Research on Network Security Automatic Protection Technology Based on Artificial Intelligence

Fengzhi Tao
Zibo Polytechnic University, Zibo, Shandong, China

Abstract: With the continuous expansion of network application scenarios and the continuous upgrading of cyber attack means, traditional manual and static network security protection methods can no longer adapt to complex and changeable cyber threat environments. This study aims to solve the problems of low efficiency, poor real-time performance and weak adaptability of existing network security protection systems. It adopts literature analysis, technical framework construction and theoretical demonstration methods to sort out the application logic of artificial intelligence in network security fields. This paper analyzes the practical defects of traditional protection technologies, constructs an intelligent automatic protection system covering threat perception, identification and active response, and verifies the technical applicability of AI-driven network security defense. The research results show that artificial intelligence technology can effectively improve the automation level and threat response efficiency of network security protection, providing reliable technical support for modern network security risk prevention and control.

Keywords: Artificial Intelligence; Network Security; Automatic Protection; Threat Defense; Intelligent Perception

1. Introduction

1.1 Research Background

The rapid popularization of cloud computing, Internet of Things and 5G communication technologies has promoted the full penetration of network information systems in industrial production, social operation and daily life. Network boundaries have become increasingly blurred, and the types of network access terminals and data transmission scales have shown explosive growth. The continuous evolution of cyber attack modes has brought unprecedented challenges to network security governance. Modern cyber threats present obvious characteristics of intelligence, diversification and concealment. Common attack behaviors such as network intrusion, data leakage, virus propagation and malicious scanning are no longer limited to single and fixed attack modes. Attackers use variable attack paths and camouflage means to break through traditional security defense barriers, which greatly increases the difficulty of network security operation and maintenance.

Traditional network security protection relies on fixed rule bases, manual monitoring and passive defense mechanisms. Security operation personnel need to screen massive network traffic data and log information to identify potential threat behaviors. This manual intervention mode consumes a large amount of human resources and cannot cope with high-frequency and large-scale network attacks in real time. The fixed defense rules set by traditional systems have poor adaptability to unknown zero-day threats and variant attack behaviors, which easily leads to missed detection and false detection of threats. In the current complex network ecological environment, the gap between traditional static defense technologies and actual security protection demands is gradually expanding. It is urgent to introduce intelligent technical means to realize autonomous perception, automatic identification and intelligent disposal of network security risks.

Artificial intelligence technology represented by machine learning and deep learning has strong data mining, feature learning and autonomous reasoning capabilities. It can extract implicit threat features from massive and complex network data, realize dynamic identification of unknown attacks, and complete automatic response and disposal of security incidents without excessive manual intervention. In recent years, artificial intelligence has been gradually applied in many subdivisions of network

security such as threat detection, vulnerability mining and security early warning. The integration of artificial intelligence and network security automation protection has become the core development direction of modern network security defense system construction, and also provides a new technical path to make up for the defects of traditional defense modes.

1.2 Research Significance

The research on artificial intelligence-based network security automatic protection technology has important practical value and theoretical significance for the development of network security discipline and industrial security construction. In terms of theoretical significance, this study systematically sorts out the internal correlation mechanism between artificial intelligence technology and network security automatic protection, clarifies the technical logic of intelligent algorithms acting on network threat perception, feature recognition and risk response. It optimizes the theoretical system of intelligent network security defense, makes up for the deficiency of systematic research on automated protection technology in existing intelligent security research, and provides theoretical reference for subsequent in-depth research on AI-enabled network security intelligent defense.

In terms of practical significance, with the continuous upgrading of social informatization level, industrial control systems, electronic communication networks and public service network platforms have higher requirements for network security stability and threat response efficiency. The intelligent automatic protection technology constructed in this study can effectively reduce the dependence of network security operation and maintenance on manual work, improve the real-time and accuracy of network threat identification, and realize active early warning and rapid disposal of network security risks. It can solve the pain points of low defense efficiency and poor adaptability of traditional security systems, effectively guarantee the safe and stable operation of various network information systems, and provide solid technical support for social network information security and industrial data security governance.

