A REVIEW ON DDOS PREVENTION AND DETECTION METHODOLOGY

Subramaniam.T.K[1] and Deepa.B[2]

[1]M.E.Scholar, Department of Computer Science & Engineering Nandha Engineering College, Erode, Tamil Nadu, India
[2]Assistant Professor, Department of Computer Science & Engineering, Nandha Engineering College, Erode, Tamil Nadu, India

ABSTRACT

Denial of Service (DoS) or Distributed-Denial of Service (DDoS) is major threat to network security. Network is collection of nodes that interconnect with each other for exchange the Information. This information is required for that node is kept confidentially. Attacker in network computer captures this information that is confidential and misuse the network. Hence security is one of the major issues. There are one or many attacks in network. One of the major threats to internet service is DDoS (Distributed denial of services) attack. DDoS attack is a malicious attempt to suspending or interrupting services to target node. DDoS or DoS is an attempt to make network resource or the machine is unavailable to its intended user. Many ideas are developed for avoiding the DDoS or DoS. DDoS happen in two ways naturally or it may due to some botnets .Various schemes are developed defense against to this attack. Main idea of this paper is present basis of DDoS attack. DDoS attack types, DDoS attack components, survey on different mechanism to prevent DDoS.

KEYWORDS

DDoS, Security, botnets

1. INTRODUCTION

In the web service and network computer system's large number of computer machines are connected through geographically distributed network. Attacks and security is a major problem in computer networks. The web service or network security is a process of gaining unauthorized access to network. And also the attacks play a major role in security. The attacks are classified into two type's active attacks and passive attacks. The network intruder intercepts data travelling through the network is called as a passive attack. Wire tapping, idle scan and port scanner are examples of passive attacks. Intruder initiates command to disrupt networks normal operation. This is called active attacks. Denial-of-service attack, spoofing, Man-in-middle attack, buffer over flow, heap over flow are examples of active attacks.An "attack" is one of the exploitation flaws in a network computing system (operating system, software program or user system) for purposes that are not known by the system operator and that are generally harmful.Attacks are always taking place on the internet, at a rate at which the several attacks per minute on each connected machine. These attacks are mostly done automatically from infected machines (by

DOI:10.5121/ijasa.2015.3301

Trojan horses, viruses, worms, etc.) user of the computer does not know about it. In some cases, these are launched by computer attackers or hackers.

2. RELATED WORK

The DDoS or DoS is one type of active attack. .The DoS attacks which means that the attackers send certain messages to the vulnerabilities leading to the abnormality or it may send attack messages quickly to a anyone node to run out the network system resources, resulting in business network system failures. As the process of stopping the optimization vulnerabilities of the performance to the network business systems, the DoS attack might be simple. A DDoS or DoS attack is small for Distributed Denial of Service attack, which is developed on the concept of DoS attack and the multiple distributed attack sources. The attackers usually, use a more number of controlled zombies which are distributed in different locations to promote a large number of denials of service attacks to a single target server or multiple target machines. With the rapid development of attackers in recent years, the attack traffic caused by DDoS or DoS attacks has been growing, with the destination attack, including not only Internet infrastructures such as routers and firewalls and also business servers, and utilize network bandwidth. The attack influence ratio has become broader.

2.1. Attack

An attack usually is perpetrated by someone with bad intentions: Black hated attacks falls in this category; while other perform Penetration testing on an organization information system to find out if all foreseen controls are in place. The attacks can be classified according to their origin: i.e. if it is conducted using one or more computers: in the last case is called a distributed attack. Botnets are used to conduct distributed attacks. Other classifications are according to the procedures used or the type of vulnerabilities exploited: attacks can be concentrated on network mechanisms or host features.

Some attacks are physical: i.e. theft or damage of computers and other equipment. Others are attempts to force changes in the logic used by computers or network protocols in order to achieve unforeseen (by the original designer) result but useful for the attacker. Software used to for logical attacks on computers is called malware. Active attacks includes wiretapping, Port scanner, Idle scan.etc., passive attacks includes Denial-of-service attack ,spoofing, Man in the middle attack, Ping of death, Buffer overflow, Heap overflow, Stack overflow, Format string attack.

