Academic Journal of Science and Technology
ISSN: 2771-3032 | Vol. 3, No. 3, 2022

Research on Network Intrusion Detection Based on an Improved Deep Learning Method

Le Yang [1], Hua Chen[2, *]

[1] Foshan Network Security Emergency Command Center, Foshan, 528000, China
[2] Foshan Human Resources Public Service Center, Foshan, 528000, China

[*] **Corresponding author**: Hua Chen (Email: chenh393@mail2.sysu.edu.cn)

Abstract: Network intrusion detection is an important research direction in the field of network security. The traditional detection algorithm is based on feature extraction and feature separation, which has the problems of low detection accuracy and high false alarm rate. In order to improve the accuracy of network intrusion detection, this paper proposes an intrusion detection model based on deep asymmetric convolutional encoder and Random Forest(RF). First, use DACAE to extract features from the preprocessed data, and then use the random forest algorithm to divide the network traffic data into normal and abnormal classes, and finally achieve the purpose of network intrusion detection. It is tested on three public benchmark datasets of network intrusion detection NSL-KDD and KDD99 datasets. The experimental results show that the accuracy and false alarm rate of the improved method are better than the comparative method.

Keywords: Network security, Intrusion detection, Deep learning, Random forest.

1. Introduction

With the development of Internet technology and application, DoS attacks, ransomware and other attacks are increasing. In recent years, with the emergence of big data technology, deep learning, reinforcement learning, visualization and other technologies have been widely used, and have achieved great success in natural language processing, image recognition, video detection and other fields. At the same time, in the field of network security, a lot of research work has been done to use these technologies for network intrusion detection, and some results have been achieved. Julisch [1] proposed a new method for detecting intrusion alerts. The data is processed by eliminating the root cause of the event, and the new alarm clustering method is used to help researchers identify the network anomaly detection type. Zhang [2] et al applied random forest algorithm to network intrusion detection system. Its network service mode is constructed and implemented on the network data flow through the random forest algorithm. The algorithm is based on unsupervised learning to overcome the label dependence problem in supervised learning. Chen [3] et al. used two data mining methods, Artificial Neural Network (ANN) and Support Vector Machine (SVM) to detect potential system intrusions. Gao [4] et al. began to introduce deep belief networks into the field of anomaly detection, and composed multiple layers of restricted Boltzmann machines into neural network classifiers to obtain better performance. Vinayaku Mar [5] used convolutional neural network (CNN) for network intrusion detection. The network traffic is modeled as a time series, and the data packets of TCP / IP protocol are modeled using supervised learning method within a predefined time range. The validity of the network structure in intrusion detection is also proved on KDD99 data set. The traditional machine learning methods are still based on the prior knowledge of experts, and still rely on the label of data sets. An excellent intrusion detection system should not only detect anomalies from known network traffic, but also detect new unknown traffic from massive and high-dimensional data flows.

2. Improved Deep Learning Model

2.1. Autoencoder

Based on the back-propagation algorithm and optimization method, the auto-encoder uses the input data X itself as a supervision to guide the neural network to try to learn a mapping relationship, thereby obtaining a reconstructed output XR. In the time series anomaly detection scenario, anomalies are rare for normal, so if the difference between the output XR reconstructed by the auto-encoder and the original input exceeds a certain threshold (threshold), the original time series is abnormal.

The function of the encoder is to encode the high-dimensional input x into the low-dimensional hidden variable h so as to force the neural network to learn the most informative features; The function of the decoder is to restore the hidden variable h of the hidden layer to the initial dimension. The best state is that the output of the decoder can perfectly or approximately recover the original input, that is, $X' \approx X$.

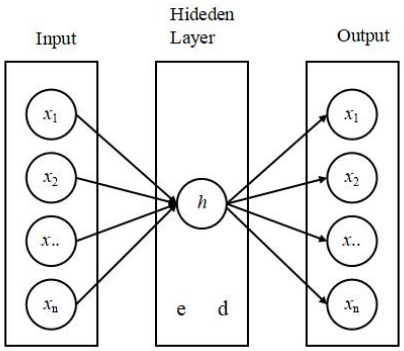

Figure 1. The antoencoder

As shown in figure 1:

The encoding process of the original data X from the input

layer to the hidden layer:

$$h = g_{\theta_1}(x) = \sigma(w_1 x + b_1) \quad (1)$$

The decoding process from the hidden layer to the output layer:

$$\hat{x} = g_{\theta_2}(h) = \sigma(W_2 h + b_2) \quad (2)$$

Then the optimization objective function of the algorithm is:

$$MinimizeLoss = dist(X, X^R) \quad (3)$$

Where dist is the distance measurement function, usually using (mean square difference) MSE.

