Innovation of Network Attack Detection and Defense Strategies Based on Deep Learning

Zhenghui Feng[1], Han Ye[2]

Hebei Fangwei Network Technology Co., Ltd. Shijiazhuang, Hebei 050000

Abstract: ***With the rapid development of information technology today, the means of network attacks are becoming increasingly diverse and complex, posing a serious threat to network security. The aim of this study is to explore the innovative aspects of network attack detection and defense strategies through deep learning, in order to provide a new perspective and approach in the field of network security. Firstly, analyze the significance and challenges of research on network attack detection, as well as the application of deep learning in this field. Next, the article elaborates on a network attack detection model that is based on convolutional neural networks, bidirectional long short-term memory networks, attention mechanisms, and integrates multiple deep learning techniques. And based on this, further discuss innovative network attack defense strategies such as deep reinforcement learning, autoencoders, and Petri net modeling. These research results provide a new technological approach and new ideas for improving the accuracy and efficiency of network attack detection, and building intelligent network security protection systems.***

Keywords: Deep learning; Network attack detection; Network defense strategy; Convolutional neural network; Intelligent security protection.

1. INTRODUCTION

The rapid development of information technology has greatly promoted social progress, but the accompanying network security issues have become increasingly prominent. The increasingly sophisticated and sophisticated methods of cyber attacks pose serious challenges to the existing network security protection system. In this case, deep learning technology provides a new solution for network attack detection and defense with its powerful data processing and pattern recognition capabilities. This paper focuses on researching innovative network attack detection and defense strategies based on deep learning, with the aim of exploring a more effective and accurate new approach to network security protection. Zhang (2025) developed a knowledge graph-enhanced multimodal AI framework designed for intelligent tax data integration and compliance enhancement, demonstrating the application of structured semantics in complex regulatory environments [1]. Security for specialized network applications is addressed by Bi and Su (2025), who proposed a secure access method for English education networks based on edge computing, highlighting the role of distributed architecture in safeguarding sensitive data [2]. Enhancing perceptual capabilities in physical spaces, Xie et al. (2025) introduced MARNet, a multi-scale adaptive relational network for robust point cloud completion through cross-modal fusion, improving 3D environmental understanding [3].

This focus on monitoring and securing physical and digital infrastructure has a strong foundation. Early work by Hou et al. (2017) established a camera-based triggering system for bridge structural health monitoring using a cyber-physical system framework, showcasing the integration of sensing and analysis [4]. In the digital commercial sphere, Tian et al. (2025) applied cross-attention multi-task learning to create an innovative business intelligence approach for improving ad recall in digital advertising [5]. For autonomous systems, a fundamental control mechanism was explored by Zhang, Tian, and Hua (2025), who designed an autonomous vehicle speed control system based on a PID controller [6]. To protect the data ecosystems underpinning these technologies, Zhang, Bai, and Luo (2025) developed an AI-driven monitoring and response system specifically for cloud computing data security [7].

As collaborative AI becomes more prevalent, ensuring privacy within federated learning frameworks has become critical. Deng and Yang (2025) proposed multi-layer defense strategies and privacy-preserving enhancements to counter membership reasoning attacks [8]. Building upon this, Sultan et al. (2026) presented FedGuard, a robust federated AI framework inspired by DARPA GARD principles for privacy-conscious collaborative anti-money laundering [9]. Finally, the analysis of complex human motion integrates many of these themes, as seen in the work of Zhu, Yu, and Li (2025), who employed a spatiotemporal attention-weighted graph convolutional network (SAGCN) with IoT integration for detailed adolescent tennis motion analysis [10].

2. OVERVIEW OF NETWORK ATTACK DETECTION TECHNOLOGY BASED ON DEEP LEARNING

2.1 The Importance and Challenges of Network Attack Detection

Network attack detection determines possible attack behaviors and takes defensive measures based on data analysis of network traffic and system logs. This process is of great significance for maintaining network system security [1]. With the rapid development of network technology, network attack methods continue to evolve and present diverse and covert features. Traditional feature matching based detection methods are often powerless in the face of new attacks and difficult to effectively identify. In addition, network attacks often involve cross platform and cross protocol issues, which increases the complexity of detection. So how to improve the accuracy, real-time performance, and adaptability of testing is currently a major challenge facing network attack testing.

