DDOS Attacks: Trends, Challenges and Possible Solutions

Sandeep Kaur[1] Rakesh Kumar[2] Girdhar Gopal[3]
[1]Research Scholar [2]Professor [3]Assistant Professor
[1,2,3]Department of Computer Science & Applications
[1,2,3]Kurukshetra University

Abstract— Advancement in networking technologies brings the world together by introducing millions of innovative web applications such as WWW(World Wide Web) that give a common platform for all varieties of tasks like business, commercial, educational, health care, ministerial etc. Due to this rapid development and dependence on web application services their confidentiality, integrity and availability becomes a target of several security threats. DoS attack is constantly evolving security threat to web service availability. DoS exploit vulnerability or sending huge amount of packets to exhaust available bandwidth of targeted host and to bring it down. In this paper a detailed study of DoS attack with their attack techniques is provided. Some DDoS attack incidents are discussed to analyze with their attack method and adopted solutions to understand the impact criteria of this attack. Some possible solution guidelines are provided with each discussed DDoS attack vector to mitigate the impact of attack.

Key words: DoS, DDoS, Flood, Web, Vulnerability

I. INTRODUCTION

Today with over billions of users, the Internet becomes a vital part of our life. It has become a medium for people and business organizations to regularly access useful information, to do daily life tasks such as banking, and shopping etc through things like website. The Internet was designed to give web services such as easy sharing of information between various globally distributed computers and networks; it was not designed with security in mind. Due to several design principles of the Internet such as resource sharing, multipath routing, decentralized management, its infrastructure becomes vulnerable to serious security threats such as SQL injection, XSS attacks, buffer overflow or DoS attacks. These vulnerabilities are increasing day by day. This increase in the vulnerabilities in Internet connected devices is not only because more applications are available for the attack, but also due to the fact that more systems or tools are available from which the attack could be carried out. These attack tools, codes are freely available on Internet and can be used easily by any non technical people having small knowledge.

DoS attack is one of the top network security threats. DoS attacks are used to prevent normal users from accessing services of targeting host or resource. DoS attacks generally conquer the victim by overwhelming its resources. DoS attack can target Gaming, Educational, Financial, health, Governmental organizations including ISP (Internet Service Provider). According to Radware Global security report 2015 [1], ISP is at top in list of targets of DDoS, attack vectors for these attacks was amplified UDP NTP and SSDP reflected floods. This paper provides analysis of DDoS attack trends with guidance to mitigate these risks by reducing the opportunities for attackers.

This paper is organized in seven sections. Section II defines DoS and DDoS attacks, and its types. Section III discusses detailed study of commonly used DDoS attack vectors with guidelines to prevent them. Section IV contains description of some online available tools for DoS attacks. In section V Case studies of vulnerable applications are discussed with some guideline. In Section VI some existing solutions for DDoS attack are discussed with their limitations and effectiveness. Section VII presents the conclusion of the paper.

II. DOS AND DDOS ATTACKS

A denial of service (DoS) attack used to deny access to any shared devices or resources for legitimate users. DoS attack is launched by a single host or system. Two most common methods used by DoS attacker to perform attack are [2] :

- By exploiting web application vulnerabilities or weakness in Internet, for example logic attack is LAND attack.
- By sending a huge amount of malicious traffic towards victim (flooding attack). Example of flooding attack is TCP/SYN flood attack, UDP flood attack etc.

Flooding attacks can target a particular web application by consuming key resources of any computing network and service like memory or I/O or link bandwidth, TCP connection buffers, application service buffer, CPU cycles, etc. They can disturb normal functioning of any network by disabling its service or downgrade service performance by exhausting resources for providing services. When attack traffic comes from multiple resources, residing at different locations then this type of attack is Distributed Denial of Service attack (DDoS). DDoS attack uses hundreds or thousands of compromised hosts called zombies (bots, attacking hosts) in a controlled manner to launch the attack. Due to dispersed location of attack sources the problem of defense becomes more complicated. Figure 1 shows the scenario of DDoS attack using Zombies hosts. DDoS attackers are usually motivated by several factors such as gaining financial benefits, slow network performance, service unavailability, political issues, revenge etc.