In computer and computer networks an attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. An attack can be active or passive. An "active attack" attempts to alter system resources or affect their operation. A passive attack attempts to learn or make use of information from the system but does not affect system resources. An attack can be perpetrated by an insider or from outside the organization. An inside attack is an attack initiated by an entity inside the security perimeter, i.e., an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization. An outside attack is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system. In the Internet, potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

3. TYPES OF ATTACK

3.1. Bandwidth-based attacks

This type of DDoS attack can send mass junk data to cause the server to be overloaded, leading to the consumption of network bandwidth or network equipment. Resource processed by firewall is also limited. Overload traffic leads to failure of network and reduce a quality of service.

3.2. Traffic-based attacks

In this traffic based method the botnets send legimate traffic to target server, which causes a flooding attacks. The server cannot respond and cannot able to handle a request cause DDoS.

3.3. Application-based attacks

This type of attack, send specific data massages to application layers according specific feature. This done for some business specific attack which causes business performance.

3.4. Direct flooding attack

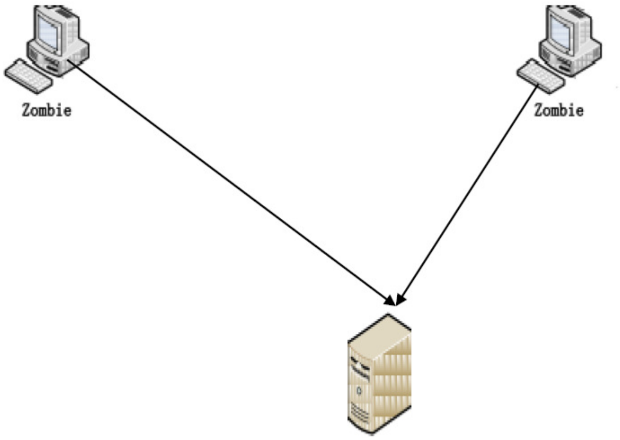

Fig. 1 Direct flooding attacks

Normally DDoS attacks are happened by overloading the server. the one type of attack is said to be a direct flooding attacks . In direct flooding attacks te zombie machines directelly send attacks packets inoreder to increase the bandwidth. This will decrease the processing capacity of the server and network devices which cause the Denial of Services.

The direct is mainly cateriozed into two types ICMP AND IGMP. ICMP stands for Internet Control Message Protocol (ICMP). This ICMP is a underlying core protocol in TCP/IP suite. This protocol is mainly used to send control messages. It is also used to report errors during communication failures. the attacker send a ICMPmessages to target which consues a more bandwith which results in Denial of service attack.

The IGMP stands for Internet Goup Management Protocol. This IGMP protocol which is used in router as well as host to establish a multicast member ship. The attacker take the advandatage of IGMP and send flood message packets to network which may results in Denial of Service.

3.5. UDP Flood attacks

The UDP stands for User Data Gram protocol. Main advantage of UDP is a connection less protocol and also it does not need sequencing while transferring packets. In this attacker send packets to target by two types of packets. That is small packets and large packets.

The small packets its size is 64 bytes long. Even the packet size is a small in size the attacker send many numbers of smaller packets. It may result in overloading of server and also network devices. The large packets is size is 1500bytes. The attacker transmits a larger packer to communicating network which may lead to increase the network bandwidth. Finally these result in Denial of service attacks.

3.6. Reflection and Amplification Attacks

The attacker which hides the address by reflection attacks. The attacker does not directly send packets to the network or target server. They send attack packets to the intermediate server or router. This intermediate will send packets to the target network.

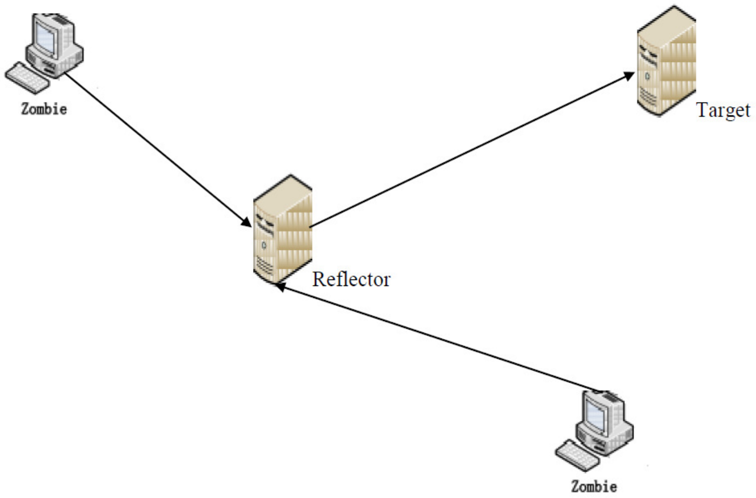

Fig 2 Reflection Attacks

4. Literature review

The literature review includes both DDoS detection and DDoS prevention methodology. By usingdifferent methodology and we can eliminate the DDoS attacks.

