Research on Intrusion Detection Based on Convolutional Neural Network

Min Sun, Min Gao(✉), and Ni Liu

School of Computer and Information Technology, Shanxi University, Taiyuan 030006, China
932944929@qq.com

Abstract. This paper proposes an intrusion detection model based on a convolutional neural network. First, a one-dimensional convolutional neural network structure is used to speed up the convergence of the model and prevent overfitting. Then, using the method based on SMOTE-GMM, the sample data is equalized by the method of combined sampling. Finally, a wrapped recursive feature addition algorithm is introduced to select the feature subset that makes the model detection effect the best. This paper uses the UNSW-NB15 and CICIDS2017 data sets to verify the effect of the model. Experimental results show that the intrusion detection model proposed in this paper has been improved in various evaluation indicators in the binary-classification and multi-classification. The model proposed in this paper can meet the real-time detection requirements of current complex networks.

Keywords: Intrusion detection · Depth learning · Smote · Convolutional neural network

1 Introduction

With the advent of the era of big data and the vigorous development of new network technologies, network security issues have become increasingly severe. As a real-time monitoring system for network traffic transmission, intrusion detection system identifies abnormal traffic by analyzing the characteristics of network connection data, thereby protecting the network environment from attacks and intrusions [1]. Traditional intrusion detection methods usually use rule matching to detect intrusion behaviors, which cannot effectively extract characteristic information in data traffic, and cannot meet the needs of today's network environment in terms of generalization ability, false alarm rate and detection efficiency. Therefore, introducing new technologies into the field of intrusion detection has important research value.

With the rise of deep learning technology in recent years, it has been widely used in various fields. Convolutional neural network [2] is one of the representative algorithms of deep learning. It can learn independently and effectively extract data feature information by using a multilayer neural network structure. Applying it to intrusion detection can improve the system's data feature analysis and generalization capabilities.

Q. Liang et al. (Eds.): Artificial Intelligence in China, LNEE 854, pp. 473–480, 2022.
https://doi.org/10.1007/978-981-16-9423-3_59

Therefore, this paper proposes an intrusion detection model based on convolutional neural network. First, for the dimensional characteristics of the data set, a one-dimensional convolutional neural network structure is used to speed up the convergence speed of the model and prevent overfitting. Then, for the problem of sample imbalance, based on the SMOTE-GMM method, the sample data is balanced by the combined sampling method, and then combined with the convolutional neural network to build the model, thereby improving the binary-classification effect of the model and the ability to detect categories with a small total number of samples under multi-classification. Finally, for the efficiency of model training and detection, a wrapped recursive feature addition algorithm is introduced, a feature recursive addition algorithm based on a greedy search strategy, combined with the convolutional neural network model, and finally the feature subset that makes the model's detection effect the best is selected, so that the model can improve the detection efficiency while maintaining the detection effect as much as possible, and reduce the consumption of computing resources.

This paper uses UNSW-NB15 and CICIDS2017 datasets to verify the effect of the model. The experimental results show that the model achieves a detection rate of 99.74% in the binary-classification on the UNSW-NB15 dataset. On the UNSW-NB15 and CICIDS2017 datasets, the detection rates of this model on multi-classification reached 96.54% and 99.85%, respectively. By comparing with other five imbalance processing methods and two classification algorithms, the model can effectively improve the intrusion detection capability and is superior to the current intrusion detection methods.

2 Proposed Solution

The architecture of the intrusion detection model proposed in this paper is shown in Fig. 1. The model is composed of three important modules: data preprocessing, imbalance processing and classification decision module. The data preprocessing module is responsible for performing operations on the original data to make the data more conducive to the prediction of the model. Using wrapped recursive feature addition algorithm in feature selection. We proposed a method, SMOTE-GMM in imbalance processing. Finally, in the classification decision module, we use a six-layer 1D-CNN model.

