# Research on Network Intrusion Detection Technology Based on DCGAN

Wang Chao[1], Wang Wenhui[2,3], Dong Jiahan[1], Guo Guangxin[1]
1. State Grid Beijing Electric Power Company, Beijing, China
2. Global Energy Interconnection Research Institute, Beijing, China
3. State Grid Key Laboratory of Information & Network Security, Beijing, China
29681987@qq.com

2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) | 978-1-7281-8028-1/20/$31.00 ©2021 IEEE | DOI: 10.1109/IAEAC50856.2021.9390891

***Abstract*—Traditional network intrusion detection algorithms tend to lack learning in a small number of classes due to data imbalance. In reality, intrusion detection systems pay more attention to the detection accuracy of a small number of classes, that is, attack samples. In order to improve the detection accuracy of intrusion detection system, a network intrusion detection method based on deep convolution generative adversarial networks (DCGAN) was proposed. Firstly, the sample data of network intrusion is preprocessed, and the character data set is replaced by image data. Then, DCGAN is used to train and test the sample data. Both the generator and the discriminator are constructed by CNN. The generator is used to construct attack samples, balance the number of training samples, and solve the over fitting problem caused by insufficient training samples. Finally, the trained discriminator is used to test the classification accuracy of samples. Experimental results show that, compared with the traditional algorithm, the proposed algorithm can not only balance the detection accuracy of various types of samples, but also has higher detection accuracy for attack samples.**

***Keyword—Intrusion detection; DCGAN; CNN; Data preprocessing***

## I. INTRODUCTION

With the development of Internet technology, a variety of network attacks and illegal intrusions are common, and the attack means are more and more complex. How to effectively and quickly identify various network attacks has become an urgent problem in network information security. Network intrusion detection is an active security technology. By detecting and monitoring network traffic in real time, it can effectively sense network attacks and provide response decisions for security managers.

With the continuous upgrading of hacker attacks and the massive network data, the traditional machine learning method is no longer suitable for new network intrusion detection scenarios. In recent years, big data, deep learning and other technologies have been widely used, and have achieved great success in natural language processing, image recognition, video detection and other fields. In addition, with the development of computing hardware and the improvement of computing power, the deep learning neural network model is gradually moving from theory to application, and has achieved good application in intrusion detection[1~3]. A hybrid intrusion detection method based on clustering and genetic algorithm is proposed in the paper [4]. The method uses unsupervised algorithm and does not use the sample label information, so the detection performance is easy to reach the upper limit. In the paper [5], harmony search algorithm is used to optimize BP neural network, and applies it to network intrusion detection. Experiments show that the method is excellent in the field of intrusion detection, but it has low robustness, low convergence speed and long training time when dealing with massive data. In the paper [6], an intrusion detection method based on multi-scale convolution neural network is proposed, which uses convolution kernel of different scales to extract the optimal features of data. This method not only has fast convergence speed, but also can improve the detection accuracy.

The above-mentioned deep learning algorithms have achieved good results in the field of network intrusion

detection technology, but the related algorithms do not consider the actual situation, it is difficult to obtain attack samples for training and learning. However, deep learning algorithms usually require a high amount of sample data. In the case of imbalanced sample sets, it is easy to reduce the classification and recognition accuracy of deep learning algorithm, especially the identification accuracy of attack samples. For the classification problem of imbalanced samples, the usual solutions are based on sample resampling and based on improved algorithm. Based on DCGAN algorithm, the generator is used to generate fake samples similar to real attack samples, which can meet the needs of training sample set, improve the quality of training samples, and avoid the over fitting problem caused by insufficient training samples. In addition, the character network intrusion samples are transformed into image samples in advance, and the convolution neural network algorithm features are used for accurate learning and classification to improve the recognition accuracy of network intrusion detection test samples.

## II. DCGAN PRINCIPLE

DCGAN is improved on the basis of the original GAN [7]. The application of deep convolution neural network in generative adversarial networks greatly improves the stability of training and the quality of generated images. Compared with GAN, the main improvements of DCGAN include: (1) removing all pooling layers; (2) except for the first layer of the generator and the last layer of the discriminator, the full connection layer is no longer used; (3) except for the output layer of the generator and the input layer of the discriminator, the batch normalization operation BN is used in other places; (4) modification of activation function. According to the above improvements, the DCGAN generator structure is constructed as shown in Figure 1. In the figure, the generator is composed of a full connection layer and a four-layer deconvolution network. The input is still random noise, which is expanded and reshaped into a 4×4×1024 feature map through the first layer, and then the generated image of 64×64×3 is obtained through the four-layer conv network. In the figure, conv represents a one-layer network structure, which includes transposition convolution, batch normalization and activation function.

