A Review of Ddos Attack and Their Countermeasure in TCP Based Network

Priyanka[1], Professor Nasib Singh Gill[2]

[1]M.Tech (CSE), MDU Main Campus, Rohtak
[2]HOD, Dept. Of Computer Science and Application, MDU Main Campus, Rohtak

ABSTRACT: Now a day, the chief medium for communication is internet which is valuable for a lot of users across the World but in chorus, it marketable nature make increase vulnerability to increase cyber crimes and also has been a vast increase in the number of DDOS (distributed denial of service attack) attacks on the internet over the past few decade. The victims of DDOS attacks are the network recourses like web server, throughput, bandwidth of the network and network switches etc. This paper will summarize almost techniques of DDoS and its countermeasures by using different In this paper basically summarizing different techniques of DDoS and its countermeasures by different schemes for instance Trace Back method, Independent Component Analysis and TCP Flow Analysis ,Bloom Filter

Keywords: Bloom Filter, DDOS attack, Independent Component Analysis, Trace Back Method, TCP Flow Analysis

I. INTRODUCTION

Some enviable security phases are require by secure communication like confidentiality, authentication, message integrity. Above and beyond, at present a lot of people are conscious About that availability and access control are vital constraint of secure communication because of the tarnished(infamous) Denial of Service (DoS) attacks that render by the illicit users into a network, other piece of network infrastructure to harm them, particularly it is done against the most visited websites and the sites which are related to government and repudiated companies. DDoS (Distributed Denial of Service) attack utilizes adequate marionette (dummy) computers to generate amount of data packets, the attacks become harmonized and come from multiple marionettes at the same time thus the results are shocking .there are two stages of attacks of any typical ddos attack , the first stage is to negotiate susceptible systems that are easily reached in the Internet and install attack tools in these particular systems. This stage act is named as "zombies." In the second stage, through a secure channel to launch a bandwidth attack the enemy sends an attack command to the "zombies"targeted victim(s). The current attacks on trendy web sites like Amazon, Yahoo, e-Bay and Microsoft and their ensuring trouble of services have uncovered the weakness of the Internet to Distributed Denial of Service (DDoS) attacks. it is to be seen from from reports (International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, November 2011) that 85% of the DoS attacks use TCP [19]. The TCP SYN flooding is the most frequently worn attack. There is a stream of spoofed TCP SYN packets directed to a eavesdrop TCP port of the victim. Not only the Web servers but also any systems connected to the Internet given that TCP-based network services.

II. TYPES OF DDOS ATTACK

A typical DDoS attack scenario is presented before going further with classification. Then we define why it is so established, and its genuine reasons why it is so comfortable to launch.

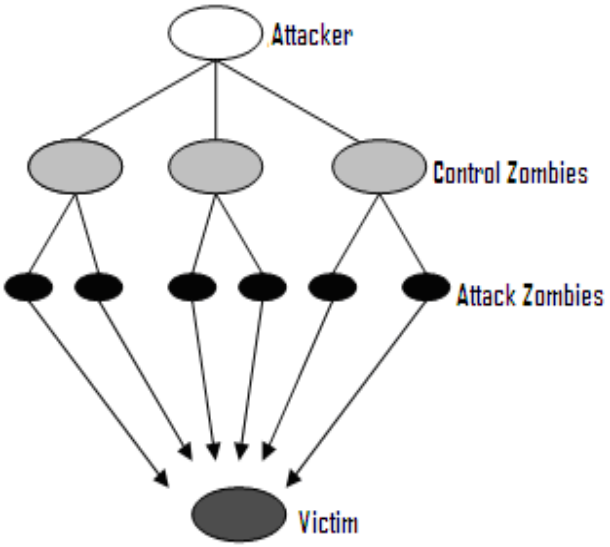

Fig 1: A typical DDoS Attack

Figure (1) shows a hierarchical model of a DDoS attack. It is divided into 2 types.