2. Related Theoretical Basis and Technical Overview

2.1 Core Theories of Network Security Automatic Protection

Network security automatic protection refers to a comprehensive security defense mode that relies on computer technology, network technology and intelligent algorithm technology to realize autonomous monitoring, automatic identification, intelligent early warning and automatic disposal of network security risks without continuous manual intervention. The core goal of automatic protection is to break the limitations of manual defense and passive defense, build a closed-loop defense system of "real-time monitoring - accurate identification - rapid early warning - automatic disposal - dynamic optimization", and realize the whole-process intelligent management of network security risks.

The theoretical system of network security automatic protection covers network traffic analysis theory, security risk assessment theory and dynamic defense theory. Network traffic analysis theory focuses on mining abnormal data features in network transmission processes, distinguishing normal business traffic from malicious attack traffic through data feature comparison and rule matching, which is the basic support for threat identification. Security risk assessment theory quantifies the threat level, vulnerability degree and loss risk of network security events, providing basis for hierarchical disposal of security risks. Dynamic defense theory emphasizes real-time adjustment of defense strategies according to changes of network threat environments, realizing adaptive matching between defense mechanisms and attack behaviors, which is the core theoretical support for improving the flexibility of automatic protection systems.

Different from traditional static protection, automatic protection has the typical characteristics of real-time, autonomy and dynamics. Real-time performance is reflected in the uninterrupted monitoring of network operation status and traffic data, which can capture threat behaviors in the first time. Autonomy is reflected in the completion of threat analysis and disposal through system algorithms without manual operation. Dynamics is reflected in the continuous iteration and optimization of defense rules and identification models with the accumulation of network data and threat samples, which can adapt to continuously changing network threat

environments.

2.2 Mainstream Artificial Intelligence Technologies for Network Security

A variety of artificial intelligence technologies have been widely applied in the field of network security automatic protection, among which machine learning, deep learning and intelligent data analysis technologies are the most mainstream technical means. Machine learning technology realizes autonomous learning of network threat features through sample data training. Classical algorithms such as random forest, isolation forest and support vector machine have good application effects in network abnormal traffic detection. These algorithms can efficiently screen out abnormal data in massive network traffic, complete preliminary identification of low-dimensional threat features, and have the advantages of low operation complexity and fast detection speed, which are suitable for real-time monitoring of large-scale network traffic.

Deep learning technology represented by convolutional neural network and recurrent neural network has outstanding advantages in high-dimensional feature extraction and complex threat identification. Network attack behaviors under complex network environments often have hidden and variable feature attributes, and traditional algorithms are difficult to capture deep implicit features. Deep learning models can conduct layered mining of network data information, extract fine-grained threat features, and realize accurate identification of variant attacks and unknown zero-day threats. In addition, with the development of large model technology, semantic analysis and intelligent reasoning capabilities of artificial intelligence have been further improved, which can realize contextual analysis of network attack behaviors and improve the comprehensiveness of threat judgment.

Intelligent data mining and prediction technology is also an important part of AI-enabled network security protection. This technology can summarize the evolution rules of network threats based on historical network security event data and traffic data, predict potential security risks in advance, and realize active early warning of network threats. The combination of the above artificial intelligence technologies constructs a multi-dimensional technical support system for network security automatic protection, and lays a solid technical foundation for realizing full-automatic and intelligent network security defense.

3. Defect Analysis of Existing Network Security Protection Technologies

3.1 Limitations of Traditional Network Security Protection Technologies

Traditional network security protection technologies mainly include firewall, intrusion detection system, virus killing system and manual security audit, which form a relatively mature static defense system and play a certain role in preventing conventional network attacks. However, with the continuous complexity of network environment and intelligence of attack means, the inherent limitations of traditional technologies are increasingly prominent. The core defect of traditional protection technologies lies in passive defense mode. Most defense mechanisms rely on preset fixed rule bases and feature databases. The system can only identify and intercept known attack behaviors that match the rules, and cannot effectively identify unknown attacks and variant attack behaviors, resulting in obvious blind spots in defense.

Traditional protection technologies have low automation and excessive dependence on manual participation. Network security operation and maintenance personnel need to regularly update threat feature libraries, adjust defense rules, and manually verify and dispose of early warning information generated by the system. Massive network monitoring data and frequent security early warnings bring huge work pressure to operation and maintenance personnel, and manual processing efficiency is difficult to match the generation speed of network threats. Delayed disposal of security incidents often leads to the expansion of threat impact scope, bringing hidden dangers to network data security and system operation stability.

