

# The Development Direction of Information Security in Wireless Communication

Weyao Li\*, Jiayu Li

School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing, 100044

\*Corresponding author. Email: liweiyao220324@163.com

## ABSTRACT

In today's society with the rapid development of information technology, wireless communication technology has been widely used in people's life. People only need a mobile or fixed terminal device to enjoy the convenient services such as voice, video and data exchange brought by wireless communication technology anytime and anywhere, which also exposes a large amount of private information and data to be snooped on. This essay will focus on the generation of information leakage problems and solutions in wireless communication, and dialectically analyze the development direction of wireless communication when information security issues are considered.

**Keywords:** *wireless communication technology; information leakage; information security*

## 1. INTRODUCTION

According to the statistics of author Mannes (2019), in the first half of 2018, more than 25 million pieces of data were invaded or leaked every day, and 291 pieces of information were leaked every second, including medical care, financial data and personally identifiable information. Information leakage refers to the process in which information is stolen in the process of transmission, storage and use, resulting in the leakage of important information. In the process of wireless communication, a large amount of personal data is transmitted, most of which people are unwilling to disclose and share. In addition, some criminals steal national and commercial secrets, endangering social security. More seriously, information security risks make many individuals and organizations dare not accept some emerging wireless communication technologies, hindering the further development of wireless communication[1]. Therefore, it is important and urgent to study how to improve the information security of wireless communication

Based on the above content, first of all, this paper will introduce the classification of information leakage problems that most people face in the process of wireless communication, followed by an analysis of the impact of people's consciousness and thoughts on information leakage. Secondly, the current common communication information leakage solutions will be elaborated and analyzed. In addition, the significance of effective

systems and laws for wireless communication information security will also be investigated. Finally, this paper will draw a conclusion that only by balancing the development of wireless communication technology, personal acceptability, legal norms and the development of anti-information leakage technology, the future development of wireless communication and information security protection can be balanced and sustainable.

## 2. ANALYSIS OF RELEVANT LITERATURE

It can be seen from the paper (Cho, Gilsu et al, 2018) that information leakage in the process of wireless communication is mainly divided into three categories, namely wireless device leakage, network security loophole leakage and electromagnetic radiation leakage. There are only the first two types of information leaks that individuals can prevent by raising awareness. Wireless device leaks will be introduced first. The equipment with wireless networking function can connect the wireless LAN and then connect the Internet under the normal working condition. The transmissions of devices connected to a particular wireless network are exposed in space. The secret stealer can intercept the information bar with special equipment to obtain the information content. Even if the transmission is encrypted, it can be cracked. It is worth noting that wireless network card, wireless keyboard, wireless mouse and Bluetooth, infrared interface are all devices

with wireless networking functions. Music that people listen to through Bluetooth headsets and words that people type through wireless keyboards can be stolen. However, this type of disclosure is something that individuals can prevent. Since most formal wireless networks have their own protection mechanisms, which put a lot of pressure on the skills of the snooty, most information leaks can be prevented as long as people do not connect to wireless networks from unknown sources and do not log on to warning sites[2]. In addition, it is also an effective way to prevent the disclosure of such information to pay close attention to some official early-warning websites and illegal wireless networks in real time, and not to click the website connection casually because it is convenient and cheap.

The second common wireless leak is network security leaks. Electronic information systems, especially computer information systems, are interconnected through communication networks. While remote access, remote transmission and information resource sharing among various systems, they also provide favorable channels for hostile forces and terrorists to infiltrate and attack networks. Because the computer information system runs many programs, the synchronization uses the communication protocol complex, causes the computer in the work existence many kinds of loopholes, the back door and the hidden channel, and so on, is easy to be used by the thief. In the face of such potential information leakage, for individuals, the best way to prevent this is to install corresponding virus detection and anti-virus software on the communication equipment, and regularly use these software to check the communication equipment, when there is a problem that can not be solved by individuals, in a timely manner to seek help from professional companies. The third type of electromagnetic radiation leakage. People's daily use of mobile phones, computers and other intelligent devices will produce electromagnetic waves when working, electromagnetic waves may carry sensitive information will be stolen by special equipment. Especially the leakage of computer electromagnetic radiation is the weak link of preventing theft. Because the solution of such information leakage is to increase the protection distance and use electromagnetic shielding, which is not easy to achieve for families and units, electromagnetic radiation leakage is the most difficult to solve among the above three types of leakage[3].