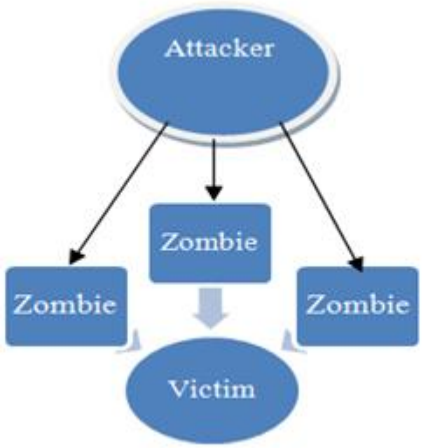

Fig. 1: DDoS attack scenario

A. DDos Attack Phases:

DDoS attack basically follows a four phase process:

- Discovering vulnerable hosts or agents and building an attack network

DDoS attack uses geographically distributed compromised hosts for achieving the desired scope of impact on victim. These compromised systems form an attack network called Botnet and in this network Zombies are called bots. Examples of attack network are Botnet Honeynet (2005), Glooglebot, BaiduSpider [3]. For finding vulnerable hosts in network attacker can use random scanning and install malicious code in it or Worms can be used (such as Mydoom, Codered etc.). Today Botnet are easily available online, attacker can use them by purchasing or paying rent.

- Compromise

The attacker exploits vulnerabilities in the agent machines and installs the attack code. These compromised hosts further scan for vulnerable systems, due to this self propagation nature a large-scale attack network can be easily built having thousands of compromised hosts.

- Communication

The attacker communicates with the agents to find the active agents, to plan attacks or to upgrade agents. The communication among the attackers and agents can be done through various protocols such as TCP, UDP or ICMP.

- Attack process

Attacker is the master of these compromised hosts; whole attack process is controlled by it. Attacker sends commands to zombies (compromised hosts) to launch attacks. Zombies perform action depending on command given by the attacker.

B. Types Of Ddos Attack:

There are three main Categories of DDoS based on how they affect the victim are:

- Volumetric attacks are used to exhaust the bandwidth of victim's network. In this type of attack large volume of traffic is send towards victim to consume its bandwidth. The effect of these attacks is measured in Bps (bit per second).
- Protocol based attacks consumes actual server resources such as firewall and load balancers. The size of the attack is measured in Packet per second.
- Application based attacks target a particular application. The aim is to consume available resources of web server to make it unuseful. Measure for the attack is Request per second.
- Based on traffic generation method used DDoS attack can be:
- Direct DDoS attack: Direct DDoS attack [4] in which attacker directly sends large number of attack packets to victim. These packets can be ICMP, UDP or combination of both.
- Reflector attack: Reflector attack uses intermediate nodes known as reflectors as attack launchers. Attackers send packets to reflector with spoofed IP address. Without realizing these packets are malicious reflector forward packets to victim. IP traceback do not work for these attacks because of IP spoofing. Specific methods for Direct and Reflector attack are discussed in Section III.

III. DDOS ATTACK VECTORS

DDoS attack uses a variety of vectors for scaling the intensity and influence of attack. Distribution of various attack vectors are shown in Figure 2. Some commonly used DDoS attack vectors are discussed in this section:

A. Direct Ddos Attack Vectors:

Direct DDoS attackers directly target victim through agents without any other intermediate reflector node. Some specific Direct DDoS attack vectors are:

- TCP SYN flood

TCP is a connection oriented protocol. It requires a connection before starting actual communication. Attacker's abuses this feature by sending multiple fake SYN requests without acknowledgement and repeat this process; this causes multiple half-open connections at server tying up its available resources capcity. This will cause unavailability of server for legitimate users. In October 2014, a new type of SYN flood that transmits very large sizes SYN packet approximately 1000 bytes per packet which will complicate defense process. These attack exhaust's victim's bandwidth capacity faster than previously observed SYN Floods.

Guidelines: Use Firewalls, SYN Cookies for validating the incoming request. Network monitoring traffic monitoring tools like Tcpdump or Wireshark can be used for identifying the attack signatures.

- UDP flood

UDP is a connection less protocol. It does not require any handshake before communication as in TCP. In this attack multiple UDP packets with ICMP packet are sent to the victim using random ports. Real life Examples of these attacks are DNS root servers attacks against Github (2015).

