IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 19 September 2023, accepted 11 November 2023, date of publication 20 November 2023,
date of current version 8 December 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3334916

RESEARCH ARTICLE

CNN-AttBiLSTM Mechanism: A DDoS Attack Detection Method Based on Attention Mechanism and CNN-BiLSTM

JUNJIE ZHAO[1,2], YONGMIN LIU[1,2], (Member, IEEE), QIANLEI ZHANG[1,2], AND XINYING ZHENG[3]

[1]School of Computer and Information, Central South University of Forestry and Technology, Changsha 410000, China
[2]Research Center of Smart Forestry Cloud, Central South University of Forestry and Technology, Changsha 410000, China
[3]Business School, Hunan Normal University, Changsha 410000, China

Corresponding author: Yongmin Liu (T20040550@csuft.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 31870532, and the Natural Science Foundation of Hunan Province under Grant 2021JJ31163.

This work involved human subjects or animals in its research. The authors confirm that all human/animal subject research procedures and protocols are exempt from review board approval.

ABSTRACT DDoS attacks occur frequently. This paper proposes a DDoS attack detection method that combines self attention mechanism with CNN-BiLSTM to address the issues of high dimensionality, multiple feature dimensions, low classification task accuracy, and high false positive rate in raw traffic data. Firstly, the random forest algorithm is combined with Pearson correlation analysis to select important features as model inputs to reduce the redundancy of input data. Secondly, one-dimensional convolutional neural networks and bidirectional long-term and short-term memory networks are used to extract spatial and temporal features respectively, and then the extracted features are ''parallelized'' to obtain fused features. Once again, an attention mechanism is introduced to ensure that useful input information features are fully and completely expressed, and different weights are given based on the importance of different features. Finally, the softmax classifier is used to obtain the classification results. To verify the effectiveness of the proposed method, binary and multi classification experiments were conducted on the CIC-ISD2017 and CIC-DDoS2019 datasets. The experimental results show that compared with existing models, the proposed model has the highest accuracy, precision, recall, and F1 values of 95.670%, 95.824%, 95.904%, and 95.864%, respectively.

INDEX TERMS DDoS attacks, convolutional neural network, long short-term memory network, self-attention mechanism, feature selection.

I. INTRODUCTION

DDoS (Distributed Denial of Service) attacks are extremely difficult to defend against and can seriously damage the money, services, and reputation of the victim. According to Huawei's Special Report on Botnets and DDoS Attacks released in 2013 [1], frequent DDoS attacks cause significant economic losses to governments and enterprises, with more than 65% of DDoS attacks causing losses of up to ten thousand dollars per hour.

As network technology continues to update, the number, frequency, sophistication, and impact of DDoS attacks are increasing dramatically, making it particularly difficult to detect how they are attacked, making it more difficult to distinguish between normal traffic and DDoS attack traffic.

Therefore, DDoS attack detection aimed at distinguishing between normal traffic and attack traffic has been paid attention to and deeply studied by scholars both domestically and internationally. Its research methods can be divided into:

The associate editor coordinating the review of this manuscript and approving it for publication was Tyson Brooks.

statistical learning based, machine learning based, and deep learning based.

With regard to the application of statistical learning in DDoS attack detection, Yu et al. [2] proposed a detection model based on the random forest method. This method marks DDoS attacks by calculating the information entropy of the source and destination IP addresses and the source and destination port addresses in the data, and uses the random forest model to increase the stability of the fitting degree to establish the detection model; Zheng et al. [3] proposed to use the adaptive method to analyze and find the attacker to detect the attack traffic; Behal et al. [4] detect attacks based on the amount of data and information distance received within the specified time window. At the same time, machine learning has achieved better detection accuracy and lower false alarm rate. Diro and Chilamkurti [5] proposed that all nodes in the distributed environment will deploy the model, and parameter information can be shared and optimized between nodes, which will speed up the whole training process. Ye et al. [6] proposed to use SVM to classify feature vectors in SDN networks. These feature vectors are composed of source IP, source port and other information in network data, and finally achieve the function of DDoS attack detection. Koay et al. [7] use information entropy to construct features to detect slow DDoS attacks, and use multiple classifiers to classify and evaluate the comprehensive results.

In recent years, with the development of deep learning and big data, more and more scholars have studied the use of deep learning methods to detect DDoS attacks. Deep learning is to analyze and learn the internal laws from massive data, build a network model through multi-layer neurons or perception mechanism, and train the model. The deep learning method can process high-dimensional data and also solve the problem of data noise to make up for the lack of machine learning. The method proposed by Oena [8] is to analyze the attack behavior, combine CNN and LSTM to form the CNN-LSTM3 model, and use gradient descent algorithm to update the weight in the back propagation process; Wang et al. [9] proposed an intrusion detection system based on layered spatiotemporal features (HAST-IDS). First, the deep convolutional neural network (CNN) was used to learn the low-level spatial features of network traffic, and then the short-term and short-term memory network was used to learn the high-level temporal features. The experimental results show that the performance of the proposed model is superior to other in-depth learning methods; Cheng et al. [10] proposed a DDoS attack detection method based on the gray scale matrix feature of network flow of convolutional neural network. According to the different characteristics of attack flow and normal flow in IP protocol, a 7-tuple is defined to describe the characteristics of network flow, and the binary is converted into gray scale features, and multi-scale convolutional neural network model is used for feature extraction training.

