IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# Distributed Denial of Service Attack in Real Time Environment

[1]Kailash Chand, [2]Mohit Sharma

[1]Mtech, [2]HOD CSE,

[1]Computer Science and Engineering,

[1]Yaduvanshi college of Engineering and Technology, Narnaul, India

***Abstract:*** A Distributed Denial of Service (DDoS) attack try to build an online service or a website inaccessible by overloading it with huge pile of internet traffic generated from various sources. Exploited machines can include computers and other networked resources such as IoT devices. A Denial of Service (DoS) attack, in which one computer and one Internet connection are used to flood a targeted resource with packets, but a DDoS attack uses many computers and many Internet connections, often distributed globally in what is referred to as a botnet. A large-scale volumetric DDoS attack can generate traffic measured in tens of Gigabits (and even hundreds of Gigabits) per second. A regular network will not be able to handle such traffic. Attackers build a network of hacked machines known as botnets by spreading malicious code through emails, websites, and social media. Once these computers are infected, they can be controlled remotely, without their owners' knowledge, and used as an army to launch an attack against any target
Keywords: Measurement, Entropy, Communication traffic, Floods, Probability distribution, , Computer crime

## I. INTRODUCTION

A Distributed Denial of Service Attack or DDOS, is an attempt to make a web service unavailable to its intended users. An attacker accomplishes this by flooding the target server with unnecessary network traffic in the form of webservice requests. In this manner, the web service becomes overburdened responding to the requests and it slows downresponses to valid requests from actual users. As the name suggests these attacks are distributed, meaning a group ofcomputers spread over multiple locations but affected by same Trojan virus can be used. Like any other virus it's a computer program that executes remote commands by the attacker on a user's infected computer, without their knowledge. The Trojan infected user's computer is called zombie and a network of zombies makes up a roboticnetwork, called a botnet. A botnet is responsible for DDOS attacks. Your computer could be a zombie i.e. a node of alarger botnet without your knowledge. It is estimated that there are more than 10 million zombies worldwide.

### DDOS ATTACK

when hackers are able to flood an IP address with hundreds or thousands of messages, often through the use of botnetsor through a coordinated activist effort, taking the network to the point where legitimate users aren't able to get through – hence, the denial of service

There are different types of DDos attack

1. .PEER-TO-PEER ATTACKS

The evolution of computing continues to lead to greater decentralization. Mainframes gave way to local areanetworks (LANS), which provided greater economies of scale. The Internet has allowed for even greater distribution capability; peer to peer computing has grown as a result. Examples of peer to peer networks include the popular Kazaa and Napster file sharing services. These types of networks allow for significant transfers of data, yet they are vulnerable to attack from multiple sources.

2. TEARDROP ATTACKS

A teardrop attack is a denial-of-service (DoS) attack that involves sending fragmented packets to a target machine. Since the machine receiving such packets cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, the packets overlap one another, crashing the target network device.

3. LOW-RATE DENIAL-OF-SERVICE ATTACKS

Low-rate denial of service attack on TCP flows that exploits TCP's retransmission timeout mechanism. Theyshow that a square wave pulse equal to the link capacity but lasting only for a short duration (about one to two round-trip times), sent periodically every 1 second, can effectively throttle other TCP flows down to a fraction of their ideal rate. Since 1 second is the minimum retransmission timeout period (minRTO) for TCPflows, such a pulse forces all TCP flows to synchronize with the attacker and remain in slow start with verysmall window sizes. Also, since the ratio of the burst length to the period of the attacking flow is very small (0.1), the average rate of the attacking flow is also small and thus hard to detect at routers.

4. INTERNET CONTROL MESSAGE PROTOCOL (ICMP) FLOOD

An ICMP flood attack is also known as a ping attack in which attackers send a large number of ICMP ping packets to a DNS server repeatedly in order to hinder the server's ability to respond to other requests. It can also be an attempt to send a large number of ping packets to the broadcast IP of a sub network, otherwise known as a Smurf attack, as a basic means of amplifying an attack across more hosts than a normal ping would typically permit. These types of attacks can be dealt with by setting a policy to disallow pings to the broadcast IP on the network.