To sum up, most of the hidden dangers of the above two types of information leakage can be solved through simple prevention by individuals. Therefore, the improvement of personal awareness and attention can prevent the occurrence of a large part of information leakage events, which is an important way to solve wireless communication leakage. According to the survey of Xiaobin Wu (2019), 68.8 percent of communication information leakage is caused by the relatively low technical requirements of secret theft,

which is largely due to people's indifference to the security awareness of wireless communication and the lack of understanding of the process of wireless communication[4]. Therefore, the study of the reasons and ways of information leakage can enable people to have a basic understanding of it, to have some basic knowledge to prevent and respond to possible information leakage events, and at the same time to improve the awareness of personal privacy protection in the process of wireless communication. It can be concluded that the improvement of personal protection awareness and the improvement of personal basic skills are the necessary conditions for the future development of information leakage prevention[5-7].

### **3. CONTENT ANALYSIS**

Paying attention to the development and improvement of information security technology is an important way to prevent and reduce information leakage and its harm. As mentioned above, information leakage in the process of wireless communication is mainly divided into three categories, namely wireless device leakage, network security loophole leakage and electromagnetic radiation leakage. All of these three types of information leakage can be reduced and avoided by technical means of different difficulty. Xueqi (2015) emphasizes in the report that the improvement of encryption technology and encryption mechanism is the most popular research direction of information leakage prevention at present. Encryption technology encrypts transmission information through password, so as to achieve the function of protecting information security. But for now, the breakability of a single password still gives criminals an opportunity. Therefore, to improve the encryption technology and encryption mechanism is to ensure the security of user information. In the process of wireless communication, the system should prohibit access to devices that are not authorized by the user, and for information that is authorized by the user, the defense method should be adopted to prevent a single password from being cracked. The methods to strengthen the defense mainly include prohibiting the dynamic acquisition of host configuration protocol through the network, breaking the relevant parameters in the wireless network device, and strengthening the monitoring of the relevant access list. In addition, by regularly erasing the data, people can ensure the security of user information, further improving the wireless network environment. By doing this, people can prevent most wireless device leaks and some electromagnetic radiation leaks. Even if the current encryption technology is still immature, people can still see the importance of the future encryption technology from the current development environment. Therefore, the development of encryption technology and optimization of encryption mechanism is a significant direction to prevent information leakage. At the same time, the development of encryption technology can not

only be used to protect the transmission of information, but also to assist the transmission of some important information, which is also a very important part of wireless communication. Therefore, the development of anti-information leakage technology is extremely important and can be complemented by wireless communication technology to a large extent.

Another main method to suppress the leakage of communication information is filtering. A suitable filter on the power line or signal line can block the conduction leak path, thus greatly inhibiting the conduction leak. By grounding and lapping the wires well, the stray electromagnetic energy can be given a low resistance loop to the ground, thus diverting to some extent the stray electromagnetic energy that may be transmitted through the power and signal lines. Using this method with shielding, filtering and other technologies, the electromagnetic leakage of electronic equipment can be inhibited with half the effort.

It can be seen that preventing information leakage needs to integrate a variety of technologies, and it also needs time to improve and promote step by step. Taking the example of an author (Rahalkar, Sagar, 2018), he adopted the above measures to comprehensively protect a computer in the system. Rahalkar Install electromagnetic shielding glass on the display screen to close the source of leakage; The power line, keyboard line and communication cable of the display terminal are shielded twisted pair; Connectors with filters are used for the connectors of the interconnect. For such a computer with a higher level of security policy, it can be said that the information security factor is already very high. For ordinary people, the relevant technology and hardware can be adjusted according to the needs to prevent information leakage. Unfortunately, while there are a few companies that offer this kind of communication security services to individuals, not many people are aware that they should do this in their own homes or work places. And the current technology is still low cost performance, immature technology and cannot be widely popularized.

Technology still takes time. It is worth noting that, according to the paper of author (Chengqiong Ye, Wenyu Shi et al.,2021,), the development of such information leakage prevention technology and the rise of related industries are closely related to the wireless communication industry, and there is A certain degree of technical overlap between the two. In other words, the development of information security protection industry is attached to the wireless communication industry on the one hand, on the other hand, it also helps the development of the wireless communication industry. This conclusion is not only drawn from the technical field, but also from the social and human perspective, once the problem of information leakage troubles users on a large scale, wireless communication technology will not be trusted and used. To sum up, it can be concluded that, in the

development of wireless communication technology, attention must be paid to the development and improvement of anti-information leakage technology, which is the inevitable development direction.

