Research on Computer Network Information Security Problems and Prevention Based on Wireless Sensor Network

Haiwei Wu, Hanling Wu*
Hainan Vocational University of Science and Technology
Haikou, Hainan 571126, China
*Corresponding author e-mail: 917795486@qq.com

2021 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC) | 978-1-7281-9018-1/20/$31.00 ©2021 IEEE | DOI: 10.1109/IPEC51340.2021.9421303

***Abstract*—With the continuous improvement of China's scientific and technological level, computer network has become an indispensable part of people's daily life. It can not only effectively improve the efficiency of production and life, and shorten the distance between people, but also further promote the speed of China's social and economic development, which has a positive impact on the realization of China's modernization. Under the new information security demand environment at present, we should pay attention to the related information security work and formulate effective security measures and strategies. In order to effectively prevent these information security problems, people should actively adopt firewall technology, encryption technology, network access control technology and network virus prevention technology for effective protection. This paper analyzes the security problems in the application of wireless sensor networks and explores the mechanism of defending information security, hoping to strengthen the security and stability of wireless sensor networks through effective measures, so that people can better enjoy the convenience brought by the network age.**

Keywords—Computer network, Wireless sensor, Information security

I. Introduction

With the rapid development and maturity of microelectronic technology, computer technology and wireless communication technology, wireless sensor network has been gradually applied to military, environmental monitoring and other fields, and has gradually entered the practical stage [1]. This kind of micro sensor network with computing and communication capabilities is a multi hop self-organizing network formed by a large number of cheap micro sensor nodes through wireless communication, which can complete the data collection, transmission and fusion of various monitoring objects in the deployment area in a cooperative way [2]. Wireless sensor network is a new technology with the development of sensor technology, computer technology, wireless communication technology and distributed information processing technology in recent years [3]. The application environment of wireless sensor network is usually complex, especially in the military field. How to ensure the security of wireless sensor network is the basis of its application [4]. Wireless sensor network is a large-scale self-organizing network, through a large number of low-cost, resource constrained sensor nodes to work together to achieve a specific task [5]. In the information age, it is very important and critical to effectively prevent information security, and it has also become an important research topic in the development of computer network technology [6]. Wireless sensor network (WSN) is a new information acquisition and processing technology. Since it usually operates on its own and does not require personnel to perform duties, the security of wireless sensor network has a great threat [7].

With the development of science and technology, computer network technology has brought great convenience to people's life, but at the same time, there are hidden dangers of information security, such as software vulnerabilities, hackers and viruses. If we do not pay attention to the security of information, it will have serious consequences [8]. Due to the openness, expansibility, interactivity and many other characteristics of the computer network, in the actual application process, it often causes some security risks and brings unnecessary economic losses to users [9]. Under the background of Internet, on the one hand, it is necessary to improve the safety awareness of users, master more computer operation skills, and ensure the privacy and security of personal information. On the other hand, relevant departments should constantly optimize the network operation environment, increase the publicity and education of computer network security, improve the stability and security of computer network, and realize the orderly development of China's overall economy [10]. This paper analyzes the security problems in the application of wireless sensor network, and explores the mechanism of information security defense, hoping to strengthen the security and stability of wireless sensor network through effective measures, so that people can better enjoy the convenience brought by the network era.

II. Analysis of Computer Network Security

A. Analysis of the Characteristics of Sensor Networks

The network topology of most sensor networks is unpredictable before deployment, and the whole network topology and the role of sensor nodes in the network often change after deployment. Network connection is a process in which all sensor nodes meet and gather, and it is also a process in which sites meet in the pre-data transmission stage. In this process, there may also be artificial damage to network connection. According to the above analysis of wireless sensor characteristics, wireless sensor networks are vulnerable to many threats and attacks, such as physical manipulation of sensor nodes, eavesdropping of sensor

information, denial of service attacks, disclosure of private information and so on. With the rapid development of computer network technology, people have become more dependent on computer network information in their study, work and life, and put forward higher requirements for the security management and information confidentiality of classified computers.

