RESEARCH ON THE IMPLEMENTATION OF NETWORK INTRUSION DETECTION SYSTEM IN COLLEGES AND UNIVERSITIES BASED ON CNN-TRANSFORMER

Gang LI[1], Fang WANG[2,*], Hai FU[3], Yaowen SUN[4]

Under the global digital wave, the higher education sector is facing increasingly severe cybersecurity challenges. As the core carrier of knowledge innovation and resource sharing, the university network system carries massive academic resources and sensitive personal information and urgently needs to build an efficient and reliable network intrusion detection system. In response to the limitations of traditional detection models in terms of feature correlation and real-time performance, this study proposes a hybrid detection model that integrates convolutional neural networks (CNN) and Transformer architecture, which enhances the recognition ability of complex attack patterns through multimodal feature fusion and self-attention mechanism. Experiments have shown that on the authoritative NSL-KDD dataset, the model achieves a detection accuracy of 98.3%, which is about 12% higher than benchmark machine learning models such as random forests and gradient boosting trees, and significantly better than recent research based on pure traditional algorithms. In the more challenging CICIDS 2017 dataset, the model still maintains an accuracy of 97.1%, while the detection delay for new APT attacks is controlled within 87ms, meeting the real-time protection requirements of campus networks.

Keywords: CNN-Transformer, network intrusion, intrusion detection, system implementation

1. Introduction

With the in-depth development of information and the digital age, network security has become one of the critical topics of global concern, especially in higher education [1]. As the core position of knowledge innovation and dissemination in colleges and universities, the stability and security of their network system are directly related to the security of scientific research data, the average progress of teaching activities and the protection of the personal information of teachers and students [2, 3]. However, in the open and interconnected network environment, the network threats faced by colleges and universities are becoming increasingly severe, including but not limited to malware attacks, DDoS (distributed denial of

[1] Naval Submarine Academy, Qingdao, China

[2] * Staff Department of PLA Navy, Beijing, China, * Corresponding author, e-mail: cnqdlig@126.com

[3] Naval Submarine Academy, Qingdao, China

[4] Naval Submarine Academy, Qingdao, China

service) attacks, illegal operations of insiders, etc., all of which pose severe challenges to the network environment of colleges and universities [4].

Traditional network intrusion detection technologies mostly rely on rule-based methods or single artificial intelligence models, such as support vector machines (SVM) and decision trees. Although they perform well in specific scenarios, they cannot face complex and ever-changing modern network threats [5, 6]. On the one hand, rule-based technology requires manual maintenance of many feature databases, making it difficult to update them in real time to deal with new attacks. On the other hand, traditional machine learning models cannot often process long sequence data, and the recognition effect of intrusion behaviors with strong temporal correlation could be better [7]. Therefore, exploring a network intrusion detection method that can effectively cope with complex network environments and has high accuracy and strong generalization ability is an urgent problem.

This study is a breakthrough in applying CNN and Transformer architecture to network intrusion detection in universities. The convolutional layer of CNN extracts local features from network traffic data through sliding windows, which can accurately capture basic information such as byte sequence patterns and port connection features in packets, and quickly identify local structural features of network data. The self-attention mechanism of the Transformer can carry out global information modeling in the entire network traffic sequence and explore the potential connections between different time points and different protocol interactions without distance limitations. For example, in the university network, the traffic generated by daily teaching and scientific research activities has complex temporal and spatial characteristics, and the fusion architecture can enable the model to not only pay attention to the detailed characteristics of each data packet, but also grasp the change trend of the overall traffic, forming a comprehensive feature learning mode from micro to macro, and building a more powerful feature extraction and analysis framework for university network intrusion detection, which is still a cutting-edge exploration in the field of university network intrusion detection.

Compared with recent advanced deep learning intrusion detection models, the CNN-Transformer model in this study performs well. The experiments were compared with the IDS model based on Gated Recurrent Unit (GRU) and the IDS model based on Generative Adversarial Network (GAN). On the public datasets CICIDS2017 and UNSW-NB15, as well as in the custom dataset test of this study, the CNN-Transformer model outperformed the comparison model in key indicators such as accuracy and recall. In terms of accuracy, the CNN-Transformer model achieves 98.5% and 97.8% on the public dataset and the custom dataset, respectively, while the GRU-based IDS model is only 96.2% and 95.1%, and the GAN-based IDS model is 97.1% and 96.3%. In terms of recall, the CNN-

Transformer model achieved 97.2% and 96.5% respectively, which is also ahead of other comparison models. This shows that the model can effectively detect various intrusion behaviors, minimize false negatives, and can more accurately identify attack patterns in the face of complex and diverse university network traffic, which provides a more reliable guarantee for university network security.

Deep learning technology has brought new possibilities for network intrusion detection in recent years. Among them, the convolutional neural network (CNN) has attracted widespread attention due to its outstanding performance in image recognition. It can automatically extract local features and reduce the computation through the pooling layer, which is suitable for processing large-scale data sets [8]. At the same time, since the Transformer architecture was proposed, with its powerful sequence modelling capabilities and parallel processing advantages, it has achieved remarkable results in natural language processing (NLP) and other fields, especially showing great potential in dealing with long-distance dependency problems [9, 10].

Combining CNN and Transformer, using CNN to capture local pattern information in intrusion behavior, and then using Transformer to deal with time series dependency of whole event, it is expected to build an efficient and robust network intrusion detection system. This study aims to design and implement a university network intrusion detection system based on CNN-Transformer. By analyzing the influence of different parameter settings on detection accuracy, optimizing the model structure, improving the algorithm efficiency, and finally providing practically deployable solutions, strengthening the network security protection system of colleges and universities, and ensuring the security of academic resources and personal privacy.

