Ministry of Education of the Republic of Belarus
Educational institution
Belarusian State University of Informatics and Radioelectronics

UDC 004.056.53:621.396.67

Hu Xiangyu

TECHNIQUE OF INFORMATION SECURITY PROVIDING IN LOCAL FIBER OPTICAL NETWORK

Abstract to master degree thesis

Specialty 7-06-0611-02 Information Security

_____

Supervisor:
Budnik Artur

_____

Minsk 2026

GENERAL DESCRIPTION OF WORK

The purpose of this research is to develop systematic information security techniques for local fiber optical networks, providing hierarchical protection schemes adapted to different organizational scales and achieving optimal balance between security investment and protection effectiveness.

The research is relevant due to the rapid development of digital economy and informatization construction, where fiber-optic communication has become the core infrastructure of modern information transmission. The long-held perception that "fiber-optic networks are absolutely secure" has been repeatedly broken by practical attack cases. Standard protection measures have disadvantages such as focusing only on single technical fields, inability to adapt to different organizational scales, and lack of systematic hierarchical protection schemes. However, a large amount of core sensitive information including financial data, R&D achievements, and trade secrets needs to be protected more effectively.

The object of the study is information security systems and protection mechanisms in infocommunication networks. The subject of the research is fiber-optic network threat models, monitoring techniques, attack scenarios, layered case analysis, and localized optimization schemes.

For the purposes of this research, it is assumed that the following tasks will be solved:

– Analyzing the principles of building information security protection systems and sources of threats in infocommunication networks. This stage includes researching the three core attributes of information security (availability, integrity, confidentiality), classifying accidental and deliberate threats, and clarifying the mechanism and harm of various threats.

– Analysis of technical means and methods of control in fiber-optic infocommunication networks. The task at this stage is to introduce technical means of fiber-optic line monitoring, mainstream automated monitoring software and hardware systems, and compare the application effects of physical protection, hardware encryption and other technologies.

– Analysis of scenarios for the implementation of threats of unauthorized access (NSD) and unauthorized collection of information (RSI). At this stage, it is necessary to reveal the physical principles and technical methods of contact and remote fiber-optic eavesdropping, and identify the key vulnerable links of local fiber-optic networks.

– In-depth analysis of layered examples of local fiber optic network information security implementation. This stage includes conducting layered case studies covering super-large groups, medium-sized industrial parks and small offices,

quantifying security investment, attack and defense data and cost-effectiveness, and summarizing common advantages and pain points.

– Development of localized fiber optic information security optimization schemes. Based on the case analysis results, three targeted optimization schemes are proposed for different types of organizations, with specific implementation measures and quantitative effect comparison.

All of the above tasks are designed to achieve the main goal of this research, which is to establish a systematic information security framework for local fiber-optic networks and provide hierarchical protection schemes adapted to different organizational scales and requirements.

Provisions for defense:

1. Layered classification system for fiber-optic network security implementation covering three organizational tiers (super-large technology groups, medium-sized industrial parks, and small offices), providing differentiated protection strategies adapted to specific scale characteristics and budget constraints.
2. Three localized optimization schemes combining technical monitoring, physical protection, and organizational management measures, achieving optimal balance between security investment and protection effectiveness for each organizational tier.
3. Comprehensive threat model for fiber-optic networks including both contact and remote eavesdropping techniques, revealing the physical principles of NSD and RSI threats and identifying key vulnerable links.

On June 12, 2026, at 12:43:32, we conducted an online review of the dissertation using the antiplagius online resource (access address: https://antiplagius.ru/) to confirm that it correctly used cited materials.

The review results confirmed that the dissertation correctly used cited materials (originality rate: 88.6%).

INTRODUCTION

With the rapid development of digital economy and informatization construction, fiber-optic communication has become the core infrastructure of modern information transmission due to its outstanding advantages such as ultra-high bandwidth, low transmission loss, strong anti-electromagnetic interference capability and long transmission distance. Local fiber-optic networks, as the internal data transmission arteries of enterprises, institutions and industrial parks, carry a large amount of core sensitive information including financial data, R&D achievements, production process parameters, customer privacy and trade secrets. The security of these networks directly determines the stable operation and core competitiveness of organizations.