Network attack detection not only has important significance in detecting and defending attacks in a timely manner, reducing potential losses, but also has the ability to perceive and warn of network security situations. Continuous monitoring and analysis of network traffic can timely detect abnormal situations in the network, providing decision support for network security management. At the same time, network attack detection plays a crucial role in the network security defense system. It cooperates with firewalls, intrusion prevention systems, and other security measures to form a multi-level defense system.

The detection of network attacks also faces many challenges. One is that the methods of cyber attacks are constantly evolving, increasing the difficulty of detection. Attackers use various techniques such as encrypted communication and botnets to avoid detection. Secondly, the complex network environment also poses challenges to detection. The diversity, dynamism, and massive nature of network traffic have led to a significant increase in the amount of data that detection systems need to process and analyze. In addition, issues such as false positives and false negatives are urgent problems that need to be solved in network attack detection. False positives bring unnecessary resource waste and trouble to users, while false negatives may prevent attack behavior and result in serious consequences.

2.2 Application of Deep Learning in Network Attack Detection

The application of deep learning technology in the field of network attack detection is mainly manifested in its strong data processing and feature extraction capabilities [2].

Firstly, deep learning can efficiently process high-dimensional data. Network traffic data generally has high-dimensional features, and conventional machine learning methods often encounter dimensional disasters when processing such data. Deep learning models, such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), have the ability to automatically extract high-level features from data through multi-level nonlinear transformations, thereby achieving efficient pattern recognition in high-dimensional spaces.

Secondly, deep learning can capture complex patterns in data. Network attack behaviors usually have complex patterns and dynamic changes, and traditional rule-based methods are difficult to accurately identify them. Deep learning models, especially neural networks with strong adaptive learning capabilities, can perform data learning and effective generalization detection on these complex patterns.

Furthermore, deep learning can enhance real-time detection. Network attack detection requires real-time analysis of network traffic and rapid detection of potential attack behaviors. Deep learning models, especially lightweight network architectures like MobileNet and ShuffleNet, can maintain high detection accuracy while also achieving fast data processing and response capabilities.

Finally, deep learning can adapt to new types of attack methods. In the context of constantly evolving network attack methods, conventional detection methods typically require updating rules and feature libraries. And deep learning models can automatically adapt to new attack patterns by continuously learning new data to reduce dependence on manual intervention.

2.3 Overview of Network Attack Detection Models Based on Deep Learning

The network attack detection models based on deep learning can be mainly divided into several main categories, one of which is based on convolutional neural network (CNN) models. CNN, as one of the common models in deep learning, utilizes convolutional and pooling layers to extract spatial features from data. When detecting network attacks, CNN can be used to extract features from network traffic data, such as packet size and packet spacing, to determine attack behavior. Taking LeCun et al. as an example, the LeNet-5 model is one of the typical CNN structures and has made remarkable achievements in the field of image recognition. When detecting network attacks, the LeNet-5 architecture can be used as a reference to design a CNN model suitable for network traffic data detection.

This is a model constructed based on Recurrent Neural Network (RNN). RNN, as a neural network capable of processing sequential data, captures temporal dependency information in the data through cyclic connections. When detecting network attacks, RNN can be used to analyze the time series characteristics of network traffic, such as traffic fluctuations and abnormal peak situations. Taking LSTM (Long Short Term Memory Network) and GRU (Gated Recurrent Unit) as examples, both variants of RNNs can efficiently handle the gradient vanishing problem in traditional RNNs and demonstrate excellent performance in processing sequential data.

Starting from the attention mechanism, establish a model. Attention mechanism is a technique that enables models to focus on important components of data. For network attack detection, attention mechanism helps the model discover key features of traffic data to improve detection accuracy. The sequence to sequence model based on attention mechanism, such as Bahdanau, efficiently encodes and decodes the input sequence by calculating the weights between the input sequence and the output sequence.

3. RESEARCH ON NETWORK ATTACK DETECTION MODEL BASED ON DEEP LEARNING

3.1 Network Attack Detection Model Based on Convolutional Neural Network

Convolutional neural network (CNN), as an advanced deep learning model, has a wide range of applications in various fields such as image and speech recognition. In terms of network attack detection, CNN can effectively extract the characteristics of network traffic data and achieve attack behavior recognition. The CNN model adopts a structure of convolutional layers, pooling layers, and fully connected layers to achieve automatic learning of local and global features of data, thereby improving detection accuracy [3].

