A Deep Learning Approach for Network Anomaly Detection Based on AMF-LSTM

Mingyi Zhu, Kejiang Ye(✉), Yang Wang, and Cheng-Zhong Xu

Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences,
Shenzhen, China
{my.zhu,kj.ye,yang.wang1,cz.xu}@siat.ac.cn

Abstract. The Internet and computer networks are currently suffering from different security threats. This paper presents a new method called AMF-LSTM for abnormal traffic detection by using deep learning model. We use the statistical features of multi-flows rather than a single flow or the features extracted from log as the input to obtain temporal correlation between flows, and add an attention mechanism to the original LSTM to help the model learn which traffic flow has more contributions to the final results. Experiments show AMF-LSTM method has high accuracy and recall in anomaly type identification.

1 Introduction

The Internet and computer networks are currently suffering from different security threats [1]. The Global State of Information Security Survey 2015 [2] found there is a great increase in security incidents during the last several years. Network anomalies stand for a large fraction of the Internet traffic and compromise the performance of the network resources [1,3]. With the growing network scale, the traditional methods face two problems: (i) the processing speed is too slow, unable to cope with the massive network traffic data in today's Internet environments; (ii) it may invade the user's privacy. This situation can be alleviated by using machine learning methods, which are successfully used in many other areas. However, most of the traditional machine learning methods always focus on the traffic itself and extract their own characteristics to detect the potential anomalies.

As we know the data transmitted in network is in the form of *flows*. There is always a temporal correlation between flows, which is also true for abnormal traffic in the network. In previous work, researchers focus on the characteristics of traffic itself, but ignore that many network anomalies have potential temporal correlation. RNN (Recurrent Neural Networks) is widely used in the fields that are time series related. Recently, there are some works using RNN and LSTM (Long-Short Term Memory) to detect abnormal traffic [4,5], but they only use

Published by Springer Nature Switzerland AG 2018
F. Zhang et al. (Eds.): NPC 2018, LNCS 11276, pp. 137–141, 2018.
https://doi.org/10.1007/978-3-030-05677-3_13

a single flow to repeat multiple times, which can only learn the relationship between themselves and cannot learn the relationship between different flows.

This paper presents an anomaly detection method using deep learning model based on AMF-LSTM. The proposed method has three important features: (i) use the previous traffic flows as auxiliary features of the traffic to be detected; (ii) use LSTM to find the hidden temporal correlation between these flows, and (iii) use the attention mechanism to make model focus on the traffic and features that are useful for the results.

2 AMF-LSTM Model

We proposed an AMF-LSTM (Attention-base Multi-Flow LSTM) model for network anomaly detection. *Attention* means that our model is based on the attention mechanism [6]. *Multi-Flow* means that we not only use the characteristics of the current flow itself to detect the anomalies, but also use the previous traffic flows with temporal correlation to assist in detecting abnormal traffic. *LSTM* means the main body of our network is based on the long short-term memory networks [7]. Figure 1 shows the structure of AMF-LSTM model.

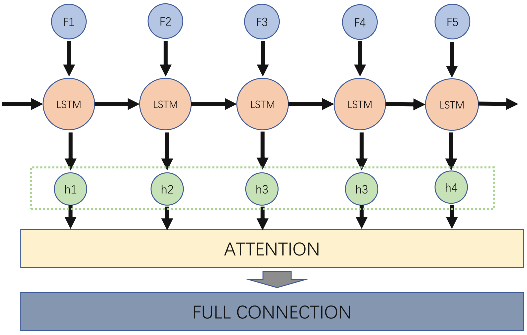
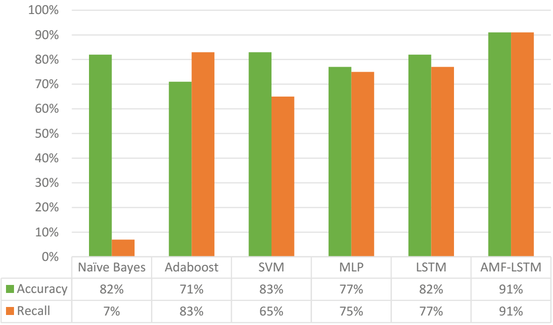


Fig. 1. Structure of AMF-LSTM

3 Experiment

We use CICIDS2017 [8] as the experimental dataset. The dataset contains benign and the most up-to-date common attacks, which resembles the true real-world data. The implemented attacks includes the most common attacks based on the 2016 McAfee report [9].

Our experiment mainly has the following hyperparameters: n, the number of flows are selected to detect the traffic; the *learning rate*, which is the step size of neural network for each learning; and the number of LSTM *hidden nodes*, which is the number of nodes that LSTM uses to learn.



	Naïve Bayes	Adaboost	SVM	MLP	LSTM	AMF-LSTM
🟩 Accuracy	82%	71%	83%	77%	82%	91%
🟧 Recall	7%	83%	65%	75%	77%	91%

Fig. 2. Accuracy and recall of 8-category classification

We first study the effect of learning rate and hidden nodes on the model accuracy, and find the best value of hidden nodes is 256, and the optimal learning rate is 0.0001. Then, we perform two sets of experiments with n = 10 and n = 20. The experimental results are similar, probably because the attention can focus on where it is needed. We compare the performance of our model with several classic machine learning algorithms, such as Naive Bayes, SVM, AdaBoost, MLP, and the original LSTM. The results of accuracy and recall comparison are shown in the Fig. 2. We can see that our model is significantly better than other machine learning algorithms, both in accuracy or recall.

We further conduct a deeper study on model with n = 10, lr = 0.0001, node_num = 256, which achieves the best performance. The evaluation metrics are shown in the Table 1. As we know, it is far more harmful for a system to judge abnormal traffic as normal traffic than to judge normal traffic as abnormal traffic. Therefore, we pay more attention to the value of recall. According to the table, our model can identify most of the anomalies correctly.