The structure of discriminator is symmetrical with that of generator, but the convolution layer of discriminator adopts forward convolution. The output of the input image is the probability of judging whether it belongs to the real sample or the fake sample. The structure of the generator shown in the Fig.1 is not fixed. For different data sets and different generation requirements, the structure can be changed accordingly. Otherwise, the generated results may be biased, and the discriminator is the same.

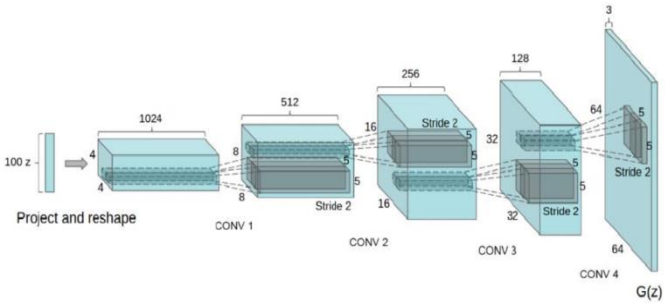


Fig.1. The structure of DCGAN generator

## III. THE ARCHITECTURE OF INTRUSION DETECTION SYSTEM

The architecture of intrusion detection system is based on the idea of generative adversarial networks, and the architecture model is shown in Fig.2. Firstly, the data preprocessing module is used to obtain training samples and test samples, and then generator G and discriminator D are used for training and testing. The algorithm model is composed of convolution neural network. The generator is used to generate attack training samples and balance training samples. The discriminator realizes the accurate classification of training samples through continuous iteration, and finally completes the Nash equilibrium between generator G and discriminator D, forming the classification model needed by intrusion detection.

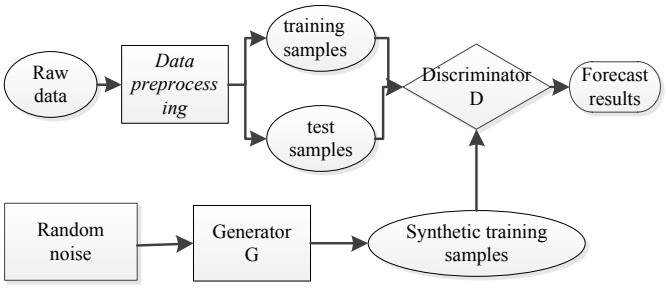


Fig.2. The architecture of intrusion detection system

### A. The Steps of Intrusion Detection

The steps of intrusion detection are divided into training stage and testing stage.

The training stages are as follows:

Step1: The original intrusion detection data is preprocessed to obtain training samples;

Step2: The generator G is used to obtain the synthesized training samples, which are mainly attack samples in intrusion detection;

Step3: The discriminator D was used to classify and identify training samples and synthetic training samples;

Step4: If the discriminator D can effectively predict the discriminating training samples and meet the accuracy requirements, the training will be terminated, otherwise step 1 will be executed again.

The test stages are as follows:

Step1: The original intrusion detection data is preprocessed to obtain the test samples;

Step2: The discriminator D was used to classify and identify the test samples, and the test results were obtained.

### B. Data Preprocessing

The purpose of data preprocessing is to convert the original character data into image data that CNN can process. The data preprocessing process mainly includes three parts: numeralization, normalization and image conversion.

1) Numeralization. Through numerical processing, the common character data in the original data of intrusion detection can be converted into numerical data. If the value of the characteristic character type is converted to integer data and the feature character type is n, the value of the numerical value can be mapped into (1, 2 ,n).