In summary, the current research hotspots of DDoS attack detection technology are mainly divided into two aspects: feature selection [11], [12], [13], [14] and optimization of training algorithms: (1) The original dataset has the problem of feature redundancy. High data feature dimensionality not only increases model training time, but also reduces model performance. How to filter out key information from massive network data to effectively improve detection efficiency is crucial. (2) The detection efficiency of the attack detection model is low. It is precisely because of the large number of feature dimensions in the original traffic data that the information obtained by a single model is not comprehensive, such as CNN-based training does not consider the sequence characteristics of network traffic, LSTM-based algorithms do not consider the spatial characteristics of data, and the one-sidedness of the single model detection function leads to the low performance of the above model.

In order to solve the above problems, this paper designs a new DDoS attack detection method based on CNN-BiLSTM, that is, a fusion convolutional neural network and two-way long short-term memory network introduction attention mechanism are used to construct a new DDoS attack detection model. Its specific contributions are as follows:

- Aiming at the feature redundancy problem caused by the high dimension of the dataset, this paper proposes a new feature selection algorithm (REP algorithm), which introduces a random forest algorithm to calculate the feature importance, and combines the Pearson correlation coefficient analysis to perform feature selection.
- For DDoS attack detection, the one-dimensional convolutional neural network model and the bidirectional short-term and short-term memory network model are combined in parallel. At the same time, the spatial and temporal characteristics of the input data are extracted respectively, and the data characteristics are comprehensively and effectively learned.
- In order to improve the classification accuracy and detection efficiency, after fusing the features extracted from the two, the attention mechanism is used to assign corresponding weights to the input features according to their different importance, and the calculation is carried out. The classification results are obtained through softmax classifier.

The rest of paper is organized as follows. Section II summarizes the related work. Section III proposes an improved network intrusion discovery method. Section IV introduces the dataset and all evaluation metrics, and shows the results of the experiment. Finally, Section V concludes the paper.

II. RELATED WORK

A. A CNN-BASED DDoS ATTACK DETECTION METHOD

In the field of network anomaly detection, CNN models have better characteristics than other machine learning methods in obtaining local features and processing data with statistical smoothness and local correlation. In addition, two-dimensional CNNs are mainly effective for two-dimensional images, while one-dimensional CNNs learn features on time series datasets by serializing TCP/IP packets within

a predetermined time range, so as to perform efficient classification. Therefore, this paper uses a one-dimensional CNN to process the input data for the sequence data of network traffic.

The CNN model usually consists of five parts: input layer, convolutional layer, pooling layer, fully connected layer and output layer. The schematic framework of CNN-based DDoS attack detection is shown in Figure 1.

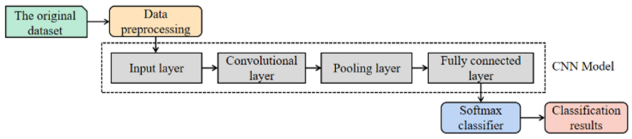

FIGURE 1. Framework diagram of DDoS attack detection system based on CNN.

B. A DDoS ATTACK DETECTION METHOD BASED ON LSTM

RNNs are good at processing sequence data, but they are prone to gradient vanishment, gradient explosion and long-term dependence during the training process, and the long short-term memory module in the LSTM model can solve the long-term dependence problem caused by RNNs. The Long Short-Term Memory Module is an addition of 3 gates (forgetting gate, input gate, output gate) and 1 cell state update to the hidden layer in the RNN model, as shown in Figure 2.

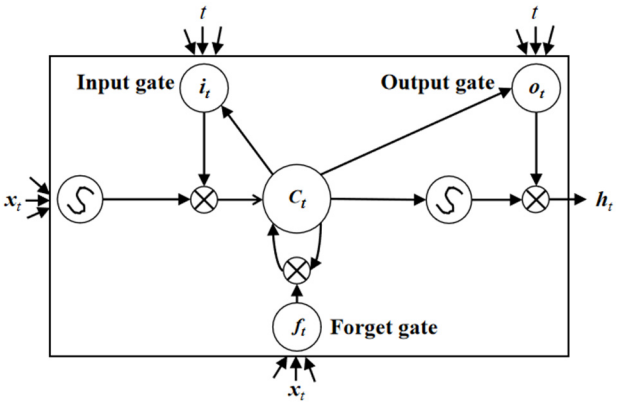

FIGURE 2. LSTM cycle structure.

The forgetting gate screens the state of the previous layer of cells, leaving useful information and forgetting useless information, calculated as follows:

$$f_t = \sigma(w_f \cdot [h_t - 1, x_t] + b_f) \tag{1}$$

wherein, w_f and b_f are respectively the weight matrix and bias term of the forgetting gate, and h_{t-1} is the output value of the upper layer LSTM, σ Activate the function for sigmoid, [,] means to connect two vectors into one vector.

The input gate judges the importance of the information, sends the important information to the cell status update, and completes the cell status update. This process consists of two parts. In the first part, sigmoid function is used to determine the new information to be added to the cell state. In the second part, tanh function is used to generate a new candidate vector. The calculation process is shown in Formula (2).

$$\begin{aligned} f_t &= \sigma(w_f \cdot [h_t - 1, x_t] + b_f) \\ \tilde{c}_t &= \tanh(w_c \cdot [h_t - 1, x_t] + b_c) \end{aligned} \tag{2}$$

where w_i and b_i are the weights and offsets of the inputs, w_c and b_c are the weights and offsets of the cell state. After the above processing, the original cell state c_{t-1} is updated to the current cell state c_t, and the formula is shown in Formula (3).

$$c_t = f_t^* c_t - 1 + i_t^* \tilde{c}_t \tag{3}$$

where * represents element multiplication, $f_t^* c_{t-1}$ represents deletion information, and $i_t\ ^* c_t$ represents new information.