1) bandwidth depletion. This method is to dam the network, vast make use of the bandwidth then lead the network breakdown.

2) resource depletion. Attacker exhausts the key resources. Then break the server [1]. The attack usually starts from different- different sources to seek at a single target. Multiple target attacks are rare; however, there is the chances for attackers to launch such type of attack Spoofed, altered, or replayed routing information

2.1 SYN flood attack

If any system provide TCP based network services then it impend to this attack. The attackers use semi -open network connections to cause the server wear out its resources . This cause system crash or system inoperative [9].

2.2 TCP Reset Attack

The feature of tcp is also exploiting by tcp reset attack. TCP reset also utilize the characteristics of TCP protocol. By snooping the TCP connections to the victim, TCP RESET packet is send by the attacker to the victim. Then it causes the victim to inadvertently terminate its TCP connection [2].

2.3 ICMP attack

Smurf attack sends phony ICMP ricochet request packets to IP broadcast addresses. These attacks escort huge amounts of ICMP ricochet reply packets being sent from an in-between site to a victim, due to which network congestion occur.

2.4 UDP storm attack

This sort of attack can not only blight (damage) the hosts. Services, but also the speed of the network is also affected and network becomes congested. When a network connection is set up among two tcp services each of which turn out a very vast number of packets, thus cause an attack.

2.5 DNS request attack

The attack sends a number of UDP-based DNS requests to a name server using source IP address the mail server behave as a inconsistent part, responds by sending back to the spoofed IP address as the victim destination. Because of the amplification effect of DNS response, it can cause serious bandwidth attack [10].

2.6 CGI request attack

By normally transferring multiple CGI request to the target server, the attacker guzzle the CPU resource of the victim. At that time the server forcefully dismiss the services..

2.7 Mail bomb attack

A mail bomb is the sending of a vast amount of e-mail to a particular person or system. A huge amount of mail may simply fill up the recipient's disk space on the server.

2.8 ARP storm attack

During a DDoS attack, the ARP request content can become very immense, and then the victim system can be negatively affected .

III. TOOLS TO DO ATTACKS

By meeting information such as Firewall, operating system, IP Address, number of open ports and number of active systems in a network we can make attack with the help of tools. DDOS attack can be carried out with the help of tool Good Bye V3.0 and to perform IP spoofing, TOR software with add on tor-button is also helpful in it . The target system can be proved by the IP address.For **IP spoofing** it is require to download TOR software with add on tor-button. First time tor button (at the bottom right corner) is hinder. After this we will enable that button. At This time we become able to see the tor button and color will change to green. And open Vidalia control panel. Click on new identity button.

IV. COUNTERMEASURES AGAINST DDOS ATTACK

Most recent DDoS attack detection and prevention schemes are arranged either at the victim server, or at the attack source side, or among these two. In the respective, we describe schemes representative of each of these three arrangements and describe respective crisis. Victim server side detection of DDoS attacks has collected the immensity of past research attention, certainly because the main goal of researchers has been to save the victim server. Wang et al. [4], detected SYN flooding attacks at folio routers that join end hosts to the Internet. They servey that the SYN-FIN packets join all together in the normal network traffic and proposed a non-parameter CUSUM method to accumulate these pairs. Cheng [5] utilized the TTL (Time-To-Live) value in the IP header to estimate the Hop-Count of each packet. The spoofed packets could be separate from normal ones by the Hop- Count deviation. Lemon [6] incorporated SYN cache and cookies to avert DDoS attacks, using cache or cookies to evaluate the security status of a connection before establishing the real connection with a protected server.

