Intrusion Detection Model Based on Weighted Extreme Learning Machine

Chen Chen[1,2], Gang Wei[2](✉), Fan Qiang[3], Dejiang Wan[4], and Guangyu Chen[1]

[1] State Key Laboratory of Astronautic Dynamics, Xi'an, China
[2] College of Air and Missile Defense, Air Force Engineering University, Xi'an, China
wei_gang@163.com
[3] Xichang Satellite Launch Center, Xichang, China
[4] Military Representative Bureau of Space System Equipment Department, Beijing, China

Abstract. An intrusion detection model based on weighted extreme learning machine (WELM) is proposed. By using the advantages of short training time and good generalization performance of WELM, the imbalance phenomenon in NSL-KDD intrusion detection dataset is increased, and the detection rate of rare attacks in network attacks is greatly improved compared with traditional machine learning methods, thus realizing the classification of NSL-KDD intrusion detection dataset. Experiments show that the precision and recall of this model for rare attacks are improved.

Keywords: intrusion detection · weighted extreme learning machine · imbalanced dataset · hyperparameters selection

1 Introduction

In the real network environment, the number of intrusion behaviors was often far less than the number of normal access, that was, the normal network access data and intrusion access data had serious uneven distribution. For example, in the network connection data collected by the US Air Force LAN, the illegal access of ordinary users to local superuser privileges was far less than the normal access [1]; At the same time, there were great differences between different network attacks, and the connection records of some intrusion behaviors (such as denial of service attacks) were far more than those of other network attacks (such as privilege attacks) [2].

Traditional machine learning models tend to favor the majority and ignore the minority when dealing with imbalanced dataset to obtain higher classification accuracy, which made it difficult to effectively distinguish the minority [3]. Therefore, the effective classification of imbalanced dataset has become one of the hot topics in the field of intrusion detection, and its fundamental goal is to effectively improve the classification accuracy of minority classes, thus improving the performance of intrusion detection systems [4].

In this paper, an intrusion detection model based on weighted extreme learning machine (WELM) is proposed, which can easily lead to false positives or false negatives because of intrusion behavior as a minority sample in network intrusion detection, and the

R. B. B. M. Hussain et al. (Eds.): ICHSSR 2023, ASSEHR 765, pp. 1115–1120, 2023.
https://doi.org/10.2991/978-2-38476-092-3_139

existing extreme learning machine (ELM) model cannot solve the classification problem of imbalanced dataset. By increasing the weight of minority samples, the imbalanced dataset can be effectively detected.

2 Weighted Extreme Learning Machine

Based on ELM, this paper establishes a WELM classification model. Suppose N training samples are given $\{x_i, t_i\}_{i=1}^{N}$, where $x_i = [x_{i1}, x_{i2}, \cdots, x_{in}]^{\mathrm{T}} \in R^n$ n is the feature number of the samples and m is the category number of the samples. A feedforward neural network output model with L hidden layer nodes can be expressed as follows:

$$\sum_{h=1}^{L} \beta_h G(a_h, b_h, x) = o_i, i = 1, 2, \cdots, N \tag{1}$$

where: β_h is the output weight of the h hidden layer neuron; G is the activation function of neurons in the hidden layer; a_h and b_h are the input weights and bias of the h hidden layer neurons, respectively; x is the input sample, and o_i is the actual output value of the ith training sample; t_i is the expected output of the ith training sample.

For a training sample with a number of N, $\{x_i, t_i\}_{i=1}^{N}, x_i \in R^n$, there exists a (a_h, b_h) and β_h, and there is a $\sum\limits_{i=1}^{L} \|o_i - t_i\| = 0$, which enables the single-hidden layer feedforward network (SLFN) to approach the training set $\{x_i, t_i\}_{i=1}^{N}, x_i \in R^n$ with zero error, that is

$$\sum_{h=1}^{L} \beta_h G(a_h, b_h, x_i) = t_i, i = 1, 2, \cdots, N \tag{2}$$

Formula (2) can be further simplified as:

$$\boldsymbol{H\beta} = \boldsymbol{T} \tag{3}$$

where: $\boldsymbol{H}$ is the hidden layer output matrix; $\boldsymbol{\beta}$ is the output weight matrix of hidden layer; $\boldsymbol{T}$ is the expected output matrix corresponding to the training sample.