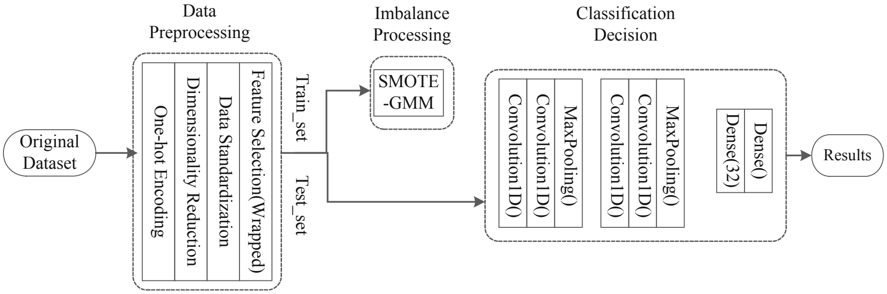

Fig. 1. A schematic diagram of the intrusion detection model

2.1 Datasets' Description

UNSW-NB15 dataset [3] was collected and distributed by the cybersecurity research group at the Australian Centre for Cyber Security. This dataset contains a total of 2,540,044 network traffic samples, involving nine attack categories. Each sample has 49 features, two of which are class label features. This dataset has serious class imbalances, in which normal traffic accounts for 87.35% of the entire dataset, and all attack traffic accounts for only 12.65%.

The CICIDS2017 dataset [4] was collected and compiled by the Canadian Cyber Security Institute with the help of the B-Profifile system [5] at the end of 2017. The dataset contains 2,830,473 network traffic samples, including one benign class and 14 attack categories, with benign traffic accounting for 80.30% and attack traffic accounting for 19.70%. The dataset extracts 84 features from the generated network traffic, of which the last column is the multiclass label.

2.2 Data Preprocessing

One-Hot Encoding. It is used to quantify the nominal features in the UNSW-NB15 dataset that cannot be processed by machine learning algorithms. After applying one-hot encoding, the feature dimension of the UNSW-NB15 dataset changes from 47 to 208. It is used in class label numeralization of two datasets.

Dimensionality Reduction. We drop redundant and meaningless features in the dataset. The feature dimensions of the UNSW-NB15 dataset and the CICIDS2017 dataset are reduced to 202 [6] and 77 [7], respectively.

Data Standardization. We standardize all remaining features and normalize them to a Gaussian distribution with a mean of 0 and a variance of 1.

Feature Selection. Wrapped feature selection mainly uses the recursive feature elimination (Recursive Feature Elimination) method, which uses a base model (leaner) for multiple rounds of training, removes several features after each round of training, then performs the next round of training based on the new feature set. The base model used is the convolutional neural network model sampled by SMOTE-GMM, and the performance of the learner is evaluated by the detection rate. This paper adopts the opposite method and uses the recursive feature addition algorithm. Essentially, recursive feature elimination and addition algorithms are the same idea. The recursive feature adds a search strategy based on greed. Its principle is to initialize an empty feature set first, and then continuously add new features to it. If the added new feature can improve the model effect, keep the feature, otherwise discard it. Because of this recursive method, new feature sets need to be continuously used to train the model, a lot of calculations are required.

2.3 Class Imbalance Processing

The number of abnormal samples in the intrusion detection dataset is inherently small. We propose a method SMOTE-GMM that resample all categories of samples to a uniform number of instance $I_{Resample}$ (hereinafter referred to as I) [7].

$$I_{Resample} = int\left(\frac{N}{C}\right) \tag{1}$$

where N is the total number of samples in the training set, and C is the number of classes.

The method uses SMOTE to oversample classes with less than I to I. SMOTE is a classic oversampling method proposed by Chawla et al. in 2002 [8]. SMOTE increases the quantity of minority class samples by "synthesizing" minority class samples. The "synthesis" is to generate a sample that does not exist in the original dataset and avoid overfitting in the process of building a classification model.

For classes with more samples than I, we use a GMM-based clustering method to undersample the majority class samples to I. GMM is a parameterized probability distribution model that represents a linear combination of multiple Gaussian distribution functions. Assuming that all samples come from multiple Gaussian distributions with different parameters, and samples that belong to the same distribution are divided into the same cluster, GMM returns the probability that sample x belongs to different clusters according to Eq. (2):

$$P(x|\theta) = \sum_{k=1}^{K} \alpha_k \Phi(x|\theta_k) \tag{2}$$

SMOTE-GMM not only avoids the excessive time and space cost caused by using oversampling alone, but also prevents random undersampling from losing important samples. It significantly improves the detection rate of minority classes.