Hussein et al. [6] proposed a setup for classifying DoS attacks based on the header content and the momentry ramp-up behaviour. Keromytis et al. employed the secure overlay service (SOS) [7, 8] to proactively prevent DDoS. SOS architecture is composed of SOAP, superimpose nodes, beacon, secret servlet and filtered region, which makes it difficult for an attacker to target nodes along the path to a specific SOS-saved destination. Based on SOS, researchers from Columbia University continued their proactive defence research. MOVE [9] and WebSOS [10] are modified forms of the SOS architecture but with different prominence. Puzzle based methods [11, 12] compel heavily overhead to zombies, which can mitigate attacking rate and make zombies depicted to host owners. Each of these must minimize resource usage while promptly responding and recording the states of numerous connections. With the same time ,

the scheme itself must be impervious to DDoS attacks. Source side mechanism for detecting and preventing of DDoS attacks can be difficult to setup. Source-end setup methods have some advantages but are difficult to arrange. For reasons related to performance, however, ISPs are disinclined to deploy source-end defences in their domains. Mirkovic and Prier [13] introduced a DDoS defence system at the source-end in which attacks were detected by constantly monitoring two way traffic flows and parallely tracking them with normal flow models. The RFC2827 [14], for example, is designed to filter out spoofed packets with spoofed IP addresses at each ingress router and can drop a suspicious packet that does not belong to its routing domain. However, the fact that it may degrade routing performance makes ISPs reluctant to participate in this defense system. After an attack is detected, it is possible to find the attacking source using trace back [15] and pushback techniques. Traceback attempts to identify the real location of the attacker. Source IPs used during a DDoS attack are often frequently and cannot be used to detect the real location of the attack source. Most trail back schemes respond to this by either marking some packets along their routing paths or by sending special packets [18]. By tracking these special marks, it is possible to reconstruct the real routing path reconstructed and locate the true source IP. After the real path of the skit packets has been identified, the pushback technique can be used for advanced filtering and work at the last few routers before the malicious traffic reaches the target victim.

A. The TCP-Based DDoS Attack

Most DDoS attacks make the use of most of TCP control packets by spoofing the three-way handshake between the source and the destination server [24]. In this section we explore the behavior of TCP control packets first in a normal three-way handshake and secondly in spoofed three-way handshake. The below Figure shows a normal three-way handshake. Initially client C sends a synchronization Syn(k) request to the server S1, and the reply comes with a packet containing both the acknowledgement Ack(k + 1) and the synchronization request Syn(j) and then stay back with a half-open connection in its memory space for the acknowledgement from the client C. till when the acknowledgement receiving both Ack (k + 1) and Syn (j) client C will finish the set up of connection by sending Ack (j + 1). When server S1 gets new acknowledgment Ack (j + 1), it dismiss the last stored half-open connections in its memory space. The unconfined (released) memory space on server S1 makes it enable to handle more connection requests from clients and a network can run in well form. k and j are respectively sequence numbers produced randomly by the server and the client during the three-way handshake. In the remainder of this paper, SY N means a request sent to a server S inside the TCP control packet during the first round of the three-way handshake protocol; ACK/SY N will indicate a packet containing both Ack (k + 1) and Syn (j) that is delivered back from the server S in the second round; and ACK will point a control package representing Ack (j + 1) in the third round. During the normal three-way handshake procedure, SYN, ACK/SYN and ACK all appear at both the edge router Rc which is near the client and at the edge router Rs which is near the server, figure shows a spoofed three-way handshake and the implementation of a DoS attack. Within the valid authentication process the packets at the very first round is malicious one with their spoof IP address. The edge router Ra in the attacker province (area) frontward the SYN packet with the spoofed address PI, the IP address of the innocent host I, to the server S2. The server S2 replies with an ACK/SYN packet and a half-open connection are in anticipation. This ACK/SYN will be sent to the innocent host I because the server S2 regards the SY N packet from I according to the spoofed source IP PI. The edge router RI on the true host side will accept the ACK/SY N packet but as no previous SY N request had been forwarded by the client detector at RI, the ACK/SY N packet is dropped. The remaining semi-open connection on the server S2 is maintained for a long time. More accreted half-open connections will quickly consume all the memory space reserved for handling TCP requests and the server S2 will deny any new requests. It is difficult to trace back the attackers true address because the innocent host I , whose IP is used as the skit source IP, is usually not in the same domain s the attacker, sender A.