2.2. Convolutional Autoencoder

The training method of the convolutional autoencoder is similar to that of the autoencoder. In each round of training operation of the convolutional layer, k convolution sums are initialized, and each convolution has a weight w and a bias b. The convolution kernel produces k feature maps after the convolution operation on the input vector x. The formula is shown in (4.3), σ represents the activation function, and the symbol * is the convolution operation.

$$h^k = \sigma(x * w^k + b^k) \quad (4)$$

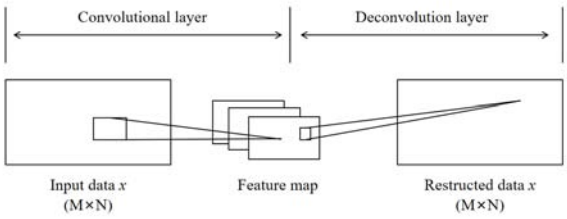

Figure 2. Convolutional autoencoder

Reconstruct the convolutional layer obtained from the previous layer to obtain the following equation (5)

$$y = \sigma(\sum^{k} h^k * \bar{W^k} + c^k) \quad (5)$$

In Equation (5), y is the feature after reconstruction of the convolution output, w represents the transpose of the weight w of the *k-th* feature, and ck represents the bias. The convolutional autoencoder compares the input data with the output data results, and trains and adjusts the parameters for optimization.

2.3. Deep Asymmetric Convolutional Auto-Encoder

The input vector of the encoder in the DACAE model is set to $x \in R^l$. After learning the input of each layer, the hidden layer is coded and mapped to $x_i \in R^l$, and l represents the dimension of the vector. The coding function can be determined as:

$$h_i = \sigma(w_i h_i + b_i), i = 1,2...,n \quad (6)$$

The DAC AE model proposed in this paper does not have a decoder. After the conversion between the n-layer encoder hidden layer and the sigmoid activation function, the output data can be expressed as equation (4.6)

$$h_n = \sigma(w_n h_{n-i} + b_n), i = 1,2...,n \quad (7)$$

In the unsupervised learning process, back propagation is used for error adjustment. Finally, the reconstruction error generated by DACAE can be expressed as equation (7):

$$E(\theta) = \frac{1}{2m}\sum_{i=1}^{m}(x_i - y_i)^2 \quad (8)$$

2.4. Random forest

Random forest is a classifier that uses multiple decision trees to train and predict samples. It contains multiple decision tree classifiers, and the output categories are determined by the mode of the categories output by individual trees. Random forest is a flexible and easy to use machine learning algorithm. Even without super parameter tuning, it can get good results in most cases. Random forest is also one of the most commonly used algorithms, because it is simple and can be used for both classification and regression. Random forest integrates all classified voting results, and specifies the category with the most votes as the final output, which is the simplest Bagging idea.

RF basic construction algorithm process:

1). N represents the number of training cases (samples), and M represents the number of features.

2). Input the feature number m to determine the decision result of a node on the decision tree; Where m should be much less than M.

3). Take N samples from N training cases (samples) in the way of put back sampling to form a training set (bootstrap sampling), and use the unselected cases (samples) for prediction to evaluate the error.

4). For each node, m features are randomly selected, and the decision of each node on the decision tree is determined based on these features. According to the m features, calculate the optimal splitting method.

5). Each tree grows completely without pruning, which may be used after building a normal tree classifier).

2.5. Establishment of Improved Deep Learning Model

The combination of deep learning model and shallow classification learning model can better improve the accuracy of classification detection. The overall framework of the DACAE-RF based detection model includes three modules: data preprocessing module, depth asymmetric convolutional encoder training module, and intrusion detection module.