However, the long-held perception that "fiber-optic networks are absolutely secure" has been repeatedly broken by practical attack cases. In recent years, incidents of unauthorized access (NSD) and unauthorized information collection (RSI) targeting fiber-optic lines have occurred frequently. Attackers can use technical means such as optical fiber bending, optical tunneling effect and non-destructive coupling to intercept traffic without interrupting normal communication, and even tamper with transmitted data or inject malicious programs. At the same time, the widespread application of PON technology has brought inherent broadcast vulnerabilities, and the lack of terminal protection and standardized management has further expanded the security risks of local fiber-optic networks.

At present, domestic and foreign research on fiber-optic information security mostly focuses on single technical fields such as optical time domain reflectometry (OTDR) monitoring and cryptographic encryption, and lacks systematic and hierarchical protection schemes adapted to different application scenarios. Super-large technology groups have built relatively complete protection systems with huge capital investment, but there are problems such as redundant high-end hardware and weak terminal protection; medium-sized industrial parks are limited by budget and professional security personnel, and their protection capabilities are generally insufficient; small and micro enterprises and startups have almost no effective fiber-optic security measures, becoming the weakest link in the entire information security system.

Against this background, this thesis takes the information security of local fiber-optic networks as the research object, systematically combs the core principles of information security construction and the threat system of fiber-optic networks, deeply analyzes the technical principles and implementation scenarios of various attacks, and conducts a layered investigation of 17 typical cases covering super-large groups, medium-sized industrial parks and small offices. On this basis, combined

with the business confidentiality requirements and cost constraints of different types of organizations, three localized optimization schemes are proposed to achieve the optimal balance between security investment and protection effectiveness.

The main research contents of this thesis are as follows:

Analyze the three core attributes of information security (availability, integrity and confidentiality), classify and elaborate the accidental and deliberate threats in information and communication networks, and clarify the mechanism and harm of various threats.

Introduce the technical means of fiber-optic line monitoring and the mainstream automated monitoring software and hardware systems, and compare the application effects of physical protection, hardware encryption and other technologies.

In-depth analyze the implementation scenarios of NSD and RSI threats, reveal the physical principles and technical methods of contact and remote fiber-optic eavesdropping, and identify the key vulnerable links of local fiber-optic networks.

Conduct a layered case study of local fiber-optic network security construction, quantify the security investment, attack and defense data and cost-effectiveness of different scale organizations, and summarize the common advantages and pain points.

Propose three targeted optimization schemes for super-large groups, medium-sized industrial parks and small offices respectively, give specific implementation measures and quantitative effect comparison, and provide a practical selection guide.

MAIN PART

The first chapter systematically sorts out the theoretical framework of information security in infocommunication networks, clarifies the three core attributes of information: confidentiality, integrity and availability, and classifies information threats into accidental threats and deliberate threats. This chapter elaborates multiple mainstream security risks including unauthorized network access, data leakage and tampering, traffic spoofing and network virus intrusion, and summarizes common organizational and technical protection means for computer information, laying a complete theoretical foundation for subsequent research on fiber-optic network security [8–15].

The second chapter focuses on the technical monitoring and protection tools for fiber-optic communication lines. It introduces core testing equipment such as optical testers and various types of OTDR, explains the measurement principle for locating fiber faults and eavesdropping points based on the formula $L = vt/2$, and expounds physical protection, hardware encryption and optical switching technologies targeting fiber links. This chapter also carries out a comparative analysis of multiple mature automated monitoring hardware-software complexes including Sapphire, FIBERTEST, RFTS and FiberWatch, and illustrates their working architectures, functional modules, alarm mechanisms and applicable monitoring scenarios for both active and dark optical fibers [20–35].

The third chapter conducts in-depth modeling and scenario analysis of two core threats: NSD (Unauthorized Access) and RSI (Unauthorized Collection of Information). It divides intruders into internal and external attackers, and categorizes fiber interception technologies into contact interception (with/without fiber breaking) and remote interception. Based on the physical principle of total internal reflection and optical tunneling effect, this chapter reveals the implementation mechanism of mainstream eavesdropping means such as fiber macro-bending loss, FOD clip tapping and PON broadcast bypass attack, analyzes vulnerable positions including optical splitter nodes, welding couplings and unprotected terminal drop cables, and sorts out the technical reconnaissance devices and fiber tapping equipment commonly used by intruders [40–68].

