The Application of Artificial Intelligence in Computer Network Technology

Zhang Ge

Shenzhen Huayi Digital Intelligence Information Technology Co., Ltd.Guangzhou, Guangdong, China

Abstract: With the rapid advancement of information technology, computer networks have permeated all aspects of human production and daily life, exhibiting increasingly large-scale and complex structures that demand new approaches to efficient network security management. Artificial intelligence (AI) technology provides scientific and rational support for the adaptive, automated, and intelligent evolution of computer networks. This paper systematically explores the specific applications of AI in critical areas such as network security protection, network management and optimization, intelligent resource scheduling, and future network architecture design, aiming to offer theoretical references for the sustainable development of computer network technology.

Keywords: Artificial Intelligence; Computer Network; Network Security

The continuous advancement of digital technologies has expanded the development potential of computer networks while presenting new challenges to network architectures. Artificial intelligence (AI), particularly data-driven machine learning methods, can automatically extract patterns and predictive insights from complex, high-dimensional data to assist users in decision-making. By integrating AI into computer networks, we enhance their deep thinking and learning capabilities, enabling them to perceive environmental changes, understand user and business intentions, predict potential risks, and make optimized decisions. This approach ultimately builds a more efficient, reliable, and secure intelligent network ecosystem.

1. Deep Application of Artificial Intelligence in the Field of Cybersecurity

1.1 Intelligent Intrusion Detection and Threat Hunting

Traditional intrusion detection systems heavily rely on known attack signatures, resulting in limited detection capabilities for emerging variant attacks. Big data-enhanced AI-powered network solutions, through unsupervised learning that analyzes network traffic, system logs, and user behavior patterns, effectively identify baseline-deviating anomalies. This enables timely detection of cyber threats and internal risks, allowing proactive prevention. For instance, deep learning models process time-series network data to uncover complex attack chain patterns. Furthermore, AI can correlate fragmented clues within massive datasets to reveal sophisticated attack techniques employed by advanced cybercriminals. The technique and procedure can effectively do the defense and reduce the user network intrusion rate.

1.2 Adaptive Security Policy and Dynamic Access Control

Traditional static access control lists and firewall rules struggle to meet fine-grained and context-dependent security requirements. In contrast, AI-powered policy engines dynamically adjust access permissions and security policies by analyzing user identities, device statuses, geographic locations, behavioral patterns, and real-time threat landscapes. For instance, when detecting abnormal login attempts or access from high-risk regions, the system automatically activates multi-factor authentication or restricts access to sensitive resources. This adaptive zero-trust security architecture enhances user network security through intelligent threat response.

1.3 Intelligent Malware Analysis and Phishing Detection

Artificial intelligence models can perform static analysis of file features like header information and opcode sequences, or dynamic analysis of their sandbox behavior, enabling rapid and accurate classification and identification of new malware. In phishing attack prevention, natural language processing technology deciphers email and webpage content, while computer vision technology evaluates the similarity between website interfaces and real sites to comprehensively determine fraudulent activities, significantly enhancing network interception rates.

1.4 Safety Prediction and Response Automation

Artificial intelligence (AI) employs time-series prediction models to analyze historical attack data and security incidents, forecasting potential attack types and intensity to enable proactive alerts. By integrating AI decision-making modules, security orchestration, automation, and response platforms can automatically assess medium-to-low risk alerts and respond to confirmed attacks. This significantly reduces average detection and response times, thereby alleviating the workload of security personnel.

2. Application of Artificial Intelligence in Network Management and Performance Optimization

2.1 Network Fault Management

Traditional fault management approaches only initiate troubleshooting after issues emerge, resulting in prolonged resolution times and significant business disruptions. AI-powered predictive maintenance, however, enables effective transformation of management paradigms by identifying early warning signs before failures occur. AI technology can perform deep mining on massive multi-source time-series data, where performance metrics from network devices, log timestamps, and environmental sensor data collectively form a continuous health status stream. Machine learning models—particularly time-series architectures like Long Short-Term Memory (LSTM) networks—can learn intricate correlations and dynamic equilibrium patterns among these metrics under normal conditions. When one or multiple indicators exhibit subtle anomalies... By detecting anomalies, the machine learning model can alert potential risks.

After a fault occurs, AI-powered intelligent analysis technologies significantly reduce diagnosis time. Traditional methods require engineers to conduct layer-by-layer troubleshooting, whereas AI systems based on knowledge graphs and graph neural networks integrate structured and semi-structured knowledge such as network topology, configuration dependencies, application service chains, and historical fault databases. When multiple alerts trigger simultaneously, AI can rapidly analyze the propagation paths and chronological order of alert events on the topology graph. By applying causal inference algorithms, it identifies the most likely source fault point, provides confidence level assessments, and offers repair recommendations, thereby substantially reducing average repair time.

2.2 Intelligent Control of Network Traffic and Performance

Artificial intelligence can perform precise traffic prediction by utilizing spatiotemporal graph neural network models. It can not only analyze the time series characteristics of individual link traffic but also simultaneously model the spatial correlations between different nodes and links in the network topology. The accurate traffic prediction capability provides critical support for proactive network capacity planning and resource pre-allocation.

In real-time performance optimization, networks can continuously experiment with different actions and observe environmental feedback to learn optimal strategies for maximizing long-term performance returns under changing conditions. For instance, when data center networks experience sudden congestion, a DRL-based traffic scheduler can rapidly calculate the optimal traffic diversion plan to bypass congestion points within milliseconds. In wireless networks, AI can dynamically learn user distribution and channel interference conditions in real time, adjusting base station power, frequency bands, and beam direction to ensure edge user coverage while maximizing overall spectrum efficiency.