The input gate controls the output of the cell state of this layer to determine which cell states are input to the next layer. The calculation formula is shown in Formula (4).

$$\begin{aligned} o_t &= \sigma(w_o \cdot [h_t - 1, x_t] + b_o) \\ h_t &= o_t^* \tanh(c_t) \end{aligned} \tag{4}$$

The DDoS attack detection method based on LSTM first quantifies, standardizes and normalizes the original detection data set, then inputs the preprocessed data set into the trained LSTM model, and finally inputs the results of the LSTM model into the softmax classifier to obtain the classification results. This method is when working with sequence data [15].

Bi-LSTM model is a structural variant of LSTM, which is composed of two subnetworks, namely forward and backward transfer LSTM. This structure improves the ability to store the two-way information of the network traffic data sequence at the same time, thus solving the congenital deficiency that the traditional RNN can only remember the information in a short time and the one-way LSTM can only keep the previous context information. Therefore, this paper uses the BiLSTM network as the time feature extraction model, which can better learn the time feature of network traffic.

C. SELF-ATTENTION MECHANISMS

In recent years, attention mechanisms have been gradually applied in a wide range of fields such as bioinformatics, such as serial data processing in speech recognition [16], [17], machine translation [18] and part-of-speech annotation [19]. For example, in a machine translation task, the attention mechanism specifies which part of the source sentence the neural network learning should focus on in order to obtain a higher quality translation.

With the continuous high development of deep learning, neural networks based on attention mechanism have aroused great interest in image classification research, Lin et al. [20] use the attention mechanism on the RNN model to classify images, focus on the key parts of the image to reduce

the complexity of the task, and the attention mechanism enables the neural network to pay more attention to the input image part related to the result. Yang et al. [21] use a text recognition method based on deep learning to generate a three-dimensional matrix format after preprocessing the obtained model training dataset, input it to a CNN with an attention mechanism module for feature extraction and final classification effect recognition.

The invention and operation mechanism of the attention mechanism is inspired by the biological visual phenomenon in real life. Its basic principle is to learn by focusing on the area of interest, that is, when the scene reappears, enough attention will focus on the key information to highlight the important local information. The attention mechanism will give more weight to the important information through learning, so as to make better and more accurate judgments. Its ideological framework is shown in Figure 3.

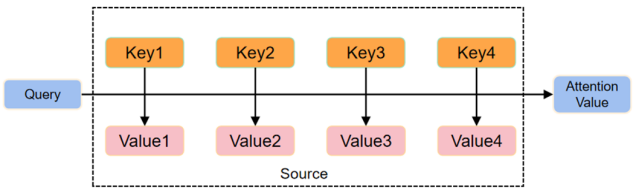

FIGURE 3. Attention mechanism frame diagram.

As shown in Figure 3, a source is represented as a collection of value values stored in the address key. Evaluate whether the storage content contained in the key address is associated with Query and calculate its similarity. The addressing process of the soft attention mechanism is that it will obtain content from multiple key addresses, calculate the correlation with Query, and then add the attention weight vector and value to get the final value. The calculation process of attention mechanism has two steps:

(1) Calculate the similarity between the input value and Query to get the weight vector.

$$s_i = score(W_s h_i + b) \tag{5}$$

Equation (5) Calculate the importance score si of the input information and query vector through the attention scoring function score, where W refers to that the weight matrix of each information of the attention mechanism is a learnable network parameter, b is the bias term of the attention mechanism, and hi refers to that the hidden state dimension is the input of the attention mechanism.

(2) Normalization of weights

$$a_i = soft\ \max(s_i) = \frac{\exp(s_i)}{\sum_i \exp(s_i)} \tag{6}$$

In Formula (6), after obtaining each important score si for the hidden state vector hi, use the softmax function to evaluate the attention weight a_i.

(3) Weighted Sum of Weights and Values

$$v = \sum_{N}^{i} a_i h_i \tag{7}$$

In equation (7), the attention weight vector and the hidden state vector are weighted and summed to calculate the final output vector v.

III. METHODOLOGY

In our research, we construct an intrusion detection system based on CNN-BiLSTM. The IDS methodology is depicted in Figure 4.

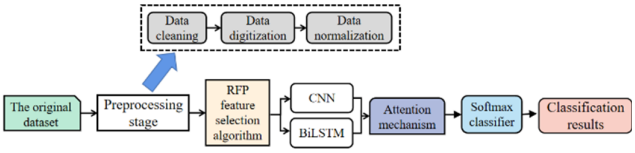

FIGURE 4. Block diagram of DDoS attack detection based on CNN-AttBiLSTM.

A. DATA PREPARATION

In the field of DDoS attack detection, there are few datasets that can be used to train deep learning algorithms. The commonly used CAIDA2007 [22] and ISCX-2012 [23] datasets have a long history. With the complexity of network architecture and the constant changes of attacks, these datasets are not completely representative.

The experiment in this article used two publicly available datasets collected by the Canadian Institute of Cybersecurity (CIC) and Wireshark in a simulated environment, namely CIC-IS2017 [24] and CICDDoS2019 [25]. These two datasets were first generated using two types of usage profiles and multi-level attacks such as Heartbleech, as well as various DoS and DDoS attacks. Then, the collected traffic was preprocessed using the CICFlowMeter tool to generate a CSV format containing various DoS and DDoS traffic data. Table 1 shows the sample sizes for different categories in the CIC-ISDS2017 and CIC-DDoS2019 datasets.

1) CIC-IDS2017

CIC-IDS2017 dataset encompasses eleven new attacks, including 151 Brute Force, PortScan, DoS, web attacks including XSS and SQL Injection, FTP-Patator, and SSH-Patator. It was developed in 2017 by the Canadian Institute for Cybersecurity, and its eighty features are used to monitor benign and malicious traffic.

2) CIC-DDoS2019

CIC-DDoS 2019 dataset contains 86 network traffic package attributes that have been generated using the open-source tool, which produces network packets and collects attributes from them. DDoS attacks based on reflection utilize

TABLE 1. Dataset flow label distribution.