Guidelines: Define the connection threshold limit for your network filter or Firewall that it can pass at a particular instance of time, when packet arrival rate exceed this threshold value drop it.

- HTTP flood

Web applications are accessed via HTTP protocol. HTTP GET request can be used for DDoS attack. It sends multiple HTTP GET requests rapidly to consume the resources and available bandwidth of target system. LOIC is a tool used to perform a HTTP Get based DDoS attack.HTTP flood can be used for reflection based DDoS attacks. Examples of HTTP reflection attacks are JavaScript-based DDoS, WordPress pingback and Joomla reflection attacks.

Guidelines: Investigate network logs at port 80 (default port for HTTP) for large number of traffic having same source IP addresses. Tcpdump or Wireshark can be used for network monitoring. Web Application firewall can be used to filter attack traffic.

Challenges: Headless browsers, such as PhantomJS and HTML Unit behave like browser normal but without GUI. These browsers easily bypass HTTP traffic easily. Today, Headless browsers are most concerning issue for DDoS mitigation.

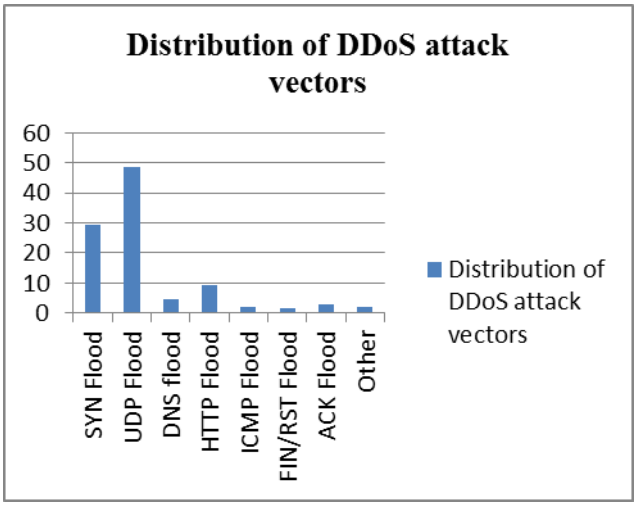

Fig. 2: DDoS attack vectors distribution

– ICMP flooding attack

In this attack, attackers send large volume of ICMP_ECHO requests directed at the victim. Victim then reply to each ICMP_ECHO request consuming its resources and bandwidth. This in turn causes crash or unavailability of victim host.

B. Reflected Amplified Flood Attacks:

A reflective amplification attack uses UDP, HTTP and TCP flood vectors amplification for achieving the desired scope of damage. These attacks become most disastrous when reflection is added. These types of DDoS attacks started in 2013 and becoming more persistent day by day. In 2015, UDP based reflection amplification attack rate increased, over 100 Gbit/s as compared to previous year. These DDoS attacks consists large SYN flood or UDP-based reflection amplification attacks. NTP, DNS, SSDP, and CHARGEN reflection attacks are common UDP-based reflection amplification attacks.

– NTP amplification attacks

Network time protocol is used to synchronize clocks of Internet connected devices and provide a list of servers or host connected to internet. For this "monlist" command is sent to NTP Server and server will send the list of active hosts on that sever. One "monlist" return a list of 600 hosts at a time, this "monlist" command can be sent with spoofed address, response will go to victim address whose address is used as requester.

Impact: An attacker can use tool like Metasploit or data from the OpenNTP Project to find the list of open NTP servers to perform DDoS attack. In DNS amplification attacks the 70:1 ratio [5] of query to response which means an attacker having 1 machine of capcity 1Gbps can use 70Gbps amplified traffic to launch DDoS attack. In an NTP amplification attack, this ratio can vary between 20:1 and 200:1 or more.

Guidelines: In UNIX operating system [6] the following command "ntpc" can be used to check for "monlist" vulnerability.

/user/sbin/ntpdc<remote server>

Disable monlist query features using "disable monitor" to your ntp.conf file and restarting the NTP process or upgrade your NTP server with ones having no "monlist" command capability for example "OpenNTPD".

