Theory and Practice of Science and Technology
2025, VOL. 6, NO. 8, 100-104
DOI: 10.47297/taposatWSP2633-456919.20250608

A Review of AI-Based Network Anomaly Traffic Detection

Kehan Li

School of Information Engineering, Sichuan Agricultural University, Chengdu, Sichuan, 611230, China

ABSTRACT
In the face of increasingly complex and covert cyberattacks, cybersecurity has become paramount, yet traditional methods face limitations. Consequently, AI-driven anomaly traffic detection has emerged as a hot research topic in the field. This review systematically organizes research progress in AI-based network anomaly traffic detection. It first defines anomaly traffic types and analyzes limitations of traditional detection methods, then focuses on key technologies of machine learning and deep learning models in feature learning and anomaly identification. The review compares the advantages and disadvantages of different models, finally analyzing current challenges and outlining future research directions.

KEYWORDS
Anomaly traffic detection; Machine learning; Deep learning; Cybersecurity

1 Introduction

As a core component of proactive defense, network anomaly traffic detection requires precise identification of malicious activities within massive data streams to enable early warning. Traditional methods, which predominantly rely on rule-based and threshold analysis, are widely adopted but exhibit significant limitations: dependence on prior knowledge, difficulty in detecting unknown attacks, and rule update delays leading to high false positives and false negatives. Their performance and scalability also struggle to handle high-speed traffic.

To overcome these limitations, researchers have turned to AI technologies. Machine learning and deep learning offer new avenues for building next-generation intelligent detection systems through automated feature extraction, complex nonlinear modeling, and big data mining capabilities.

This review analyzes multiple AI-based anomaly traffic detection methods, examining their core technologies, innovations, and shortcomings, while exploring challenges and future research directions.

2 Types of network anomalies and traditional detection methods

2.1 Concept and types of network anomalous traffic

Network abnormal traffic refers to traffic data that significantly deviates from normal behavioral patterns, expected benchmarks, or legitimate operational norms within computer networks. Based on its motivation and technical characteristics, it can be primarily categorized as follows:

(1) Denial-of-Service (DoS) Attack-Based Anomalies: These attacks aim to exhaust target system resources, rendering them unable to provide normal services, such as distributed denial-of-service (DDoS) attacks.

(2) Intrusion and malware-based anomalies: This traffic is typically associated with specific malicious activities, such as information theft or system sabotage.

(3) Anomalies stemming from network failures and configuration errors: These anomalies are non-malicious in origin but still impact network health and require detection and remediation.

2.2 Limitations of traditional detection methods

Traditional detection methods primarily rely on rule-based signature matching and predefined statistical threshold analysis, but they have significant limitations:

(1) High false positive rate: Fixed rules struggle to detect unknown attacks or variants and are easily bypassed by encryption and obfuscation techniques;

(2) Difficulty in processing high-dimensional data: Ineffective analysis of encrypted traffic and high-dimensional features, resulting in low computational efficiency;

(3) Lack of Adaptability: Inability to dynamically adjust to behavioral changes necessitates manual intervention, and models are prone to degradation.

Traditional detection methods excel in interpretability and known threat detection. However, their static nature and reliance on prior knowledge make them ill-suited for unknown attacks and encrypted traffic, failing to meet modern dynamic defense requirements. AI, by automatically learning complex features from raw data, offers a new pathway to

overcome these traditional challenges, propelling the field into a new era.

3 Several AI-based methods for detecting network anomalies

3.1 CNN-based detection method

The core of CNN-based detection lies in extracting data features using CNN architecture, as illustrated in Figure 1. Zhu Huarong collected traffic data via Wireshark and applied weighted average filtering for equalization to smooth fluctuations. Feature extraction was performed using CNN: the convolution layer detected local features, the pooling layer downsampled to retain key information, and the fully connected layer implemented nonlinear transformation via the Sigmoid function to output anomaly feature vectors. The overall similarity of abnormal traffic is then computed, with a dynamic threshold set. Finally, anomaly identification and alerts are achieved by calculating the probability of abnormality [1].

