2025 Volume 3, Issue 4
Educational Innovation Research
ISSN: 3029-1844(Print)
ISSN: 3029-1852(Online)

Analysis on the Application of Artificial Intelligence Network Algorithm in Network Information Processing

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

Abstract

With the explosive growth of network information, traditional information processing methods such as rule-based filtering systems face challenges like low efficiency and insufficient accuracy, making them inadequate for handling high-speed, heterogeneous real-time data. This paper focuses on core technologies in artificial intelligence network algorithms, including deep learning, convolutional neural networks (CNN), and recurrent neural networks (RNN) applications in network information processing. By examining algorithmic principles and their operational mechanisms across scenarios like data processing and real-time analysis, this study demonstrates the critical advantages of AI algorithms in enhancing network processing efficiency, improving intelligence, and ensuring security. The research provides theoretical support and practical guidance for intelligent upgrades of network information processing systems, contributing to the development of more efficient and reliable information ecosystems.

Keywords

Artificial intelligence
Network algorithm
Network information processing
Application

Online publication: May 26, 2025

1. Introduction

Amid the deep penetration of internet and widespread adoption of IoT technologies, network information has experienced exponential growth in scale and complexity. Traditional data processing methods like label classification and static analysis have shown significant limitations in real-time performance and scalability, struggling to meet the demands of high-speed multi-source data processing. With accelerated AI advancements, deep learning algorithms—particularly convolutional neural networks (CNNs)—have achieved breakthroughs in image recognition and feature extraction. Recurrent neural networks (RNNs) demonstrate advantages in long-term dependency processing for time-series data, with initial applications emerging in network information filtering, security monitoring, and adaptive optimization. This study systematically explores the application value of AI network algorithms in information processing, focusing on core technical approaches and potential of CNNs in data processing and RNNs in time-series analysis. It highlights their transformative role in enhancing information processing accuracy, efficiency, and intelligence levels, providing theoretical guidance and practical pathways for network technology innovation,

thereby facilitating efficient iteration of future intelligent network systems.

2. Artificial intelligence network algorithm

Artificial Intelligence Processing Technology (AI) is an algorithmic framework integrating machine learning, deep learning, and data mining. It mimics human cognition and logical reasoning to process massive, multi-dimensional datasets in network systems. In its early stages, AI relied on expert systems and rule-based reasoning. With the continuous advancement of deep learning technologies, AI network models have gained enhanced adaptive learning capabilities through multi-layer neural architectures. These models can automatically uncover nonlinear patterns in data, enabling efficient feature extraction and complex pattern recognition. Core deep learning technologies like Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have been widely adopted, giving AI algorithms processing advantages in large-scale data and real-time network scenarios while demonstrating stronger perturbation resistance and self-regulation capabilities[1].

3. Network information processing

Network information processing involves collecting, mining, and transforming diverse data in cyberspace to extract knowledge. This process integrates computer science, artificial intelligence, and linguistic analysis methods to handle multi-dimensional data including text, images, audio, and video. Key challenges include data deduplication, reliability verification, and real-time update mechanisms. By combining machine learning with text analysis technologies, the system achieves efficient data categorization and semantic association, enhancing decision-making accuracy and facilitating knowledge extraction. Information processing technologies enable search engines to convert web content into structured search data, while e-commerce platforms generate personalized recommendations through user behavior analysis.

4. Application of artificial intelligence network algorithm in network information processing

4.1. Application of deep learning in network information processing

Deep learning, a technology that relies on multi-layer neural networks, excels at automatically identifying abstract features from massive complex datasets. It particularly demonstrates exceptional capabilities in solving high-dimensional nonlinear challenges where traditional methods falter. In network traffic monitoring applications, deep neural network (DNN) models employ stacked architectures to automatically generate discriminative features from raw network data. When determining whether traffic is normal or abnormal, DNNs extract critical traffic characteristics through hierarchical processing—such as packet length, transmission rate, and source address—then perform classification or predictive analysis based on these high-dimensional features. In practical implementations, DNNs achieve precise traffic classification through parameter adjustments during training phases[2].

In the field of security threat detection, conventional rule-based approaches often require manual pre-determination of signatures and matching rules, which presents significant limitations when addressing evolving attack methods and unknown threats. Deep learning, however, leverages automated training systems to automatically identify potential attack patterns through extensive historical data, demonstrating strong generalization capabilities. Particularly in production environment protection systems, deep learning utilizes deep neural networks for network data modeling, isolating signature indicators of attack behaviors to effectively distinguish normal traffic. By training on DDoS attack datasets, the model can recognize unique data patterns during rapid traffic fluctuations, enabling swift response to sudden attacks and efficient anomaly detection. When confronting security challenges like SQL injection and phishing websites, deep learning models can learn from historical attack signatures to enhance both the precision of security event detection and the speed of incident response[3].

