Improvement and Verification of Deep Learning-Driven Network Anomaly Traffic Detection Model

Zhao Liangpan[12] Wei Chaoxin[12]

1 Mongolian National University，Ulaanbaatar city, Bayangol District, 11th Khoroo, National University of Mongolia，16060；

2 Jiangxi Institute of Fashion Technology，No. 103, Lihu Middle Avenue, Xiangtang Development Zone, Nanchang City, Jiangxi Province，330201；

Abstract： In the context of digital transformation, network security faces severe challenges. Traditional anomaly traffic detection methods have significant limitations. Although deep learning offers a new direction for this field, existing models suffer from issues such as single-feature capture, weak scenario adaptability, and insufficient real-time response. This paper constructs an optimization system from three dimensions: "Feature Fusion - Architecture Design - Training Mechanism." Multi-dimensional feature fusion is achieved through "Micro - Meso - Macro" three-level extraction and dynamic weighting, addressing the problem of incomplete feature coverage. The LFA lightweight architecture is designed, simplifying modules and optimizing the preprocessing pipeline to enhance real-time response capability. Multi-scenario fusion training and dynamic adjustment strategies are adopted to improve the model's scenario adaptability and robustness. Multi-scenario verification shows that the optimized LFA model outperforms traditional deep learning models in detection accuracy, scenario adaptability, and real-time responsiveness. Finally, the study points out limitations regarding dataset coverage and the identification of sparse anomaly traffic, and suggests future research directions.

Keywords： Deep Learning; Network Anomaly Traffic Detection; Feature Fusion; Scenario Adaptability

DOI:10.69979/3041-0843.25.03.059

Introduction

In the process of digital transformation, networks have become critical infrastructure. However, the continuous evolution of attack methods poses serious threats to network security. Traditional detection methods (such as rule-based, statistical, and traditional machine learning approaches) have numerous limitations. Deep learning provides a new research direction for network anomaly traffic detection, but existing deep learning detection models face problems like single-feature capture, poor scenario adaptability, and high detection latency. Optimizing these models holds significant theoretical and practical importance: theoretically, it helps enrich the application of deep learning in the field of network security; practically, it can improve the effectiveness of network protection and promote the practical application of models in multiple scenarios. Relevant research domestically and internationally has different focuses: domestic research primarily concentrates on improving model architectures and optimizing features, while international research emphasizes model practicality and scenario adaptation. This paper addresses the problems of existing models by optimizing them from three aspects: expanding feature dimensions, lightweight architecture design, and adaptive training mechanisms. The performance of the optimized model is analyzed through scenario-based verification.

1 Related Theoretical Foundations

1.1 Overview of Network Anomaly Traffic

Network traffic refers to the total amount of data and its characteristics during network transmission. Normal network traffic follows protocol specifications and exhibits stable patterns, whereas anomalous traffic deviates from regular patterns, potentially caused by network attacks, equipment failures, or configuration errors, manifesting as characteristics like repeated requests or abnormal data formats. Based on causes, anomalous traffic can be divided into three categories: Attack-based anomaly traffic (e.g., DDoS attacks, SQL injection attacks) poses the greatest threat to network security; Failure-based anomaly traffic is caused by equipment or link failures; Configuration-based anomaly traffic stems from incorrect network settings. The evaluation of network anomaly traffic detection models typically considers four core dimensions: Detection Accuracy (including resistance to false positives and false negatives), Scenario Adaptability (i.e., the model's adaptation capability in different network environments), Real-time Responsiveness (reflected in detection speed), and Robustness (i.e., the model's ability to resist data interference).

