Research Based On The Security Of Optical Fiber Transmission

Yonghao Li[1], Yifeng Wang[2, a)]

[1] *College of Information and Electronic, Shandong Technology and Business University, Yantai, China*
[2] *College of Information Engineering, Shanghai Maritime University, Shanghai, China*

[a)] 202310320136@stu.shmtu.edu.cn

Abstract. At present, the optical fiber transmission technology is developing more and more rapidly. In the meantime, the discussion on the security issues triggered by it has become more and more intense. Based on this, this article summarizes the mainstream methods for improving the security of optical fiber transmission technology at the present stage. This can provide the certain reference direction for future research and exploration. Currently certain accomplishments have been attained in the physical layer, management layer, the network layer, the encryption technology, and the access control. But at the same time, there are also some disadvantages in certain aspects. For example, the complexity of the encryption technology is too high, the cost of the management layer is too excessive, and the difficulty of constructing the network layer is too great. In the future, more in-depth research can be conducted in material improvement, intelligent management, optimization of encryption technology, construction of secure networks, and detection of intrusion signals. This will further enhance the security of optical fiber transmission technology.

INTRODUCTION

Optical fiber communication has been widely applied in today's era. As the constant improvement and development of optical fiber communication technology, it has had many characteristics such as high quality, anti-distortion, secure and huge-capacity [1]. However, more security flaw will be brought because of the high usage rate. Any security flaw may cause large-scale data leakage and cessations of transmissions. In recent years, facing the increasingly complicated internet safety menaces, scientists proposed new systems and techniques of safety transmissions and continuously optimized existing conservation system. During the courses of innovation, enormous challenges emerged.

The paper concludes the mainstream approaches to protect the security of the transmission up to now, including the protection strategies in several dimensions such as encryption technologies, physical security, network layer security, access control and human management. Various cutting-edge technologies in encryption technology and network layer security are analyzed. The advantages and disadvantages of chaotic encryption technology, optical code multi-addressing and quantum noise stream encryption as well as network structure design of communication security, fiber optic communication security defense methods, fiber tapping detection technology and other network layer technologies are discussed.

PHYSICAL SECURITY AND HUMAN MANAGEMENT

Physical Security

If there is no shelter in case of strong wind and heavy rain in the external environment, the impact on the fiber optic transmission will be serious, which will directly affect the signal propagation speed and communication capacity, even directly block the signal transmission [2]. Therefore, the impact of severe weather on fiber optic transmission is

relatively large, and corresponding defense measures should be taken. The transmission loss of fiber by the severe natural conditionsto secure the safe transmission of information can be reduced by upgrading the material of fiber. In the current stage, BT polybutylene terephthalate, Ultraviolet cured ink, etc. is mainly used in our country, the protection against the external environment will be improved in the future with the improvement of optical fiber materials [2].

Human Management

Improve the Professional Quality of Technicians

The professional skills and work literacy of relevant technicians will directly affect the security of optical fiber transmission. Only by solving problems in time through professional means can avoid many unnecessary leaks and delays. Therefore, it is necessary to establish a complete talent training system. In the talent selection stage, establishing a scientific evaluation system requires paying attention to both the examination of theoretical knowledge and practical operation ability. In the work stage, special seminars and technical exchanges should be organized regularly to draw lessons from the successful experience of foreign countries, actively learn advanced technology and help technicians master the latest technical dynamics and safety protection methods in time. Especially in the current era of rapid technological progress, it is even more important to pay attention to the construction of an updated system. In addition, the enthusiasm of technicians should be improved by reasonable salary increase, rewarding those who have made contributions and improving working conditions.

Strengthen Management

For optical fiber transmission network, a multi-dimensional security monitoring system needs to be established. By deploying professional equipment such as optical power monitoring and OTDR test, technicians can make real-time detections of the status of optical fiber lines, timely identification of potential interference factors and risk factors. When building a communication network system, scientific safety control strategies should be implemented. Establish a systematic management system and operation standards. Ensure that equipment is in accordance with the relevant standards with strict management, to maintain the continuity and stability of power supply, providing a more reliable guarantee for signal transmission.

