A Method for Network Intrusion Detection Based on GAN-CNN-BiLSTM

Shuangyuan Li[1], Qichang Li[2], Mengfan Li[3]
Information Construction Office, Jilin Institute of Chemical Technology, Jilin, China[1]
School of Information and Control Engineering, Jilin Institute of Chemical Technology, Jilin, China [2, 3]

***Abstract*—As network attacks are more and more frequent and network security is more and more serious, it is important to detect network intrusion accurately and efficiently. With the continuous development of deep learning, a lot of research achievements are applied to intrusion detection. Deep learning is more accurate than machine learning, but in the face of a large amount of data learning, the performance will be degraded due to data imbalance. In view of the serious imbalance of network traffic data sets at present, this paper proposes to process data expansion with GAN to solve data imbalance and detect network intrusion in combination with CNN and BiLSTM. In order to verify the efficiency of the model, the CIC-IDS 2017 data set is used for evaluation, and the model is compared with machine learning methods such as Random Forest and Decision Tree. The experiment shows that the performance of this model is significantly improved over other traditional models, and the GAN-CNN-BiLSTM model can improve the efficiency of intrusion detection, and its overall accuracy is improved compared with SVM, DBN, CNN, BiLSTM and other models.**

***Keywords*—Intrusion detection; GAN; CNN; BiLSTM**

I. INTRODUCTION

Technology is developing very fast these days, and the internet has become an indispensable tool in our daily lives. It brings great convenience to all walks of life. However, in today's network environment, a variety of new means of attacking the network continue to emerge, with increasingly larger impact scales and higher attack frequencies. As a result, network security has become a growing concern. The task of network intrusion detection is to find suspicious attacks and take appropriate protective measures to re-duce the possibility of subsequent attacks and minimize corresponding economic losses. Therefore, research on Intrusion Detection (ID) has become a major research direction in the field of network security [1-2].

The intrusion detection system is one of the most promising methods for quickly identifying and dealing with network intrusions. It can identify whether the system is being attacked or has been attacked, and can take preventive measures against possible network attacks. An intrusion detection system can detect and analyze network activities on a computer, thereby protecting sensitive information, preventing unauthorized user access, system misoperation, and malicious intrusion. However, in the current network traffic, the volume of normal data flow is much larger than that of abnormal data flow. This results in a serious imbalance in the proportion of data occupied by normal flow and abnormal flow, which significantly reduces the learning performance and accuracy of the classifier.

Intrusion detection technology has developed rapidly over the years and has become a crucial aspect of network security. The main focus of intrusion detection is to detect any suspicious activity that may lead to network breaches and take appropriate measures to prevent them. There are two primary methods of intrusion detection - signature-based and anomaly-based. Signature-based intrusion detection is a rule-based method that compares incoming network traffic with a pre-defined set of signatures or patterns. While this method is highly accurate, it cannot detect new or unknown attacks and requires frequent updates of the signature database to maintain effectiveness [3].On the other hand, anomaly-based intrusion detection works by identifying abnormal patterns in network traffic that deviate significantly from the expected behavior of the network. This method is useful for detecting unknown attacks that do not match any known signature, but it can also produce false positives by flagging normal behavior as suspicious. Anomaly-based intrusion detection can be achieved through various techniques such as machine learning, data mining, data statistics, and deep learning.

Machine learning algorithms can learn from labeled data sets and identify the patterns that distinguish normal and malicious traffic. Data mining techniques can be used to extract useful knowledge from large-scale network data sets and identify abnormal behaviors. Data statistics can help identify unusual changes in the network, while deep learning algorithms can analyze large amounts of data and identify complex patterns and correlations that are difficult to detect through other methods.

In conclusion, intrusion detection is critical for ensuring network security, and the choice of intrusion detection method depends on the specific needs of the network and the level of threat faced. Both signature-based and anomaly-based intrusion detection methods have their advantages and limitations, and the optimal approach often involves combining multiple techniques to achieve the best results.

At present, machine learning has been widely used in intrusion detection, but machine learning is mostly shallow learning, focusing on feature engineering and selection, and the accuracy will be degraded when dealing with a large volume of real network traffic data. Deep learning can deal with a large volume of data, and thus it is more accurate and effective in intrusion detection. Convolutional Neural Networks (CNN) and Bidirectional Long Short-Term Memory (BiLSTM) can

automatically learn feature representations from input data, while Random Forest, Decision Tree, and SVM require manual feature design or rely on feature engineering. This gives CNN and BiLSTM an advantage in handling complex data such as images, speech, and text. BiLSTM is specifically designed for handling sequential data and can capture long-term dependencies within sequences. In contrast, methods like Random Forest, Decision Tree, and SVM are not well-suited for modeling sequential data. CNN and BiLSTM have the property of parameter sharing and weight sharing, making the training of the models more efficient and allowing them to handle problems with a large number of parameters. On the other hand, Random Forest and Decision Tree require more parameters and computational resources. The generator in Generative Adversarial Networks (GANs) utilizes a CNN architecture, which exhibits excellent generation capabilities and can generate realistic synthetic data. CNN and BiLSTM can efficiently process large-scale data through mini-batch training, especially when accelerated by GPUs. In comparison, Random Forest and Decision Tree may face limitations in memory and computational resources when dealing with large-scale data. However, due to the imbalance of the data sets, the performance will be significantly degraded as the volume of abnormal data is much smaller than the volume of normal data. Therefore, this paper proposes to solve data imbalance via GAN, which has been widely and effectively used in speech and image fields. In this paper, GAN is used to create virtual data similar to the minority class for resampling to improve the efficiency and accuracy of intrusion detection. Moreover, it is found that the effect of using multi-model mixture is better than that of using single model. Therefore, this paper adopts the method of combining CNN and BiLSTM to conduct experiments. The main contributions of this paper are summarized as follows:

1) Proposed to use of GAN pairs to solve the problem of data imbalance, and add an attention mechanism to solve the problem of inaccurate model results caused by unreasonable convolution kernel settings.