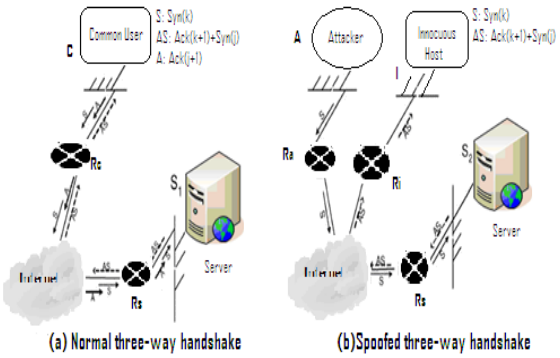

Fig 2: The general architecture of TCP-Based DDoS Attack

B. Bloom Filter

The Bloom filter was explained by Burton Bloom [20] and main purpose of it is to

reduce the disk access times to different files and other applications, e.g., spell checkers. Now it is improved to fight against DDoS attacks. The Bloom filter is a compact pack of a vector v of m bits, initially all set to 0.there are k independent hash functions, h1, h2, and hk, each with a range {0 . . . m − 1}. The vector v can show

the presence of an element in A. Given an element a ı A, the bits at positions h1 (a), h2 (a). . . hk (a) in v are set to 1 . Note that a particular bit might be set to 1 multiple times which may cause potential false results. Given a query of the existence of b in A, we check the bits at positions h1 (b), h2 (b). . . hk (b). If any one of them is 0, then certainly b is not in the set A. Otherwise we interference that b is in it. Otherwise we presume that b is a part of that set. There is, however, a certain probability that the Bloom filter will give a false result, a "false positive". The parameters k and m should be chosen such that the probability of a false positive is small.

V. CONCLUSIONS

Two important factors which are the must requirement in design of defence against DDoS attack are efficiency and scaliblity. This paper demostrate study of various DDOS attack techniques and their prevention techniques. All these techniques based on filtration mechanism and pattern matching based on the different normal or abnormal packet pattern. One great advantage of the development of DDoS attack and defence classifications is that effective communication and cooperation between researchers can be achieved so that additional weaknesses of the DDoS field can be acknowledged . DDoS attacks are not only a grim threat for wired networks but also for wireless infrastructures.
On the basis of all these review, a argue against developed filter Mechanism using the Independent component analysis has been proposed for the future work which will not only detect the DDOS traffic but also help in filtering that unwanted traffic.

VI. REFERENCES

[1]. Liang Hu, Xiaoming Bi, "Research of DDoS Attack Mechanism and Its Defense Frame," Computer Research and Development (ICCRD), 3rd International Conference, pp. 440–442, March 2011.

[2]. Robert Vamosi, "Study: DDoS attacks threaten ISP infrastructure," Online at http://news.cnet.com/8301-1009_3-10093699-83.html, CNET News, Nov. 2008.

[3]. Elinor Mills, "Radio Free Europe DDOS attack latest by hactivists," Online at http://news.cnet.com/8301-10784_3-9933746-7.html, CNET News, May. 2008.

[4]. Christos Douligeris and Aikaterini Mitrokotsa, "DDoS Attacks And Defence mechanisms: A Classification," in Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology, (ISSPIT'03), pp. 190-193, Dec 2003.

[5]. IEEE Communications Magazine, pp. 42-51, Oct. 2002 Rocky K. C. Chang," Defending against Flooding-based Distributed Denial-of-service Attacks: A Tutorial,".

[6]. Internet World Stats, Internet User Statistics – The Big Picture: World Internet Users and Population Stats, http://www.internetworldstats.com/stats.htm International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, November 2011 187

[7]. L.D. Stein, J.N. Stewart, The World Wide Web Security FAQ, version 3.1.2, February 4, 2002, Available from http://www.w3.org/Security/Faq.