DataSet	Traffic type	Number of cases	Proportion	total
CIC-IDS2017	BENIGN	2363910	80.8583	2923522
	DoS	252661	8.6423	
	Portscan	158930	5.4363	
	DDos	128027	4.3792	
	Patator	13835	0.4732	
	Bot	3932	0.1345	
	Infiltration	36	0.001231	
	HeartBleed	11	0.000376	
CIC-DDoS2019/NTP	BENIGN	14365	0.0118	1217007
	DDoS/NTP	1202642	0.9881	
CIC-DDoS2019/LDAP	BENIGN	1612	0.0007	2181542
	DDoS/LDAP	2179930	0.9992	
CIC-DDoS2019/SSDP	BENIGN	763	0.0002	2611374
	DDoS/SSDP	2610611	0.9997	
CIC-DDoS2019/ Syn	BENIGN	392	0.0002	1582681
	Syn	1582289	0.9997	
CICDDoS2019/NetBIOS	BENIGN	1707	0.0004	4094986
	DDoS/NetBIOS	4093279	0.9995	

authorized servers, such as Domain Name Server (DNS), Lightweight Directory Access Protocol (LDAP), Network Basic Input/Output System (NETBIOS), and (Simple Network Management Protocol) SNMP, that render various services over the network.

Due to the research on DDoS attacks in this article, two CSV files containing only Benign and DDoS were separated for preprocessing of the CIC-ISD2017 dataset. Through feature selection algorithms, flow features, basic features, connection features, time features, general features, some additional generated features, and label features were extracted, totaling 52 dimensional features; For the CIC-DDoS2019 dataset, 67 dimensional features are preserved after preprocessing. This article is based on the CIC-ISD2017 dataset for binary classification experiments. Normal traffic is represented by 0, and DDoS attack traffic is represented by 1; To verify the effectiveness of the proposed model in detecting multi class attacks, multi class experiments were conducted based on the CIC-DDoS2019 dataset.

B. PRE-PROCESSING

The preprocessing layer cleanses the CIC-IDS2017 dataset, and then performs one-hot encoding and normalization. The specific process is divided into 3 steps.

(1) Data cleansing ensures that data is clean, comprehensive, and error-free. Data cleaning mainly handles abnormal data. In this paper, the KNN Imputer method in Scikit-learn is used to fill in, and the missing values can be fitted for the case of a large number of missing sample data. In cases where there are fewer missing sample data, you can use a filling such as mode.

This method uses the Euclidean distance matrix to find the nearest neighbor and help estimate the missing values in the observation. Taking matrix input = [[3,nan,7]],[4,3,10],[2,4,8] as an example, when the number of ''neighbor'' samples is taken as 1, the first column feature 3 and the third column feature 7 of the first sample are the closest Euclidean distance from the first column feature 2 and the third column feature 8 of the last sample, so the missing value is filled with 4.

(2) The one-hot method is used to process the CIC-IDS2017 dataset, and the symbolic features in the original dataset are converted into numerical features to ensure that all data are numeric, so as to facilitate the learning of data features.

(3) Since dataset normalization can reduce the variance of traffic characteristics to a certain range and reduce the influence of outliers, the data is encoded by one-hot, and the min-max normalization is used to normalize the feature values to values between 0 and 1. As shown in Equation (8):

$$h_{i,j} = \frac{h_{i,j} - \min(h_{i,j})}{\max(h_{i,j}) - \min(h_{i,j})} \tag{8}$$

where $h_{i,j}$ represent the eigenvalues of row i and column j in the dataset.

C. RFP FEATURE SELECTION ALGORITHM

In order to solve the problem of feature redundancy in the dataset, a new RFP feature selection algorithm is proposed. The algorithm first calculates the importance of each feature in the sample through the random forest algorithm and ranks it according to the importance; Then, the Pearson correlation coefficient is used to calculate the correlation between features; Finally, the two results are combined to achieve feature selection.

The random forest algorithm (RF) is an ensemble learning algorithm based on decision trees. In feature engineering, RF algorithms can identify important features from a large number of sample features; Its essence is to analyze the contribution of each feature of the calculated sample on the tree, then calculate its average, and compare the size of the contribution between features to identify important features [26]. Existing methods typically use the Gini index or out-of-bag data (OOB) error rate as evaluation metrics to measure the size of the contribution. This paper uses OOB as an indicator to measure the size of contribution. The specific steps to calculate the importance of a feature feature are as follows:

(1) For each decision tree in the random forest, select the corresponding out-of-bag data to calculate the out-of-bag data error, which is recorded as errOOB1.

(2) Randomly add noise interference to the feature featurei of all samples of out-of-bag data (that is, randomly change the value of the sample at feature X), and calculate the error of the out-of-bag data again, which is recorded as errOOB2.

(3) Assuming that the random forest contains M trees, the importance value of the feature can be calculated by Equation (9):

$$Impor\tan ce = \sum \frac{errOOB_2 - errOOB_1}{M} \tag{9}$$

(4) Filter out features of high importance to build a new dataset.

The Pearson correlation coefficient is used to measure the correlation between two variables X and Y. It calculates

the covariance and standard deviation between two feature values and quotients by equation (10) to obtain the Pearson correlation coefficient between the two features:

$$\rho X, Y = \frac{cov(\mathrm{X}, \mathrm{Y})}{\sigma X \sigma Y} = \frac{E[(X - \mu X)(Y - \mu Y)]}{\sigma X \sigma Y} \quad (10)$$

Pearson's value range is (−1,1), and the larger the absolute value, the stronger the correlation between the two variables, and the strength of the correlation is generally judged by Table 2.

