A Novel Framework for Mitigating the DDoS attacks

Upma Goyal[1], Gayatri Bhatti[2], Prabhdeep Singh[3]
[123]Computer Science Department, Punjab Technical University Kapurthala, Jalandhar, India.
upmagoyal.pit789@gmail.com, Gayatribhatti.pit@gmail.com, ssingh.prabhdeep@gmail.com

Abstract— Distributed Denial of Service (DDoS) attacks are a destructive, relatively new type of attack on the availability of Internet services and resources, andamong the hardest security problems. Over the past few years, DDOS attacks have increased up to a large extent. As a result of which we need to fight against the severe effects of these attacks. In this paper, we will discuss different types of DDOS attacks, the way they affect the networks and the appropriate defence mechanisms for them. Also, a solution is proposed to mitigate these attacks which work in four steps including detection of DDOS attacks, diverting the attack traffic for treatment, monitoring and filtering the attack traffic and finally forwarding the good traffic to the final destination.

Index Terms— Attacks,Defence, DDoS, DoS, Filtering, Mitigation,Traffic.

1 Introduction

As the vast Internet is growing on a fast pace, its vulnerabilities and weaknesses are achieving a faster pace. This gave rise to a flame of viruses, worms, website defacement, and many attacks and so on. Anyone can take advantages of such vulnerabilities which results in degradation of the network. These severe attacks have led to the rise of various defense mechanisms. Since security refers to secrecy, integrity, authentication and non-repudiation, any proposed defense mechanism should be able to provide all these four features. But the attacks like DoS and DDoS have overpowered these security mechanisms, there by loading so much of attack traffic on the system. So following are discussed some of the types of DDoS attacks along with the effects they cause on the system and the defense mechanism proposed for them.
sentence use the author names instead of "Reference [3]," e.g., "Smith and Smith [3] show ... ." Please note that references will be formatted by IJSER production staff in the same order provided by the author.

2 Different Types Of Ddos Attacks And The Consequences

2.1 Bandwidth Attack

These attacks[1] have become a major security issue now days which led to the downfall of very high profile websites such as Microsoft, Yahoo resulting in a huge financial loss[2]. Bandwidth attack shuts off the services by throwing a huge amount of useless traffic there by resulting in the consumption of large number of host's resources, network bandwidth, memory etc.

2.2 Typical DDoS Attack

It is one of the known types of DDoS attacks [1]. In this attack, the attacker installs all the relevant tools which leads to the advancement of the attack into all the systems and turns those computers or systems into "zombies".

2.3 Reflector Attack

Reflector attack is one of the most serious type of DDoS attacks. Here, what happens is, the attacker goes for the help of a third party. This third party can be a person, system or a victim. The attacker will send the attack traffic to the third party and the third party will further bounce the attack traffic towards the target[1,2].

2.4 Protocol Attack

Since various networks involve the functionalities of various protocols such as TCP/IP [2,12] protocol, the vulnerabilities or weaknesses can reside in these protocols also. The attacker taking advantages of these vulnerabilities sends the attack traffic towards the target there by causing memory and resources loss[4].

2.5 SYN FLOOD Attack

Similar to the above mentioned protocol attack, this attack also exploits the vulnerabilities of TCP/IP[2,12] protocol performs a three way handshake as well[3]. In this handshake, large number of acknowledgements accumulates to generate a high volume of harmful attack traffic. This traffic is then forwarded to the target system[5,6].

2.6 UDP FLOOD Attack

This type of attack occurs when the victim is unable to distinguish between the legitimate and illegitimate packet flows moving at a high sending rate. Since UDP has no flow control mechanisms, due to which the traffic results in congestion at the receiver end[5].

2.7 ICMP FLOOD Attack

It is a type of bandwidth attack which uses ICMP packets. Here, the packet is directed to an individual ma-

chine which is then broadcast to the entire network resulting in the degraded network status[5,6].

3 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.

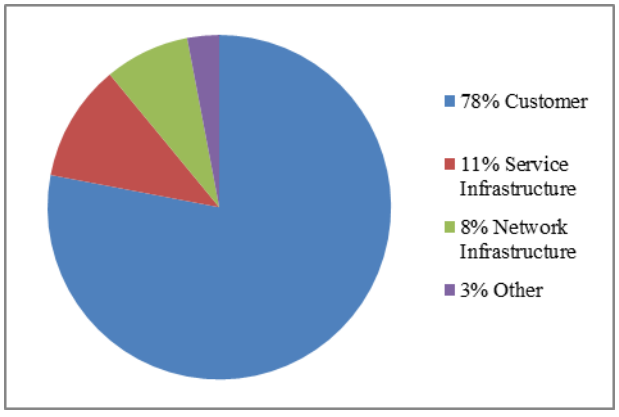

Fig 1.Victim of DDoS Attacks

Following TABLE I list some more kinds of DDoS attacks along with the penalties they cause and the defense procedures for them.