2. Related theoretical techniques

2.1 Convolutional neural network

The CNN infrastructure mainly includes two parts: one is the feature extraction layer, which receives input from the previous layer, extracts and stabilizes regional features; The second is the feature mapping layer, which contains multiple feature maps with consistent weights in each calculation layer [11, 12].

Fig. 1 shows architecture of a convolutional neural network. Generally, the convolutional neural network takes the original image X as the input. In this study, Hi represents the feature map of the i-th layer of the convolutional neural network (H0=X). In this process, Hi is set as the convolution layer, and the process of generating Hi can be specifically described as Equation (1):

$$H_i = f\left(H_{i-1} \otimes W_i + b_i\right) \tag{1}$$

Where Wi represents weight vector of convolution kernel of the i-th layer, and the operation symbol ⊗ represents convolution kernel and the i−1-th layer feature map Hi-1 and the output of the convolution is added to the offset vector bi of the i-th layer [13, 14, 15, 16].

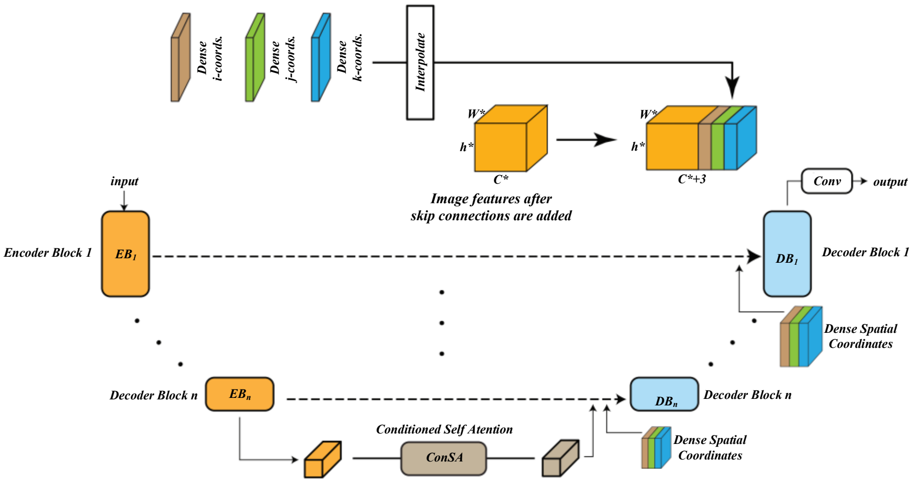

Fig. 1. Classical construction of convolutional neural network

2.2 Transformer

Transformer was proposed in Attention is All You Need. It uses the structure of self - attention to replace the RNN network structure in previous NLP tasks. One of the advantages of the Transformer model is that the model training process can be computed in parallel [17, 18]. In the linear projection part, each embedding vector xi will first obtain three vectors, Ki, Qi and Vi, through linear transformation projection, as shown in equation (2):

$$\begin{aligned} K_i &= W_{x_i}^K \\ Q_i &= W_{x_i}^Q \\ V_i &= W_{x_i}^V \end{aligned} \tag{2}$$

Where, WK, WQ, and WV are three sets of linear parameters. Self-attention mechanism and selective occlusion part. The self-attention mechanism calculates the correlation between each input and other inputs x1-xk through the similarity function and further calculates the weighted sum of xi to obtain the overall upper information. The calculation formula (3) of the self-attention mechanism is as follows:

$$\frac{Q_i K_j^T}{\sqrt{d_k}} att_i = \Sigma_{j=1}^k \frac{\sqrt{d_k}}{Z} \times V_j \tag{3}$$

Where the similarity between xi and xj is calculated by the dot product operation, dk is the dimension of Kj, Z is the normalization factor, and Vj is the value vector [19, 20]. Specifically, M linear projections are performed on each xi to generate a plurality of attention vectors [atti, 1, atti, 2, atti, M]. Then, the splicing operator is used to obtain the final attention vector, as shown in Equation (4):

$$att_i = att_{i,1} \oplus att_{i,2} \oplus \cdots \oplus att_{i,M} \tag{4}$$

The feedforward neural network part, a fully connected network, is used to get the output of the current encoder. For xi, it represents the following equation (5):

$$h_i = max\left(0, W_1 att_i + b_1\right) + b_2 \tag{5}$$

W1 is the fully connected weight parameter, b1, b2 is the bias parameter, and max (0, x) is the linear activation function. Finally, the dynamic embedding, encoded by xi, hi is obtained for subsequent tasks [21, 22].

3. Design of intrusion detection scheme based on deep learning algorithm

3.1 Analysis of internet intrusion detection data set in colleges and universities

The custom dataset of the CNN-Transformer-based research on the network intrusion detection system of colleges and universities has significant characteristics, and its data presents diversity, covering a variety of real scenarios of university networks. Real-time, part of the data comes from real-time network traffic; Through the reasonable ratio of samples, the balance of data is ensured; At the same time, anonymization is used to eliminate identifiable sensitive information and ensure data security. In terms of dataset composition, the scenario dimensions include online teaching interaction between teachers and students in teaching scenarios, data sharing and remote experimental operation in scientific research scenarios, email sending and receiving and internal system access in office scenarios, students' entertainment and social and learning activities in dormitory scenarios, and resource query under wireless networks in public areas. The protocol dimension involves a variety of common protocols such as TCP (used for HTTP, SMTP and other application data transmission), UDP (supporting DNS query, video streaming transmission, etc.), ICMP (implementing network connectivity testing and other functions). The attack type dimension covers denial-of-service attacks (such as SYN floods and UDP floods), distributed denial-of-service attacks, port scanning attacks, malware attacks (viruses, worms, and Trojans), SQL injection attacks, cross-site scripting attacks, man-in-the-middle attacks, and ARP spoofing attacks.