4.1. DDoS detection Methodology

4.1.1. Rank Correlation Based Detection

In this rank correlation based technique the incoming packets are tested with rank correlation. It uses an algorithm called spearman's rank correlation [1] . If there are no repeated data values, a perfect Spearman correlation of +1 or −1 occurs when each of the variables is a perfect monotone function of the other which the detect an DDoS by define all the packet count in suspicious flow according to time value.

4.1.2. Multivariate co-relation analysis

They propose an approach called as MAC which follows a triangular area to extract correlative feature. This uses a threshold-based anomaly detector, which contains a traffic profile that is normal traffic profiles. When new packets are arrives in the network it generate the network traffic profile [2]. This traffic profile is compared with the statistical data of normal traffic profile, by which it detect a DDoS attack. The detection of DDoS is achieved by a technique called triangular area and also they follow a multivariate correlation technique. They extract a geocentric correlation feature of network traffic. The detection is mainly based on the statistical analysis of data that is network traffic. They propose an approach called as MAC which follows an triangular area to extract correlative feature. This uses a threshold-based anomaly detector, which contains a traffic profile that is normal traffic profiles. When new packets are arrives in the network it generate the network traffic profile. This traffic profile is compared with the statistical data of normal traffic profile. They fix a threshold value for traffic profile in detector. If the new incoming packets traffic profile rate is greater the threshold value it is said to be an attack. In this they use a lower MAC triangle and higher MAC triangle is to be used for traffic profile generation and attack detection. The evaluation is conducted by using tenfold cross validation and the performance is evaluated using a KDD cup 99 dataset.

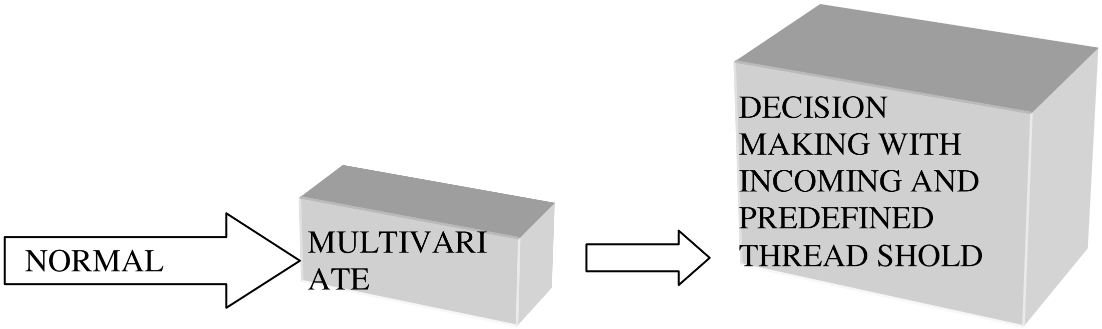

Fig. 3 flow diagram multi correlative anaysis

4.1.3. Flow correlation coefficient

The DDoS attack is detected by using a similarity based algorithm is used. And also they used a flow correlation and coefficient as a metric to find a DDoS attack. Flow correlation which defines a stastiscal relationship between two edge routers [10] .The coefficient defines a quantative measure or specific property. For a given community network, we set up an overlay network on the routers that we have control over. We execute software on every router to count the number of packets for every flow and record this information for a short term at every router. If the packet size is greater than the threshold value it will dropped. Under this framework, the requirement of storage space is very limited and an online decision can be achieved. A real community network may be much more complex with more routers and servers than the example network. However, for a given server, we can always treat the related community network as a tree, which is rooted at the server. We must point out that the topology of the community network has no impact on our detection strategy, whether it is a graph or a tree, because our detection method is based on flows rather than network topology.