Table 1. The results of different evaluation metrics

	Precision	Recall	F1-score	Flows
Normal	0.98	0.91	0.94	348631
DDoS	0.83	0.98	0.90	25606
PortScan	0.82	0.99	0.90	31786
BOT	0.05	0.75	0.10	394
Infiltration	0.00	0.75	0.01	8
Web attack	0.04	0.81	0.07	436
Patator	0.38	0.53	0.44	2767
DoS	0.87	0.88	0.87	50532

4 Related Work

In prior studies, a number of approaches have been proposed for network anomaly detection. Sun et al. [10] present a survey of intrusion detection techniques for mobile ad-hoc networks (MANET) and wireless sensor networks (WSN). Sperotto et al. [11] explain the concepts of flow and classified attacks, and provide a detailed discussion of detection techniques. Abbes et al. [12] introduce an approach that uses decision trees with protocol analysis for effective intrusion detection. Khan et al. [13] use genetic algorithms to develop rules for network intrusion detection. Tthere are also large number of methods using Neural Network. An example of ANN-based IDS is RT-UNNID [14]. Thilina et al. [15] propose a novel framework to perform intruder detection and analysis using deep learning nets and association rule mining. Yuan et al. [16] use the LSTM-CNN framework to find user's anomalous behavior. Most recently, Zhu et al. [4] use CNN model for network anomaly detection and identification and achieve better performance than traditional machine learning algorithms. Although RNN [5] and LSTM [17] have been used to detect abnormal traffic before, they only use a single flow as the input of RNN and recurrent itself multiple times. In our opinion, they can only learn the relation in the traffic itself, and can not fully utilize the characteristics of RNN, which can learn the potential relations between different traffic.

5 Conclusion

This paper presents a method for abnormal traffic detection in the Internet by using deep learning model based on AMF-LSTM. We use the statistical features of multi-flows rather than a single flow as the input to obtain temporal correlation between flows, and add an attention mechanism to the original LSTM to help the model learn which traffic flow has more contributions to the result. Compared with other classic machine learning algorithms, our model achieves about 10% improvement in accuracy and recall on the multi-classification problems.

Acknowledgment. This work is supported by the National Key R&D Program of China (No. 2018YFB1004804), National Natural Science Foundation of China (No. 61702492, U1401258), and Shenzhen Basic Research Program (No. JCYJ20170818153016513, JCYJ20170307164747920).

References

1. Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., Vázquez, E.: Anomaly-based network intrusion detection: techniques, systems and challenges. Comput. Secur. **28**(1–2), 18–28 (2009)
2. Ahmed, M., Mahmood, A.N., Hu, J.: A survey of network anomaly detection techniques. J. Netw. Comput. Appl. **60**, 19–31 (2016)

3. Benson, T., Akella, A., Maltz, D.A.: Network traffic characteristics of data centers in the wild. In: Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement, pp. 267–280 (2010)
4. Zhu, M., Ye, K., Xu, C.-Z.: Network anomaly detection and identification based on deep learning methods. In: Luo, M., Zhang, L.-J. (eds.) CLOUD 2018. LNCS, vol. 10967, pp. 219–234. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-94295-7_15
5. Yin, C., Zhu, Y., Fei, J., He, X.: A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access **5**, 21954–21961 (2017)
6. Chorowski, J.K., Bahdanau, D., Serdyuk, D., Cho, K., Bengio, Y.: Attention-based models for speech recognition. In: Advances in Neural Information Processing Systems, pp. 577–585 (2015)
7. Hochreiter, S., Schmidhuber, J.: Long short-term memory. Neural Comput. **9**(8), 1735–1780 (1997)
8. Intrusion detection evaluation dataset (cicids2017) (2018). http://www.unb.ca/cic/datasets/ids-2017.html
9. Mcafee labs threats report (2018). https://www.mcafee.com/cn/security-awareness/articles/mcafee-labs-threats-report-mar-2016.aspx
10. Sun, B., Osborne, L., Xiao, Y., Guizani, S.: Intrusion detection techniques in mobile ad hoc and wireless sensor networks. IEEE Wirel. Commun. **14**(5), 56–63 (2007)
11. Sperotto, A., Schaffrath, G., Sadre, R., Morariu, C., Pras, A., Stiller, B.: An overview of IP flow-based intrusion detection. IEEE Commun. Surv. Tutor. **12**(3), 343–356 (2010)
12. Abbes, T., Bouhoula, A., Rusinowitch, M.: Efficient decision tree for protocol analysis in intrusion detection. Int. J. Secur. Netw. **5**(4), 220–235 (2010)
13. Khan, M.S.A.: Rule based network intrusion detection using genetic algorithm. Int. J. Comput. Appl. **18**(8), 26–29 (2011)
14. Amini, M., Jalili, R., Shahriari, H.R.: RT-UNNID: a practical solution to real-time network-based intrusion detection using unsupervised neural networks. Comput. Secur. **25**(6), 459–468 (2006)
15. Thilina, A., et al.: Intruder detection using deep learning and association rule mining. In: IEEE International Conference on Computer and Information Technology (CIT), pp. 615–620 (2016)
16. Yuan, F., Cao, Y., Shang, Y., Liu, Y., Tan, J., Fang, B.: Insider threat detection with deep neural network. In: Shi, Y., et al. (eds.) ICCS 2018. LNCS, vol. 10860, pp. 43–54. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-93698-7_4
17. Kim, J., Kim, J., Thu, H.L.T., Kim, H.: Long short term memory recurrent neural network classifier for intrusion detection. In: International Conference on Platform Technology and Service (PlatCon), pp. 1–5 (2016)