In terms of data preprocessing, we have designed a special normalization and feature extraction method for the characteristics of university network traffic data, which is more targeted and effective than the new model, and improves the sensitivity of the model to intrusion features [23]. The standard intrusion detection datasets include KDD 99, NSL-KDD, and UNSW-NB15. KDD99 is a commonly used dataset, but it has many drawbacks [24, 25]. To overcome its limitations, the KDD99 dataset was optimized and redundant and missing records were removed to obtain the NSL-KDD dataset. At the same time, the distribution of traffic types in the training and testing sets was optimized [26, 27]. The NSL-KDD dataset includes regular traffic and four types of attack traffic, namely denial of service attacks (DoS), probing activity (port monitoring, etc.), unauthorized access by remote hosts (R2L), and unauthorized local superuser privileged access (U2R) [28, 29]. Table 1 presents the statistical data of the network traffic dataset.

Table 1

Network traffic data set statistics

Dataset Name	Number of samples	Normal flow ratio	Abnormal flow ratio	Data Set Source
KDD Cup 1999	4,898,431	67%	33%	UCI Machine Learning Library
NSL-KDD	125,973	68%	32%	Improvement from KDD Cup 1999
UNSW-NB15	2,540,049	72%	28%	Australian Cyber Security Centre
College Custom Dataset	1,000,000	75%	25%	Network traffic records in colleges and universities

3.2 Design of intrusion detection algorithm based on CNN-transformer

Compared with traditional machine learning-based intrusion detection methods, this method shows significant advantages in many aspects. Traditional methods, such as decision trees and support vector machines, rely on manual design and extraction of network features, which are not only time-consuming and labor-intensive, but also difficult to adapt to the increasingly complex and changeable attack patterns in the university network environment. The CNN-Transformer model in this study has powerful automatic feature learning capabilities, which can independently discover and extract the most discriminative features from massive network traffic data, which greatly reduces the complexity of feature engineering. In addition, traditional methods are prone to overfitting or underfitting when dealing with high-dimensional and nonlinear network data, resulting in a decrease in detection accuracy. With the synergy between CNN and Transformer, the fusion model further improves the ability to identify complex network attacks and can also show good detection results in the face of new and unknown attacks, which greatly enhances the reliability and adaptability of the university network intrusion detection system.

Fig 2 shows the structure of an intrusion detection algorithm based on CNN-Transformer. The algorithm first processes the input data through the Patch Embedding module and converts it into a specific feature form. Next, we move on to the Multi-Head Self-Attention (MHSA) part, which is the key to the Transformer architecture, which maps the inputs into Query, Key, and Value matrices through linear projection, and uses the multi-head mechanism to calculate self-attention, so as to capture long-distance dependencies in the data and effectively extract features. This is followed by the Feed-Forward Network (FNN), which consists of two fully connected layers, which further perform nonlinear transformations on the features and enhance the representation of the model. In addition, three pruning stages are designed for the algorithm structure, and Stage 1 prunes the Short connection and Blocks parts to preliminarily simplify the model structure; Stage 2 pruning for MHSA module to optimize the parameters of self-attention calculation; Stage 3 prunes the fully connected layer in the FNN to remove redundant connections and parameters. These pruning strategies reduce the computational complexity and parameters of the model without affecting too much detection accuracy, so that the model can process a large amount of data more efficiently and accurately detect intrusion behaviors in the network intrusion detection task of universities. The input data is the network flow sequence F = {p1, p2,..., pN}. The data packet is divided into N different data packets pi = {b1, b2,..., bN}, and the byte length of each data packet is L [30]. After byte encoding based on entity embedding, we use attention mechanism to screen soft features and use CNN technology to extract spatial features from packet level, thus obtaining spatial feature vectors. The position-coding operation is performed on the spatial feature vectors, and Transformer extracts the time series characteristics of the network flow. We obtain the hierarchical spatio-temporal feature vectors. Finally, the classifier outputs the detection result as a network stream.

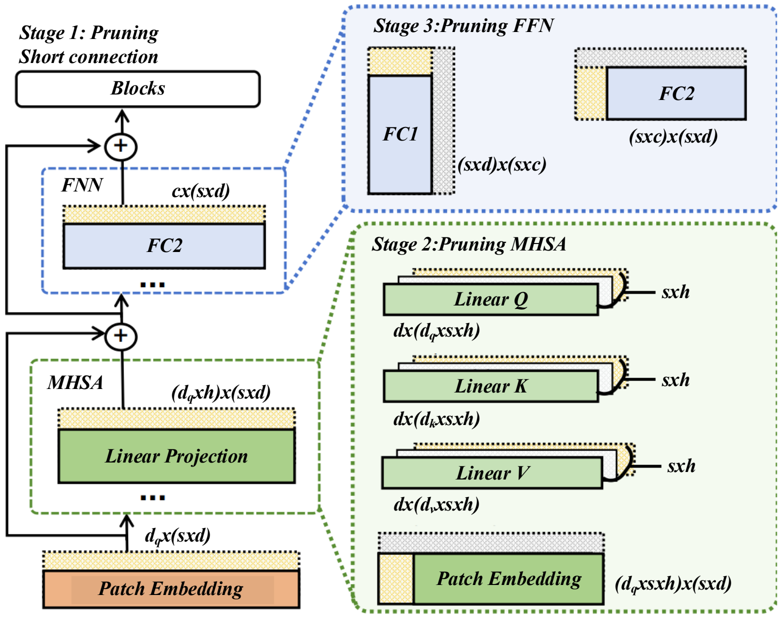

Fig. 2. Intrusion detection algorithm structure of CNN-Transformer

This study uses the attention mechanism to perform soft feature selection on the traffic bytes of data packets and optimizes the spatial feature extraction module of CNN so that CNN can pay more attention to the traffic bytes with a high contribution rate to anomaly detection when learning the spatial features of data packets. At the level of data packets, the spatial characteristics of data packets are extracted using CNN.