In addition, traditional network security protection systems lack dynamic optimization capabilities. The defense rules and identification standards of the system remain fixed for a long time, and cannot be dynamically adjusted according to network operation changes and threat evolution trends. In the face of increasingly complex and diversified network attack modes such as collaborative attacks and disguised attacks, traditional static defense systems are difficult to form effective defense

barriers, and the overall defense robustness is insufficient.

3.2 Practical Shortcomings of Current AI Network Security Protection Applications

Although artificial intelligence technology has been widely applied in the field of network security and has achieved certain application effects, restricted by technical maturity, data quality and application scenarios, the current AI-based network security protection system still has many practical shortcomings in actual operation. First of all, the threat identification model has insufficient generalization ability. Most existing intelligent detection models are trained based on single-scene network data samples, and the model adaptability in complex and heterogeneous network environments is poor. The detection accuracy will drop significantly when facing cross-scene network attacks and emerging threat behaviors, and the problems of false detection and missed detection still occur frequently.

Secondly, the degree of automation of security response is insufficient. Most current intelligent security systems only complete the automatic identification and early warning of threats, and the subsequent threat isolation, vulnerability repair, traffic interception and other disposal work still need manual intervention. The whole-process closed-loop automatic defense mechanism has not been fully formed. The disconnection between intelligent detection and automatic response greatly limits the overall operation efficiency of the intelligent protection system, and cannot give full play to the technical advantages of artificial intelligence in autonomous decision-making.

Moreover, the existing intelligent protection technology lacks targeted optimization for industry-specific network scenarios. Network security requirements and threat characteristics of power monitoring systems, electronic communication networks and industrial control networks are significantly different from ordinary civilian networks. However, most current AI protection models adopt universal technical frameworks, and do not build targeted identification rules and defense mechanisms for industry-specific threat characteristics, resulting in poor matching between protection effects and actual scenario demands. Meanwhile, the interpretability of some deep learning models is insufficient, and the threat identification basis and decision-making logic cannot be clearly explained, which brings certain obstacles to the optimization and iteration of protection systems.

4. Construction of AI-Based Network Security Automatic Protection Technical System

4.1 Design of Intelligent Network Threat Perception and Identification Module

Intelligent threat perception and identification is the core basic module of network security automatic protection system, which undertakes the functions of real-time monitoring of network operation status, collection of traffic data and accurate identification of threat behaviors. This module takes multi-source network operation data as the research object, including network transmission traffic data, system operation log data, user access behavior data and equipment operation state data, and realizes full-coverage collection and real-time analysis of network state information through data preprocessing, feature extraction and intelligent model recognition.

In terms of data preprocessing, the module cleans and standardizes the collected original network data, removes invalid data, duplicate data and noise data that interfere with threat identification, unifies data dimension and format, and improves the quality of input data of the intelligent model. In the process of feature extraction, combined with the characteristics of modern network threats, it extracts multi-dimensional feature information such as traffic duration, data packet size, access frequency, operation behavior and data transmission path, and constructs a fine-grained network threat feature set, which covers both conventional attack features and implicit variant attack features.

In terms of model recognition, this study adopts a hybrid intelligent algorithm framework combining machine learning and deep learning. The isolation forest algorithm is used for real-time screening of abnormal traffic in network operation, which quickly eliminates normal network business data and locks potential threat data. On this basis, the convolutional neural network model is used for deep feature mining of suspected threat data, which accurately identifies specific attack types and threat levels, and realizes hierarchical classification of network security threats. The hybrid model can not only ensure the real-time performance of

network monitoring, but also improve the accuracy of complex threat identification, effectively solving the problems of low efficiency and low accuracy of single algorithm identification.

4.2 Construction of Automatic Response and Active Protection Mechanism

On the basis of realizing accurate intelligent perception of network threats, building a perfect automatic response and active protection mechanism is the key to realize full-automatic network security protection. This study constructs a hierarchical automatic threat disposal mechanism according to the threat level identified by the intelligent module, forming a closed-loop defense process of threat identification, automatic disposal, state feedback and strategy optimization. For low-level network threats such as ordinary malicious scanning and invalid access attempts, the system automatically completes real-time interception of access requests and records threat feature information, and updates the system defense feature library synchronously to prevent repeated attacks.

