Threat Detection-Oriented Network Security Situation Assessment Method

Hongyu Yang[1,2(✉)], Zixin Zhang[2], and Liang Zhang[3]

[1] School of Safety Science and Engineering, Civil Aviation University of China, Tianjin 300300, China
[2] School of Computer Science and Technology, Civil Aviation University of China, Tianjin 300300, China
[3] School of Information, University of Arizona, Tucson, AZ 85721, USA

Abstract. To analyze the impact of network threats and accurately reflect the security situation of the network, we propose a threat detection-oriented network security situation assessment method. Firstly, a network threat detection model is designed. The model is composed of parallel feature extraction (PFE) with the sparse auto-encoder and an improved bi-directional gate recurrent (IBiGRU) with the attention mechanism. The PFE is established to extract the key information of different network threats and fuse the extracted features with the original information. Secondly, the PFE-IBiGRU is used to detect the threats in the network, and the occurrence number of each attack type and the false alarm reduction matrix are counted. Finally, according to the model detection results, combined with the proposed network security situation quantification method, the network security situation value is calculated. The experimental results show that our method is more accurate for identifying network attacks and can effectively and comprehensively evaluate the overall situation of network security.

Keywords: Parallel feature extraction · Sparse auto-encoder · Attention mechanism · False alarm reduction matrix · Network security situation assessment

1 Introduction

With the development of communication and cloud computing technology, network security is becoming increasingly important. Network security situation assessment (NSSA) can build an appropriate model according to related security incidents, and then assess the threat degree of the entire network system, and assist security managers to grasp the current network status [1].

Javaid et al. [2] used sparse auto-encoder (SAE) to extract features, the detection accuracy was significantly improved, but the model only used a single SAE to extract features, resulting in long extraction time and can not well fit the distribution of different attack types. Liu et al. [3] used a deep neural network based on the attention mechanism for real-time detection of Web attacks and proved the feasibility of this method in real

W. Shi et al. (Eds.): SPNCE 2021, LNICST 423, pp. 238–245, 2022.
https://doi.org/10.1007/978-3-030-96791-8_17

network traffic. Hu et al. [4] proposed a network security situation prediction model based on MapReduce and SVM, which solved the shortcoming of long training time of the SVM prediction model but did not conduct a comprehensive evaluation of the network situation, and the evaluation dimension was relatively single, which could not reflect the overall situation of the network. Lin et al. [5] tested the UNSW-NB15 data set based on various neural network models such as long-short term memory (LSTM) and bi-directional gate recurrent unit (BiGRU). The results show that BiGRU has the highest accuracy compared with other models.

Aiming at the difficulties in extracting feature elements and poor timeliness of available network security situation assessment methods, we propose a threat detection-oriented network security situation assessment method.

2 Threat Detection-Oriented Network Security Situation Assessment Method

The network security situation assessment framework proposed includes three parts: situation extraction, situation analysis, and situation assessment. The network security situation assessment process is designed as follows:

(1) Situation extraction: The network traffic data is collected, and then the data is pre-processed such as feature numericalization, feature normalization, and data balance. After that, the data is input into the PFE-IBiGRU threat detection model for training.
(2) Situation analysis: The test dataset is input into the trained threat detection model PFE-IBiGRU. Then the occurrence number of each attack type and the false alarm reduction matrix are recorded for the calculation of network security situation value in the third step.
(3) Situation assessment: Based on the detection results of the PFE-IBiGRU network threat detection model, combined with the quantified index of the network security situation, the network security situation value is calculated and the overall situation is evaluated.

2.1 Threat Detection Model

Parallel Feature Extraction (PFE). SAE is an improvement on auto-encoder (AE). It provides an idea to avoid the auto-encoder learning to be an identity function. Firstly, the number of neurons in the hidden layer is less than that in the input layer, and it is an incomplete auto-encoder, which enables the hidden layer to learn the significant compression characteristics of the input vector. Secondly, the sparsity penalty is added to the hidden layer, which limits the activation of neurons in the hidden layer to a relatively small range and avoids the complete equivalence of x' and x. However network threats contain a variety of attack types, and the distribution of these types of information is different. Feature extraction through a single SAE takes a long time and does not fit the distribution of different attacks well. Therefore, this paper uses multiple SAEs to complete feature extraction in parallel, learn the distribution of each attack, and better express the information differences between different attack types. The parallel

feature extraction is designed as follows: Firstly, according to different attack types, the preprocessed dataset is input into the SAE-based feature extractor FE_N for training. The loss function L_{SAE} is the minimum, and the FE_N training is completed. Then, the feature extraction function can be completed by taking the output of the encoder as the feature representing the original data. Finally, the extracted features are fused with the original features and input to the IBiGRU network for training.

