Universe Scientific Publishing

ORIGINAL ARTICLE

Based on the Data Transmission Security of Internet of Things IPv6

Zhenfeng Li, Lijie Gao

Zhengzhou University of Science and Technology, Henan Zhengzhou 450064, China.

Email: lzf1978@ha.edu.cn

Abstract: With the rise and development of new technology of Internet of things, the demand of new intelligent terminal to access the Internet is increasing day by day, and the interconnection of all things is an inevitable trend. The traditional IP protocol in the past can not meet the requirements of "wide access, high-speed interconnection, safe transmission ", but the IPv4（Internet Protocol Version 4）protocol itself has security defects. Traditional Internet is based on IPv4 protocol, the protocol design at the beginning of more consideration of efficiency, security considerations are inadequate, such as IP deception, source routing attacks, network listening and other issues. Therefore IPv6（Internet Protocol Version 6）protocols emerge as the times require, and the application of Internet of things based on IPv6 is becoming more and more common, and then the problems of data transmission security, equipment control security and data exchange security are becoming more and more prominent.Compared with the IPv4, IPv6 did make great progress, mainly in: service quality, security, address capacity and mobility. For the Internet of things technology, IPv6's progress is of great significance. Based on the data transmission security of IPv6 Internet of things is discussed in this paper, and the countermeasures are put forward to solve the problems of data transmission security of Internet of things.

Keywords: IPv6; Internet of Things (IOT); Data Transmission; Data Security; Inquiry Strategies

There is powerful network function based on IPv6 network, which makes network application more deeply integrated with people's life and the development of various industries. However, in order to apply the rapid development of IPv6 network, many network equipment and technology also need to upgrade, innovate, and cooperate with IPv6 application on the basis of the original. Among them, the issues of data transmission security of Internet of things technology have attracted attention. During the application of the Internet of things technology, because the Internet of things terminals generally have the characteristics of low power consumption and low complexity, the characteristics of data transmission are usually SD (Small Data) transmission, This means that even the transmission of a small piece of data in the Internet of things database can have a huge impact on network security. By exploring the problems of data transmission security based on Internet of things IPv6, on the one hand, it is to perfect the security application of Internet of things technology, on the other hand, it is also an important measure that is beneficial to the sustainable development of the whole Internet industry in China.

1. Based on the problems of data transmission security of Internet of Things IPv6

1.1 Analysis of security risks in Internet of things data transmission

Regarding the security of Internet of things technology, the security risk of its data transmission is an important aspect. In the Internet of things technology, by using a compressor, it can increase the anti-interference ability, reduce the pressure of data

doi: 10.18686/ahe.v4i5.2239

transmission, and greatly improve the efficiency of data transmission. However, when the compressor perception theory does not differentiate the transmission of data, conventional data will be mixed with privacy data, which will lead to data being stolen or falsely used. In this case, based on the current situation of data processing at the same time, it will increase the operation load of the sensor and reduce the transmission speed of information. In order to avoid this situation, some enterprises will encrypt and protect the privacy data through digital watermark in practical application. However, there are still many enterprises to this piece of security risk that is not enough attention. The use of the Internet of things has been gradually spreading from the basic field, which can be used in many aspects, such as industrial safety production, environmental monitoring, urban public safety, intelligent transportation, public health, health monitoring, smart home and so on. Data security protection for these core areas is also an important aspect of national data security protection.

1.2 Security risks for data acquisition of Internet of things

In modern society, convenient communication between people is actually an important embodiment of Internet of things technology. In the past, the fastest way to transmit information was to send a telegram, and now a phone, WeChat, can immediately contact each other. No matter where you are or how far you are, you can communicate information in seconds. So, what is the principle of Internet of things technology? The foundation of the Internet of things technology is the sensor, and the working principle of the sensor is to obtain data information by sensing, scanning and scanning. With the continuous development of Internet of things technology, the industry that uses Internet of things technology is becoming more and more huge. In the case of a large number of sensor nodes, wireless sensor networks exist and can collect a large number of data content. We transmit data over wireless or wired networks, after the wireless sensor takes this data, all the information can be transmitted to the Internet of things platform. It is worth noting that in the process of obtaining the data information of the Internet of things, there will be a lot of data information between wireless sensor nodes, which will lead to a series of security problems, such as the easy theft of node data, malicious access and so on. Once these problems occur in the process of data transmission, it will affect the identity authentication of node data, and eventually lead to the failure to complete data acquisition. At present, the development of Internet of things technology has penetrated into people's daily life bit by bit and all aspects of enterprise construction, and the security problem of Internet of things data acquisition must be highly valued and actively dealt with.

