Information Security Transmission Technology in Internet of Things Control System

https://doi.org/10.3991/ijoe.v14i06.8707

Ying Zou(✉)
SiChuan Judicial and Police Officers Professional College, DeYang SiChuan, China
zouyinghilton@163.com

Jiezhuo Lv
Southeast University, NanJing JiangSu, China

Abstract—To solve the information security problem in Internet of things control system, the information security transmission technology was mainly discussed and studied, and the basic structure of networking control system was analyzed. From the main control equipment, communication equipment, control equipment, monitoring equipment, information storage device, connecting equipment and other aspects, the further research was carried out. Secondly, the structure of the Internet of things was studied, the security problems which may exist were discussed, and it was analyzed from the access security, transmission security and delays stability safety three aspects. Finally, the information security transmission technology based on the Internet of things control system was explored, and the encryption technology, authentication technology and isolation technology were analyzed in detail. The results showed that the networking control system not only had the advantages of transmission reliability, convenient interaction, and simple assembly, but also had the strengths of disperse structure, real-time data, remote monitoring and others. At last, it is summed up that the existing reliable communication resources are maximized in the transmission mechanism of the Internet of things.

Keywords—Internet of Things, control system, information security

1 Introduction

Network control system is a new control system, which is developed with the rapid development of control technology, network technology and computer application technology. Its emergence is in line with the development trend of modern science and technology. It also reflects in mutual intersection, mutual penetration and mutual integration between various discipline theories and applications in the field of modern science and technology with information science as backbone. As a result, the control field pays special attention to the network control system. Norbert Weiner, the founder of cybernetics, pointed out that control researchers should constantly apply new science and new ideas in the control system. These new science and new ideas pro-

vide rich opportunities for researchers to innovate and help control systems move to go towards new future. Therefore, the concept of IOT provides new opportunities and challenges for networked development of control system. The control system based on Internet of things will become one of the development directions of next generation control system. The Internet of things control system can be said to be the extension and expansion of modern network control system. It is similar to that the Internet of things is the extension and expansion of the Internet. This research will analyze the definition, basic structure and application advantages of the Internet of things control system, and profoundly discuss the technology of information security output.

2 State of the art

A closed loop control system generated through the network is called network control system. The Internet of things control system refers to the system with Internet of things as the communication medium, to interconnect the control system elements so that the related information can be safely interacted and shared, so as to achieve the desired control objectives. In the Internet of things control system, the components of the control system include sensors, intelligent controllers, actuators, management equipment and so on. At the same time, the control relevant information refers to the sampling information, monitoring information, control decision results, control command, control program, device parameter information, product parameter information, equipment state, control state, control rules, control decision, control objectives and other related information. As a result, the control goal means the ultimate control goal that the whole control system will realize.

The foreign scholars discussed information security transmission technology from various aspects. Kim, S. and Na, W. [1] proposed the safe data transmission architecture for the Internet of things ecosystems, which was a kind of software defined network base cloud and it could provide the safe data transmission. Budiyanto, S. et al. [2] evaluated the performance of various data transmission technique on IP over Radio, so as to determine which data transmission that is the best for supporting the Internet of things system. Lee, J. H. et al. [3] proposed a fast intra-prediction unit decision method to reduce the computational complexity of the HEVC RExt encoder, which was closely related to Internet of things control system. Saha, A. et al. [4] put forward a context-aware adaptive pattern-based ME algorithm for multimedia Internet of things platform to improve video compression and performance of Internet of things control system. Yildirim, E. Y. et al. [5] discussed the major factors affecting information security management in small-and medium-sized enterprises to examine the performance of enterprise information security transmission.

