Chapter 8
DDoS Attacks and Defense Mechanisms Using Machine Learning Techniques for SDN

Rochak Swami
National Institute of Technology, Kurukshetra, India

Mayank Dave
https://orcid.org/0000-0003-4748-0753
National Institute of Technology, Kurukshetra, India

Virender Ranga
https://orcid.org/0000-0002-2046-8642
National Institute of Technology, Kurukshetra, India

ABSTRACT

Distributed denial of service (DDoS) attack is one of the most disastrous attacks that compromises the resources and services of the server. DDoS attack makes the services unavailable for its legitimate users by flooding the network with illegitimate traffic. Most commonly, it targets the bandwidth and resources of the server. This chapter discusses various types of DDoS attacks with their behavior. It describes the state-of-the-art of DDoS attacks. An emerging technology named "Software-defined networking" (SDN) has been developed for new generation networks. It has become a trending way of networking. Due to the centralized networking technology, SDN suffers from DDoS attacks. SDN controller manages the functionality of the complete network. Therefore, it is the most vulnerable target of the attackers to be attacked. This work illustrates how DDoS attacks affect the whole working of SDN. The objective of this chapter is also to provide a better understanding of DDoS attacks and how machine learning approaches may be used for detecting DDoS attacks.

DOI: 10.4018/978-1-7998-0373-7.ch008

INTRODUCTION

Nowadays, the world has become digitally oriented and full of networking services. Networking is an essential part of our lives because of providing several flexible and easy way of communications. With the increasing growth in advanced network services, chances of cyber-attacks are also growing. There are various attacks that disturb the normal functioning of the networks. One of these attacks is Distributed denial of service (DDoS) attack (Mirkovic et al., 2004). DDoS has become the most frequently used attack for infecting the system's services. It tries to make the services unavailable for normal users by overwhelming it with a huge amount of traffic. DDoS attacks target the system's resources to disrupt the proper functioning of the system's services. Most commonly targeted resources by DDoS attacks are bandwidth, memory, and CPU. These attacks are rapidly growing year by year. As per Arbor's report (Novinson, 2018), DDoS attacks have increased from 1Gbps in 2000 to 100Gbps in 2010, and to more than 800Gbps in 2016 from the perspective of size. One of the biggest DDoS attacks targeted the GitHub in 2018 with a very high rate of traffic. One more such disastrous DDoS attack called "Dyn attack" happened in 2016. It affected the working of many sites such as PayPal, Amazon, GitHub, Netflix, and many more. This attack used a malware named "Mirai" to target these websites. To defend against these vulnerable attacks, more useful research work should be done and efficient intrusion detection system (IDS) should be designed. These IDS systems are very helpful in identifying the attacks in time. Many IDS systems have been developed by researchers and networking companies. A new networking technology "Software-defined networking" (SDN) has also become very famous due to its unique characteristics. Separation of control logic from its data forwarding devices and its centralized global visibility to the entire network topology are two main characteristics of SDN (Nunes et al., 2014). It can become very helpful in DDoS detection using these unique features. SDN can resolve various security issues of conventional as well as trending networking technologies. However, SDN also attracts DDoS attacks due to its centralized controller. DDoS attack targets the SDN controller by sending a large number of malicious packets. By targeting the SDN controller, the whole network can be compromised as a single point of failure. Therefore, efficient defense mechanisms are required to detect the attack in SDN. By overcoming these security issues, SDN serves as a security resolver in a more effective and better way. For these detection mechanisms, machine learning algorithms can be utilized (Michie et al., 1994). Machine learning is widely being used for cyber security. Various machine learning based IDS systems have been proposed by the researchers. They classify the traffic as malicious and normal traffic, which helps to identify the attack. Machine learning based IDS gives better classification results with high accuracy.