ANN Based Intrusion Detection Model

Seunghyun Park[1] and Hyunhee Park[2](✉)

[1] Graduate School of Information Security, Korea University, Seoul, South Korea
cloakingmode@gmail.com

[2] Department of Computer Software, Korean Bible University, Seoul, South Korea
parkhyunhee@gmail.com

Abstract. Anomaly based Intrusion Detection Systems (IDSs) are known to achieve high accuracy and detection rate. However, a significant computational overhead is incurred in training and deploying them. In this paper, we aim to address this issue by proposing a simple Artificial Neural Network (ANN) based IDS model. The ANN based IDS model uses the feed forward and the back propagation algorithms along with various other optimization techniques to minimize the overall computational overhead, while at the same time maintain a high performance level. Experimental results on the benchmark CICIDS2017 dataset shows that the performance (i.e., detection accuracy) of the ANN based IDS model. Owing to its high performance and low computational overhead, the ANN with Adam optimizer based IDS model is a suitable candidate for real time deployment and intrusion detection analysis.

1 Introduction

Network attacks prediction is an important technology of security management. Existing network intrusion detection and prediction methods did not fully consider the specific environment factors of target network, which may make the results deviate from the true situation [1]. In addition, the existing intrusion detection technology uses an intrusion detection technique that detects a traffic event based on the signature of the attacker and comparing it with the existing signature. However, as attack techniques evolve and become more sophisticated, a technique for defending against attacks in real time is becoming necessary. As diverse attacks occur, the existing pattern-matching based intrusion detection technology cannot detect attacks with new patterns and has difficulty detecting attacks in real time [2]. Owing to these limitations, the amount of research on intrusion detection technology for detecting attack patterns based on data mining is increasing [3].

The performance of intrusion detection systems may be changed through the selection of a traffic detection model, traffic detection criteria, and detection factors. In particular, such techniques may use many different resources for analysis and may result in large numbers of false positives. Therefore, a technique for reducing the use of resources is required for precise traffic modeling and analysis that can lower the false-positive rate. In this paper, we propose an

L. Barolli et al. (Eds.): WAINA 2019, AISC 927, pp. 433–437, 2019.
https://doi.org/10.1007/978-3-030-15035-8_40

intrusion detection model based on an artificial neural network (ANN) model. We model the influencing factors of network attack probabilities on the constructed ANN model. Experimental analysis shows that our model leads in more accurate results.

2 Dataset for Network Traffic

In this paper, we use a recent IDS dataset namely CICIDS2017, which covers all the eleven necessary criteria with common updated attacks such as Denial-of-service (DoS), Distributed DoS (DDoS), Brute Force, Cross-site Scripting (XSS), SQL Injection, Infiltration, Port scan and Botnet. The dataset is completely labelled and more than 78 network traffic features extracted and calculated for all benign and intrusive flows by using CICFlowMeter software which is publicly available in Canadian Institute for Cybersecurity website [4]. Unlike the existing datasets such as DARPA dataset, KDD Cup 99 dataset [5] and CAIDA dataset, CICIDS2017 dataset provides 14 different attack methods to which attack detection techniques can be applied. In particular, it includes various types of DoS attacks that deplete the server resources, such as DoS Hulk, GoldenEye, Slowloris, and Slowhttptest, as well as a port scan, which is a typical network attack, and brute force attacks to capture an authority such as FTP-Patator and SSH-Patator [6].

This study proposes an intrusion detection and prediction model applying the machine learning algorithm based on 78 data features using the above-mentioned CICIDS2017 dataset[1] [6,7].

3 ANN Based Network Traffic Prediction

We test the 78 extracted features using the Pearson correlation analysis to select the best short feature set for each attack which can be best detection features set for each attack. Then, we examine the performance and accuracy of the selected features with ANN machine learning model. In this paper, we use the feed forward and the back propagation algorithms to develop an ANN based IDS model. The hyperparameters used in applying the learning algorithm are defined in Table 1.