TABLE I
DDoS ATTACKS, THEIR EFFECTS AND DEFENSE MECHANISMS

S.No.	Name of the attack	Function of the attack	Solution against the attack
1.	Bandwidth Attack	Consumes target's resources	Multops, tree of nodes, detects the disproportional packets going and coming from the attacker
2.	Typical DDOS Attack	Turns the computer into "zombies"	Using AhnLab TrusGuard DPX, designed to ensure immediate responses and mitigating the typical DDOS attacks
3.	Application layer attacks	Includes slowloris, Zero-day DDOS attacks	Incapsula examines the behavior and blocks the bad traffic
4.	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.
5.	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
6.	SYN Flood Attack	Exploit the vulnerabilities of TCP/IP protocol and perform three way	Filtering, increasing backlog, reducing SYN-RECEIVED Timer, SYN cookies eliminating the resources allocated to the target host.

		handshake	
7.	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.
8.	Slowloris	Enables one web server to take down another server without affecting target network	Increasing the clients, limiting the connections, restricting the length of time of a client.
9.	Zero-Day DDOS	New attacks exploiting vulnerabilities of the computer	Using single packet authorization, keeping up-to-date software, white listing allowing good applications to access the system.
10.	Amplification attack	Attacker makes a request that generates a larger response	Using high performance OS, load balancer, limiting the connection, limiting the connection rate.
11.	APT(Advanced Persistent Threat)	Powerful entity intents to gain access to a specific target such as political group or government	Using McAfee, which allows only the installation or execution of important programs.
12.	Booter Shell Scripts	Makes difficult to distinguish between legitimate and illegitimate traffic	Continues testing of web applications and known vulnerabilities in commercial applications.
13.	C99 Shell	Exploits web application vulnerabilities and takes control of web servers	Have up-to-date scripts and programs, disable remote URL, turns the safe mode on.
14.	DNS Flood	Attacks both infrastructure and DNS application	Radware carrier solution, allowing continuous DNS service even under the attack and mitigating the DNS attack.
15.	Exploit	System vulnerability use to obtain unauthorized access	Cyclope Employee Surveillance Solution v 6 SQL Injection prevents the user from manipulating the SQL query.
16.	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.
17.	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.
18.	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.

19.	Infrastructure DDOS attack	Overloads the network infrastructure by consuming large amount of bandwidth	First Line of Defense provides corero's DDS tool to inspect, detect and protect the infrastructure attacks.
20.	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.
21.	Layer 7 DDOS attacks	Overloads the specific elements of an application server infrastructure	Apache, shows the message request time out and IIS, limit the size of the request to each requirement.
22.	Public Exploit	Released to the public via standard channels like mailing lists, exploit archives, mainly through JAVA	Either unplug JAVA from your browser or uninstall it from your computer completely.
23.	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 will limit the ability of an intruder to take advantage of these attacks.
23.	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 will limit the ability of an intruder to take advantage of these attacks.
24.	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.
25.	Local Privilege Escalation Exploit	A small piece of code that enhances the user to root attack by exploiting vulnerabilities	Install the vendor patch such as Windows Anti 4.0, Windows 2000, Windows Vista etc.
26.	Website Defacement	Attacker obtains access to a website in order to alter its visual appearance	Employee the security management installed by a top-tier technology consulting group which makes it difficult to attack the website.
27.	Volume Based Attack	Includes UDP floods, ICMP floods and other spoofed	Incapsula absorbs the attack with the global network

		packet floods	
28.	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.
29.	User-to-Root Attack	Normal user gains access to a computer by exploiting its vulnerabilities	Intrusion Detection System with genetic algorithm which filters the traffic and reduces the complexities.
30.	Remote-to-local Attack	Remote user gains local access to a computer by exploiting its vulnerabilities	Applying direct, indirect, Identity-based validation techniques which prevents the reverse look ups and limits the extent of damage.
31.	Scan Attack	Attacker gains access of OS and open ports of the target network	Alternative engine blocking system takes less detection time and is much more effective than PSAD and ClearOS
32.	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.

All, the above listed defense procedures along with their respective attacks are able to mitigate the DoS attacks up to some extent. But when it comes to DDoS attacks i.e. Distributed Denial of Service attacks, these defense mechanisms fail to cop up. This is because now the attack traffic is not coming from a single source; instead it is coming from a collection of systems i.e. distributed systems.

