NETWORK TRAFFIC ANALYSIS BASED ON DEEP LEARNING ALGORITHMS

Xia Enduo, Fan Linda, He Hongyan
Department of Radiophysics and Computer Technologies, Belarusian State University
Minsk, Republic of Belarus
E-mail: enduoxia@gmail.com, fld420605545@gmail.com, hehy9527@gmail.com

We propose a unified anomaly detection framework based on CNN-BiLSTM-Attention to address the low accuracy and high false positive rates of existing traffic-based network anomaly detection methods. The framework represents each network session as a 2D grayscale image, uses 2D-CNN for spatial feature extraction, BiLSTM for long-range temporal dependency capture, and an attention mechanism to highlight the most discriminative features. Experiments on the USTC-TFC-2016 and CICDDoS 2019 datasets show that this framework significantly outperforms state-of-the-art methods in accuracy, detection rate, and false positive rate, demonstrating its effectiveness and generalization for network traffic classification.

Introduction

With the rapid development of the Internet and information technology, cyberattacks pose a significant threat to network and user information security. Traditional solutions relying on past experience or localized packet information often result in false detections and false positives. To address these issues, this paper proposes a hierarchical model combining 2D-CNN with Bi-LSTM-Attention. The USTC-TFC-2016 and CICDDoS 2019 datasets were normalized to 16,000 bytes and reshaped into 40×40 grayscale images. The model uses 2D-CNN to extract spatial features from each packet image and Bi-LSTM-Attention to model long-term dependencies across the session. Experimental results show that the proposed model significantly outperforms traditional methods, with an inference latency of less than 0.8 ms per flow on an RTX 2080Ti graphics card. This confirms that reshaping packet data into 2D images and mining local patterns enhances the accuracy and robustness of real-time malicious traffic detection.

I. Related Work

Traditional ML methods like Random Forest [4], SVM [6], DT [2], and KNN [5] are widely used for intrusion detection but struggle with large-scale anomalies. Deep learning, with algorithms like CNN [1], and BiLSTM [3], offers better feature extraction. BiLSTM reduces false alarms, and the attention mechanism is gaining popularity in this field. This paper proposes a CNN-BiLSTM-Attention intrusion detection model. It combines 2D-CNN and BiLSTM to extract spatiotemporal features and uses the attention mechanism to filter significant features, thereby enhancing classification performance. Experiments on two public datasets show that the proposed model achieves superior classification results.

II. CNN-BiLSTM-Attention Model

Figure 1 shows the framework of the CNN-BiLSTM-Attention algorithm. We first segment the original data stream into conversation streams, convert each packet in the conversation stream into a grayscale image, and then concatenate them to obtain a grayscale image of the conversation stream. Next, for the conversation stream image, we use a 2D-CNN to split the conversation into a sequence of packets and perform linear embedding. An LSTM is used to extract the temporal relationship between each packet in the conversation stream. The input of each hidden layer of the LSTM serves as the final embedding of the packet sequence in the conversation. The conversation stream embedding is fed into a multi-head attention layer to obtain a feature map for each session. A CNN is then used to extract the final features of the conversation stream from this feature map. Finally, a fully connected layer is used to identify data flow.

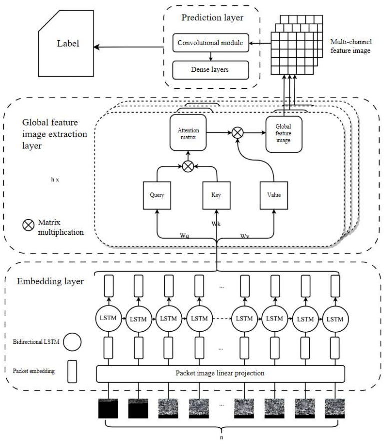

Figure 1 – Overall of CBAM

During the preprocessing phase, we focus on the payload of application layer packets and ignore other layers.The network flow is divided into sessions S based on five-tuples.

$$S = \{P_1,P_2,\ldots,P_n\} \tag{1}$$

The packet size is uniformly set to 1600 bytes, with any missing bytes padded with 0x00. The first t packets are taken, and any missing bytes are padded to t. Each packet is converted to a 40x40 grayscale image, generating a sequence of packet images that are then merged to form the session flow image S.For example, Figure 2. In the embedding layer, a 2D-CNN is used to decompose the session image into a sequence of packet images, generating an initial embedding for each packet. Specifically, a two-dimensional convolution operation is performed on each packet image D_i to create a linear embedding:

$$E_i = W_{\text{conv}} * D_i + b_{\text{conv}} \tag{2}$$

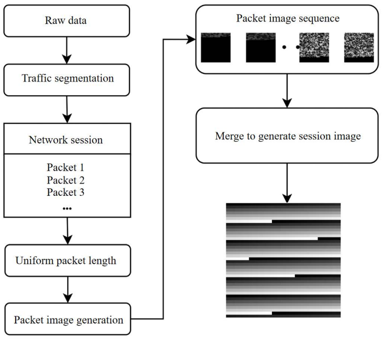

Figure 2 – Data preprocessing of CBAM

For each linear embedding E_i, a bidirectional LSTM layer is used to obtain contextual information:

$$H_i = [\overrightarrow{h_t}, \overleftarrow{h_t}] \tag{3}$$

Finally, all H_i are assembled into the final output representation X of the session, where $d = 2 \times \text{lstm}_d$.he global feature map extraction layer introduces a self-attention mechanism to extract global features from the conversation flow. First, a linear transformation is performed:

$$Q,K,V = XW_q, XW_k, XW_v \tag{4}$$

Then the self-attention weight matrix A is calculated:

$$A = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right) V \tag{5}$$

The global feature map M is obtained:

$$M = A \cdot V \tag{6}$$

Furthermore, a multi-head self-attention mechanism is used to project the query, key, and value matrices into h subspaces, generating multiple feature maps Z_i:

$$Z_i = \text{softmax}\left(\frac{Q_i K_i^T}{\sqrt{d_k}}\right) V_i \tag{7}$$

These feature maps are then concatenated into a three-dimensional tensor Z. At the prediction layer, a convolutional neural network is used to extract features from the feature map Z. First, a convolution operation is performed:

$$F‘ = \sigma(W * Z + b) \tag{8}$$

Then global average pooling is performed:

$$v = \frac{1}{t‘ \cdot m‘} \sum_{i=1}^{t‘} \sum_{j=1}^{m‘} F‘_{i,j} \tag{9}$$

Finally, classification is performed:

$$\hat{y} = \text{softmax}(W‘ \cdot v + b‘) \tag{10}$$

III. Experimental analysis

To validate the generalization performance of our experimental model, this study employed a widely used public network traffic dataset. In our experiments, we primarily evaluated our experimental model and compared it with several advanced flow classification methods. These methods employ different feature extraction and classification techniques. As shown in Figure 3, our experimental model outperforms other models across all metrics, demonstrating its strong generalization capabilities across various encryption scenarios.

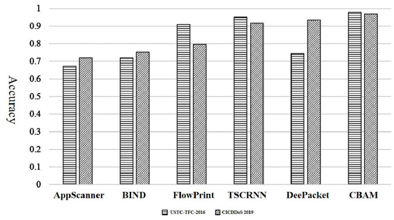

Figure 3 – Accuracy of different models

IV. Conclusion

The CNN-BiLSTM-Attention model uses self-attention to extract global network flow information and LSTM to embed packets, addressing the temporal limitations of attention mechanisms. This design enhances the model's ability to capture packet relationships and temporal information, yielding more stable and comprehensive features and improving classification accuracy. Future work will focus on increasing CNN-BiLSTM-Attention's classification speed and efficiency, adding more network flow statistical features, and exploring model interpretability.

V. References

1. Chen G., Su J., Abnormal Traffic Detection Algorithm Based on Deep Neural Network[J]. Netinfo Security, 2019, 19(6): 68–75. DOI: 10.3969/j.issn.1671-1122.2019.06.0068-08.
2. Li Qiang, Yan Cheng-hua, Zhu Yao. Analysis and Detection of Network Traffic Anomaly Based on Decision Tree // Computer Engineering. – 2012. – Vol. 38, No. 5. – P. 92–95. DOI: 10.3969/j.issn.1000-3428.2012.05.027.
3. Sun H., Wang J., Wang P., An Y. L., et al. Network Intrusion Detection Method Based on Attention-BiTCN[J]. Netinfo Security, 2024, 24(2): 309–318.
4. Lin Weining, Chen Mingzhi, Zhan Yunqing, Liu Chuanbao. Research on an Intrusion Detection Algorithm Based on PCA and Random Forest Classification // Information Security. – 2017. – No. 11. – P. 50–55. DOI: 10.3969/j.issn.1671-1122.2017.11.005.
5. PNess S., Eswarakrishnan V., Sridharan H., Shinde V., Janapareddy N.V.P., Dhanawat V. Anomaly Detection in Network Traffic Using Advanced Machine Learning Techniques [J]. IEEE Access, 2025, 13: 16133–16149. DOI: 10.1109/ACCESS.2025.3526988.
6. Moore A. W., Zieve D. Internet Traffic Classification using Bayesian Analysis Techniques[J]. Published in 2005.