ENCRYPTION TECHNOLOGY

Chaotic Encryption Technology

On the encryption end, first generate the basic chaotic sequence, and preprocess the plain text to be encrypted. The plain text data is then scrambled with the chaotic sequence to generate a cipher text and sent to the decryption end. Then, the decryption end generates a chaotic sequence that is synchronized with the initial sequence to decrypt, according to the predetermined conditions, the correct initial plain text [3]. Chaos encryption can be combined with orthogonal frequency division multiplexing (OFDM), which greatly reduces the complexity of the algorithm and can also be applied in network data security. Although chaotic encryption has high security and strong anti-jamming ability, the difficulty of synchronizing the current chaotic sequence has become the biggest obstacle to its upgrade and optimization.

Optical Code Division Multiple Access

Each different user is divided into a unique optical code that is never repeated, and the code is transmitted through the same fiber. Data is only recovered at the receiving end when the address code received matches the address code transmitted [4], [5]. And through the wavelength-division multiplexing (WDM) or optical time-division multiplexing (OTDM) is combined to improve the capacity and transmission rate of fiber optic transmission. However, the complexity of optical code division multiple access is high, which also affects its prospects and development.

Quantum Noise Stream Encryption

Quantum noise stream transforms binary signals into high-dimensional signal sets, taking advantage of the fluctuations of the phase and amplitude of light to perform encryption, and establishes security through the huge difference in signal-to-noise ratio (SNR) between legitimate receivers and eavesdroppers. The quantum noise conceals the genuine plain text among false items, and the difficulty of cryptanalysis is increased by the addition of random noise components [6]. It has been experimentally proven that under the correction of low-density parity-check (LDPC), the legitimate communicator can still guarantee a bit error rate of 0 within 300 km. As the distance increases, the probability of Eve intercepting the information becomes increasingly lower. When the transmission distance is 300 km, Eve's error rate approaches 100%, and the information interception probability is 0.001% [6]. Currently, quantum noise flow encryption is mainly divided into three categories: phase modulation noise flow encryption (PSK/QNSC), amplitude modulation noise flow encryption (ASK/QNSC), amplitude-phase modulation noise flow encryption (QAM/QNSC) [7]. Table 1 is a comparative analysis of the three types of noise flow encryption.

TABLE 1 Comparison of three categories of quantum noise flow encryption

Technical name	Features	Effects
PSK/QNSC	The sending and receiving parties share a seed key and signal mapping rules. Without knowing the bases, even if Eve knows the content of the protocol, the signal is masked by the noises. Therefore, the content is still hard to be judged.	The probability that Eve can correctly identify it is low.
ASK/QNSC	The noise comes with the 0, 1 signal, the legitimate receiving end can correctly generate the original signal, while Eve, the eavesdropper, even if he knows the large number of bases, needs to prepare the detection of the electrical level. Due to the superposition of noise, the expected signal SNR decreases, and the signal is covered by noise, which is hard to identify.	The greater the number of bases, the better the security.
QAM/QNSC	High data rates, long distances, and high spectral efficiency. The legitimate receiver can recover the data by pre-shared the key, while Eve cannot, which guaranteed the security.	Since the noise is random, such noise flow encryption has good security.

Specifically, at the application level, QNSC plays an important role in terahertz communication, ensuring the security of partial data, but still faces problems such as eavesdropping and jamming to be resolved. In satellite communication, QNSC can achieve secure protection for remote data transmission. Quantum noise flow encryption can coexist with traditional wavelength division multiplexing communication system, and can be transmitted over a long distance [8]. Table 2 is a comparison of three encryption techniques.