[8]. <http://cisco.com> viewed on 15 may 2015.

[9]. S. M. Khattab, C. Sangpachatanaruk, R. Melhem, D. Mosse, and T. Znati, "Proactive Server Roaming for Mitigating Denial-of-Service Attacks," in Proceedings of the 1st International Conference on International Technology: Research and Education (ITRE'03), pp. 286-290, Aug. 2003.

[10]. A. Yaar, A. Perrig, and D. Song, "PI: A path identification mechanism to defend against DdoS attacks," in proceedings of the IEEE symposium on Security and Privacy, pp. 93-109, May 2003.

[11]. P. Feruson and D. Seine, "Network Ingress Filtering: Defeating Denial Of Service Attacks Which Employ IP Source Address Spoofing," RFC2827, May 2000.

[12]. A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, B. Schwartz, S. T. Kent, and W. T. Strayer, "Single-Packet IP Traceback," IEEE/ACM Transactions on Networking, Vol. 10, No. 6, pp. 721-734, Dec. 2002.

[13]. J.Ioannidis and S. M. Bellovin, "Implementing Pushback: Router-Based Defense Against DdoS Attacks," in Proceedings of the Network and Distributed System Security Symposium (NDSS'02),pp. 6-8, Feb. 2002.

[14]. Yao Chen1, Shantanu Das, Pulak Dhar, Abdul-motaleb El Saddik, and Amiya Nayak, "Detecting and Preventing IP-spoofed Distributed DoS Attacks," International Journal of Network Security, Vol.7, No.1, pp.70–81, Jul. 2008.

[15]. B. Bloom, "Space/Time Trade-Offs in Hash Coding with Allowable Errors," Comm. ACM, vol. 13, no. 7, pp. 422-426, 1970.

[16]. Wang H, Zhang D, Shin KG (2002) Detecting SYN flooding attacks. In: Proceedings of Annual Joint Conference of the IEEE Computer and Communications Societies(INFOCOM), vol. 3, pp 1530–1539.

[17]. Jin C,Wang HN, Shin KG (2003) Hop-count filtering: An effective defense against spoofed DdoS traffic. In: Proceedings of the 10th ACM Conference on Computer and Communication Security (CCS), ACM Press, pp 30–41.

[18]. J.Lemon, "Resisting SYN Flooding Dos Attacks with A SYN Cache", Proceeding of USENIX BSDCon'2002,February, 2002.

[19]. Keromytis A, MisraV, RubensteinD(2002) SOS: Secure overlay services. In:ACMSIGCOMMComputer Communication Review, Proceedings of the 2002 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, Pittsburgh, PA, vol. 32, pp 61–72.

[20]. Keromytis A, Misra V, Rubenstein, D (2004) SOS: An architecture for mitigating DDoS attacks. IEEE Journal on Selected Areas in Communications 22:176–188.

[21]. A. C. Snoeren. Hash-based IP traceback. In Proceedings of the ACM SIGCOMM Conference, pages 3–14. ACM Press, August 2001.

[22]. Yuji Waizumi , Tohru Sato and Yoshiaki Nemoto: A new Traffic Pattern Matchinng for DdoS trace back Using Independent Component Analysis in Procedding of World Academy of science,Engineering and Technology 2009.

[23]. Anand Bisen, Shrinivas Karwa, B.B.Meshram, "Countermeasure tool-Carapace for Network Security". In International journal of Network Security & its Applications (IJNSA), VOL.3, NO.3, pp.16-28, May 2011.

[24]. Bin Xiao, Wei Chen, Yanxiang He, "A Novel approach to detecting DDoS attacks at an early Stage". In Springer Science + Business Media LLC 2006.

[25]. Dhinaharan Nagamalai, Cynthia Dhinakaran, Jae Kwang Lee. "Multi Layer Approach to Defend DDoS Attacks Caused by Spam". In aaXiv.org

