Hierarchical Structure and Security Model of Internet of Things

Lulu Zheng

School of Communication and Information Engineering, Xi'an University of Science & Technology, Xi'an, Shaanxi, 710021, China

1003419372@qq.com

Keywords: Internet of things; Hierarchical structure; Network security; Internet platform

Abstract: In order to overcome the problems and difficulties in the operation of the Internet of things, this paper proposes a novel hierarchical structure and security model of the Internet of things. The security model also combines the characteristics of the Internet of things security problems and the format types of the Internet of things data information, starting from the hierarchical structure of the Internet of things, puts forward different solutions for different hierarchical structures. The results show that the security model can standardize the format and type of data information of the Internet of things, give full play to the advantages and characteristics of the three levels of the Internet of things, and meet the needs of the safe operation of the Internet of things.

1. Introduction

With the rapid development of science and technology, all kinds of information science and technology have penetrated into people's production activities, among which the Internet of things technology is one of the high-tech in the 21st century. The Internet of things technology can establish the connection between the goods and the Internet through a variety of intelligent devices, such as sensors, RFID devices, positioning systems, so that users can track the location of the goods in real time and get the required data information. Therefore, the Internet of things technology has been widely used in people's practical activities, which has multiple functions, such as identification, positioning, tracking, supervision and so on, greatly promoting the progress and development of human social civilization. In today's network security incidents occur frequently, to ensure the security of the network environment can make the network serve the human society. Therefore, the importance of network security cannot be overemphasized. At present, with the further development and application of Internet of things technology, Internet of things security, as an important branch of network security, is also the extension and development of network security, which also has a profound impact on human practice. If we want to realize the Internet of things to serve users, we must improve the security of the Internet of things.

2. Definition and content of Internet of things

The Internet of things, in essence, is a high-tech science and technology based on the Internet platform. This technology can realize the connection between objects through a variety of intelligent devices and science and technology [1]. At the same time, the Internet of things is mainly used in the connection between objects and computers. Through the Internet of things, users can timely understand the dynamic information of the target object, so as to make judgments and decisions at any time. Through the Internet of things, users can remotely monitor the location of objects, and also remotely control objects and change data information. Therefore, the emergence of the Internet of things enables people to explore the relationship between different objects, and also to understand the trend of the target object at any time [2]. In addition, the Internet of things is usually regarded as the carrier of information and data, which mainly transports the relevant data information of target objects for users. Through the Internet of things, people can deeply feel the close relationship between things, and thus feel that the world is an interconnected community.

  DOI: 10.25236/iccem.2021.079

3. Hierarchical structure of Internet of things

The hierarchical structure of the Internet of things has three parts: perception layer, network layer and application layer. Among them, the perception layer mainly collects and obtains all kinds of data information, and perceives the dynamic of all kinds of data information. The network layer relies on the Internet platform to realize the transmission and exchange of data and information. The application layer realizes the processing and application of data information through the data information collected and transmitted by the first two layers [3].

Specifically, the function of the perception layer is to obtain the data information between objects, so as to provide users with all kinds of data information of the target object. It can not only help users screen out valuable data information, but also store the data information in the database. The function of network layer is mainly to transport and exchange data and information for a long distance, which enables users to monitor and manage the target object remotely, and obtain the data and information of the target object in real time [4]. In addition, the network layer also enables users to exchange data and information with other users. The application layer is mainly to process and analyze the collected data of the target object, and strengthen the human-computer interaction. Therefore, the three levels of the Internet of things show that the main function of the Internet of things is to obtain the data information of the target object, and realize the exchange of the collected data information, so as to carry out a series of processing and analysis of these data information, and then apply to the actual field [5].

Figure 1 illustrates the three levels of the Internet of things in detail, and shows the content and specific functions of each level.