2) Propose the design and implementation of an intrusion detection model based on CNN-BiLSTM, and combine CNN with BiLSTM to build the intrusion detection classification model. In addition, add a self-attention mechanism to BiLSTM to make the model more effective and more accurate.

3) Study the performance and effect of the data set in machine learning such as Naive Bayes, Random Forest and Decision Tree, and compare with the model in this paper. The experimental result shows that the performance of GAN-CNN-BiLSTM is higher than the traditional classification model, so the performance of the model proposed in this paper is higher than other traditional models, which can improve the efficiency of intrusion detection and the overall accuracy.

Starting from the data, this paper first uses GAN to balance the data, which lays a good foundation for the subsequent training of the classification model, improving the accuracy of intrusion detection. Then, it obtains the final model through continuous improvement. Moreover, the CIC-IDS-2017 data set is used for experimental verification, and compared with CNN, BiLSTM, SVM and other models. The experimental result shows that the detection model proposed in this paper has a better effect and higher accuracy.

The proposed model in this paper can provide network security protection for the following:

1) Protection of critical infrastructure: It can be applied to critical infrastructure such as power grids, water supply systems, transportation systems, etc. It helps detect and prevent potential network attacks, hacker intrusions, and data breaches, ensuring the security and reliable operation of this infrastructure.

2) Security for companies and organizations: It can protect the network and information security of companies, organizations, and institutions. It helps identify malware, phishing attacks, data theft, and other security threats, providing real-time threat intelligence and defense measures.

3) Government agencies and military applications: It holds significant importance in government agencies and military sectors. It can be applied to network security and intelligence analysis, aiding in the discovery and prevention of cyber espionage, malicious attacks, and information warfare.

4) Security in the financial industry: It can be used in the financial industry to safeguard the network security of banks, payment systems, and financial institutions. It detects and prevents network fraud, credit card fraud, hacker attacks, and other financial crimes.

In Section II, a review of prior research and methods related to network intrusion detection is provided. Traditional intrusion detection techniques, as well as machine learning and deep learning-based approaches, are introduced, and their advantages and disadvantages are discussed. In Section III, the architecture and working principles of the proposed GAN-CNN-BiLSTM model are presented. The functionality and interactions of each component are explained, highlighting the model's strengths and innovations. Section IV describes the experimental setup designed and executed in this study, showcasing the experimental results and performance evaluation. A comparison is conducted between the proposed model and other methods, analyzing the reliability and effectiveness of the results. Finally, the main findings and contributions of the paper are summarized in Section V, and prospects for further research are outlined.

II. Related Work

A. Related Study on Intrusion Detection Models

Intrusion detection generally consists of two steps: preprocessing and classification. Preprocessing technology, also known as feature selection technology, is a key technology in the process of intrusion detection. It can reduce the size of the original data, improve the training efficiency of the model and the accuracy of the classifier. According to whether feature selection is independent of classifier, feature selection methods can be divided into two categories: filtering and packaging. Filtering method is independent of classifier, and it carries out feature selection according to the statistical characteristics of original data. In traditional intrusion detection system, the original data needs to be sent to a classifier after preprocessing.

Because of the progress of artificial intelligence (AI) technology in intrusion detection system (IDS), detection methods based on AI, such as Decision Tree[4], Support Vector Machine (SVM)[5], CNN[6-8], Long Short-Term Memory (LSTM)[9-11] and Recurrent Neural Network (RNN)[12-13], are widely and effectively used in intrusion detection systems. Vinayakumar R et al. proposed an intrusion detection method in combination with CNN and LSTM, and the experimental result show that it performs better in all indicators than only using CNN or CNN-RNN [14]. Tetsushi Ohki, et al. proposed a dimensionality reduction technique in combination with information gain and principal component analysis (PCA), using support vector and other means to detect intrusions, and the experimental result shows that the mixed dimensionality reduction method is better than the single dimensionality reduction method[15]. Liu Yuefeng et al. proposed an intrusion detection method based on multi-scale CNN, which uses convolution kernel of different scales to extract the optimal features of data. This method not only converges quickly, but also improves detection accuracy [16]. Lirim Ashiku et al. used the DNN network for intrusion detection training, which is optimized on the basis of CNN and deepens the network structure to improve the detection accuracy [17]. Yin C L et al. proposed the use of RNN to build an IDS detection model for identification in consideration of the time series relationship for feature extraction, but for high-dimensional features, RNN is significantly incapable of feature extraction, resulting in poor model performance [18].

The research shows that these deep learning-based intrusion detection systems perform better when dealing with big data, but there are still some problems:

1) Outdated data set: Most of the previous intrusion detection research is based on KDD-CUP99 or NPL-KDD data set, which has a history of more than 20 years, and cannot reflect the current network situation well.

