WHIOCE PUBLISHING PTE. LTD.
PROVIDING
FIRST-CLASS SCIENTIFIC INFORMATION
FOR TOP SCHOLARS

2025 Volume 3, Issue 4
Contemporary Education Frontiers
ISSN (Online): 3029-1860   ISSN (Print): 3029-1879

Analysis on the Application of Artificial Intelligence Technology in Communication Network Security Management

Xiaodong Qian, Hongchen Liu
Xinhua Three Group Company, Hangzhou 310000, Zhejiang, China

Abstract: The rapid advancement of information technology has driven continuous expansion of communication network coverage. With the increasing complexity of network architectures and the explosive growth of data traffic, security management now faces severe challenges. Traditional static protection mechanisms relying on rule-based approaches struggle to address the stealthy nature and real-time characteristics of emerging threats. Leveraging its powerful capabilities in data mining, analysis, intelligent recognition patterns, and autonomous learning, artificial intelligence provides a core foundation for intelligent upgrades in communication network security management. This paper focuses on key features of AI technology, systematically outlining its specific application scenarios and practical implementation methods in communication network security management, aiming to enhance the precision and proactive nature of security defenses.

Keywords: artificial intelligence technology; communication; network security; management

Online publication: May 26, 2025

1. Introduction

Communication networks have become critical infrastructure driving societal operations and economic development, handling the transmission and exchange of massive amounts of sensitive information. With deepening network penetration, security threats are becoming increasingly diverse, frequent, and complex. Incidents such as malicious exploitation of system vulnerabilities, data theft, and unauthorized intrusions frequently emerge, directly threatening user privacy, corporate operations, and national security. Traditional security management systems show significant limitations in response speed, identification of unknown threats, and adaptive protection capabilities. There is an urgent need to introduce innovative technologies to enhance defensive effectiveness. In this context, artificial intelligence technology, which mimics human cognitive logic and learning mechanisms, offers a new opportunity for building dynamic and intelligent security management systems. Exploring the integration of its technical principles with management practices holds significant practical value for enhancing network resilience and reducing security risks.

2. Overview of artificial intelligence technology

2.1. Concepts

In the 1950s, the concept of artificial intelligence began to emerge. Its research scope was extensive and deeply integrated with disciplines such as physiology and psychology. Leveraging its unique advantages, AI applications have covered numerous fields. Its advancement is reflected in improving computer operation efficiency, streamlining manual processes, enhancing work effectiveness, and elevating quality standards. Fundamentally, AI is rooted in computer science, utilizing advanced technologies and high efficiency to drive comprehensive transformations in daily life. As its applications grow increasingly widespread, cybersecurity management has become a critical focus[1].

Artificial intelligence (AI) technologies have been commercialized in fields such as smart manufacturing, intelligent healthcare, and smart home systems. In accordance with the top-level design of the "New Generation Artificial Intelligence Development Plan", research on AI standard frameworks is required to establish an initial AI technology standards system by the end of 2020. This system will cover foundational common specifications, cross-platform interoperability, vertical application domains, cybersecurity and privacy protection, as well as specialized industry standards for autonomous driving and service robots. By establishing an internationalized standard framework, products and services can gain global market access and secure a proactive position in international standard-setting. When drafting the "13th Five-Year Plan" standard system construction plan for the communications sector, the Ministry of Industry and Information Technology (MIIT) plans to develop a comprehensive AI standards system covering terminal interaction, intelligent capabilities, security defense, network communication, and platform support[2].

2.2. Characteristics of artificial intelligence

With the continuous advancement of computing technology, traditional centralized management architectures and unified operational models for computer network maintenance have become inadequate to meet modernization demands. While maintaining high efficiency and stability in network operations, standardized security protocols can effectively mitigate system risks, making cybersecurity management indispensable. Intelligent systems enable systematic data processing to ensure secure and efficient network operations. By leveraging artificial intelligence, hierarchical network management can be achieved through a three-tier architecture (decision-making layer → processing layer → execution layer). This approach prioritizes development around the processing and decision-making layers while monitoring execution dynamics, thereby maximizing potential advantages across tiers and achieving deep integration. The technology's dual characteristics of autonomous learning and self-explanation enable data-driven monitoring and control, addressing challenges beyond conventional IT solutions. AI-powered cybersecurity management enhances threat detection capabilities and automated decision-making, effectively reducing potential risks while improving system autonomy. This significantly drives intelligent and technological system development, with cybersecurity threat identification and response becoming core competencies. This field should be a key breakthrough direction for AI research and development[3].

2.3. The significance of artificial intelligence technology

The rapid evolution of internet technologies has enabled individual users to swiftly adapt to diverse online activities. Modern service systems—including e-commerce platforms, government portals, social networks, and open data initiatives—have significantly enhanced daily convenience. Artificial intelligence (AI) is driving global technological innovation, with modern life increasingly relying on computer-assisted operations. This highlights AI's irreplaceable role in the AI field discussed in this thesis[4].

