An Effective Approach to Detect DDos Attack

R. Manoj and C. Tripti

Rajagiri College of Social Sciences,
Kakkanad, Ernakulam,
Kerala, India
manojr11@gmail.com
tripti84_05@rediffmail.com

Abstract. TCP connection is a connection oriented, reliable service. It uses 3 way handshake process to establish the connection. Distributed Denial of Service (DDoS) has emerged as one of the major threats to network security as evident from a series of attacks that shutdown some of the most popular websites. This attack prevents legitimate users from accessing the regular internet services by exhausting the victim's resources, and TCP SYN flooding attack is the most common type of DDoS attack. TCP SYN flooding exploits the TCP's 3-way handshake mechanism and its limitation in maintaining half open connection. The SYN flooding attack is very hard to detect, because it is difficult to distinguish between legitimate SYN packets and attack SYN packets at the victim's server. This paper concentrates on the different IP spoofing techniques like Random spoofed source address, Subnet spoofed source address, Fixed spoofed source address and the schemes to detect the DDoS attack. The different schemes are SYN-dog, SYN-cache, SYN-cookies. These schemes are effective only up to a particular extent. This paper concentrates more on a newly proposed scheme which is a router based scheme that uses Counting Bloom Filter algorithm and CUSUM algorithm. The new scheme is highly sensitive and always require a shorter time for the detection of both low intensity and high intensity attacks.

Keywords: DDos, Flooding, 3 way handshake.

1 Introduction

Distributed Denial of Service attack (DDoS) has recently emerged as one of the major threats to network security as evident from a series of attacks that shut down some of the world's most high profile websites, like Amazon and Yahoo [1]. This attack prevents legitimate users from access the regular Internet services by exhausting the victim's resources [2]. It was found that TCP carries 95% of Internet traffic and 80% of the total number of flows in the Internet [3], so the TCP SYN flooding attack is the most common type of DDoS attack.

N. Meghanathan et al. (Eds.): Advances in Computing & Inf. Technology, AISC 178, pp. 339–345.
springerlink.com

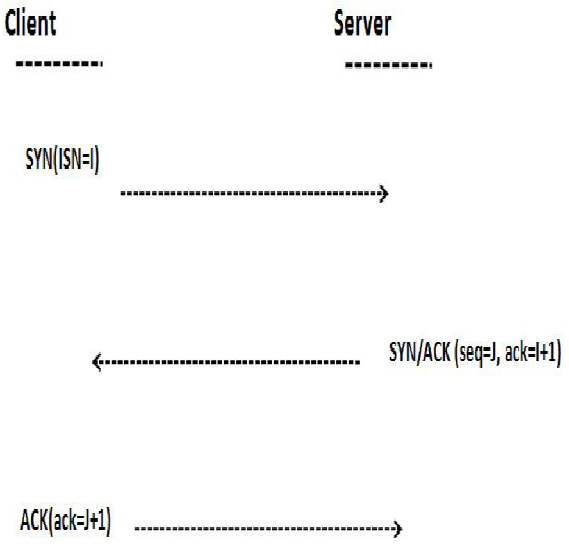

Fig. 1. TCP 3 way handshake

The TCP SYN flooding exploits the TCP's three-way handshake mechanism and its limitation in maintaining half-open connections. In the TCP SYN flooding attack, the attacker first compromise attack machines called masters, which in turn compromise attack machines called agents. The attack scenario begins by ordering agents to send at the same time a stream of flooding SYN packets with inaccessible IP addresses to the victim' server, such that server's backlog queue for half open connections will be exhausted and any new legitimate SYN packets will be dropped. It is notable that SYN flooding attack is very hard to detect, because it is difficult to distinguish between legitimate SYN packets and attack SYN packets at the victim's server.

Many schemes have been proposed for mitigating the flooding effect on the victim, such as [4], [5] and [6], but few have been reported for detecting the SYN flooding agents. A router based detection scheme called SYNdog has been proposed in [7] to sniff SYN flooding sources by exploring the inherent behavior of TCP SYN-SYN/ACK pair without restoring to expensive IP traceback. The idea behind SYN-dog is to explore the inherent abnormal behavior of TCP SYN-SYN/ACK pair under SYN flooding attack for the detection of it. Since one SYN packet of a normal TCP connection will result in the SYN/ACK packet in the reverse direction within one round-trip time (RTT) (please refer to Fig.1), so the difference between the number of outgoing SYN packets and the incoming SYN/ACK packets in a given subnetwork small (may not be zero) under normal condition. Under a SYN flooding attack, however, the number of outgoing SYN packets from the attacker's subnetwork will be significantly higher than the number of incoming SYN/ACK packets, because the attacker sends a lot of SYN packets to the victim at the same time with spoofed IP addresses. To detect the SYN flooding source of a subnetwork based on the above abnormal traffic behavior, the SYN-dog scheme first records the total numbers of the