<table>
<tr><td rowspan="2">Perception Layer</td><td>Perception Subsystem</td><td rowspan="2">The perception subsystem perceives the physical environment, and the control subsystem acts on the physical environment.</td></tr>
<tr><td>Control Subsystem</td></tr>
<tr><td>Network Layer</td><td>Heterogeneous Network Convergence</td><td>Next generation heterogeneous convergence network: Internet, telecommunication network, etc.</td></tr>
<tr><td rowspan="2">Application Layer</td><td>Information Application</td><td rowspan="2">Realize traffic monitoring, urban management, environmental monitoring, etc.</td></tr>
<tr><td>Information Processing</td></tr>
</table>

Figure 1. Hierarchy of Internet of things

3.1 Perception Layer

The perception layer of the Internet of things is mainly composed of all kinds of intelligent devices with perception function, such as RFID, GPS, sensors, readers, cameras, etc. these intelligent devices can give full play to their perception function and accurate recognition ability, so as to quickly collect the data information of the target object.

3.2 Network Layer

The network layer of the Internet of things, as the name suggests, relies heavily on the Internet platform. At the same time, the network layer of the Internet of things can be divided into two kinds of network environment, which are communication network environment and Internet network environment. Network layer can speed up the ability of network operation, but also can carry massive data information, so as to speed up the speed of data information exchange [6]. The network layer involves sensor technology, cloud computing technology, Internet technology and so on. It can transmit and store massive data information, so as to realize the communication between users and give full play to its own interconnection function.

3.3 Application Layer

The application layer of the Internet of things combines the science and technology of various industries, reflecting the intelligence of the Internet of things. The main function of the application

layer of the Internet of things is to ensure the sharing, openness and security of data and information. At the same time, the application layer of the Internet of things also covers the display of the user information interface and various related management devices. At the same time, the application layer of the Internet of things also includes the application support platform and application service platform.

4. Security model of Internet of things

4.1 Security Issues of Internet of Things

With the rapid development of Internet technology, Internet of things technology based on Internet platform also provides convenient services for major industries. The Internet of things, in essence, takes the Internet platform as the material carrier, which combines sensor technology, integration technology, etc., and can give full play to various functions of Internet technology, so as to provide users with high-quality services. In addition, with the social attention to network security, the Internet of things can play the advantages of some security technologies based on the Internet platform, such as authentication technology, encryption technology and so on[7]. However, it is worth noting that there is still a big difference between the Internet and the Internet of things. Therefore, the security technology for the Internet platform can not be directly applied to the use of the Internet of things. Technicians must adjust and develop a more suitable security mechanism for the Internet of things according to the characteristics of the Internet of things.

In addition, the application system based on Internet of things technology can provide people with a variety of convenient services, but also can help people complete a series of high risk work. Therefore, in the actual application process, intelligent devices based on the Internet of things are usually placed in the more remote and open space, which also greatly reduces the security of the Internet of things devices. It is easy for criminals to attack the Internet of things devices, and even replace the key parts of the Internet of things devices, thus threatening the integrity and security of the Internet of things devices [8].

4.2 Security Requirements of Internet of Things

Compared with the Internet technology, the Internet of things has its own outstanding characteristics, which can effectively realize the information exchange between users and between users and target objects. Therefore, the Internet of things has significantly expanded the scope of data and information exchange. In order to fully solve the current security problems of the Internet of things, this paper proposes a novel security mechanism of the Internet of things, and puts forward specific requirements and standards from the following three aspects.

1) Authentication mechanism

Authentication mechanism, in essence, is to identify and confirm the user's identity by some way or means. There are two main authentication mechanisms, identity authentication and information authentication. Through the authentication mechanism, users can exchange keys, which is to ensure the security and timeliness of data and information exchange. At the same time, important data information can be transmitted in the form of cipher-text, so as to avoid the security problems of data information in the transmission process. Therefore, with the development of science and technology, the authentication mechanism based on sensor technology has become an important research topic in the current Internet platform and Internet of things technology [9].

2) Key management mechanism

At present, with the advent of the information age, people pay more and more attention to the security of personal privacy. Key management mechanism is one of the main means to provide data information protection for users. There are two main management modes of key management mechanism: centralized management mode centered on Internet and distributed management mode centered on each sub-net. Through the key management mechanism, the user's personal data information can be unlocked by password, which strengthens the security and confidentiality of the user's personal privacy.