Service	Port
NTP	120
DNS	111
CHARGEN	19
SSDP	1900
MC-SQL	1434

Table 1: Service port numbers for reflection attacks

– DNS amplification attack

DNS servers are responsible for converting IP address into corresponding domain names for example domain name "yahoo.com" to IP addresses "66.94.234.13". IP address is difficult to remember so domain names are used. Attacker can use multiple DNS resolving requests with spoofed IP address of Victim to overwhelm the overall capacity of victim. For this attackers use various methods in query for example a word "ANY" in DNS query expose all the available information about DNS [7]. DNS attack queries are much similar to normal query so finding attack signature is a difficult task.

DNSSEC protocol attack [8]: DNSSEC protocol prevents the modification of DNS information. In this protocol additional authentication information is sent with DNSSEC reply to minimize IP spoofing DNS attacks. DNS reply contain 512 bytes but the DNSSEC reply comes to about 4096 bytes (including additional information). Attackers exploit this feature of DNSSEC protocol to perform amplification DDoS attacks.

Guidelines: To identify if a DNS Reflection Attack with Amplification is occurring, monitor network logs and look for large DNS query responses with no matching DNS query requests. Rate limiting mechanism can be used to limit number of requests per server at a particular instance of time

– CHARGEN Reflective Attack

CHARGEN a character generation protocol defined in RFC864 works at UDP or TCP port 19 for monitoring, testing and debugging network traffic and applications [9] . Mostly it uses UDP and generates a large number of requests with spoofed IP address for exploiting multiple servers at once. In this way victims are flooded with UDP traffic generating larger response with small requests.

Guidelines: Disable CHARGEN if not needed. Monitor your network traffic so that packets having internal addresses will not your network so that IP spoofing can be prevented.

– SSDP protocol reflection attack

Simple Service Discovery Protocol (SSDP) is used for discovering and controlling Universal Plug and Play (UpnP). Over of 50 million UPnP devices on the Internet are suffering from UPnP and SSDP vulnerability [10]. UPnP is a networking protocol allows network devices to connect and communicate to each other. SSDP amplification attack sends malicious SOAP (used to deliver control messages to UPnP devices) requests with spoofed Source IP to many UPnP devices causes large response size exhausting the significant portion of available bandwidth of victim. SSDP can cause 30x amplification of attack traffic.

Guidelines: Monitor network web logs for large number of traffic from similar source IP addresses. Block all outbound traffic from UDP port 1900 for limiting the attack traffic.

– MC-SQL Reflection attack

The MS SQL server resolution protocol allows clients to get detailed information about the instances of SQL server running on a particular host this information can be abused to conduct DDoS attack by sending many SQL request. These small requests generate large size of responses. This type of attack was observed first in 2014 [11] against Missouri, a city of Columbia generating 440 amplification factors.

Guidelines: Filters can be used at SQL Server port. Servers having a single instance can disable this service.

Some more examples of reflection based DDoS attacks are RPC (Remote Procedure Call), Stream Protocol, Bittorent, NetBIOS etc.

C. Multivector Ddos Attack:

In 2014, a new trend for DDoS comes in existence called multivector DDoS. This attack gains popularity in 2015. It uses more than one attack vector for single attack such as UDP, NTP, SSDP, ESSYN, XML-RPC, CHARGEN and SSYN protocols etc. Multivector attacks confuse and overwhelm defense measures at target to achieve their. Multivectors attacks can use Network based attack vectors such as HTTP, DNS, NTP or brute force attack or Application based attack vectors such as XSS, SQL injection CSRF etc.

– Advance Persistent DoS (APDoS) attack

2015 [1] year network security report outlines the rise of advanced persistent denial-of-service (APDoS) attacks. APDoS attacks are flood attack applicable on both network layer and application level. APDoS attacks mainly target application layer using HTTP flood including repeated XSS and SQL injection attack vectors. So APDoS are multi vector attacks using 5-6 vectors with millions of query per second. APDoS can also use SYN flood to perform network layer DoS attacks on victim, these attacks can also compromise Internet service provider (ISP).

IV. DDOS ATTACK TOOLS

In starting DDoS attacks was carried out by using Worms Codered, Mydoom, SQLslammer, Slapper worm, Witty worm etc. As technologies grow, adaption in attack technologies also takes place. Today Worm's code and DoS attack tools are easily available online tools. These tools can be easily downloaded and used for sending malicious data flood towards victim. Some common online attack tools [12] are:

A. LOIC:

LOIC can send massive volumes of TCP, UDP, or HTTP traffic to overwhelm victim bandwidth. These tools can be used for testing of servers under heavy network traffic loads. Attacker can use these tools for targeting any host or network service. LOIC sends packets without HTTP headers for hiding there identity.