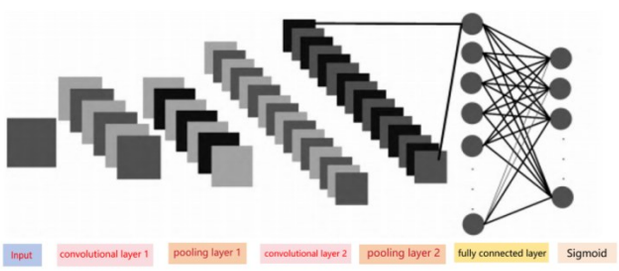

Figure 1 CNN learning architecture

The key innovations of this technology are as follows:

(1) Integration of CNN and filtering techniques: First implementation of weighted average filtering to process network traffic fluctuations, enhancing data stability.

(2) Feature extraction optimization: Incorporating a Sigmoid activation function into the CNN fully connected layer to enhance nonlinear feature representation capabilities.

(3) Dynamic threshold mechanism: Thresholds are adaptively set based on overall similarity to reduce false alarm rates.

However, its limitations are also evident, such as: the preset parameters of weighted average filtering struggle to adapt to large-scale networks; dynamic thresholds rely on manual configuration and lack adaptive optimization mechanisms.

To address the adaptability issue, Xu Yifan introduced MHSE after feature extraction via CNN. Following spatial feature extraction by CNN, each convolutional layer was followed by batch normalization and ReLU activation to accelerate convergence and suppress overfitting. MHSE was then applied to enhance multi-scale features, while BiLSTM captured bidirectional temporal dependencies. Finally, Softmax was employed for anomaly traffic classification [2]. The innovation lies in leveraging MHSE's multi-scale perception, integrating dilated convolutions with SE attention to adaptively enhance key features. Simultaneously, it deeply fuses spatio-temporal features through CNN-BiLSTM collaboration, overcoming limitations of single-model approaches. Figure 2 depicts the MHSECNN-BiLSTM architecture.

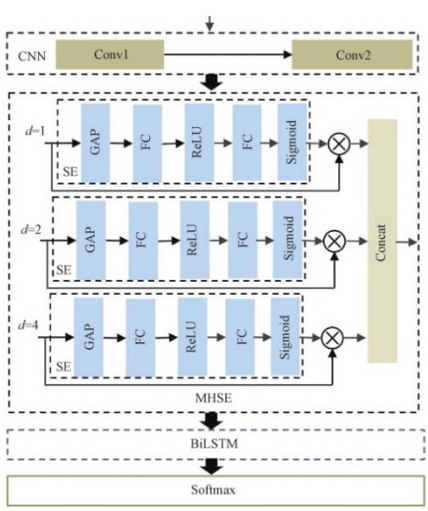

Figure 2 MHSECNN-BiLSTM architecture

3.2 RNN-based detection methods

LSTM is a specialized RNN designed to overcome the difficulty of traditional RNNs in capturing long-term dependencies in lengthy sequences. Wei Bo preprocessed data using Wireshark, then generated feature vectors via learnable weights and filtered key features using Softmax. Subsequently, an LSTM with forget gate, input gate, and output gate was constructed for training. Finally, anomaly detection was achieved by calculating reconstruction error and setting dynamic thresholds [3]. The LSTM architecture constructed by this technique is shown in Figure 3:

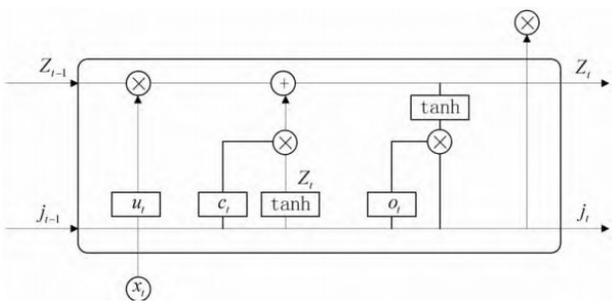

Figure 3 LSTM Model structure

The advantages of this approach are as follows:

(1) Unsupervised detection paradigm: Requires training the LSTM model solely on normal traffic, identifying anomalies through reconstruction error, thereby avoiding reliance on labeled anomaly samples.

(2) Dynamic threshold adaptation: Thresholds are automatically adjusted based on the error distribution of normal traffic, enhancing generalization capabilities against novel anomalies.