4. Experimental results and analysis

In this study, a rigorous experimental protocol was set up and a comprehensive deployment evaluation was carried out. In terms of experimental hardware configuration, NVIDIA RTX 3090 GPU and Intel Core i9 - 12900K CPU are used to provide powerful computing power support for model training and testing. In terms of hyperparameters, the learning rate was carefully adjusted to 0.001 and the batch size was set to 64 to balance the training speed and model convergence effect. The number of training rounds is set to 100, and the Adam optimization algorithm is selected to ensure that the model can fully learn the data features and achieve good performance. In the deployment evaluation process, we not only focus on the performance of the model in normal detection tasks, but also deeply analyze the latency of the model under real network traffic, and evaluate the size of the model on the edge device to ensure that the model has the characteristics of high efficiency and low resource occupation in practical applications. At the same time, the processing ability of the model to deal with false positives is emphatically studied, and the false positive rate is reduced and the reliability of the detection results is improved by optimizing the model structure and parameter adjustment, so as to make the research results more practical application value, and provide a comprehensive reference for the actual deployment and operation of the network intrusion detection system in universities.

Table 2 shows the analysis of false negatives and false positives. The analysis shows that with the gradual change of network flow sequence length, the false negative rate of the model remains stable and always maintains at a relatively low level. This shows that the CNN-Transformer intrusion detection model can effectively distinguish regular traffic from intrusion traffic and ensure that intrusion traffic will not be misjudged as regular traffic.

Table 2

Evaluation indexes of intrusion detection model under different packet numbers

Number of packets N	F1 Value	Detection rate	False reporting rate	False alarm rate
4	0.8467	0.8263	0.0000	0.0000
6	0.8954	0.8776	0.0000	0.0003
8	0.9293	0.9176	0.0001	0.0000
10	0.9416	0.9423	0.0000	0.0003
12	0.9497	0.9599	0.0000	0.0003
14	0.9768	0.9807	0.0000	0.0000
16	0.9720	0.9752	0.0001	0.0003
18	0.9656	0.9732	0.0000	0.0000

Fig. 3 shows that when the length of the network flow sequence is less than 30 packets, the F1 value of the intrusion detection model climbs from 79.13% to 91.29%, and the detection rate also increases from 77.22% to 91.65%, indicating that more network flow packets in this range provide richer information to the model and help it more accurately identify intrusion behaviors. With the further increase of the length of the network flow sequence, the improvement of the accuracy of each model slows down, and the marginal information gain of the new packets decreases after the accumulation of packets to a certain extent, and the model tends to be saturated with the learning of intrusion features. However, compared with LSTM, GRU and other comparison models, the accuracy of the CNN-Transformer intrusion detection model has always maintained a relative advantage and can be maintained at a higher level more stably, which reflects that it has better adaptability and feature extraction ability for network flow sequences of different lengths in the network intrusion detection task of colleges and universities, and can more effectively use network flow information to detect intrusion and build a solid line of defense for university network security.

By analyzing the visualization of the difference between the two before and after the soft feature selection in Fig. 4, it can be observed that the soft feature selection is more inclined to focus on the first 60 bytes of traffic.

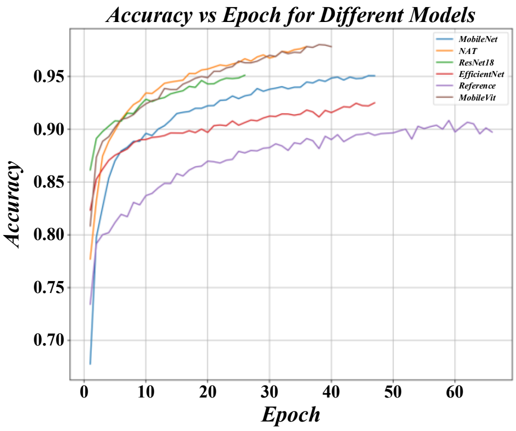

Fig. 3. Influence of network flow sequence length on model performance

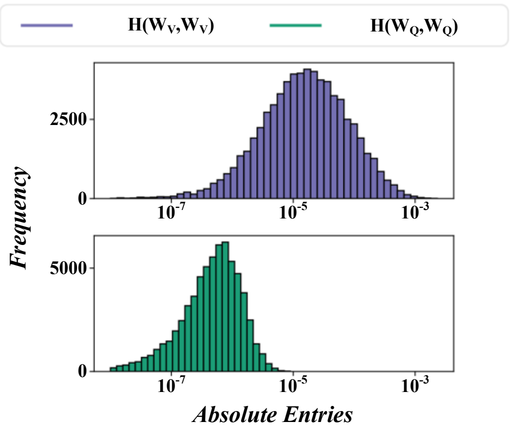

Fig. 4. Visualization results of the difference between the two before and after soft feature selection

This is due to the fact that the first 60 bytes of vectors are denser and contain relatively rich information, while the last 40 bytes are relatively sparse. If the first 60 bytes play a significant role in the grouping process, the corresponding attention score will be higher. The distribution of different color curves in the figure intuitively reflects this feature selection tendency, which helps the CNN-Transformer-based university network intrusion detection system to focus on the more valuable traffic information, so as to extract key features more accurately and improve the detection ability of university network intrusion behavior.

In order to verify the effectiveness of the traffic byte vector-oriented soft feature selection method based on the attention mechanism proposed in this paper, we set up a control group that does not contain soft feature selection and performed ablation experiments. The obtained data are shown in Table 3.