B. HOIC:

This tool provide a new method of adding random header with each data packet for avoiding attack detection. One tool for this type of attack is HOIC which allow users to add random header information made by combination of selected valid user headers. It uses simple GUI and can send massive HTTP POST and GET requests.

C. Slowloris:

Slowloris sends HTTP request with a very slow rate. It sends HTTP headers in small chunks with a very slow rate to the target; the server is forced to continue to wait for the headers to arrive.

D. R U Dead Yet? (R.U.D.Y.):

It injects HTTP POST requests and causes application threads to await the end of never-ending posts in order to perform processing. It causes crash or unavailability of system.

E. Botnet:

Botnet can be used as attack tools. Botnet is a network of millions of compromised hosts used to launch a coordinated attack. These compromised hosts are called Zombies. Attack based on Botnet amplify the effect of attack and causes more disasters results. Most common example of DDoS bots are Darkness, Optima, Dirt Jumper, Russkill, BroBot and BlackEnergy.

V. CASE STUDIES

DDoS attack impact can vary from minor user inconvenience to high revenue losses to the biggest financial organizations. According to CIAC (Computer Incident Advisory capability), the first large scale DDoS attack incident was occurred in 1999. After that in February 2000, DDoS flooding attack hit Yahoo, eBay, Amazon.com, ZDnet, Buy.com, the FBI, E-Trade and many other web sites. In this section some DDoS attack incidents are discussed in detail.

A. Wordpress Attack:

Wordpress is Content Management system hosting approximate 18 million websites. In earlier 2014 approximate 162,000 Wordpress sites were targeted by DDoS attack [13]. This attack was entirely based on Wordpress pingback function and uses 50,000 pingback requests per second. This attack resulted in hours of unavailability of Wordpress site. Wordpress support XMLRPC function for remote procedure calls. Attacker on Wordpress abuses a function Pingback in it. Pingback function provides an opportunity for attackers to use Wordpress sites for DDoS attack. Pingback requests were sent as HTTP POST requests to xmlrpc.php page. This pingback function notifies the website owner when their article or post is linked by other web site. Attackers abuse these pingbacks requests to redirect the response to the targeted host. Many pingback requests could be generated to exhaust the number of connections available or bandwidth available at targeted site. Attacker uses XMRPC system.multicall method for guessing passwords of wordpress admin page wp-login.php.

Guidelines: One simple method to stop XML-RPC attack is disabling pingbacks and if possible XML-RPC functionality also, on your website. Adding a plug-in filter can also help in limiting the effect of attack.

B. DNS Server Attack (2015):

On November 2015, DNS Root servers hit by a massive DDoS attack. Each DNS root name server was flooded with 5 million queries/second [14]. This attack resulted in congestion near the DNS server, timeouts for valid, normal queries to some DNS root name servers (B, C, G, and H). For attacking attacker's uses various methods in query for

example a word "ANY" is used by attacker in its query request to expose all the available information about DNS. On December 2015 DDoS attack against DNS servers in Turkey [15] was noticed. This attack was a massive cyber attacks due to which 400,000 websites being forced offline.

Guidelines: DNS attack queries seems like normal query so finding indication of attack signature is a difficult task, to identify DNS Reflection Attack existence, investigate network logs for abnormal queries. Use Firewalls; disable DNS recursion to mitigate the effect of attack.

C. Estonia (2007):

Estonia (capital is Tallinn) the most wired and advance country in Europe in terms of e-Government becomes a target of Cyber attack from 27 April to 11 March 2007. Primary target of these attacks was availability and functionality of services of Estonian government infrastructure. Attack on Estonia has two phases: In the initial phase, Windows command shell scripts was published on Russian language web forms along with execution request. Execution of these scripts causes high web traffic on network increases from 100 to 1000 times leads to successful DDoS attacks. The second phase attack relied on Botnet, which are used as the main vehicle and platform for cyber-crime today. According Jose Nazario technical analysis of data collected by ATLAS2, Web sites affected by DoS attack in Estonia includes valitsus.ee, the Prime Minister (peaminister.ee), the Ministry of Economic Affairs and Communication (mkm.ee), the Ministry of Internal Affairs (sisemin.gov.ee), the Ministry of Foreign Affairs (vm.ee), and the Estonian Parliament (riigikogu.ee) etc. This attack causes web defacement, unavailability of financial or governmental web sites.

