Analysis of Internet of Things Computer Network Security and Remote Control Technology

Mei Wang¹, Baohua Zhang

Company: Changzhou Vocational Institute of Engineering, 213000

¹mwang@czie.edu.net

Abstract: The Internet of Things system is a product of the combination of information technology in the rapid development of computer technology, and it is an important foundation for the development of the information age. But we cannot ignore computer network security issues in the application of the Internet of Things. In order to effectively control the security issues of the Internet of Things, we have to study and analyze the potential security risks in the current Internet of Things computer network. In addition, we should explore reliable network security control measures and computer remote control technology. Only in this way can the further development of the IoT system be promoted.

1. Overview of the Internet of Things

The Internet of Things is a goods-connected system based on the Internet. It is an extension and extension of the Internet of Things network in the development and application process. There are many types of technologies involved in the actual application of the Internet of Things. The technical content of the Internet of Things mainly includes GPS positioning technology, radio frequency technology, ubiquitous computing technology, and infrared sensors. In the actual application of the Internet of Things, we need to use the data protocol as the core to complete the data connection of any item, and carry out data communication and information exchange at the same time. The main role of the Internet of Things is to improve the automation and intelligence level of certification positioning, tracking monitoring and management. The runtime system of the Internet of Things includes a perception layer, a transmission layer, a processing layer, and a control layer. The sensing layer can collect application information of various smart cards, sensor networks and REID tags in a timely and accurate manner during operation. In the application process, the transport layer can give full play to the advantages of Internet wireless networks, fixed networks, and computer networks to realize information exchange and communication functions. The processing layer can use cloud computing platform, data mining and intelligent computing functions to complete data information collection and processing tasks. The application layer can not only operate on applications in different fields, but it can also analyze the processed information in the actual application field. Meanwhile, the Internet of Things also can grasp the information data to determine the user's personalized and intelligent application requirements, and finally complete the connection between objects, people and objects[1].
2. Internet of Things Computer Network Security Issues

2.1 Security Issues in Perception Layer Network
The security issue of sensor network is one of the main issues affecting the security of the Internet of Things computer network. Firstly, if there is a problem with sensor network security, the node identity is vulnerable to malicious attacks. In this case, the network attacker can deploy malicious nodes within the range of perception to obtain information during data transmission. Secondly, this will seriously threaten the security and privacy of data transmission and affect the integrity of the data. Because as long as there is an error in one copy of the data in the IoT system, it will affect the judgment result of the data receiving node. As a result, the system cannot accurately evaluate the reliability of the information.

2.2 Security Issues in End Nodes
The complex and diverse characteristics of the network terminal equipment of the Internet of Things will increase the security risks of the terminal equipment. Because the network terminal equipment is in an unattended environment during operation, it is vulnerable to illegal intrusion. After entering the terminal device, the attacker can illegally pull out the UICC and use it for other purposes, which seriously affects the application security of the IoT terminal device. In addition, the attacker will also read the node information. The attacker can directly damage the terminal device and expose the non-external interface inside the device. Once the non-external interface is exposed, the attacker can obtain the session key of the terminal device and important data information, which will seriously threaten the security of the terminal node of the Internet of Things [2].

2.3 Network Communication Security Issues
The process of computer network operation needs to design communication methods based on human needs. However, the number of communication terminals is relatively small. Besides, the carrying capacity of the communication network still has certain limitations, which will increase the security problems of the communication network. First, the problem of network congestion is mainly due to
the large number of network devices. Second, when applying to the communication network, we need to use encryption algorithms to ensure data integrity. However, a single network device is the main component of the Internet of Things network, and its data transmission volume itself is relatively small. If we use more complex encryption algorithms to protect data information, this will affect the transmission speed of information and increase resource consumption.