2.4 CNN Modeling

We use 1D convolution. The convolution of a signal sequence x_1, x_2,…at time t can be expressed by:

$$y_t = f\left(\sum_{k=1}^{m} (\omega_k \otimes x_{t-k+1}) + b_t\right) \tag{3}$$

The pooling layer needs to undersample the features to reduce the network complexity and avoid overfitting.We use Max-Pooling [9], as shown in Eq. (4).

$$Y_i = {}^{\max}_{i \in \Re} x_i \tag{4}$$

We use a six-layer 1D-CNN suitable for NIDS. The data is simply mapped into two-dimensional information as input to the network. The first four layers are convolutional layers. The number of convolution kernels in the four 1D convolution layers is 32–32-64–64. Every two convolutional layers are followed by a Max-Pooling layer and a Dropout layer with a parameter of 0.2. The Max-Pooling layer undersamples the parameters of the convolution layer by two times. The Dropout layer prevents overfitting. Multiple stacked convolutional layers have fewer parameters and more nonlinear transformations than a large-size convolutional layer, and can provide stronger feature learning capabilities [10]. The last two layers are dense layers, which integrate the previously learned local features into global features, of which the fifth layer has 32 neural units. The sixth layer is the output layer, which is mainly used for classification prediction. The optimization algorithm uses “Nadam”, the learning rate is 0.008, and the loss function uses “categorical_crossentropy”.

3 Experimental Results and Analysis

3.1 Evaluation Indicator

The evaluation index of the network intrusion detection model mainly includes these indicators: accuracy (ACC), detection rate (DR), false alarm rate (FAR), Recall, Precision and F_1score. For each attack type, we consider the samples as positive ones and the others as negative ones. ACC is defined as the percentage of correctly classified ones among all samples. Recall, which is essentially DR, refers to the ratio of positive samples that are correctly detected. FAR is defined as the ratio of negative samples that are wrongly judged as positive ones. Precision refers to how many of the samples that the model judges to be positive are truly positive samples. F_1score is the harmonic average of Precision and Recall.

3.2 Binary Classification Experiment Results

In the binary classification experiment, to demonstrate the effectiveness of SMOTE-GMM, we compare four different class imbalanced processing techniques. Also, to evaluate the effectiveness of the proposed CNN model, we compare two machine learning classification algorithms, namely, Random Forest (RF) and Multi-Layer Perceptron (MLP).

Table 1 shows the binary classification results on the UNSW-NB15 dataset, where the bold part is the optimal result on a certain index. We observe that the best classification results are obtained by using the SMOTE-GMM-CNN model. The classification effect of 1D-CNN is better than RF and MLP. In terms of the overall performance, no matter which classification algorithm is used, such as RF, MLP, and CNN, SMOTE-GMM consistently achieves the best results. The combined performance of undersampling and oversampling is better than using oversampling alone.

Table 1. Performance evaluation of the proposed model in binary classification on the UNSW-NB15 dataset (%)

Model	Imbalanced Process	ACC	DR	FAR	Precision	F_1score
RF	ROS	98.67	99.99	1.52	90.49	95.01
	SMOTE	98.68	99.99	1.52	90.53	95.02
	RUS + SMOTE	98.66	99.87	1.51	90.52	94.97
	K-means + SMOTE	98.68	99.99	1.51	90.53	95.03
	SMOTE-GMM	**98.68**	**99.99**	**1.51**	**90.54**	**95.03**
MLP	ROS	98.66	**99.86**	1.51	90.52	94.96
	SMOTE	98.67	99.80	1.50	90.61	94.98
	RUS + SMOTE	98.65	99.82	1.52	90.49	94.93
	K-means + SMOTE	98.71	99.84	1.46	90.84	95.13
	SMOTE-GMM	**98.74**	99.82	**1.42**	**91.08**	**95.25**
CNN	ROS	98.68	**99.99**	1.52	90.53	95.02
	SMOTE	98.78	99.93	1.39	91.22	95.38
	RUS + SMOTE	98.78	99.91	1.39	91.25	95.39
	K-means + SMOTE	98.76	99.97	1.41	91.10	95.33
	SMOTE-GMM	**98.82**	99.74	**1.31**	**91.66**	**95.53**

3.3 Multi Classification Experiment Results

In the multi classification experiments, we use the same comparative experiment with the binary classification scenario. The 10-class classification results on the UNSW-NB15 dataset of CNN are shown in Fig. 2, The 15-class classification results on the CICIDS2017 dataset of CNN are shown in Fig. 3.

The experimental results show that the CNN model after class imbalance processing significantly improves the detection rate of attack classes. With the CNN classification algorithm, the oversampling method alone is better than the combination of RUS or K-means undersampling and SMOTE, but is not as good as the combination of GMM-based clustering undersampling and SMOTE.

