Research on deep learning method of intrusion attack prediction in software defined network

Jing Wang[1], *Hongyan* Liu[2], and *Fangfang* Liu[1,*]

[1]Changchun College of Electronic Technology, Changchun 130000, China
[2]Network management center of China Mobile Communication Group Jilin Co., Ltd, Changchun 130012, China

Abstract. At present, with the increase of the number of network attacks, in the software defined network, the controller is equivalent to the brain, which is an entity with a complete view of the network. When the attacker directs the malicious traffic to the controller, it may lead to the paralysis of the whole network. Therefore, although there are many solutions for intrusion detection, the attack prediction of network intrusion is still a problem worthy of study. This paper proposes a deep learning model based on gating loop unit (Gru) to identify and prevent intrusion attacks. The model can deeply learn the dependencies of security alarm sequences, and use data sets to evaluate the model. Experiments show that it can show the significant improvement of attack detection.

Keywords: Software defined network, Deep learning, Gated circulation unit.

1 Introduction

Software defined network (SDN) is evaluated as having the ability to respond to all requests and dynamic characteristics of modern applications by providing the best solution of network architecture. SDN enables network managers, network developers, network engineers and network suppliers to use the functions of the network in a flexible way [1].

At present, several prediction methods have been proposed in the field of network security. Although these methods prove that predicting future attacks is feasible, most of the work focuses on predicting future attacks against a single target, so it is very limited in practical application. Bartos et al. Showed that [2], it is also very meaningful to predict the future behavior of previously identified malicious sources. It allows the attack information for different targets to predict future attacks, and this is one of the important targets to predict the future work of attackers.

For the above reasons, due to the limited resources of the controller in the software defined network, it will not be used when the number of requests received exceeds its capacity. When the number of requests increases due to temporary reasons, the behavior of benign users is sometimes similar to that of malicious users. Therefore, it is very important

* Corresponding author: 8624949@qq.com

to implement reliable security measures on the controller to protect the controller from distributed denial of service (DDoS) attacks.

This paper proposes a deep learning model based on gating loop unit (GRU), which is a method for predicting network attacks. This method can not only predict the probability of observed attacks, but also predict the specific parameters such as the type, intensity and target of expected attacks, which makes the defense measures better applied.

The organizational structure of this paper is as follows. Section 2 describes the relevant methods. Section 3 introduces the methods proposed in this study. Section 4 evaluates the proposed method through simulation experiments. Section 5 summarizes.

2 Related work

The software defined network architecture includes different functions, and implements different security measures for different functions. In addition, it also has the advantages of programmability, flexibility and easy deployment. Network security prediction methods are divided into three fields: attack prediction, intention identification, intrusion prediction and network security situation prediction. This paper mainly studies the second kind, intrusion detection. The prediction method can be based on alarm correlation, action sequence, statistical and probability methods and feature extraction. At present, the machine learning methods used in attack prediction basically use simple shallow learning methods [3].

At present, the only relevant example of the application of deep learning to alarm prediction is a recent work by Shen et al. In which the author proposed an RNN based solution to predict future events on the machine based on previous observations [4]. However, the solution is tailored to specialized data collected from machines running Symantec intrusion detection software. However, the current work considers common fields such as attack detection time, attack volume, target IP and port, so it is applicable to any alarm data set containing these fields [5].

3 Proposed method

Deep learning algorithm is considered as a part of machine learning algorithm. It is a special node called neuron that can receive data and operate accordingly.

The prediction depth neural network proposed in this paper is shown in Figure 1. The dashed box on the right shows the specific operations of training, verification and super parameter tuning, and the test operation is displayed in the dashed box on the left.

The details of the early warning model are shown in Figure 2. In Figure 2, it can be seen that the prediction data adopts the three-layer sequential model, and the Gru layer is stacked on the top of the dense layer of each layer.

Gru is an advanced type of RNN, which is similar to LSTM. However, because the door structure of Gru is simple and there is no book to go out, it needs less time for training.