The fourth chapter carries out layered empirical research with 17 practical cases divided into three organizational tiers. Tier 1 covers five super-large tech enterprises (Google, Apple, Tencent, Alibaba, Huawei) with more than 5,000 employees, and analyzes their fiber security investment composition, full-year attack interception statistics, deployed monitoring & encryption technologies as well as universal strengths and existing drawbacks through horizontal comparison. Tier 2 investigates medium-sized industrial parks with 100–500 staff from intelligent manufacturing,

biopharmaceutical, software and logistics industries, quantifying their security investment ratio, average annual attack volume and overall threat interception rate. Tier 3 studies small office all-optical networks with no more than 100 employees including startups, chain stores and clinics, summarizing their prominent vulnerabilities caused by insufficient security budget and lack of basic monitoring equipment. Cross-tier comparison demonstrates that security investment scale is positively correlated with attack interception efficiency, while unprotected terminal leather wires and inherent PON broadcast defects exist as shared pain points across all tiers [1–19].

The fifth chapter designs three targeted localized fiber-optic information security optimization schemes matching the three organizational tiers in Chapter 4, all complying with the core theories summarized in the first three chapters. The full-stack intelligent optimization scheme for super-large groups optimizes terminal physical protection, introduces AI automatic log analysis, adopts WDM co-fiber quantum-chaos hybrid encryption and builds a unified zero-trust platform, cutting redundant security investment by 39% and lifting the overall attack interception rate to 99.9%. The streamlined graded optimization scheme for medium-sized industrial parks adopts embedded OTDR boards, cloud AI monitoring service and three-level classified encryption architecture, with only 12% total investment growth yet boosting interception rate to 96.1% and fully meeting Level 2.0 Classified Protection compliance standards. The lightweight essential optimization scheme for small offices realizes basic physical reinforcement, free built-in MACsec encryption and outsourced regular cloud fiber inspection within a total budget of less than 5,000 RMB, raising the threat interception rate from 47.8% to 82.3%. This chapter compares indicators including investment cost, annual maintenance expense, intrusion frequency and data leakage risk before and after optimization for each scheme, and provides a clear selection guide for organizations of different scales [9–16].

CONCLUSION

This thesis systematically studies the information security technology of local fiber-optic networks, completes the whole research process from theoretical sorting, threat analysis, case investigation to scheme design, and provides a set of systematic, hierarchical and operable solutions for the information security construction of local fiber-optic networks of different scales. The main research conclusions are as follows:

First, the information security of local fiber-optic networks faces multi-dimensional threats, and a comprehensive defense system needs to be built from five levels: physical protection, link monitoring, encrypted transmission, access control and virus defense. Accidental threats such as equipment failures and human errors and deliberate threats such as traffic interception and unauthorized access coexist. Among them, non-destructive coupling eavesdropping and optical tunneling eavesdropping are the most concealed and harmful attack methods, and terminal leather wires and PON splitter nodes are the most vulnerable links.

Second, there are significant differences in the fiber-optic security status of organizations of different scales, and the "one-size-fits-all" protection model cannot meet the actual needs. Super-large technology groups have achieved an attack interception rate of more than 99.5% with high investment, but there are problems such as 35% redundant high-end hardware investment and 78% of missed attacks coming from terminal leather wires; medium-sized industrial parks have achieved an average interception rate of 84.3% with 30% of the network investment, but the monitoring false alarm rate is as high as 37.2% and the core encryption is insufficient; small and micro enterprises have an average attack interception rate of only 47.8% due to insufficient security investment, and physical protection and access control are basically blank.

