Volume 4, Issue 3, March 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Survey on Different Solutions to DDoS Attacks

Darshan Lal Meena
(Ph.D Scholar) Department of Computer Science.
MP, Bhoj Open University, Bhopal (MP) -462016
INDIA.

Dr. R.S.Jadon
Professor &HOD Department of Computer Application
MITS, Gwalior (MP)-474005
INDIA.

Abstract— Denial of Service (DOS) attacks are an immense threat to internet sites and among the hardest security problems in today's Internet. The problem of DoS attacks has become well known, but it has been hard to find out the Denial of Service in the Internet. Distributed Denial of Service (DDoS) attack is a large-scale, coordinated attack on the availability of services of a victim system or network resource, launched indirectly through many compromised computers on the Internet. Researchers have come up with more and more specific solutions to the DDoS problem. However, existing DDoS attack tools keep being improved and new attack techniques are developed. It is desirable to construct comprehensive DDoS solutions to current and future DDoS attack variants rather than to react with specific countermeasures. In order to assist in this, we conduct a thorough survey on the problem of DDoS. We propose taxonomies of the known and potential DDoS attack techniques and tools. Along with this, we discuss the issues and defend challenges in fighting with these attacks. Based on the new understanding of the problem, we propose classes of solutions to detect survive and react to the DDoS attacks.

Keywords— Denial of service, DoS, DDoS, DRDoS, Attacks, Internet Relay Chat(IRC) ,CAPTCHA, DefCOM

I. Introduction

Denial **of** Service **(DOS)** attacks constitutes a severe problem in the Internet. Distributed Denial of Service (DDoS) attacks exhaust victim's bandwidth or services . A recent attack report of year 2013—'Quarter 4' from Prolexic Technologies identifies that 1.56 percent increase in total number of DDoS attacks has been recorded as compared to similar attacks of previous quarter.The fourth quarter report (Fig-1.1 refer) Six of the top 10 source countries for DDoS attack in Fourth Quarter ,2013 were in Asia. The United state was the main source of DDoS attack during fourth quarter 2013, accounting for 23.62% of attack. China took second place this quarter at 19.09% percent. In an interesting turn of event, Thailand not only rejoined the top 10 after several quarter of not appearing on the list, but also ranked third with 13.5%.The united Kingdom(8.49%) and the Republic of Korea(South Korea 7.33%) round out of the top five. The remainder of the top ten list include India(6.57%),Turkey(5.84 %),Italy(5.76%),Brazil(5.30%) and Saudi Arabia(4.43%) percent.**[1]**

Denial of Service (DoS) attacks is very common in the world of internet today. Increasing pace of such attacks has made servers and network devices on the internet at greater risk than ever before. Due to the same reason, organizations and people carrying large servers and data on the internet are now making greater plans and investments to be secure and defend themselves against a number of cyber attacks including Denial of Service. A distributed denial of service attack (DDoS attack) is a large-scale, coordinated attack on the availability of services of a victim system or network resource, launched indirectly through many compromised computers on the Internet [**2**].(Fig-1.2 refer) Today's the Changing Nature of the Threat intruders are prepared and organised. Internet attacks are easy, low risk, and hard to trace .Intruder tools are becoming increasingly sophisticated and easy to use by novice intruders **[3]**

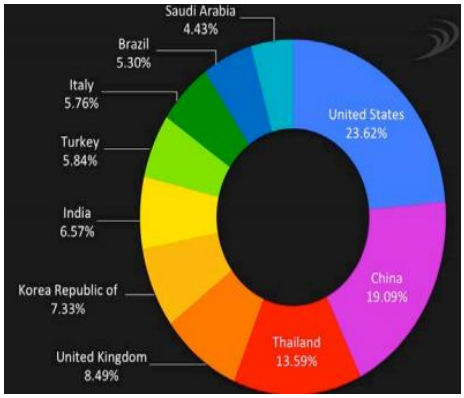

Fig:1.1 Six of the top 10 Source countries for DDoS attack in Asia

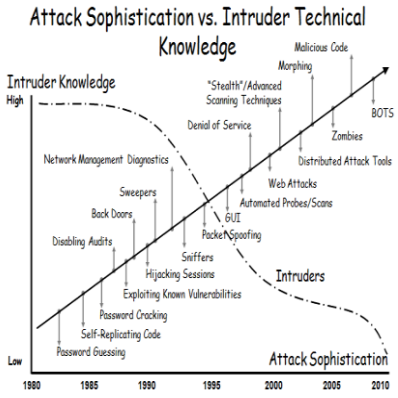

Fig 1.2 Attack Sophistication vs. Intruder Technical Knowledge

There have been a number of proposals and solutions to the DDoS attacks. However there is still no comprehensive solution which can protect against all known forms of DDoS attacks. In *this paper we try to introduce some structure and solutions to the DDoS and* analyze and classify the current solutions to the DDoS attack. By examining the pros and cons of each solution, we can know about the effectiveness of the solutions. *Our purpose is to describe the existing problems so* that a better understanding of DDoS attacks can be achieved and more efficient defense mechanisms and techniques can be devised. This paper is organized as follows. **Section 2** investigates the problem of DoS and DDoS attacks and presents a classification of DOS attacks. In **Section 3** we also discuss the current trends in DDoS attack. In **Section 4**, we propose **Taxonomies of DDoS Defense Mechanisms** and DDoS Attack Solution Considerations .In **Section 5**, We propose and analyze the desirability of that solution. Finally, We conclude the paper in **Section 6**.