Any defense mechanism should be designed by keeping in view the following principles.

1. The defence mechanism should be followed at every stage of the entire network.
2. The defence procedure should preserve the legitimate traffic as much as possible there by preventing the damage.
3. Defence method should facilitate a complete, secure and authenticated communication channel.
4. A defence method should take care of the scalability issues as per further requirements in the future.
5. A defence mechanism should not only detect but mitigate the attack as well.

4 Solution Proposed For DDoS Mitigation

In order to mitigate the DDoS attacks this paper has proposed the following defense scenario which involves the four steps. These are as follows:

1. The Detection of DDoS attack.
2. Sending the attack traffic first for the treatment and not to the target.
3. Monitoring and filtering the illegitimate packets from the legitimate packets there by allowing the legitimate traffic to complete the transactions and preventing the illegitimate traffic.
4. Forwarding the good traffic to the target or the receiver end.

This mechanism will provide complete protection not only against the known DDoS attack but those that have never been examined before also. This defense architecture will deliver an immediate response to DDoS which will be measured in seconds and not hours. This mechanism will be throwing light on two components:

1. The Detector
2. The Guard

Following fig 2, is a flowchart depicting all the above mentioned steps in order to specify how each and every phase of this defense mechanism works.

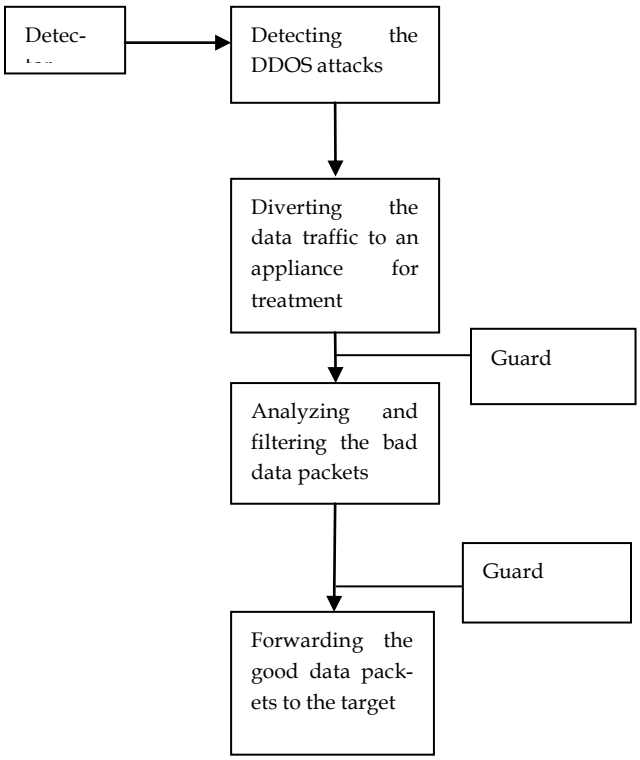

Fig. 2 Flowchart for Solution Set against DDoS Attacks

The components, Detector and Guard by working hand in hand will ensure a complete DDoS protection against all type of DDoS attack. A brief description of these components is given below.

4.1 Detector

This component will give a complete analysis of complex DDoS attack. It will examine the network traffic. If any misbehavior or deviation from the normal behavior is found in the traffic, it will immediately indicate a DDoS attack. After the attack's indication, the detector alerts the guards, the other component, to quickly react to the attack.

4.2 Guard

It is a DDoS mitigation device deployed upstream at the data center which gives a high performance output. When the guard is indicated of the attack, the malicious traffic which was to be forwarded to the target is diverted to the guard and is subjected to a five stage analysis to separate the legitimate and the illegitimate packets. The guard provides instant protection without causing any impact on the data traffic flow of other systems.

The fig. 3 shows how detector and guard detect and mitigates the attack.