Gru contains two S-shaped doors and a hidden state. The calculation formula is:

$$Y_t = (1 - x_t) \otimes Y_{t-1} \oplus x_t \otimes i_t \tag{1}$$

The main difference between Gru and LSTM lies in the number of doors and the state of holding units. Compared with Gru, LSTM has three gates, namely input gate, ignore gate and output gate. Therefore, LSTM has the advantages of more flexibility and the disadvantages of low storage efficiency and time efficiency. Although Gru and LSTM are interdependent relationships that need long-term tracking, it is recommended to train LSTM extensively at the initial stage because it has more parameters and is more flexible. However, if there is no

quantifiable difference in performance between the two sides, Gru will be simpler and more efficient.

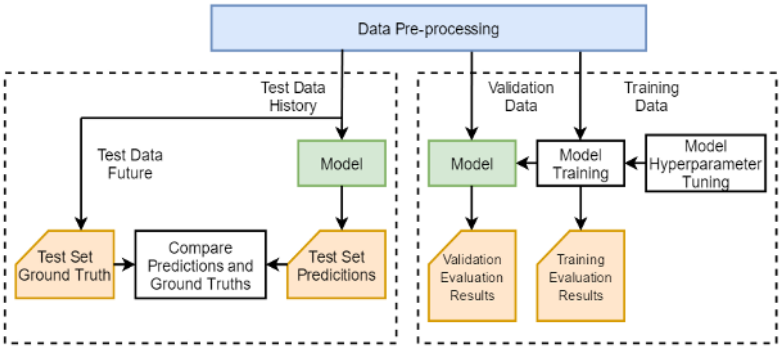

Fig. 1. Architecture block diagram of network intrusion early warning and prediction system based on Gru.

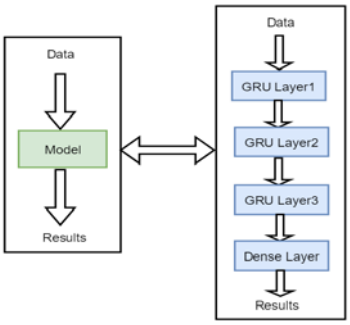

Fig. 2. Deep learning model.

4 Experimental data

Firstly, the detection performance of 48 features of Gru is analyzed from the aspects of accuracy, accuracy, recall and F1 score. As shown in Table 1, the results are good, and about 10% enhancement is achieved compared with the model with six features.

Table 1. Attack detection performance.

	48 Features				6 Features			
Algorithm	Precision	Recall	F1 Score	Accuracy	Precision	Recall	F1 Score	Accuracy
GRU	0.97947	0.99759	0.98842	0.98205	0.90172	0.99546	0.94625	0.91311

In addition to the expected results, the experiment also provides more analysis for the detection of different attacks. As shown in Figure 2, Gru has excellent performance in terms of accuracy, which is very suitable for DDoS, dos and probe detection. In addition, the effects of predicting botnets, web attacks, violent attacks and u2r attacks were also tested. Through the analysis, it is found that it has advantages in all indicators of DDoS, dos and detection. However, on botnets, web attacks and u2r, due to the small number of samples of these attacks in the data set, there is a significant decline in performance. Because attack categories usually have common characteristics, when the model works with the whole data set, it can better detect attacks. And in Web attacks and u2r attacks, Gru's recall rate and F1 score are relatively low. In terms of training time, Gru requires relatively less training time.

Table 2. Gru assessment with 48 characteristics.

Learning Model	DDos	DoS	Probe	Botnet	Web-Attack	U2R
Accuracy Score						
GRU	0.99939	0.98339	0.98191	0.99581	0.96347	0.99952
Precision Score						
GRU	0.99921	0.97569	0.97362	0.36667	0.06895	0.28578
Recall Score						
GRU	0.99981	0.98665	0.99578	1.00000	0.94879	0.50000
F1 Score						
GRU	0.99948	0.98117	0.98485	0.53661	0.12849	0.36359
Training Times						
GRU	21.13245	18.36079	23.72635	18.99158	19.18376	11.51245

The quality of the predicted alarm is estimated by comparing and analyzing the predicted alarm of all test vectors with the corresponding real alarm. The difference measure between the actual alarm and the predicted alarm is calculated as the weighted sum of the dissimilarity of a single field.