II. Overview of DDoS Attacks:

2.1 **Denial of Service type:** A "Denial-of-Service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include:
Attempts to "flood" a network, thereby preventing legitimate network traffic, Attempts to disrupt connections between two machines thereby preventing access to a Service, Attempts to prevent a particular individual from accessing a service, Attempts to disrupt service to a specific system or person.
The United States Computer Emergency Readiness Team (**US-CERT**) defines symptoms of denial-of-service attacks to include[4]☹(i)Unusually slow network performance (opening files or accessing web sites)(ii)Unavailability of a particular web site.(iii)Inability to access any web site(iv)Dramatic increase in the number of spam emails received—(this type of DoS attack is considered an e-mail bomb)(v)Disconnection of a wireless or wired internet connection.

Denial of service can be divided into three forms.

Fig-2.1 DoS Attacks

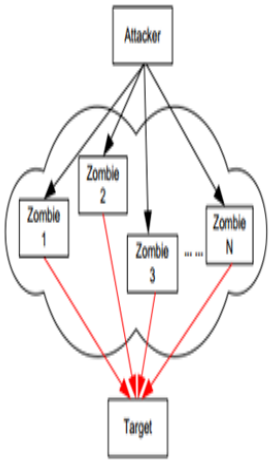

Fig :2.2 DDoS Attacks

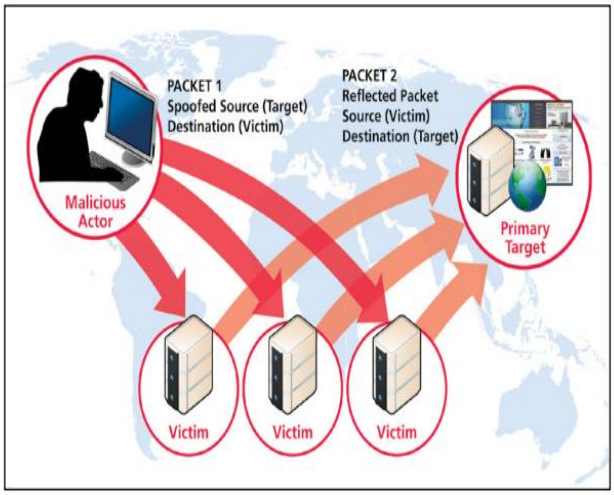

Fig-2,3 DRDoS Attacks

- **2.1.1 DoS Attacks:** DoS attacks (refer to Figure 2.1), a large number of malicious packets are sent from a single machine, with the aim of exhausting the target's computational and networking resources, or crashing the target. The purpose of such attacks is to deprive legitimate users of access to the target's services**.** In a DoS attack, one computer and one internet connection is used to flood a server with packets, with the aim of overloading the targeted server's bandwidth and resources[**5**]. Denial-of-service (DoS) attacks exceeding 20G bps, which will overwhelm almost any online service's bandwidth, more than quadrupled so far in 2013, compared with the previous year, according to the network management firm. While the attacks account for only approximately 1 percent of all data floods, the increase in large-bandwidth DoS attacks suggests that more serious groups are now using denial of service as a common tactic.[**6**] . DOS attacks can be classified as follows:
  - **Network Device Level**: DOS attacks in the Network Device Level include attacks that might be caused either by taking advantage of bugs in software or by trying to exhaust the hardware resources of network devices.
  - **OS Level**: In the OS Level DOS attacks take advantage of the ways operating systems implement protocols.
  - **Application-based attacks**: A great number of attacks try to settle a machine or a service out of order either by taking advantage of specific bugs in network applications that are running on the target host or by using such applications to dram the resources of their victim.
  - **Data Flooding**: An attacker may attempt to use the bandwidth available to a network, host or device at its greatest extent, by sending massive quantities of data and so causing it to process extremely large amounts of data.
  - **Attacks based on protocol features**: DOS may take advantage of certain standard protocol features, for example several attacks exploit the fact that P source addresses can be spoofed

2.1.2 DDoS attack: A distributed denial of service attack (DDoS) (refer to fig 2.2) occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. This is the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. When a server is overloaded with connections, new connections can no longer be accepted [**7**]

2.1.3 DR-DoS attacks : distributed reflector denial of service (DRDoS) **(refer to** Figure 2.3) Illustrates another type of bandwidth attack called a **distributed reflector denial of service** (DRDoS) attack, which aims to obscure the sources of attack traffic by using third parties (routers or web servers) to relay attack traffic to the victim. These innocent third parties are also called the reflectors. Any machine that replies to an incoming packet can become a potential reflector. In 2012 there was a significance increase in the use of a specific distributed denial of service (DDoS) methodology known as Distributed Reflection Denial of Service attacks (DR-DoS). DR-DoS attacks have been a persistent and effective type of DDoS attack for for more than 10 years. The techniques shows no sign of obsolescence; it continuous to grow in effectiveness and popularity. The four types of DR-DoS are:

(i)DNS (Domain Name System): In a DNS reflection attack, the malicious actor execute a large number of DNS queries while spoofing(pretending to be form) the IP address of the primary target. The victim DNS server respond to the spoofed IP address, sending a large flood of traffic to the primary target.