3.1.4. Flow Level Detection

In this approach, flow level detection and filtering is used. It detects and filters the low-rate DDoS attacks. It normally occurs in TCP congestion control mechanism [13]. It causes a packet lose and timeout of user. It will not send traffic directly to the network. It will send traffic to the network at regular interval of time. The packets are monitored with threshold value and detect the attack.It normally occurs in TCP congestion control mechanism. It causes a packet lose and timeout of user. It will not send traffic directly to the network. It will send traffic to the network at regular interval of time. And also it causes a time out of client. In normal TCP flow actively avoids the congestion in network flow. In low-level DDoS causes congestion in the network and may delay the service because attack Existing system which detects only LDDoS but fail to detect a flow. In this proposed approach they use a Congestion Participation rate is used. (CPR). Low –level DDoS attacks: Detecting and filtering .This approach is expected to be deployed on router. It samples the each incoming packet with threshold. It identifies a flow between the normal flow and LDDoS flow. When network bandwidth is sufficiently high it drop the packet n network. In this paper congestion participation rate is used .it is used to detect the low-rate DDoS attack. By using a detecting and filtering mechanism they avoid a DDoS attack in the network.

4.1.5. Multi –dimensional sketch Design

In this paper Flooding attack is a DDoS attack that is designed to bring a network or service down by flooding it with large amount of traffic [18]. This occurs due to incomplete connection request. In this paper they propose a online detection scheme for attacks by three dimensional sketch design. It composed of multiple two dimensional attribute hash table and have hash table and K-entries .It is used to measure the distance between two probability distributions. This approach is to quantify similarity of two dataset in either normal and anomalies situation. DDoS attacks is detected in hash table with HD(Hellinger Distance).If number of rows increase in the hash table then threshold then attack detection is registered. In this paper, we propose an online SIP flooding detection and prevention scheme by integrating two techniques, i.e., sketch and Hellinger distance. The three-dimensional sketch design is capable of summarizing each SIP attribute and sketch design provides attack detection.

4.2. DDoS prevention methodology

4.2.1. Identifier – Location Separation 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.ths approach which follows a mapping service [16]. 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.

4.2.2. FuzzingBased 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 [17]. 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.

4.2.3. Reducing -vulnerability by network mechanism

In this approach the vulnerability metric is followed. All the network system follows vulnerability metric. For example closed hah is much more vulnerable to DDoS attacks then open hash function [20]. The FCFS queuing system is vulnerable because attackers can send large number of job packets. We can eliminate vulnerability by FCFS with job size. We can eliminate the vulnerability of the system and prevent a DDoS attacks. In this technique proposing a metric that evaluates the vulnerability of a system. We then use our vulnerability metric to evaluate a data structure which is commonly used in network mechanism the Hash table data structure. We show that Closed Hash is much more vulnerable to DDoS attacks than Open Hash, even though the two systems are considered to be equivalent by traditional performance evaluation. We also apply the metric to queuing mechanisms common to computer and communications systems. Consider the FCFS queuing system one way attack the system is send large job to system. The queuing system is vulnerable if job size is not fixed. Furthermore, we apply it to the practical case of a hash table whose requests are controlled by a queue, showing that even after the attack has ended, the regular users still suffer from performance degradation or even a total denial of service. In this paper the vulnerability factor that measures relative effect of malicious users. Closed hash is much more vulnerable to open hash. And also queuing system are vulnerable if job size are not fixed.

4.2.4. 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 [4]. 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 [13].

4.2.5. 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 [19].

5. CONCLUSION

In this survey various DDoS attack prevention mechanism and detection mechanism are explained .By the above technique we can effectively prevent and also detect the DDoS/DoS attacks. These techniques are evaluated using DDoS Dataset, KKD Cup Dataset and some of techniques are implemented in real time system. By these above prevent the attacks and also we can reduce vulnerability.

REFERENCE

[1] Wei Wei, Feng Chen, Yingjie Xia, and Guang Jin, “A Rank Correlation Based Detection against Distributed Reflection DoS Attacks”, IEEE Communications Letters, Vol. 17, No. 1, January 2013.

[2] zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Senior Member, IEEE, Priyadarsi Nanda, Member, IEEE,andRenPingLiu,Member, IEEE,” A System for Denial-of-Service Attack Detection Based on MultivariateCorrelation Analysis.”, IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 2, February 2014.

[3] Sanjeev Khanna, Santosh S. Venkatesh, Member, IEEE, Omid Fatemieh, Fariba Khan, and Carl A. Gunter, Senior Member, IEEE, Member, ACM,” Adaptive Selective Verification: An Efficient Adaptive Countermeasure to Thwart DoS Attacks”, IEEE/ACM Transactions On Networking, Vol. 20, No. 3, June 2012.

[4] Moti Geva, Amir Herzberg, and Yehoshua Gev l,” Bandwidth Distributed Denial of Service: Attacks and Defenses”, Copublished by the IEEE Computer and Reliability Societies January/February 2014.