1.2 Principles of Core Deep Learning Models

Convolutional Neural Networks (CNNs) are adept at processing grid-structured data. They primarily consist of an input layer, convolutional layers (extracting local features via sliding kernels with parameter sharing), pooling layers (reducing data dimensionality and computation), fully connected layers (integrating extracted features), and an output layer. They can effectively extract local correlation features in network traffic. Recurrent Neural Networks (RNNs) are suitable for processing sequential data. Their hidden layers form a "memory chain" through recurrent connections, but they can suffer from "memory decay" when processing long sequences. To address this, improved models like Long Short-Term Memory networks (LSTMs) use a three-gate mechanism to select and retain key information, while Gated Recurrent Units (GRUs) merge gating mechanisms to simplify computation. These models can capture temporal patterns in network traffic. The Attention Mechanism simulates the human attention allocation process by assigning dynamic weights to data. In anomaly detection, it can optimize the feature fusion process and enhance focus on key temporal nodes, thereby improving the model's judgment accuracy.

2 Analysis of Core Problems in Existing Deep Learning Detection Models

Current deep learning-based network anomaly traffic detection models, while theoretically breaking through the limitations of traditional detection and possessing the ability to autonomously learn features, are constrained by technical design flaws and complex network environments in practical deployment. They face three core problems that limit their detection performance and application value.

2.1 Single Feature Capture Dimension, Difficulty Covering Complex Traffic Attributes

Network traffic contains three types of features: local details (data packet field combinations, protocol formats), temporal patterns (changes in IP connection frequency), and overall distribution (total traffic volume fluctuations, port usage density). Existing models are generally "dimension-dependent," only capable of capturing one type of feature, leading to identification blind spots. For example, a single CNN is good at extracting local features but ignores temporal patterns, easily missing latent attacks involving sudden changes in IP connection frequency. A single LSTM or GRU can track temporal features but is insensitive to local details like abnormal fields in SQL injection, making it difficult to identify immediate attacks. Furthermore, models lack "scale adaptability," mostly using a single time scale: millisecond-level scales are prone to misjudgment due to data noise, minute-level scales easily miss short-term, concentrated anomalous packets, and they fail to synergize multi-scale features.

2.2 Weak Scenario Adaptability, Difficulty Coping with Diverse Network Environments

Existing models exhibit prominent "scenario rigidity," where performance depends heavily on the training data's scenario characteristics, leading to poor stability across environments. On one hand, models are often trained on specific scenarios (e.g., enterprise intranets), learning normal patterns like "fixed IP high-frequency interaction," which conflict with features of other scenarios like "temporary IP short-term connections" in public WiFi, causing false positive rates to soar when applied directly. On the other hand, models adapt poorly to evolving attacks. New attacks (e.g., IoT DDoS) have significantly different features from traditional attacks, but models mostly operate on a "static training - static application" basis, with fixed parameters unable to autonomously learn new features, requiring retraining which is time-consuming and creates a "protection lag," making it difficult to cope with rapidly changing attack landscapes.

2.3 Insufficient Real-time Response Capability, Difficulty Meeting Real-time Protection Needs

"Computational redundancy" leads to high detection latency, making models unsuitable for real-time protection, stemming from two design flaws. First, architectural "complexity redundancy": some hybrid models (e.g., traditional CNN-LSTM) blindly stack modules without optimizing parameter transfer, leading to parameter explosion and cumbersome computation. Under large-scale traffic, delay exceeds real-time thresholds, rendering detection results meaningless for protection. Second, preprocessing "pipeline redundancy": models perform full preprocessing on all traffic, whereas in practice, most normal traffic has clear identifiers (e.g., regular transmissions from fixed IPs in an enterprise intranet). Full processing wastes computational resources, further slowing detection speed and exacerbating the real-time response problem.

3 Optimization Scheme for Deep Learning-Based Network Anomaly Traffic Detection Model

Aiming at the core problems of existing deep learning detection models in feature capture, scenario adaptation, and real-time response, this paper constructs an optimization system from three dimensions: "Feature Fusion - Architecture Design - Training Mechanism," aiming to build a network anomaly traffic detection model that is comprehensive, adaptable, and efficient.