(ii)SNMP (**Simple Network Management protoco**l)/**NTP** (**Network Time Protocol**)/**CHARGEN**(**Character Generator Protocol:)** SNMP attacks allow malicious actor to hijack unsecured network device such as router ,printer, cameras and sensors and other devices and use them as a bots to attack third parties. Similarly , basic vulnerabilities in NTP and CHRGEN Protocol(used for time synchronization and response test respectively),can be used to misdirect and amplify server response to third parties victim

(iii)SYN : A SYN flood takes place when the original SYN connection request is repeated in rapid succession, until it overwhelm the target infrastructure with request.

(iv)Gaming server attacks: Online multiplayer Gaming server are being gamed by hackers to launch aggressive attacks against financial and other organizations using DNS reflection Denial of sevice (DRDoS) techniques that have been honed to a fine art by online gamers that regularly use them to cripple online opponents.

2.2 Elements, Tools, and strategy of DDoS attacks: A DDoS attack uses many computers to launch a coordinated DOS attack against one or more targets. Using client /server technology, the perpetrator is able to multiply the effectiveness of the DOS significantly by harnessing the resources of multiple unwitting accomplice computers, which serve as attack platforms. A DDoS attack is composed of four elements as illustrate in figure 2.4

(i)The real attacker. (ii)The handlers or master compromised hosts, who are capable of controlling multiple agents. (iii) The attack daemon agents or zombie hosts, who are responsible for generating a stream of packets toward the intended victim.(iv) A victim or target host.

(i) Recruitment: The attacker chooses the vulnerable agents, which will he used to perform the attack. The attacker chooses the vulnerable agents, which will he used to perform the attack. V. Yegneswaran et al [**8**] aggregated and analyzed firewall logs from over 1600 networks and reported that about 3 million scans happened everyday and 20% to 60% of these scans are Web server vulnerability scans and are linked to worm propagation attempts. Attackers use various kinds of scanning strategies to chose addresses of potentially vulnerable machines to scan [**9**].

There are important scanning are Random Scan, Hit list Scan, Route-based Scan, Divide-and-conquer Scan, Local Preference Scan, Topological Scan and Permutation Scan

(ii)Zombie Compromise: The attacker exploits the vulnerabilities of the agents and plants the attack code, protecting it simultaneously from discovery and deactivation.

(iii)Communication: The agents inform the attacker via handlers that they are ready. The communication channels between the attacker and the agents have two models (i) **Agent-Handler Model(ii) -IRC-based Model** Internet **Relay Chat (IRC)**

(iv)Attack The attacker commands the onset of the attack. Sophisticated and powerful DDoS toolkits are available to potential attackers increasing the danger of becoming a victim in DOS or DDoS attack. Some of the most **known** DDoS tools are **Trinoo,** TFN, Stacheldraht, **TFNZK,** mstream and Shaft.

2.3: DDoS attack classification: There are two main classes of DDoS attacks **(Figure 2.5):** (i) Bandwidth depletion and (ii)Resource depletion attacks.

2.3.1 Bandwidth depletion attack is designed to flood the victim network with unwanted traffic that prevents legitimate traffic from reaching the victim system. Bandwidth attacks can be divided to(i)**Flood attack** (ii) **Reflect attack**

2.3.1.1Flood Attack In a direct attack, zombies flood the victim system directly with IP traffic. The large amount of traffic saturates the victim's network bandwidth so that other legitimate users are not able to access the service or experience severe slow down. Normally in those attacks, the following packets are used.

-TCP floods A stream of TCP packets with various flags set are sent to the victim IP address. The SYN, ACK, and RST flags are commonly used

-ICMP echo request/reply (e.g., ping floods) A stream of ICMP packets are sent to a victim IP address.

-UDP floods: A stream of UDP packets are sent to the victim IP address.

2.3.1.2 Reflected Attack or Amplification: A reflected denial of service attack involves sending forged requests of some type to a very large number of computers that will reply to the requests. Using Internet protocol spoofing, the source address is set to that of the targeted victim, which means all the replies will go to (and flood) the target. ICMP Echo Request attacks can be considered one form of reflected attack, as the flooding host(s) send Echo Requests to the broadcast addresses of mis-configured networks, thereby enticing a large number of hosts to send Echo Reply packets to the victim

2.3.2. Resource depletion Attacks:

2.3.2.1 TCP SYN Attack :The TCP SYN attack exploits the three-way handshake between the sender and receiver by sending large amount of TCP SYN requests with spoofed source address. If those half-open connection binds resources on the server or the server software is licensed per-connection, all these resources might be taken up.

2..3.2.2 Malformed Packet Attack a ping of death (abbreviated "POD") is a type of attack on a computer that involves sending a malformed or otherwise malicious ping to a computer. A ping is normally 64 bytes in size; many computer systems cannot handle a ping larger than the maximum IP packet size which is 65,535 bytes. Sending a ping of this size often crashes the target computer