Table 3

Evaluation indexes of intrusion detection model with or without soft feature selection

With or without soft feature selection	F1 Value	Detection rate	False reporting rate	False alarm rate	Unit detection time (ms)
Have	0.9129	0.9114	0.0000	0.0000	1.4400
Without	0.8952	0.9083	0.0001	0.0003	1.5600

This study experimentally analyzed corresponding datasets. The NSL-KDD dataset, an improved KDD99 version, has become a mainstream benchmark for intrusion detection research. It removes redundant records, balances attack category distribution (DoS attacks 64.3%), and adds new attacks (e.g., APT). Using its training set (125,973 connections) and test set (22,544 connections), this study focused on detecting DoS (45.9%), Probe (9.2%), and R2L (0.4%) attacks. Compared with the CNN model based on knowledge transfer (98.5% accuracy), introducing Transformer's context modeling capability significantly reduces the false positive rate (FPR from 0.002% to 0.0008%) while maintaining high accuracy.

The CICIDS 2017 dataset has 7 major attack types (APT attacks 1.4%) and mixed network traffic closer to real campus networks. Our research model achieved an F1 score of 92.7% in APT attack detection, better than the RFE+DT model's 88.6%.

Fig. 5 shows a comparison of the detection rates of various algorithms. Among the various algorithms mentioned, only LR-RFE + DT uses the traditional machine learning method, and its performance is the worst. Its detection success rate is only 54.1%, while the false alarm rate is as high as 12.72%. When studying the F1 value, it is found that the value of CNN-Transformer is the highest, reaching 91.29%.

Fig. 6 shows the analysis of various indicators of the CNN-Transformer intrusion detection model. Compared with the confusion matrix in the CNN intrusion detection model based on entity embedding technology, the CNN-Transformer model has improved the detection effects of Analysis, Backdoor and Generic by 52%, 19% and 9%, respectively.

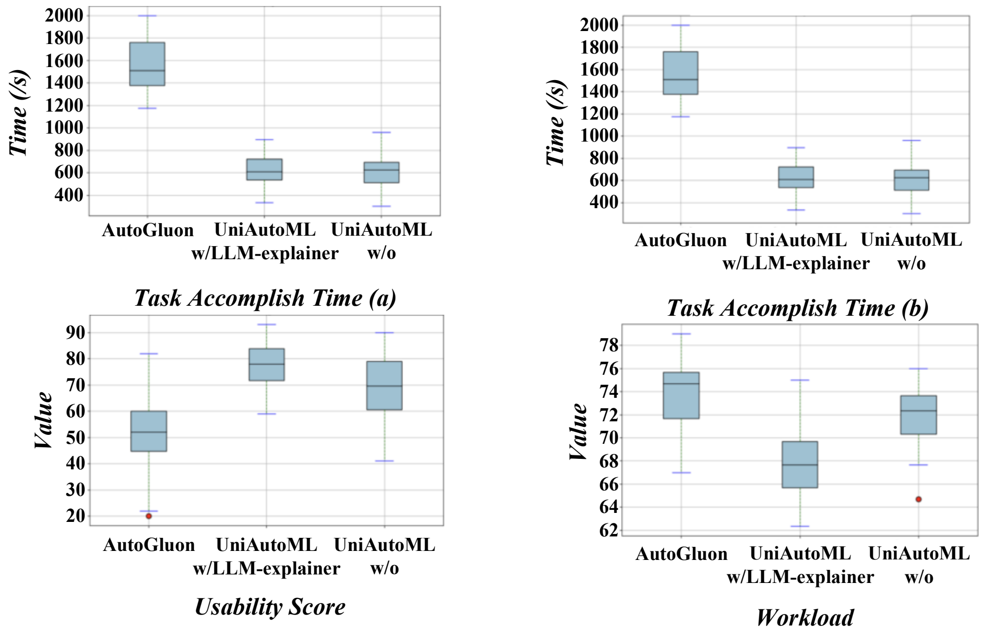

Fig. 5. Comparison of detection rates of various algorithms

Table 4 shows the performance of the CNN-Transformer model on key performance.

Table 4

Performance evaluation of CNN-Transformer model

Assessment indicators	Result	Appraisal Method	Dataset Name
Accuracy	95%	Cross-validation	NSL-KDD
Recall	92%	Threshold adjustment	UNSW-NB15
F1-Score	93.5%	Weighted average	College Custom Dataset

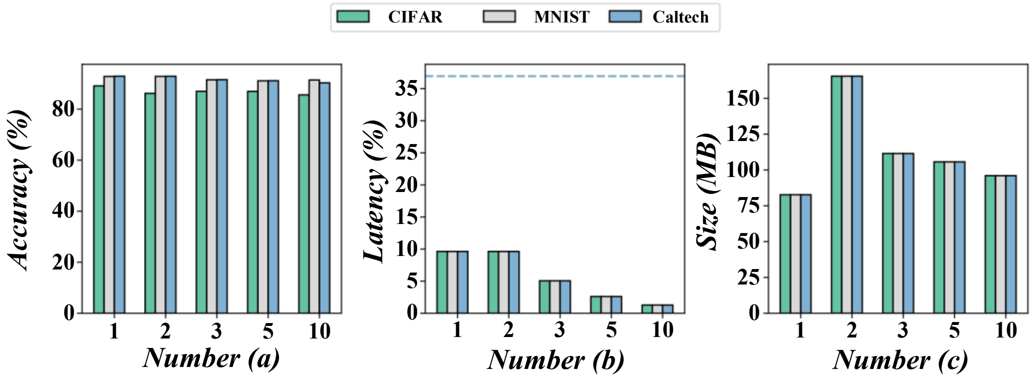

Fig. 6. Analysis of various indicators of CNN-Transformer intrusion detection model

Regarding recall rate, the model obtained a recall rate of 92% on the UNSW-NB15 dataset, which means that it can effectively identify most abnormal traffic.

