parameters of industrialized optical fiber sensors in civil engineering," *Optics & Laser Technology*, vol. 100, pp. 119–128, 2018.

[2] H. Wang, L. Jiang, and P. Xiang, "Improving the durability of the optical fiber sensor based on strain transfer analysis," *Optical Fiber Technology*, vol. 42, pp. 97–104, 2018.

[3] R. Min, C. Marques, O. Bang, and B. Ortega, "Moire phase-shifted fiber Bragg gratings in polymer optical fibers," *Optical Fiber Technology*, vol. 41, pp. 78–81, 2018.

[4] A. G. Leal-Junior, A. Frizera, C. Marques, and M. J. Pontes, "Optical fiber Specklegram sensors for mechanical measurements: a review," *IEEE Sensors Journal*, vol. 20, no. 2, pp. 569–576, 2020.

[5] M. A. Kandi, H. Lakhlef, A. Bouabdallah, and Y. Challal, "A versatile key management protocol for secure group and device-to-device communication in the Internet of Things," *Journal of Network and Computer Applications*, vol. 150, p. 102480, 2020.

[6] X. Yi and W. Dong, "An item-level access control framework for inter-system security in the internet of things," *Applied Mechanics and Materials*, vol. 548-549, pp. 1430–1432, 2014.

[7] N. Bruce, L. Hoon-Jae, and L. Sang-Gon, "Security analysis and improvements of authentication and access control in the internet of things," *Sensors*, vol. 14, no. 8, pp. 14786–14805, 2014.

[8] S. Gusmeroli, S. Piccione, and D. Rotondi, "A capability-based security approach to manage access control in the internet of things," *Mathematical and Computer Modelling*, vol. 58, no. 5-6, pp. 1189–1205, 2013.

[9] O. Aafaf, B. P. Imane, A. E. Anas, and A. O. Abdellah, "Security analysis and proposal of new access control model in the Internet of Thing," in *Proceedings of 2015 International Conference on Electrical and Information Technologies*, pp. 30–35, Marrakech, Morocco, 2015.

[10] H. Qinlong, Y. Yixian, and W. Licheng, "Secure data access control with ciphertext update and computation outsourcing in fog computing for internet of things," *IEEE Access*, vol. 5, pp. 12941–12950, 2017.

[11] L. Logrippo, "Multi-level models for data security in networks and in the Internet of things," *Journal of Information Security and Applications*, vol. 58, article 102778, 2021.

[12] P. Kendrick, A. Hussain, N. Criado, and M. Randles, "Multi-agent systems for scalable internet of things security," in *Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing*, pp. 1–6, Cambridge, United Kingdom, 2017.

[13] A. Yang, Y. Li, F. Kong, G. Wang, and E. Chen, "Security control redundancy allocation technology and security keys based on internet of things," *IEEE Access*, vol. 6, pp. 50187–50196, 2018.

[14] M. Ammar, B. Crispo, B. Jacobs, D. Hughes, and W. Daniels, "SμV–The security microvisor: a formally-verified software-based security architecture for the internet of things," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 5, pp. 885–901, 2019.

[15] S. Siboni, V. Sachidananda, Y. Meidan et al., "Security testbed for internet-of-things devices," *IEEE Transactions on Reliability*, vol. 68, no. 1, pp. 23–44, 2019.

[16] M. Kamals and M. Tariq, "Light-Weight security and data provenance for multi-hop internet of things," *IEEE Access*, vol. 6, pp. 34439–34448, 2018.

[17] F. Ullah, H. Naeem, S. Jabbar et al., "Cyber security threats detection in internet of things using deep learning approach," *IEEE Access*, vol. 7, pp. 124379–124389, 2019.

[18] S. V. Pechetti, A. Jindal, and R. Bose, "Exploiting mapping diversity for enhancing security at physical layer in the internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 532–544, 2019.

[19] M. Bala Krishna and P. Lorenz, "Location, context, and social objectives using knowledge-based rules and conflict resolution for security in internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 407–417, 2021.

[20] M. Bradbury, A. Jhumka, and C. Maple, "A spatial source location privacy-aware duty cycle for internet of things sensor networks," *ACM Transactions on Internet of Things*, vol. 2, no. 1, pp. 1–32, 2021.

[21] L. Jiang, R. Tan, X. Lou, and G. Lin, "On lightweight privacy-preserving collaborative learning for internet of things by independent random projections," *ACM Transactions on Internet of Things*, vol. 2, no. 2, pp. 1–32, 2021.

[22] Y. Khazbak, J. Qiu, T. Tan, and G. Cao, "TargetFinder," *ACM Transactions on Internet of Things*, vol. 1, no. 3, pp. 1–23, 2020.

[23] D. Brown, A. Hedayatipour, M. B. Majumder, G. S. Rose, N. McFarlane, and D. Materassi, "Practical realisation of a return map immune Lorenz-based chaotic stream cipher in circuitry," *IET Computers & Digital Techniques*, vol. 12, no. 6, pp. 297–305, 2018.

[24] R. Kiliç and F. Yildirim, "A survey of Wien bridge-based chaotic oscillators: Design and experimental issues," *Chaos, Solitons & Fractals*, vol. 38, no. 5, pp. 1394–1410, 2008.

[25] D. Chen, D. Qing, and D. Wang, "AES key expansion algorithm based on 2D logistic mapping," in *2012 Fifth International Workshop on Chaos-Fractals Theories and Applications*, pp. 207–211, Dalian, China, 2012.