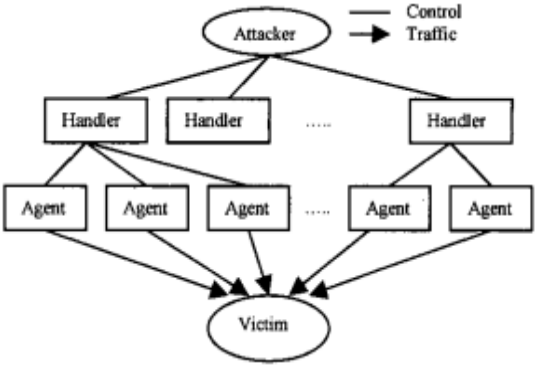

Figure 2.4- Architecture of DDoS attack

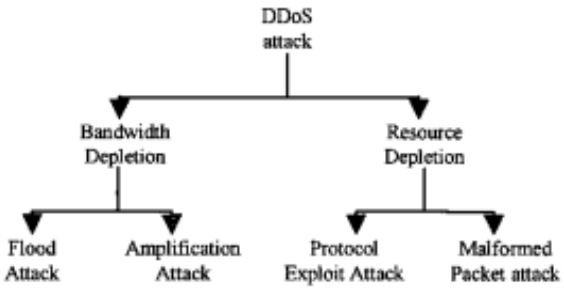

Figure:2.5 - DDoS attack classification

III DDoS Attack Trends

There is little change in the nature of the targets of DoS attacks. The Internet community, ranging from individual end-users to the largest organizations, continues to experience DoS attacks. Following are the technology trend of current DDoS attacks [**10**].

- **Larger botnet size** There is a steady increase in the ability for intruders to easily deploy large DDoS attack networks. In the race of available consumable resources versus the ability to consume those resources, today's DDoS networks continue to outpace available bandwidth in most cases.
- **Advances in master-zombie communications** recently, there is an increase in intruder use of Internet Relay Chat (IRC) protocols and networks as the communications backbone for DDoS networks. The use of IRC essentially replaces the function of a handler in older DDoS network models. IRC-based DDoS networks are sometimes referred to as botnets, referring to the concept of bots on IRC networks being software driven participants rather than human participants. The use of IRC networks and protocols makes it more difficult to identify DDoS networks.
- **Base on legitimate traffic** Where packet filtering or rate limiting can be effective to control the impact of some types of DoS attacks, intruders are beginning to more often use legitimate, or expected, protocols and services as the vehicle for packet streams. Doing so makes filtering or rate limiting based on anomalous packets more difficult. In fact, filtering or rate limiting an attack that is using a legitimate and expected type of traffic may in fact complete the intruders task by causing legitimate services to be denied.
- **Less reliance on source address spoofing** Although it is still used, less emphasis is put on source IP address spoofing in DoS attacks. With highly distributed attack sources, that many times cross several autonomous systems (AS) boundaries, the number of hosts involved as sources of an attack can be simply overwhelming and very difficult to address in response. Source IP address spoofing simply is not a requirement to obfuscate large numbers of attack sources and enable the attacking party to avoid accountability for the attack.

The resulting attacks are hard to defend against using standard techniques, as the malicious requests differ from the legitimate ones in intent but not in content. Turing test is a desirable way to tell human from machines

IV Taxonomies of DDoS Defense Mechanisms:

DDoS Defenses: There are three basic categories of DDoS defenses, namely **prevention**, **detection** and **reaction/responses**. The DDoS defense mechanisms can be roughly divided into three categories: **Survival Mechanisms**, **Proactive techniques** and **Reactive Mechanisms.**

4.1Survival mechanisms: Survival mechanisms involve increasing the effective resources to such a degree that DDoS effects are limited. This kind of enlargement can be achieved statically by purchase more hardware and use load Balance techniques to increase the system capacity, or dynamically by acquiring resources at the time of DDoS attack and replicate the service. However, the arm race with DDoS attackers still seems to be hard for the victims, as it is easier for attackers to acquire additional thousands of zombies to win the race. Thus this kind of approach cannot give a complete solution to DDoS.

4.2 **Proactive techniques**: In proactive techniques, the aim is to detect an attack earlier than it can reach the victim. After detection, a mitigation procedure can be called immediately to filter or rate-limit the attack traffic

4.3 **Reactive Mechanisms**:. In reactive techniques, the victim actually encounters a DDoS attack on its services and then a detection & mitigation procedure is called to trace the attack origin and filter the traffic coming from identified

sources. Reactive mechanisms try to detect the occurrence of the attack and react to that either by controlling attack streams, or by attempting to locate agent machines and invoking human action. There have been numerous proposals and partial solutions available today for react to the DDoS attack. Those reactive mechanisms can be further divided into several classes

4.**3.1 spoofed based**: For spoofing-based attacks, we need to identify the sources of attack traffic. This kind of approaches [11] [12] [13] try to figure out which machines attacks come from. Then appropriate measurement will be take on those machines (or near them) and eliminate the attacks. In the case where attacker has a vast supply of machines, the trace approaches become not too helpful. A good example of the trace back technique is Traceback:

Traceback [14] is a technique for locating the agent machines making the DDoS attacks. It helps a victim to identify the network paths traversed by attack traffic without requiring interactive operational support from internet Service Providers. This approach is demonstrated in Figure 4.1 Each packet header may carry a mark, containing the EdgeID, represented by the IP address of the two routers forming an edge. This is used to specify an edge it has traversed. In addition, another field in the header is reserved to specify the distance from the edge to the victim.