In the process of establishing a CNN based network attack detection model, it is necessary to first preprocess the network traffic data, including data cleaning and normalization operations. Then, the preprocessed data is fed into the CNN model for training and pattern learning on the data. The key issue in CNN models is the design of convolutional kernels, and selecting appropriate kernel sizes and stride sizes can enable feature extraction at different scales. In addition, the expression ability of the model can be enhanced by adjusting the number and depth of convolutional layers.

3.2 Network Attack Detection Model Based on Bidirectional Long Short Term Memory Network

Long Short Term Memory Network (LSTM) is a special type of Recurrent Neural Network (RNN) that can solve the problem of gradient vanishing in traditional RNNs when processing long sequence data. LSTM introduces a gating mechanism to effectively capture the long-term dependencies of time series data. In terms of network attack detection, LSTM can process the temporal characteristics of network traffic data, improving detection accuracy.

Bi LSTM, as an extended form of LSTM, can simultaneously process past and future data at each time step, thus capturing the temporal properties of data more comprehensively. When constructing a network attack detection model based on Bi LSTM, it is necessary to first serialize the network traffic data to form a time series. Next, the serialized data is fed into the Bi LSTM model and trained and learned through temporal pattern training on the data.

The most crucial advantage of the Bi LSTM model is its ability to handle time series data. It can effectively capture the dynamic changes and trends of network traffic data, and identify the temporal characteristics of attack

behavior. In addition, the Bi LSTM model has good generalization ability and can adapt to various network environments and attack types. However, the Bi LSTM model has a high computational complexity for large-scale data processing, so it is necessary to optimize the model structure and training strategy in order to improve the efficiency of detection.

3.3 Network Attack Detection Model Based on Attention Mechanism

The attention mechanism plays a crucial role in the field of deep learning, and its core idea is to enhance the model's recognition ability by adaptively paying attention to key parts of the input data through the model. In terms of network attack detection, attention mechanism models help to focus on abnormal features of network traffic, effectively enhancing detection accuracy [4]. For example, the model can identify key packets of network traffic that may contain critical information about attack behavior by constructing an attention layer. Furthermore, attention mechanisms may be integrated with different deep learning models such as convolutional neural networks or long short-term memory networks to construct a more complex network architecture that better responds to constantly changing network attack patterns.

3.4 Network Attack Detection Model Integrating Multiple Deep Learning Technologies

With the rapid development of deep learning technology, it is usually difficult for a single model to deal with complex network attack detection tasks. So, integrating various deep learning techniques has become an effective method to improve detection performance. For example, by integrating the capabilities of convolutional neural networks in local feature extraction and the expertise of long short-term memory networks in time series modeling, we can construct a deep learning model that can simultaneously process spatial and temporal information. In addition, introducing attention mechanisms can further improve the model's ability to capture key information. Through the integration of multiple technologies, a more powerful network attack detection model can be constructed to effectively respond to various types of network attack behaviors.

4. INNOVATION OF NETWORK ATTACK DEFENSE STRATEGY BASED ON DEEP LEARNING

4.1 Intelligent Network Security Protection Based on Deep Reinforcement Learning

Deep reinforcement learning is one of the important branches of deep learning, and combining reinforcement learning with deep learning can effectively solve the problem of dynamic decision-making in network security [5]. In terms of intelligent network security protection, the use of deep reinforcement learning based methods can identify and respond to network attack behaviors in real time, thereby enhancing the automation and intelligence of network security protection. The intelligent network security protection strategy based on deep reinforcement learning includes the following contents: using deep learning technology to extract network traffic characteristics and analyze them to distinguish between normal traffic and abnormal traffic; Using reinforcement learning algorithms to train intelligent agents to develop optimal response strategies for network attacks, in order to enhance their recognition and defense capabilities; Combined with multi-agent systems, multi-agent collaborative defense has been achieved, enhancing the overall effectiveness of network security protection; Adopting deep reinforcement learning algorithms to optimize network security strategies online, achieving rapid adaptation to changes in the network environment.

4.2 Deep Learning based Hierarchical Network Attack Identification and Unknown Attack Detection

Layered network attack recognition is the process of breaking down the network attack detection task into several layers, with each layer responsible for detecting various attack behaviors. The use of layered methods has improved detection accuracy and efficiency. At the same time, detecting unknown attacks is an important research area in the current field of network security. The network attack recognition and unknown attack detection strategy based on deep learning layering includes the following: using deep learning technology to extract network traffic features at multiple levels to achieve the goal of identifying different types of attack behaviors; Using autoencoder as an unsupervised learning method to establish a normal traffic model for unknown attack detection; Combining supervised learning with unsupervised learning enhances the ability to detect known and unknown attacks; Applying deep learning models to network attack behavior classification and clustering to achieve in-depth analysis and understanding of attack behavior.

