A Meliorated Defense Mechanism for Flooding Based Attacks

Gayatri Bhatti, Upma Goyal, Prabhdeep Singh

Abstract— ***The Distributed Denial of service (DDoS) attacks, over a past few years are found to be a disaster to the Internet. A flooding-based attack attacks the victim machine by sending an excessive amount of illegitimate traffic to it. The defence mechanisms existing before are unable to prevent the systems from these attacks, since it is very difficult to trace the spoofed packets and distinguished between the legitimate and illegitimate attack traffic. Flooding-based DDoS attacks use agents to send the traffic and sometimes prefer Reflectors in order to forward the traffic to the target, thereby making it impossible to be detected. So, this paper will propose a defence mechanism pronounced as Hop-based DDoS defence procedure. This mechanism will comprise of three components: detection of illegitimate packets, IP traceback of the illegitimate packets and the traffic control. This framework shows high performance in defending against the flooding-based attacks.***

***Index Terms*—DDoS, Defence, Flooding, Hop, Traffic.**

I. INTRODUCTION

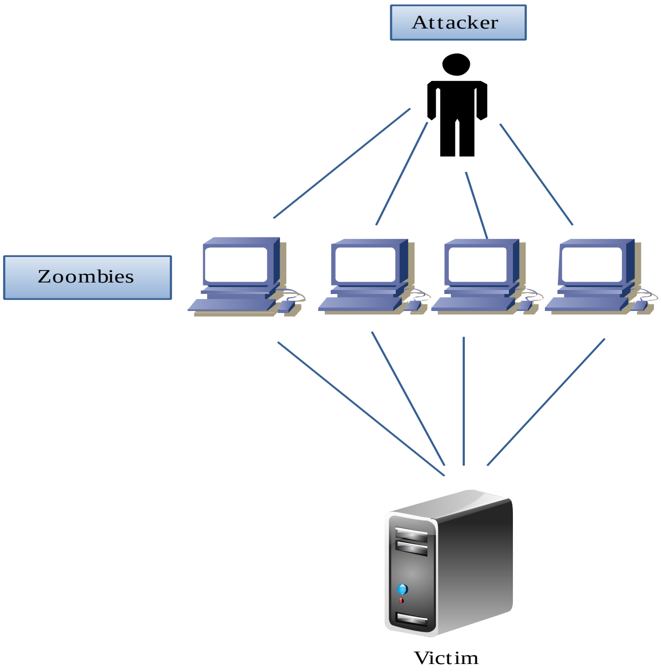
The Internet Service Providers come across the problem of excessive amount of malicious traffic due to which the ISPs cannot prevent their Quality of Service from falling down. Due to the ability to create a huge amount of malicious traffic, DDoS is one of the disastrous threats today. A numerous defending techniques have been proposed but none of them provides reliable protection for the victim. The flooding-based attacks mainly occur in the IP based networks. Despite of deploying a defending procedure on a particular part in a network, the proposed Hop-based defence mechanism will be deployed at each edge router in a network, since edge router have an ample amount of resources. The first component in this defence mechanism, the detection component, implements threeDDoS detection techniques. These are calculating the distance, average distance computation and the traffic separation. The next component of this mechanism, IP trace component focuses on monitoring the malicious traffic in order to find out the source addresses of the edge routers. The third component i.e. the traffic managing component helps to manage the rate limit for the traffic flows after getting the alert messages from other defence systems. This defence mechanism will be deployed at both source and the victim end.

II. DISTRIBUTED DENIAL-OF-SERVICE ATTACKS

DDoS, the most challenging attack, gains success to stop the victim from helping the legitimate users[1]. There are two types of DDoS attacks in which the first type deals with the thought of attacking the system by exploiting its protocol[1,12] vulnerabilities and the second type concentrates on the attack traffic which comes to be known as Flooding-based DDoS attack[2]. In this paper, the main concentration will be on how the Flooding-based DDoS attack attempts to flood the victim's network and what efficient defence mechanism is proposed against these attacks.

III. FLOODING-BASED DDOS ATTACKS

Flooding-based DDoS attack sends a large volume of unwanted traffic to the victim, thereby resulting in the consumption of a huge amount of network resources[3]. Basically Flooding-based DDoS attacks are of two types: the Direct and the Reflector attack. In the Direct attack, the attacker sends the TCP, ICMP, UDP and many other packets directly to the victim. Now, in all the DDoS attacks, a process known as IP spoofing is involved which helps to hide the real address of the attacker. Due to IP spoofing the response packets from the victim reach to the spoofed receivers. In the Reflector attack, the response packets from the Reflector, attack the victim. A Reflector is any host returning a packet if it receives a request packet. Now, victim does not need to send the response packets back to the Reflectors.



