International Journal of Information Security and Privacy
Volume 14 • Issue 1 • January-March 2020

Comparison of Various DoS Algorithm

Mainul Hasan, University of Petroleum and Energy Studies, Dehradun, India
Amogh Venkatanarayan, University of Petroleum and Energy Studies, Dehradun, India
Inder Mohan, University of Petroleum and Energy Studies, Dehradun, India
Ninni Singh, University of Petroleum and Energy Studies, Dehradun, India
Gunjan Chhabra, University of Petroleum and Energy Studies, Dehradun, India

ABSTRACT

Denial of service attack is one of the most devastating and ruinous attacks on the internet. The attack can be performed by flooding the victim's machine with any kind of packets. Throughout all these years many methods have been proposed to reduce the impact, but with machines of higher capabilities coming in, the attack has also become more potent, and these proposals are either less effective or less efficient. A DoS attack exhausts the victim's resources affecting the availability of the resource. This paper will be comparing a few methods that have been proposed and published in various papers along with a newly proposed method. The comparison of the methods is done on a number of parameters including resource utilization, reaction time, worst case scenarios, etc. This paper also checks the viability of these methods over various layers of the network. Concluding with the best aspects of all the papers and the best among these for the current real conditions.

KEYWORDS

Distributed Denial of Service, DoS, flood attacks, Queue Management

INTRODUCTION

Denial of Service attack is one of the most popular attacks. The capability of the attack to make the resources of the victim's system unavailable just by simply flooding the system with ICMP packets gives a huge advantage to the malicious user. It affects the availability in the CIA triad. A DOS attack is performed by overwhelming the victim's machine with a large no. of request packets to exhaust the resources available in the machine. Another manner of performing DoS is to get the victim's system to perform a resource consuming task, thereby rendering it useless for anyone else (Xiao-Ming, Gong, Qi, & Miao, 2012). Flooding based DoS attack is most commonly performed on the transport layer and the application layer. The transport layer is responsible for establishing the communication channel between two devices, it is more rewarding for an attacker to attack on this layer as a very less amount of research and resource is needed, but the effect is devastating. Internet is still dominated by web traffic which is based on short-lived TCP connection.

Multiple solutions have been proposed over time to solve this problem. The most used methods to solve the problem of flood attack is modifying the packet request queue which can be used to utilize low resources and can be scaled. There are queue management algorithms like FavorQueue (Aneli, Diana, & Lochin, 2014), QRM (Casoni, Grazia, Klapez, & Patriciello, 2015). There are also solutions like Deterministic Fair Sharing (Bedi, Sankardas Roy, & Shiva, 2014).

DOI: 10.4018/IJISP.2020010103

This paper compares the aforementioned AQM methods with our proposed method (Venkatanarayan, Mohan, Hasan, Singh, & Chhabra, 2017).

There have been attempts to perform a behavioral analysis on the networks to identify malicious networks and have more checks on the traffic coming through it (Noh S., Jung, Choi, & Lee, 2008). However, this doesn't scale up. Another suggestion of having trace-backs for each packet and using a marking scheme to identify malicious packets, was suggested. Automata based re-allocation of source to make sure that the legitimate user gets the resource, has also been identified.

Another method that was suggested was, a multi-modal design that portraits different jamming attacks by recognizing the interrelationship between three parameters: signal strength variation, strength of the received signal, and packet delivery rate. The above parameter profiles are generated in normal scenarios during training session and are compared with testing session to identify and classify jamming attacks (Sufyan, Saqib, & Zia, 2013).

An alternate method of detection suggested as DOMLEM, uses dominance based rough set and deals with the uncertainty at multiple layers of the network (Ahmed & Acharjya, 2015).

Muraleedharan and Lisa also discussed about jamming attacks and its detection in wireless sensor networks using ant system (Muraleedharan & Osadciw, 2006). Law et al. studied on link layer jamming attacks (Law, Hartel, Hartog, & Havinga, 2005). They are periodic listening interval, periodic control interval, periodic data packet, and periodic cluster. Wood et al. have also suggested four jamming attack models such as interrupt, activity, scan, and pulse (Wood, Stankovic, & Son, 2003).

This paper will look into the drawbacks of some of the above-mentioned Algorithms and will look into the advantages of using a threshold based AQM. This paper starts with the description of some related works. Then it describes about the threshold based AQM. Then goes on to differentiating in a very basic level of the algorithms and then a discussion is done on the basis of the results.

RELATED WORK

Denial of Service (DoS) is possible on many layers of the network. Use of TCP/IP and UDP packets are however the most commonly used for performing such an attack. There are two major types of DoS attacks that are prevalent, flood DoS and low-rate DoS. The flooding-based DoS attack relies on the multitude of packets that are sent. The low-rate DoS attack exploits the homogeneity of the minimum retransmission output (RTO) of TCP flows and causes link saturation attack. Active Queue Management (AQM), is a common method to address requests. FavorQueue suggests that certain connections which have already established and are in the active queue be given temporary priority, which in case of small Time-To-Live could cause congestion and denial. An approach involving captcha-based verification on the application layer and MAC filtration and cryptography-based authentication is proposed, but this method requires higher memory even during normal conditions. An enhanced AQM using a smaller buffer is suggested (Venkatanarayan, Mohan, Hasan, Singh, & Chhabra, 2017) .

An internet firewall having some local and some global level firewall rules could be implemented to stop an attempt of DoS before the malicious traffic reaches the victim's network, however, this would not work if the attack is happening from inside the same network using remote access (Chang, 2002).

AQM techniques can be broadly classified in two categories based on the type of traffic they can handle. The first category aims to provide fairness when the incoming traffic consists of only responsive flows (e.g. TCP flows). Typical techniques include RED, BLUE, and AVQ. The second category aims to provide fairness when the incoming traffic consists of both responsive and unresponsive flows (e.g. TCP and UDP flows). Well known techniques include CHOKE, SFB, RED-PD, and FRED (Bedi, Sankardas Roy, & Shiva, 2014).

Behavioral analysis of network traffic gives an idea whether flood attack is happening or not (Noh S., Jung, Choi, & Lee, 2008). During a flood attack trace-back gives the source and Pi's marking scheme gives the overlapping of packets and gives a more holistic idea of the flood (LI & SHEN, 2008). Automata based re-allocation of resources is also proposed, to minimize the impact of the