The above content of the article mainly from the promotion of people's awareness of protection and development of technology two aspects of wireless communication technology and information security protection direction. Bradshaw (2017) pointed out in his article that the improvement of the legal and regulatory mechanism is the guarantee of the healthy development of any industry. Indeed, strong laws can be a vital deterrent against the illegal theft of personal or state secrets. The use of laws to regulate the generation, storage, transmission and use of wireless communication information, accurate definition of various illegal acts of stealing information can provide an effective basis for the trial in the future. However, the current situation is not optimistic. First of all, due to the rapid development of wireless communication technology, the relevant laws cannot follow closely, which encourages a lot of information theft. Secondly, the country has no professional relevant departments to carry out effective supervision of wireless communication behavior. This is partly due to a lack of social awareness and partly due to the immature talents and institutions involved. Therefore, it can be concluded that the enactment of detailed laws and the establishment of effective regulatory agencies is an important way to prevent and reduce information leakage in the future, as well as an important way to the development of wireless communication in the future.

In the past, and even today, there are many people who think that people only need to develop wireless communication technology alone to continuously improve the speed and quality of communication. Many people even believe that the development of wireless information protection technology and the improvement of relevant laws and institutions is a waste of time, which will hinder the development of wireless communication. However, in the process of development in accordance with this idea, people did not balance the relationship between all parties well, resulting in a lot of problems. According to the survey in 2020 (Hongfeng, Cui, 2020), most of the information security solutions widely used by government agencies and enterprises are still on the defensive means of firewall, intrusion detection, virus protection and so on. This shows that with the rapid development of wireless communication, the relevant security measures lag far behind, which leads to the lack of information protection technology matching with communication technology in practical operation, which leads to the common occurrence of information leakage on a material basis. In addition, the lag in people's thinking is also an important reason for the general leakage of information. People's awareness of protecting information during wireless communication is very weak, and many people even do not know if and when their

information is stolen. The lack of awareness leads people not to believe that information leakage will have a serious impact, let alone actively install the corresponding software and hardware to protect their information. But when people receive a steady stream of spam text messages on their mobile phones, when nuisance calls continue to appear, and even when fraud and payment impersonation incidents occur, people may realize the importance of information security, but by then it may be too late. The past development history tells people that the development of wireless communication should not abandon the relevant security protection technology, nor should it ignore the improvement of ideology and law.

#### 4. CONCLUSION

This essay reveals three development directions in the field of information leakage prevention in the future wireless communication, that is, improving personal protection awareness, developing protection technology and improving relevant laws and regulatory institutions. There are still a lot of people who think that the focus of wireless development should be on speed and quality, rather than wasting time and effort on the side. The article still suggests that the development of wireless communication technology, which takes into account information security, personal awareness and legal perfection, is healthier and more sustainable. As the author Shunqing Zhang (2017) emphasized in the article, the balanced sustainable and healthy development concept is the development goal of the wireless communication industry. Because national and personal information is the right that cannot be compromised, once the trust of information security collapses, the result will seriously affect the development of wireless communication itself. Even if the industry's energy is limited and a focus on a few directions is inevitable, a

more balanced approach should still be pursued. How to balance these factors requires the wisdom of countless people in the future.

#### REFERENCES

- [1] Mannes, Elisa, & Maziero, Carlos. (2019). Naming Content on the Network Layer. *ACM Computing Surveys*, 52(3), 1-28.
- [2] Cho, Gilsu, Kim, Sangwho, & Ryou, Jaecheol. (2018). Method to Analyze Information Leakage Malware using SSL Communication in Android Platform. *Inteonet Jeongbo Hakoe Nonmunji = Journal of Korean Society for Internet Information*, 19(3), 1-6.
- [3] Wu, Xiaobin, Pratt, Thomas G, & Fuja, Thomas E. (2019). Polarization Shift Keying for Wireless Communication. *IEEE Transactions on Wireless Communications*, 18(10), 4927-4941.
- [4] Cheng, Xueqi, Yuan, Jinhong, Tajer, Ali, Hu, Aiqun, & Zhou, Wanlei. (2015). Special issue on recent advances in network and information security— security and communication networks journal. *Security and Communication Networks*, 8(1), 1.
- [5] ahalkar, Sagar. (2018). *Network Vulnerability Assessment*. Birmingham: Packt Publishing, Limited. p5-14
- [6] ngqiong Ye, Wenyu Shi, & Rui Zhang. (2021). Research on gray correlation analysis and situation prediction of network information security. *EURASIP Journal on Information Security*, 2021(1), 1-6.
- [7] dshaw, Paul. (2017). Chilling Effect. *Digital Journalism*, 5(3), 334-352.