Literature Review

Student Name: Xinnan SHEN

Student ID: 1051380

1. Introduction

A distributed denial of service (DDoS) attack is one of the most severe Internet attacks, and it can generate severe problems for the attacked target machine [1]. DDoS is a type of Internet attack that attackers use multiple computers to attack one or more host machines simultaneously [2]. This type of attack differs from traditional network attacks in that it uses the distributed method rather than the conventional point-to-point method to attack a target machine [3].

DDoS attacks have serious consequences. Host machines or website servers will become unavailable to users after such attacks. When the telephony system is attacked, the service will become unavailable and users will not be able to make phone calls [4]. A severe consequence of a DDoS attack is that it affects services and clients. The telephony system will become inaccessible to legitimate clients after the DDoS attack [5].

Defending against DDoS attack through the use of traditional information techniques is quite difficult, because the traffic of DDoS attacks is similar to ordinary programs that use services provided by the Internet [3]. We can defend and predict DDoS attacks efficiently with the help of machine learning algorithms. Machine learning algorithms can be employed to defend against the DDoS attack in two ways. One way is through the establishment of an intrusion detection system that can defend against DDoS attack after it happens. The other way is through the prediction and prevention of a DDoS attack before it happens.

Several related studies have already been done to propose a possible solution to defend against DDoS attacks. Some of them have focused on the detection of DDoS attacks while others have highlighted the prevention of DDoS attacks. In the following sections, the contributions and shortcomings of the papers will be further discussed. This literature review is organized as follows. First, section 2 presents the details of related studies that contribute to DDoS attack detection. Then, section 3 demonstrates the methods involved in DDoS attack prediction. Finally, section 4 summarizes this literature review.

2. DDoS Attack Detection

DDoS attack detection is a relatively common topic, which is also the main subject of many related studies. In fact, traditional methods are effective in the detection of DDoS attacks. These papers focus on the use of machine learning algorithms to accurately detect DDoS attacks. However, such algorithms can only help detect DDoS attacks but cannot prevent them from happening, and the enhancement of the DDoS attacks detection accuracy is still very limited. In other words, some DDoS attacks cannot be detected though we have utilized machine learning techniques. In this section, I will review related papers that have contributed to DDoS attack detection.

Some papers have used different machine learning algorithms to detect DDoS attacks and compared their accuracy in an experiment. Khuphiran Panida et al. [6] compared the effectiveness between the support vector machine (SVM) algorithms and the deep feedforward (DFF) algorithms. In the experiment, machine learning algorithms have been used to detect a DDoS attack. The author has made contrasts between the effectiveness of the two algorithms. The final results of the experiment have shown that DFF has a higher accuracy than SVM in regard to the detection of the DDoS attack. Similarly, paper [7] has also made a comparison among different machine learning techniques. Three algorithms have been compared in regard to the effectiveness of detecting DDoS attack. These algorithms that are compared in the experiment are RFC, HMM and SVM algorithms respectively. In fact, these algorithms are used to detect different types of complicated DDoS attacks, such as TCP flood attacks, UDP flood attacks and ICMP flood attacks. The result of the experiment has shown that SVM is not an effective algorithm in the detection of DDoS attacks while RFC algorithm exhibited better results in the experiment. The RFC algorithm does greater than the other algorithms in terms of accuracy when there is excessive background traffic. According to Alsadhan Abeer Abdullah et al. [8], several new methods have been introduced to improve the effectiveness of DDoS attack detection. In their experiment, the authors used an intrusion detection system to try to detect the occurrence of an attack. They employed five different algorithms to detect DDoS attacks, and the results have shown that the decision tree algorithm has demonstrated to be the greatest accuracy. Moreover, several machine learning algorithms are compared in [9] when they are used in the field of detecting DDoS attacks. The author mentioned that certain algorithms, such as Naive Bayes and Random Forest Tree, are quite suitable for DDoS attack detection.

However, there are still a number of studies that employed some new machine learning techniques to detect DDoS attacks. The new algorithms they propose are generally based on existing machine learning algorithms, which are effective in detecting DDoS attacks. Myint Oo Myo et al. have developed an Advanced Support Vector Machine (ASVM) algorithm in [10] to enhance the effectiveness of the SVM algorithm in regard to the detection of DDoS attacks. Based on the principles of traditional SVM algorithm, ASVM algorithm has made some modification to make it more suitable for detecting DDoS attacks. The results of the study have shown that the ASVM is quite effective in detecting DDoS attacks, and that its accuracy of detecting DDoS attacks has increased to 97%, which is much better than that of traditional SVM algorithms. Therefore, the ASVM is a suitable algorithm to detect DDoS attack and can help protect the target machines. Daneshgadeh Salva et al. [11] have mentioned that Traffic Rate Analysis (TRA) can also be used to detect DDoS attacks, which is traditionally used in the machine learning field. In this study, the authors have used the TRA to analyze the traffic characteristics during a serious DDoS attack. Therefore, they are able to distinguish between the normal traffic and the DDoS attack traffic on the Internet by the use of TRA so that they can easily detect DDoS attacks.