3. Strategies for Controlling the Security of Internet of Things Computer Networks

3.1 Privacy Protection Mechanism
In order to be able to effectively control the security issues of the Internet of Things computer network, we must establish a privacy protection mechanism, which is an important foundation for ensuring the security of the Internet of Things. From a technical analysis, staff should fully apply encryption mechanisms, access control mechanisms, and authentication mechanisms when establishing privacy protection mechanisms to ensure the personal privacy of network users. (1) Authentication mechanism. It is the main function of the authentication mechanism that the data receiver accurately judges the sender's identity. In the meantime, the staff have to judge the safety and integrity of the data during data transmission. (2) Identity authentication mechanism. In order to improve the reliability of data transmission, staff need to ensure the accuracy of node identity information. This can effectively prevent unauthorized users from obtaining the transmitted data. For example, using PKI authentication in WSN can build a mutual trust relationship between terminal devices, thereby improving the reliability of information transmission. Otherwise, the staff can also use the mutual authentication mechanism to complete the identity authentication between the receiving end and the sending end to ensure the reliability of the identities of both parties. (3) Access control technology. The main function of access control technology is to authorize access to trusted IoT machines and equipment in order to achieve restricted distribution and data interaction. Take an instance, an access control list is set in each terminal node, and each node can only receive node information based on the access control list. This method helps to improve the security of the network [3].

3.2 Secure Routing Protocol
Perception layer network and communication network are two major components in the operation of the Internet of Things. There are many types of networks in the Internet of Things, among which the router protocol is based on the IP protocol. Sensors, routing algorithms, etc. are all based on tags. The security routing protocol is mainly based on wireless sensing and the location of nodes in the network to realize the protection function in the application. Using a random routing strategy can ensure that data packets are not directly transmitted from the source node to the sink node during each transmission. The actual data transmission process requires a forwarding node to realize data transmission. During data transmission, the data packet will be processed according to a certain probability, so that it will be transmitted to a certain distance from the sink node. Then, from this location, the data is transmitted to the sink node. In addition, the transmission path of the routing strategy itself is relatively random and changeable, and the transmission path can be randomly generated according to the specific conditions of the data packet during transmission. Faced with this situation, it is difficult for an attacker to obtain accurate node location information. Therefore, this data transmission method has a good security protection effect. The secure routing protocols of the Internet of Things mainly include wireless sensing and secure routing protocols, which can prevent malicious information input and illegal intrusion applications from being passed. However, these devices cannot effectively adapt to the new features of the Internet of Things during use. Because the Internet of Things has new networking features in the triple play. Although a secure routing protocol can improve the security of the Internet of Things to a certain extent, it will adversely affect the performance of the Internet of Things. At present, the two secure routing protocols have shortcomings in the process of use, so we must strengthen the design and research of secure routing protocols, and develop secure routing algorithms with strong feasibility to prevent intruders from malicious routing of the Internet of
Things attack. When designing a secure routing protocol, we can use the key mechanism to establish a secure network communication environment to ensure the security of routing information interaction. Furthermore, we can use redundant routing to transmit data packets to ensure the security and privacy of data transmission. In the design of secure routing protocols, the networking characteristics of the Internet of Things and the performance requirements of the Internet of Things are the main points we need to consider. We must ensure that the secure routing protocol has strong practicability so that the secure routing protocol can meet the operational requirements of the Internet of Things. Only in this way can we prevent bad information and illegal requests, and ensure the application effect of the Internet of Things.

3.3 Firewall and Intrusion Detection Technology

In order to improve the security of the Internet of Things computer network in the data transmission process, we can develop a firewall specially used in the Internet of Things system based on the characteristics and performance requirements of the Internet of Things network. Simultaneously, we need to develop a more secure access control strategy based on the actual development needs of the Internet of Things to achieve the purpose of isolating different types of networks. Only in this way can the security of the entire transport layer be guaranteed. At the application layer, we can also use intrusion detection technology to detect intrusion intentions and intrusion situations in time, and then take effective measures to repair the vulnerabilities of the IoT system. In the application process of intrusion detection technology, we combine the detected data information with computer resource conditions to accurately grasp the intrusion behavior. We can quantitatively analyze the acceptable network behavior characteristics and complete the setting tasks to distinguish between abnormal and potential illegal intrusions. In addition, we can effectively detect misuse intrusions. When researching and designing intrusion detection technology, we must comprehensively consider the characteristics of the Internet of Things itself and adopt an intrusion detection technology that can adapt to the Internet of Things system, and use this technology to improve the security of the Internet of Things system.

4. Internet of Things Computer Remote Control Technology

4.1 Technical Principle

The Internet of Things technology can effectively realize data communication and transmission between multiple computers in the application of remote control technology. This enables engineers to use the Internet to control multiple computers. Under normal circumstances, the implementation process of remote control technology includes the following. Firstly, use the computer of the control terminal to send instructions to operate multiple client computers to achieve the purpose of remote control. Secondly, remote control technology is a technology that uses a main computer to control one or more sub-computers. In the process of applying remote control technology, remote does not only refer to distance. Some control terminals and client devices are in the same data center. Thirdly, use the Internet to complete remote control operations based on remote control software. This can ensure the final control effect. As the main body of sending instructions, the control terminal can also view the feedback results after the instruction is executed. The client is the main body that executes the instructions issued by the control terminal and can synchronously feedback the execution result to the control terminal. We must not confuse the functions of the control and client.