5. SYN FLOOD

A SYN Flood is a type of DDos attack which aims to make a server unavailable to traffic

Consuming all available resources. By repeatedly sending initial connection request (SYN) packets, the attacker is able to overwhelm all available ports on a targeted server machine, causing the targeted device torespond to legitimate traffic sluggishly or not at all

## LITERATURE SURVEY

[1]Kumar, Mirkovic and Specht presented the taxonomies of attack tools but did not categorized the attack tools andtraffic generators. Hoque and Srivastava provided the taxonomy of DDoS attacks and key features of few popular DDoS attack tools but lack the technical details. Kaur et al. presented the some of the typical DDoS attack tools usedby the attackers but did not give any information about traffic generators and their usage. .. DDoS attacks have seriousconsequences amongst all of the other internet based attacks, e.g., TCP, UDP, ICMP and HTTP flood attacks. The DDoS attacks have targeted not only social networking sites and business enterprises but also government websites, forcing them to close down their websites and causing the loss of millions of dollars. Recently, “Snort " has emergedas an effective open-source solution for more secure network computer systems

[2]Muhammad Aamir (2013) has studied that with the increasing need of information technology, network security is one of the major issue as number of DDoS attacks are increasing at higher pace the various techniques of DDoS attacks and Defense of DDoS attack on the FTP server. The various parameters are observed using the opnet test bedenvironment. Observation parameters are a utilization of CPU, TCP Delay, and processing time and show the effect of DDoS attacks on these parameters. As the size of botnet increases, the effect on these parameters also increases. 3botnet sizes 50,100,200 was considered to launch the attack in this paper. How FTP server gets affected has shown inthis paper.

[3]Firstly Yang Xiang (2011) has discussed about the most destructive type of attack known as low rate DDoS attacks.Authors of [1] have classified DDoS attacks in two categories as flooding and logical (software) attacks. In flooding attacks, they have highlighted SYN flooding, ICMP attack, UDP flooding and in logical attack they have identified ping of death, teardrop attack, and land attack.

[4]Saman Taghavi (2013) has presented about DDOS flooding attack as it is one of the challenging issue to prevent the network security. In this type of attack an armies are set up to launch an attack. Various computers are hired by anattacker, it is called botnets or Zombies, and the coordinated attack is performed by all the hired computers. The appropriate defense mechanism is required to bar the DDOS flooding attacks. The purpose of this paper is to seek about DDOS flooding trouble and the various steps to encounter it. The Study is about the consideration of previous counter steps to handle the DDOS Flooding attacks. The main consideration of this paper is to give the survey of traditional and current handling mechanism which helps the research community to develop their DDOS flooding handling problem when or after attack launched. IlkerOzcelik (2013) has presented about the detection approach on Denial of Services. The detection is based on the anomaly based metrices. The Cumulative Sum (Cusum) approach has applied to detect the effect of the attack on the network. This algorithm is performing at high and low bandwidthof the network. The main purpose of this work is to show the better detection results with the cusum algorithm as it reduces the utilization of the network. This whole work was performed by using the background traffic in the paper's scenario

[5].Arun Pragash, Dr.S.Mercy Shalinie, M.Vijaylakshmi (2012) has studied that IP trace back is the appropriate approach to find the source of the attack. This metric was used to detect the DDoS attacks in the network by tracing the router which is nearer to the incoming traffic. The tracing of the router is done by packet marking scheme in which each incoming packet is marked and then send to the network. This detection technique is used when the attacker launches the attack by sending spoofed IP addresses. These kind of attacks is performed in network and application layer. Proactive traffic shaping and reactive filtering mechanism were also used. It is used to evaluate the efficiency of the system and in this paper the test bed used was NTRO sensor smart and secure environment. The main contribution of this paper is to determine the attacker.

## PROPOSED PROBLEM

Problem formulation

There are different types of DDOS attack as discussed above.