Marking procedure at router R:
for each packet w
let x be a random number from [0..1)
if x < p then
write R into w.start and 0 into w.distance
else
if w.distance = 0 then
write R into w.end
increment w.distance

Path reconstruction procedure at victim v:
let G be a tree with root v
let edges in G be tuples (start,end,distance)
for each packet w from attacker
if w.distance = 0 then
insert edge (w.start,v,0) into G
else
insert edge (w.start,w.end,w.distance) into G
remove any edge (x,y,d) with d 6= distance from x to v in G
extract path (Ri..Rj) by enumerating acyclic paths in G

Figure 4.1: Traceback edge sampling algorithm

Routers mark the packets with some probability. And when a router decides to mark a packet, it writes its own address into the start field of the EdgeID and mark the distance field to zero. Otherwise, if the distance field is already zero this indicates that the packet was marked by the previous router. In this case, the router writes its own address into the end field of the EdgeID. Thus this represents the edge between itself and the previous router. In addition, if the router doesn't mark the packet then it always increments the distance field. This is important for assist in figure out the attacker spoofing those fields. The victim under attack reconstructs the path from the marked packets using the algorithm described in Figrue 4.1

Strictly speaking, traceback does nothing to stop the DDoS attacks. Actually it only identifies attackers' true IP addresses within a subnet. If the IP spoofing are prohibited in the Internet, traceback would be of no use. The pro side of traceback is that it can be incrementally deployable, because edges are constructed
only between participating routers. It is effective for non-distributed attacks and those highly overlapping attack paths. The information about the attack paths can help locating routers close to the source. Yet the con side of this approach is that packet marking incurs overhead at routers and reassembling the widely distributed attack paths is computational expensive. Furthermore, the path reassembly is quite complex and it is hard to make sure of its complete correctness. In addition,because the routers only mark the packet probabilistically, chances are that some of the packets are not marked at all. If those happen to be the spoofed packet from the attacker, they can produce false outcome.

4.3.2Non-spoofing-based Filtering Based on Traffic Anomaly Filtering and rate-limiting are the basis for most defensive approaches. This defense category addresses the core of the problem by limiting the amount of traffic presented to target. Filtering drops packets with particular characteristics. As long as the characteristics of the traffic are correctly identified, collateral damage can be low, but there is no guarantee that enough packets have been dropped. On the other hand, rate-limiting drops packets on basis of the amount of traffic. This technique does assure that target is not overwhelmed, but part of the legitimate traffic might also be dropped. Those filtering are done in the IP-layer.**:**

4.3.2.1Core-based Filtering: **Pushback** [16] [17] is a mechanism to preferentially drop attack traffic to relieve the congestion. Aggregate-based congestion control (ACC) that operates at the granularity of aggregates was proposed. An aggregate is a collection of packets from one or more flows that have some property in common. An example of aggregates are TCP SYN packets and ICMP ECHO packets. To reduce the impact of congestion caused by such aggregates, two related ACC mechanisms are used. The local aggregate-based congestion control (Local ACC), consists of an identification algorithm used to identify the aggregate(s) causing the congestion, and a control algorithm that reduces the throughput of this aggregate to a reasonable level. The second ACC mechanism, pushback, allows a router to request adjacent upstream routers to rate-limit the specified aggregates. Pushback prevents upstream bandwidth from being wasted on packets that are only going to be dropped downstream. In addition, for a DoS attack, if the attack traffic is concentrated at a few upstream links, pushback protects other traffic within the aggregate from the attack traffic. Figure 4. 2 depict the architecture of an ACC-enabled router. Using this approach, even a few core routers are able to control the high volume attacks. ACC mechanisms fall between the traditional granularity of per-flow control (which looks at individual flows) and active queue management (which does not differentiate between incoming packets). This kind of separation of traffic aggregates improves current situation with the right granularity. As routers are well equipped

to handle high traffic volumes and deployment at a few core routers can affect many traffic flows due to core topology, this approach is possible to successfully control the attack and relieve congestion in the Internet .Yet on the other hand, Pushback only works in contiguous deployment and deployment requires modification of existing core routers and might need to purchase new hardware.

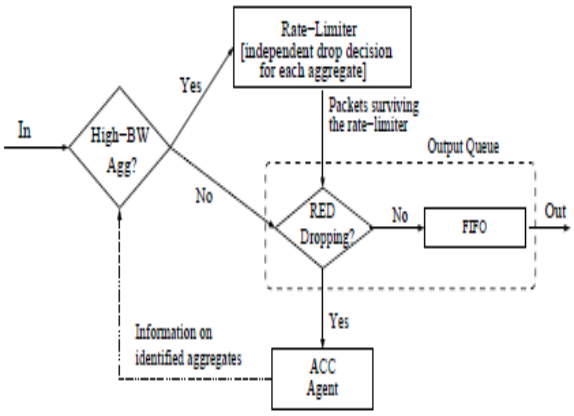

Fig 4.2Architecture of an ACC-enabled router. Packets with high bandwidth aggregates pass through the rate limiter. All packets drop by RED are passed to the ACC agent for identifying aggregates

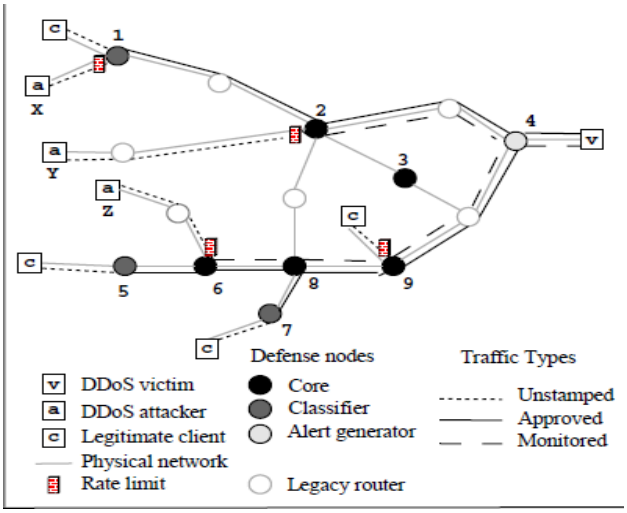

Figure 4.3: DefCOM deployment overview

4.3.2.2Edge-based Filtering: Egress filtering monitors and filters the packets that leave internal network to external network. Certain rules can be set up in the router to determine whether a packet should be filtered or not. If the packet pass all the rules, they are routed the sub-network. In DDoS attacks, the IP address of a packet are often be spoofed, thus there is a good probability that the spoofed source address of this packet is not a valid source address of that sub-network. When the firewall rule explicitly filters out all the traffic without an IP address originating from this subnet, those DDoS packets with spoofed IP source addresses will be discard.