To enhance the accuracy of traffic prediction and intrusion detection, we employ a training-optimized

deep learning model strategy. Through multiple rounds of training, the model gradually converges errors while improving detection capabilities. For network traffic prediction, we analyze massive historical traffic data using deep learning models and implement parameter adjustments to dynamically respond to real-time traffic fluctuations, enabling trend forecasting. To achieve precise inference, this e-commerce system is currently handling a composite security incident involving DDoS paralysis attacks, SQL injection vulnerabilities, and WebShell Trojans. By strengthening cybersecurity defenses, the system utilizes DNN-driven network intrusion detection methods. Through online traffic analysis, it collects key packet characteristics such as packet length, transmission speed, and source addresses to automatically distinguish between normal and abnormal traffic patterns. When facing distributed denial-of-service attacks, the system dynamically identifies sudden traffic surges by analyzing temporal patterns and packet sizes, enabling rapid interception and containment to effectively prevent attacks from escalating[4].

During the identification phase of SQL injection attacks, the system utilizes a deep neural network (DNN) model trained with extensive attack data to optimize its capabilities. By analyzing traffic patterns from SQL injection attempts, it can promptly detect abnormal execution requests and identify attack patterns often overlooked by traditional rule-based systems. This significantly enhances the platform's ability to handle diverse network demands. To improve response efficiency and accuracy in combating cyber threats, the DNN-powered security monitoring system automatically performs intrusion detection tasks, substantially boosting the capability to identify emerging attack variants. These advancements demonstrate the vast potential of deep learning in optimizing cybersecurity protection effectiveness.

4.2. Application of CNN in data processing

As a deep neural network, CNN demonstrates exceptional feature learning capabilities. Its core advantage lies in autonomously extracting data features, particularly excelling in processing high-dimensional data with spatial or temporal correlations. In cybersecurity detection systems, CNNs can automatically capture localized network traffic characteristics without relying on predefined rules, directly processing network data streams through their framework. Most traffic patterns are converted into matrices or tensor architectures compatible with neural networks. Through convolutional layer computations, the system identifies traffic fluctuation patterns, temporal feature vectors, and packet size metrics. This enables effective detection of abnormal activities such as DDoS attacks, port scanning, and SQL injection attempts. The application of sliding convolution kernels is a standard method for CNNs to process time-series data, effectively extracting localized traffic patterns[5].

In the context of malicious traffic detection, the architecture employs a multi-stage convolutional framework. The Convolutional Neural Network (CNN) repeatedly extracts spatiotemporal patterns from network traffic. When confronting DDoS attacks, this model analyzes sudden spikes in data flow characteristics by segmenting time series through convolution operations to capture abrupt fluctuations. By leveraging automatic learning mechanisms, the CNN acquires traffic data features to achieve effective detection. This approach improves traditional detection methods while balancing high accuracy with rapid intrusion analysis feedback [6].

As cyber threats continue to escalate, telecommunications security departments have implemented a CNN-based threat detection system targeting common cyber threats like DDoS attacks, port scanning, and SQL injection. To enhance detection accuracy, the system first converts historical network traffic data into CNN-compatible spatiotemporal matrices containing time-segmented and IP-source-differentiated traffic logs. During model training, CNN employs sliding convolution kernels to capture spatial features of traffic data, dynamically extracting localized spatiotemporal correlations. Particularly in DDoS attack scenarios, the network can promptly identify sudden traffic surges and classify them—effectively detecting abrupt abnormal fluctuations rather than relying on manual rule-based configurations. This system significantly improves intrusion detection timeliness and precision, enabling rapid response to traffic spikes and effectively reducing service downtime[7].

4.3. Application of RNN in time series data analysis

Unlike simple feedforward networks, recurrent neural networks (RNNs) employ recursive connections to analyze and predict continuous time-series data. Their self-reinforcing architecture enables dynamic response and integration of historical input, allowing efficient time series analysis in complex network environments. In traffic prediction, network data typically exhibits clear temporal correlations. By leveraging historical traffic patterns, RNNs can predict traffic trends through direct correlation with current changes and previous state coupling. This enables network administrators to optimize traffic management through iterative training that gradually adjusts weights and biases, enhancing the model's ability to understand long-term dependencies. The model predicts traffic fluctuations using backpropagation algorithms to minimize prediction errors. Through recursive relationships, RNNs model time-series data by leveraging the self-referential nature of output data, effectively capturing temporal correlations in traffic patterns[8].

ht = f(Whh ht-1 + Wxh xt + bh yt = Whyht + by. Here, h represents the current hidden state; Whh denotes the transition weight matrix; xt is the input variable; Wxh and Why are the weights corresponding to the state and input respectively; bh and by serve as bias terms; yt is the predicted output value; and ht-1 is the cached previous state [9].