However, relying solely on normal data for training means anomaly intrusion can cause threshold drift and reduced sensitivity. The association between reconstruction error and anomaly types is unclear, making it difficult to pinpoint attack origins. For handling complex, high-dimensional data, Deng et al. introduced a Random Forest (RF) approach. This combines RF's feature selection capability with LSTM's temporal modeling ability, performing normalization to complete key feature selection and dimensionality reduction [4]. The RF stage effectively reduces the dimensionality of data input to the LSTM, forming a complementary hybrid model.

3.3 GAN-based detection method

The GAN-based detection process involves training a GAN model using preprocessed normal traffic data. The generator receives random noise as input, aiming to generate data as similar as possible to normal traffic features. The discriminator then receives two inputs: real normal traffic data and data generated by the generator.

Setting thresholds for reconstruction error or discriminator scores requires empirical tuning or adjustment. Zou Xintong et al. improved the GAN model by employing a joint temporal distribution for feature analysis. They constructed a model based on the TadGAN framework, where both the generator and discriminator utilize LSTM structures to capture temporal dependencies. By combining reconstruction error with discriminator output, they calculated anomalies using a non-parametric dynamic threshold [5].

The innovation of this method lies in:

(1) Innovative temporal modeling: Integrating LSTMs into both the generator and discriminator of the GAN enhances the ability to capture long-term dependencies in supply chain time-series data.

(2) Dynamic Threshold Algorithm: Introduces a non-parametric dynamic threshold that adaptively selects thresholds, addressing the bias issues of fixed thresholds in volatile data.

3.4 Decision tree-based detection method

The decision tree-based detection process involves: After data preprocessing and feature selection, the decision tree model recursively selects optimal features to partition the data, forming tree-like classification rules. Its optimization core lies in suppressing overfitting and enhancing generalization capabilities. However, fixed-parameter decision tree models may struggle to effectively identify novel or highly dynamic anomalous traffic. To address this, Zhang Renfei et al. employed K-Means clustering during feature standardization, followed by real-time prediction using a decision tree model [6].

This method innovatively combines K-Means clustering with decision trees. By analyzing traffic distribution patterns through clustering, it provides structured input to the decision tree, enhancing its learning capability for complex traffic patterns and overcoming the limitation of single decision trees in adapting to variable traffic. Decision tree parameters are optimized to ensure real-time detection with low computational overhead. Strict TCP/GPRS feature thresholds enhance robustness, making the method suitable for high-dimensional heterogeneous data environments in mobile

communication networks. However, a drawback is that the iterative process of clustering and decision tree training may introduce delays in ultra-large-scale traffic scenarios, necessitating further improvements in computational efficiency.

3.5 Isolated forest-based detection method

Isolated forests are ensemble learning algorithms based on decision trees. This algorithm constructs multiple isolated trees, performing random splits on the data until each sample is isolated. During tree construction, anomalous samples are typically isolated more quickly, exhibiting shorter path lengths, while normal samples require more partitioning steps to isolate, resulting in longer path lengths. By calculating the average path length of each sample across all isolated trees, an anomaly score is derived for that sample. A higher score indicates a greater likelihood of the sample being anomalous.

However, isolated forests are insensitive to local density anomalies. If anomalous points cluster into small groups, they may be missed due to the additional steps required for isolation. Li Cheng et al. constructed a spectral feature model, detecting spectral density and computing difference parameters through multi-level reconstruction. They employed local polynomial regression and SVM loss optimization for anomaly feature analysis. Traffic sequences were processed using low-pass filtering and rough set theory to extract dynamic features and localize anomalies. Finally, the Isolated Forest algorithm performed adaptive clustering and parameter expansion to achieve real-time anomaly traffic identification [7].

The innovation lies in pioneering the application of the Isolated Forest algorithm for anomaly detection in elastic optical networks, combined with multidimensional spatial structure reorganization to achieve adaptive optimization control of anomaly points. However, spectral feature extraction involves multiple reconstructions and rough set computations, resulting in high computational resource demands during training.