3 Simulation Experiment

3.1 Experimental Environment

The operating system of the selected server is CentOS 7, the CPU processor is 64 × AMD 7452@2.35 GHz, and the memory is 256 G. The simulation software is MATLAB R2022a.

Table 1. Data distribution in training set and test set.

Label class	Normal	DoS	Probe	U2R	R2L	Total
Training set	67343	45927	11656	52	995	125973
Test set	9711	7458	2421	200	2754	22544

3.2 Dataset Selection

In this paper, the NSL-KDD dataset is selected as the experimental dataset, and KDDTrain + and KDDTest + in the NSL-KDD dataset are selected as the training set and test set respectively. Each dataset has 42 dimensions of data, in which the first 41 dimensions are dataset features and the 42nd dimension is dataset tag bits. The tag bits include Normal data and 39 types of attacks, among which the 39 types of attacks belong to DoS, Probe, U2R and R2L respectively, and the five types of tags are labeled as 1–5 respectively. The training set includes 21 types of intrusion attacks, while there are 18 types of intrusion attacks in the test set. These intrusion attacks, which only appear in the test set, can be used to evaluate the detection ability of the intrusion detection algorithm in this paper to unknown attacks. Table 1 shows the distribution of each tag class in the training set and the test set.

3.3 Evaluation Indicators

In this paper, the confusion matrix is used to display the experimental results, and two evaluation indexes, precision and recall, are used to compare the experimental results.

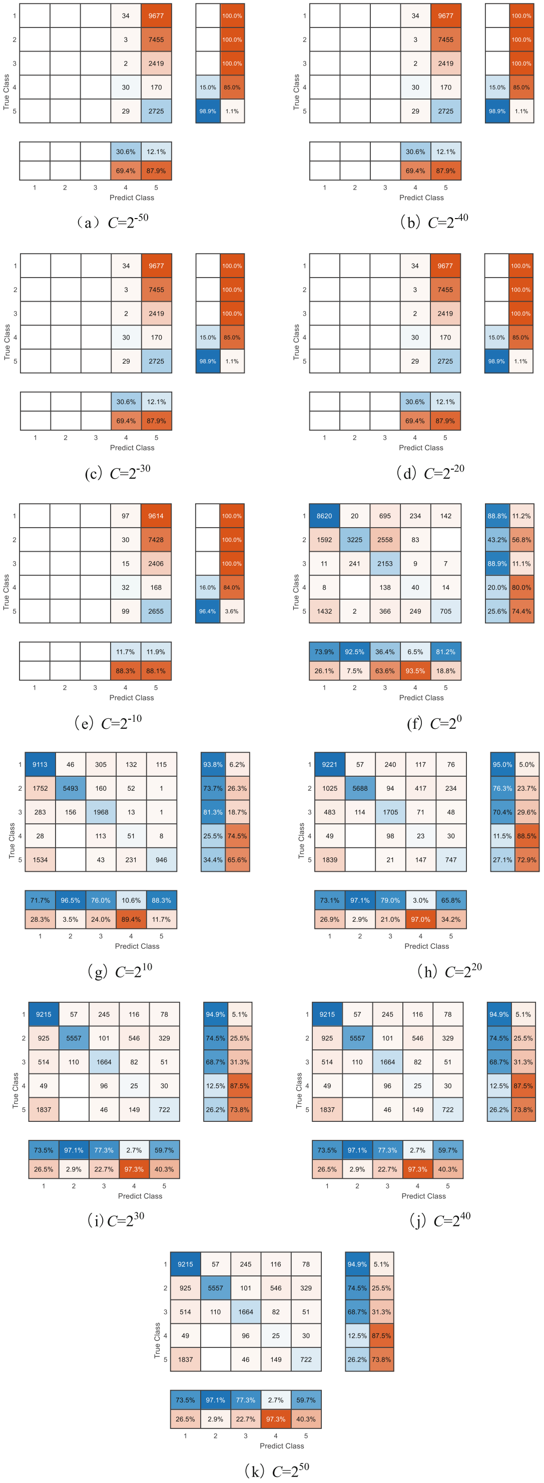
$$precision = \frac{TP}{TP + FP} \tag{4}$$

