Introduction for literature review

Distributed denial of service (DDOS) attack is a very serious attack that can cause severe problems to target machines and the system [1]. Providing several practical approaches to prevent DDOS attack from happening can be beneficial to the machine as well as the whole IT system. If the DDOS attack happens in the telephony system, the target machine may be out of service, which leads people unable to use telephony system [2]. In my research, I will utilize machine learning to try our best to stop the DDOS attack happening in the telephony system so that the machines and the entire system can be protected.

Most of the recent researches of this topic involve predicting DDOS attack by using some artificial intelligence techniques like machine learning. They use algorithms in machine learning to predict the DDOS attack as precise as possible [3][4]. However, there are still a few papers focusing on using some methods to reduce the influence of the DDOS attack. These papers use algorithms to make intrusion detection system more effectively [5][6]. My research involves using machine learning algorithms to prevent DDOS from happening in the telephony system so that the target machine and system will be safe from being attacked.

In this literature review, I will discuss some related works that have been done on this topic. First, I will discuss the methods mentioned in related papers that can be used to predict the DDOS attack. These algorithms are based on machine learning techniques in order to predict the time and the extent of DDOS attack when it happens. After mentioning the machine learning ways that can predict the attack, I will then present some other methods to help to reduce the effect of the DDOS attack, which is mentioned in some other papers. Besides, I will explain what my research does and why it is different from the previous papers.

References

[1]Zhang, B., Zhang, T., & Yu, Z. (2017, December). DDoS detection and prevention based on artificial intelligence techniques. In 2017 3rd IEEE International Conference on Computer and Communications (ICCC) (pp. 1276-1280). IEEE.

[2]Guri, M., Mirsky, Y., & Elovici, Y. (2016). 9-1-1 ddos: Threat, analysis and mitigation. arXiv preprint arXiv:1609.02353.

[3]Khuphiran, P., Leelaprute, P., Uthayopas, P., Ichikawa, K., & Watanakeesuntorn, W. (2018, November). Performance Comparison of Machine Learning Models for DDoS Attacks Detection. In 2018 22nd International Computer Science and Engineering Conference (ICSEC) (pp. 1-4). IEEE.

[4]Hoon, K. S., Yeo, K. C., Azam, S., Shunmugam, B., & De Boer, F. (2018, January). Critical review of machine learning approaches to apply big data analytics in DDoS forensics. In 2018 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-5). IEEE.

[5]Cadet, F., & Fokum, D. T. (2016, March). Coping with denial-of-service attacks on the IP telephony system. In SoutheastCon 2016 (pp. 1-7). IEEE.

[6]Misono, M., Yoshida, K., Hwang, J., & Shinagawa, T. (2018, August). Distributed Denial of Service Attack Prevention at Source Machines. In 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) (pp. 488-495). IEEE.