TABLE 2. Strength of correlation table.

Range of correlation coefficient	Degree of strength
0.0~0.2	Very weak correlation or no correlation
0.2~0.4	Weak correlation
0.4~0.6	Moderate correlation
0.6~0.8	Strong correlation
0.8~1.0	Extremely strong correlation

In this paper, more important features are retained according to the degree of importance, so features with a correlation coefficient greater than 0.8 or less than −0.8 are selected to be retained; for features whose correlation coefficient is not in the analysis interval, the feature importance is analyzed, and if it is lower than 0.001, it is excluded. Finally, the CIC-IDS2017 dataset left 52 features.

The pseudocode of the RFP feature selection algorithm proposed in this paper is as follows.

Input:

Original data set, D

Output:

Processed data set, New D

Procedure:

(1) Choose corresponding out of bag data and calculate the error, errOOB_1

(2) Randomly add interference to all samples of data outside the bag and calculate its error, errOOB_2

(3) Calculate feature importance

(4) Feature importance ranking

(5) Calculate Pearson correlation coefficient

(6) Selection feature in combination with (4) and (5)

(7) Processed data set New D

D. ALGORITHMIC PROCESS

In order to achieve efficient detection of DDoS attacks, this model is mainly divided into four parts, the first part is the data preprocessing stage, the second part is the feature selection stage, the third part is the design core, including the feature extraction of spatial dimension and time dimension with CNN and BiLSTM, the feature fusion of the two is assigned to different weights by self-attention mechanism, and the fourth part is the classification stage.

In this paper, we first use the random forest algorithm to calculate the importance of the features (in this paper, referred to as the importance), and then rank them; Then, Pearson correlation analysis is used to calculate the correlation between features, and the two obtained results are combined to achieve feature selection, reducing the problem of data redundancy. The combination of spatial features and temporal features extracted by CNN and BiLSTM respectively increases the weight distribution of the "importance" of input features by the self-attention mechanism, so as to further improve the detection rate. The specific workflow is as follows.

Algorithm 1 DDoS Attack Detection Algorithm Based on CNN-AttBiLSTM

Input: The original dataset

Output: Positive/Malicious sample

The model extracts spatiotemporal features and classifies them

(1) Spatial feature extraction

a) Data preprocessing is performed to input the results into the convolutional layer;

b) The convolutional layer extracts features, and the weight sharing reduces the parameters;

c) Use the activation function to non-linearly map the convolutional layer output;

d) Use the output of the previous step as the input of the pooling layer, and the pooling layer reduces the data dimensionality;

e) Convolutional and pooled layers are stacked;

f) The fully connected layer integrates the extracted high-dimensional features into the output.

(2) Temporal feature extraction

a) The same spatial features were extracted, the data was preprocessed, and the results were sent to BiLSTM;

b) The BiLSTM model performs temporal feature extraction by updating the gate information.

(3) Feature fusion (fusing information from the previous two steps into "parallel features")

(4) Self-attention mechanisms

The results obtained in the third step are fed into the self-attention model, and the secondary feature extraction is carried out to select important information.

(5) Use the softmax function for classification

E. HYBRID DEEP LEARNING MODEL

In this paper, 1D CNN is used to extract the spatial features of input data, BiLSTM is used to extract sequence features, and self attention mechanism is introduced to assign different weights to the mentioned spatio-temporal features according to their importance. Then, the two gods "parallel" fuse the feature information extracted from the network, process it through the fully connected network, and output the classification results through the Softmax classifier. The principle block diagram of this algorithm is shown in Figure 4.

In this paper, CNN and BiLSTM neural networks are combined in parallel rather than in series, which avoids the problem that when CNN is used for feature extraction in the literature [27], there is a certain probability that

some feature information will be lost, thus affecting the detection efficiency, and also ensures that the model proposed in this paper still has a high accuracy rate and a low false alarm rate, Thus, to a certain extent, the problem that a single neural network cannot fully obtain features is solved.

F. EVALUATION

In order to evaluate the detection performance of the model, this paper uses accuracy, precision, recall and F1 value as the evaluation indicators of the model. The precision indicates the proportion of all correctly classified samples to all samples; The accuracy rate indicates that the prediction result is the proportion of positive samples with actual labels; Recall rate indicates the proportion found in all positive samples; F1 value is a combination of accuracy rate and recall rate, which is used to comprehensively reflect the overall indicators. These indicators are calculated from the classification results of positive and negative samples. The calculation process of each evaluation indicator is as follows:

$$Accuracy = \frac{TP + TN}{TP + FN + FP + TN}$$

$$\Pr ecision = \frac{TP}{TP + FP}$$

$$\mathrm{Re}\, call = \frac{TP}{TP + FN}$$

$$F1 = \frac{2 * precision * recall}{precision + recall}$$

TP represents the number of positive samples correctly classified, FN represents the number of negative samples wrongly classified, FP represents the number of positive samples wrongly classified, and TN represents the number of negative samples correctly classified.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The hardware environment for the experiment: The operating system is Windows 10, the graphics card is a processor with Intel i7-10875 CPU, and 8 GB of memory. Software environment: The programming language is Python 3.7, and the learning framework is Keras 2.4.3.

A. COMPARISON BASED ON DIFFERENT FEATURE SELECTION METHODS

In order to validate the effectiveness and applicability of the proposed feature selection method, this section conducts comparative experiments on different feature selection methods. Under the same experimental conditions, the proposed RFP feature selection method is compared with commonly used PCA and AE feature selection methods. The experimental comparison is shown in Table 3.

From Table 3, it can be observed that the proposed RFP algorithm achieves comparable results on all three datasets compared to the other two methods. This is because

TABLE 3. Comparison results of different feature selection methods.