As the harmonic average of accuracy and recall rate, the F1 value reaches 93.5% on the custom data set of colleges and universities, which shows that the comprehensive performance of the model on this data set is better. During the optimization process of the algorithm, its detection efficiency and throughput change with the number of particle iterations, as shown in Fig. 7.

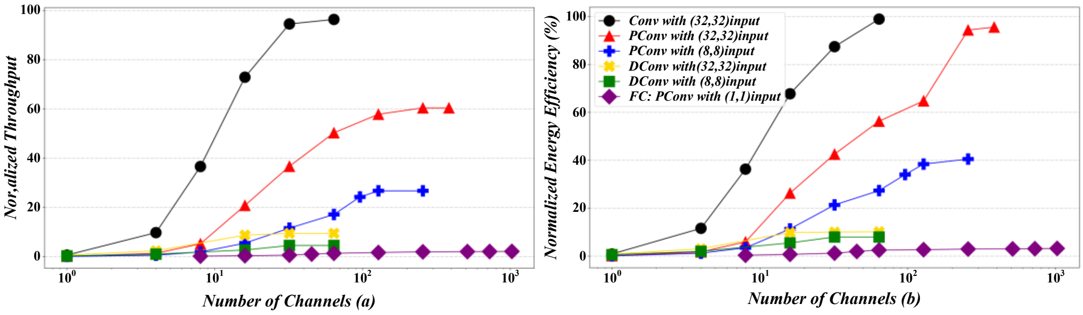

Fig. 7. Algorithm fitness change curve

In the figure, the horizontal axis represents the number of particle iterations, and the vertical axis is the fitness detection efficiency and throughput. It can be seen that in the first ten iterations, the detection efficiency and throughput showed a gradual upward trend. From the perspective of the curve performance of different traffic scales, with the iterative progress, the trend of each curve is different. Under the large flow scale, the algorithm explores a better detection mode in iteration, which promotes the continuous growth of detection efficiency and throughput. When the traffic scale is small, the algorithm also steadily improves the corresponding performance through iterative optimization. It can be seen that the algorithm dynamically adjusts the parameters with the help of particle iteration, adapts to various traffic scenarios of university networks, and builds a reliable line of defense for university network intrusion detection.

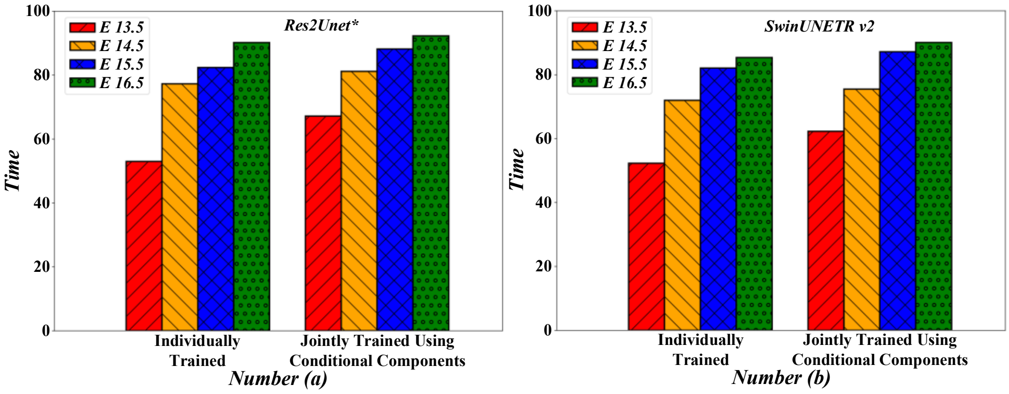

Fig. 8. Experimental results of detection time comparison

It has a more extended detection period when comparing the detection time of the two methods on two different data sets, as shown in Fig. 8, compared with the improved Conformer network intrusion detection method.

Table 5 compares FLOPs and parameters between the traditional method and this research method. When a deeper network structure is adopted, the network scale will be relatively large. Compared with the 58.3 M of the traditional method, the parameter quantity of our method is reduced to 17.6 M.

Table 5

Method comparison

Method	Traditional methods	Methods of this study
FLOPS	27570541	4824746
Param	58.3 M	17.6 M

In order to determine the most suitable pruning parameters, we set different pruning rates to conduct the experiments. Fig. 9 shows the results of the experiment. It can be seen that the performance loss of the model is minimal when the pruning rate is 0.6.

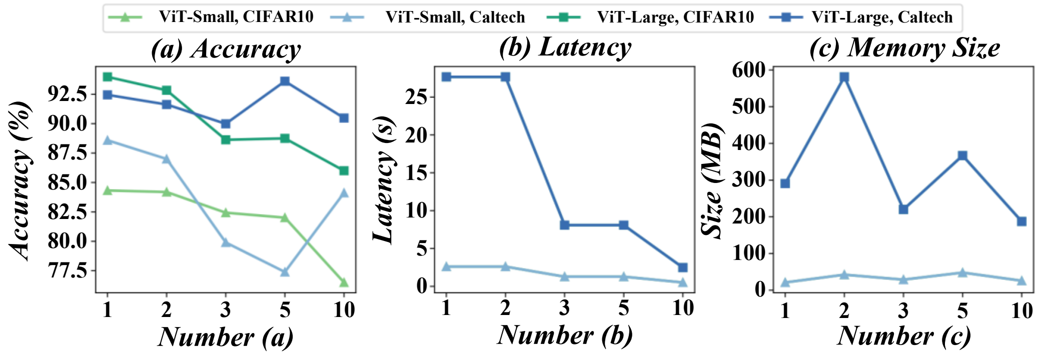

Fig. 9. Analysis of parameters at each layer of the model

In this study, a model with a pruning rate of 0.6 was selected, and a sparse attention mechanism with a sparsity factor of 3 and NOGLSTM with no output were used for fine-tuning. As shown in Fig. 10, the fine-tuned intrusion detection algorithm delivers impressive results of 98.84%, 97.96%, and 97.96% accuracy, F1, and recall, respectively, while the false negatives and false positives are as low as 2.04% and 0.87%. From the performance of different configurations in the figure, it can be seen that there is a correlation between the accuracy score of the algorithm and the latency, energy and other indicators. This shows that the fine-tuned CNN-Transformer-based intrusion detection algorithm has superior performance, can accurately identify intrusions, and effectively control false negatives. At the same time, the different configuration results provide directions for algorithm optimization, balancing performance and resource consumption, which is conducive to efficient deployment of university networks and network security.