Solution adopted: Blocking of all Russian domain (.ru). Advance filters were implemented to filter attack traffic, like Cisco guard to limit the traffic rate.

D. Boston Children's Hospital (Bch):

In 2014 [16] DDoS attacks first time targeted a health care organization, Boston Children's Hospital. This attack started from slow rate packet and lasted at TCP, UDP floods with XSS, SQL injection attacks. Attack rate peaked at 28 Gbps approximately. Attackers used "spear phishing" emails to get access hospitals network. Attack on BCH is a clear indication that it is impossible to predict the next target of attack.

Guidelines: Health care organizations stores critical information about patients. So proper defense measures are required to protect these organizations. Always be prepared for any suspicious event. DDoS solution providers can be contacted; filters can be implemented for complete defense.

E. Github Ddos Attack:

This attack was HTTP based refection attack. A malicious JavaScript code was injected on web pages of China's Internet [17]. When users are trying to access China web pages, HTTP traffic will be directed to the GitHub website.

Guidelines: Predicting the next target of DDoS attack is impossible so company should have a strong plan for surviving in attack condition. Monitoring the network traffic for malware or any suspicious activity should be the first step; for this network monitoring tools can be used for this.

VI. EXISTING DDOS ATTACK DEFENSE MESURES

There is no standard technique to mitigate and prevent all types DDoS of attacks. DDoS attacks are more complex and harder to prevent due to its several unique features such as:

- The attack traffic come from many sources and can be geographically distributed. So it is difficult to trace original attack source.
- Attack traffic looks like genuine traffic so it is hard to filter attack traffic. DDoS attack traffic can look similar to flash crowd (when many genuine users access resources at same time).
- Attacker can use IP spoofing to hide their identity, finding the true origin of attack is a difficult task.

Various approaches were proposed in literature to overcome these challenges and to reduce the impact of DDoS attack. DDoS defense measures can be deployed at Sources end for example Filtering or D-WARD, at Destination end for example IP traceback or at network level such as router based filtering and Aggregate-based Congestion Control. All these defense measures are discussed below:

A. Filtering Measures:

P.Ferguson and D.Senie uses ingress/egress filtering techniques to detect the attack traffic having spoofed source IP addresses. Due to these spoofed addresses victims can not differentiate between attack packets and real ones. Ingress/Egress filtering detects and filter spoofed IP addresses based on valid IP address range in any network. This approach greatly reduces attack power but limitation is processing overhead and requirement of installing filters on all routers [18]. Park et al. [19] analyzed the effectiveness of route-based packet filtering in preventing source IP spoofing. They analyzed an idealized version of route-based packet filtering that is every router has the global information of how the other routers choose routes, and then discards packets that do not follow legitimate routes according to the source and destination addresses in the packets. Strict Reverse Path Forwarding [20] can be considered as an enhanced version of Ingress Filtering.

Effectiveness against DoS and DDoS Attacks: Filtering reduces the impact of DDoS attack at some extent, but universal deployment of filters is a difficult task.

B. Traceback Method:

Trace back in DDoS defense is finding the real origin/source of attack by tracing the path through upstream routers so that attack can be mitigated. PPM (Probabilistic packet marking) scheme which uses assumes that attack packets come more frequently than other packets [21] are used to find the real identity of attack source. In this packet marking scheme each router through which data packet pass probabilistically attach its IP address in packets; this attached information is used for reconstruction of paths. PPM scheme is purposed called DPM (deterministic packet marking) which marks all the packets at ingress interfaces. In deterministic packet marking [22] scheme most of the processing is done at the victim. DPM can work for reflector DDoS which was the limitation of PPM scheme.

Effectiveness: The attack traffic route may be of any length, the process of obtaining the log files may be difficult. IP spoofing and the stateless nature of IP routing make tracing a difficult task.