2) Normalization. In order to avoid the dimensional difference of the numerical data, it is necessary to normalize the numerical data. The maximum - minimum normalization method is used to normalize the data in the data set to the interval of [0,1]. For the original data $x$, $x_{min}$ is the minimum value of the current attribute in the dataset, and $x_{max}$ is the maximum value of the current attribute in the dataset, then the normalized data is obtained.

$$x^* = \frac{x - x_{min}}{x_{max} - x_{min}} \quad (1)$$

### C. DCGAN Loss Function

In the process of DCGAN training, the purpose is to maximize the accuracy of D to judge whether the input samples are from real data or generated samples, and to maximize the degree of the sample data generated by G approaching the real data. Therefore, the training problem of G and D is transformed into the minimization problem of the evaluation function V(G, D). After training, the random noise Z is input into G to start learning model parameters. At this time, the probability of sample data generated by G after discrimination D is 1, and the mathematical model is D(G(z)) =1, that is, 1−D(G(z)) =0, that is, the minimum model G. When model D is trained, if the input sample data is real data, the expected target is that the probability after discrimination D is 1, and the mathematical model is D(x) =1; if the input sample data is forged data, the probability after discrimination D is expected to be 0, that is, D(G(z)) =0 , so 1−D(G(z)) =1, thus maximizing model D. However, DCGAN is composed of generator model and discriminator model. In the discriminator model, the loss function is as follows:

$$\max_D V(D,G) = E_{x\sim P_{data}}[\lg(D(x))] + E_{z\sim P_g(z)}[1 - \lg(\mathrm{D}(\mathrm{G}(\mathrm{z})))] \quad (2)$$

Where $P_{data}$ is the real data distribution and $P_g(z)$ is the noise distribution. In the actual training, the model G and D are updated alternately. First, fix G to train D, update the parameters of D model, then update the network parameters of iterative G model, and repeat the process until the adversarial

network is stable.

In formula (2), the former term is the result of real sample discrimination, and the latter term is the result of generated sample. The closer the former item is to 1, the better, while the latter is the closer to 0, the better. Therefore, the final expected result is close to 1, so logarithmic function was added to get the prototype of discriminator loss function. Like the discriminator model, the generator loss function is obtained as follows:

$$\min_G V(D,G) = E_{z\sim P_g(z)}[1 - \lg(D(G(z)))] \quad (3)$$

## IV. EXPERIMENTAL ANALYSIS

### A. Experimental Data

The more widely used data sets in intrusion detection are KDDCUP 99 and NSL-KDD [8]. The KDDCUP99 dataset contains a large number of redundant records, which will affect the detection results. The NSL-KDD data set is an optimized version of the KDDCUP 99 data set. The training set and test set do not contain duplicate records, so a better quality NSLKDD data set was selected. Each record in the NSL-KDD dataset is a join vector containing 41 features and 1 label. The NSL-KDD dataset consists of four sub-datasets: KDDTrain+, KDDTrain+_20Percent, KDDTest+ and KDDtest-21. Two sub-sets of KDDTrain+ and KDDTest+ were used for training test, as shown in TABLE I. It can be seen from the table that the number of Normal sample types in KDDTrain+ sub-data set is 67345, while the U2R type of attack sample is only 52, with a sample size ratio of 1295 times. It can be seen that the number of Normal samples and attack samples is extremely imbalanced.

TABLE I. THE PSNR, SSIM AND FSIM SCORES OF COMPARED METHODS

| Type / Sub-sets | Normal | Dos | Probe | U2R | R2L |
|---|---|---|---|---|---|
| KDDTrain+ | 67345 | 45926 | 11655 | 52 | 995 |
| KDDTest+ | 9711 | 7458 | 2421 | 200 | 2754 |

### B. Experimental Setup

The host configuration used in the experiment is Intel Core i7-9750H CPU, NVIDIA GeForce GTX1040Ti GPU, windows 10 system and 16GB RAM. The code is developed and implemented with Python 3.5. The construction of common exception detection algorithm models is based on the open source Pyod library. Tensorflow 2.0 is used in deep learning framework.

The input layer of the discriminator is the real data samples and the false samples generated by the generator. The input layer of the generator is designed as 41 dimensional random noise data to generate forged attack sample data. CNN consists of two hidden layers, the sizes of the two convolution kernels are 10 × 1 × 3 and 20×1×5, respectively. The convolution step size of the two convolution layers is 1.