2) The data samples are unbalanced: Classification research usually pays more attention to improving the overall evaluation indicators of the model, such as accuracy, precision, etc., and ignores the classification of minority samples. But in the real network environment, these minority attacks will produce more damage and impact than the majority attacks. However, the current researches based on KDD-CUP99 and other datasets usually directly use the official training and testing samples, and few research works deal with the problem of data imbalance under the intrusion detection problem and the related solutions.

3) Feature learning is not comprehensive most of the previous studies are based on a single neural network: CNN can learn the spatial features in the data and extract the local features accurately, but it cannot learn the temporal features. RNN can extract temporal features in data and analyze long-term dependencies of information, but it cannot effectively extract spatial features. In addition, RNN can only learn the temporal characteristics of the data in a single direction, and does not fully consider the joint influence of the information before and after the traffic data on the current state.

Intrusion detection is being extensively studied because it is an important security guarantee not only for the traditional Internet, but also for the Internet of Things and other networks. However, most of the previous studies used traditional machine learning or simple deep learning, and the data sets used, such as KDD-CUP99 and NSL-KDD, are too old to reflect the current network traffic well, and it is difficult for traditional machine learning algorithms to deal with a large volume of data, therefore, this paper uses the large data set CIC-IDS 2017 containing the latest attacks to solve the problems in current research by a multiway method.

B. Related Study on Data Imbalance

Data imbalance means there are large quantitative gaps among different data categories. Deep learning algorithms can get the best result when there are similar quantities among categories, so data imbalance is one of the factors degrading the deep learning performance.

In order to solve the problem of imbalanced data, one idea is to start from the algorithm level, according to the defects of the algorithm in solving the imbalanced problem, combined with the characteristics of imbalanced data, the algorithm is improved to improve the ability of the algorithm to deal with imbalanced classification problems. The other is to start from the data level. Existing studies solve the problem of data imbalance mainly through random undersampling, random oversampling and SMOTE. Random oversampling will expand the data scale and prolong the training time, which is easy to fall into overfitting; random undersampling will blindly delete some data, influencing the classification accuracy; the samples generated by SMOTE have no diversity [19].

To improve the model performance by sampling and optimizing the data, Yan B, et al. used SMOTE technology to sample the NSL-KDD data sets, and compared the performance of the newly sampled data with some algorithms such as RF, SVM and Backpropagation Neural Network (BPNN) [20]. Min E X, et al. built a new network architecture on GAN to generate data against data imbalance [21]. However, it has been proven that GAN training may lead to gradient vanishing, making the generator output invalid and making the result poor.

Therefore, this paper proposes a method to solve the problem of data imbalance and generate higher-quality data sets via Generative Adversarial Networks (GAN), GAN is a new generative model, which learns the probability distribution of the target data sample to generate forged samples that are greatly similar to the target data sample. It is a new generative model that directly compares the distribution of forged samples and target samples for training and generation, and continuously generates forged samples that are as close as possible to the real sample by means of confrontation. It improves the generation quality of forged samples and effectively solves the problem of overfitting caused by the lack of training samples in the generation process of traditional generative models. Therefore, GAN has been applied to the generation of data in many fields and achieved good results, but it has not been applied to the imbalance problem of network intrusion detection data. Then, a classification model is built in combination with CNN and BiLSTM, and balanced

data sets are used for training to obtain a model which is more stable in training and gives better results.

III. Intrusion Detection Model based on GAN-CNN-BILSTM

Fig. 1 shows the structure of the GAN-CNN-BiLSTM model, as there is only a little abnormal data in intrusion detection, data distribution of the data sets used for intrusion detection is unbalanced. Thus this paper generates and expands the minor training samples with GAN to reduce the impact of imbalanced training samples on the detection accuracy. After the data set is balanced using GAN, the generated minor samples and the original data set are combined into a new data set with balanced sample distribution, and then the data set is normalized and other preprocessed. Finally, the data set is used to train the CNN-BiLSTM model and obtain the classified detection results.

A. Data Set Balance

Generative Adversarial Networks (GAN), a new regression generation model proposed by Goodfellow, et al in 2014, consists of Discriminative Network (D) and Generative Network (G), which are rivals, as Generative Network creates a new data instance while Discriminative Network evaluates the data authenticity, both try to outperform each other and thus gradually improve in this process [22]. GAN learns the probability distribution of the target data samples to generate fake samples highly similar to the target data samples, it is a generative model as it directly compares the distribution of the fake samples and the target samples to train and generate new ones, and fake samples which are as close as possible to real samples are continuously generated by confronting, improving the generation quality of fake samples and solving the problem of overfitting caused by insufficient training samples in traditional generative models. Its structure is a two-person zero-sum game, where one's gain is the other's loss.

If the convolution kernel setting of GAN is too small, the dependency in the data will not be obvious, while if the convolution kernel setting is too large, the computational efficiency will be degraded. Therefore, this paper intends to introduce an attention mechanism, which sets different weights for different parts of these vectors according to their importance, so as to sort the importance of information and quickly extract the key feature information. It not only saves model computation and storage but also enables the model to judge more accurately.