The proposed model is shown in Figure 4.3. It uses DACAE to extract features from the preprocessed data, and uses the random forest algorithm to divide the network traffic data into normal classes and abnormal classes by generating new abstract features. For the current data and models, there are some unavoidable problems, such as the scarcity of labeled data resources, and the problem of gradient dispersion is prone to occur in deep neural networks. Therefore, using an

unsupervised asymmetric convolutional encoder can avoid this problem.

(1) In the data preprocessing module, the intrusion detection model will be tested with two datasets, the KD99-based NSL-KDD dataset and the NSL-KDD dataset. The preprocessing of the dataset includes removing socket information, label encoding and data normalization, etc. Among them, the 1D data of 41 features is filled with 0 to 64 features, and then converted into 8×8 2D data.

(2) In the deep asymmetric convolutional encoder module, the corresponding encoder structure is established through multi-layer convolutional layers and pooling layers, and unsupervised pre-training is performed for weight adjustment.

(3) After the first two modules preprocess the data and perform feature extraction on the neural network, new abstract feature data is obtained and the new data is used as the training data of the random forest. Random forest makes judgments and identifies the types of intrusion data to achieve the purpose of intrusion detection.

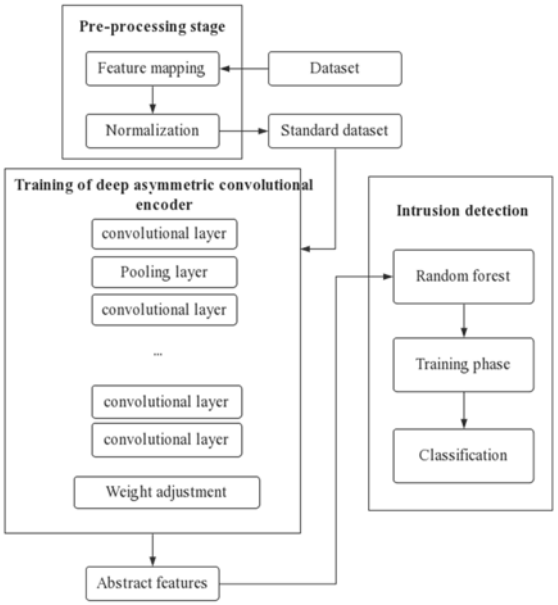

Figure 3. Using DACAE-RF to detect network traffic intrusion

3. Experiments

In the experimental part, the DACAE-RF detection model is compared with the model in research [6]. The experimental results were compared between NSL-KDD and KDD99 datasets. The evaluation criteria include accuracy, precision, recall and 1-score. The proposed model and the detection model mentioned in the study [6] were compared and analyzed, as shown in Table1 and Table 2.

Table 1. Performance of DACAE-RF on KDD99 dataset

Category	Precision (%)		Accuracy (%)		Recall (%)		F1-score (%)	
	S-NDAE	DACE-RF	S-NDAE	DACE-RF	S-NDAE	DACE-RF	S-NDAE	DACE-RF
Dos	100	100	99.78	99.75	99.78	99.82	99.79	99.92
Normal	100	100	99.46	99.55	99.51	99.66	99.71	99.83
Probe	100	100	99.71	99.78	98.68	99.32	99.38	99.64
U2L	0	40.81	0	10.20	0	46.98	0	44.58
R2L	100	100	9.30	24.39	9.29	89.21	17.45	94.86
Total	97.81	98.37	99.99	99.99	97.86	98.27	98.14	99.14

It can be seen from the Table 1 that the DACAE-RF detection model proposed in this paper is better than S-NDAE in accuracy, precision, recall rate and F_1-score in the classification of large-scale samples, such as Dos Normal, Probe and other attack types. S-NDAE and DACAE-RF also use the encoder structure to extract the features of the data, and use the random forest to classify the types of network intrusion. The experimental results show that the model proposed in this paper has better detection results on anomaly types than S-NDAE.

The experiment also evaluated the DACAE-RF model on the NSL-KDD data set. Table 2 is Different results of performance indicators of DACAE-RF intrusion detection classification.