4.2 Data Protocol

TCP/IP protocol is the basis of network data communication when applying remote control technology. The main function of the current IP protocol is to split data and then transmit the data in the form of data packets. Moreover, the IP protocol does not require the accuracy of the transmission result when transmitting data. The biggest disadvantage of this network protocol is that it is not reliable. When using this protocol as the basis for data transmission, the requirements for the control terminal and client device programs are relatively high. In order to realize the remote control function, we must
ensure that the control terminal and the client device program are consistent. When the TCP protocol completes data transmission, it first divides the data and then packs the data. Completing the data transmission process in the way of data flow can effectively realize the data connection between the computer and the computer. The main advantage of the TCP protocol is to ensure that data has strong continuity, accuracy and two-way arrival during transmission. When applying IP and TCP protocols, we will divide the two protocols into simple network management protocols and core protocols. Among them, the simple network management protocol mainly realizes work such as Hp Open View. The core protocol is based on UDP protocol, ERP protocol, ICMP protocol, etc. to complete the data processing process. When processing data, we can regard it as a collection of network protocols to comprehensively apply two protocols [4].

4.3 Controlled Network
A controlled network is a process of achieving control purposes and providing control services based on software or hardware. The controlled network system will take the computer as the center in the application process and make full use of data collection to form a control system. This kind of control system must abide by computer security rules when designing it to prevent leakage of user information. In addition, we need security protection. Only in this way can the entire computer system be repaired in time after a security problem occurs, and the information security can be ensured as much as possible. When in use, we need to use remote control technology to complete content transmission, and send relevant information to the main control terminal, so as to achieve remote control of the computer's switch or restart operations. Furthermore, we can also use the controlled network to control computer hardware equipment to complete file transfer and management.

4.4 Master Network
The computer network remote control system is mainly based on the main control network and the controlled network system for information and data transmission. The main control network can realize a centralized structure and a decentralized structure. The operation of the centralized structure is relatively simple and easy, but the installation cost of the centralized structure is relatively large, and it takes more time. This may affect the sharing benefits of resources. The decentralized structure itself has strong security. Compared with other structures, it is more secure and reliable when transmitting information. Although the decentralized structure will have problems in some links, the reliability and stability of the network are relatively high for the entire system. Therefore, when the system cannot be centralized structure, the decentralized structure can fully play its role to ensure the stability of the network system [5].

5. Conclusion
All in all, in the process of continuous application and promotion of the Internet of Things technology, ensuring computer network security is an important part of improving the application level of the Internet of Things system. First of all, we need to research and design security protection technologies according to the networking characteristics and performance requirements of the Internet of Things system to improve the security of the Internet of Things system in the data transmission process. Secondly, in the process of applying computer remote control technology, we also need to accurately grasp the various components of remote control technology based on the application requirements of the Internet of Things system. Only in this way can we make full use of reasonable security control strategies from the actual situation and improve the security of computer networks. At the same time, ensure the remote control level of the Internet of Things computer and promote the long-term development of the Internet of Things.

Acknowledgments
Project ID: CDGZ2019043
Topic: Institute of higher vocational education, Changzhou University; Project title: Research on
the application of information based intelligent classroom in Higher Vocational Education;

References:
[1] Guo Jinhua, Ming Xiaobo. Internet of Things Computer Network Security and Remote Control Technology [J]. Contemporary Educational Practice and Teaching Research, 2016(3).
[2] Wang Jingui. Talking about the security and control of the Internet of Things computer network[J]. China New Communications, 2020.
[3] Li Yuanyuan, Hu Jun, Ye Bing. Computer and Internet of Things Network Security and Control[J]. Computer Fan, 2018, 000(021): 62.
[4] Li Lei. Research on Security and Control Strategy of Internet of Things Computer Network[J]. Wireless Internet Technology, 2018, 015(011):38-39.
[5] Xie Xiaoxia. Internet of Things Computer Network Security and Control[J]. Science and Technology Innovation and Application, 2019, 000(018):141-142.