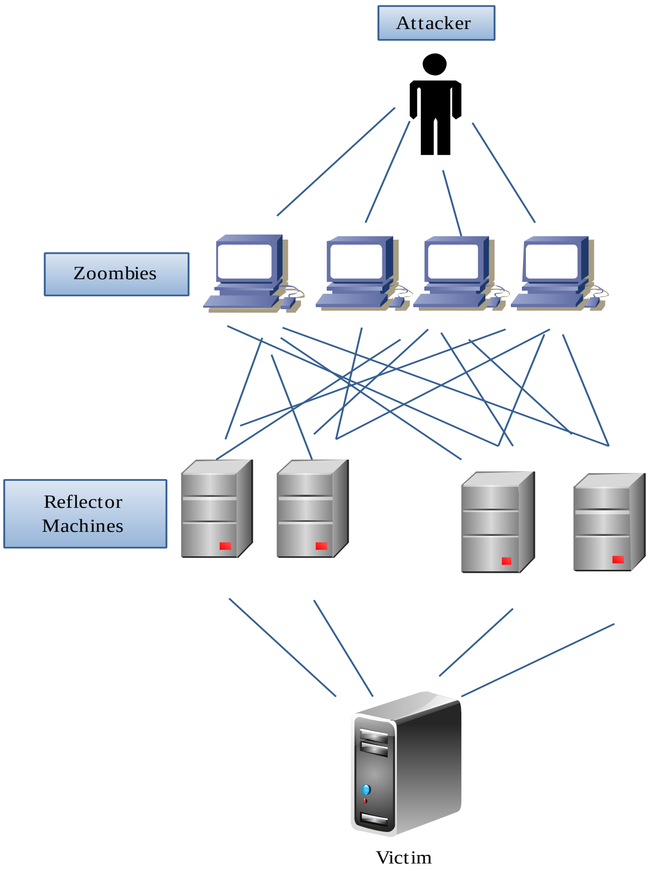


Fig. 1 Architecture of Direct and Reflector Flooding Attacks

Direct attacks involve three mechanisms: TCP SYN flooding, ICMP echo flooding and UDP data flooding. On the other hand, Reflector attacks depend upon the protocol features in the victim. The protocol sending a response message to the victim will be used for the Reflector attack. The Packet Amplification Technique can be further utilised by the attacker in order to create a stronger Reflector attack.To tolerate the Flooding-based attacks, one must increase the bandwidth and resources of the network[4][5]. Now, The different types of Flooding-based attacks are:

A. ICMP Flooding-based Attack

This attack, also known as Smurf attack uses ICMP REQUEST and ECHO REPLY messages to carry control information. The source address of ICMP ECHO REQUEST message is set as the victim address. As a result of which the ICMP ECHO REPLY message will be forwarded to the victim instead of the real request message sender. Here, if we use an amplifier to broadcast the ECHO REQUEST messages to all the IP addresses in the subnet, the effect of the attack will be amplifying. Larger the number of ICMP ECHO REPLY messages, more will be the consumption of bandwidth and resources in the victim.

B. TCP SYN Flooding-based Attack

In this type of attack, the client first sends a TCP SYN packet, deciding the memory block to be used for connection control, to the server with the client's request of connection establishment. The TCP SYN ACK packet will be forwarded back to the client by the server with a sequence number and other server information. Finally, client will send a TCP ACK packet back to the server, confirming that it had received server's ACK packet. This is called the Three-way handshake procedure. The actual TCP data communication can be started after the connection establishment. . If large number of TCP SYN packets is received in a short period of time, the server will run out of the memory. The IP spoofing technique can also be triggered in this type of attack. So, in order to increase the speed of memory recycling, one proposed solution can be lowering the TCP time out.

C. UDP Flooding-based Attack

UDP Flooding-based attack also known as the Trinoo attack sends numerous UDP packets at random ports in order to attack the victim. This results in the consumption of a large amount of bandwidth at the victim end, thereby making the connection unavailable for the legitimate traffic. Basically, UDP flooding-based attack is a Direct attack but if the attacker sets the source address as another victim's address, this attack can be a Reflector attack. UDP based communication has no built in mechanism to maintain the flows of the networks, thereby making it even harder to detect the spoofed traffic at the victim end. In order to deal with this problem, the victim must set up a defence mechanism in the upstream network.