A lot of domestic researchers also studied the information security transmission technology and discussed the technology of Internet of things. Li [6] proposed a heterogeneous ring sign-cryption scheme for secure communication from sensors to servers and applied information security transmission technology in the control of Internet of things. Lin and Wei [7] put forward a two-stage scheme to control preamble transmission in multiple periods so as to ensure the safe transmission of infor-

mation and improve the performance of Internet of things control system. He [8] introduced the basic concept and key technology of the Internet of things compared to the traditional environment of information technology. He also talked about the application of Internet of things of information collection, transmission and processing technology in environmental monitoring and other environmental supervision. Chen and Xu [9] made a self-developed production environment supervision and monitoring control system, including environment collecting terminal, environment controller, embedded repeater and supervision and control server. Xia et al. [10] combined Internet of things and cloud computing to develop the control system of Internet of things and make information transmission more secure.

In conclusion, the safe data transmission architecture, the performance of various data transmission technique, the major factors affecting information security management and so on are discussed. However, the information security problem in Internet of things control system is not effectively solved. To guarantee the information security, the information security transmission technology is mainly discussed and studied, and the basic structure of networking control system is analyzed. The structure of the Internet of things is studied, the security problems which may exist are discussed, and it is analyzed from the access security, transmission security and delays stability safety three aspects. Finally, the information security transmission technology based on the Internet of things control system is explored in detail. The networking control system not only has the advantages of transmission reliability, convenient interaction, and simple assembly, but also has the strengths of disperse structure, real-time data, remote monitoring and others. At last, it is summed up that the existing reliable communication resources are maximized in the transmission mechanism of the Internet of things.

3 An overview of the Internet of things control system

A closed loop control system generated through the network is called network control system. The Internet of things control system refers to the system with Internet of things as the communication medium, to interconnect the control system elements so that the related information can be safely interacted and shared, so as to achieve the desired control objectives. In the Internet of things control system, the components of the control system include sensors, intelligent controllers, actuators, management equipment and so on. At the same time, the control relevant information refers to the sampling information, monitoring information, control decision results, control command, control program, device parameter information, product parameter information, equipment state, control state, control rules, control decision, control objectives and other related information. As a result, the control goal means the ultimate control goal that the whole control system will realize.

3.1 Basic structure of the Internet of things control system

In order to achieve its control goal, the Internet of things control system should include at least the following parts: the control part, the controlled part, the control link and the feedback link. From this concept, the building model diagram of the Internet of things (IOT) control system is shown in Figure 1. The main functions of each part are as follows.

Equipment 1: main control equipment, which mainly refers to the intelligent agent controlling whole process of control and entire control system, including intelligent controller, intelligent computer, intelligent industrial control computer, intelligent control software in intelligent PDA, hardware devices and people.

Equipment 2: communication equipment, including computer, PDA, mobile phone and embedded devices, to enable authorized users to remotely control and state monitor the control equipment through the Internet. In the control end, a separate set of control communication equipment, but not putting control equipment or monitoring equipment, intends to meet the requirements of real time of data transmission and security, so as to enhance the operation and processing speed.

Equipment 3: control device, which is usually embedded intelligent controller. It controls the operation of terminal devices by receiving control commands or control programs from communication devices.

Equipment 4: monitoring equipment, including temperature sensor, sound sensor, vibration sensor, pressure sensor and signal acquisition devices, used for collecting control terminal and control equipment required information, and giving feedback to the control terminal through communication equipment. The emergency stop controller is to ensure that when a fault occurs, a charged part can urgently stop operation, thus making the losses reduced to the minimum.

Equipment 5: information storage device, which is used for recording the interaction information between authorized users and control system. The video monitoring device is to store the actual running state of control system. The two devices are to analyze the accuracy and safety of the whole system in the initial stage. When it is confirmed that the whole system is mature, these two devices can be removed, so we use the dashed line to mark in Figure 1.

Equipment 6: connect devices. This part is not shown in the map. It mainly refers to the information exchange and interconnection between different devices of the system. With Internet of things as the main part, it includes wired connection and wireless connection, so as to facilitate system establishment and equipment replacement.