Fig. 2 shows the structure diagram of a GAN model with added attention mechanism. Real data is the real data of the data set, and generated data is the data generated by G. Random noise can make the network random and generate distribution, so that it can be sampled. In the training process of GAN, G and D are continuously optimized and enhanced, as G is to make D unable to distinguish while D is to enhance its ability to judge the authenticity of the data through continuous improvement, and the principle can be expressed as formula (1):

$$\min_G \max_D V(D,G) = E_{x\sim P_{data}(x)}[lnD(x)] + E_{z\sim P_z(z)}\left[ln\left(1-D\left(G(z)\right)\right)\right] \quad (1)$$

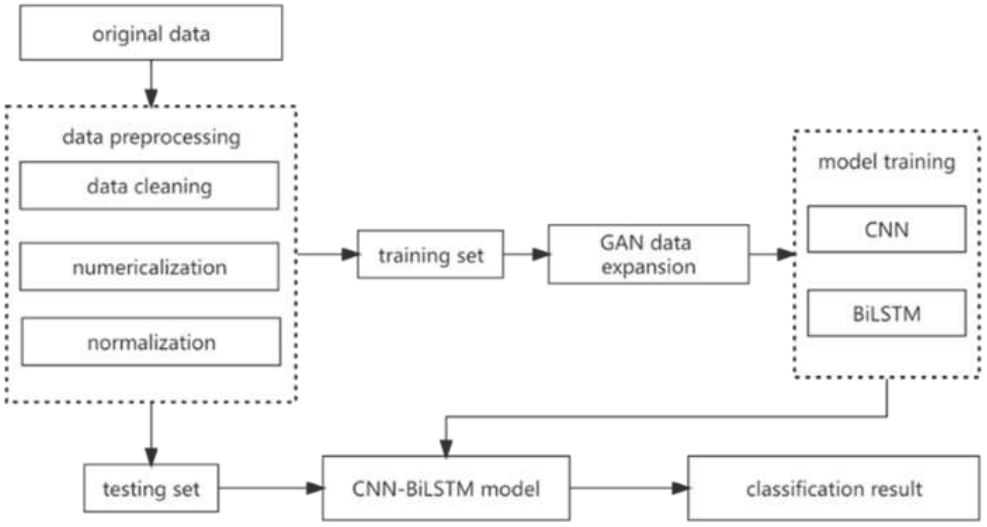

Fig. 1. Flow Chart of intrusion detection model based on GAN-CNN-BILSTM.

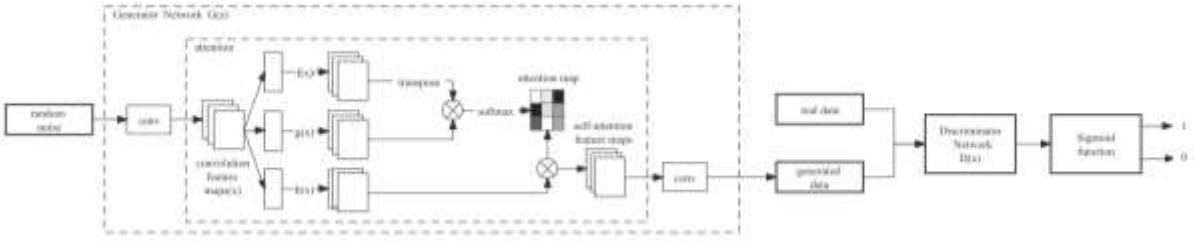

Fig. 2. Structure diagram of a GAN model with added attention mechanism.

In the formula, V(D, G) is the objective function, P_{data} is the real sample distribution, P_z is the generated sample distribution, D(x) is the probability of x being the real sample, and G(z) is the sample generated by model G based on the input z.

After the convolution processing in the attention mechanism module of the model, the resulting convolution feature vector X serves as input. The processing shown in formulas (2) to (4) is then applied to obtain $f(x)$, $g(x)$, and h(x) with different output channel sizes, where W_f, W_g, and W represent weight matrices trained through different methods. Next, $f(x)$ is transposed and multiplied by $g(x)$ using formula (5). Finally, an attention map is obtained after Softmax processing.

$$f(x) = W_f x \tag{2}$$

$$g(x) = W_g x \tag{3}$$

$$h(x) = W\ x \tag{4}$$

$$s_{ij} = f(x_i)^T g(x_j) \tag{5}$$

Next, $h(x)$ is used to perform pixel-by-pixel multiplication with the obtained attention map, resulting in the feature map of adaptive attention. Eq. (6) is used to compute the attention weights, where $\beta_{j,i}$ represents the degree of influence of the model on the ith position when synthesizing the JTH region. Then, Eq. (7) is used to obtain the attention feature map. Finally, the feature map with attention mechanism is combined with the feature vector X using formula (8) to obtain the feature map with attention mechanism.

$$\beta_{j,i} = \frac{\exp(s_{ij})}{\sum_{i=1}^{N} \exp(s_{ij})} \tag{6}$$

$$o_j = \sum_{i=1}^{N} \beta_{j,i} h(x_i) \tag{7}$$

$$y_i = \gamma o_j + x_j \tag{8}$$

The main process of GAN model training is shown in Algorithm 1.

Algorithm 1: GAN model training algorithm

Input: normal traffic T_{normal}, attack traffic T_{attack}, noise N

Output: GAN model, trained generator G and discriminator D

Initial generator G,Discriminator D,Deep Intrusion Detection System CNN-BiLSTM

for i = 0,1,2,do

  for G-steps do

    attention model generate attention weights.