Improved BiGRU (IBiGRU). BiGRU is an improved version of GRU. It can learn the temporal relationship between past and future states and the current state, and can effectively learn the representation relationship between network threat traffic to enhance the feature learning ability of the detection network.However, when BiGRU learns too long sequence data, it will have the problems of low efficiency and long time. The attention model [3] provides a way to solve this problem. Figure 1 shows the IBiGRU model structure designed in this paper. The specific steps of IBiGRU are as follows:

Step 1. Input data into the BiGRU network for learning and get output y_{ij}.

Step 2. Add weight to local features through the attention layer. The calculation method is as follows:

$$d_{ij} = tanh\left(\boldsymbol{A_w} y_{ij} + \boldsymbol{C_w}\right) \tag{1}$$

$$e_{ij} = softmax\left(d_{ij} + \boldsymbol{d_w}\right) \tag{2}$$

$$\mathbf{z_i} = \sum_j e_{ij} d_{ij} \tag{3}$$

where d_{ij} refers to the state of the hidden layer, e_{ij} refers to the weight, $\boldsymbol{A_w}$ refers to the weighting coefficient, $\boldsymbol{C_w}$ refers to the bias term, and $\boldsymbol{d_w}$ refers to the randomly initialized attention matrix.

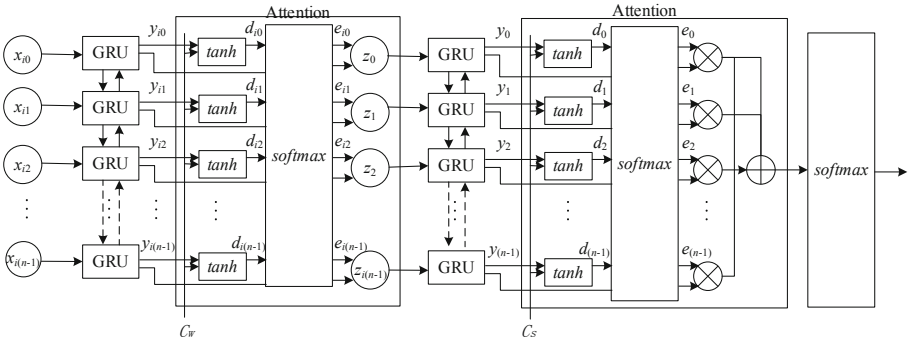

Fig. 1. IBiGRU's model structure

Step 3. Input the results obtained in Step 2 into the BiGRU network for learning. Similar to Step 2, the attention layer is used to add weight to the global features. The calculation method is as follows:

$$d_i = tanh(\boldsymbol{A_s} y_i + \boldsymbol{C_s}) \tag{4}$$

$$e_i = softmax(d_i, \boldsymbol{d}_s) \tag{5}$$

$$\mathbf{z} = \sum_j e_i d_i \tag{6}$$

Step 4. Input the result z of Step 3 into the classifier to complete model training.

2.2 Network Security Situation Assessment

The network security situation assessment result is determined by the threat severity and threat impact.

Threat Severity. The threat severity is obtained by the occurrence number of each attack type, the false alarm reduction matrix, and the threat severity factor of each attack type. The specific calculation process is as follows:

Step 1. Randomly select several sets of data from the test dataset, and input them into the PFE-IBiGRU model for threat detection. The occurrence number of each attack type detected by the model is N_i.

Step 2. Input the training dataset into the trained threat detection model, calculate b_{ij} based on the model test results and the actual number of attack types, then obtain the model's false alarm reduction matrix $\boldsymbol{M} = [b_{ij}]_{n\times n}$.

Step 3. Use the weight coefficient generation algorithm [6] to obtain and calculate the threat severity factors F_i of each attack type.

Step 4. Use the false alarm reduction matrix to correct the occurrence number N_i of each attack type, and the corrected occurrence number is recorded as Q_i.

$$Q_i = \boldsymbol{N} \cdot [\, b_{i1}\ b_{i2}\ \ldots\ b_{in}\,]^T \tag{7}$$

where $\boldsymbol{N}$ is a vector composed of the occurrence number of each attack type N_i.

Step 5. Calculate the threat severity S_i according to Eq. (8).

$$S_i = f(Q_i, F_i) = Q_i \times 10^{F_i} \tag{8}$$

Threat Impact. Combined with the common vulnerability scoring system (CVSS) [7] to evaluate the impact degree and scores of confidentiality (C), integrity (I), and availability (A). C, I, and A are divided into three grades according to no impact, low impact, and high impact, with values of 0, 0.22, and 0.56 respectively. Then, calculate the threat influence degree Ii of each attack type through Eq. (9).

$$I_i = Round_2(\log_2(\frac{d_1 2^{Con_i} + d_1 2^{Int_i} + d_3 2^{Ava_i}}{3})) \tag{9}$$

where Con_i, Int_i, and Ava_i represent the C, I, and A impact scores of attack type i, and d_1, d_2, and d_3 respectively correspond to the weight of threat impact degree.