3) Access control mechanism

At present, in the application process of Internet of things, access control mechanism has become the main means of rational use of data resources. Access control mechanism, in essence, can block and manage the users who access the database. Through the access control mechanism, users can set the resource content that different types of visitors can access. This way can not only ensure the security of data information, but also provide different visitors with data information to query and browse.

4.3 Internal Structure of IOT Security Model

1) Security structure of perception layer

The sensing layer of the Internet of things is mainly a closed system composed of WSN, which can ensure the security of WSN itself. At the same time, the perception layer of the Internet of things mainly realizes the communication between the internal networks through the network joints. Therefore, the security of IOT perception layer should be improved as much as possible, for example, key management mechanism should be added.

In addition, when the nodes in the perception layer obtain the data information, if there is no corresponding security measures, the data information is likely to be leaked or illegally obtained by a third party, resulting in great economic losses. In addition, some perception layer nodes will take simple information security protection, but these simple protection measures not only can not improve the security, but also may cause the transmission of data information to be disclosed. Moreover, when the criminals steal the data information of one of the nodes in the perception layer, they are likely to control other nodes and obtain all kinds of data information of the perception layer. Therefore, the author believes that in order to improve the security of the perception layer of the Internet of things, it is necessary to predict and intercept the behavior of malicious nodes [10].

Moreover, the perception layer of the Internet of things will eventually be connected with the external network, which will inevitably be attacked by the external network. The main attack type of these external networks is DOS. In other words, if the nodes in the perception layer of the Internet of things are difficult to accurately identify DOS attacks, the network system is likely to be completely paralyzed. The author thinks that the sensing node must have the ability to resist DOS attack.

Figure 2 clearly shows the main contents and functions of the security structure of the perception layer of the Internet of things.

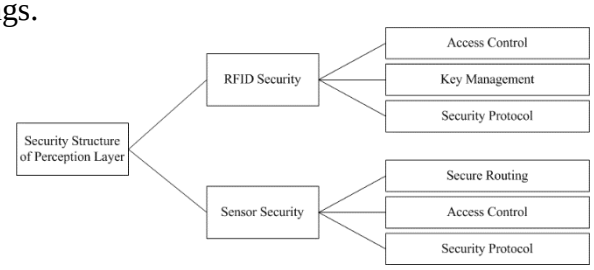

Figure 2. Security structure of perception layer

2) Security structure of network layer

According to the different types of network architecture, the security authentication types of different network architectures are also different. Therefore, the network attack defense ability of different types of networks is also greatly different. Moreover, in the network layer of the Internet of things, there are still huge challenges in the security of data set information exchange in different network environments. We should upgrade and update the security defense system of the network layer in time.

The Internet of things, in essence, is a network which takes the Internet platform as the carrier and continues to extend and develop on the basis of the original Internet. Due to the differences in the characteristics and application scope of the Internet and the Internet of things, as well as their security standards and service standards, the security technology mode of the Internet of things can not simply copy the security technology mode of the Internet, but should be adjusted and optimized on the original security technology mode of the Internet.

At present, the main reason for the security problems of the network layer of the Internet of things lies in the diversity of data information types. Therefore, the author believes that the format of data

information entering the network layer can be required, that is, the unified data information format.

Figure 3 illustrates in detail the main contents and functions of the security structure of the Internet of things network layer.

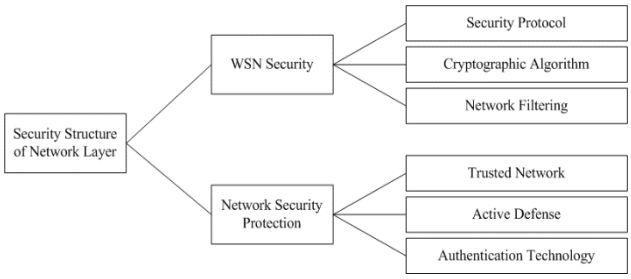

Figure 3. Security structure of network layer

3) Security structure of application layer

Therefore, compared with the perception layer and network layer of the Internet of things, the application layer of the Internet of things involves the most fields. Therefore, the application layer of the Internet of things needs to deal with massive data information, which is a huge challenge to the security and reliability of the Internet of things. It is mainly reflected in two aspects, namely business control and privacy protection.