Detection accuracy is used as parameters for evaluation of different intrusion detection models. Accuracy is defined as the fraction of elements correctly classified as true alarms out of all the elements the intrusion detection model classified as positive elements in the dataset.

$$Acc = \frac{TP}{TP + FP}, \tag{1}$$

where TP and FP represent the True Positive and False Positive, respectively.

[1] https://www.unb.ca/cic/datasets/ids-2017.html.

Table 1. Common hyperparameters

Parameters	Value
Independent variable	y
Dependent variables	x, {x = 1, ...,39}
Learning rate	1, 0.1, 0.01, 0.001, 0.0001
Optimizer	Adam, Adagrad, RMSProp, Gradient Descent, Momentum
Hidden dimension	256, 512
Dropout	1, 0.9, 0.8, 0.7

In this study, the abnormal traffic prediction model applying the deep learning algorithm is implemented using the CICIDS2017 dataset provided by the CIC (Canadian Institute for Cybersecurity) as mentioned above, and the modeling results are compared [5]. Through deep-learning based modeling, the normal traffic and attack traffic of the CICIDS2017 data are predicted, and finally, which attack will occur in the attack traffic is predicted. The experimental environment used to evaluate the performance of the model is outlined with the GeForce GTX1070 8 GB for GPU, Python 3.7, and TensorFlow 1.9. The CICIDS2017 dataset is composed of 2,830,743 records, of which 70% is used for training, 20% for evaluation, and 10% for validation. A total of 39 independent variables are extracted by conducting feature-selection based on the Pearson correlation coefficient from the 78 features representing the data characteristics. Selected 39 independent variables are below for input dataset: Bwd Packet Length Std, Bwd Packet Length Max, Bwd Packet Length Mean, Avg Bwd Segment Size, Packet Length Std, Max Packet Length, Packet Length Variance, Fwd IAT Std, Packet Length Mean, Average Packet Size, Idle Max, Idle Mean, Flow IAT Max, Fwd IAT Max, Idle Min, Flow IAT Std, Min Packet Length, Bwd Packet Length Min, Fwd IAT Total, Flow Duration, FIN Flag Count, PSH flag Count, Flow IAT Mean, Bwd IAT Std, Fwd IAT Mean, URG Flag count, Destination Port, ACK Flag Count, Fwd Packet Length Min, Bwd IAT Max, Idle Std, Init Win bytes backward, Fwd Packet Length Mean, Avg Fwd Segment Size, SYN Flag Count, Fwd PSH Flags, Down/Up Ratio, Fwd Packet Length Max, and Fwd Packets/s.

Furthermore, 8 dependent variables for detecting attacks are extracted, excluding some attacks that have an extremely small dataset only to a traffic imbalance. Selected 8 dependent variables are below for output dataset: Benign, DDoS, DoS GoldenEye, DoS Hulk, DoS Slowhttptest, DoS Slowloris, FTP Patator, and Portscan.

To validate the feature selection and traffic imbalance, the prediction results are compared with the results using the complete datasets without an extraction process. The 39 independent variables selected as input are regularized using StandardScalar, and one-hot encoding is conducted for the 9 dependent variables selected as output.