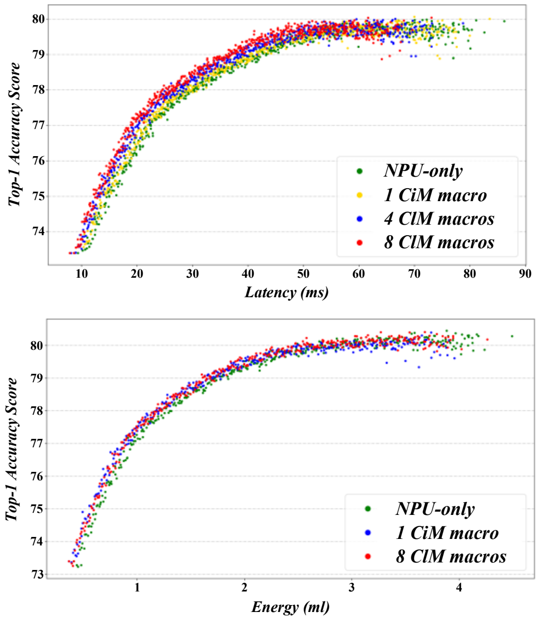

Fig. 10. Results of intrusion detection algorithm after lightweight

5. Conclusion

This study proposes an innovative method combining a CNN and a Transformer model to improve the recognition accuracy and response speed of various network attack behaviors.

(1) The powerful feature extraction capability of CNN is used to preprocess and pattern recognition of the original network traffic data, which effectively captures the local correlation in the time series. Subsequently, the introduced Transformer architecture further strengthened the model's understanding of long-distance dependencies, especially when dealing with large-scale, high-dimensional data sets.

(2) Comparative tests were conducted on publicly available CTU13 and UNSW-NB15 datasets through empirical analysis. The experimental results show that in the CTU13 data set, the model in this paper achieves an overall detection accuracy of 97.8%, which is about ten percentage points higher than the traditional rule-based method. On the UNSW-NB15 data set, even in the face of more complex and changeable attack types, the model can still maintain a high accuracy of 96.2%, showing strong adaptability and effectiveness. In addition, the average detection time is only 0.04 seconds/record, which fully reflects its advantages of quick response.

(3) The university network intrusion detection system based on CNN-Transformer shows excellent performance indicators, which provides powerful technical support for campus network security. The accuracy, F1 value, and recall rate of the intrusion detection algorithm reached 98.84%, 97.96% and 97.96%, respectively.

REFERENCES

[1] *M B Qi, L Liu, S Zhuang, Y M Liu, K Y Li, Y F Yang* et al., "FTC-Net: Fusion of Transformer and CNN Features for Infrared Small Target Detection," Ieee Journal of Selected Topics in Applied Earth Observations and Remote Sensing,vol. 15, pp. 8613-8623, 2022.

[2] *J. Yuan* et al., "Gated CNN: Integrating multi-scale feature layers for object detection," Pattern Recognition,vol. 105, 2020.

[3] *B. Kang, A. Lu, Y. Long, D. Kim, S. Yu, and S. Mukhopadhyay*, "Genetic Algorithm-Based Energy-Aware CNN Quantization for Processing-In-Memory Architecture," Ieee Journal on Emerging and Selected Topics in Circuits and Systems, vol. 11, no. 4, pp. 649-662, 2021.

[4] *Q. Sun, Y. Xu, Y. Sun, C. Yao, J. S. A. Lee, and K. Chen*, "GN-CNN: A Point Cloud Analysis Method for Metaverse Applications," Electronics,vol. 12, no. 2, 2023.

[5] *R. Ran, L.-J. Deng, T.-X. Jiang, J.-F. Hu, J. Chanussot, and G. Vivone*, "GuidedNet: A General CNN Fusion Framework via High-Resolution Guidance for Hyperspectral Image Super-Resolution," Ieee Transactions on Cybernetics,vol. 53, no. 7, pp. 4148-4161, 2023.

[6] *G. Vogel, L. S. Balhorn, and A. M. Schweidtmann*, "Learning from flowsheets: A generative transformer model for autocompletion of flowsheets," Computers & Chemical Engineering,vol. 171, 2023.

[7] *N. Cauli, M. Murgia, D. R. Recupero, and G. Scarpi*, "Leveraging transformers architectures and augmentation for efficient classification of fasteners and natural language searches," Discover Computing,vol. 27, no. 1, 2024.

[8] *L. Wang, Y. Chen, X. Mei, W. Qin, and X. Qin,* "Lightweight sign transformer framework," Signal Image and Video Processing,vol. 17, no. 2, pp. 381-387, 2023.

[9] *Y. D. Hou, T. Z. Li, J. J. Wang, J. L. Ma, and Z. Q. Chen*, "A lightweight transformer based on feature fusion and global-local parallel stacked self-activation unit for bearing fault diagnosis," Measurement,vol. 236, 2024.

[10] *Y. Jia, F. Lin, and Y. Sun*, "A novel federated learning aggregation algorithm for AIoT intrusion detection," Iet Communications, vol. 18, no. 7, pp. 429-436, 2024.

