RESEARCH ARTICLE OPEN ACCESS

Literature Review on Prevention and Detection of DDoS Attack

Inzimam Ul Hassan[1], Amandeep Kaur[2]
1(M.tech scholar, Lovely Professional University Jalandhar)
2(Assistant Professor, Lovely Professional University Jalandhar)

Abstract:

In today's world rate of internet is becoming so popular that everyone is using. It is not used only by researcher but it is used by everyone to share information. So all the information that is transmitted to any part of world is being transmitted through the internet. Therefore this internet needs to be safe, reliable and more secure. With the rise of internet there is an exponential rise in the number of attacks. Among all the attacks DDOS (distributed denial of service) is the most disruptive and intense attack for depleting the resource or the bandwidth of the network.

Keywords— **Denial of Service (DoS), Distributed Denial of Service, System security, Attacks.**

I. INTRODUCTION

Computer network technology may be an important technology for many of the applications. So security for these applications is most important. As network security is a great requirement in the growing networks, there is a lack of security techniques that can be implemented easily. There are many loopholes in the network security as there exists a communication barrier between the network security technology developers and the network developers. Network design is a well-established process that is basically based on Open System Interface (OSI) model. There are so many advantages of OSI model for network designs. OSI model offers flexibility, modularity, ease-of-use and standardization of protocols. The protocols that are used at different layers of the OSI model can be combined easily to create a stack that allow the development of the modules. The implementation of the individual layers of OSI model can be changed afterwards without making other changes which allows the flexibility in the network development.

In comparison to the design of networks, secure design of network is not a well-developed process. There is not a defined methodology for managing the complexity of requirements of security. Secure design of network does not contain the same advantage as that of the design of a network. For considering the network security, there must be emphasis that whole of the network is secure. Security of a network does not concern only the computers at each end of the whole chain of communication. The communication channel in between should not be vulnerable to the security attacks while transmitting the data. The attacker in the middle of the network could attack the communication channel, obtain the information, then it can decrypt the data and then re-insert that false message.

II. Network security attacks

Security attacks may be defined as any attempt that compromises the security of thedata owned by any organization. These attacks are divided into many categories. Someof the attacks are used to gain personnel information or system knowledge. Otherattacks are used to interfere with the planned function of the system. Some attacks areused to consume all the resources of the system uselessly. Security attacks squaremeasure classified as active and passive attacks.An active

attack is that type of attack in which the attacker tries to alter the resourcesof the system or affects the operations of the system. A passive attack is that sortof attack within which the wrongdoer uses the info of the system however doesn't havean effect on the resources of the system.

1. *Passive attacks*

Passive attacks monitor the traffic and transmission of the data. The aim of the attacker is to gain knowledge of data that is being transferred.

2. *Active attacks*

Active attacks are that type of attacks that involve the alteration of the data or involve the forming of the false data stream.

III. Denial of service attacks

This type of attack actually inhibits or prevents the normal use of communicationfacilities. It can disturb the whole network either by overburdening the network with the message so that the performance of thenetwork gets degraded or by disabling thenetwork. It can either have a particulartarget or it can degrade the whole network.Active attacks have the reverse features of the passive attacks. As the passive attacksare hard to get detected but there are measures available to prevent the passive attacks.On the other hand, the active attacks can be detected but is very difficult to preventthem. It is because of the great variety of the software, network and physicalvulnerabilities.

IV. Distributed Denial of Service Attacks

Distributed Denial of Service Attack is a type of attack in which an attacker creates alarge effect on the target by multiplying the influence of attack derived from largenumber of computer agents. The attacker controls a large number of computers overthe internet before attacking. The attacker utilizes the weakness of these computers byusing some hacking techniques or by inserting malicious code so as to make these Computers under his control. These computers are usually called as zombies. The groupof zombies is termed as botnet. The magnitude of the attack depends upon the size ofthe botnet. Larger the botnet more disastrous and severe will be the attack. In a botnet, handlers are chosen by the attacker that perform control functions and passall the guidelines of the attacker to the zombies and also the information that theyreceive from zombies to the attacker about the victim under each handler there is agroup of zombies and these handlers communicate with the zombies and the attacker[1]. Zombies and the handlers are the machines from the public network but the usersof these machines do not know the fact that these computers are used as botnet.

A DDOS attack uses many computer system in order to launch an attack. The attackersends-off a synchronized DOS attack against one or many target computers. By using the client server technology the attacker tries to increase the effect of DOS by using theresources of multiple unknowing computers that serves as the platform for the attack.The most important DDOS main program is installed on one of the computers using theaccount that is stolen. At a defined time the master program communicates to anynumber of programs installed on different computers at different places that act asagents. After getting the command, the agent initiate the attack. By using the client servertechnology, the main program installed on a certain computer can initiatehundreds or thousands of agents program within no time.