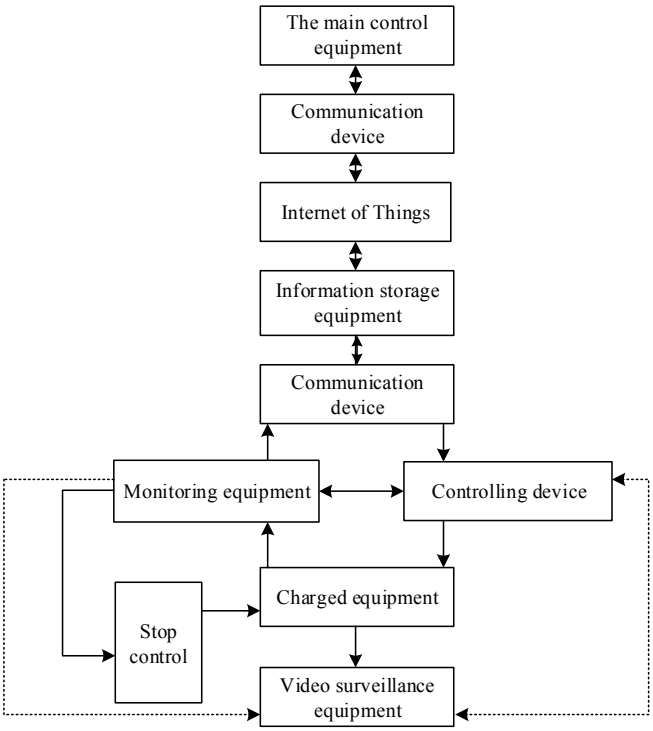

Fig. 1. Model architecture of Internet of things control system

3.2 Advantages of the Internet of things control system

The control system of the Internet of things can be said to be a comprehensive extension of the networked control system and the distributed control system rather than a simple addition of the two parts. Therefore, it has its own unique advantage based on the many advantages of the two control systems. The advantages of the Internet of things numerical control system are as follows:

Advantage one: reliable transmission. It mainly refers to that the information can be safely and reliably transmitted, which is the basic requirement of Internet of things implementation. The Internet of things control system depending on IOT can be further improved on the transmission protocol and transmission mode on this basis, so as to achieve the required goals of control system.

Advantage two: convenient interaction. The information interaction between the authorized user and the equipment, the equipment and the vendor management system, as well as the equipment and the equipment will be more convenient. It should be noted that, for some authorized users, the design parameters, control procedures, control command and control process may need to be confidential. And it needs to hire manufacturers' control equipment production and their products. Now, the handling of the situation in general is that the authorized user himself manipulates the equipment on site.

Advantage three: simple establishment. In the Internet of things control system, each control element may use the wired or the wireless way to carry on the establishment. It is easy to satisfy the information interaction and the coordination work request, which has omitted the complex wiring implementation process.

Advantage four: structural decentralization. Because of the convenience of terminal devices into the network, it can make the whole control structure highly dispersed, instead of placing each control element in a unified geographical location.

Advantage five: real-time data. In the Internet of things control system, theoretically, each device can communicate information between each other. It can also make the control information and production information to interact with the management system in a timely manner, so as to facilitate the establishment of a comprehensive and real-time data repository.

Advantage six: remote monitoring. Through Internet of things, information exchange with remote terminal technical personnel can be conducted by the control system. Therefore, technical staffs can make remote monitoring and remote fault diagnosis, which can help to reduce maintenance costs and save a lot of manpower and financial resources.

4 Internet of things architecture and analysis of security problems

The Internet of things is a compound and complex system of diversified forms. The system and architecture of the Internet of things can be divided into three levels: the perception layer, the network layer and the application layer, and each level can involve a lot of relevant information technologies. The three-layer architecture diagram of the Internet of things is illustrated in Figure 2.

