Chapter 8
Cluster-Based Countermeasures for DDoS Attacks

Mohammad Jaleb Morshed Chowdhury
Daffodil International University, Bangladesh

Dileep Kumar G
Adama Science and Technology University, Ethiopia

ABSTRACT

Distributed Denial of Service (DDoS) attack is considered one of the major security threats in the current Internet. Although many solutions have been suggested for the DDoS defense, real progress in fighting those attacks is still missing. In this chapter, the authors analyze and experiment with cluster-based filtering for DDoS defense. In cluster-based filtering, unsupervised learning is used to create profile of the network traffic. Then the profiled traffic is passed through the filters of different capacity to the servers. After applying this mechanism, the legitimate traffic will get better bandwidth capacity than the malicious traffic. Thus the effect of bad or malicious traffic will be lesser in the network. Before describing the proposed solutions, a detail survey of the different DDoS countermeasures have been presented in the chapter.

INTRODUCTION

Among the many security threats in the current Internet, Distributed Denial of Service (DDoS) attacks are considered to be one of the most serious. Denials of Service (DoS) attacks aim to make the resources of the computer system of the victim unavailable or unreliable in providing their intended services. In the context of this work, DoS attacks try to consume and exhaust the victim’s bandwidth or the server capacity. In DDoS attacks, the attacker compromises a large number of hosts in Internet and instructs them to conduct a coordinated attack. The network of the compromised hosts is called a botnet. In recent years, a sharp increase in large DDoS attacks has been reported (Figure 1).

While progress has been made in preventing or at least significantly lessening the impact of various security vulnerabilities, real progress in fighting DDoS is still missing. While automated software updates and antivirus programs can limit the number of compromised computers, there are still botnets compris-
Cluster-Based Countermeasures for DDoS Attacks

Figure 1. Size of largest reported DDoS Attack (Gbps)

Another potential defence is to filter the packets sent by the DDoS attacker at a firewall after detecting the attack with and intrusion detection system (IDS). These rule-based detection and filtering techniques have not been successful in filtering DDoS attack because the DDoS attacker can send seemingly legitimate traffic. In the case of open services, such as web servers, the DDoS attacker only needs to send large quantities of useless service requests. Thus, there might be no specific features of DDoS attack traffic that the rule-based filters can be instructed to filter. With such malicious but legitimate traffic, DDoS attackers are able to relatively easily bypass most means of DDoS defence.

This work analyzes and experiment with cluster-based filtering for DDoS defense. In cluster-based filtering, unsupervised learning is used to create a normal profile of the network traffic. Then the filter for DDoS attacks is based on this normal profile. This work focuses on the scenario in which the cluster-based filter is deployed at the target network and serves for proactive or reactive defense.

A game-theoretic model is created for the scenario, making it possible to model the defender and attacker strategies as mathematical optimization tasks. The obtained optimal strategies are then experimentally evaluated. In the test bed setup, the hierarchical heavy hitters (HHH) algorithm is applied to traffic clustering and the Differentiated Services (DiffServ) quality-of-service (QoS) architecture is used for deploying the cluster-based filter on a Linux router.