Electronic information systems store vast amounts of sensitive data linked to personal privacy. Malicious attackers may breach these systems to steal private information, causing financial losses and psychological distress for users while achieving their illegal objectives. This creates persistent security vulnerabilities that degrade the quality of life for victims. AI cybersecurity management has become a top priority to protect individual rights and leverage AI's unique capabilities for public service. To effectively manage cybersecurity, it is essential to identify threat sources. Historical data shows that human factors remain the core issue, with cybersecurity risks primarily stemming from human errors and deliberate attacks. Users' digital literacy and operational behaviors are closely tied to cybersecurity risks. If individuals neglect security precautions and visit risky websites without protection, the risk of malware attacks on terminals significantly increases. Successful virus attacks can stealthily steal user data, corrupt files, and create security vulnerabilities. Cybersecurity management involves addressing identified issues through targeted actions to purify cyberspace and ensure positive content orientation[5].

3. Common security threats in communication networks

Cybersecurity threats in computer networks manifest in diverse forms, categorized by attack methods and objectives. The first category involves malicious software intrusions, including encryption-based ransomware that encrypts user data and demands payment for decryption keys. Malicious components embedded in regular applications may covertly collect sensitive information or enable remote system control. The fourth category includes data breaches and eavesdropping, involving exposed transmission links and unauthorized access to information. The second type combines phishing with social engineering, where attackers create realistic website replicas to trick users into submitting payment credentials or personal data for financial fraud. Social engineering tactics involve deceiving victims through deception, impersonation, or coercion to disclose confidential information or execute malicious actions. The third category is service denial attacks, which flood system resources with saturated requests until services collapse. Distributed denial-of-service (DDoS) attacks amplify destructive power by generating malicious traffic through multiple compromised devices. Data corruption and similar incidents may allow attackers to obtain confidential information from individuals and organizations. Unauthorized access and internal security threats encompass these aspects, including unauthorized monitoring of data streams for privacy theft. Unauthorized access specifically refers to unauthorized operations on networks or computers without approval, involving identity impersonation, compromising authentication systems, conducting illegal activities through unauthorized access, and improper operations by authorized users. These threats primarily originate from current and former employees, business partners, and other groups. Improper use of access permissions can compromise secure network transmissions, while other attack methods such as replay attacks, data tampering, and electronic fraud also exist[6].

4. Application of artificial intelligence technology in communication network security management

4.1. Improve security protection capability by using anomaly detection algorithm

In cybersecurity defense, anomaly detection algorithms serve as critical technologies. Their core mechanism involves identifying anomalies within large datasets to screen for potential threats. During the risk management phase, multi-layer feedforward neural networks are constructed using deep representation learning-based anomaly traffic analysis methods to perform feature extraction and classification[7]. The process begins with preliminary operations on raw traffic data, extracting 42 key characteristics. Labeling traffic data enhances the model's binary classification performance through multiple rounds of parameter tuning. After 100 standard training cycles, test evaluations demonstrate the model's outstanding capabilities: it accurately detects 98.7% of abnormal traffic samples with a true anomaly detection rate of 99.1%, meeting practical application standards. To optimize anomaly detection efficiency, attention mechanisms are employed to enhance model performance through automatic weight optimization, highlighting core features while reducing noise interference. An integrated learning strategy combines multiple algorithms to build an anomaly detection ensemble model, improving detection accuracy. By employing Bagging and Boosting hybrid integration techniques, 10 foundational detection models operate independently while leveraging their strengths through a weighted voting system[8].

4.2. Build a protection system based on adaptive learning mechanism

In the face of escalating cyber threats, traditional security frameworks struggle with rigid rule systems and static threshold standards. To overcome these limitations, this work develops an autonomous learning adaptive architecture that continuously learns through online updates and model version upgrades, enabling real-time adjustments to security measures[9]. The framework integrates online learning algorithms with policy optimization models, employing gradient descent-based progressive learning to optimize parameters through continuous data streams. Unlike traditional centralized learning methods, this technology proactively adapts to dynamic network environments, rapidly adjusting defense strategies to address emerging risks[10]. Utilizing reinforcement learning (RL)-based deep Q-network architecture, the framework transforms protective measures into state-action pairs, empowering autonomous exploration and optimization of defense strategies for long-term benefit maximization. When developing adaptive learning models, reward mechanism configuration and feature selection are critical. During training, a DQN model with dual networks and experience replay mechanisms significantly reduces convergence time. By employing multi-dimensional and multi-layered feature integration techniques, this approach combines dynamic traffic characteristics, protocol operation behaviors, and host activity patterns to construct a 256-dimensional feature vector for systematic cybersecurity assessment. The reward function design balances security requirements with system efficiency, determining optimal protection output-to-resource allocation ratios through weighted aggregation. This validates the feasibility of the strategy. Utilizing an auto-optimizing learning framework, the defense model dynamically adjusts security parameter thresholds and defense strategies in real-time, enabling on-demand configuration of protection mechanisms[11].