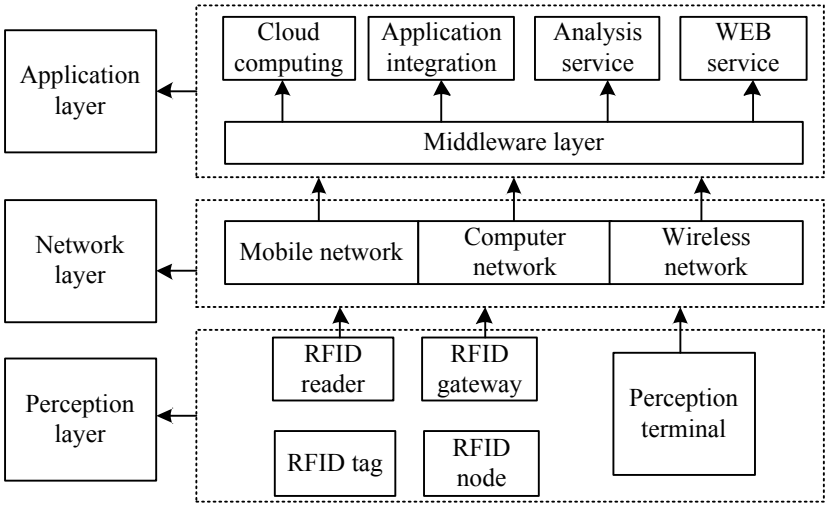

Fig. 2. Three-layer architecture map of the Internet of things

In terms of the structure of the control system of the Internet of things, attacks on it can be divided into the following categories: passive attack, active attack, physical proximity attack, internal personnel attack and hardware and software configuration attack. Because the control system of the Internet of things may be attacked by various kinds, it is necessary to discuss the safety objectives of the control system of the Internet of things. It aims at developing a security service strategy for them, so as to achieve the purpose of protecting the system security. The security goals of the IOT control system are mainly manifested in the security, integrity, reliability, availability, non-repudiation and controllability of the system.

The Internet of things control system security mainly includes three aspects. The first is access security. Due to the widespread of Internet of things, anyone, at any time and any place, can access to the control system of service providers through the Internet of things, and monitor and operate the bottom generating equipment, which is obviously not reasonable. This requires shielding of unauthorized users and only allowing authorized users to access security. The second is transmission security. In the communication process of control system of authorized users and service providers, illegal attacker can monitor the transmission information of cable network and wireless network, and steel and tamper important information. It leads to a leakage and relief of trade secrets and decrease in manufacturers' credit, which will bring a huge threat to authorized users and manufacturers. To solve this problem is one of the basic things to implement Internet of things control system. The last one is the stability and the safety of delay. In the process of Internet of things transmission, information will go through the wireless network and wired network. Therefore, it will bring the transmission delay and decision treatment time delay. As a result, it may cause a threat to the stability of the whole control system, which is one of the problems that need to be solved for implementing Internet of things control system.

5 Information security transmission technology of Internet of things

5.1 Encryption technology

Encryption technology is the core of information security technology, and it has an irreplaceable position in the security of the entire Internet of things. Encryption technology uses cryptographic algorithm to transform plain-text into cipher-text information and transmit to the receiving end. The legitimate receiver then uses the prior secret pin to restore the cipher-text into plain-text information by decryption algorithm. The encryption algorithm is also the key to the encryption technology. The commonly used encryption algorithms are symmetric encryption algorithm, asymmetric encryption algorithm, Hash algorithm and so on.

In block ciphers, DES, 3DES and AES are more commonly used. Among them, the DES algorithm is using the key of 56bit to encrypt the 64bit cipher-text message group, and the length of the encrypted cipher-text packet is also 64bit. The specific encryption process is shown in Figure 3.

