ATLANTIS PRESS
Advances in Social Science, Education and Humanities Research (ASSEHR), volume 130
2nd International Forum on Management, Education and Information Technology Application (IFMEITA 2017)

Optical Fiber Communication Network Eavesdropping and Defensive Measures

Haiying Si [1,a] , Hao Liu [1,b]* and Hao Ma [1,c]

[1]Information Engineering School, Beijing Institute of Fashion Technology

[a]1293294245@qq.com, [b]gxyliuh@bift.edu.cn, [c]gxymh@bift.edu.cn

Keywords: optical fiber eavesdropping; optical code division multiple access; IPSec quantum key distribution

Abstract. With the development of optical fiber communication network eavesdropping technology, its security is facing new challenges in recent years. Some of the optical fiber communication eavesdropping technology cannot be detected with its hidden features, so it is necessary to study optical fiber tapping technology and its defensive measures. This paper summarized the cases in which the international optical fiber communication network had been eavesdropped in recent years, and introduced the intrusion and non-intrusive optical fiber eavesdropping methods. Based on the analysis of the general misunderstanding of optical fiber communication network security, the effective measures to defense fiber eavesdropping are put forward.

Introduction

It is widely believed that optical network is a good way to prevent hacking through wiretaps intercepting network data. But in recent years, fiber hacking technology development mature, which makes the security of the optical fiber communication. Optical fiber wiretaps is basically can be divided into invasive and noninvasive [1]. The former need to cut and optical fiber to connect again. While the latter is not to cut off the fiber or cause the disruption of any business can achieve eavesdropping. Invasive hacking main beam separation, noninvasive eavesdropping mainly includes optical fiber bending coupling method, evanescent wave coupling method, method of V groove and grating method.

Optical fiber hacking method

The beam separation. Beam separation method is the simplest and the most primitive methods of optical fiber eavesdropping. Hackers will cable cut and connected to the optical coupler, by hacking can get information you want. It should be noted that this approach can lead to link temporary interruption, usually will trigger the alarm [2]. However, for skilled technical personnel.

In this case, it may not take 1 min to connect the optical coupler to the optical link, resulting in a brief interruption that the network administrator considers to be an environmental factor or a glitch in the network. In addition, since most carriers have pre-installed point cuts on their networks to achieve the purpose of maintenance, these places naturally become an attack point for hackers.

Fiber bending coupling is legal. The optical cable is able to guide the light with the bending radius of 5 ~ 10 mm. The excessive bending of the optical cable will leak out. All internal reflection conditions will no longer be satisfied. This time can be captured and converted into electrical signals. The device developed for this purpose is known as a clip coupler, which clips the clip-type coupler onto a cable, and the signal is transferred to another optical fiber [3]. This method is simple, and even the protective layer of the cable can be removed. Carriers typically use such devices to check the connections of cables, which hackers use to intercept data. This wiretapping method takes less than 10 minutes of

operation time and is usually undiscovered because there is no link interrupt and only a very small insertion loss. By capturing a tiny fraction of the light, hackers can get 100% of the information.

The decoupling method is legal. Optical fiber communication is believed to be reliable and secure because light is trapped in optical fibers. However, although most of the signal is concentrated in the core, there is also a small amount of light leaking into the envelope, which is known as the ephemera. Remove the fiber optic cable coating and a small number of layers without touching the core, which enables the hacker to contact the dead wave and eavesdrop on the line. For a skilled technician, the whole process requires only l h. There are several ways to remove the package layer. For example, chemical etching or mechanical polishing of hydrofluoric acid. Once the target fiber optic cable is etched, a second wiretapped cable is placed on the target cable to collect the dead wave. The advantages of the decoupling legal advantage are whether the link is broken or not. Adjustable coupling ratio and extremely low loss.

V groove method. The method is to cut a V groove into the fiber envelope and close to the core. Thus, the method of wiretapping of optical fiber signals is derived. The Angle between the surface of V groove and fiber signal transmission direction needs to be greater than the critical Angle of full internal reflection. In this way, the light signal is reflected across the V groove, leaking from the other side of the fiber. The disadvantage of this approach is that the V groove requires precise cutting of optical fiber and precise polishing. And it takes a long time to install. But the light attenuation caused by this wiretapping method is so small that it is difficult to detect.