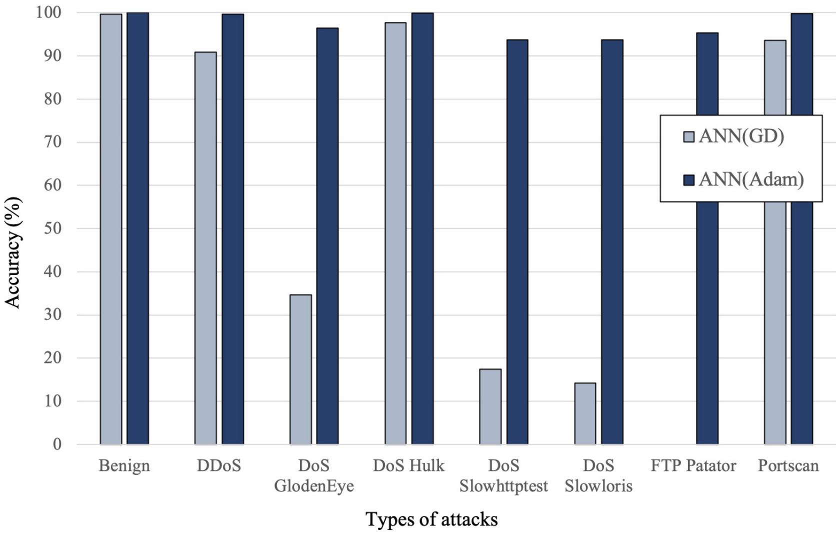

Fig. 1. Simulation result of ANN model with GD and Adam optimizers.

4 Experimental Results

To obtain the optimal hyperparameters for ANN modeling, the model is trained while varying the learning rate and dropout. As a result, the optimal result is obtained when the learning rate is 0.001 and the dropout is 1. Figure 1 shows the results of applying the Gradient Descent (GD) and Adam optimizers to the above hyperparameters. According to the modeling results of an ANN using the GD optimizer, the prediction accuracy is 98% or higher for most attacks. However, for FTP-Patator attacks, the sensitivity is 0, which indicates that the ANN modeling cannot predict certain attacks that show a class imbalance. Consequently, the results of applying other optimizers are analyzed in addition to ANN modeling. Although only the optimizer is changed, the class imbalance problem in certain attacks (e.g., FTP-Patator) disappeared. When the Adam optimizer is applied to ANN modeling, the prediction ratios are constant for all attacks in general.

5 Conclusion

In this paper, we proposed an anomaly detection model based IDS using the ANN learning algorithm. Experimental results on the benchmark CICIDS2017 dataset shows that its performance is comparable to that of the ANN with GD optimizer and ANN with Adam optimizer. However, since the ANN with Adam optimizer based IDS model uses only a single hidden layer, its computational overhead is comparatively less than that of the ANN with GD optimizer based IDS models. Therefore, the ANN with Adam optimizer based IDS model is an appropriate candidate for real time deployment and intrusion detection analysis. For our future work, we aim to fine tune various parameters of the proposed IDS model to further enhance its performance.

Acknowledgements. This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. NRF-2017R1C1B5017556).

References

1. Roesch, M.: Snort - lightweight intrusion detection for networks. In: Proceedings 13th USENIX Conference on System Administration, pp. 229–238 (1999)
2. Mukkamala, S., Janoski, G., Sung, A.: Intrusion detection using neural networks and support vector machines. In: Proceedings International Joint Conference on Neural Networks, pp. 1702–1707 (2002)
3. Yu, Y., Wu, H.: Anomaly intrusion detection based upon data mining techniques and fuzzy logic. In: Proceedings IEEE International Conference on Systems, Man, and Cybernetics, pp. 514–517 (2012)
4. CICFlowMeter for network traffic generator and analyser. Canadian institute for cybersecurity (CIC) (2017). https://www.unb.ca/cic/research/applications.html
5. Tavallaee, M., Bagheri, E., Lu, W., Ghorbani, A.: A detailed analysis of the KDD CUP 99 data set. In: Proceedings IEEE Symposium on Computational Intelligence for Security and Defense Applications, pp. 1–6 (2009)
6. Sharafaldin, I., Lashkari, A., Ghorbani, A.: Toward generating a new intrusion detection dataset and intrusion traffic characterization. In: Proceedings 4th International Conference on Information Systems Security and Privacy, pp. 108–116 (2018)
7. Shiravi, A., Shiravi, H., Tavallaee, M., Ghorbani, A.: Toward developing a systematic approach to generate benchmark datasets for intrusion detection. Comput. Secur. **31**(3), 357–374 (2012)