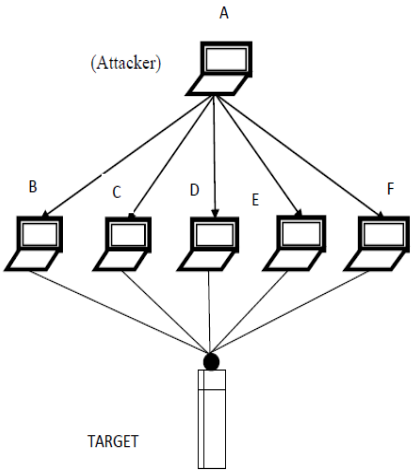

Fig. 1: DDoS attack

V. LITERATURE SURVEY

Ingress/egress filtering

Network Ingress Filtering is a mechanism that a router should not receive the packets whose source address is not reachable [1]. The ingress filtering prevents the packets having spoofed sources from entering the network. The firewalls that are connected to a network are having some interface connected to both the internet network and the internal network. If firewalls apply the ingress filtering to the internet interface and drop all the packets that have source address of the internal network then it can prevent the attacker to masquerade the attack as a host within the same network [2]. Egress Filtering is a type of filtering applied to the packets of the internal interface that are going out of the network. In egress filtering the firewall drops all the packets that are having the source address that do not belong to the local network. If these methods are applied to the network these will help to prevent the DDOS attacks using IPspoofing.

Rate limiting mechanism

This type of mechanism is used to limit the rate of arriving packets that are matching the criteria of Distributed Denial of Service Attacks. This mechanism limits the rate of harmful packets only so the legitimate traffic is not effected at all. The main job is to limit the rate of aggregates instead of IP source addresses. Aggregates are the subsets of traffic having some characteristics. If the routers detect that the aggregates are overpowering them then they send a message and information about it to the upstream router so as to rate limit it [3]. If the rate limit is respected by the aggregate packet then it is allowed to go through, otherwise these packets are dropped and the message is again sent to upstream router. Other rate limiting methods are also used. These methods detect the bandwidth attack by analysing an asymmetry between all packets that are coming to the network or going from the network. If it is analysed that the host is not replying to all the packets being sent to it, then it is an indication for the host being attacked by Distributed Denial of Service Attacks.

SYN Cookies techniques

This technique known as SYN cookies technique [6] is a successful defence mechanism for SYN flood attacks. By using this method the server stores the SYN/ACK packet authentication information instead of an Initial Sequence Number (ISN) of the SYN packets. The verification data stored is the sequence number i.e. the authentication cookie that is generated and stored by the server. This code is generated after the server responses of the requesting party with a SYN ACK packet. The hash function i.e. MD5 is used by the server on some parameters of the packet to calculate the sequence code. The parameters used to calculate the hash function are the source port, address of source, destination port, maximum segment size value and the address of destination. A counter is used that is calculated after every minute. After every bootof the server a secret value is changed which is also used. After receiving the packet which has an ACK flag set which is

last step of a three-way handshake the server verifies the cookie. It establishes the connection only if the value found is correct. This technique is a responsive method for protecting from SYN flood attack, but it is a victim-and method [5].

Hop count filtering

This mechanism is a perfect filtering mechanism that is used at the victim-end to observe the Time to Live (TTL) value of all the incoming packets. This time-to-live value of the packet is observed and then the value of TTL is guessed that should be inserted in the sender's packet. So hop count is the difference between the initial TTL value and the observed values [4]. A table of frequently communicating users is maintained by the victim-end server that contains their IP addresses and the respective hop counts. When there is any DDOS attack, the packets that have the spoofed source address are dropped as they have no entry value or their source address is not matching with the hop counts. This type of technique is used at victim-end and it protects the victim against direct DDOS attacks [5].

Captcha based defence

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is the most operative mechanism in countering the application layer Distributed Denial of Service Attacks in present times [5]. In this technique a challenge-response test is made with a user requesting for establishing a connection with the server. The main purpose of this connection is to assure that reply generated is from the human and not from a computerized machine that is aiming to target the server. Today the CAPTCHA is used by many websites from login and registrations so as to provide the safety to the servers against application layer DDOS attacks.