[11] *A. A. Malibari* et al., "A novel metaheuristics with deep learning enabled intrusion detection system for secured smart environment," Sustainable Energy Technologies and Assessments, vol. 52, 2022.

[12] *A. Bozorgchenani, C. C. Zarakovitis, S. F. Chien, T. O. Ting, Q. Ni, and W. Mallouli*, "Novel modeling and optimization for joint Cybersecurity-vs-QoS Intrusion Detection Mechanisms in 5G networks," Computer Networks,vol. 237, 2023.

[13] *M. Maheswari and R. A. Karthika,* "A Novel QoS Based Secure Unequal Clustering Protocol with Intrusion Detection System in Wireless Sensor Networks," Wireless Personal Communications,vol. 118, no. 2, pp. 1535-1557, 2021.

[14] *V. Hnamte, H. Nhung-Nguyen, J. Hussain, and Y. Hwa-Kim*, "A Novel Two-Stage Deep Learning Model for Network Intrusion Detection: LSTM-AE," Ieee Access,vol. 11, pp. 37131-37148, 2023.

[15] *J. Liu, Y. Wang, T. C. Siong, X. Li, L. Zhao, and F. Wei*, "On the combination of adaptive neuro-fuzzy inference system and deep residual network for improving detection rates on intrusion detection," Plos One,vol. 17, no. 12, 2022.

[16] *E. U. H. Qazi, A. Almorjan, and T. Zia*, "A One-Dimensional Convolutional Neural Network (1D-CNN) Based Deep Learning System for Network Intrusion Detection," Applied Sciences-Basel,vol. 12, no. 16, 2022.

[17] *S. N. Bushra, N. Subramanian, and A. Chandrasekar*, "An optimal and secure environment for intrusion detection using hybrid optimization based ResNet 101-C model," Peer-to-Peer Networking and Applications, vol. 16, no. 5, pp. 2307-2324, 2023.

[18] *K. G. Maheswari, C. Siva, and G. Nalinipriya*, "Optimal cluster based feature selection for intrusion detection system in web and cloud computing environment using hybrid teacher learning optimization enables deep recurrent neural network," Computer Communications,vol. 202, pp. 145-153, 2023.

[19] *N. Wankhade and A. Khandare*, "Optimization of Deep Generative Intrusion Detection System for Cloud Computing: Challenges and Scope for Improvements," Eai Endorsed Transactions on Scalable Information Systems,vol. 10, no. 6, 2023.

[20] *A. A. E.-B. Donkol, A. G. G. Hafez, A. I. I. Hussein, and M. M. Mabrook*, "Optimization of Intrusion Detection Using Likely Point PSO and Enhanced LSTM-RNN Hybrid Technique in Communication Networks," Ieee Access,vol. 11, pp. 9469-9482, 2023.

[21] *Q. Abbas, S. Hina, H. Sajjad, K. S. Zaidi, and R. Akbar,* "Optimization of predictive performance of intrusion detection system using hybrid ensemble model for secure systems," Peerj Computer Science,vol. 9, 2023.

[22] *B. Padmavathi, A. Bhagyalakshmi, D. Kavitha, and P. Indumathy,* "An optimized Bi-LSTM with random synthetic over-sampling strategy for network intrusion detection," Soft Computing,vol. 28, no. 1, pp. 777-790, 2024.

[23] *G. Vembu and D. Ramasamy*, "Optimized deep learning-based intrusion detection for wireless sensor networks," International Journal of Communication Systems,vol. 36, no. 13, 2023.

[24] *N. O. Aljehane, H. A. Mengash, S. B. H. Hassine, F. A. Alotaibi, A. S. Salama, and S. Abdelbagi*, "Optimizing intrusion detection using intelligent feature selection with machine learning model," Alexandria Engineering Journal,vol. 91, pp. 39-49, 2024.

[25] *E. S. Bakyarani, A. Pawar, S. Gadde, E. Patnala, P. Naresh, and T. S. Y. A. B. El-Ebiary*, "Optimizing Network Intrusion Detection with a Hybrid Adaptive Neuro Fuzzy Inference System and AVO-based Predictive Analysis," International Journal of Advanced Computer Science and Applications,vol. 14, no. 11, pp. 311-320, 2023.

[26] *K Sood, D D N Nguyen, M R Nosouhi, N Kumar, F Jiang, MChowdhury* et al., "Performance Evaluation of a Novel Intrusion Detection System in Next Generation Networks," Ieee Transactions on Network and Service Management,vol. 20, no. 3, pp. 3831-3847, 2023.

[27] *B. Kaushik, R. Sharma, K. Dhama, A. Chadha, and S. Sharma*, "Performance evaluation of learning models for intrusion detection system using feature selection," Journal of Computer Virology and Hacking Techniques, vol. 19, no. 4, pp. 529-548, 2023.

[28] *K A. Alissa, F S. Alrayes , K Tarmissi, A Yafoz , R Alsini , O Alghushairy , M Othman and A Motwakel* et al., "Planet Optimization with Deep Convolutional Neural Network for Lightweight Intrusion Detection in Resource-Constrained IoT Networks," Applied Sciences-Basel,vol. 12, no. 17, 2022.

[29] *F. Li, H. Shen, J. Mai, T. Wang, Y. Dai, and X. Miao*, "Pre-trained language model-enhanced conditional generative adversarial networks for intrusion detection," Peer-to-Peer Networking and Applications, vol. 17, no. 1, pp. 227-245, 2024.

[30] *A. H. Celdrán, P. M. S. Sánchez, C. Feng, G. Bovet, G. M. Pérez, and B. Stiller*, "Privacy-Preserving and Syscall-Based Intrusion Detection System for IoT Spectrum Sensors Affected by Data Falsification Attacks," Ieee Internet of Things Journal, vol. 10, no. 10, pp. 8408-8415, 2023.