4.3 Industrial Control System Network Attack Detection Method Based on Petri Net Modeling

Industrial control systems are an important component of a country's critical infrastructure, and their security directly affects national security and social stability. However, industrial control systems are often threatened by complex network attacks. The method of using Petri net modeling for network attack detection can effectively analyze and identify network attack behaviors in industrial control systems.

The network attack detection methods for industrial control systems modeled using Petri nets mainly cover the following key areas: modeling the network architecture and behavior patterns of industrial control systems through Petri nets to achieve visual display of the internal state of the system; By analyzing the Petri net model, potential security vulnerabilities and attack paths in the system can be identified; Train and optimize Petri net models using deep learning techniques to improve the accuracy and real-time performance of network attack detection; Using Petri net models to formalize and infer network attack behavior, in order to quickly identify and respond to attack behavior.

5. CONCLUSION

The article delves into innovative network attack detection and defense strategies based on deep learning, with the aim of addressing the increasingly serious challenges of network security. Using comparative analysis, logical reasoning, and other methods to reveal the many influencing factors of deep learning technology applied in areas such as network attack detection and defense, reflecting the ability to analyze complex academic papers and think critically. The research conclusion shows that innovative network attack detection and defense strategies based on deep learning can effectively enhance network security protection capabilities and cope with complex and diverse network attacks. However, deep learning models still need further research and improvement in terms of generalization ability, interpretability, and real-time performance.

REFERENCES

[1] Zhang, T. (2025). A Knowledge Graph-Enhanced Multimodal AI Framework for Intelligent Tax Data Integration and Compliance Enhancement. Frontiers in Business and Finance, 2(02), 247-261.
[2] Bi, Y., & Su, T. (2025). A secure access method in English education network based on edge computing. Alexandria Engineering Journal, 128, 1125-1133.
[3] Xie, J., Zhang, L., Cheng, L., Yao, J., Qian, P., Zhu, B., & Liu, G. (2025). MARNet: Multi-scale adaptive relational network for robust point cloud completion via cross-modal fusion. Information Fusion, 103505.
[4] HOU, R., JEONG, S., WANG, Y., LAW, K. H., & LYNCH, J. P. (2017). Camera-based triggering of bridge structural health monitoring systems using a cyber-physical system framework. Structural Health Monitoring 2017, (shm).
[5] Q. Tian, D. Zou, Y. Han and X. Li, "A Business Intelligence Innovative Approach to Ad Recall: Cross-Attention Multi-Task Learning for Digital Advertising," 2025 IEEE 6th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT), Shenzhen, China, 2025, pp. 1249-1253, doi: 10.1109/AINIT65432.2025.11035473.
[6] Y. Zhang, Z. Tian and H. Hua, "Design of an Autonomous Vehicle Speed Control System Based on a PID Controller," 2025 International Conference on Advances in Electrical Engineering and Computer Applications (AEECA), Dalian, China, 2025, pp. 491-495, doi: 10.1109/AEECA65693.2025.00092.
[7] Y. Zhang, Z. Bai and Q. Luo, "AI-Driven Cloud Computing Data Security Monitoring and Response System," 2025 International Conference on Advances in Electrical Engineering and Computer Applications (AEECA), Dalian, China, 2025, pp. 817-821, doi: 10.1109/AEECA65693.2025.00148.
[8] Deng, X., & Yang, J. (2025, August). Multi-Layer Defense Strategies and Privacy Preserving Enhancements for Membership Reasoning Attacks in a Federated Learning Framework. In 2025 5th International Conference on Computer Science and Blockchain (CCSB) (pp. 278-282). IEEE.
[9] Sultan, N., Patwar, N., Wei, X., Chew, J., Liu, J., & Du, R. (2026). FedGuard: A Robust Federated AI Framework for Privacy-Conscious Collaborative AML, Inspired by DARPA GARD Principles. International Academic Journal of Social Science, 2, 1–16. https://doi.org/10.5281/zenodo.18253151
[10] Zhu, Y., Yu, W., & Li, R. (2025). SAGCN: A spatiotemporal attention-weighted graph convolutional network with IoT integration for adolescent tennis motion analysis. Alexandria Engineering Journal, 128, 652-662.