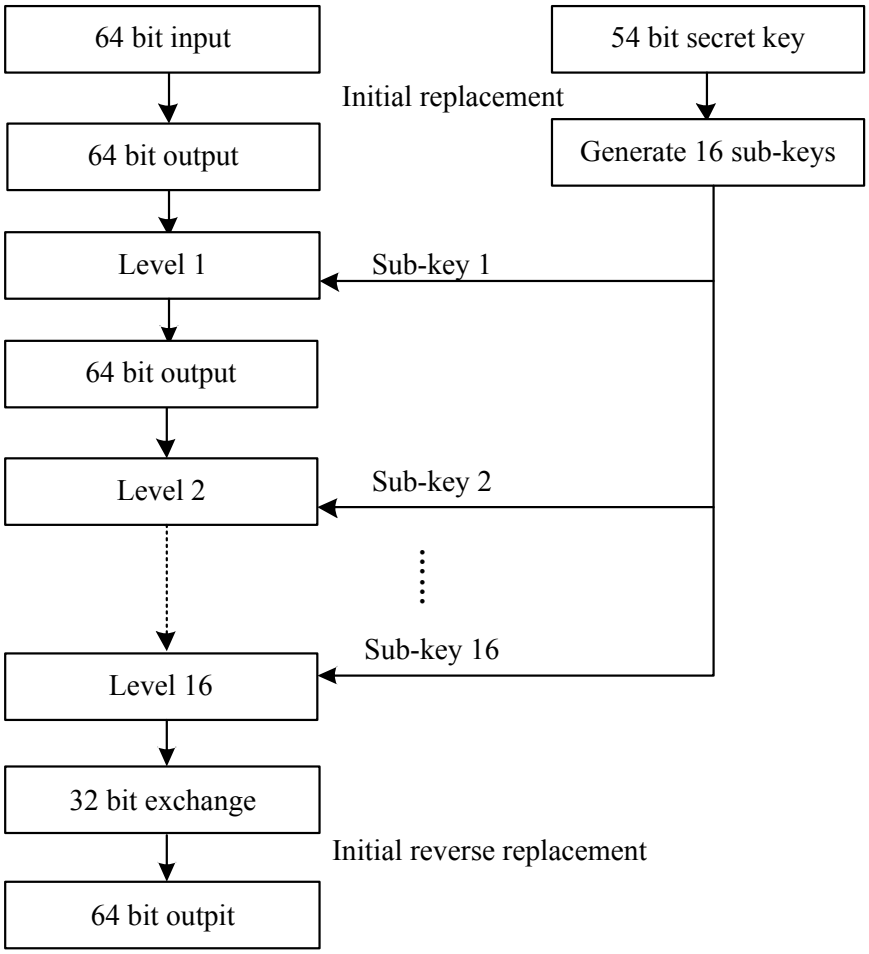

Fig. 3. The overall framework of guide teaching system

As shown in Figure 4, the DES encryption process is a sub key that generates 16 48bit before the key of the 54bit. After that, the first group of 64bit's plain-text input is initially replaced, and the output of 64bit is obtained. The output is obtained by the first round operation under the action of the key 1, and the output result is obtained. By analogy, under the action of 16 sub keys, after 16 rounds of operations, the input of 64bit is divided into left and right 32bit output. Then the left and right data are transferred to each other, and finally, the initial inverse replacement is performed to get the output of 64bit packet cipher-text.