In **ingress filtering**, packets coming into the network are filtered if the network sending it should not send packets from IP address of the originating computer. In order to do ingress filtering, the network needs to know which IP addresses each of the networks it is connected to may send. This is not always possible. For instance, a network that has a single connection to the Internet has no way to know if a packet coming from that connection is spoofed or not. Thus this requires that the ingress filtering deployed at the border of Internet Service Providers where address ownership is relatively unambiguous and traffic load is low. However, the success of ingress filtering requires widespread deployment. Yet up until now, the majority of ISPs are reluctant to implement this service because of the administrative complexity and potential overhead. In addition, even ingress and egress filtering are universally deployed,
attackers can still forge addresses from the hundreds or thousands of hosts within a valid customer network [18].

***DefCOM**: Jelena et al. [19] suggested a distributed framework, the Defensive Cooperative Overlay Mesh (**DefCOM**) for DDoS defense. DefCOM consists of heterogeneous defense nodes organized in a peer-to-peer network, communicating to achieve a dynamic cooperative defense. Figure 4.3 shows the high-level overview of DefCOM's operation. There are three types of nodes **(i)Alert generator**: detect the attack and inform other nodes(ii) **Classifier**: distinguish legitimate traffic from malicious traffic, forward the legitimate packets marked with legitimate mark, limit the rate of the suspicious packets and mark them with monitored mark.(iii) **Rate-limiter**: limit the rate of all traffic to the victim and give the highest priority to legitimate traffic.

Alert generators and classifiers deployed at the edge while rate-limiters deployed at the network core. Alert generator at the victim-end can detect the malicious traffic with high accuracy, while classifier at the source side can effectively stops attacks with the information provided by the alert generator and thus the collateral damage can be limited to minimum. Rate-limiter in the network core can handle attacks from those networks that do not have classifier nodes.DefCOM is different from other DDoS defense system in that it perform all actions in the place where they are most suitable to be carried out: accurate detection in victim side, classification of the traffic types in the source side, rate-limiting in the network core. In addition, the incremental deployment is possible as the core nodes can handle attacks from legacy networks. On the other hand, this approach is only effective with at least some core router deployment. In addition, the compromised overlay nodes can do harm to the DefCOM operation

Filtering Based on Client "Authentication"

***Turing test:** Kill-Bots [22] is a kernel extension to protect Web servers against DDoS attacks that mimic flash crowds. Figure 4.5 summarizes the stages of Kill-Bots processing. When a new connection arrives, it is first checked against the list of detected zombie address. If the IP address is not recognized as a zombie, Kill- Bots admits the connection with probability decided by the current load. In Stage1, admitted connections are served a graphical puzzle. If the client can solves the puzzle, it is given a Kill-Bots HTTP cookie which allows its future connections, for a short period, to access

the server without being subject to admission control and without having to solve new puzzles. While in Stage 2, Kill-Bots no longer issues puzzles, admitted connections are immediately given a Kill-Bots HTTP cookie. That is because during Stage 1, Kill-Bots should have identified the malicious attacker and added them in the recognized zombie list. Figure 4.4 Shows the graphical tests that Kill-Bots used to authenticates clients. In DDoS attack, instead of identifying individual users, we just need to distinguish between humans and machines as all known DDoS attacks are based on automated agents. Efforts to tell human and machine apart have led to a family of new security protocols known as "Human Interactive Proofs," or HIP's. For our purposes, Another well known and widely used defense against application layer DDoS attacks is CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) puzzle [20], which is considered to be the most promising technique against application layer DDoS attacks in current times [21]. In this scheme, a challenge-response test is presented to a prospective client requesting to establish a connection with a server. The purpose is to make sure that the response is generated by a human and not an automated machine targeting the server against some kind of attack. It is a good defense against e-mail spam and automated posting to forums and blogs etc. Today, many websites use CAPTCHA at initial login and registration phases to protect servers against application layer DDoS attacks such as HTTP flood etc. In Fig. 4.4, an example of CAPTCHA test is shown. CAPTCHA test is an effective technique against HTTP flood and SYN flood attacks. It is a victim-end, filtering technique with threshold-based mechanism [21].