D. DNS Amplification Attack

It is a new kind of Reflector attack which uses recursive name servers to create an Amplification effect. In this type of attack, the sender forwards a very small sized packet and receives a large sized response packet back by the DNS server. DNS Amplification attack is much harder to defend against than to defend against the normal DDoS attacks. This is because there is the presence of complex interactive mechanisms between the clients and DNS server, and among the DNS servers themselves[6].

IV. SURVEY OF DDOS ATTACKS

The first most DoS attack was carried out by David Dennis, a thirteen year old student at University High School in 1974. In late 1990s, Internet Relay Chat (IRC) was very popular which caused IRC chat floods[7,11] there by forcing all the users within a channel to logout and they gain the access. In August 1999, a tool named Trinoo[8] was used to disable the University's computer network for over two days which resulted in the first large scale DDoS attacks[9,10]. During February 2000, the most well-known websites[10, 11] including Yahoo, CNN, and Amazon came down due to these attacks. In 2002, another disastrous DDoS threat came into notice which targeted all the thirteen Internet's root domain name service (DNS) servers. In 2003, the DDoS attacks took hold on the web sites like Clickbank and Spamcop. In 2004, Qatar-based Al-Jazeera News was took down by DDoS attacks. In 2007-2008, DDoS attacks were used as a part of cyber wars against Estonia and Georgia by Russia. In 2009, many heavy DDoS attacks targeted South Korean, Iranian Government and American web sites. In the same year, Facebook, Twitter, Google were also targeted by such attacks. In year 2010, some Anonymous, using DDoS attacks took down the Operations Payback.in year 2011-2012, Hacktivists targeted Operation Tunishia, Operation Sony, Operation Russia, Operation India, Operation Japan etc. using such attacks[13,14,15].

Over these years, it has also been surveyed that the largest targets of the DDoS attacks are customers. Network infrastructure and service infrastructure are also influenced by these attacks. So here, a fig. 1 is drawn in order to illustrate the target of DDoS attacks.

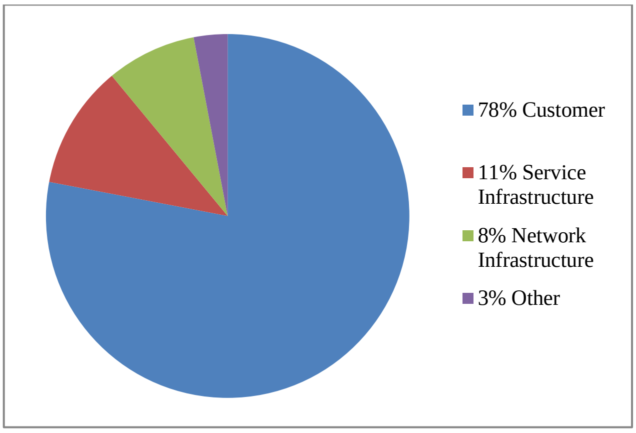


Fig. 2 Victim of DDoS Attacks

Following table represents different kinds of flooding-based attacks, along with their effects and defence mechanisms.

TABLE I. FLOODING-BASED DDOS ATTACKS, THEIR EFFECTS AND DEFENSE MECHANISMS

S.No.	Name of the attack	Function of the attack	Solution against the attack
1.	UDP Flood	Where both legitimate and illegitimate packet flows will not reduce their sending rates	Provide the sufficient ISP service so that one host cannot DOS you.
2.	ICMP (Ping) Flood	Bandwidth attack that uses ICMP packets	ScreenOS, providing a Screening option which sets a threshold that once exceeded invokes the ICMP flood attacks
3.	SYN Flood Attack	Exploit the vulnerabilities of TCP/IP protocol and perform three way handshake	Filtering, increasing backlog, reducing SYN-RECEIVED Timer, SYN cookies eliminating the resources allocated to the target host.
4.	Ping of death	Sends multiple malformed or malicious pings to a computer	Add checks for each incoming IP fragment telling whether the packet is invalid or valid.
5.	Amplification attack	Attacker makes a request that generates a larger response	Using high performance OS, load balancer, limiting the connection, limiting the connection rate.
6.	DNS Flood	Attacks both infrastructure and DNS application	Radware carrier solution, allowing continuous DNS service even under the attack and mitigating the DNS attack.
7.	HTTP GET Flood	Attackers send a huge flood of requests to the server and consume its resources	NS FOCUS provides web application firewall, Intrusion prevention system, carrier-grade anti-DDOS system.
8.	HTTP POST Flood	Large volume of POST requests are targeted to the server so that the server stops responding	Authentication on web application, ensuring only identified list of authenticated and authorized users.
9.	IGMP Flood	Consumes large amount of network bandwidth	On receiving each IGMP packet check the MAC address. If not a multicast Ethernet address drops the packet.
10.	Layer 3 and layer 4 DDOS attacks	Attackers send high flood of data to slow down the web server performance, degrades the access for legitimate users, consume bandwidth	Begin the application transactions, limit the rate of transaction.
11.	TCP Flag Abuse Flood	Emerged from out of state requests or TCP messages with odd combinations or modifications to the control bits in the TCP headers	Install patches to guard against these attacks which we limit the ability of an intruder to take advantage of these attacks.
12.	TCP Fragment Flood	Overloads the target's processing of TCP messages in order to reconstruct the datagram	Packet sniffer which detects all the illegitimate packets.
13.	Volume Based Attack	Includes UDP floods, ICMP floods and other spoofed packet floods	Incapsula absorbs the attack with the global network
14.	Reflector Attack	Where third parties bounce the attack traffic from attacker to the target	DERM (Deterministic Edge Router Marking), helps in identifying, tracking and filtering the attack.
15.	Smurf Attack	Attackers use ICMP echo request packet to generate DOS attacks	Ingress filtering, configuring all the hosts and routers not to respond to ICMP requests and not to forward the packets directly to broadcast addresses.