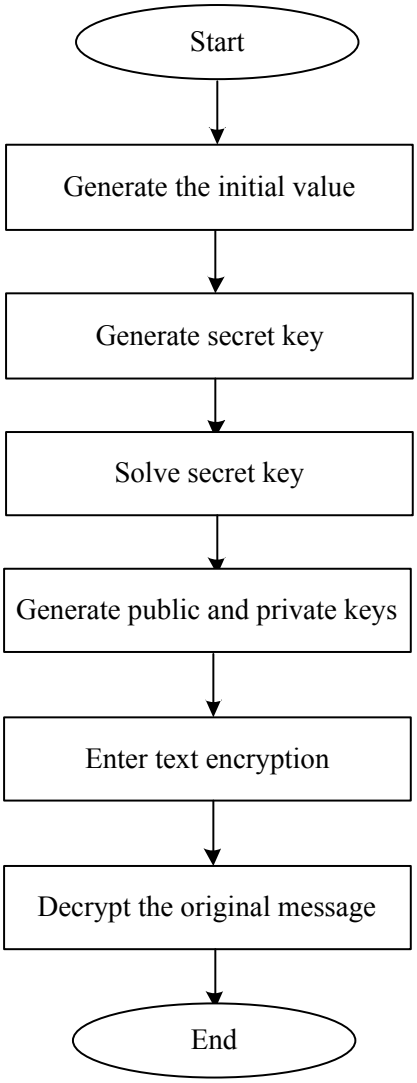

Fig. 4. RSA algorithm flow chart

The security of RSA depends on the large number decomposition. Both the public key and the private key are two large prime numbers. According to the analysis, the difficulty to deduce the plain-text from a key and cipher-text is equal to the decomposition of two large prime numbers, which is a difficult problem in the mathematical field. Therefore, the RSA algorithm has high security and reliability. Figure 5 shows the flow chart of the RSA algorithm implementation.

Hash algorithm: it is also called Hash function. The design of Hash functions cannot be decrypted, that is, it can only be encrypted. Its application is very wide, such as digital signature, message integrity detection, message non-repudiation detection and

so on. Hash algorithm is an algorithm that maps any message of any length into a fixed length message, which is called an information summary or a hash value. The following Hash algorithm is unified as the Hash function. A Hash function must be strictly characterized by unidirectional and collision constraints, which can be considered as a secure Hash function. Unidirectional feature is the irreversibility of its operating direction. That is, the Hash function operation can only derive output from the input, and it is extremely difficult to push back. Collision constraint means that no input can be found, so that the output result is equal to another known output result, or two different inputs cannot be found at the same time to make the output result exactly the same. The advantages and disadvantages of symmetric and asymmetric encryption algorithms and hash algorithms are compared, as shown in Table 1.

Table 1. Comparison of the advantages and disadvantages between symmetric and asymmetric encryption algorithms and Hash algorithm

Algorithm type	Algorithm advantages	Algorithm disadvantages
Symmetric key algorithm	The algorithm is simple; the encryption speed is fast and the efficiency is high. It is suitable for a large number of data encryption, and the requirement of hardware is not high.	Security is not the best; digital signatures are not supported; large keys are difficult to manage and deliver.
Asymmetric key algorithm	The key distribution is simple and easy to manage; the information encryption and digital signature can be realized; the secrecy is high.	The computational complexity is high and efficiency for encrypting a large number of data is low; it takes up more resources
Hash algorithm	The algorithm implementation speed is fast; the security is high; and it is unidirectional hash	It cannot be used for data encryption, only for verifying data validation.

5.2 Authentication technology

In network security, encryption technology can guarantee the security of information content, and authentication technology is to ensure the security of the information system. The main purpose of certification has two points. Firstly, authentication is to verify the reliability of the sender's identity, that is, to prevent the identity of the sender from being impersonating. Secondly, authentication is to verify the integrity of the received information, that is, whether the authentication information is tampered or destroyed in the process of transmission. The essence of authentication is also very easy to understand, namely the authenticated password. There are some special information commands and hardware and so on in the authenticated part, and in addition to its own part, any third party cannot forge. The authentication process is the process that the authenticated part shows its own special information and thus allows the authentication part to recognize its identity. Because of the different authentication objects, the authentication methods can be divided into message authentication, digital signature and identity authentication. Specific authentication requirements and methods are described in Table 2.