		Evaluation metrics (%)			
DataSet	Method	ACC	Pre	Rec	F1
CIC-IDS2017	AE	88.703	88.837	88.702	88.815
	PCA	93.742	93.871	93.741	93.826
	RFP	**96.817**	**96.764**	**96.812**	**96.793**
CIC-DDoS2019	AE	84.913	84.624	84.315	85.416
	PCA	89.172	89.365	89.172	89.205
	RFP	**94.705**	**94.681**	**94.402**	**94.537**

the PCA algorithm relies more on variance during data dimensionality reduction, but non-principal components with small variances may still contain important information about sample differences, which can affect subsequent data processing. On the other hand, AE relies more on the training data for feature space reconstruction. Therefore, both of these methods may not achieve better results. In contrast, the proposed RFP algorithm selects features based on their importance and relevance, aiming to improve the classification accuracy of the model.

B. HYPER-PARAMETERS ANALYSIS

This paper analyzes the influence of super parameter setting on the detection effect from two aspects:

1) INFLUENCE OF CONVOLUTION KERNEL SIZE ON DETECTION PERFORMANCE

The size of the convolution kernel will directly affect the quality of feature extraction, and the inappropriate size of the convolution kernel will affect the incomplete feature extraction. In order to study the influence of the size of convolution kernel on the detection performance, six convolution kernels of different sizes are set in this paper, ranging from 1 to 6. The size of convolution kernel selected in this paper is 3. The experimental results are shown in Figure 5.

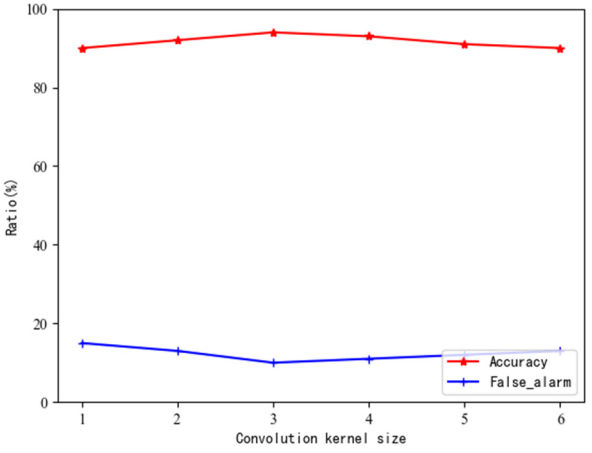

FIGURE 5. The effect of convolution kernel size on detection performance.

It can be seen from Figure 3 that the size of the convolution kernel has a significant impact on the accuracy

rate. When the size of the convolution kernel is 3, the accuracy rate is the highest. The convolution kernel continues to increase, but its accuracy rate decreases. Therefore, the convolution kernel should not be too large. The size of convolution kernel has little influence on the false positive rate, and when the size of convolution kernel is 3, the false positive rate is the lowest. In conclusion, when the size of convolution kernel is 3, the experimental results are good.

2) EFFECT OF MEMORY MODULE OF LSTM ON DETECTION PERFORMANCE

The memory module of LSTM is the core of LSTM model, which plays a crucial role in processing long-distance dependent information. It can determine whether the features in the recorded information are forgotten, and appropriate memory modules can improve the phenomenon of high false positive rate. In order to find the LSTM structure most suitable for the method in this paper, five different LSTM topologies are set and compared. The specific information is as follows:

(1) one memory module, each module has one cell;
(2) two memory modules, each module has two cells;
(3) four memory modules, each module has two cells;
(4) four memory modules, each module has four cells;
(5) one memory module, each module has four cells;

The experimental results of five LSTM topologies are shown in Figure 4. It can be seen that since LSTM can control whether some features are forgotten, its topology has a greater impact on the false alarm rate. When the number of memory modules is 1 and the cell infusion of each module is 2, the accuracy rate is the lowest; When the number of memory modules is 2 and the number of cells in each module is 2, the false positive rate is the highest; When the number of memory modules is 4 and the number of cells in each module is 2, the false positive rate is the lowest and the accuracy rate is ideal. In conclusion, when the number of memory modules is 4 and the number of cells in each module is 2, the best experimental effect is achieved. The experimental results are shown in Figure 6.

C. COMPARISON BASED ON DIFFERENT LEARNING ALGORITHMS

In order to verify the effectiveness of the new model, the CIC-IDS2017 dataset will be used to conduct comparative experiments on CNN, LSTM, BiLSTM, and CNN BiLSTM. The accuracy rate, accuracy rate, recall rate and F1 value of the model are used as evaluation indicators. The comparison of experimental results is shown in Table 4.

It can be seen from Table 3 that LSTM based methods are higher than CNN based methods in accuracy, accuracy, recall and F1 value, which proves that LSTM method has the advantage of processing long-distance dependent information compared with CNN; Similarly, the performance of the method based on BiLSTM is better than that of the method based on LSTM, indicating that

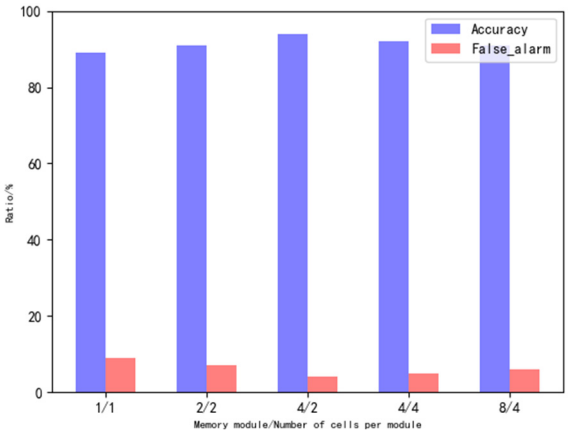

FIGURE 6. The effect of BiLSTM memoty module number on detection performance.