The application of Internet of things technology based on IPv6 has greatly improved people's quality of life, the change brought is not a certain industry or a certain aspect, but the formation of the whole industrial chain. For example, people shop online on a large scale, this trend of online shopping will lead to the emergence of logistics, the continuous improvement of logistics has spawned a variety of efficient management of APP applications, as well as the optimization of resource allocation of artificial intelligence research direction. In order to promote the healthy development of the Internet of things, it is of great social significance and value to pay attention to the security of data transmission in the Internet of things.

2. The improvement strategy of Internet of Things data transmission based on IPv6

2.1 The data transmission model of privacy, reducing the risk of data transmission in Internet of Things

"Internet of things security" is a large category, among which, data security in the process of Internet of things data transmission is a very important aspect, has always been the object of various experts and scholars. In real life, some enterprises can reduce the risk of Internet of things data transmission through encryption algorithm, but some enterprises are difficult to do. In this case, network security personnel need to actively build the "the model of privacy data security transmission". In general, the construction of this transmission model needs to start from these aspects: first, compression perception is carried out; secondly, digital watermarking is processed. The general flow is that the sensor node is encoded by the end of the watermark, and then the carrier data is added to the watermark, while the compression sensing technology is used to gradually sparse the signal. With the continuous improvement of Internet of things security technology, data transmission security may have a greater breakthrough in the future.

2.2 The authentication mechanism of two-way, avoiding the hidden trouble of Internet of things data acquisition

The Internet of things has a huge data storage and data processing center, which can be summarized as the architecture from terminal to transmission, from transmission to cloud. This architecture logic can also be divided into perception layer, transport layer and application layer. With the wide application of Internet of things technology, the requirements for its perception, processing and transmission related capabilities are also increasing, which are the factors that cause the risk of Internet of things data acquisition. In order to ensure the security of Internet of things data acquisition, the first link to pay attention to is "the identity of access devices is legal." Under this premise, the introduction of standby nodes, the introduction of node state monitoring, the introduction of alarm mechanism, etc., can enhance the safety factor of Internet of things data acquisition. In a word, to realize the authentication mechanism of two-way of Internet of things data, we should pay attention to two aspects, one is the initial authentication and the main node warning, the other is the backup node authentication. Through this method, the base station database and sensor nodes can realize two-way identity authentication, and avoid the security hidden trouble when the Internet of things data is obtained.

3. Conclusion

The rapid development of Internet of things technology is constantly changing people's lives, in this dynamic process, the wider it spreads, the more factors that may be limited, this is a complementary process. IPv6 Internet of things data transmission security problems in the future enterprises, may become a key factor restricting the further development of enterprises. From this point of view, our country should not only attach importance to the strategic layout of network security, but also vigorously train network security professionals, and strengthen the control of data security in the Internet of things.

References

1. Wang Y, Xu Q.Research on privacy data security for Internet of Things. Computer Programming Skills and Maintenance 2017; (24): 90-91+94.
2. Lu L. Research on privacy data security in Internet of Things. Modern Computer (Professional Edition) 2017; (10): 60-64.
3. Bai Y. Research on privacy data security for Internet of Things [dissertation]. Tianjin University of Technology; 2015.
4. Tian h, Liu J, Cao L. Based on theimplementation of IPv6-IPsec network security access. Microcomputer information 2008; 2-3: 95-96.
5. Chen W, Long X, Gao X. Amixed authentication method for mobile IPV6. Journal of Software 2005; 16(91): 1617-1624.
6. Lin H, Zhang S, Zhang H. Based on IPv6 intrusion detection system current. Television technology 2005; (10): 89-94.
7. Feng D.Computernetwork and communication security (2nd Edition). Beijing: Tsinghua University Society; 2001.
8. Du G, Qiu Y, Guo H.IPv6 network security architecture research. Microcomputers Machine Information 2006; (4-3): 82-84.