Although the computer network has been popularized on a large scale, there are still some computer users who lack the awareness of network security and do not pay attention to the installation and update of anti-virus software and firewall system, thus making personal information leaked and network security not guaranteed. Data transmission is the last step in the whole network operation process. Malicious destruction at this level will lead to the tampering and loss of the whole transmission data. The conceptual model of Internet architecture is hierarchical, as shown in Figure 1.

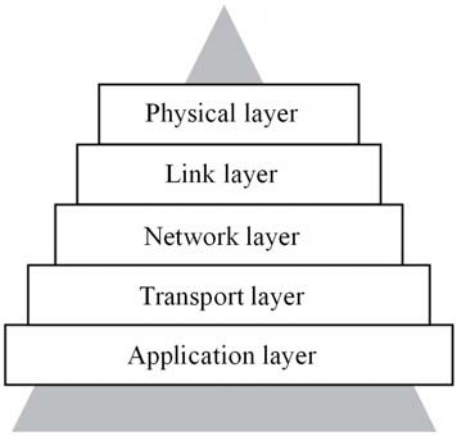

Figure 1 Internet underlying construction model

In the current computer network operation process, it is necessary to carry out the security work. We should start with the specific situation of the current computer network security and take reasonable precautions to ensure the absolute security of network information. After the virus invades the computer system, it can copy and destroy important information and programs, which makes the network unable to work normally, and leads to the system collapse, resulting in huge economic losses. In the actual attack process, advanced equipment can be used to frequently send data packets to the wireless sensor network, which makes the communication within the wireless sensor network blocked, or advanced equipment can be used to disguise as a base station to monitor the wireless sensor network [11]. Both ends of data transmission know that it is a symmetric key to decrypt data files with the same key. Considering the actual situation, the lightweight encryption algorithm can reduce the burden of sensor nodes. Therefore, in general, this type of algorithm will be chosen when data encryption is carried out. When an information security incident occurs due to force majeure, the problem can be solved to a great extent only through artificial maintenance and management.

B. Potential Threats in Wireless Sensor Networks

Network security means that the software and hardware of the network system and the data in the system are protected and will not be damaged, changed or leaked due to accidental or malicious factors. Most of the common hacker problems in the network occur in this process, they will consciously screen and intercept the network data, and after illegally invading the computer, personal privacy information will also be stolen. Computer network virus mainly refers to the virus program written by people entering the normal computer network system and causing damage to the computer system and computer network. Compared with traditional wired network, wireless communication is easier to be monitored [12]. By injecting bit stream, the previous data packets can be simply replayed. However, the establishment of wireless sensor networks usually has no technical staff, and after the equipment is placed in a certain place, it completely depends on the equipment itself to run [13]. This mode of operation makes the acquisition of network nodes very simple. After the attacker finds the corresponding nodes, he can replace them with other sensors or directly rewrite the memory, so that he can monitor the whole wireless sensor network. Once the computer network has security problems, it is very likely to cause incalculable consequences and losses.

III. Countermeasures of Information Security Prevention in Wireless Sensor Networks

A. Network Access Control Technology

From the perspective of computer network security managers, we should strengthen the management of local area network, correct our working attitude, improve the network security management process, build a good computer network operating environment, and realize the effective promotion of professional and technical level. Network access control technology is often used in network security prevention and protection. It is generally divided into network access control, network authority control, network server security control and attribute security control, which can effectively ensure that network resources will not be illegally used or accessed. Through the assembly software, the acquired information can be conveniently converted into the assembly file format, so that the confidential information such as program code, routing protocol and key stored in the sensor node can be analyzed, and at the same time, the program code can be modified and loaded into the sensor node. From the point of view of computer network users, we should constantly improve our own security awareness, set relatively complex computer login passwords, encrypt important files in computer systems, and repair vulnerabilities regularly to improve the security of computer network systems.

At present, most attacks against wireless sensor networks are carried out on the routing layer, for example, by modifying the routing information, pretending to be the network route, and directly attacking the wireless sensor network, so as to divide the network or make the original route generate wrong data. Figure 2 is a schematic structural diagram of an intrusion detection system.

