Research on Network Security Problems and Countermeasures Based on the Internet of Things Technology

Wenfu Yang\textsuperscript{1,*}
\textsuperscript{1}College of Internet of Things, Jiangxi Teachers College, JTC, Yingtan, Jiangxi, China, 335000

*Corresponding author e-mail: yangwenfu@jxsfgz.edu.com

Abstract. With the development of computers and the popularity of the Internet of things (IOT) technology in real life, the Internet of things computer network technology will be the trend of development in the future. While the IOT is widely used to improve the speed of resource sharing and transmission, we should also pay attention to the security problems in the network environment. This study analyzes the security status of the IOT, and puts forward several technical measures that are being studied according to its security risks.

Keywords: Internet of Things, Network Security, Security Risks

1. A brief introduction to the technology of the Internet of things (IOT)

1.1. The concept of IOT

The Internet of things itself is closely related to the Internet. The Internet of things is not only developed from the Internet, but also belongs to the extension of the Internet. The definition of the Internet of things is as follows: the Internet of things is the Internet connected to the Internet of things. The Internet of things is not only an important aspect of the new stage of information technology, but also a substantive aspect of the information age\textsuperscript{(1)}.

Figure 1. The model of IOT.
The old kind of internet is always divided into three parts:

1) The transport layer: The transport layer is a bridge between the perception layer and the application layer, which can connect the two together. To some extent, the transport layer is responsible for the communication between the sensing layer and the application layer. In other words, the transport layer is always responsible for data transmission, which can make the traditional Internet or private network combine with each other to transmit information together. This increases the dimension of information transmission and collection.

2) The application layer: The application layer is primarily developed and designed for users, mainly responsible for data display and user operations on the hardware.

3) The sensing layer: The sensing layer is usually composed of a variety of sensors, which are used to collect perceptual data.

The Internet of things is the latest thing, a combination of almost all the latest technologies in the world with computer and Internet technologies. The Internet of things can realize the information sharing between different objects, including environment and state, as well as the collection, processing and execution of data and information of different objects.

1.2. Characteristics of the Internet of things

(1) The IOT is a wide range of sensing technologies.

There is no doubt that there are a large number of rich and diverse sensors on the Internet of things. Moreover, the data obtained from the sensor is very timely and useful. Because the frequency of the sensor on the Internet is too appropriate, it can allow it to regularly collect information fluctuations and changes in the environment, so as to constantly update the data, so as to make the data of the Internet of things more effective.

(2) The Internet is a substantial basis and key of IOT.

The way that the Internet of things unites all kinds of Internet and all aspects of the same Internet is to make use of a large number of wired and wireless networks. This makes the data transmitted by the Internet of things more timely and accurate, and has higher practical value and significance. The sensors on the Internet of things usually mine all kinds of useful information from the network through the transmission system and detection system within a certain time interval, and transmit it as a whole. However, due to the excessive data generated on the network every day, in the overall data and upload process, the sensor needs to have a variety of heterogeneous networks and protocols to protect the immediacy of the data.

(3) The IOT not only offers the connection among sensors, but also has capacity for intelligent processing and can cleverly manage objects. The IOT combines intelligent processing and sensors...
together, using cloud computing and some other intelligent technologies for expanding the area of application.

2. Analysis of the current situation of network security of the Internet of things

(1) Business.

Internet of things business technology can support many platforms, including massive information processing systems, a variety of distributed systems and cloud computing and other artificial intelligence-related technologies. These platforms have a variety of unrelated network technologies and strategies to ensure security. These technologies and strategies can achieve large-scale application construction for the upper network and upper users, and can help the management of the platform to establish an efficient and reliable system. However, the Internet of things usually has the characteristics of many business types, various platforms and large scale. Because of these characteristics, the security problems of the Internet of things need to be vigilant by developers and users. These security problems require people to develop new and more effective methods, check and fill gaps in the original methods, and constantly improve the security mechanism of the system. Therefore, it can be clear that the premise of the promotion and use of the Internet of things is that the private information of any organization or individual cannot be disclosed. And all the steps that users of the Internet of things need to complete on the network should be highly secure. This can help to establish a relatively secure Internet of things and network environment, so as to protect personal information and institutional secrets from illegal intrusion[3].

(2) Information transmission.

Information transmission is the core of the Internet of things, and the network security of information transmission is also very important.

Because the Internet of things is a very large network. The number and nodes of the core network of the Internet of things are very large. The number of core networks of the Internet of things basically exists in the form of clusters. In fact, the core network can improve the security of information collection, arrangement and transmission to a certain extent, but it can not guarantee its effectiveness. In fact, there are loopholes in the security measures of the core network. Therefore, one of the problems that the managers of the Internet of things must pay attention to is that the Internet of things collects more and more complex data every day, and the transmission of a large amount of machine data usually slows down the web page and makes the network congested. In this case, data transmission often occurs some denial of service phenomenon, and will be accompanied by some aggressive behavior. In addition, under the current network environment and development, the target object of the Internet of things, that is, the process of sharing and transmitting information and data between various things, needs a very effective and smooth security system to ensure the confidentiality of data and increase users’ confidence in its use.