2.3 Automation and Intelligence of Network Configuration

AI constructs intent-driven networks through natural language processing and machine learning. Network operators can complete basic operations by declaring high-level business objectives. The AI intent translation engine automatically interprets these requirements and decomposes them into executable low-level configuration commands—such as SDN controller flow rules and firewall policies—compatible across vendors and technical domains. This approach not only significantly reduces configuration complexity and error rates but also ensures network states consistently align with business intent.

In configuration verification and compliance checks, AI learns from massive correct configuration samples to build a network configuration model. When new configuration changes are submitted, AI can perform simulation analysis or model-based inference to predict in advance whether these changes may cause policy conflicts, security vulnerabilities, or performance degradation.

2.4 User-Centric Performance Optimization

Traditional network optimization primarily focuses on key performance indicators (KPIs) at the network level, such as broadband performance. In the context of digital technology advancement, artificial intelligence (AI) achieves precise optimization of user needs by establishing deep, nonlinear mapping models between user experience quality and service quality. For instance, in video streaming services, AI models can comprehensively analyze real-world experience quality metrics reported by clients, including frame rate, initial buffering time, and bitrate switching frequency, alongside service quality data monitored from the network side, such as throughput, latency, and fluctuations. Through deep learning techniques, AI can accurately quantify wireless signal quality, intermediate network congestion, and server load. The specific impact of factors on user viewing experience, and adjust the direction of user demand push in a timely manner based on these data.

3. The Role of Artificial Intelligence in Intelligent Scheduling of Network Resources

3.1 Data Center Resource Scheduling

Traditional schedulers primarily focus on CPU and memory load balancing, often leading to traffic congestion and suboptimal application performance due to excessive reliance on network bandwidth. AI-driven scheduling systems, however, can conduct more precise workload profiling and prediction. By analyzing historical task execution data—including dependencies, required data volumes, and computational intensity—machine learning models can forecast resource demands for newly submitted tasks. The deep reinforcement learning-based scheduling framework treats data centers as dynamic environments, where decisions can trigger cascading effects. Through continuous interaction with this environment, intelligent agents can... Find the long-term optimal balance in learning and reduce the resources spent on data transfer.

3.2 Edge Computing and Computing Offloading

Edge computing decisions are influenced by multiple factors, including the remaining battery power and computing capacity of terminal devices, instantaneous fluctuations in wireless channel quality, and the current load and queue latency of edge servers. Through continuous experimentation with different offloading strategies and monitoring their performance metrics, artificial intelligence gradually learns optimal approaches tailored to varying requirements. For instance, in urban congested areas with stable 5G signals, the preprocessing of perception data for autonomous vehicles may be offloaded to roadside units to conserve onboard computing resources. When the vehicle enters tunnels with weak signals, the system immediately switches to prioritizing local processing of critical control commands to ensure driver safety. safe 。

3.3 Wireless Network Resource Management

Traditional resource allocation methods relying solely on simple interference coordination struggle to meet the comprehensive demands of modern wireless networks. Artificial intelligence (AI) provides technical support for infinite resource management. By analyzing massive channel state information, user distribution, service history, and implementation requirements, AI models can accurately characterize the spatiotemporal variation patterns of wireless environments, thereby enhancing the precision of scheduling decisions. AI algorithms can also estimate channel quality based on users' uplink probe signals, predict user movement trajectories and service arrival patterns, and make dynamic decisions within milliseconds. The joint optimization of these highly coupled decisions helps improve the worst-case performance of users. Verify fairness.

4.Conclusion

In summary, with the rapid advancement of digital technologies, artificial intelligence (AI) is integrating into computer network systems at an unprecedented pace. It plays a pivotal role in addressing the complex challenges faced by traditional networks in security, management, and resource allocation, while providing innovative technical support. The application of AI has significantly enhanced network performance, reliability, and intelligence levels. However, the integration of AI with computer network technology still requires overcoming various challenges. Moving forward, collaborative efforts across industries are essential to develop more efficient and scientifically sound AI algorithms, design novel network architectures and protocols, and establish comprehensive standards. Only through such coordinated efforts can we fully realize the potential of AI in modern networks. To fully harness the potential of artificial intelligence and provide robust technological support for the digital economy and social development.

References

[1] Li Jiaxiao. Application of Artificial Intelligence in Computer Network Technology [J]. Science and Technology Information, 2025,23(23):43-45.

[2] Wu Xiaoqian. Application of Artificial Intelligence in Computer Network Technology in the Era of Big Data [J]. Software, 2025,46(11):58-60.

[3]Zhan Pengfei, Wang Zhipeng, Yang Lei, et al. Application research of artificial intelligence in computer network technology[J]. Software, 2025,46(11):184-186.

[4] Xu Guanjia Shuo. Application Research of Artificial Intelligence in Computer Network Technology under the Perspective of Big Data [J]. Science and Technology Information, 2025,23(22):57-59.

[5] Zhang Fangkun, Wang Yinuo. Application of artificial intelligence in computer network technology under the background of big data [J]. China New Communication, 2025,27(21):46-48.

[6] Huang Yifan. Application of Artificial Intelligence in Computer Network Technology in the Era of Big Data [J]. Industrial Science and Technology Innovation, 2025,7(05):13-16.

[7] Zhou Rongdi. Application of artificial intelligence in computer network technology [J]. China Science and Technology Information, 2025(19):41-43.

[8] Huang Chunhua. Analysis of Artificial Intelligence Applications in Computer Network Technology [J]. Communication World, 2025,32(09):179-181.

[9] Wang Xuejiao. Application of Artificial Intelligence in Computer Network Technology [J]. Electronic Technology, 2025,54(09):280-281.

[10] Wei Fangyu. Application Research of Artificial Intelligence in Computer Network Technology in the Era of Big Data [J]. China Broadband, 2025,21(09):10-12.