4.3. Protection methods of applying active defense strategy

In the risk prevention and control of network communications, artificial intelligence approaches are employed to implement proactive defense strategies. These primarily involve preemptive identification and interception of cyber attack intentions, controlling threats at their source to effectively suppress negative impacts. The paper proposes an active defense system with a GNN-driven threat prediction module as its core technology. By constructing a multi-dimensional information network, this model accurately reflects complex communication scenarios, enabling GNN to analyze intricate interconnections and evolutionary trends between network nodes. It issues early warnings for emerging threats through node embedding and graph attention mechanisms—both methods converting network entities into low-dimensional vector spaces while intelligently adjusting coupling weights between modules, thereby significantly enhancing the model’s transferability. The game-theoretic-based active protection decision-making framework represents a core technological innovation. Upon detecting suspicious activities, the system constructs dynamic game analyses between attackers and defenders, rapidly evaluating pros and cons of various defense strategies to ultimately select the optimal defense strategy set[12]. Compared with traditional rigid protection methods, the game theory model allows defense strategies to adapt dynamically to evolving attacks, enhancing proactive protection reliability and flexible response capabilities. The paper employs a meta-learning-driven strategy transfer architecture that integrates diverse network environment defense strategies into a shared meta-strategy space, enabling rapid adaptation of meta-learning algorithms under new environments and threats, thereby reducing retraining costs[13].

5. Conclusion

Through capabilities such as pattern recognition, behavioral analysis, and predictive alerts, artificial intelligence technology has significantly enhanced the speed of detecting cybersecurity threats and improved response accuracy in communications networks, laying a technological foundation for intelligent security management transformation. Its applications in intrusion detection, abnormal traffic monitoring, risk assessment, and decision-making effectively address the latency and rigid rule-based limitations of traditional methods[14]. In the future, with continuous optimization of deep learning frameworks and coordinated development of edge computing, AI will play a more central role in building adaptive security defense loops and optimizing security resource allocation. Concurrent attention must be paid to emerging challenges like algorithmic transparency and adversarial sample defense to promote the construction of a more efficient and trustworthy intelligent security ecosystem, providing robust safeguards for digital societies[15].

Disclosure statement

The author declares no conflict of interest.

References

[1] Qin Weirong, Peng Jianming, Huang Hao. Application and Development of Artificial Intelligence in Cybersecurity [J]. China Digital Medicine, 2025,20(07):1-9.

[2] Lou Xidong. Application research on artificial intelligence technology in communication network security management [J]. China Broadband, 2025,21(08):37-39.

[3] Wang Hu. Application research of artificial intelligence technology in computer network security [J]. Network Security Technology and Application, 2025, (06):27-29.

[4] Fan Zeyu. Security risk assessment and defense measures of computer network communication under the perspective of artificial intelligence [J]. Software, 2025,46 (05):157-159.

[5] Yang Jia. Research on Network Communication Information Data Security Encryption Technology Based on Artificial Intelligence [J]. Information Record Materials, 2025,26 (03):120-122.

[6] Zhu Jie. Research on Network Communication Information Data Security Encryption Technology Based on Artificial Intelligence [J]. Information Record Materials, 2025,26 (02):144-146.

[7] Fu Yang, Wan Jiahua, Lu Hongying, Liu Hu, Wan Yong. Research on the Application of Artificial Intelligence Technology in Cybersecurity [J]. China Broadband, 2024,20(11):49-51.

[8] Yao Shicong. Application of Artificial Intelligence in Mobile Communication Network Security Protection [J]. China New Communications, 2024,26(20):13-15+19.

[9] Jian Liqiong. Computer network security defense based on big data and artificial intelligence technology [J]. Software, 2024,45(09):7-9.

[10] Lu Bai Chuan. Design and Implementation of Computer Network Security Defense System Based on Artificial Intelligence Technology [J]. Information and Computer (Theoretical Edition), 2024,36(16):115-117+121.

[11] Zhang Qian. Security risk assessment and protection of computer network communication based on artificial intelligence [J]. Software, 2024,45(01):152-154.

[12] Zhang Li. AI-based network communication security risk assessment and protection [J]. China Broadband, 2023,19(09):142-144.

[13] Luo Zhiqiang. Research on Network Communication Security Risk Protection Based on Artificial Intelligence [J]. China Broadband, 2023,19 (06):13-15.

[14] Wang Bin, Li Hongfei, Xu Shaowei. Application and Research of Artificial Intelligence Technology in Communication Security Defense System [J]. Electronic Test, 2022, (01):125-127.

[15] Yan Bo. Development of artificial intelligence technology and its application in the field of communication security [J]. Post and Telecommunications Design Technology, 2019, (04):86-89.