C. Aggregate-Based Congestion Control:

Mahajan et al. purposed a method Aggregate-based Congestion Control (ACC) [23]; where an aggregate (signature) is defined as a subset the traffic with some identifiable property. For example, "of packets to destination M," "TCP SYN packets," or "IP packets with a bad checksum" all are descriptions of aggregates. This method identifies aggregates responsible for congestion on the network and drops them at the routers. Pushback [24] is an extended version of method Aggregate-based Congestion Control (ACC). Pushback identifies attack packets and drops them immediately and notifies the upstream routers about the attack information. Rate limiting request is sent to upstream router with a Rate-Limiting Session Identifier (RLS-ID) included with each request, which is used to match responses of the requests.

D. Intrusion Detection System:

Intrusion Detection Systems (IDS) monitor the network traffic for known attack signatures. IDS observe the incoming traffic for logging attack signatures and make statistic from it; these systems are known as knowledge-based systems for example CISCO IOS NetFlow [25]. Data mining is another major area used for attack detection attacks based on mining the traffic features and behavior for similarity and dissimilarity. Minnesota Intrusion Detection System (MINDS) [26] uses clusters to find outliers that violate from normal connection behavior. It also addresses insider attacks. SNORT is an IDS based on signature analysis to detect known attacks. B.S Kiruthika Devi et. al. [27] Purposed a model based on Hop count filtering to detect DDoS attack having capability to detect IP spoofing also. In this HCF based method SVM classifier is used to identify which one traffic is legitimate or which one is attack. SVM vector machine is trained to learnt and build a normal traffic profile for the inspection of the attack traffic.

Problem with IDS: Flooding and logic DoS attacks can be used against IDS to prevent it from collecting information.IDS are also useless if attack traffic look like legitimate traffic too much.

– Some general solutions for DDoS mitigation

DDoS attacks are rapidly growing in frequency and size. Traditional solutions like firewall, IDS, Filtering techniques are not sufficient to handle this rate of traffic. Some general solutions for DDoS attacks are:

1) Successful mitigation of DoS attacks require regular monitoring of network traffic for identifying and mitigating attack signatures. For this centralized network traffic monitors having ability to detect and drop unwanted traffic should be deployed.
2) Organizations should have scalability and flexibility features in there infrastructure to survive under attack conditions.
3) It is necessary to monitor normal application requests behavior with its usage, patterns for addressing and configuring security issues.
4) There are many DDoS solution provider organizations that help in DDoS mitigation. They offer several solutions for redirecting and filtering attack traffic such as Border Gateway Protocol for filtering the outbound traffic.
5) Contact to ISP for monitoring your network services activity to detect & mitigate DDoS attack before reaching to your network services.
6) Use network traffic monitoring tools for example NetFlow, Wireshark and update security patches regularly for identifying and detecting the latest versions of attacks.

VII. Conclusion

Over the last few decades, DDoS is a growing security issue. These attacks have grown in frequency and size of up to 400 Gbps. Due to the fact that usage and vulnerabilities of Web application are increasing rapidly; availability of web services becomes a major issue of concern. DDoS attacks target availability of web services by crashing or overloading of web servers. Results of these attacks can vary from minor inconvenience of users to major revenue, reputation losses in bigger organizations. These attacks are easy to perform and do not need much knowledge of application vulnerabilities, easy to use tools are available online at free of cost. The period of DDoS attacks can vary from minutes to hours, but this is enough to mete out a lot of damage at the target site. Currently UNIX servers zombie attacks, Botnet attacks, application based attacks, reflection attack with amplification techniques are gaining popularity day by day. Amplification or reflection based attacks by using DNS or NTP servers, SSDP protocol are the trendiest attacks today. These methods amplify the attack traffic by a factor of 50-100 times. Botnet are used to conduct these volumetric attacks. Motive of these DDoS attacks are political reasons, malicious competition, extortion, and economic crimes.

In this paper study of some DoS attack incidents such as attack against Estonia, Wordpress, BCH, DNS servers is carried out to analyze the modus operandi of attackers and to examine the effectiveness of existing defense measures. An exhaustive analysis of DDoS attack methods is carried out and a set of guidelines are provided with each discussed attack vector so that a framework may be designed to make the application full proof against such attacks.