Table 2. Authentication technology explanation

Authentication name	Authentication purpose	Specific authentication method
Message authentication	Message integrity authentication, message source authentication, and message timing identification	Message authentication code (MAC), public key encryption algorithm, hash algorithm and public key encryption algorithm combined application, time-stamp, etc.
Digital signature	Message integrity authentication, message source authentication, and signers non-repudiation verification	Public key signatures (RSA, ECC, etc.) and hash algorithm (MDS, SHA-1, etc.)
Identity authentication	Identification of the sender's identity and legitimacy	Password authentication method (command, key password, etc.), property verification (identity card, message digest, etc.), biometric feature verification method (DNA, fingerprint and handwriting) and smart card authentication

5.3 Isolation

Nowadays, the vast majority of enterprises, military, government and other internal networks should be interconnected with the public network to achieve the purpose of information exchange. However, because of the widespread and complex public network, the network attackers are trying to invade the internal network nodes and obtain the internal network information. Once the invasion is successful, not only a large number of confidential information have been leaked, but also a joint attack may be produced, resulting in a greater range of internal losses. Therefore, a certain safety isolation measures are essential to the security of the internal and external network.

Network isolation technology actually refers to the security barrier set between networks in different security domains. The goal is to isolate harmful network attacks. The premise of such isolation is to ensure that the internal information is not leaked, and at the same time, secure data exchange between trusted network and untrusted network is realized. Network isolation technology originates from the original security technology, makes up for the shortcomings of the original security technology, and has its own unique advantages. The general network isolation technology is based on the idea of access control as strategy and physical isolation as the basis, and it defines related constraints and rules to ensure the security strength of the network.

At present, network isolation technology is divided into various forms, the most important, such as logical isolation, physical isolation and so on. Their essence is the isolation of data or information. Logical isolation is an internal and external network that is physically connected, but it is logically isolated by the corresponding technical means. The classification of logical isolation is shown in Figure 5 and its detailed description is shown in Table 3.

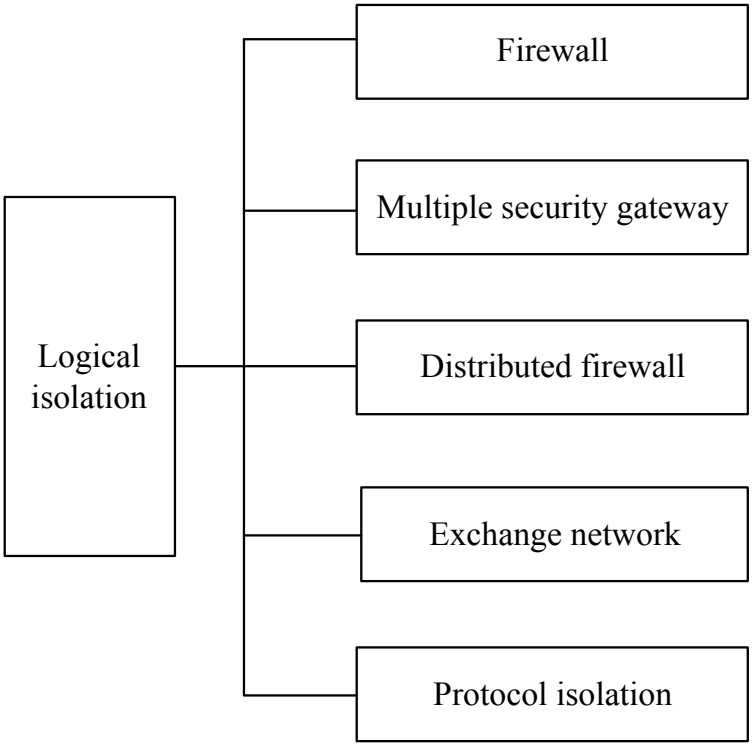

Fig. 5. Classification of logical isolation

Table 3. Logical isolation classification explanation

Logical isolation	Explanation
Firewall	The flow direction of the packet is controlled by controlling the network routing to control the communication lines. It includes a filter firewall, a state detection firewall and a proxy service firewall.
Multiple security gateways	It is an upgraded version of the firewall that can make the entire check from the network layer to the application layer.
Distributed firewall	It is made up of network firewall, host firewall and central management system. It can extend the firewall's security protection system to all hosts and terminal desktops in the network.
Switching network	A data exchange area is established between two isolated networks, which is responsible for the exchange of business data (one-way or two-way).
Protocol isolation	The connection of the original communication protocol is blocked by a special protocol or storage, and only the information transmitted by the system can be passed.