TABLE 2 Comparison of three encryption techniques

Method	Advantages and disadvantages	Application	References
Chaotic encryption technology	Advantages: Strong anti-interference capability, unpredictability; Disadvantage: High difficulty in synchronization.	Combined with orthogonal frequency division multiplexing, internet data	<The Application of Chaotic Encryption Technology in Network Data Secure Transmission>
Optical Code Division Multiple Access (OCDMA)	Advantages: High security, large capacity, simple structure; Disadvantages: High complexity.	Combined with wavelength division multiplexing or optical time-division multiplexing	<Research on Optical Fiber Physical Layer Security Technology for Key Life cycle>
Quantum Noise Stream Encryption (QNSC)	Advantage: High security Disadvantage: Encryption and decryption will cause additional SNR loss	Terahertz communication, satellite communication, etc.	<Fiber Physical Layer Secure Transmission Technology Based on Quantum Noise Stream Cipher>

NETWORK LAYER SECURITY

Design of Communication Security Network Architecture Based on Optical Cable Network

By expanding and renovating the optical cable section, selecting Huawei OSN3500 series 10G equipment for networking., adjusting the distance between the equipment sites., adopting the networking with intersecting rings between the access network and the backbone network, as well as tangent rings between access networks. These measures can optimize the optical cable network structure, upgrade the backbone network equipment, adjust resources and reconstruct the structure of the fiber optic access network. Thereby improving the security performance of the transmission network [9].

Defense Methods for Security of Fiber-Optic Communication Based on Big Data Technology

At first, according to the Bayes' theorem, optimize the links of abnormal signal collection and identification. And then, use the support vector machine to classify abnormal signals and determine the type of the attack signal. Finally, construct a defense time series to defend against the attack information. Through this method, the false positive rate can be reduced to less than 1%, and the defense success rate can be increased to more than 98%, thereby ensuring security effectively [10].

Optical Fiber Eavesdropping Detection Technology Based on the State of Polarization of the Signal

Use the angular velocity of the polarization state as the key indicators for distinguishing the eavesdropping behavior. By setting different thresholds to distinguish different signal states, so that the recognition accuracy rate can reach 95.38%. Besides, using a machine learning algorithm to analyze the data and further optimize the parameters of the LSTM model. This can increase the classification accuracy rate to 99% [11].

Use Network Traffic Analysis Tools

By deploying network traffic analysis tools, configuring monitoring parameters, collecting network traffic data and detecting the presence of abnormal traffic to provide real-time warnings. These actions can help security officers find and solve potential security problems, and maintain the security of the network layer [12]. Table 3 is a comparison of these four methods.

TABLE 3 Comparison of four methods

Method	Result	Application	References
Design of communication security network architecture based on optical cable network	Optimize the structure of the optical cable network, improve the resource utilization rate of optical cable resources, enhance the security of the communication service network	Construction of communication networks	<Construction of Communication - security Network Based on Optical Cable Network>
Defense methods for security of fiber-optic communication based on big data technology	Reduce the false alarm rate and miss-alarm rate of attack signal detection, improve the success rate of defense	Security monitoring, intrusion detection and defense systems	<Defense method of optical fiber communication based on big data technology>
Optical fiber eavesdropping detection technology based on the state of polarization of the signal	Improve the recognition accuracy rate of eavesdropping detection and the classification accuracy rate among different states	fiber - optic anti - eavesdropping technology	<Fiber Optic Eavesdropping Detection Technology Based on State of Polarization of Signal>
Use network traffic analysis tools	Enable real-time monitoring and provides real - time early warnings	Automated response to security incidents	<Security - guarantee Technology for Data Transmission in Fiber - Optic Communication>

ACCESS CONTROL

Access Control

As another significant method to ensure the security of fiber transmission, the access control mechanism can significantly enhance the security of transmission by managing permissions. This strategy adopts a hierarchical authorization mode for key management, where high-level users can not only access data at their level but can also derive the access permissions of lower-level users based on the keys, thereby accessing more resources [13]. By authenticating user identities in real-time, illegal intrusion attempts can be effectively intercepted. This strategy not only prevents external invasions but also guards against the escalation of privileges by internal users. Based on the analysis of abnormal behavior, potential security threats such as data theft and information tampering are promptly identified, ensuring the integrity and security of transmission.