Network Security Situation Quantitative Value. Calculate the network security situation value *V.*

$$V = \frac{1}{n} \sum_{i=1}^{n} S_i \times I_i \tag{10}$$

According to the interval of the V, refer to the "National Emergency Plan for Public Emergencies" [8], the network security situation assessment is divided into five levels: safe, low-risk, medium-risk, high-risk, and super-risk, corresponding to five intervals of 0.00–0.30, 0.31–0.60, 0.61–0.90, 0.91–1.20 and 1.21–1.50 respectively.

3 Experiments and Results

To verify the effectiveness and comprehensiveness of the method in this paper for network security situation assessment, experiments are conducted to verify the performance improvement effect of the PFE and attention mechanism on the basic model BiGRU. At the same time, through comparative experiments with typical methods, the objectivity and feasibility of the application of this method in network security situation assessment are verified.

3.1 Dataset Description and Data Preprocessing

The NSL-KDD dataset solves the problem of the KDD99 dataset [9]. And it is selected for the experiment. Data preprocessing includes feature numericalization, feature normalization, and data balance.Firstly, we apply the one-hot encoding method to convert the classification features into digital features. Secondly, the range between the maximum and the minimum value of some features in the NSL-KDD dataset is very different. To eliminate the influence of unit and scale differences between features on model training, we map the feature to the interval [0,1]. Finally, in the KDDTrain +, there are 67343 Normal data, while DoS and U2R only contain 52 and 995 data. The imbalance of data amount of different attack types will lead to the weak detection problem of the model. Therefore, we use the ADASYN algorithm to solve the problem of data imbalance to improve the detection effect.

3.2 Evaluation Metrics

To evaluate the performance of the model, we select the following metrics:

True Negatives (TN), the number of samples correctly classified as normal;

False Negatives (FN), the number of attack samples incorrectly classified as normal;

True Positives (TP), the number of samples correctly classified as attacks;

False Positives (FP), the number of normal samples incorrectly classified as attacks.

Precision (P), a percentage of the number of correctly predicted attacks and the total number of predicted samples, calculated by:

$$P = \frac{TP}{TP + FP} \times 100\% \tag{11}$$

Recall (R), a percentage of the number of correctly predicted attacks and the total number of attack samples, calculated by:

$$R = \frac{TP}{TP + FN} \times 100\% \tag{12}$$

F1-score ($F1$), considering P and R comprehensively, is an important metric to measure the performance of model detection, calculated by:

$$F1 = \frac{2 \times P \times R}{P + R} \times 100\% \tag{13}$$

3.3 Network Model Threat Testing Results

In the experiment, 125973 data of the KDDTrain + are selected for learning, 22543 data of the KDDTest + are selected for threat detection.To analyze the threat detection accuracy of the proposed model PFE-IBiGRU in this paper, we compare it with the original model BiGRU, the PFE-BiGRU model that only applies PFE to improve the original model, the IBiGRU model that only uses the attention mechanism to improve the original model, and the attention mechanism. The precision, recall, and $F1$ of four models are depicted in Table 1.

Table 1. Precision (%), Recall (%), $F1$ (%) of six models

Model	Precision	Recall	$F1$
BiGRU	76.85	77.71	77.28
PFE-BiGRU	79.70	80.78	80.24
IBiGRU	80.49	81.94	81.21
PFE-IBiGRU	82.13	83.36	82.74

As can be seen from Table 1, compared with the BiGRU model, the precisions of the PFE-BiGRU, and IBiGRU models are increased by 2.85%, and 3.64%. The precision of the PFE-IBiGRU is 82.13%, which is 5.28% higher than the BiGRU model. And Table 1 also shows that the recall and $F1$ of PFE-IBiGRU are better than the other three models. Compared with the BiGRU, PFE-BiGRU, and IBiGRU models, the recall rate is increased by 5.65%, 2.58%, and 1.42%; the $F1$ is increased by 5.46%, 2.5%, and 1.53% respectively. The reason is that the PFE-IBiGRU model in this paper adopts PFE to improve the characterization ability of the original data, and applies the attention mechanism for weighted feature learning, which verifies the advantages of the above two improved methods.

3.4 Network Security Situation Quantitative Assessment Results Analysis

We conduct 200 group threat tests with random data of the same size which is selected from the test dataset. SVM [4], LSTM [5], BIGRU [5], and PFE-IBIGRU carry out

threat testing experiments respectively. The network security situation values based on the above four models are obtained by using the method in this paper and compared with the real network security situation. Q_i in Eq. (8) is replaced by the actual number of each attack type in the test samples, and the actual situation value is further calculated by Eqs. (9) and (10). Figure 2 shows the comparison results of the network situation values in 20 groups of experiments.