Dward mechanism

DWARD (DDOS Network Attack Recognition and Defences) is the DDOS defence mechanism which is installed at the source end system. It detects all the outgoing Distributed Denial of Service Attacks and stops it by regulating all the traffic that is outgoing to victim. It also provides good service to the legitimate traffic between installing network and target during the attack. DWARD can distinguish the genuine, attack and suspicious traffic. DWARD also limits the rate of all traffic for a target that is recognized to be in the danger of attack and then gives the preference to the genuine traffic to go for the other connections and destinations [7]. DWARD can function either as a member in a distributed defence system or as the independent system.

Use of Neural Networks in DOS Detection

As artificial neural network is known as a model for learning as they have the ability to handle the demands of the varying environments [8] .These models are good choice for the processes that require fault tolerance, robustness and parallelism as these models are self-organising and self-learning. This self-organising property of these models make them good enough so as to resist and identify the unidentified disorders in that system. So some of the properties of neural networks to identify the DOS attacks as neural networks are accomplished of recognising the unidentified patterns in a system. Authors in [9] have taught backpropagation neural network to estimate total quantity of the zombies that would be after the DOS attacks. The system was taught with dataset of deviations in which traffic entropy is given as input and number of zombies that were after a DOS attack are as output. 10 to 100 zombies were trained using a dataset having 5 as increment. There was a constant rate of attack strength of 25mbps. Different

random inputs of entropy deviations were used to test the model and it was seen that the backpropagation neural network output was seen favourable having few or little errors.

New craking algorithin

Due to increase in number of users on internet, many people want to attack other system resources. Competitors also want to make their web site more popular than others. So they want to attack the service of other's web site. They keep on logon to a particular web site more times, and then service provided by the web server performance keeps degraded. To avoid that one, this application maintains a status table. In that it keeps the IP addresses of current users and their status. If the particular IP address has been signed on for a first time, it makes the status as genuine user. For 2, 3, 4 it marks as Normal user. For the fifth time it makes the particular IP address status as Attacker. In the time calculations we are only consider 5 times. User wish to server increase the time depends up on the application. After that, the user cannot allow get the service of that particular web site. The service is denied to that particular IP address [10].

Packet monitoring TTL approach

In the proposed algorithm, hop count filtering (HCF) technique is used to detect the DoS attack in a cloud network. It is deployed at cloud environment. In this algorithm, the data packets are monitored continuously over the cloud network and three parameters are extracted from that packets, a) SYN flag, b) TTL and c) Source IP [11]. There are four possible scenarios for each packet evaluation:

i. If a data packet is received and there is information of IP2HC table. Extract the parameters such as SYN flag, source IP and TTL. If the source IP is already available in the table and SYN flag is HIGH then calculate hop-count using TTL information. If the calculated hop-count matches with stored value of hop-count in IP2HC table then do nothing. Otherwise, update the stored hop-count field in IP2HC table with this new hop-count for that source IP. [11]

ii. If the SYN flag is HIGH but the source IP does not exist in IP2HC table then calculate the hop-count, add a new entry for this new IP and store the calculated hop-count for the corresponding IP in IP2HC table.

iii. If the SYN flag is LOW and source IP exist in the IP2HC table, then calculate the hop-count. If the calculated hop-count matches with the existing hop count of IP2HC table for the corresponding IP then this packet is real otherwise this packet is spoofed.

iv. If the SYN flag is LOW and the source IP information is also not present in IP2HC table then it is sure that this received packet is spoofed because every genuine packet always contains valid IP information of the source in IP2HC table.

This algorithm only needs information of SYN, source IP and TTL. Using TTL value, hop-count is calculated which is then compare with the stored of value of hop-count of IP2HC table. Using only these three parameters, the authenticity of a received data packet is analysed. Hence on detection of spoofed data packets, the server simply ignores that packet and be ready to serve a genuine user [11]. Its drawback is that the algorithm requires continuous monitoring of packets travelling over the network in the Cloud.

Filter based approach.

Bloom filter based approach the Multicast enables the sender to reach a large number of receivers even though it only sends each packet once. The use of Bloom filter creates a probabilistic element in packet forwarding which reduce the vulnerability of DDoS attack. It mainly focuses on injection attacks [12]. Without giving many details attackers can derive new filter and inject attacks. This can be eliminated and also vulnerability is

reduced. Another approach is flow –level filtering which reduce the vulnerability of low rate DDoS attacks in TCP. Instead of sending large Data to network the attack send traffic at particular interval of time this is said to be a low –level DDoS attack or screw attacks. By using a filter based approach the attacks and also vulnerability can be reduced.

Software puzzle based approach

In this approach the DDoS attacks can be eliminated. The client can request a service and server provides a service only after clients solves software puzzle. This will be generated dynamically. If a client solves a puzzle the requested service will be provided. In this they reduce the vulnerability of DDoS attack happening because the human only solves a puzzle [13].

