IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 6, Ver. IV (Nov – Dec. 2014), PP 24-33
www.iosrjournals.org

Impact Analysis of Dos & DDos Attacks

[1.]Mrs.S.Thilagavathi, [2.]Dr.A.Saradha
[1]*Head, Department of Computer Science, Terf's Academy College of Arts Science*
Tirupur, Tamilnadu, India
[2]*Head, Department of Computer Science & Engineering,*
Institute of Road and Transport Technology Erode, Tamilnadu, India

Abstract: *Denial of Service attacks constitutes one of the major threats, which poses immense threats to the Internet. In the present Internet has changed the way of traditional essential services such as banking, transportation and defense being operated. These operations are being replaced by cheaper, more efficient Internet-based applications. It is all because of rapid growth and success of Internet in every sector. Unfortunately with the growth of Internet, count of attacks on Internet has also increased incredibly fast. The researchers have to find details of these type of attacks because due to avoid the damaging reputation issues, In this paper, an overview of Denial-of-Service(DoS)&Distributed denial-of-service (DDOS) attacks are provided. Real distributed denial-of-service incidents with their financial impact are analyzed and finally DOS and DDOS solution is highlighted.*

Key words: *Denial-of-service, Distributed denial-of-service, incidents of DDoS attack, DDoS Defense*

I. Introduction

The main aim of the internet is to provide an inexpensive communication mechanism and it accomplishing the successful goal. A DoS attack is not a traditional crack in which the attacker is to gain unauthorized privileged access, but it can be just as malicious. The target of DOS attack is inconvenience and these types of attacks are easy to launch. Denial of service is about without permission of service knocking off service. This article describe a DoS impact metric that speaks to the heart of the problem. It measure if the legitimate client receive acceptable service. DDOS attacks are difficult to stop because they can be coming from anywhere in the world[5][15].

This paper presents an overview of the DoS problem in section 2 and it includes Dos and DDOS of DoS attacks and how they are accomplished in section 3. In section 4 Automated attack tools and in section Section 5 various Recent DDoS incidents are outlined. In section 6 DDoS Defence are briefed, Section 7 DDoS impacts are explained. In section 8 Comparative analysis are explained and in section 8 Testing approaches are described finally section 9 concludes the paper.

II. Overview of Attack Methodology

The goal of the DDoS attacks is to degrade or even disable the service(s) provided by the target.. A denial-of-service attack can be realized in either two techniques:

- exploiting the vulnerability in network protocols and software; and
- Leveraging high volume of address-spoofing, bogus traffic.

These two kinds of attacks are usually mixed together in order to bring about a large amount of damage [6].

2.1 Vulnerability-based attack

This kind of attack leverages the flaws in protocol designs and the defects in software. Once such vulnerabilities are exploited, the service provided by the victim will be shut or degraded.

2.1.1. ICMP Flood

Smurf attack is one specific form of a flooding DoS attack that occurs on the public Internet. In order to fight against Denial of Service attacks on the Internet, there are services such as the Smurf Amplifier Registry that have given the ability to the internet service providers to identify the networks with incorrect configuration and also to take the right action like filtering.

Ping flood is a method that relies on sending a large number of ping packets to the victim, and this is done by using the "ping" command from unix-like hosts Launching it is quite simple, as it requires access to more bandwidth than the victim. Ping of death is another method that is based on sending a malformed ping packet to the victim, as a result of which the system can crash

2.1.2. SYN flood

SYN flood is a result of TCP/SYN packets flooding sent by host, mostly with a fake address of the sender. The handling of these packets is done in the same manner like connection request, which makes the server to produce a semi-open connection, as it sends TCP/SYN-ACK packet back (Approve/Acknowledge), and waits for a packet to be received as a response from the address of a sender (ACK Packet's response). Actually the sender never responds as his address is not real. The saturation of available connections takes place by the semi-open connections that the server can actually make, so that it cannot respond to legal requests even after the attack is over.

2.1.3 Teardrop attacks

In case of a Teardrop attack the injured IP fragments are sent to the target machine with expanded, overlapping, payloads. As there is a bug in the TCP/IP fragmentation re-assembly code so this can result in crashing different operating systems.

2.1.4 Low-rate Denial-of-Service attacks

The Low-rate DoS (LDoS) this type of attack actually exploits the TCP's slow-time-scale dynamics of retransmission time-out (RTO) mechanisms so that it reduces TCP's output. Attacker can make the repeated entry of a TCP flow to a RTO state as the attacker can send the bursts at high-rate within short-duration, and this can be repeated periodically at slower retransmission time-out time-scales. This results in reduced output of TCP.

2.2 Flood-based attack

Flooding is a Denial of Service (DoS) attack that is designed to bring a network or service down by flooding it with large amounts of traffic. Flood attacks occur when a network or service becomes so weighed down with packets initiating incomplete connection requests that it can no longer process genuine connection requests. By flooding a server or host with connections that cannot be completed, the flood attack eventually fills the host memory buffer. Once this buffer is full no further connections can be made, and the result is a Denial of Service.