1. Layer 3: IP attacks on the network bandwidth
2. Layer 4: TCP attacks on server sockets
3. Layer 7: HTTP attacks on web server threads
4. Layer 7+: Web application attacks on CPU resources

While examining DDOS attack, we all refer the various layer of OSI model; especially focus is on the seventh layer,the application layer. This layer provides an interface to end user tasks and facilitates different applications and programs. As per survey, total application layer attacks increased from 2011 to 2012 is 42.97%

## DETECTION AND PREVENTION

There are many approaches used to detect and mitigate the effect of DDOS attack. Different approaches have differentlimitations like legal users have to wait more time for service, high false positives, high false negatives, more time consuming and

Complex, require more memory usage etc. Here, I propose one light weight mechanism to detect and mitigate the DDOS attack against web server. My proposed solution divided into three phase.

1. Identify DDOS attack.
2. Differentiate DDOS attack traffic from normal traffic.
3. Mitigate the effect of DDOS attack.

**First phase** is to identify DDOS attack. It is a veryimportant stage to defend against any attack. Attack should be identifying as early as possible before it could lead noticeable damage. If we identify attack after its damage then it isneed less. So,focus is to identify DDOS attack as early as possible before further steps.

**Second phase** is to differentiate DDOS attack traffic from normal traffic. In today's days, attackers use BOTNET machines for attack. This zombie machines (compromised systems) are available easily on internet in few dollars. Soattackers use thousands of such machines for attack against victim (web server). So, my focus is to differentiate that traffic from normal Traffic.

**Third phase** is to mitigate the effect of DDOS attack. After identifying and detecting the attack, next step is to mitigatethe effect of this attack. So, my focus is to increase the availability of web server for legal users by mitigate the effectof DDOS attack

## CONCLUSION

DDoS attacks are rising as a threat. Over the last few years, these attacks have grown in intensity and now have traffic volumes of up to 400 Gbps. These attacks are easy to carry out and do not require great knowledge or access to zero-day vulnerabilities. The duration of the attacks is often just a few hours or even minutes, but this can be enough to inflict a lot of damage at the target site. Currently, amplification or reflection attacks are the most popular attack. These attacks use DNS or NTP servers to amplify the attack traffic by a factor of 50-100 times. This allows small botnets to conduct huge volumetric attacks. Many initiatives can help to protect reflection servers, but there are still more than enough open amplifiers that can be misused. In 2014, we have noticed an increase in compromised UNIX servers being used to launch attacks. They are of great interest to the attacker, since they provide a large bandwidth. DDoS botnets can be rented as a service starting at $5 for small attacks. Application-layer attacks, which target the Web application, are gaining in importance as well as they are difficult to mitigate. They will become even more important in the future as often, attackers adapt their methods during an attack in an attempt to bypass any short termdefense mechanism. In the future, we might see more DDoS attacks coming from mobile devices or even the Internetof Things, but this is currently not happening on a large scale. The motivation of the attacker can vary widely, with hacktivism, profit, and disputes being the main reasons. Considering the ease of conducting large DDoS attacks, Symantec expects that the DDoS growth trend will continue in the future. The likelihood of being targeted by short but intensive DDoS attacks is rising.

## REFERENCES

1. Monowar H. Bhuyan1, H. J. Kashyap1,D. K.Bhattacharyya, Detecting Distributed Denial of Service Attacks:Methods, Tools and Future Directions, The Computer Journal first published online March 28, 2013
2. PyungKoo Park, SeongMin Yoo, Chungnam Nat, Service-Oriented DDoS Detection Mechanism Using Pseudo State in a Flow Router , 2013 International Conference on Information Science and Applications (ICISA)
3. Muhammad Aamir , Muhammad Arif, Study and Performance Evaluation on Recent DDoS Trends ofAttack& Defense, I.J. Information Technology and Computer Science, 2013, 08, 54-65
4. Vijayalakshmi, Shalinie, Arun Pragash, IP Traceback System for Network and Application Layer Attacks, Recent Trends In Information Technology (ICRTIT), 2012 International Conference