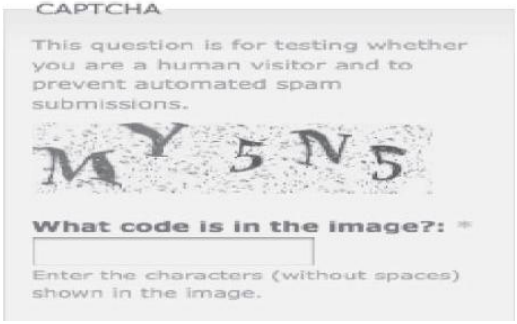

Fig :4.4 An example of CAPTCHA test

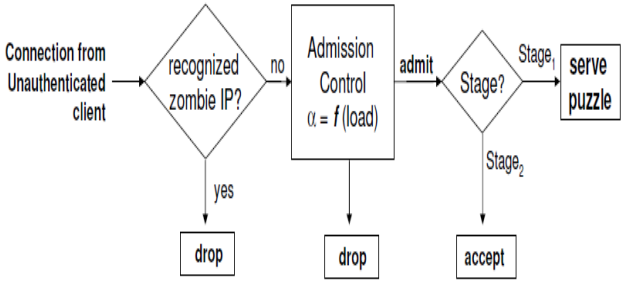

Fig:4.5 Stages of Kill-Bots processing

4.4 DDoS Attack Solution Considerations:

An ideal DDoS defense solution should have the following characteristics: effective, transparent to existing Internet infrastructure, low performance overhead, invulnerable to attacks aim at defense system, incremental deployable and no impact on the legitimate traffic. We will further discuss the solutions to DDoS attack based on those considerations

4.4.1 Effectiveness:

In the approaches for identify the source of attack traffic; Traceback facilitates locating routers close to the attack sources. Yet it does not work well for highly distributed attacks and its result is not 100% accurate. It is more effective for non-distributed attacks and for highly overlapping attack paths. Packet marks used in Traceback can be forged by the attackers.

In the attempts to filter the traffic, *pushback* is likely to successfully using the core routers to control the attack, relieving congestion in the Internet *DefCOM* adopts a distributed deployment and performs the action in where most successful: accurate detection at the victim, rate-limiting in the core and traffic differentiation at the source.

Some legitimate clients do not support certain legitimacy tests (i.e. ping test). *Kill-bots* uses a stateless authentication, provides solution to serves legitimate users who dont answer CAPTCHAs and optimizes the balance between authentication & service. It also improves the performance during Flash Crowds. All those make Kill-bots an efficient solution for online web business. *Low Bandwidth Turing Test* facilitates to defeat software agents without aggravating the DDoS problem, which makes the Turing test approach more effective.

4.4.2.Transparency to existing Internet infrastructure: Most of the approaches requires the changing of the Internet infrastructure, thus make the solution not so applicable. For example, the deployment of pushback requires modification of existing core routers and likely purchase of new hardware. The use of overlay network provide an alternative approach. These approaches don't require to change the network protocol or routers. Such system uses Internet-wide network of nodes to act as a distributed firewall, and carry out authentication for the clients. The protected servers hide behind the overlay network, only authorized clients can access protected servers through the overlay network. Overlay network is nothing but a nontransparent way of packet interception. Once all incoming packets into a protected server can be intercepted, whether the server's identity is secret or not is immaterial

4.4.3 Extent of modification to client-side software:

Most of the solutions don't require the modification to client-side software, like Egress Filtering and Ingress Filtering Yet the following solutions require the client-side change: In SOS, clients must be aware of overlay and use it to access the victim. When Client Puzzles are used, client modification is required to support receiving and solving the puzzles.

4.4.4 Performance overhead:

Some of the approaches have little overhead, for example, in Pushback; the operation is simple and nearly no overhead for routers. In trace back, Packet marking incurs moderate overhead at routers. Yet Reassembly of distributed attack

paths is prohibitively expensive, but this can be countered by doing the computation offline. When using the Client Puzzles, the puzzle verification consumes quite some of server resources.

4.4.5Accuracy of DDoS Defense DDoS defense usually requires dropping packets. But at the same time, legitimate traffic should be protected. Collateral damage should be kept minimum. *Pushback* minimizes collateral damage by placing response close to the sources. Collateral damage is inflicted by response, whenever attack traffic is not clearly different than legitimate traffic.

DefCOM uses selective response provides low collateral damage. In the case of using Turing test for client authentication, if the human client can not solve the Turing test properly, he might be refused for futher communication. *Kill-bots* distinguished the human user and attack agent further by how many unsuccessful attempts they have made. Then human users who do not answer CAPTCHAs can access the server despite the attack in the second stage.

V. Proposed Solution

Currently intruders are beginning to more often use legitimate, or expected, protocols and services as the vehicle for packet streams. The resulting attacks are hard to defend against using standard techniques, as the malicious requests differ from the legitimate ones in intent but not in content.

Thus a lot of approaches described in this survey are not suitable to handle this kind of traffic. Filtering or rate limiting based on anomalous packets are not feasible at all. In fact, filtering or rate limiting an attack that is using a legitimate and expected type of traffic may in fact complete the intruder's task by causing legitimate services to be denied. Currently, the most feasible way to handle this kind of situation is using the Turing Test mechanism as in *Kill-bots*. The graphical CAPTCHAs are most widely used today. It consists of a picture with some degraded or distorted image, which will take up a lot of valuable bandwidth especially in the case of the attack. Those graphical CAPTCHA consists of a picture with some degraded or distorted image. In the case of DDoS attack, sending those images from the server to the client for authentication actually consumes quite considerable bandwidth. T. Y. Chan has used the text-to-speech approach to generate the audio-based Turing test, yet it shows that the audio CAPTCHA largely ineffective. And actually

Audio-based Turing test will also consume remarkable bandwidth. Thus low bandwidth Turing test is very desirable for preventing the DDoS attack. One possible low-bandwidth Turing test is using **text-based question answering**, since computational linguistics is one of the most prominent research disciplines in artificial intelligence, and at the same time, Turing test in text format normally consume much less bandwidth.