Grating method. The use of Bragg grating is the most advanced wiretapping technology, and it is difficult to detect and monitor through network test and monitoring. It USES ultraviolet laser to produce ultraviolet light for coherent superposition. The Bragg grating is formed in the target light fiber core. A partial optical signal that is reflected by the grating in the optical fiber of another optical fiber captures the hidden eavesdropping of the target fiber.

Common misunderstanding of optical fiber communication network security

The optical fiber network is safe. As mentioned earlier, fibre-optic networks can be easily tapped, and there is no absolute data security. The cable can be easily found through the well cover. In addition. The telco is another location that can easily get involved in fiber-optic networks. It is usually an important node in the network. Although the telecommunication machine room is usually protected by physical access control. But as more services are outsourced and deregulated. Old telecom operators are being forced to open their machines to outside companies, meaning the fibre network is becoming harder to protect.

These factors make OCDMA and WDM technology have significant security advantages. However, the security performance of OCDMA is lower than that of signal source encryption.

Quantum secure communication technology. Quantum communication is a kind of the information transmission by using the quantum state of communication, quantum mechanics and classical communication cross form emerging research area, and quantum information science research in the field of the earlier one of the branches, has more than 20 years of development. At present, quantum secret communication technology with quantum key distribution is developed rapidly. Quantum key distribution originated in 1984, when Bennett from IBM and Brassard of Canada jointly proposed the first quantum key distribution protocol: BB84 protocol. Unlike the classical cryptosystem, in quantum key allocation. The security of communication is guaranteed by the fundamental law of quantum mechanics.

These laws include measurement of collapse theory, Heisenberg uncertainty principle and quantum non-cloning law. Because of these laws, eavesdroppers cannot obtain the state information of a quantum state accurately, even if they intercept quantum states. This ensures that the key is fully resistant to eavesdroppers during distribution [4]. Once the two parties share a set of absolute security keys through quantum key allocation, they can use a variety of traditional encryption methods for secure and extremely secure communication. When the key length is long enough, the user can select a single one to achieve unconditional secure communication. The security of the BB84 agreement has been rigorously proved.

Although the security of quantum key distribution technology is perfect, but the actual application has a long distance journey, from the perspective of system application, the technology exists the following problems to be solved: light source, the key device, key performance rate, network application form etc.

IPSec encryption technology. IPSec encryption is an open layer 3 encryption technology that encrypts the transmitted IP data packets at the network layer (i.e., the Internet layer). IPSec encryption provides a mechanism for secure communication on unreliable IP networks, where only the sender and receiver need to know about IPSec.

Because IPSec encryption increases the size of the data packet and needs to be decrypted at both ends. So it increases the delay in communication. In IPv4, IPSec is optional, and in IPv6 it is mandatory. In this way, as IPv6 becomes more popular, IPSec will be more widely used [5].

Summary

In the three encryption techniques introduced in this paper, quantum secret communication security is the highest, and the IPSec center is the worst. The strategy of deploying encryption technology is to select according to the value and security level of the transmission information. Second, consider the probability of eavesdropping.

Once again, the maturity of the encryption technology and the construction cost should be considered, and the long-term development should be considered. With the promotion of science and technology, China's optical fiber communication technology has developed better, which has satisfied people's increasing communication needs and promoted people's interpersonal communication.

Based on optical fiber communication technology, the development of hacking technology matures, also not only reduces the confidentiality of the optical fiber communication, and hindered the development better optical fiber communication technology, so the technical personnel must take effective defense eavesdropping detection technology, guarantee the information security, so as to better play the role of optical fiber communication.

Acknowledgements

This research was financially supported by Beijing Institute of Fashion Technology under Grant NHFZ20170061/001 and KYTG02170201/013.

References

[1] Chen hui, zhu shixiong. Discussion on optical fiber communication wiretapping and detection technology [J]. Information security and communication confidentiality, 2012.

[2] Wang dingwang. Discussion on optical fiber communication wiretapping and its detection technology [J]. Construction engineering technology and design, 2015.

[3] Richard c.haskelli Rui. Optical fiber communication network eavesdropping methods and defensive measures [J]. Journal of telecom science, 2012.

[4] Deng dapeng, sheng xing, zhang bin, et al. Research on eavesdropping detection methods in interferometric optical fiber sensor systems [J]. Optical communication research, 2011.

[5] Yu ningna. Research on the multiplexing technology of quantum key distribution and single wavelength of classical fiber communication [D]. South China normal university, 2014.