These studies mentioned above have employed machine learning technologies to detect the DDoS attacks. With the help of machine learning algorithms, the detection of DDoS attacks has become increasingly accurate. If the DDoS attack can be detected accurately, the target machine will be more likely to be saved and losses caused by DDoS attacks can be reduced to the minimum. Therefore, the machine learning algorithms that previous studies have used make considerable contributions to the detection of DDoS attacks. However, the machine learning algorithms are far from perfect as the DDoS attacks sometimes cannot be detected in spite of the usage of machine learning algorithms. Hence, additional researches need to be done to enhance the effectiveness of DDoS attack detection.

3. DDoS Attack Prediction

In addition to the detection of DDoS attacks, machine learning algorithms can also be used to predict DDoS attacks so that people can defend against DDoS attacks at an early stage. Actions can be taken to prevent DDoS attacks if they can be accurately predicted. Hence, the prediction of DDoS attacks is much more important than the detection of them. In terms of the prediction of DDoS attacks, there are still a few studies that have focused on this topic.

With the use of machine learning algorithms, we can predict the occurrence of DDoS attacks more accurately. However, the prediction of DDoS attacks is far from perfect, and the effectiveness of machine learning algorithms in the field of DDoS attack prediction still remains limited. In this section, I will describe the contributions of different studies related to the prediction of DDoS attacks.

Numerous studies have employed machine learning techniques to predict DDoS attacks. Hoon Kian Son et al. [12] have proposed that certain algorithms in machine learning field could be used for DDoS attack forensics. In the study, different algorithms have been compared when the algorithm is applied to predict DDoS attacks. In contrast to other researchers, the authors compared both supervised learning algorithms and unsupervised learning algorithms. From the results of the experiment, we can draw a conclusion that supervised learning algorithms may perform worse than unsupervised learning algorithms if the experimental data are not designed properly. Therefore, both supervised learning and unsupervised learning algorithms can be used to predict DDoS attacks. In the study [13], the author has discovered that machine learning algorithms can predict DDoS attacks and help protect the target machine. The author has also developed a reliable method to predict and prevent DDoS attacks by using the machine learning algorithms in the filter rule. Moreover, the author has simulated a serious DDoS attack to evaluate the reliability of his proposed scheme. The results have demonstrated that the scheme can protect the machine from a DDoS attack in most cases and that the scheme is extremely useful in predicting and preventing DDoS attacks. Similarly, Pelloso Mateus et al. [14] have also designed a system to predict DDoS attacks, which is a self-adaptable DDoS attack prediction system that can predict and prevent DDoS attacks in most cases. Their design of the self-adaptable system is based on machine learning algorithms. Without knowing the characteristic of a network, the system can analyze the data traffic in the network and discover the abnormal data that are the trends of a DDoS attack. The result of system evaluation has shown that the system is quite useful in predicting a potential DDoS attack, and that it can be used to prevent certain DDoS attacks as well. Moreover, paper [15] has analyzed the different methods of predicting and preventing DDoS attacks. The author has mentioned that using certain machine learning algorithms can be helpful in regard to predict the occurrence of DDoS attacks.

Plenty of studies have already been conducted in the DDoS attack prediction field. Previous studies have used machine learning technologies to help improve the accuracy of DDoS attacks prediction. In addition, several studies have identified a number of new approaches that can be helpful in predicting and preventing certain types of DDoS attacks, thereby making considerable contributions to this field. However, the prediction of DDoS attacks is not perfect at all. Although many people have proposed new methods to predict the DDoS attacks which are quite effective to some extent, the accuracy of DDoS attack prediction can be improved further in the future. Thus, further research needs to be done to enhance the result of the DDoS attack prediction.

4. Summary

DDoS attacks are serious Internet attacks and they cause threats to individuals, companies and the government. Thus, we need to improve the accuracy of DDoS attack detection so that we can stop attacks as soon as possible to reduce the losses caused by the attacks. A better solution is to predict the future occurrence of them and prevent it from happening. In the past, traditional algorithms have been used to detect and predict the DDoS attacks. It is relatively difficult to defend against DDoS attacks only through using traditional algorithms. At present, with the rapid development of artificial intelligence, the machine learning techniques can also be used in the field of detecting and predicting DDoS attacks. When the machine learning algorithms are applied in the field of detecting and predicting DDoS attacks, the accuracy will have increased remarkably. In this literature review, I have analyzed different studies that make contributions to the detection and prediction of DDoS attacks by the use of machine learning techniques. Comparisons and contrasts are used when mentioning different papers in this field. However, the accuracy of DDoS attack detection and prediction should still be enhanced and further research should be done to improve the effectiveness of DDoS attacks detection and prediction.