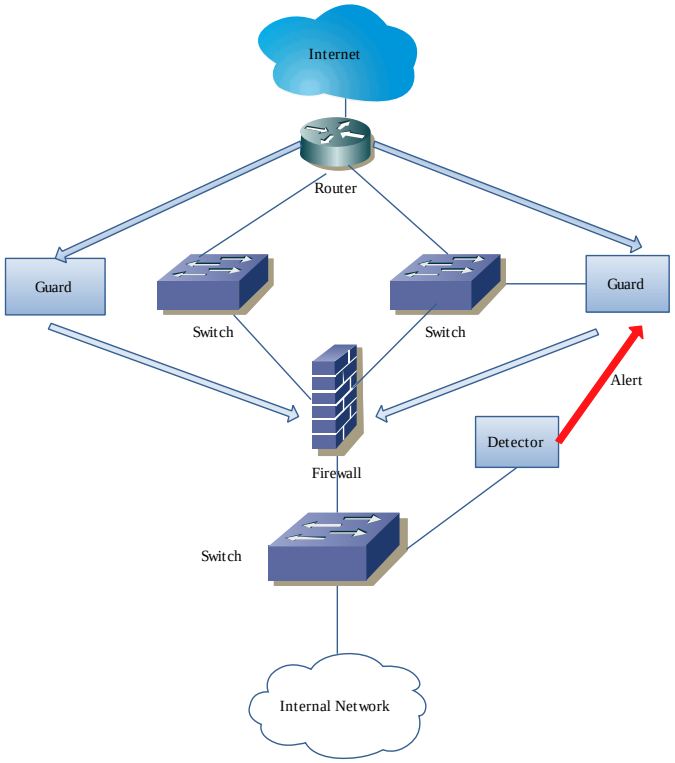

Fig. 3 Modified Architecture for DDoS Mitigation

The five steps purification of the malicious traffic is as follows:

4.3 Purification Process

4.3.1 Filtering

Static and dynamic DDoS filters for the purpose of filtering of malicious traffic. To block the non-essential traffic from reaching the victim, static filters are used. In order to have real time updates of suspicious flows or block sources, dynamic filters are used. Dynamic filters are deployed by other modules on the basis of complete analysis of traffic flows and behaviour.

4.3.2 Anti-Spoofing

This process helps to check that packets entering the system are not spoofed. The guard mentioned above, uses a numerous authentication procedures to stop the spoofed packets from reaching the victim. This module also verifies the proper identification of the good traffic there by removing the risk of good packets being discarded.

4.3.3 Anomaly Recognition

This stage of the purification process monitors all the traffic which is not stopped by filtering and anti-spoofing module. It will again check the normal behaviour of the packets which was recorded again and again over time. If any deviation from the normal behaviour is found, it will detect the malicious packet.

4.3.4 Protocol Analysis

This phase manages the flows of the traffic which were found suspicious in the above phase in order to identify attacks like HTTP-Error attacks. This phase also prevents any sort of misbehaviour in the protocol transactions.

4.3.5 Rate Limiting

This part of the purification procedure stops the malicious flows from increasing the rate with which they are heading towards the target.

The following fig. 4 shows how malicious attack traffic is purified through above steps.

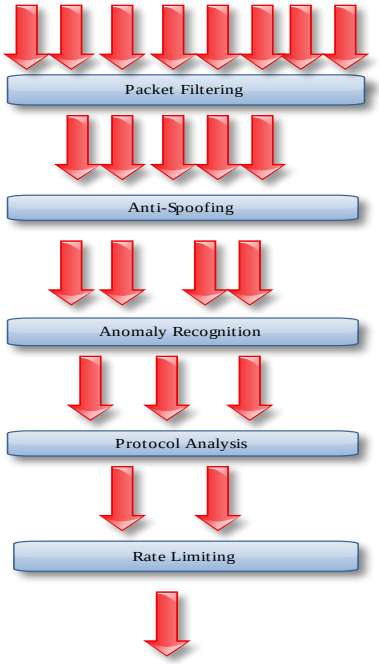

Fig 4. Purification Architecture for Malicious Traffic

5 Conclusions

The Distributed Denial-of-Service attacks have led to the decline of numerous web sites and networks there by resulting in the proposition of different defense mechanisms. Therefore, this paper had proposed a four step solution to defeat the DDoS attacks. These four steps included the detection and deviation of the attack traffic by the Detector, first for the treatment instead to the target, then the traffic is sent to the Guard for further sending it for filtering and finally forwarding the legitimate traffic to the target.

ACKNOWLGMENT

Foremost, we Upma Goyal and Gayatri Bhatti 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] A. Sperotto, G. Schaffrath, R. Sadre, C.Morariu, A. Pras and B. Stiller, "An Overview of IP Flow-Based Intrusion Detection," IEEE Communications Surveys & Tutorials, Vol. 12, No. 3, Third Quarter 2010.

[4] M. Sung and J. Xu, "IP Traceback-Based Intelligent Packet Filtering: A Novel Technique for Defending against Internet DDoS Attacks," IEEE Transactions on Parallel and Distributed Systems, Vol. 14, No. 9, September 2003.

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

[6] 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.

[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.