### C. Experimental Result

The experimental results were compared with common deep learning algorithms RNN[9], BPNN[5] and CNN[10]. The results are shown in Fig.3. It can be seen from the figure that, compared with RNN, BPNN and CNN deep learning algorithms, the overall detection accuracy of intrusion detection algorithm based on DCGAN is improved by 5.2%, 9.8% and 2.4%, respectively, which is obviously better than other algorithms. Especially for Dos, Probe, U2R, R2L and other small types of attack samples, the detection accuracy is higher. To a certain extent, the detection false alarm rate of normal samples is improved, but the missed detection rate of intrusion detection system is reduced, and the overall detection accuracy of intrusion detection system is improved.

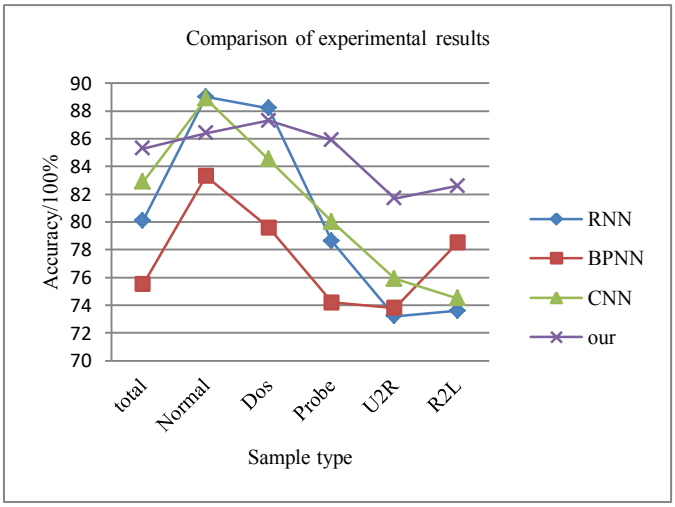


Fig.3. Comparison of experimental results

## V. CONCLUSION

An intrusion detection algorithm based on DCGAN was proposed to solve the problem of low detection rate caused by imbalanced sample training in intrusion detection. The method uses the generator to generate attack samples which belong to a small number of samples and balance the training sample set. The experimental results show that compared with the traditional deep learning algorithm, the proposed algorithm can improve the detection accuracy of attack samples, reduce the missing rate and improve the overall detection accuracy of intrusion detection system. In the next step, we will continue to optimize the structure of the generation network and the number of generated samples to make the distribution of generated samples closer to the distribution of real samples, improve the detection performance of the discriminator, and further improve the detection accuracy of attack type samples.

## REFERENCE


[1] QING S H, JIANG J C, M A H T, et al. Research on intrusion detection technique : a survey[J]. Journal on Communications, 2004, 25(7):19-29.

[2] Chong Zhou and Randy C. Paffenroth. Anomaly detection with robust deep autoencoders. Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 665-674, 2017.

[3] Liu Y, Li Z, Zhou C, et al. Generative adversarial active learning for unsupervised outlier detection[J]. IEEE Transactions on Knowledge and Data Engineering, 2019.

[4] Chakrabarty B, Chanda O,Islam S. Anomaly based intrusion detection system using genetic algorithm and K-centroid clustering[J]. International Journal of Computer Applications, 2017, 163(11):13-17.

[5] DING Hong-wei, WAN Liang, DENG Xuan-kun. Optimizing intrusion detection of BP neural networks by a modified harmony search algorithm[J]. Computer Engineering& Science, Vol,41, No.1,2019.

[6] LIU Yuefeng1, WANG Cheng, ZHANG Yabin, YUAN Jianghao. Multiscale Convolutional CNN Model for Network Intrusion Detection[J]. Computer Engineering and Applications, 55(3),2019.

[7] GOODFELLOW I, BENGIO Y, COURVILLE A. Deep Learning [M]. Cambridge, UK: MIT Press, 2016:23-34.

[8] Revathi S, Malathi A. A detailed analysis on NSL-KDD dataset using various machine learning techniques for intrusion detection[C]. Proceedings of International Journal of Engineering Research & Technology, 2013:1350-1351.

[9] YIN C,ZHU Y,FEI J, et al. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks [J] .IEEE Access, 2017, 5(99):21954-21961.

[10] DING Hong-wei, WAN Liang, ZHOU Kang, LONG Ting-yan, XIN Zhuang. Study on Intrusion Detection Based on Deep Convolution Neural Network[J]. COMPUTER SCIENCE, Vol.46, No.10 , 2019.