References

[1] "GLOBAL APPLICATION & NETWORK SECURITY REPORT," 2015-2016.
[2] V. Moore, "Inferring Internet Denial of Service activity," ACM Trans. Comput. Syst., pp. 115-139, May 2006.
[3] "Incapsula," [Online]. Available: www.incapsula.com/blog/know-your-top-10-bots.html. [Accessed may 2016].
[4] M. Aamir, "DDoS Attack and Defense: Review of Some Traditional and current techniques," January 2014..
[5] "Imperva, Incapsula," [Online]. Available: https://www.incapsula.com/ddos/attack-glossary/ntp-amplification.html. [Accessed 9 June 2016].
[6] "NTP Amplification Attacks Using CVE-2013-5211," US-CERT, 2014. [Online]. Available: www.us-cert-gov/ncas/alerts/TA14-013A.html. [Accessed April 2016].
[7] US-CERT, march 2013. [Online]. Available: www.us-cert.gov/ncas/alerts/TA13-088A.html. [Accessed 2016].
[8] "DNSSEC Targeted in DNS Reflection Amplification DDoS Attacks," [Online]. Available:

www.blogs.akamai.com/2016/02/dnnssec-targeted-in-dns-reflection-amplification-ddos-attacksduring-the-past-few-quarters-akamai-has-.html. [Accessed 2 june 2016].
[9] "start chargenampattack looking at chargen protocol denial of service attacks," Posh Security, [Online]. Available: www.poshsecurity.com/blog/2014/5/28start-chargenampattack-looking-at-chargen-protocol-denial-of.html.
[10] Computer World, [Online]. Available: www.computerworld.com/article/2474293/malware-vulnerabilities/unplug-universal-plug-and-play--about-50-million.html.
[11] "MC SQLR Amplification: MC SQL Server Resolution Service enables reflected DDoS with 440x amplification," [Online]. Available: www.kurtaubuchon.blogspot.in/2015/01/mc-sqlr-amplification-ms-sqlserver.html.
[12] "common-ddos-attack-tools," Radware, [Online]. Available: https://security.radware.com/ddos-knowledge-center/ddos-attack-types/common-ddos-attack-tools/.
[13] Sucuri, [Online]. Available: www.blog.sucuri.net.
[14] [Online]. Available: www.root-servers.org/news/events-of.html.
[15] "Turkey DNS server Under Attack," Radware, [Online]. Available: www.blog.radware.com/security/2015/12/turkey-dns-server-under-attack.html.
[16] "DDoS case study: DDoS Attack Mitigation Boston Children's Hospital," Radware, [Online]. Available: www.security.radware.com/ddos-experts-insider/ert-case-studies/.
[17] "China's Man-on-the-side Attack on Github," [Online]. Available: www.netresec.com.
[18] P. F. a. D. Senie, "Network ingress filtering: defeating denial of service attacks that employ IP source address spoofing," 2000.
[19] K. Park and H. Lee, "On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets," ACM SIG-COMM, 2001.
[20] F. Baker and P. Savola, "Ingress Filtering for Multihomed Networks," 2004.
[21] S. Subhashini, "Tracing Sources of DDoS Attacks in IP Networks Using Machine Learning Automatic Defence System," International Journal of Electronics Communication and Computer Engineering, vol. 3, no. 1, pp. 164-169, January 2012.
[22] B. Ansari, "IP Traceback With Deterministic Packet Marking," IEEE, vol. 7, no. 4, pp. 162-164, APRIL 2003.
[23] R. Mahajan, S. M. Bellovin and S. Floyd, "Aggregate-Based Congestion Control".ICSI Center for Internet Research (ICIR) AT&T Labs – Research.
[24] J. Ioannidis and S. M. Bellovin, "Implementing Pushback: Router-Based Defense Against DDoS Attacks".
[25] "CISCO IOS NetFlow," CISCO, 2006. [Online]. Available:http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html..
[26] L. Ertoz. [Online]. Available: http://www-users.cs.umn.edu/~kumar/papers/minds_chapter.pdf. [Accessed 5 5 2016].
[27] G. P. Preetha, K. S. Drvi and S. M. Sha, "Autonomous Agent for DDoS Attack Detection and Defense in an Experimental Testbed," International Journal of Fuzzy Systems, vol. 16, no. 4, 2014.
[28] "ddos-attacks," [Online]. Available: https://www.incapsula.com/ddos/ddos-attacks/.