On one hand, business control. One of the main functions of the Internet of things technology is to enable users to operate the equipment remotely, and even realize the automatic operation of various services in an unsupervised environment. Obviously, in an unsupervised environment, the Internet of things is vulnerable to malicious attacks. Therefore, in order to solve this problem, the Internet of things must build a strong security management platform, strengthen the relationship between the Internet of things and business platform, and improve the security of business.

On the other hand, privacy protection. The application layer of the Internet of things is directly for users, and the user data information it carries involves all walks of life. Therefore, the privacy protection of the application layer must be considered. In my opinion, there are two privacy protection methods in the application layer, which are peer-to-peer computing and semantic web. The former can exchange and share data information, while the latter can standardize and organize information, so that data information can be understood and applied by computer, and then realize the communication between users.

Figure 4 shows the main contents and functions of the security structure of IOT application layer.

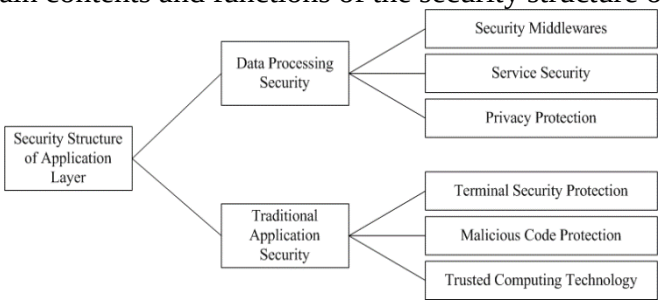

Figure 4. Security structure of application layer

5. Conclusion

To sum up, at present, the Internet of things has made great progress in many fields, such as logistics, retail, anti-counterfeiting, e-commerce, trade, transportation and so on.

With the further development and application of Internet of things technology, it not only provides great convenience for people's life and work, but also promotes the rapid development of major industries, which is constantly creating huge economic wealth. We believe that people will overcome the problems in the application of Internet of things technology, and will continue to improve the security and intelligence of Internet of things.

References

[1] Granjal J , Monteiro E , Sa Silva J . Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues[J]. IEEE Communications Surveys & Tutorials, 2015, 17(3):1294-1312.

[2] Zhao K , Ge L . A Survey on the Internet of Things Security[C]// International Conference on Computational Intelligence & Security. IEEE, 2014.

[3] Raza S , Duquennoy S , Hglund J , et al. Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN[J]. Security and Communication Networks, 2014, 7(12).

[4] Herold R . The Criticality of Security in the Internet of Things[J]. ISACA journal, 2015, 6:18-24.

[5] Sandor H , Sebestyen-Pal G . Optimal security design in the Internet of Things[C]// 2017 5th International Symposium on Digital Forensic and Security (ISDFS). IEEE, 2017.

[6] Baskaran S B M , Arumugam S , Prasad A R . Internet of Things Security[J]. Journal of ICT Standardization, 2019, 7(1):21-42.

[7] Kaur R , Raina B L , Sharma A . Internet of Things: Architecture, Applications, and Security Concerns[J]. Journal of Computational and Theoretical Nanoscience, 2020.

[8] Wu H , Han H , Wang X , et al. Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey[J]. IEEE Access, 2020, PP(99):1-1.

[9] Shuaiqi, Shen K , Zhang Y , et al. Security in edge-assisted Internet of Things:challenges and solutions[J]. Science China(Information Sciences), 2020, v.63(12):27-40.

[10] Obaidat M , Khodiaeva M , Obeidat S , et al. Security Architecture Framework for Internet of Things (IoT)[C]// 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). IEEE, 2020.