Global cloud service providers face operational challenges in ultra-large distributed environments. To address high-frequency network terminals and services, they implement proactive defense mechanisms to reduce network failures and service disruptions. The platform employs a RNN-based fault prediction system that analyzes historical traffic patterns and device response time series. By leveraging RNN architecture to examine temporal features of faults, the system detects abnormal fluctuations in device response times or traffic. When anomalies are detected, the RNN combines historical data to identify potential fault types, automatically triggers alerts, and provides maintenance personnel with actionable guidance. This optimization significantly enhances overall service reliability, dramatically reducing downtime caused by faults[10].

By leveraging recurrent neural networks that model long-term temporal correlations in time series, the platform enables real-time monitoring of equipment operational status and rapid processing of early warning signals. This breakthrough fundamentally transforms traditional fault detection systems that rely on slow, reactive approaches. Through extensive training and optimization, the system not only accurately identifies historical failure patterns but also anticipates emerging faults[11].

The platform has achieved significant improvements in automated operations and maintenance. To enhance RNN's performance in capturing continuous time series, enhanced RNN architectures such as Long Short-Term Memory (LSTM) and its gated variant GRU have become widely adopted in the industry. However, the original RNN architecture struggles with severe gradient anomalies (vanishing/exploding) when processing long-span data, making it difficult to learn long-range dependency relationships[12]. By adopting gating mechanisms as their core architecture, LSTM and GRU enable intelligent control of information transmission, thereby improving the reliability and stability of prediction results. In cybersecurity, denial-of-service attacks typically manifest as sudden spikes in data traffic. Leveraging RNN, systems can track historical traffic patterns to detect abnormal fluctuations in real-time and trigger rapid alerts. Additionally, long-term learning from historical attack patterns enhances the system's ability to identify emerging attack methods, driving intrusion detection systems toward intelligent development[13].

5. Epilogue

This paper provides a comprehensive review of the core technical framework of artificial intelligence network algorithms, focusing on analyzing the advantages of Convolutional Neural Networks (CNN) in data processing and the practical effectiveness of Recurrent Neural Networks (RNN) in time-series analysis. It validates the fundamental significance of AI algorithms in enhancing real-time responsiveness, boosting innovative decision-making capabilities, and optimizing resource utilization patterns within network information processing

activities[14]. With the continuous advancement of deep learning technologies and cross-domain integration, AI network algorithms are poised to assume more critical roles in network information processing. Future directions include algorithmic lightweight design, multimodal integration, and addressing privacy and ethical challenges, which will facilitate the development of safer, more efficient, and highly self-managed global network ecosystems, injecting new vitality into digital society transformation[15].

Disclosure statement

The author declares no conflict of interest.

References

[1] Liu Donghui, Xie Jiarui. Application of Artificial Intelligence Network Algorithm in Network Information Processing [J]. Information Record Materials, 2025,26(07):91-93.

[2] He Bin. Research on AI-driven Network Information Processing and Data Analysis Technology [J]. Home Appliance Maintenance, 2025, (06):82-84.

[3] Yang Tingzhang. Security of Generative Artificial Intelligence Algorithms from Cybersecurity Perspective [J]. Information Security and Communication Confidentiality, 2025(03):39-45.

[4] Li Chaoyi. Research on artificial intelligence-based electronic information processing technology [J]. China High-tech, 2025(04):14-16.

[5] Yu Guanjie. Research on Network Communication Topology Optimization and Resource Allocation Algorithm Based on Artificial Intelligence [J]. Home Appliance Maintenance, 2024, (12):62-64.

[6] Jiehao, Application of Artificial Intelligence Information Processing Technology in Network Information Retrieval [J]. Information Record Materials, 2024,25(01):133-135.

[7] Li Xifeng. Embedded autonomous maintenance and security assurance technology for next-generation network information processing and control critical facilities. Sichuan Province, University of Electronic Science and Technology of China, 2022-03-25.

[8] Niu, C. Lei. Research on deep network recommendation technology based on text information processing [J]. Science and Technology Innovation and Application, 2022,12(04):162-164.

[9] Lü Jiayin. The Meaning, Legal Principle and Application of the Necessary Principle in Online Personal Information Processing [J]. Nanjing Social Sciences, 2021, (12):118-125.

[10] Zhu Jinnuo. Discussion on Computer Information Processing and Security Technology in Network Environment [J]. Wireless Internet Technology, 2021,18(22):102-103.

[11] Chen Jianan. Application research of artificial intelligence in computer network technology in the era of big data [J]. Science and Technology Innovation Guide, 2021,18(28):111-113.

[12] Liang Yunmiao. Private Law Protection of Personal Information in the Internet Information Age [D]. Lanzhou University, 2021.

[13] Qiao Qingpeng. Application of artificial intelligence in network information research in the era of big data [J]. Journal of Henan Institute of Education (Natural Science Edition), 2020,29(03):33-35.

[14] Tang Yu. Research on the Application of Artificial Intelligence in Computer Network Technology [J]. Cybersecurity Technology and Application, 2020, (09):107-108.

[15] Xu Wei. Computer information processing and analysis in the era of "Big Data" [J]. Computer Knowledge and Technology, 2020,16(15):65-66.