[5] Zahid Anwar and Asad Waqar Malik,” Can a DDoS Attack Meltdown My Data Center?A Simulation Study and Defense Strategies”, Ieee Communications Letters, Vol. 18, No. 7, July 2014.

[6] Shui Yu, Senior Member, IEEE, Yonghong Tian, Senior Member, IEEE,Song Guo, Senior Member, IEEE, and Dapeng Oliver Wu, Fellow, IEEE,” Can We Beat DDoS Attacks in Clouds?”, IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 9, September 2014.

[7] Xinlei Ma and Yonghong Chen,” DDoS Detection Method Based on Chaos Analysis of Network Traffic Entropy”, IEEE Communications Letters, Vol. 18, No. 1, January 2014.

[8] Markku Antikainen, Tuomas Aura, and Mikko Särelä,” Denial-of-Service Attacks in Bloom-Filter-BasedForwarding”, IEEE/ACM Transactions On Networking, Vol. 22, No. 5, October 2014.

[9] Zhenhai Duan, Senior Member, IEEE, Peng Chen, Fernando Sanchez, Yingfei Dong, Member, IEEE, Mary Stephenson, and James Michael Barker,” Detecting Spam Zombies byMonitoring Outgoing Messages”, IEEE/ACM Transactions On Networking, Vol. 22, No. 5, October 2014.

[10] Shui Yu, Member, IEEE, Wanlei Zhou, Senior Member, IEEE, Weijia Jia, Senior Member, IEEE, Song Guo, Senior Member, IEEE, Yong Xiang, and Feilong Tang," Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient ", IEEE Transactions On Parallel And Distributed Systems, Vol. 23, No. 6, June 2012.

[11] G.V. Nadiammai, M. Hemalatha," Effective approach toward Intrusion Detection System using data mining techniques", Egyptian Informatics Journal (2014) 15, 37–50

[12] Jérôme François, Issam Aib, Member, IEEE, and Raouf Boutaba, Fellow, IEEE, " FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks" IEEE/ACM Transactions On Networking, Vol. 20, No. 6, December 2012 .

[13] Changwang Zhang, Zhiping Cai, Weifeng Chen , Xiapu Luo, Jianping Yin," Flow level detection and filtering of low-rate DDoS", Computer Networks 56 (2012) 3417–3431

[14] Zhang Fu, Marina Papatriantafilou, and Philippas Tsigas,"Mitigating Distributed Denial of Service Attacks in Multiparty Applications in the Presence of Clock Drifts", IEEE Transactions On Dependable And Secure Computing, Vol. 9, No. 3, May/June 2012

[15] Jingtang Luo, Xiaolong Yang, Senior Member, IEEE, Jin Wang, Member, IEEE,JieXu,Member, IEEE, Jian Sun, Member, IEEE, and Keping Long, Senior Member, IEEE," On a Mathematical Model for Low-Rate Shrew DDoS", IEEE Transactions On Information Forensics And Security, Vol. 9, No. 7, July 2014.

[16] Hongbin Luo, Yi Lin, and Hongke Zhang, Beijing Jiaotong University Moshe Zukerman, City University of Hong Kong," Preventing DDoS Attacks by Identifier/Locator Separation", IEEE Network • November/December 2013.

[17] 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.

[18] Jin Tang, Member, IEEE, Yu Cheng, Senior Member, IEEE, Yong Hao, and Wei Song, Member, IEEE. ," SIP Flooding Attack Detection witha Multi-Dimensional Sketch Design", IEEE Transactions On Dependable And Secure Computing, Vol. 11, No. 6, November/December 2014

[19] 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.

[20] Udi Ben-Porat, Student Member, IEEE, Anat Bremler-Barr, Member, IEEE, and Hanoch Levy, Member, IEEE. ," Vulnerability of Network Mechanisms to Sophisticated DDoS Attacks", IEEE Transactions On Computers, Vol. 62, No. 5, May 2013.

AUTHORS

T.K.SUBRAMANIAM received the B.Tech degree in Information technology from Nandha Engineering College in 2014.He is currently doing his M.E Computer science and Engineering in Nandha engineering college, Erode, India.

B.DEEPA received the M.E degree in Computer Science and Engineering from Nandha Engineering College in 2011.She is currently working as Assistant Professor in Nandha Engineering College, Erode, India.