V. PROPOSED SOLUTION: HOP-BASED DDOS DEFENCE MECHANISM

The Hop-based DDoS defence system is deployed in each edge router of the network, due to which the defence system at the victim end edge router can easily detect the attack[16]. However, the heavy attacks at the victim end edge router are impossible for the defence system to react against. Basically, in our framework, the detection of and response to the flood attacks happen at the edge routers. This is because the edge router has an ample amount of resources resulting in less traffic at the edge network. Hop-based attack traffic rate limit control will be triggered in the source end edge network after getting an alert message from the defence system of the victim end edge network to drop the spoofed packets effectively. Now, the alert messages used are of three types: request messages, update messages and cancel messages in order to defeat the flood attacks in different phases.

The three Components of Hop-based DDoS Defence Mechanism is shown in fig. 3 and explained as follows:

A. The Detection Component

This component works in the following steps:

1. Computes the distance using a Single-Bit Field

This portion of the Detection Component calculates the number of hops; a packet has travelled from an edge router to a victim. Here, the Fast InternetTrace back (FIT) technique[17] is used in order to find out the entire source end edge network. This technique uses only a single bit in the IP Identification field to mark the distance. During transit, every router decrements the TTL value of an IP packet by one. So, the distance calculated will be number of hops made by the packet to reach the victim.

2. Calculates the Average distance

This portion detects the changes of mean distance values. A technique called Exponential Smoothing Estimation Technique (ESET) is used which will calculate two things: the mean value of the distance and the Mean Absolute deviation (MAD) value at the next time interval. Here, at the next time interval, we set a scope for the legal value. Any value, out of the legal scope will be thought of as anomalous.

3. Separates the attack traffic

This portion of the Detection Component detects the changes found in the separated traffic rates. This is done on the basis of the technique called Minimum Mean Square Error (MMSE). Here, separate the traffic based on different traffic arrival rates on each distance values. In this portion, the arrival rate and the deviation will be calculated by using MMSE and MAD model.

B. IP Trace Component

This component helps to find the source end edge routers which forward the attack traffic. By using the FIT technique, find the IP addresses of all the source end edge routers on the basis of information in the attack packets. This technique calculates a Hash of the IP addresses of the edge routers and splits the Hash into n fragments, keeping n as a global constant. There is no need to add any defence mechanism into the core routers; it will itself detect the anomalous traffic by scanning the Hash table in order to find out the real IP address of the source and edge router.

C. Traffic Manage Component

The purpose of this component is to limit the rate of the attack traffic in order to protect the victim end edge network from the attack. Also, it decreases the percentage of the whole attack traffic. So, set up a rate limit on those edge routers which are close to the attacker. To rate limit the attack traffic, this paper will propose a distance based Max-Min rate limit technique. This technique will allocate bandwidth among all the incoming traffic packets from those routers forwarding the attack traffic. The rate limits will be on the basis of packet drop histories of individual routers which will affect the final value of rate limit of each router. The traffic value exceeding this limit will detect an attack[18].