3.6 Random forest-based detection method

Random forest-based network anomaly traffic detection methods first construct decision trees, then combine multiple decision trees into a random forest model. By integrating multiple decision trees, the model's generalization capability and accuracy are enhanced, making it highly suitable for processing high-dimensional, complex network traffic data. However, random forest parameter settings require careful adjustment, as inappropriate parameters may lead to model overfitting.

Yuanquan leveraged random forest to compute feature importance for key feature selection, feeding these into the TabNet model for spatio-temporal feature extraction and training. This ultimately achieved anomaly traffic detection, with model performance evaluated via loss curves and accuracy metrics [8]. The core structure of the TabNet model is illustrated in Figure 4.

The innovation lies in the novel integration of RF and TabNet: RF provides feature importance scores, while TabNet enables efficient feature extraction. This approach maintains high accuracy even in scenarios with limited features and effectively addresses overfitting issues.

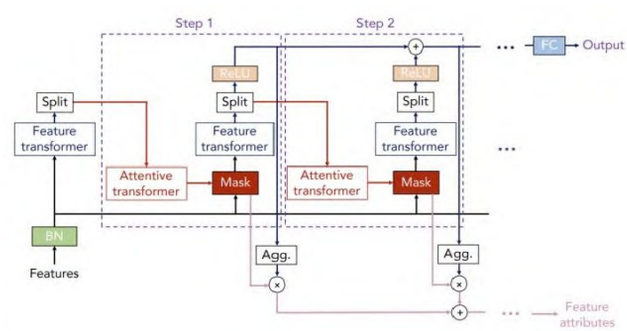

Figure 4 Tabnet architecture

4 Challenges and future prospects

4.1 Challenges

This field still faces several critical challenges:

(1) Evolution of Adversarial Attacks: Attackers leverage AI to generate adversarial traffic and samples to evade detection

(2) Data Quality and Processing: Complexities in handling unstructured data and challenges in feature engineering constrain model accuracy

(3) Dynamic and Unknown Threats: Cyberattack methods continuously evolve, requiring models to continuously learn and adapt to new threats, such as difficulty in countering zero-day attacks and APTs

4.2 Future outlook

Future research should focus on the following areas:

(1) Adaptive and Continuous Learning: Develop online mechanisms that sustainably acquire new knowledge, adapt to shifting behavioral baselines, and prevent catastrophic forgetting to address dynamic cyber environments.

(2) Federated Learning and Privacy-Preserving Computation: Designing more efficient and secure cross-domain collaborative training frameworks that balance data privacy and model performance.

(3) Lightweight and Edge Computing: Develop low-power, low-latency edge-side detection algorithms through techniques like model compression, pruning, and distillation.

5 Conclusion

AI has injected powerful new momentum into network anomaly traffic detection, reshaping cybersecurity defense strategies. This paper systematically reviews AI research advancements and applications in network anomaly traffic detection, detailing core technologies, innovations, and limitations of models like CNNs, RNNs, and LSTMs. Finally, it proposes future development directions addressing current challenges.

References

[1] Zhu , R. (2024)Fast identification of abnormal traffic in communication networks based on deep learning. Yangtze River Information and Communication.,37(12):96-98.

[2] Xu,Y.(2025)Network anomaly traffic detection method based on spatio-temporal feature fusion. Electronic Measurement Technology., 48(14): 19-25.

[3] Wei, B. (2025)Anomalous behavior detection method for large-scale network traffic based on LSTM. Industrial Control Computer.,38(08):89-91.

[4] Deng, H. W.. (2023)Deep learning-based network traffic anomaly identification and detection. Computer System Applications.,32(02):274-280.

[5] Zou, X. (2025)Anomaly identification model of supply chain data based on improved adversarial network. Computer Applications and Software., 42(07): 107-110.

[6] Zhang, R . (2024)Decision tree mining based anomaly identification in mobile communication networks. Telecommunications Express., (10): 36-39.

[7] Li, C . (2024)Automatic identification of anomalous traffic in resilient optical networks based on isolated forest algorithm. Laser Journal., 45 (01): 179-183.

[8] Yuan, Q. (2024)Network traffic anomaly identification and detection based on RF+TabNet. Network Security Technology and Application., (12): 38-42.