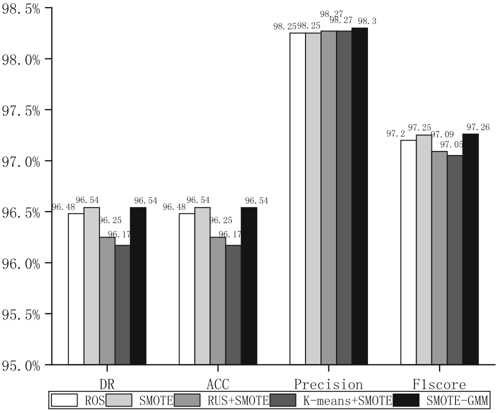

Fig. 2. Performance evaluation of the model in 10-class classification on the UNSW-NB15 dataset using CNN

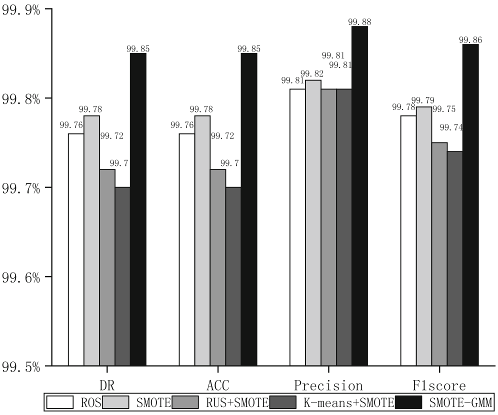

Fig. 3. Performance evaluation of the model in 15-class classification on the CICIDS2017 dataset using CNN

4 Conclusion

The intrusion detection model based on convolutional neural network proposed in this paper introduces a wrapped recursive feature addition algorithm, and uses a combined sampling method to balance the sample data, which can effectively improve the intrusion detection capability and is superior to the current intrusion detection methods.

But there are still shortcomings. In future work, we will try to combine two intrusion detection methods, anomaly and misuse. Intrusion detection based on misuse is more convenient and accurate, but has a high rate of false negatives, while intrusion detection based on anomalies can identify unknown new attacks, but has a high rate of false positives. Under the premise of ensuring system performance, hybrid intrusion detection methods will be one of the future research directions.

Acknowledgements. The work described in this paper is supported by Shanxi Natural Science Foundation (No. 201701D121052).

References

1. Zong, W., Chow, Y.-W., Susilo, W.: Interactive three-dimensional visualization of network intrusion detection data for machine learning. Future Gener. Comput. Syst.- Int. J. Esci. **102**, 292–306 (2020)
2. Liu, Y., Wang, C., Zhang, Y., Yuan, J.: Multiscale Convolutional CNN model for network intrusion detection. Comput. Eng. Appl. **55**(3), 90–95 (2019)
3. Moustafa, N., Slay, J.: UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 Network Data Set). IEEE (2015)
4. Sharafaldin, I., Lashkari, A.H., Ghorbani, A.A. (eds.) Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. International Conference on Information Systems Security and Privacy (2018)
5. Sharafaldin, I., Gharib, A., Lashkari, A.H., Ghorbani, A.A.: Towards a reliable intrusion detection benchmark dataset. Softw. Networking. **2017**(1), 177–200 (2017)
6. Zhang, H., Wu, C.Q., Gao, S., Wang, Z., Xu, Y., Liu, Y., et al.: An effective deep learning based scheme for network intrusion detection. In: 2018 24th International Conference on Pattern Recognition. International Conference on Pattern Recognition, pp. 682–687 (2018)
7. Abdulhammed, R., Musafer, H., Alessa, A., Faezipour, M., Abuzneid, A.: Features dimensionality reduction approaches for machine learning based network intrusion detection. Electronics **8**(3), 322 (2019)
8. Chawla, N.V., Bowyer, K.W., Hall, L.O., Kegelmeyer, W.P.: SMOTE: Synthetic minority over-sampling technique. J. Artif. Intell. Res. **16**, 321–357 (2002)
9. Tran, N.N., Sarker, R., Hu, J.: An approach for host-based intrusion detection system design using convolutional neural network. In: Hu, J., Khalil, I., Tari, Z., Wen, S. (eds.) MONAMI 2017. LNICSSITE, vol. 235, pp. 116–126. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-90775-8_10
10. Simonyan, K., Zisserman, A.: Very deep convolutional networks for large-scale image recognition. Comput. Sci. (2014)