$$recall = \frac{TP}{TP + FN} \tag{5}$$

where: true positives (TP) indicates the number correctly divided into normal flows; false positives (FP) indicates the number that is wrongly divided into normal flows; false negatives (FN) indicates the number of intrusion attacks that have been wrongly classified; true negatives (TN) indicates the number of intrusion attacks correctly classified.

3.4 Hyperparameters Selection

The hyperparameters of WELM include the number of hidden layer nodes L and regularization parameter C. According to the characteristics of WELM, when C takes an appropriate value, the performance of WELM is less affected by the size of L; When C takes a large value, such as 2^{50}, with the increase of L, the performance of WELM decreases obviously. Therefore, we can first take a very large value of L, then choose the appropriate value of C through trial and error, and finally reduce the size of L without affecting the performance after the value of C is determined.



（a）C=2^{-50} （b）C=2^{-40}

（c）C=2^{-30} （d）C=2^{-20}

（e）C=2^{-10} （f）C=2^{0}

（g）C=2^{10} （h）C=2^{20}

（i）C=2^{30} （j）C=2^{40}

（k）C=2^{50}

Fig. 1. Confusion matrix.

3.5 Analysis of Experimental Results

The experimental results are shown in Fig. 1. In Fig. 1, the lower part of the confusion matrix is the precision, and the right part is the recall.

According to the numbers in Fig. 1 corresponding to different models, 11 models are designated as a-k. As can be seen from Fig. 1, when $C < 0$, the prediction ability of models a-e for the first three types of data is 0, which indicates that models a-e have no intrusion detection ability, so the C value corresponding to model a-e is no longer considered. When $C \geq 0$, the models f-k can detect all five types of data. However, no model has the highest precision and recall on all five types of data, so it is necessary to measure the comprehensive performance of the model. Among the models f-k, the precision of model e is higher than 70%, and the precision of the fourth category is 10.6% and the recall is 25.5%, which are the highest. Through comprehensive consideration, the performance of model e is the best, so $C = 2^{10}$ corresponding to model e is taken.

4 Conclusion

Aiming at the problem of data imbalance in intrusion detection, this paper uses WELM algorithm to increase the detection weight of minority groups. The simulation results show that WELM algorithm has improved the precision and recall rate of two major minority attacks to a certain extent, so WELM is more suitable for intrusion detection research. In the next research, aiming at the problem of randomly generating weights and thresholds of WELM model, intelligent optimization algorithm will be used to optimize parameters and improve model performance.

References

1. Chen, C., Liu, S., Wang Yifei, Song, Y. and Zhu, Y. (2022) A Network intrusion detection method based on PSOGWO-SVM. Journal of Air Force Engineering University, 23(2): 97-105.
2. Chen, C., Song, Y., Yue, S., Xu, X., Zhou, L., Lv, Q. and Yang, L. (2022) FCNN-SE: An Intrusion Detection Model Based on a Fusion CNN and Stacked Ensemble. Applied Sciences, 12(17): 8601.
3. Milosevic, M. S., and Ciric, V. M. (2022) Extreme minority class detection in imbalanced data for network intrusion. Computers & Security, 123: 102940.
4. Li, X., Kong, K., Shen, H., Wei, Z., and Liao, X. (2022) Intrusion detection method based on imbalanced learning classification. Journal of Experimental & Theoretical Artificial Intelligence, 1–21.
5. Zong, W., Huang, G. B., and Chen, Y. (2013) Weighted extreme learning machine for imbalance learning. Neurocomputing, 101: 229-242.