    G generates the malicious traffic examples based on T_{attack}

    Update the parameters of G

  end for

  for D-steps do

    D classifies the training set including T_{normal} and G(T_{attack},N)

    D classifies the training set , getting predicted labels

    Update the parameters of D

  end for

end for

B. CNN-BiLSTM Model

Convolutional Neural Networks (CNN), belong to a multi-layer supervised learning neural network, consists of the input layer, the convolutional layer, the pooling layer, the fully connected layer and the output layer. A CNN model can be composed of multiple convolutional layers, pooling layers and fully connected layers, and the convolutional layer and the pooling layer generally appear alternately. The pooling layer is usually followed by the fully connected layer and the output layer is usually followed by the fully connected layer, or the classification layer in other words. Classification is realized by logistic regression, Softmax regression or even a SVM, and the features extracted by the CNN, which is the result of the classification, are classified and output by the output layer. The loss function takes the gradient descent to reversely regulate the weight parameters in the neural network layer by layer at minimum, and improves the accuracy of the network through continuous training. CNN can extract and classify features in the meantime, so that feature classification can effectively use feature extraction; weight sharing can effectively reduce the training parameters, making the neural network structure simpler and more adaptable, and Fig. 3 shows its structure.

For Bidirectional Long Short-Term Memory (BiLSTM), the Long Short-Term Memory (LSTM) is a variant of traditional RNN, but the structure of LSTM, which is more complex, can be divided into four parts for interpretation: forget gate, input gate, cell state and output gate. Compared with the classical RNN, the gate structure of LSTM can effectively capture the semantic correlation between long sequences and alleviate gradient disappearance or explosion. BiLSTM is composed of forward LSTM and backward LSTM, which enhances the LSTM and improves the performance of the model. It trains two LSTMs on the input data, the first LSTM is on the original data and the other is on the reversed data so that more features are added to the network, the result is obtained faster, and the defect of gradient vanishing is eliminated. Fig. 4 shows the structure of BiLSTM.

BiLSTM needs to calculate the output according to the time sequence, if the distance between the interdependent features is too far, it will take several time steps to accumulate information and connect the two, and with the increase of the distance, the possibility of capturing effective information will gradually decrease. However, the self-attention mechanism will connect any two words directly through a calculation result, which shortens the distance between long-distance dependent features and is conducive to the effective use of these features. Therefore, this paper adds a self-attention mechanism to BiLSTM to improve the efficiency of the model.

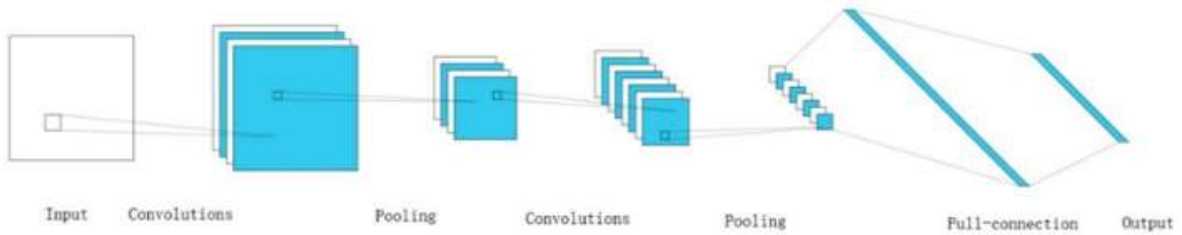

Fig. 3. Model of CNN.

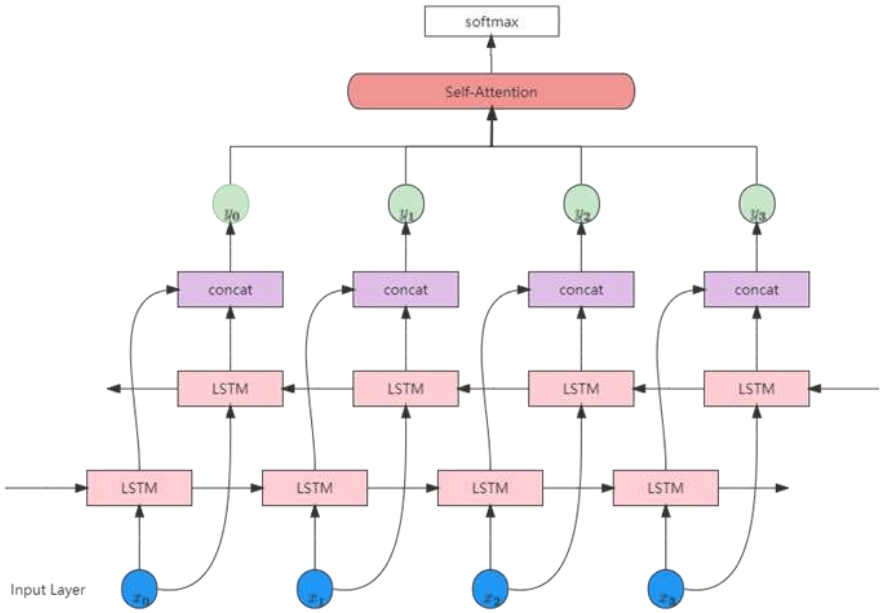

Fig. 4. Model of BILSTM.

IV. Experiment and Result Analysis

A. Experimental Environment

In order to verify the intrusion detection model in this paper and build a simulation experiment environment, the Pytorch 10.2 deep learning framework is used to build the model in Pycharm, and data are processed by Python 3.6; the operating system is 64-bit Windows 10, the CPU is Intel core i5-7300HQ 2.50 GHz, and the memory is 16 GB DDR.