3.1 Multi-dimensional Feature Fusion Optimization: Covering Complex Traffic Attributes Across Scenarios

To solve the problem of single-feature capture in existing models, this paper adopts a "hierarchical extraction - dynamic weighting" mechanism. A "Micro - Meso - Macro" three-level feature extraction module is constructed: The Micro module uses a simplified CNN to extract millisecond-level local features (e.g., abnormal fields). The Meso module uses a GRU to capture second-level temporal patterns (e.g., changes in connection frequency). The Macro module utilizes statistical techniques to obtain minute-level overall features (e.g., total traffic volume fluctuations), ensuring comprehensive capture of multi-scale traffic features. Simultaneously, a multi-scale attention fusion mechanism is introduced to dynamically adjust the weights of each module, filter redundant features, and focus on key dimensions, thereby improving the model's detection accuracy.

3.2 Lightweight Architecture Design: Balancing Performance and Real-time Response

To address the insufficient real-time response capability of existing models, this paper uses a "module simplification - pipeline optimization" approach to build the LFA lightweight architecture. In terms of core module modification: the convolutional module retains only a "1 convolutional layer + 1 pooling layer" structure, reducing the number of kernels; the temporal module uses GRU instead of LSTM to simplify computation; the attention module connects directly to the output layer, omitting complex fully connected layers, thus significantly reducing the model's detection latency. Regarding data preprocessing, it is optimized into a "layered mechanism": For obviously normal traffic, judgment is made directly through a fast filtering channel; for potentially anomalous traffic, it enters the fine-processing channel, reducing invalid computation and improving the model's overall processing speed.

3.3 Adaptive Training Mechanism: Enhancing Scenario Adaptability and Robustness

To improve the poor scenario adaptability of existing models, this paper adopts a "multi-scenario fusion - dynamic adjustment" strategy. A cross-scenario training dataset is constructed, integrating network traffic data and new attack features from multiple scenarios, and a scenario-label attention mechanism is introduced, enabling the model to learn the relationship between scenarios and features, thus better adapting to different network environments. During training, a dynamic learning rate adjustment strategy is used, adjusted according to the training phase: in the early stage, a higher learning rate is used for rapid parameter space exploration; in the middle stage, optimization is based on real-time changes in the loss function; in the later stage, a lower learning rate is used for fine convergence. Additionally, simulated network noise and a noise-adaptation loss function are incorporated during training to guide the model to focus on stable anomalous features, improving the model's robustness and reducing misjudgments.

4 Model Verification and Effect Analysis

To verify the effectiveness of the optimized LFA architecture model, this paper designs multi-scenario simulation experiments, analyzing the model's advantages in detection accuracy, scenario adaptability, and real-time responsiveness from a qualitative level. Comparison subjects include a single CNN, a single LSTM, and a traditional CNN-LSTM hybrid model.

4.1 Verification Scenarios and Experimental Design

Three types of typical network scenario simulation environments are constructed: Scenario 1 is an enterprise intranet environment, containing regular business data transmission between fixed IPs, with anomaly types being port scanning and unauthorized access. Scenario 2 is a public WiFi environment, containing numerous short-term connections from temporary IPs, with anomaly types being malware download and fake AP requests. Scenario 3 is an industrial control network environment, containing transmission of device control commands, with anomaly types being command tampering and illegal firmware updates. During experiments, all scenarios incorporate network noise to simulate real network environments. After model training, new attack features not involved in training (e.g., new DDoS attacks targeting industrial devices) are introduced to test the model's ability to identify unknown attacks.

4.2 Detection Accuracy Analysis

In the three simulated scenarios, the detection accuracy of the LFA model is significantly better than the comparison models. For immediate attacks (e.g., SQL injection), the LFA model, through micro-feature extraction and dynamic weighting, effectively avoids the missed detection problems of single temporal models, whereas the single LSTM struggles to identify short-term local anomalies. For latent attacks (e.g., slow infiltration attacks), the LFA model's meso-temporal module (GRU) can track dynamic changes in traffic, avoiding missed detection issues of single CNN models, as single CNNs only focus on local features and cannot identify long-term gradual anomalies. For large-scale attacks (e.g., DDoS), the LFA model's macro module can identify overall distribution anomalies in traffic, avoiding misjudgments caused by feature redundancy in traditional hybrid models through multi-scale feature fusion, whereas traditional hybrid models are easily disturbed by normal traffic fluctuations. Furthermore, due to its generalization ability from multi-scenario training, the LFA model can identify new attacks, while comparison models, having not learned relevant features, show significant missed detections.

