Detection and Prevention of Distributed Denial-of-Service (DDoS) attack: A Review

Kamalpreet Kaur[1] Navpreet Kaur Walia[2]
[1]M.Tech Student [2]Assistant Professor
[1,2]Department of Computer Science and Engineering
[1,2]Sri Guru Granth Sahib World University, Fatehgarh Sahib

Abstract— In the advance computer technology, cyber attacks are effecting and surging day by day. The very common one is Distributed Denial-of-Service (DDoS) attack which is on the top speed of destroyer. Distributed Denial-of-Service (DDoS) attack works in very systematic way, like the attacker dispatched this attack from multiple arbitrary systems those are frequently infected with malware-also called botnet. According to this attack, attackers originate the flood of massages which essentially force to shut down the targeted system for denying the services. This paper illustrate about detection and prevention of Distributed Denial-of-Service (DDoS) attack. In this paper we are discussing the existing algorithms and their contribution for the detection and prevention of DDoS attack.

Key words: Distributed Denial-of-Service (DDoS), Botnet, Attacker

I. INTRODUCTION

Network security is a strategy and provision to protect the network from attackers and stop them from entering or spreading on your network. Network security is a specialized field in computer networking that consists of policies adopted to prevent and monitor modifications, unauthorized access and misuse of computer network infrastructure. Network security ensures the authentication with username and password. Many components are there those are efficaciously handles the security of network e.g. network administrator and security software in addition to hardware and appliance. Although the huge protection in advance, attacks are indulging with high rate[6]. There are two main categories of attacks-

A. Passive Attack

Those attacks which does not modify the data and damage the system, just fetch the information are called passive attacks. For example- Wiretapping, Port scanner, Idle scan[6].

B. Active Attack

These are totally opposite to the passive attacks, in these attacks, attackers enforce integrity and availability and does not harm the systems are called active attack. For example: Denial-of-service attack, DNS spoofing, Man in the middle, ARP poisoning, VLAN hopping, Smurf attack etc[5].

The execution of Distributed Denial-of-Service (DDoS) attack is totally different from others. In Distributed Denial-of-Service (DDoS) attack firstly, the attacker build a network- approximately hundreds of thousands or more that they will use to produce traffic flooding to deny the services of victim.

Attackers choose vulnerability hosts those are running weak on network or malware infected. These hosts have either no or out of date antivirus. Then the attacker force the harmed nodes to gain the access of other nodes those are just like vulnerable node. Later new programs are installed on the victim's nodes by the intruders to create the attack network. All the attacks are carried out under the attacker's control by zombies-those are running attack tools. When the number of zombies works together they are form as army. Fig1 shows the information about Distributed Denial-of-Service (DDoS) attack on Stacheldraht software written for Linux and Solaris systems which works as the agent of Distributed Denial-of-Service (DDoS) attack[9].