B. Data Set

The data set used in this paper is CIC-IDS-2017, which contains normal data similar to real data and the latest attacking data. The information of this data set, which contains a large number of network intrusion traffic data, can better reflect the current network environment, and the training set and test set are adjusted to improve the test result in the complex network environment at present, 80% was randomly selected as the training set and 20% as the test set. This data set contains benign and recent common attacks, similar to real-world data (PCAPs). It also includes the result of network traffic analysis by CICFlowMeter, using tagged flows based on timestamp, source and destination IP, source and destination port, protocol and attacks (CSV file), and a data set containing 15 class labels (1 normal label + 14 attack labels). Table I lists the volumes of various attack data:

TABLE I. CIC-IDS-2017 Dataset

Attack Type	Number of Instances
BENIGN	2359087
FTP-Patator	7938
SSH-Patator	5897
DDos	41835
Dos Hulk	231072
Dos GoldenEye	10293
Dos slowloris	5796
Dos Slowhttptest	5499
WebAttack-Brute Force	1507
Web Attack-XSS	652
WebAttack-SQL Injection	21
Bot	1966
Infiltration	36
PortScan	158930
Heartbleed	11

C. Data Preprocessing

1) Data cleaning: The missing values in this dataset all appear under the Flow Bytes/s feature. When dealing with the problem of missing data, methods such as deletion, completion and imputation are usually used. Since the dataset is very large and the missing ratio is small, this paper uses the tuple deletion meth-od to delete the data rows with missing values. Infinite values exist under the features Flow Bytes/s and Flow Pkts/s. During data processing, the infinity value cannot be calculated properly. The infinite values of this data set basically appear in normal traffic and have no effect on classification. Therefore, the information lines containing infinite values are directly deleted. Duplicate data is hardly helpful to the training of intrusion detection system, therefore, only the first occurrence of data is kept and the duplicate data is removed. When the data set is recorded, the table header information is mistakenly written into the data multiple times, and it is directly deleted here to ensure that the data is comprehensive, clean, and error-free.

2) Numericalization of character-type features: Convert character attributes in the data set to binary features. This is a crucial step in many machine learning tasks as most algorithms cannot work directly with non-numeric data. In the context of intrusion detection, many datasets contain character-based features such as protocol types, service types, or flag values. These features are often categorical in nature, meaning that they take on a limited number of distinct values. To turn these categorical features into numerical ones, one common technique is to use binary encoding. By converting categorical features into binary features, we can ensure that all features in the dataset are numerical, which is necessary for most machine learning algorithms. This process also helps to reduce the impact of bias on the algorithm's results and increase the accuracy of the model. Overall, numericalization of character-type features is an important step in preprocessing data for intrusion detection and other machine learning tasks. It helps to ensure that the data is ready for use with a variety of algorithms and can improve the performance of the model.

3) Normalization processing: Normalization is an essential preprocessing step in machine learning, which involves scaling the features of a dataset to a standardized range. This is necessary because different features often have different scales or units, which can lead to biased predictions or overemphasis on certain features. In intrusion detection, normalization is particularly important due to the diverse nature of network traffic data. The min-max normalization method is a popular technique for scaling data to a standardized range. It involves scaling the values of each feature to a range of [-1, 1], based on the minimum and maximum values of that feature in the dataset. This normalization method preserves the relative distances between values within a feature and ensures that all features have equal influence on the learning process. The advantage of the min-max normalization method is that it is simple and easy to implement, and it maintains the original information and structure of the data. It also helps to prevent the model from being overly influenced by outliers or extreme values. The min-max formula is shown in Eq. (2), where max represents the maximum value of each feature, and min represents the minimum value.

$$y_i = \frac{x_i - Min}{Max - Min} \tag{9}$$

D. Parameter Setting

In the model of this paper, the parameters of GAN were set as batch-size 50, epoch 500 and learning rate 0.001, the Relu function is selected as the activation function and the Adam optimizer is used for the model. The convolution layer and pooling layer of CNN have two layers respectively. The initial parameters of CNN include convolution kernel size set to 3, activation function set to the Relu function, pooling layer size set to 2 and fully connected layer size set to 16, and a Dropout layer is added to avoid overfitting. In the BiLSTM network of this paper, the output size is set to 10, the features extracted by CNN and BiLSTM are fused in parallel, the fused features are added into the self-attention layer, and different weights are assigned to different features.

E. Measurement Indicators

In this paper, Accuracy, Precision, Recall and F-score are mainly used to evaluate the models.

Accuracy: It represents the proportion of samples that are correctly predicted by the model, providing an overall measure of classification or prediction accuracy.

Precision and Recall: Precision and recall are commonly used in binary or multi-class classification problems. Precision measures the proportion of true positive predictions among all samples predicted as positive, while recall measures the proportion of true positive samples correctly identified by the model.

F1 Score: The F1 score is a metric that combines precision and recall, calculated as the harmonic mean of precision and recall. It provides a balanced measure of model performance, giving equal weight to precision and recall. It is particularly useful for imbalanced datasets and classification tasks.

So as to evaluate the detection performance of different models, as below:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{10}$$

$$Precision = \frac{TP}{TP+FP} \tag{11}$$

$$Recall = \frac{TP}{FN+TP} \tag{12}$$

$$F-score = \frac{2TP}{2TP+FP+FN} \tag{13}$$

Where, TP is the quantity of correct traffic, TN is the quantity of normal traffic in correct judgment, FP is the quantity of normal traffic in incorrect judgment, and FN is the quantity of incorrect traffic in incorrect judgment.

F. Results

In order to analyze the influence of the expanded data set on the detection accuracy, GAN is used to expand the minor

classes in the training set in different percentages: 0%, 40%, 80% and 120%, and the results are shown in Table II, indicating that the accuracy rate is the highest when the expansion percentage is 80%, so the expansion percentage in this experiment is 80%.