6 Conclusions

At present, the research on the Internet of things and network control system is one of the research hot-spots in modern control field. Through the research and analysis on information security transmission technology in the control system, one of the new directions of development of the control system will be Internet of things control system. The Internet of things control system is based on cryptography, with network security system and control system as the framework, as well as various security basic technologies and application technologies as the foundation. Its means and methods are network security control, and its purpose is to reduce the control cost and security risk of control network as much as possible. The following main conclusions were drawn:

Firstly, the Internet of things technology ensures the confidentiality, integrity, availability, reliability, non-repudiation and timeliness of control information, and finally completes the control target.

Secondly, the information security transmission technology based on Internet of things control system has certain practical significance in optimization of information safety information transmission technology based on Internet of things control system.

Thirdly, the existing reliable communication resources are maximized in the transmission mechanism of the Internet of things.

7 References

[1] Kim, S., & Na, w. Safe data transmission architecture based on cloud for internet of things. Wireless Personal Communications, 2015, vol. 86.1, pp. 1-14.

[2] Budiyanto, S., Nugroho, A., Nugraha, B., & Sirait, F. Ip over radio: a performance evaluation for internet of things system with various data transmission technique. Advanced Science Letters, 2017, vol. 23(6), pp. 5581-5583. https://doi.org/10.1166/asl.2017.7426

[3] Lee, J. H., Jang, K. S., Kim, B. G., Jeong, S., & Jin, S. C. Fast video encoding algorithm for the internet of things environment based on high efficiency video coding. International Journal of Distributed Sensor Networks, 2015, vol. 6, pp. 4. https://doi.org/10.1155/2015/146067

[4] Saha, A., Lee, Y. W., Hwang, Y. S., Psannis, K. E., & Kim, B. G. Context-aware block-based motion estimation algorithm for multimedia internet of things (iot) platform. Personal & Ubiquitous Computing. 2017, vol. (7), pp. 1-10.

[5] Yildirim, E. Y., Akalp, G., Aytac, S., & Bayram, N. Factors influencing information security management in small-and medium-sized enterprises: A case study from Turkey. International Journal of Information Management, 2011, vol. 31(4), pp. 360-365. https://doi.org/10.1016/j.ijinfomgt.2010.10.006

[6] Li, F., Zheng, Z., & Jin, C. Secure and efficient data transmission in the internet of things. Telecommunication Systems, 2016, vol. 62(1), pp. 111-122. https://doi.org/10.1007/s11235-015-0065-y

[7] Lin, G. Y., & Wei, H. Y. Auction-based random access load control for time-dependent machine-to-machine communications. IEEE Internet of Things Journal, 2016, vol. 3.5, pp. 658-672. https://doi.org/10.1109/JIOT.2015.2480070

[8] He, G. M. Analysis of the application of the internet of things technology in environmental monitoring. Applied Mechanics & Materials, 2015, vol. 733(6), pp. 796-799. https://doi.org/10.4028/www.scientific.net/AMM.733.796

[9] Chen, C., & Xu, X. Design and application of traceability and supervision platform for broiler based on internet of things. Nongye Gongcheng Xuebao/transactions of the Chinese Society of Agricultural Engineering, 2017, vol. 33(5), pp. 224-231.

[10] Xia, M., Li, T., Zhang, Y., & Silva, C. W. D. internet of things and cloud computing. Computer Networks the International Journal of Computer & Telecommunications Networking, 2016, vol. 101(c), pp. 5-18.

8 Authors

Ying Zou is with the SiChuan Judicial and Police Officers Professional College, DeYang SiChuan 618000, China.

Jiezhuo Lv is with Southeast University, NanJing JiangSu 211189, China.

Article submitted 27 January 2018. Resubmitted 23 February 2018. Final acceptance 01 March 2018. Final version published as submitted by the authors.