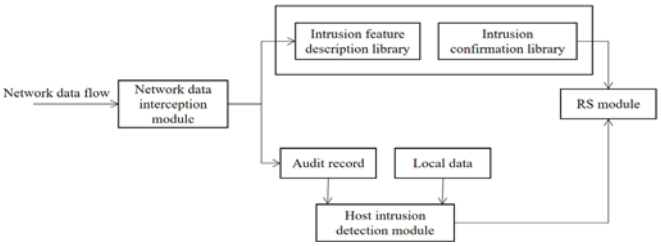

Figure 2 Schematic structure of intrusion detection system

In actual operation, encryption technology can turn important data into garbled code for transmission, and the receiver can restore the data through corresponding decryption technology, thus effectively preventing the information from being eavesdropped or interfered during transmission. Future sensor networks generally have hundreds of sensor nodes, so it is difficult to monitor and protect each node. Therefore, each node is a potential attack point, which can be physically and logically attacked by attackers. Compared with network firewall, data encryption technology has higher security and is more suitable for open network environment [14]. At the same time, data encryption technology can also protect the dynamic information of computer system in real time, which can not only intercept the invasion and attack of other programs in the first time, but also effectively prevent passive attacks and improve the security of computer system. In order to improve the application effect of computer network security measures, it is very critical and necessary to optimize and improve the software application and usage rights. In some units with high security level and strict security requirements, it is necessary to rationally plan the topological structure of internal office network and external internet, set the access rights of internal and external networks, do a good job in the distribution and control of rights, standardize visitors' behavior, and improve the prevention effect of network security problems.

B. Network Virus Prevention Technology

In real life, the setting and application of network firewall can help us resist the access and attack of foreign users, improve the security of computer network, avoid potential security risks, and effectively restrain the network management behavior. Network virus prevention technology is mainly to set up some comprehensive virus prevention software, and ensure that the software can be automatically upgraded, and automatically pop up relevant instructions in operation, so as to prevent virus invasion. Sensor networks are used to collect information as the main purpose. Attackers can obtain sensitive information by eavesdropping and joining forged illegal nodes. If the attacker knows the relevant algorithm of how to obtain limited information from multi-channel information, the attacker can derive effective information from a large number of acquired information. For enterprise computer systems, after LAN connection, it is necessary not only to resist and prevent Trojan viruses and system vulnerabilities, but also to strengthen the prevention of "hacker" attacks. Computer network security management has a long way to go in Ren Zhong [15]. In order to implement the decisions of the decision-making level, it is necessary to have a management level to manage the daily work and an implementation and maintenance level to be responsible for the implementation of safety plans and decisions. The hierarchical information security organization is shown in Figure 3.

In the key link of network information system security, human factor is also very important. Strengthening the ability and quality training of professional and technical personnel and popularizing the information security knowledge of business system users can also make the computer and network equipment in a more secure, stable, economic and reliable operation state. Anti virus software should be installed in the computer network system, so as to timely check and kill the virus that has been invaded. If you can't check and kill the virus, you should update the virus library to check and kill. If still unable to check and kill, the virus should be uploaded to the anti-virus website for help.