TABLE 4. Comparison results of different models.

	Evaluation metrics (%)			
Methods	ACC	Pre	Rec	F1
CNN	82.018	82.908	83.138	83.022
LSTM	85.129	85.402	85.319	85.360
BiLSTM	88.651	88.709	88.403	88.742
CNN-BiLSTM	92.501	92.809	92.451	92.630

bi-directional data information can be saved at the same time when dealing with network traffic sequence problems; The CNN-BiLSTM model proposed in this paper has better overall performance than the method using only BiLSTM because it extracts spatial features and temporal features respectively.

This paper adds the self attention mechanism to verify that the attention mechanism can improve the DDoS attack detection performance. Therefore, on the same CIC-IDS2017 dataset, a comparative experiment was carried out between the CNN BiLSTM model without self attention mechanism and the CNN AttBiLSTM model with self attention mechanism. The experimental results are shown in Table 5.

TABLE 5. Comparison results of similar models.

	Evaluation metrics (%)			
Methods	ACC	Pre	Rec	F1
CNN-GRU[8]	87.509	88.174	87.752	87.813
HAST-IDS[9]	89.425	87.168	89.373	88.876
MSCNN-LSTM[10]	90.862	90.749	90.615	90.652
CNN-BiLSTM	92.501	92.809	92.451	92.530
CNN-AttBiLSTM	**95.670**	**95.824**	**95.904**	**95.864**

D. MULTI CLASSIFICATION COMPARISON RESULTS

In order to verify that the attack detection method proposed in this article can effectively distinguish different types of DDoS attacks, a model multi classification performance evaluation experiment was conducted on the CIC-DDoS2019 dataset. The experimental results are shown in Table 6.

TABLE 6. Multi-classidication attack detection results based on CIC-DDoS2019 dataset.

	CNN-BiLSTM				CNN-AttBiLSTM			
Traffic type	ACC	Pre	Rec	F1	ACC	Pre	Rec	F1
BENIGN	93.825	94.673	96.274	96.283	96.251	96.732	97.232	97.470
NTP	93.974	93.813	94.324	96.631	94.528	95.871	96.132	96.126
LDAP	93.506	94.809	95.451	94.630	95.322	95.132	95.624	95.483
SSDP	92.321	92.813	96.235	94.732	93.523	94.635	96.237	96.081
Syn	94.603	95.809	95.371	95.853	95.327	96.632	96.255	96.583
NetBIOS	95.650	96.734	96.125	96.107	97.876	98.086	98.214	98.173

In the binary classification experiment, the effectiveness of the hybrid model has been verified, so in the multi classification experiment, only the performance comparison between the proposed model and CNN-BiLSTM will be conducted. From Table 6, it can be seen that compared to the CNN-BiLSTM model, the detection accuracy of this model for NTP, LDAP, SSDP, and Syn has increased by 1.544%, 1.816%, 1.202%, and 1.724%, respectively. It has achieved the highest accuracy for normal class and NetBIOS attacks, with 96.251% and 97.876%, respectively. This result indicates that the proposed model performs better in detecting multiple types of attack samples.

V. CONCLUSION AND FUTURE WORK

This article introduces attention mechanism based on CNN and BiLSTM networks and constructs a new CNN BiLSTM model, which achieves high accuracy and low false alarm rate for DDoS attack detection. At the beginning, feature selection is carried out using the RFP algorithm, and then 1D CNN and BiLSTM networks are used to simultaneously extract spatial and temporal features. The extracted spatiotemporal features are ''parallel'' fused. Then, attention mechanism is introduced to allocate corresponding weights based on the importance of the features. Finally, use a softmax classifier for traffic classification. The experimental results show that when tested using the CIC-ISDS2017 and CIC-DDoS2019 datasets, the proposed method outperforms similar published methods in four performance evaluation indicators, with the highest accuracy, accuracy, recall, and F1 values of 95.670%, 95.824%, 95.904%, and 95.864%, respectively. This proves that the model constructed using the new method can effectively detect and accurately distinguish multiple types of DDoS attacks. In the subsequent research work, the research team will improve the performance of DDoS attack traffic detection while also adding real-time analysis function of network traffic, hoping to explore detection models and methods with higher accuracy, lower error rate, and more stable performance.

REFERENCES

[1] *HUAWEI: Special Report on Botnets and DDoS Attacks in 2013*. Accessed: 2013. [Online]. Available: https://doczz.net/doc/7640522/2013-botnets-and-ddos-attacks-report

[2] P. Yu and C. Li, ''DDoS attack detection method based on random forest,'' *Appl. Res. Comput.*, vol. 34, no. 10, pp. 3068–3072, 2017.

[3] J. Zheng, Q. Li, G. Gu, J. Cao, D. K. Y. Yau, and J. Wu, ''Realtime DDoS defense using COTS SDN switches via adaptive correlation analysis,'' *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 7, pp. 1838–1853, Jul. 2018.

[4] S. Behal, K. Kumar, and M. Sachdeva, ''D-FACE: An anomaly based distributed approach for early detection of DDoS attacks and flash events,'' *J. Netw. Comput. Appl.*, vol. 111, pp. 49–63, Jun. 2018.

[5] A. A. Diro and N. Chilamkurti, ''Distributed attack detection scheme using deep learning approach for Internet of Things,'' *Future Gener. Comput. Syst.*, vol. 82, pp. 761–768, May 2018.

[6] J. Ye, X. Cheng, and J. Zhu, ''A DDoS attack detection method based on SVM in software defined network,'' *Secur. Commun. Netw.*, vol. 4, pp. 1–8, Jul. 2018.