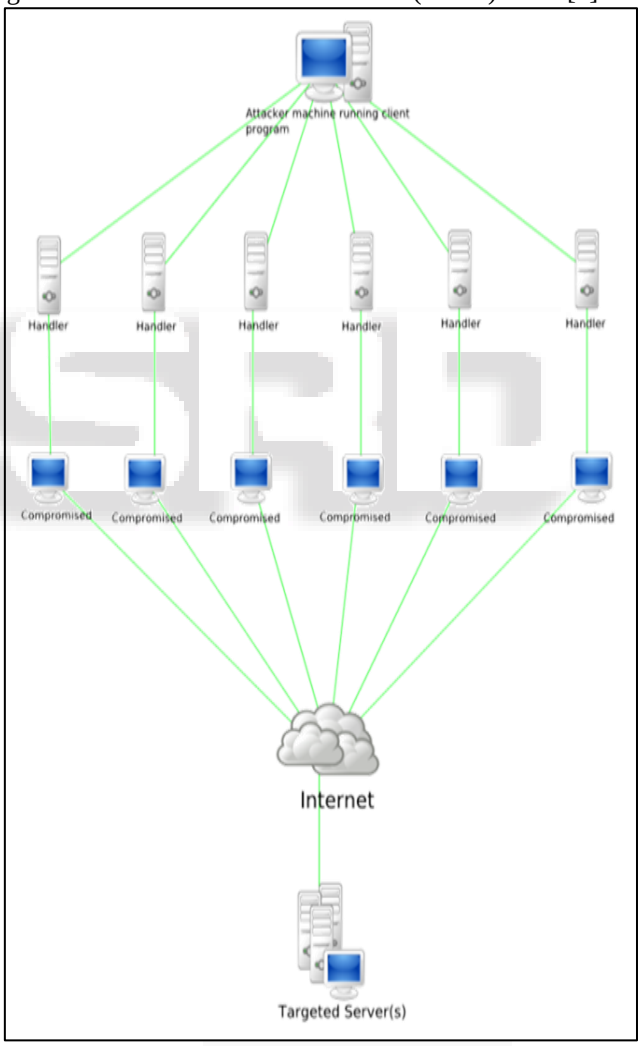

Fig. 1: DDoS Stacheldraht attack[9]

When the intruder originate the high traffic flow, it is totally preposterous to user to identify the rate of user's traffic from attack flow; only by blocking IP address, not makes it possible to prevent the attack.

II. DOS ATTACK

DoS attack is designed as to deny the service of targeted machines. In this attack data may or may not be damaged

directly or permanently but machine stops for limited time period or sometimes degrade the performance of the system or computer can no longer process legitimate user requests. During that time period attacker harm the victim's personal information or any secret data which may be confidential. Mostly the network's bandwidth or connectivity is targeted by DoS attack. These attacks are done for mainly few reasons for example: personal reasons, material grin, or for popularity. DoS attack can be classified into four categories on remote basis[13]:

1) Network Device level
2) OS level
3) Application level
4) Data flood

In the Network Device level DoS attack malware affected systems or hardware recourses are targeted. On the other hand in the case of OS level, attack sometimes crash the system of the victim with the help of in which way the operating system implement the protocols. Pings of attack comes in the category of OS level attacks. In the Application level, the attackers consume the access of resources from the user with the help of weakness of that machine. Finger bomb is example of Application-based attacks. Data flooding attack takes the advantages of bandwidth available to a network. In this the attacker sends the meaningless data with spoofed IP addresses to the victim to exploit the service[13].

III. DDOS ATTACK

Distributed Denial-of-Service (DDoS) attack is an open problem to date which poses a critical threat to the network [5]. Nowadays it becomes very complex and very difficult to detect. As the attackers are becoming very smart and modify their tools to cross the security systems, on the other hand the searchers are developing new and advance approaches to handle the attacks as well. Although we have so many techniques to detect the DDoS attack but many times we just fail to detect the ongoing DDoS attack, just because of four reasons[14]:

1) When the attack happens there is very little time to detect because to ascertain the attack the system administrators and security experts will have less than one hour.
2) Sometimes internet worms make it very complex while propagation of these worms directly result in DDoS attack.
3) Some useful defence measures those are used for detection and prevention of this attack like packet filtering, rate limiting, tweaking software parameters may limited in their capabilities.
4) Main problem is that sometimes we does not recognize the difference between the DDoS attack and flash crowds.

DDoS Strategy[13]:

- The attacker who plans to attack on the internet.
- The handlers are capable of handling multiple agents with running special programs.
- The agents or zombies, those are responsible for generating the flood of traffic towards the victim. If the attack traced back in any case, it degrade the liability of the attack.
- A victim.

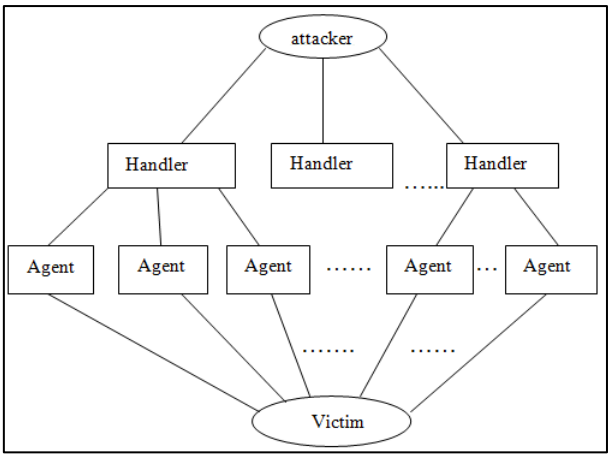

Fig. 2: Architecture of DDoS attack[13]

For preparing and conducting the DDoS attack few steps are takes place [13]:

1) Selection of agents. Firstly the attacker gains the accesses of number of machines so that attack should be strong and choose some agents those are capable to perform the attack. It is handled automatically by scanning tools nowadays.
2) Compromise. Here the attacker plans the attack by hacking those are machines which are malware affected. Because these types of machines are very weak to gain access. Attackers secure the code so that it could not be discover or deactivated. The owner of the system has no knowledge about the participation in the attack because only small amount of memory and bandwidth is used, so that the user does not realize the minimal changes in performance.
3) Communication. The attackers communicate with number of handlers to discuss about when to launch the attack and to gain the information about agents that which is running and to upgrade them. Furthermore the handlers communicate with agents about attack and this process is done via TCP, UDP or ICMP protocols.
4) Attack. Attack should be variety of properties so that it could not detect. So many parameters are considered for attack e.g. type, length, TTP, port number etc.

Nobody knows about when Distributed Denial-of-service (DDoS) attack was launched. According to Ponteves (commune in the Ver department in the France) this attack was occurred against IRC server which affected the 227 systems and shut down the server for days at University of Minnesota in 1999[16]. After that it becomes very popular and every year we face so many problems related to this attack.

IV. LITERATURE SURVEY

In this section, various techniques of the existing algorithms of DDoS attacks are discussed as following:

1) Moderate Denial-of-Service attack detection based on Distance flow and Traceback Routing[1]:They uses Trace back Routing Algorithm and Distance flow to detect the Distributed Denial of Service (DDoS) attack in routers by analyze the both inbound and outbound traffic of routers. Firstly location of attack flow is identified in upstream router then traceback request is submitted until the zombies are not identified.

2) Lightweight DDoS Flooding Attack Detection Using NOX/OpenFlow[2]: They described the lightweight method for detection of Distributed Denial of Service (DDoS) attack with the help of NOX platform to handle the switch information. They also use Self Organizing Maps for increase the rate of detection and decrease the rate of false alarms. They compare their approach with KDD-99 and prove that their proposed work is able to monitor more than one observation point and extracts features of interest with a low overhead.
3) Statistical Approaches to DDoS Attack Detection and Response [3]: They used the computing entropy and frequency-sorted distributions of selected packet attributes to detect the DDoS attack. In this they use live traffic traces for the performance and accuracy of the detection from a variety of network environments ranging from points in the core of the Internet to those inside an edge network.
4) Prevention of DDOS Attacks using New Cracking Algorithm[4]: They described the new cracking algorithm for the detection and prevention of DDoS. This algorithm stores the IP address of every user who is logging in to the website and matches the IP address from history at every visit. If the client visited the website more than five times then visitor will be saved as attacker and service could be halted.
5) Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient[5]: They recite discrimination algorithm using the flow correlation coefficient as a similarity metric among suspicious flows to differentiate DDoS attacks from genuine flash crowds. They analyse that attack flows are usually more similar to each other compared to the flows of flash crowds on the basis of size and organization of current botnets.
6) Mitigating DDoS attack and Saving Computational Time using a Probabilistic approach and HCF method [15]: They depict the probability method in which malicious packets are detected by the calculation of hop count. In this two methods are followed for the detection of DDoS attack: Probabilistic approach and HCF method. In HCF method they examine the whole packets if they are not malicious only then they are allowed to enter into server. On the other hand, in probability approach they only calculate the probability of the malicious packets and reduce the overhead in this approach.
7) IP Traceback-based Intelligent Packet Filtering: A Novel Technique foe Defending Against Internet DDoS Attacks[7]: They discussed the method to obtain the information about whether the attack is held on the network node or not with the help of IP Trace-back technique. This technique slightly eliminate the affect of DDoS attack at preliminary stage and increase the throughput of systems by 3 to 7 times during the attack.
8) Joint Entropy Analysis Model for DDoS Attack Detection[11]: They discussed that the IP-flow number and aggregate traffic size are strongly dependent and uses Joint Entropy Analysis method for the detection of DDoS. they observe that the occurrence of attack causes the rupture in time series of joint entropy values and dependence of traffic size and IP-flow number.