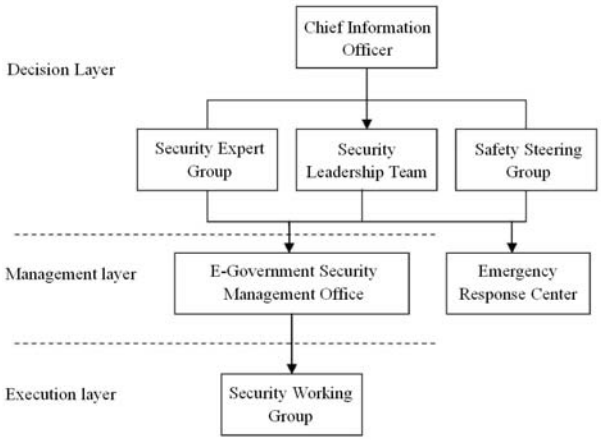

Figure 3 Hierarchical information security organization

IV. CONCLUSIONS

In the process of using computer network, it is necessary to improve users' security awareness and face up to the problems existing in the operation of computer network, and to formulate effective preventive measures, strengthen the maintenance and detection of computer system, and update anti-virus software regularly. The popularity of wireless sensor networks is the general trend. For the possible security problems, we must actively study the security defense mechanism with a professional attitude, and we cannot deny the significance of the existence of wireless sensor networks because of the existing problems. The improvement and optimization of computer network information security measures is an important guarantee of computer network security at present. We should combine the needs of computer network security, make targeted adjustments and improvements, and do a good job in technology selection and application. Computer network information security is very complex, and there are many influencing factors. Preventive measures should be carried out according to the influencing factors. Data encryption technology can protect the dynamic information of computer system in real time, which can not only intercept the invasion and attack of other programs in the first time, but also effectively prevent passive attacks and improve the security of computer system. Only by grasping the development trend of science and technology and striving to eliminate the disadvantages in the development can we increase the development of productive forces and the progress of information technology.

ACKNOWLEDGEMENTS

The authors acknowledge the The First Batch of Education Projects on University-Industry Collaborative Education Program in 2020.Project Name: Research on vehicle safety early warning system based on Cloud Computing. Project number: a52930a2-de49-48af-932d-3d0002ad655a.

REFERENCES

[1] Albagory Y, Said O. Concentric Circular Arrays for Stratospheric High-Altitude Platforms Wireless Sensor Networks. Wireless Personal Communications, vol. 81, no. 2, pp. 1-13, 2015.

[2] Ali R, Pal AK, Kumari S, et al. A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture

monitoring. Future Generation Computer Systems, vol. 84, no. 6, pp. 200-215, 2017.

[3] Liu Haijiang, Jin Yong, Hu Zhentao, et al. Relay power allocation algorithm for wireless sensor networks in eavesdropping scenarios. High-tech Communications, vol. 30, no. 2, pp. 150-156, 2020.

[4] Feng Wei, Wang Feng, Xu Dan, et al. Joint secure routing and power allocation optimization algorithm for wireless sensor networks. Journal of Sensor Technology, vol. 32, no. 4, pp. 610-617, 2019.

[5] Yuan Hao, Mao Yingying, et al. Research on privacy protection methods of node location in public mobile networks. Modern Electronic Technology, vol. 40, no. 16, pp. 35-37, 2017.

[6] Ding Lu, Li Jiying. Challenges facing wireless sensor network information security. China Instrumentation, vol. 6, no. 6, pp. 37-39, 2015.

[7] Zhang Shuo. Analysis of information security issues in wireless medical sensor networks. Modern Information Technology, vol. 3, no. 18, pp. 141-142, 2019.

[8] Bu Yu. Design of Firefighter's Physical Sign Monitoring System Based on Sensors. Information Security and Technology, vol. 7, no. 2, pp. 46-48, 2016.

[9] Ji Xiangmin, Zhao Bo, Liu Jinhui, et al. Key recovery attack in wireless sensor network based on symmetric matrix decomposition. Journal of Communications, vol. 39, no. 10, pp. 87-96, 2018.

[10] Li Wei, Wang Ou, Jin Lei, et al. Research on the secure transmission of ship power system information based on hybrid cryptographic algorithm. Ship Science and Technology, vol. 40, no. 22, pp. 94-96, 2018.

[11] Xu Jun. Application research of trusted computing mobile terminal based on biological characteristics trusted access protocol. Journal of Network and Information Security, vol. 3, no. 2, pp. 66-76, 2017.

[12] Deng Bin, Shi Zhidong, Fang Weidong, et al. Research on the secure multipath routing protocol for wireless sensor networks. Computer Applications and Software, vol. 33, no. 11, pp. 263-268, 2016.

[13] Zhou Wenqian, Wang Tao, Liu Jianlei, et al. Wireless sensor network synchronization acquisition system for impact test. Automation Instrumentation, vol. 38, no. 3, pp. 48-50+54, 2017.

[14] Cao Yueping. Analysis of wireless sensor network technology and development trend. Value Engineering, vol. 34, no. 9, pp. 302-303, 2015.

[15] Wang Yiwang, Lu Jun, Zhang Chengcheng, et al. Design of Intelligent Infusion Monitoring System Based on Wireless Sensor Network. Measurement and Control Technology, vol. 34, no. 11, pp. 64-66, 2015