Table 2. Performance of DACAE-RF on KDD99 dataset

Category	Precision (%)		Accuracy (%)		Recall (%)		F1-score (%)	
	S-NDAE	DACE-RF	S-NDAE	DACE-RF	S-NDAE	DACE-RF	S-NDAE	DACE-RF
Dos	100	100	94.58	98.12	94.58	98.13	97.22	99.06
Normal	100	100	97.73	98.27	97.73	98.27	98.85	99.13
Probe	100	100	94.67	96.29	94.67	96.29	97.26	98.11
U2L	100	100	2.7	9.32	2.7	9.32	5.26	17.05
R2L	100	100	3.82	15.27	3.82	15.27	7.36	26.49
Total	100	100	85.42	96.37	85.42	96.37	87.37	98.15

In the NSL-KDD dataset, the total accuracy, precision, recall and1-score has some improvement compared with the model proposed in other studies. In the classification of probe intrusion network types, the accuracy of DACAE-RF is improved from 94.67% to 96.29% compared with S-NDAE. In particular, in the classification of R2L intrusion events, the scores of various indicators of DACAE-RF have been significantly improved. In particular, the recall rate and "F_1-score" reached 15.27% and 26.49% respectively. This result also shows that under different data sets, the DACAE-RF detection model can effectively detect intrusion anomaly types.

In the last evaluation, the performance of multi classification of DACAE-RF model is tested. We processed the NSL-KDD training set and reserved more than 100 intrusion event categories. The purpose of this experiment is to test the stability and effectiveness of DACAE-RF when the number of intrusion attack types increases. It is a standard to measure the quality of intrusion detection system that can effectively classify a variety of different types of intrusion events. As shown in Table 3, DACAE-RF can effectively detect the types of intrusion events in the case of multiple classifications with increased detection categories. This shows that the DACAE-RF model can still maintain a high level of detection in the case of multi classification.

Table 3. DACAE-RF's multi-classification on NSL-KDD dateset

Label	Precision (%)	Accuracy (%)	Recall (%)	F_1-score (%)
Back	97.11	97.71	97.08	97.39
neptune	97.23	97.95	99.29	98.62
pod	100	100	100	100
smurf	97.98	98.96	99.22	99.09
teardrop	99.04	99.16	97.52	98.33
ipsweep	91.32	85.41	92.90	89.00
nmap	81.33	80.17	60.60	69.02
portsweep	92.27	93.87	86.83	90.21
satan	89.34	88.47	79.17	83.56
warezclient	94.11	90.27	93.4	91.81
Normal	98.39	99.27	99.53	99.40
Total	98.72	98.66	98.72	98.69

4. Conclusion

There are a large number of unlabeled network data in the Internet environment, and intrusion detection systems need to detect and classify under a variety of intrusion events. This paper combines the advantages of traditional self-encoder and convolutional self-encoder to propose a depth asymmetric convolutional encoder. The model can make good use of the ability of convolution kernel to extract local optimal features, extract new abstract features through stacked convolution encoders, and use random forest algorithm to detect and classify the generated features. From the experimental results, the DACAE-RF model has better intrusion detection performance than the traditional model. Especially in terms of the ability to detect small sample data, the DACAE-RF model has better detection ability. In terms of multi sample intrusion detection, the model can maintain a good detection level.

References

[1] Julisch, Klaus. Using root cause analysis to handle intrusion detection alarms. Diss. Universität Dortmund, 2003.

[2] Zhang, Jiong, and Mohammad Zulkernine. "Anomaly based network intrusion detection with unsupervised outlier detection." 2006 IEEE International Conference on Communications. Vol. 5. IEEE, 2006.

[3] Chen, Wun-Hwa, Sheng-Hsun Hsu, and Hwang-Pin Shen. "Application of SVM and ANN for intrusion detection." Computers & Operations Research 32.10 (2005): 2617-2634.

[4] Gao, Ni, et al. "An intrusion detection model based on deep belief networks." 2014 Second international conference on advanced cloud and big data. IEEE, 2014.

[5] R.Vinayakumar, K. P. Soman and P. Poornachandran, "Applying convolutional neural network for network intrusion detection," 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2017, pp. 1222-1228.

[6] Shone, Nathan, et al. "A deep learning approach to network intrusion detection." IEEE transactions on emerging topics in computational intelligence 2.1 (2018): 41-50.