DDoS Techniques	Parameters	Advantages	Future Work
Flow Correlation Coefficient[5]	Flash crowds, similarity, discrimination	Effectiveness of algorithm in practice	tradeoff between detection accuracy and cost
NOX/OpenFlow [2]	Programmable Networks, Artificial Neural Networks.	High rate of detection and very low rate of false alarms	statistical methods to analyze ports of OF switches to determine attack launching nodes
Packet Filtering	Filtering, Confidence, Correlation Pattern, Cloud Environment	Fast response when attack occurs	To accelerate the speed and the filtering accuracy of CBF, hash algorithm should be used.
IP Traceback-based Intelligent Packet Filtering[7]	IP Traceback, Performance Modeling and Simulation.	Packets come from attackers are effectively Filtered out	Probabilistic marking with IP Traceback

Table 1: Comparison of various techniques of DDoS attacks

V. CONCLUSION

It is concluded that to work securely on gadgets some stronger technology is to be used, to prevent and detect the Distributed denial-of-service (DDoS) attack. We have discussed about existing algorithms those do a lot for the detection and prevention of DDoS . There are some parameters of attack those help us to recognize attacks such as flood of traffic, degradation of performance etc. In future, we would try to develop such methods which will help us to detect and prevent the affect of Distributed denial-of-service (DDoS) attack more effectively.

REFERENCES

[1] Vinish Alikkal, Dr.T.Senthil Prakash, D Yuvraj "Moderate Denial-of- service attack detection based on distance flow and traceback routing" international journal on engineering technology and sciences – IJETS™ VOLUME 1, ISSUE 7, NOVEMBER 2014.
[2] Rodrigo Braga, Edjard Mota, Alexandre Passito "Lightweight DDoS Flooding Attack Detection Using NOX/OpenFlow" 35th Annual IEEE Conference on Local Computer Networks, pp. 408-415, 2010.
[3] Laura Feinstein, Dan Schnackenberg "Statistical Approaches to DDoS Attack Detection and Response" DARPA Information Survivability Conference and Exposition (DISCEX), IEEE, 2003.

[4] V.Priyadharshini, Dr.K.Kuppusamy "Prevention of DDOS Attacks using New Cracking Algorithm" International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, pp.2263-2267, May-Jun 2012.
[5] Shui Yu et.al,"Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient" IEEE Transactions On Parallel And Distributed Systems, VOL. 23, NO. 6, pp.1073-1080, June 2012.
[6] Jatinder Teji et. al, "Detection and Prevention of Passive Attacks in Network Security" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 6, November 2013.
[7] Minho Sung and JunXu, "IP Traceback-based Intelligent Packet Filtering: A Novel Technique foe Defending Against Internet DDoS Attacks" 10th IEEE International conference on network protocols, Nov. 15, 2002.
[8] Satyam Shrivastava et. al, "A Brief Introduction of Different type of Security Attacks found in Mobile Ad-hoc Network" International Journal of Computer Science & Engineering Technology (IJCSET) Vol. 4 No. 03, pp.218-222 March 2013.
[9] "Denial-of-Service Attack" Available from https://en.wikipedia.org/wiki/Denial-of-service_attack.
[10] Stuti Singh, Roshan Srivastava "Intrusion Detection Using Data Mining Technique" International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-2, Issue-4, March 2013.
[11] Hamza Rahmani et. al,"Joint Entropy Analysis Model for DDoS Attack Detection" Fifth International Conference on Information Assurance and Security, pp.267-271, 2009.
[12] Y.Dhanalakshmi, Dr.I. Ramesh Babu "Intrusion Detection Using Data Mining Along Fuzzy Logic and Genetic Algorithms" IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.2, February 2008.
[13] Christos Douligeris, Aikaterini Mitrokotsa, "DDoS attacks and defense mechanisms: classificationmand state-of-the-art" Elsevier B.V., pp. 643–666, 2004.
[14] Shuyuan Jin, Daniel S. Yeung "A Covariance Analysis Model for DDoS Attack Detection" work is supported by a Hong Kong RGC project researchgrant number B-Q571, IEEE Communications Society, 2004.
[15] Biswa Ranjan,Swain Bibhudatta Sahoo "Mitigating DDoS attack and Saving Computational Time using a Probabilistic approach and HCF method" IEEE International Advance Computing Conference (IACC), pp. 1170-1172, March 2009.
[16] "DDoS: A Brief History" Available from https://blog.fortinet.com/post/ddos-a-brief-history