VI . Conclusion

DDoS attacks are quite advanced and powerful methods to attack a network system to make it either unusable to the legitimate users or downgrade its performance. They are increasingly mounted by professional hacks in exchange for money and benefits. Botnets containing thousands of nodes impose a severe hazard to the Internet online business. Yet there seems to be no "silver bullet" to the problem. This survey examines the possible solutions to this problem, provides a taxonomies to classify those solutions and analyzes the feasibility of those approaches. Based on the analysis of existing solutions, we proposed desirable solution to defend DDoS.

ACKNOWLEDGMENT

Author like to thanks to thesis guide **Dr. R.S.Jadon** for his deep efforts and support towards the development of this research work. Also, Author would like to thanks MITS,Gwalior laboratory for providing such a valuable dataset for research in the field of different solutions to DDoS attacks.

REFERENCES:

[1]Prolexic Quarterly Global DDoS attack report Q1 2013 http://www.prolexic.com/knowledge-center-dos-and-ddos-attack-reports.html

[2] N. Long S. Dietrich and D. Dietrich, "Analysing distributed denial of service tools: the shaft case," in Proceedings of the LISA XIV.

[3]Howard F. Lipson, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues", CERT Coordination Centre, Networked Systems Survivability Program, Special Report CMU/SEI-2002-SR-009, http://www.cert.org/archive/pdf/02sr009.pdf, Nov. 2002.

[4]DDoS Defence Systems (DDS) SEMINAR ID: 1346 file:///C:/Users/admin/Downloads/Ankit_Chand-libre%20(2).pdf

[5]Charalampos Patrikakis, Michalis Masikos and Olga Zouraraki, "The Internet Protocol- Vol 7, Number 4".

[6]Aleksei Zaitsenkov, Dos Attack

[7]Jelena Mirkovic,Sven Dietrich,David Dittrich,Peter Reiher, "Internet Denial of Service:Attack and Defencse Mechanisms

[8]P. Barford V. Yegneswaran and J. Ullrich, "Iinternet intrusions: Global characteristics and prevalence," in *Proceedings of the 2003 ACM SIGMETRICS*, 2003

[9]C. Zou, D. Towsley, and W. Gong, "the performance of internet worm scanning strategies," 2003.

[10]Kevin J. Houle and George M. Weaver, "Trends in denial of service attack technology," http://www.cert.org/archive/pdf/DoS trends.pdf, October 2001.

[11] [18] Stefan Savage, David Wetherall, Anna R. Karlin, and Tom Anderson, "Practical

network support for IP traceback," in *SIGCOMM*, 2000, pp. 295–306.
[12], Stefan Savage, David Wetherall, Anna R. Karlin, and Tom Anderson, "Practical
network support for IP traceback," in *SIGCOMM*, 2000, pp. 295–306
[13] Alex C. Snoeren, Craig Partridge, Luis A. Sancheq, Christine E. Jones, Fabrice Tchakountio, Stephen T. Kent, and W. Timothy Strayer, "Hash-based ip traceback,"
[14] S. Bellovin, "Icmp traceback messages,"http://www.research.att.com/ smb/papers/draft-bellovin-itrace-00.txt, 2000.
[15]Fu hau Hsu and Tzi cker Chiueh, "A path information caching and aggregation approach to traffic source identification
[16]John Ioannidis and Steven M. Bellovin, "Implementing pushback: Router-based
defense against DDoS attacks," in *Proceedings of Network and Distributed System*
Security Symposium, Catamaran Resort Hotel San Diego, C alifornia 6-8 Februar2002, 1775Wiehle Ave., Suite 102, Reston, VA 20190, February 2002, The Internet Society.
[17] R. Mahajan, S. Bellovin, S. Floyd, J. Vern, and P. Scott, "Controlling high bandwidth aggregates in the network," 2001
[18] Computer Emergency Response Team, "Cert advisory ca-2000-01 denial-of-servic developments," http://www.cert.org/advisories/CA-2000-01.html, January 2000.
[19]J. Mirkovic, M. Robinson, P. Reiher, and G. Kuenning, "Alliance formation for ddos defense," 2003
[20]Ahn, L. V., Blum, M., and Langford, J., ''Telling humans and computers apart automatically,'' Commun. ACM, 47: 56–60(2004).
[21][24] Beitollahi, H., and Deconinck, G., ''Analyzing well-known countermeasures against distributed denial of service attacks,''Comput. Commun., 35: 1312–1332 (2012).
[22]Matthias Jacob Srikanth Kandula, Dina Katabi and Arthur Berger, "Botz-4-sale: Surviving organized ddos attacks that mimic flash crowds," in *NSDI'05*.

AUTHORS PROFILE

Mr.Darshan Lal meena is working as PGT(Computer Science) in Kendriya Vidyalaya ,Sarni and presently pursuing Ph.D in Computer Science in Department of Computer Science ,MP Bhoj Open University,Bhopal, Madhya Pradesh. Research Centre of Ph.d is MITS,Gwalior. My area of research is Network Security, DDoS Attacks in which I tried to **Novel Solution for Distributed Denial of Service Attacks.**

Dr R.S.Jadon presently working as a Head & Professor in Department Of Computer Application, Madhav Institute of Technology & Science[MITS],Gwalior. Owe the credit of more than 100 research papers published in international & national journals, conference & seminar.. His area of expertise is computer vision and image processing.