In order to illustrate the effects of the models proposed in this paper, CIC-IDS-2017 data sets were selected for experiments, and CNN, RNN, BiLSTM and CNN-BiLSTM were used for comparative experiment. Common intrusion detection algorithms such as SVM, NBM, Decision Tree and Random Forest are applied to the data set in this experiment for comparison. The results are shown in Table III and Fig. 5 shows the accuracy of the deep learning algorithm

TABLE II. THE ACCURACY OF DIFFERENT EXPANSION RATIO

data expansion ratio	Web Attack-XSS（ACC）	Web Attack-SQL Injection (ACC)	Infiltration (ACC)	Heartbleed (ACC)	Total (ACC)
0%	62.08	63.57	60.26	58.49	92.15
40%	65.27	67.08	64.92	63.64	95.03
80%	67.25	68.74	66.21	68.49	96.53
120%	65.83	67.72	65.35	65.83	95.76

TABLE III. MODEL COMPARISON

Model	Evaluation Index (%)			
	Accuracy	*Precision*	*Recall*	*F-score*
CNN	93.74	92.52	93.47	92.45
RNN	83.65	81.73	82.77	82.76
SVM	61.37	61.21	60.75	61.46
NBM	79.85	83.36	78.52	77.94
Decision Tree	84.63	85.27	84.32	84.49
Random Forest	86.26	87.48	87.27	87.64
BiLSTM	93.06	91.75	92.52	93.26
CNN-BiLSTM	94.51	93.37	92.78	94.21
GAN-CNN-BiLSTM	96.32	96.55	95.38	96.04

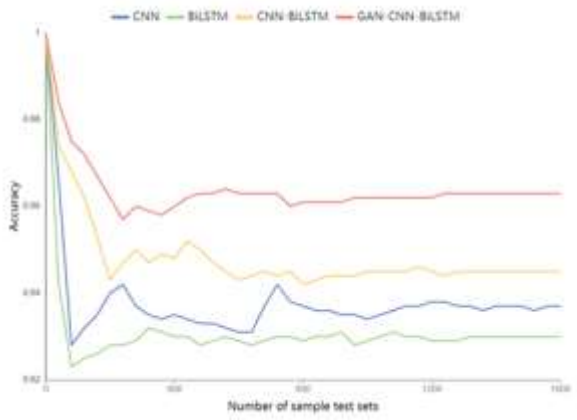

Fig. 5. Algorithm accuracy comparison.

The study compared the performance of the proposed GAN-based data expansion method with several common models such as CNN, BiLSTM, SVM, NBM, and Random Forest. The results indicated that the accuracy of the GAN-based model was significantly higher than that of CNN and BiLSTM by 2.58% and 3.26%, respectively. The accuracy of the GAN-based model was also 1.81% higher than that of CNN-BiLSTM. Additionally, the performance of some classic models such as SVM and NBM were not satisfactory, whereas the Random Forest model performed better than these models.

However, the GAN-based model outperformed all these models in terms of accuracy. The proposed model based on CNN-BiLSTM and GAN was able to solve the problem of imbalanced dataset and achieved an accuracy improvement of 10.06%. This improvement proved the effectiveness and innovation of the proposed model. Therefore, it can be concluded that the GAN-based data expansion method is a promising approach for improving the performance of intrusion detection systems. It is expected to have significant implications for the development of future intrusion detection techniques.

V. CONCLUSION

This paper proposes a novel model called GAN-CNN-BiLSTM, which aims to enhance the performance of intrusion detection. The main challenge in intrusion detection is the class imbalance problem, where the normal class dominates the data set, while the abnormal class is relatively small. To address this issue, GAN is introduced to expand the size of the abnormal class, CNN-BiLSTM is adopted for feature extraction and classification, and the CIC-IDS 2017 data set is utilized for evaluation. The proposed model is compared with other traditional models, and the experimental results demonstrate that GAN can effectively eliminate the class imbalance problem, and the CNN-BiLSTM model outperforms other models in terms of accuracy.

Although the proposed model uses a widely adopted data set, it has not been tested in a real network environment. Collecting large-scale, high-quality data and annotating it in real-world environments is a challenging task. Data privacy and security are crucial. Transferring models from the lab to real environments requires considering adaptability and generalization. Real-world data has greater variations and noise, requiring the model to maintain good performance. To overcome these challenges, reasonable data collection and processing methods are needed, ensuring dataset diversity and representativeness. Data privacy and security measures must be in place to protect the data. Model optimization is necessary, including fine-tuning, regularization, and parameter adjustment in real environments, to improve generalization. Future research will focus on exploring and improving the model by utilizing larger and more diverse data sets, and optimizing the intrusion detection model. This will enable the model to be tested in a real network environment, and validate its performance for real-world applications of network intrusion detection. The GAN-CNN-BiLSTM model's enhancements in intrusion detection bolster the identification and defense against network attacks. Its impact includes improved network security for critical infrastructure,

companies, and government institutions, minimizing risks and losses from threats. The study showcases the efficacy of multimodal data processing and deep learning in intrusion detection, providing valuable insights for future research. The integrated model's design and optimization offer new directions for further advancements in intrusion detection.

REFERENCES

[1] Zhang Hao, Zhang Xiaoyu, Zhang Zhenyou, Li Wei. A review of Intrusion detection models based on Deep Learning [J]. Computer Engineering and Applications,2022,58(06):17-28.doi: 10.3778/j.issn.1002-8331.2107-0084.