It can be seen from Fig. 2 that under the same test dataset samples, the network security situation values calculated by the PFE-IBiGRU and the real situation values are always in the same situation assessment interval, while some situation value calculated by SVM, LSTM, and BiGRU model is not in the same interval as the real situation value. This indicates that the situation assessment results of the PFE-IBiGRU are more consistent with the actual network situation.

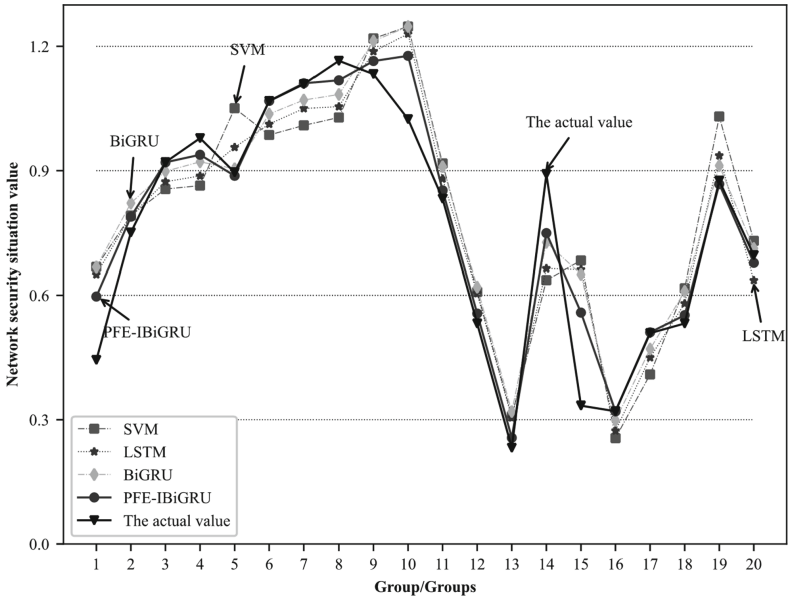

Fig. 2. Network security situation values

Besides, in some test results in Fig. 2, the situation values calculated by the four models are in the same situation assessment interval with the real situation values, but the network security situation values calculated by the PFE-IBiGRU are always closer to the real situation values. This shows that the PFE-IBiGRU model has a stronger ability to represent network threats, and the effect of this method on network security situation assessment is more intuitive and feasible.

4 Conclusion

This paper proposes a threat detection-oriented network security situation assessment method. Firstly, a threat detection model is constructed, which adopts the parallel feature

extraction method to effectively improve the characterization ability of the original data. Besides, the attention mechanism is used to improve the BiGRU network to determine the best weight of different features. Then PFE-IBiGRU is applied to detect the network threat, and the network security situation is evaluated according to the detection results and the false alarm reduction matrix. Finally, by comparing with BiGRU, LSTM, SVM, and other methods, the experiment proves that the effectiveness and reliability of the network security situation assessment results obtained by the method in this paper are more advantageous.

Acknowledgements. This work was supported by the Civil Aviation Joint Research Fund Project of the National Natural Science Foundation of China under granted number U1833107.

References

1. Zhao, D.: Study on network security situation awareness based on particle swarm optimization algorithm. Comput. Ind. Eng. **125**, 764–775 (2018)
2. Javaid, A.: A deep learning approach for network intrusion detection system. In: Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications, pp. 21–26. ICST, Brussels (2016)
3. Liu, T.: Locate-then-detect: real-time web attack detection via attention-based deep neural networks. In: Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence (IJCAI), pp. 4725–4731. Morgan Kaufmann, San Francisco (2019)
4. Hu, J.: Network security situation prediction based on MR-SVM. IEEE Access **7**, 130937–130945 (2019)
5. Lin, Y.: Time-related network intrusion detection model: a deep learning method. In: 2019 IEEE Global Communications Conference, pp. 1–6. IEEE Press, Piscataway (2019)
6. Liu, X.W.: Fusion-based cognitive awareness-control model for network security situation. J. Softw. **27**(8), 2099–2114 (2016)
7. Common Vulnerability Scoring System v3.0: Specification Document. https://www.first.org/cvss/specification-document. Accessed 5 Feb 2020
8. Council, S.: The State Council of the People's Republic of China. Overall Emergency Plans for National Sudden Public Incidents. China Legal Press, Beijing (2006)
9. Bala, R.: A review on kdd cup99 and nsl-kdd dataset. Int. J. Adv. Res. Comput. Sci. **10**(2), 64–67 (2019)