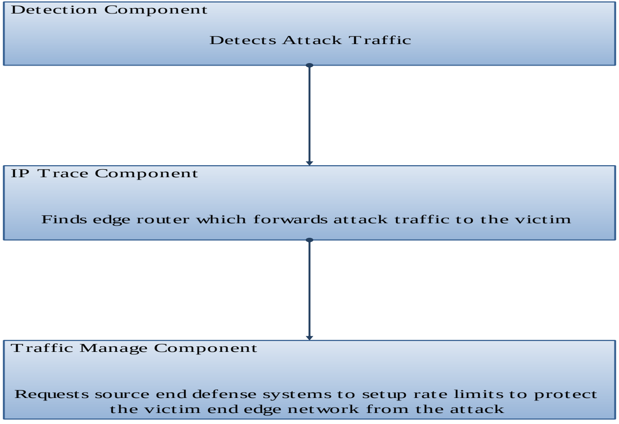

Detection Component
Detects Attack Traffic
IP Trace Component
Finds edge router which forwards attack traffic to the victim
Traffic Manage Component
Requests source end defense systems to setup rate limits to protect the victim end edge network from the attack

Fig. 3 Flowchart for Hop-based DDoS Defence Mechanism

VI. CONCLUSION

After examining the complete scenario of the Flooding attacks i.e. how they perform, what are their consequences etc. the conclusion is that the disastrous effects of Flooding attacks has captured a very stronger pace and to detect the DDoS attacks quickly and efficiently, solution is proposed called Hop-based DDoS detection mechanism, working in three phases-Detecting, Tracing and Managing the traffic, so that the system incurs a little communication overhead and yields legitimate data.

ACKNOWLEDGMENT

Foremost, we Gayatri Bhatti and Upma Goyal would like to express our sincere gratitude to our Head of the Department, Mr Rajdeep Singh and our guide Mr Prabhdeep Singh for their continuous support, their patience, motivation, immense knowledge and their complete guidance for this research paper.

REFERENCES

[1] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: Classification and state-of-the-art," Computer Networks: the Int. J. Computer and Telecommunications Networking, Vol. 44, No. 5, April 2004, pp. 643–666.

[2] J. Mirkovic, S. Dietrich, D. Dittrich, and P. Reiher, "Internet Denial of Service: Attack and Defense Mechanisms," Prentice Hall PTR, December 2004.

[3] R. K. C. Chang, "Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial," IEEE Communications Magazine, pp. 42-51, October 2002.

[4] J. Jung, B. Krishnamurthy, and M. Rabinovich, "Flash crowds and denial of service attacks: Characterization and implications for cdns and web sites," in Proceedings of the International World Wide Web Conference, May 2002, pp. 252–262.

[5] G. Carl, G. Kesidis, R. Brooks, and S. Rai, "Denial-of-service attack detection techniques," IEEE Internet Computing, Vol. 10, No. 1, January 2006, pp. 82-89.

[6] J. Jiang and S. Papavassiliou, "Detecting network attacks in the internet via statistical network traffic normality prediction," Journal of Network and System Management, Vol. 12, No. 1, 2004, pp. 51-72.

[7] S. Tanachaiwiwat and K. Hwang, "Differential packet filtering against DDoS flood attacks," ACM Conference on Computer and Communications Security (CCS), Washington, DC, October 2003.

[8] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: Classification and state-of-the-art," Computer Networks: the Int. J. Computer and Telecommunications Networking, Vol. 44, No. 5, pp. 643–666, April 2004.

[9] M. Robinson, J. Mirkovic, M. Schnaider, S Michel, and P. Reiher, "Challenges and principles of DDoS defense," SIGCOMM 2003.

[10] B. Bencsath and I. Vajda, "Protection against DDoS attacks based on traffic level measurements," Western Simulation MultiConference, San Diego, California, USA, January 2004.

[11] N. Noureldien, "Protecting web servers from DoS/DDoS flooding attacks: a technical overview," International Conference on Web-Management for International Organisations. Geneva, October 2002.

[12] G.Bhatti, R.Singh and P.Singh, "A look back at Issues in the layers of TCP/IP Model," International Journal of Enhanced Research in Management & Computer Applications, Vol. 1, Issue 2, November 2012.

[13] Y. He, T. Liu, and Q. Cao, "A survey of low-rate denial-of-service attacks," Journal of Frontiers of Computer Science & Technology, 2008.

[14] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems," ACM Computing Surveys 39.

[15] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," ACM Computing Survey 42, 2010.

[16] R. Mahajan, S. Floyd, and D. Wetherall, "Controlling high- bandwidth flows at the congested router," in Proceedings of ACM 9th International Conference on Network Protocols (ICNP), 2001, pp. 192-201.

[17] A. Yaar, A. Perrig, and D. Song, "FIT: fast internet traceback," in Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), 2005, pp. 1395-1406.

[18] S. Lee, H. Kim, J. Na, and J. Jang, “Abnormal traffic detection and its implementation," Advanced Communication Technology, Vol. 1, February 2005, pp. 246-250