References

[1] Idhammad Mohamed; Afdel Karim; Belouch Mustapha. (2018). Semi-supervised machine learning approach for DDoS detection. APPLIED INTELLIGENCE, 48(10), 3193-3208, SPRINGER. doi:10.1007/s10489-018-1141-2.

[2] Zargar S.T.; Joshi J.; Tipper D. (2013). A Survey of Defense Mechanisms Against

Distributed Denial of Service (DDoS) Flooding Attacks. IEEE Communications Surveys & Tutorials, 15(4), 2046-2069, IEEE. doi:10.1109/SURV.2013.031413.00127.

[3] Bing Wang; Yao Zheng; Wenjing Lou; Hou Y.T. (2014). DDoS Attack Protection in the Era of Cloud Computing and Software-Defined Networking. 2014 IEEE 22nd International Conference on Network Protocols, 624-629, IEEE, doi:10.1109/ICNP.2014.99.

[4] Cadet Frantz; Fokum Daniel T. (2016). Coping with denial-of-service attacks on the IP telephony system. SoutheastCon 2016, 1-7, IEEE. doi:10.1109/SECON.2016.7506691.

[5] Guri M.; Mirsky Y.; Elovici Y. (2017). 9-1-1 DDoS: Attacks, Analysis and Mitigation. 2017 IEEE European Symposium on Security and Privacy (EuroS&P), 218-232, IEEE. doi:10.1109/EuroSP.2017.23.

[6] 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.

[7] Yu Pengcheng;Qi Yong;Li Qianmu. (2017). DDoS attack detection method based on random forest. Application Research of Computers / Jisuanji Yingyong Yanjiu, 34(10), 3068-3072, Application Research of Computers Edition. doi:10.3969/j.issn.1001-3695.2017.10.042.

[8] Alsadhan Abeer Abdullah; Hussain Abir; Alani Mohammed M. (2018). Detecting NDP Distributed Denial of Service Attacks Using Machine Learning Algorithm Based on Flow-Based Representation. 2018 11th International Conference on Developments in eSystems Engineering (DeSE), 134-140, IEEE. doi:10.1109/INES.2018.8523851.

[9] Zhang Boyang; Zhang Tao; Yu Zhijian. (2017). DDoS detection and prevention based on artificial intelligence techniques. 2017 3rd IEEE International Conference on Computer and Communications (ICCC), 1276-1280, IEEE. doi:10.1109/CompComm.2017.8322748.

[10] Myint Oo Myo; Kamolphiwong Sinchai; Kamolphiwong Thossaporn; Vasupongayya Sangsuree. (2019). Advanced Support Vector Machine- (ASVM-) Based Detection for Distributed Denial of Service (DDoS) Attack on Software Defined Networking (SDN). Journal of Computer Networks & Communications, 1-12, Hindawi Limited. doi:10.1155/2019/8012568.

[11] Daneshgadeh Salva; Ahmed Tarem; Kemmerich Thomas; Baykal Nazife. (2019). Detection of DDoS Attacks and Flash Events Using Shannon Entropy, KOAD and Mahalanobis Distance. 2019 22nd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), 222-229, IEEE. doi:10.1109/ICIN.2019.8685891.

[12] Hoon Kian Son; Yeo Kheng Cher; Azam Sami; Shunmugam Bharanidharan; De Boer

Friso. (2018). Critical review of machine learning approaches to apply big data analytics in DDoS forensics. 2018 International Conference on Computer Communication and Informatics (ICCCI), 1-5, IEEE. doi:10.1109/ICCCI.2018.8441286.

[13] Misono Masanori; Yoshida Kaito; Hwang Juho; Shinagawa Takahiro. (2018). Distributed Denial of Service Attack Prevention at Source Machines. 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), Dependable, Autonomic and Secure Computing, 488-495, IEEE. doi: 10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00096

[14] Pelloso Mateus; Vergutz Andressa; Santos Aldri; Nogueira Michele. (2018). A Self-Adaptable System for DDoS Attack Prediction Based on the Metastability Theory. 2018 IEEE Global Communications Conference (GLOBECOM), 1-6, IEEE. doi:10.1109/GLOCOM.2018.8647934.

[15] Kaur Chahal Jasmeen; Bhandari Abhinav; Behal Sunny. (2019). Distributed Denial of Service Attacks: A Threat or Challenge. New Review of Information Networking, 24(1), 31-103, Taylor & Francis Ltd. doi:10.1080/13614576.2019.1611468.