Authentication Mechanism

Another important guarantee of security in fiber-optic transmission is the authentication mechanism. The authentication mechanism ensures that the user is authorized by verifying the user's real identity, preventing illegal unauthorized access. Common verification methods include but not limited to digital passwords, digital certificates, biometric recognition technology, and two-factor authentication, etc. [12]. These measures can not only effectively

maintain the confidentiality of data transmission but also optimize the overall network operation efficiency. At the same time, when formulating the permission management and authentication scheme, it is also necessary to take into account the requirements and management difficulties of the network scale, which is very important for the spread of large-scale fiber-optic networks.

CONCLUSION

This article summarizes the current methods from the encryption technology, the network layer, the access control, the human management, and the physical layer. These methods can enhance the security of optical fiber transmission technology and provide reference value for the future development direction of optical fiber transmission security technology. However, this article has not conducted in-depth research in the selection of physical materials, the reduction of the complexity of encryption technology, and the control of eavesdropping detection risks. In the future, it is hoped that new technologies and methods can be proposed in the application of new materials, the introduction of intelligent management, the improvement of encryption technology, the upgrade of signal detection technology, and the design of secure networks. This will make optical fiber transmission become a more reliable data transmission channel.

AUTHORS CONTRIBUTION

All the authors contributed equally and their names were listed in alphabetical order.

REFERENCES

1. Gang Han. Security Risks and Countermeasures of Optical Fiber Transmission Systems. China New Telecommunications, 17(07):15-16(2015).
2. Xiaoshan Liu, “Analysis of Security of Optical Fiber Transmission” in *Railway Communication Network and Its Protective Measures* in *China New Telecommunications*, 23(06):28-29(2021).
3. Chenguang Zhu and Erxin Wang, “The Application of Chaotic Encryption Technology” in *Network Data Secure Transmission*. Cyber security and IT application, (01):137-139(2025).
4. Mendez A J, Gagliardi R M, Hernandez V J, et al. “High-performance optical CDMA system based on 2-D optical orthogonal codes” in *Journal of lightwave technology*, 2004, 22(11): 2409.B. R. Jackson and T. Pitman, U.S. Patent No. 6, 345, 224 (8 July 2004).
5. Tan Y, Pu T, Zheng J, et al. “Secure performance analysis of optical CDMA systems based on secrecy capacity” //in *Frontier Research and Innovation in Optoelectronics Technology and Industry,* CRC Press, 2018: 355-360.
6. Xu Zhang, Jie Zhang, Yajie Li, Huibin Zhang, Chao Lei, Zhiwei Tu, “Fiber physical layer secure transmission technology based on quantum noise stream cipher” in *Optical Communication Technology*, 2020, 44(04):18-22.
7. Xiangqing Wang, “Research on Physical Layer Security Authentication and Encryption Technology of Optical Network”, Beijing University of Posts and Telecommunications, 2021.
8. FUTAMI F, “HIROTA O. 40 Gbit/s （4×10 Gbit/s）Y-00 protocol for secure optical communication and its transmission over 120 km” // in *Optical Fiber Communication Conference and Exposition （OFC/NFOEC）*, March 4-8, 2012, Los Angeles, United States. New York: OSA, 2012: 1-3.
9. Enyu Yuan, “Construction of Communication - security Network Based on Optical Cable Network” in *Computer Knowledge and Technology*, Vol.20, No.7(March 2024).
10. Guanghui Zhai, “Research on security defense method of optical” in *LASER JOURNAL*, Vol. 44, No. 9 (September, 2023).
11. Qing Lei, “Fiber Optic Eavesdropping Detection Technology Based on State of Polarization of Signal”, Beijing university of posts and telecommunication, 30 Date 5 Month 2024Year.
12. Jie Zhang, “Security guarantee Technology for Data Transmission in Fiber Optic Communication”, www.365master.com (2024.7).
13. Yanlong Han, Yuanyuan Hu, “Research on data access control and encrypted storage technology of Internet of things in optical fiber network communication” in *LASER JOURNAL*, 41(09):97-101(2020).