Identifier-LocationSeparation approach.

This is one of the best solutions to the DDoS attack problem. The attack can be prevented by this approach. In this approach the network nodes are represented by identifier namespace and location namespace. This approach which follows a mapping service [14]. Normally attackers attack a system first selecting a zombie's machine and then forward a packets and increase traffic to that machine. I this identifier and location approach which provides a service to user only after they finding a location. Hence, the vulnerability of DDoS attack happening are also reduced and also illegal attacks packets sending to particular machine is also going to be reduced.

Fuzzing based approach.

Most of DDoS attacks are happened due to improper protocols or it may due to some of vulnerable computer system. Buzzing based approach is a best solution to the problem. Whatever implemented in the system, it must be tested with the fuzzing tools [15]. Before implementing a software or new protocols it might be tested with fuzzing tool. It defines the vulnerability percentage. According to that output of fuzzing tool we decide and implement a new system or protocol in network system. For example we can test the robustness of the system and also we can test network protocols robustness etc.

VI. Conclusions

In this paper, an apparent vision of the DDoS attack is attained and discussed numerous techniques are discussed to prevent and alleviate these attacks. Due to an alarming increase in DDoS attacks, internet security from these attacks becomes vulnerable issue. Having clarified view of the attack, effective countermeasures can be implemented to fight against these attacks.

References

1. *L. Zhang, S. Yu, D. Wu and P. Watlers, "A Survey on Latest Botnet Attack andDefense", In Proceedings of 10th International Conference on Trust, Security andPrivacy in Computing and Communications, IEEE, pp. 53-60, 2011.*

2. *P. Ferguson et. al., "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", Technical report, The Internet Society, 1998.*

3. *Vern Paxson, Steve Bellovin, Sally Floyd and Ratul Mahajan, "Controlling high Bandwidth Aggregates in the Network" A Technical report 2002.*

4. *H. Wang, C. Jin, and K. G. Shin, "Defense against Spoofed IP Traffic using HopCount Filtering", ACM Transactions on Networking. Vol. 15, pp. 40 – 53, 2007.*

5. *H. Beitollahi and G. Deconinck, "Analysing Well- Known Countermeasures against Distributed Denial of Service Attacks" In Computer Communications, Elsevier, Vol. 35, issue 11, pp. 1312-1332, 2012.*

6. *W. Eddy, "TCP SYN Flooding Attacks and Common Mitigations," RFC 4987, August 2007.*

7. *J. Mirkovic and P. Reiher, "D-WARD: A Source-end Defence against flooding denial of Service Attacks", In IEEE Transactions on Dependable and Secure Computing, Vol. 2, pp.216-232, 2005.*

8. *Y. Liu, B. Cukic, and S. Gururajan, "Validating neural network-based online adaptive systems: a case study," Software Quality Journal, Springer, vol. 15, no. 3, pp. 309-326, May 2007.*

9. *B. Gupta, R. C. Joshi, M. Misra, A. Jain, S. Juyal, R. Prabhakar, and A. K. Singh, "Predicting Number of Zombies in a DDoS Attack Using ANN Based Scheme," Communications in Computer and Information Science, Springer, 2011, vol. 147, part 1, pp. 117-122.*

10. *V.Priyadharshini, Dr.K. Kuppusamy / International Journal of EngineeringResearch and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.2263-2267*

11. *I*nternational Journal of Computer Applications (0975 – 8887) Volume 115 – No. 8, April 2015

12. *Moti Geva, Amir Herzberg, and Yehoshua Gev \," Bandwidth Distributed Denial of Service: Attacks and Defenses", Copublished by the IEEE Computer and Reliability Societies January/February 2014.*

13. *Yongdong Wu, Zhigang Zhao, Feng Bao, and Robert H. Deng," Software Puzzle: A Countermeasure to Resource-Inflated Denial-of-Service Attacks", IEEE Transactions on Information Forensics and Security, Vol. 10, No. 1, January 2015.*

14. *Hongbin Luo, Yi Lin, and Hongke Zhang, Beijing Jiaotong University Moshe ukerman, City University of Hong Kong," Preventing DDoS Attacks by Identifier/Locator separation", IEEE Network • November/December 2013.*

15. *Tero Rontti, Anna-Maija Juuso, and Ari Takanen, Codenomicon Ltd. ," Preventing DoS Attacks in NGN Networks with Proactive Specification-Based Fuzzing ", IEEE Communications Magazine • September 2012.*

16. *Inzimam Ul Hassan and A. Kaur, "Prevention and detection of DDoS attack on WSN," pp. 245–249, 2018.*