Introduction for research plan

1. Research question

My research question is: Is the SVM algorithm efficient in predicting DDoS attacks in telephony systems?

The DDoS attack is a kind of serious Internet attack that causes severe damage to cyber security. If the DDoS attack happens in telephony systems, the server in this system will be out of service and users will be unable to make phone calls [1]. To avoid this situation, we need to try our best to predict DDoS attacks and take measures to reduce the loss caused by the occurrence of DDoS attacks. The machine learning method is one of the greatest ways to predict DDoS attacks. There are several algorithms in machine learning field that may help predict DDoS attacks [2]. In my research, I will focus on the effectiveness of the SVM algorithm to predict DDoS attacks in telephony systems.

2. Methodology

In terms of the ways to test the efficiency of using the SVM algorithm to predict DDoS attacks, I will use the method of simulation. In my experiment, I will use a series of characteristics of DDoS attacks to train the model. The characteristics come from the real DDoS attacks and the usual Internet data flow that is similar to DDoS data. After training the SVM model, I will simulate some DDoS attacks and some usual data flows and use the SVM model to try to predict the occurrence of DDoS attacks. In [3-4], we can see that the SVM algorithm is a good method to predict DDoS attacks.

After completing the experiments, I will analyze the results of the experiments. The analysis will be based on whether the system can predict the DDoS attacks precisely. The result of the prediction can be classified as four groups: true positives, true negatives, false positives and false negatives. The standards used in the process of the analysis of results are accuracy, precision and recall [5].

References

[1] Sahi, A.; Lai, D.; Li, Y.; Diykh, M. (2017). An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment. IEEE Access, 6036-6048, IEEE. doi:10.1109/ACCESS.2017.2688460.

[2] Khuphiran, Panida; Leelaprute, Pattara; Uthayopas, Putchong; Ichikawa, Kohei; Watanakeesuntorn, Wassapon. (2018). Performance Comparison of Machine Learning Models for DDoS Attacks Detection. 2018 22nd International Computer Science and Engineering Conference (ICSEC), 1-4, IEEE. doi:10.1109/ICSEC.2018.8712757.

[3] Ramamoorthi, A.; Subbulakshmi, T.; Shalinie, S.M. (2011). Real time detection and classification of DDoS attacks using enhanced SVM with string kernels. 2011 International Conference on Recent Trends in Information Technology (ICRTIT), 91-96. doi:10.1109/ICRTIT.2011.5972281.

[4] Ye, Jin; Cheng, Xiangyang; Zhu, Jian; Feng, Luting; Song, Ling. (2018). A DDoS Attack Detection Method Based on SVM in Software Defined Network. SECURITY AND COMMUNICATION NETWORKS, 1-8, WILEY-HINDAWI. doi:10.1155/2018/9804061.

[5] Chenguang Wang; Jing Zheng; Xiaoyong Li. (2017). Research on DDoS Attacks Detection Based on RDF-SVM. 2017 10th International Conference on Intelligent Computation Technology and Automation (ICICTA), 161-165, IEEE. doi:10.1109/ICICTA.2017.43.