[2] K. Zheng, Z. Cai, X. Zhang, Z. Wang, and B.Yang, ‘‘Algorithms to speedup pattern matching for network intrusion detection systems,’’ Comput. Commun., vol. 62, pp. 47–58, May 2015.doi: 10.1016/j.comcom.2015.02.004.

[3] NIKOLOVA E , JECHEVA V.Some similarity coefficients and application of data mining techniques to the anomaly-based IDS[J].Telecommunication Systems,2012,50(2):127-135.doi: 10.1007/s11235-010-9390-3.

[4] Jing X . Innovative Two-Stage Fuzzy Classification for Unknown Intrusion Detection. 2016.doi: 10.25148/etd.FIDC000288.

[5] Ahmim A, Maglaras L, Ferrag M A, et al. A Novel Hierarchical Intrusion Detection System Based on Decision Tree and Rules-Based Models[C]// 1st International Workshop on Security and Reliability of IoT Systems - SecRlot 2019.doi: 10.1109/dcoss.2019.00059.

[6] Vinayakumar R, Soman K P, Poornachandran P . Applying convolutional neural network for network intrusion detection[C]// 2017 International Conference on Advances in Computing, Communications, and Informatics (ICACCI). 2017. doi: 10.1109/icacci.2017.8126009.

[7] Y. Xiao, C. Xing, T. Zhang, and Z. Zhao, "An Intrusion Detection Model Based on Feature Reduction and Convolutional Neural Networks," in IEEE Access, vol. 7, pp. 42210-42219, 2019,doi: 10.1109/access.2019.2904620.

[8] Naseer S, Saleem Y . Enhanced Network Intrusion Detection using Deep Convolutional Neural Networks[J]. KSII Transactions on Internet and Information Systems, 2018, 12(10):5159-5178.doi: 10.3837/tiis.2018.10.028.

[9] Wang Zhu, ZHAO Jianxin, ZHANG Hongying, LI Yajun, Leng Dan. Intrusion Detection Algorithm based on Hybrid Model of VDCNN and LSTM [J]. Fire Control & Command Control,2022,47(02):170-175. doi:10.3778/j.issn.1002-8331.2107-0084.

[10] Imrana Y, Xiang Y, Ali L, et al. A bidirectional LSTM deep learning approach for intrusion detection[J]. Expert Systems with Applications, 2021, 185(8):115524.doi: 10.1016/j.eswa.2021.115524.

[11] Poornachandran P , Vinayakumar R , Soman K P . A Comparative Analysis of Deep Learning Approaches for Network Intrusion Detection Systems (N-IDSs): Deep Learning for N-IDSs[J]. International journal of digital crime and forensics, 2019, 11(3):65-89.doi: 10.4018/ijdcf.2019070104.

[12] Yan B, Han G . LA-GRU: Building Combined Intrusion Detection Model Based on Imbalanced Learning and Gated Recurrent Unit Neural Network[J]. Security and Communication Networks, 2018, 2018:1-13.doi: 10.1155/2018/6026878.

[13] Chaibi N, Atmani B, Mokaddem M . Deep Learning Approaches to Intrusion Detection: A new Performance of ANN and RNN on NSL-KDD[C]// ISPR '20: The international conference on Intelligent systems and Pattern recognition. 2020.doi: 10.1145/3432867.3432889.

[14] Vinayakumar R, Soman K P, Poornachandran P . Applying convolutional neural network for network intrusion detection[C]// 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI). 2017.doi: 10.1109/icacci.2017.8126009.

[15] T. Ohki, V. Gupta and M. Nishigaki, "Efficient Spoofing Attack Detection against Unknown Sample using End-to-End Anomaly Detection," 2019 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), 2019.doi: 10.1109/apsipaasc47483.2019.9023183.

[16] Liu Yuefeng, Wang Cheng, Zhang Yabin, Yuan Jianghao. Multi-scale convolution CNN model for Network Intrusion Detection [J]. Computer Engineering and Applications,2019,55(03). doi:10.3778/j.issn.1002-8331.1712-0021.

[17] Ashiku L, Dagli C . Network Intrusion Detection System using Deep Learning[J]. Procedia Computer Science, 2021, 185(1):239-247.doi: 10.1016/j.procs.2021.05.025.

[18] Yin C L, Zhu Y F, Fei J L, et al. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks[J]. IEEE Access, 2017, PP(99):1-1.doi: 10.1109/access.2017.2762418.

[19] Soltanzadeh P, Hashemzadeh M. RCSMOTE: Range-Controlled synthetic minority over-sampling technique for handling the class imbalance problem[J]. Information Sciences, 2021, 542: 92-111.doi: 10.1016/j.ins.2020.07.014.

[20] Yan B H, Han G D, MD Sun, et al. A novel region adaptive SMOTE algorithm for intrusion detection on imbalanced problem[C]// 2017 3rd IEEE International Conference on Computer and Communications (ICCC). IEEE, 2017.doi: 10.1109/compcomm.2017.8322749.

[21] Min E, Long J, Qiang L, et al. TR-IDS: Anomaly-Based Intrusion Detection through Text-Convolutional Neural Network and Random Forest[J]. Security & Communication Networks, 2018, 2018:1-9.doi: 10.1155/2018/4943509.

[22] Lee J H, Park K H . GAN-based imbalanced data intrusion detection system[J]. Personal and Ubiquitous Computing, 2019(9).doi: 10.1007/s00779-019-01332-y.