[7] A. Koay, A. Chen, I. Welch, and W. K. G. Seah, ''A new multi classifier system using entropy-based features in DDoS attack detection,'' in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Chiang Mai, Jan. 2018, pp. 162–167.

[8] A. Oena, ''A DDoS attack behavior detection method based on deep learning,'' 2016, *arXiv:1601.04033*.

[9] W. Wang, Y. Sheng, J. Wang, X. Zeng, X. Ye, Y. Huang, and M. Zhu, ''HAST-IDS: Learning hierarchical spatial–temporal features using deep neural networks to improve intrusion detection,'' *IEEE Access*, vol. 6, pp. 1792–1806, 2018.

[10] J. R. Cheng et al., ''DDoS attack detection via multi-scale convolutional neural network,'' *Comput. Mater. Continua*, vol. 62, no. 3, pp. 1317–1333, 2020.

[11] C. H. Tang, P. C. Liu, and S. S. Tang, ''Anomaly intrusion behavior detection based on fuzzy clustering and features selection,'' *Comput. Res. Develop.*, vol. 52, no. 3, pp. 718–728, 2015.

[12] S. Yao, F. Xu, and P. Zhao, ''Intuitionistic fuzzy entropy feature selection algorithm based on adaptive neighborhood space rough set model,'' *Comput. Res. Develop.*, vol. 55, no. 4, pp. 802–814, 2018.

[13] G. Yaqing, W. Wenjian, and S. Meihong, ''An adaptive regression feature selection method for datasets with outliers,'' *Comput. Res. Develop.*, vol. 56, no. 8, pp. 1695–1707, 2019.

[14] Y. Y. Jun et al., ''A multi-filter feature selection in detecting distributed denial-of-service attack,'' in *Proc. 3rd Int. Conf. Telecommun. Commun. Eng.*, Jan. 2019, pp. 57–62.

[15] L. Yuefeng, C. Shuang, and Y. Hanxi, ''Network intrusion detection method integrating CNN and BiLSTM,'' *Comput. Eng.*, vol. 45, no. 12, p. 7, 2019.

[16] Z. Y. Zhao, W. Q. Zhang, and J. Liu, ''End-to-end keyword search system based on attention mechanism and multitask learning,'' *Signal Process.*, vol. 36, no. 6, pp. 839–851, 2020.

[17] D. Bahdanau, J. Chorowski, and D. Serdyuk, ''End-to-end attention-based large vocabulary speech recognition,'' in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Shanghai, China, Jul. 2016, pp. 4945–4949.

[18] Q. Wang and X. Y. Duan, ''Neural machine translation based on attentiom convolution,'' *Comput. Sci.*, vol. 45, no. 11, pp. 226–230, 2018.

[19] N. Si, H. Wang, W. Li, Y. Shan, and P. Xie, ''Chinese part-of-speech tagging model using attention-based LSTM,'' *Comput. Sci.*, vol. 45, no. 4, pp. 66–70, 2018.

[20] L. Lin, H. Luo, R. Huang, and M. Ye, ''Recurrent models of visual co-attention for person re-identification,'' *IEEE Access*, vol. 7, pp. 8865–8875, 2019.

[21] H. D. Yang, K. S. Huang, and L. J. Yu, ''An attentional mechanism text recognition method based on deep learning,'' Chin. Patent 202 010 340 618.8, Nov. 23, 2023.

[22] The Cooperative Association for Internet Data Analysis. *The CAIDA UCSD 'DDoS Attack 2007' Dataset*. [Online]. Available: http://www.caida.org/data/passive/ddos-20070804_dataset.xml

[23] X. Yuan, C. Li, and X. Li, ''DeepDefense: Identifying DDoS attack via deep learning,'' in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, Hong Kong, May 2017, pp. 1–8.

[24] A. Yulianto, P. Sukarno, and N. A. Suwastika, ''Improving AdaBoost-based intrusion detection system (IDS) performance on CIC IDS 2017 dataset,'' *J. Phys., Conf. Ser.*, vol. 1192, Mar. 2019, Art. no. 012018.

[25] *DDoS Evaluation Dataset (CIC-DDoS2019)*, University of New Brunswick, Saint John, NB, Canada, 2019.

[26] Z. Y. Cui and X. L. Geng, "SVM algorithm based on RF and quantum particle swarm optimization," *Comput. Integr. Manuf. Syst.*, vols. 1–13, p. 13, 2021. [Online]. Available: http://kns.cnki.net/kcms/detail/11.5946.TP.20210910.1824.008.html
[27] W. Wang, "Deep learning for network traffic classification and anomaly detection," Univ. Sci. Technol. China, Hefei, China.

JUNJIE ZHAO received the B.S. degree from the Henan University of Technology in 2021. He is currently pursuing the master's degree with the Central South University of Forestry and Technology. His main studying area is DDoS attacks and deep learning.

YONGMIN LIU (Member, IEEE) received the B.S. degree in computer application technology from the National University of Defense Technology in 1998, the M.S. degree in computer application technology and the Ph.D. degree in control theory and application from Central South University. He is currently a Professor with the College of Computer and Information Engineering, Central South University of Forestry and Technology. His current research interests include information security and network data transmission.

QIANLEI ZHANG received the B.S. degree in engineering from the Zhengzhou Shengda College of Economics and Trade Management in 2020. He is currently pursuing the master's degree with the Central South University of Forestry and Technology. His research interests include web attack and machine learning.

XINYING ZHENG received the B.S. degree in economics from Xinyang Normal University, in 2008, the M.S. degree in economics from Xiangtan University in 2011, and the Ph.D. degree in economics from the Renmin University of China, in 2014. She is currently a Lecturer with Hunan Normal University. Her current research interests include deep learning and economics.