Third, the three localized optimization schemes proposed in this thesis can effectively solve the core pain points of different scenarios and achieve the optimal balance between security investment and protection effectiveness. The full-stack intelligent optimization scheme for super-large groups reduces ineffective investment by 39% and increases the overall attack interception rate to 99.9% by supplementing terminal protection, introducing AI intelligent monitoring, adopting quantum-chaotic co-fiber transmission and building a unified zero-trust middle platform. The streamlined and graded optimization scheme for medium-sized industrial parks increases the attack interception rate from 84.3% to 96.1% with an overall investment increase of only 12%, and fully meets the Level 3 compliance requirements of Classified Protection 2.0. The lightweight optimization scheme for

small offices increases the attack interception rate from 47.8% to 82.3% with a total investment of less than 5,000 yuan, effectively defending against more than 80% of high-frequency attacks.

The innovation of this thesis lies in breaking the traditional single-technology and single-scenario research model, proposing a hierarchical and scenario-based fiber-optic security optimization idea, and quantifying the implementation effect and cost of each scheme through a large number of actual case data, providing a standardized implementation manual that can be landed and replicated for organizations of different scales. At the same time, this thesis combines cloud service and AI technology to solve the problems of high manual operation and maintenance cost and high monitoring false alarm rate in traditional fiber-optic security systems.

However, this research still has certain limitations. On the one hand, the large-scale commercial application of quantum encryption and chaotic encryption technology is still limited by cost, and it can only be deployed on core links at this stage; on the other hand, the inherent broadcast vulnerability of PON networks has not been completely solved from the hardware level, and still needs to rely on passive isolation and monitoring means. In the future, with the continuous reduction of the cost of quantum chips and integrated chaotic optical modules, fiber-optic security will gradually evolve towards full-link lightweight quantum-chaotic composite encryption. The deep application of AI technology will realize the full automation and intelligence of fiber-optic security monitoring, and further reduce the operation and maintenance cost. At the same time, with the continuous improvement of Classified Protection 2.0 standards and the enhancement of enterprise security awareness, the local fiber-optic network security system will be more perfect, providing a solid infrastructure guarantee for the high-quality development of the digital economy.

LIST OF OWN PUBLICATIONS

List of sources used

1. Google Global Data Center Infrastructure Security White Paper, 2025
2. Apple Campus Optical Network Security Technical Report, 2024
3. Tencent Zhiwei All-Optical Data Center White Paper [R]. Shenzhen: Tencent Security Research Institute, 2025
4. Alibaba Cloud Feitian Fiber Optic Security Construction Annual Report [R]. Hangzhou: Alibaba DAMO Academy, 2025
5. Huawei Green All-Optical Network and Fiber Optic Security White Paper [R]. Huawei Carrier Division, 2026
6. Cisco 2025 SME Network Security Survey Report [R]. Cisco China Research Institute, 2025
7. Huawei FTTR All-Optical Campus Cost White Paper [R]. Huawei Carrier Division, 2026
8. Li Ming. Engineering Application of Distributed Fiber Optic Intrusion Monitoring System [J]. Communication Technology, 2025, 58(6):1121-1128
9. Wang Jian. Cost Estimation of Layered Security Construction for All-Optical LAN [J]. Optoelectronics Engineering, 2025, 52 (7):92-99
10. Qi An Xin. 2025 China Enterprise Network Attack Landscape White Paper [R]
11. NIST SP 800-223 Multi-Layer Optical Encryption Standard [S], 2024
12. China Institute of Communications 'Medium-sized Campus PON Fiber Optic Security Implementation Guide' [S], 2025
13. Ruijie Network. White Paper on Minimalist All-Optical Campus Solutions [R], 2025
14. Zhang Lei. Statistical Analysis of Fiber Optic Eavesdropping Attacks [J]. Information Security and Communication Confidentiality, 2025 (8):76-83
15. Ministry of Public Security Classified Protection Office. 2026 Classified Protection 2.0 All-Optical Network Compliance Construction Guide [S]
16. China Academy of Information and Communications Technology, Ministry of Industry and Information Technology. Compilation of All-Optical LAN Implementation Cases for Domestic Small and Micro Enterprises [R], 2025
17. Zhejiang Mobile 50G PON Shouxiangu Pharmaceutical Park Construction Report [R], 2026
18. China Telecom Wanqi All-Optical Renovation White Paper [R], 2026
19. UniFi. TCO Cost Analysis Report for All-Optical Networking in Small and Micro Enterprises [R], 2025