4.3 Scenario Adaptability Analysis

In cross-scenario testing, the LFA model's performance is more stable. When the model trained on Scenario 1 is applied to Scenario 2, comparison models (e.g., single CNN) cause a sharp increase in false positive rates because they haven't learned the normal features of "temporary IP short-term connections," whereas the LFA model can autonomously adapt to scenario differences, maintaining a low false positive rate. The traffic features of Scenario 3 (e.g., fixed-format device control commands) differ significantly from the first two scenarios. Traditional models suffer from a surge in false negative rates due to feature mismatch, while the LFA model, aided by the scenario-label attention mechanism, can quickly identify the traffic patterns of industrial networks, with no significant increase in false negative rates, effectively solving the "scenario rigidity" problem of traditional models.

4.4 Real-time Responsiveness Analysis

When processing large-scale network traffic, the LFA model's real-time response advantage is evident. Its lightweight architecture and layered preprocessing mechanism result in a processing time per traffic flow that is far lower than that of comparison models. The traditional CNN-LSTM hybrid model, due to its complex structure, exceeds the real-time protection threshold for detection latency when handling concurrent large-scale data packets, whereas the LFA model's delay is controllable, allowing timely output of detection results. The layered preprocessing mechanism plays a crucial role in improving real-time response speed. A large amount of normal traffic is judged directly through the fast filtering channel, bypassing the full feature extraction process, saving computational resources, and further enhancing the model's overall response speed.

5 Conclusion and Outlook

5.1 Research Conclusion

Addressing the problems of single feature capture, weak scenario adaptability, and insufficient real-time response in deep learning network anomaly traffic detection models, this paper proposes a three-stage optimization scheme of "Feature Fusion - Architecture Lightweighting - Training Adaptation," constructing the LFA lightweight hybrid model. Multi-scenario verification shows that: multi-dimensional feature fusion through "Micro-Meso-Macro" extraction and dynamic weighting improves detection accuracy; the lightweight architecture simplifies modules and uses layered preprocessing, reducing redundancy and controlling delay; adaptive training enhances scenario adaptation and robustness, reduces false positives/misses, and enables identification of new attacks.

5.2 Research Limitations and Future Outlook

Research Limitations: First, the training dataset only covers three types of scenarios, lacking verification of adaptability to emerging scenarios. Second, identification of sparse anomaly traffic, such as low-frequency targeted attacks, is insufficient. Future work will: Expand research into emerging scenarios and AI-driven attacks; Introduce federated learning and design dynamic update mechanisms; Integrate multi-modal data to enhance the ability to identify sparse anomaly traffic.

References

[1] Yang Yuelin, Bi Zongze. Deep Learning Based Network Traffic Anomaly Detection [J]. Computer Science, 2021(S2): 540-546.

[2] Li Yanmiao. Research on Network Anomaly Traffic Detection Technology Based on Deep Learning [D]. Beijing University of Posts and Telecommunications, 2023.

[3] Hang Mengxin, Chen Wei, Zhang Renjie. Anomaly Traffic Detection Based on Improved 1D-CNN [J]. Journal of Computer Applications, 2021, 41(2): 433-440. DOI:10.11772/j.issn.1001-9081.2020050734.

[4] Yin Chuanlong. Research on Network Anomaly Detection Technology Based on Deep Learning [D]. Strategic Support Force Information Engineering University, 2019.

[5] Gao Jia. Research and System Implementation of Network Anomaly Traffic Detection Based on Deep Learning [D]. Shihezi University, 2023.