The classification field refers to the specific fields for direct comparison and classification, namely category, port and protocol, which are used to predict alarms. The tagetip field compares the three bytes in the targetip field. Flowcount is the difference between the logarithm of the flowcount value of the actual alarm and the predicted alarm. Detecttime is a method to compare the detecttime field. Based on the same idea as the flowcount field, a logarithm is used to ensure that the alarm expected to be received soon has higher accuracy, while the alarm received in a distant time in the future has lower accuracy.

Multiple future alerts are predicted for each test sample. The overall error value is calculated as the average value of the comparison between the real alarm and the predicted alarm. In the comparison process, the order of prediction alarms is not important. This shows that in practice, the first predicted alarm will be compared with the real alarm. The second predicted alarm is then compared with the remaining real alarms. If more than two alarms are predicted, all permutations are tried and the best results are used. Because the detection time field still plays an important role in error calculation, the difference between them usually increases with rearrangement, so the original order usually gives the best results. However, if there are two different future alarms, the time is close to each other, and the predicted alarms are very similar, but when the sequence is exchanged, the overall error value will be very large when compared with the original sequence, and the error will be very small in the exchange sequence, because each predicted alarm matches the real alarm very well.

In order to get an easily interpretable result, some thresholds are applied to the result error value, and the prediction is divided into three grades: good, medium and poor. And the prediction experiment with the result that the classification error value is greater than 0.5 is poor is carried out, but the difference between the predicted value and the real value is too large, so it has no practical use. On the other hand, if the error value is less than 0.2, it indicates that the prediction effect is good, because most fields are correct or there is little difference from the actual value. Values in between are classified as medium predictions, and as a whole, predicted alarms are still similar to real alarms.

5 Conclusion

The application software defines the network to study the intrusion attack prediction. This research work proposes a deep early warning method based on Gru, and uses the deep learning algorithm. The algorithm has achieved great success in many aspects and has been

applied in different fields. The deep learning algorithm can extract the original feature vector from the measurement data without any manual intervention, analyze the training and test data, and use any ongoing data to correct the understanding of the upcoming data. The proposed method can classify the incoming alerts and assign benign or malicious tags.

In this paper, the existing technology of Gru is optimized by changing the structure and quantity of input features. In practice, 48 features related to the software defined network environment are used to evaluate the performance of the model, which achieve a high detection rate. Compared with the model with six features, the experiment achieved about 12% enhancement.

In our future work, we will study the performance of other machine learning algorithms. The better feature combination will be carefully selected by aggregating the existing features, and the best algorithm and feature combination will be selected. Finally, the real-time classification model will be applied to evaluate the network performance.

References

1. Gadze, J.D., Bamfo-Asante, A.A., Agyemang, J.O., Nunoo-Mensah, H., Opare, K.A.B., 2021. An Investigation into the Application of Deep Learning in the Detection and Mitigation of DDOS Attack on SDN Controllers. Technologies 9, 14.
2. V. Bartos, M. Zadnik, S.M. Habib, E. Vasilomanolakis, Network entity characterization and attack prediction, Future Gener. Comput. Syst. 97(2019) 674–686.
3. Mohammed, S.S., Hussain, R., Senko, O., Bimaganbetov, B., Lee, J., Hussain, F., Kerrache, C.A., Barka, E., Bhuiyan, M.Z.A., 2018. A New Machine Learning-based Collaborative DDoS Mitigation Mechanism in Software-Defined Network, in: 2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE. pp. 1–8.
4. Y. Shen, E. Mariconti, P.A. Vervier, G. Stringhini, Tiresias: Predicting security events through deep learning, in: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2018, pp.592–605.
5. K. Cho, B. Van Merriënboer, C. Gulcehre, D. Bahdanau, F. Bougares, H. Schwenk, Y. Bengio, Learning phrase representations using RNN encoderdecoder for statistical machine translation, 2014, arXiv preprint arXiv:1406.1078.