Therefore, the core point is that for the network security and concealment of the information transmission process on the Internet of things, it is the most important to ensure the security of the entire data transmission channel[4].

(3) Information collection

The role of the Internet of things is very many, and it also brings a lot of benefits to the development of human society. But among them, the most important role of the Internet of things is that users, managers and developers should realize that the smooth operation and use of the Internet of things is based on the network formed by multiple multimedia platforms. this network can realize the sharing and transmission of information and resources on different platforms. In fact, the platform of the Internet of things has been changing in a dynamic process, the operation of the Internet of things is not immutable, the content and transmission channels on the network are constantly updated and changed with the increase of frequency. Therefore, the Internet of things platform must always input the freshest information and energy in the construction and background of the network. In order to improve the immediacy of the Internet of things, the best way to solve the problem is to collect and process data and information more efficiently, which is also one of the cornerstones of the long-term
development of the Internet of things.

In general, the function and design of a single node of the Internet of things are relatively simple. The structure of each node is different, showing multiple heterogeneity. Each node carries less energy and information, so the node is fragile and can not have advanced security protection capability. Moreover, because of the simple structure, the security management of information by network nodes can not reach the highest level. Moreover, there are many kinds of Internet of things, but there are no unified protocols and regulations on the process of data and information transmission between most of the Internet of things. Therefore, the security measures between the Internet of things are actually inadequate. Therefore, it is difficult to achieve the goal of making the protection system of the Internet of things secure and unified. Moreover, for the perceptual network, the problem that needs to be solved most and needs to be paid the greatest attention is the security of information, which involves the process of information collection and transmission, which is more complex\(^5\).

3. Security risks and countermeasures in the environment of the Internet of things
At present, the research on network security mechanism is mainly focused on the following technologies\(^6\).

3.1. Secure routing technology
There are many kinds of routing threats to the Internet of things. Multiple identity attacks, synchronization attacks, denial of service supply and falsification of router information all belong to the threat types of routers. At present, there are a variety of solutions to different router attacks. According to different types of attacks, the main prevention methods have also changed. At present, the most commonly used defense methods include data fusion, protection against physical attacks and so on. However, the specific situation needs specific analysis, in practice, which method needs to be used to deal with it needs to be chosen according to the different needs of the Internet of things. Among the many protocols, there is always one that is the most suitable secure routing protocol for some kind of Internet of things.

In addition, there are two main ways to design secure routing protocols. First of all, managers can use the key system to create a secure information communication environment, and then exchange routed information. In addition, users can use redundant routes instead of traditional routes, which is more secure to transmit data.

3.2. Key management technology
At present, there are four main key management protocols. Among the four protocols, the simple key distribution protocol is the simplest, but at the same time it is also the least secure protocol. It is only suitable for low-level information transmission between the Internet of things, and can not complete higher-level tasks. Hierarchical key management protocols contain a variety of key protocols. Different mechanisms can deal with different Internet of things and different network problems. Therefore, this protocol has the highest maintainability for network security. The layered protocol can help the sensor at each node to establish a different form of key, so that the node can cope with complex and changeable data and information. The other two protocols are dynamic key management protocol and key pre-distribution protocol, which are less used than the former two protocols, but they are also effective protocols.

4. Conclusion
The Internet of things is not only the inevitable outcome of the development of information technology to a certain extent, but also a new requirement of economic and social development to a certain stage, which has been widely concerned and applied all over the world. Due to the characteristics of immature technology, there are many hidden dangers in the network under the environment of the Internet of things, and people's awareness and demand for the security of the Internet of things is becoming stronger and stronger. Before enjoying the convenience brought by the
Internet of things, engineers need to gradually develop corresponding technologies to avoid risks and hidden dangers. This is also an important topic in the field of the IOT.

References
[1] Chen Chunhua; Research on network security in the era of internet of things [J]; Network Security Technology & Application; 2016.
[2] Ye Haiyan; Research on network security in the environment of internet of things [J]; Journal of Jilin TV & Radio University; 2014.
[3] Feng Wei, Li Xuan, Tang Wei, Wu Tingting, Shen Xiaohan; Research on network security technology of mobile internet of things intelligent information terminal [J]; Cyberspace Security, 2016.
[4] Shao Yu, Zhang Bo; Research on the current situation of network security of the internet of things and related countermeasures [J]; Network Security Technology & Application; 2016.
[5] Guo Jinhua, Ming Xiaobo; Research on computer network security and remote-control technology of internet of things [J]; Contemporary Education Research and Teaching Practice; 2016.
[6] Chen Yuxia; Research on the security of wireless sensor networks based on the security of the internet of things [J]; Information & Communications; 2014.