For medium-level threats such as minor network intrusion and abnormal data access, the system starts the isolation protection mechanism in real time, limits the access authority of abnormal terminals and intercepts abnormal data transmission behaviors, and feeds back the threat disposal state to the system background. For high-level critical threats such as large-scale network intrusion, virus propagation and core data leakage risks, the system immediately starts the emergency protection strategy, cuts off abnormal network links, closes vulnerable service ports, and triggers the system security early warning mechanism to remind operation and maintenance personnel to pay attention to abnormal changes in the network environment.

In order to improve the dynamic adaptability of the protection mechanism, the system builds a self-optimization iteration mechanism. The system continuously accumulates threat disposal data and network operation data in the actual operation process, optimizes the feature extraction rules and algorithm model parameters in real time, and dynamically adjusts the threat judgment standard and automatic disposal strategy. The self-optimization mechanism enables the protection system to continuously adapt to the evolving network threat environment, realize active defense against emerging threats, and fundamentally improve the autonomous protection capability of the network security system.

5. Conclusion

This study systematically explores the application value and technical path of artificial intelligence technology in network security automatic protection, sorts out the theoretical basis and mainstream technical system of intelligent network security protection, and deeply analyzes the inherent limitations of traditional network security protection technologies and the practical application defects of current AI-based security protection technologies. A complete set of network security automatic protection technical system including intelligent threat perception identification module and hierarchical automatic response protection mechanism is constructed, which effectively makes up for the deficiencies of traditional passive defense modes and single intelligent defense technology.

The research results verify that the integration of artificial intelligence and network security protection can significantly improve the automation level, real-time response capability and threat identification accuracy of network security defense. The constructed technical system can adapt to the complex and changeable modern network threat environment, realize active early warning and automatic disposal of network security risks, and provide effective technical support for solving the problems of low efficiency and poor adaptability of traditional network security protection. In the follow-up research, the model generalization ability and scenario adaptation performance will be further optimized, and targeted technical improvement will be carried out for industry-specific network security scenarios, so as to further expand the application scope and practical value of intelligent automatic protection technology.

References

[1] Yu H, Dong P, Liu J, et al. Research on network security defense technology based on artificial intelligence technology[J]. Electrical Automation, 2025(2).

[2] Yue Z Y. Research on network security protection technology based on artificial intelligence[J]. Consumer Electronics, 2025(18):17-19.

[3] Tian F X. Research on network security protection technology of power monitoring system based on artificial intelligence technology[J]. Water Conservancy & Electric Power Technology & Application, 2025, 7(24).

[4] Song K. Research on network security protection problems based on artificial intelligence technology[J]. Science and Informatization, 2018(34):1.

[5] Li L L. Research on network security monitoring and defense technology based on artificial intelligence[J]. Mobile Information, 2024, 46(4):158-160.

[6] Zhao X, Zhang G W. Research on network security protection based on artificial intelligence technology[J]. Industrial A, 2022(10):3.

[7] Guo J Q, Zhu J, Zheng R P, et al. Research on electronic communication network security protection technology based on artificial intelligence[J]. Consumer Electronics, 2026(6):68-70.

[8] Luo Z Q. Research on network communication security risk protection based on artificial intelligence[J]. China Broadband, 2023, 19(6):13-15.

[9] Gao J. Research on network security protection strategy based on artificial intelligence[J]. Information and Computer, 2024, 36(23):98-100.

[10] Yang Y H. Research on computer network security defense system based on artificial intelligence technology[J]. Cyberspace Security, 2024, 15(4):306-309. DOI:10.3969/j.issn.1674-9456.2024.04.060.

[11] Sun T. Research on network security protection based on artificial intelligence technology[J]. Information and Computer, 2022, 34(14):157-159.

[12] Li Q, Li W G, Li J J. Research on intelligent defense system construction and active protection technology of network security based on artificial intelligence[J]. Network Security and Informatization, 2025(9).

[13] Zhang Y Y. Design of computer network security protection system based on artificial intelligence technology[J]. Information and Computer, 2023, 35(4):233-235.

[14] Zou C. Research on network security protection based on artificial intelligence technology[J]. Office Automation, 2022, 27(24):10-12.