2.3 Zombie attack

A computer that has been implanted with a daemon that puts it under the control of a malicious hacker without the knowledge of the computer owner. Zombies are used by malicious hackers to launch DoS attacks. The hacker sends commands to the zombie through an open port. On command, the zombie computer sends an enormous amount of packets of useless information to a targeted Web site in order to clog the site's routers and keep legitimate users from gaining access to the site. The traffic sent to the Web site is confusing and therefore the computer receiving the data spends time and resources trying to understand the influx of data that has been transmitted by the zombies. Compared to programs such as viruses or worms that can eradicate or steal information, zombies are relatively benign as they temporarily cripple Web sites by flooding them with information and do not compromise the site's data. Zombies are also referred to as zombie ants.

2.4 Reflector attack

The reflector attack is, therefore, by its nature, more detrimental than using the zombie attack model alone because:

- It amplifies the effect of the DDoS attack. Let us imagine that the attacker has only one zombie. By sending spoofed packets to different reflectors, one zombie is already enough to attack the victim in a distributed way;
- It also degrades the services provided by the reflectors. During the reflector attack, the reflectors are loaded by the requests from the zombies, and this degrades the services provided by the reflectors.

2.5 Peer-to-peer attack

While peer-to-peer attacks are easy to identify with signatures, the large number were of IP addresses that need to be blocked (often over 250,000 during the course of a large-scale attack) means that this type of attack can overwhelm mitigation defenses. Even if a mitigation device can keep blocking IP addresses, there are other problems to consider. For instance, there is a brief moment where the connection is opened on the server side before the signature itself comes through. Only once the connection is opened to the server can the identifying signature be sent and detected, and the connection torn down. Even tearing down connections takes server resources and can harm the server.

This method of attack can be prevented by specifying in the peer-to-peer protocol which ports are allowed or not. If port 80 is not allowed, the possibilities for attack on websites can be very limited[7].

2.6 Worm attack

The worm attack is another form of automatic attack tool. To define, a worm is a piece of software that runs on a computer, and the computer is unwillingly having the worm running. The worm has the ability to duplicate itself, and has the duplicated copies infect other computers. Many worms that have been created are designed only to spread, and do not attempt to change the systems they pass through. However, even these "payload free" worms can cause major disruption by increasing network traffic and other unintended effects. A "payload" is code in the worm designed to do more than spread the worm it might delete files on a host encrypt files in a crypto viral extortion attack, or send documents via e-mail. A very common payload for worms is to install a backdoor in the infected computer to allow the creation of a "zombie" computer under control of the worm author[8][9][15].

III. DoS and DDOS Overview

Denial of service is an attack which makes an information or data unavailable to its intended hosts. There are various methods to carry out this attack and the strategies are explained in the following section. However, there is also other way of making service unavailable rather than just dumping it with abundant IP packet. The victim could also be attacked at various loopholes making it unstable which depends on the nature of the attack

There are also attacks that could be carried out at application level, hindering the normal functioning of service. There are attack that are designed to crash a web browser, email application or even a media player. When a specific application is disrupted and when normal functioning is hindered, it is called Application level denial of service.

Distributed and denial of service has the cohesive strength of many compromised systems working towards a single cause. The first stage of this attack is to build its platform with many host systems that can work under remote commands. The to combat with DDoS that are weak in security features. According to researchers there are millions of host machines that are vulnerable without secure patches and proper updates that often fall victim to these attackers. Once the scanning procedure is completed, attackers would bring these hosts into control using software exploitation like buffer over flow, dangling pointer, code injection etc. Special root kits are also use in many cases that are installed in a host system to incur these software exploitation. After having sufficient hosts under control, attackers also create backdoors that allows special access that is used for future entry. The attackers also update the host and tighten its security so that another attacker does not use the same host. Any future entry would be done using the back entry that has been specially crafted[2][14][18].

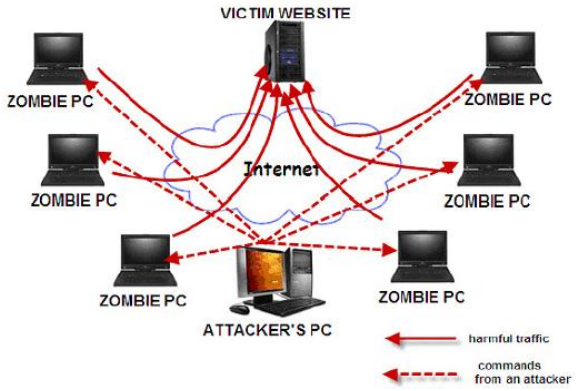

Figure 1.Defending against DDOS attacks

IV. Automatic attack tools

Several well-known DDoS attack tools adopt the above attack architectures. These tools are designed to be versatile so that they can mount different types of attack payloads to the zombies. Several famous tools include the Tribe Flood Network 2000 (TFN2K for short), the Trinoo and the Stacheldraht. These automatic attack tools are well designed and are effective in launching DDoS attacks [12].

V. DDOS Incidents of Important Websites

There are many occurrences that have been happening since the last ten years and there is still no effective control for this attack. One of the most talked about attack happened in the year 2000, February 7 when yahoo serves were crashed. The famous internet site was unavailable for several hours which affected the business of yahoo considerably. Buy .com, e-bay and CNN were the other giant companies that were attacked,

the very next day after yahoo. E-bay is an online bank that undertakes millions of transaction online. The site was completely inaccessible which incurred huge loss to the company.

- **Nov 1988 -** the Morris worm, written by Cornell CS grad student Robert Morris, was the very first significant DoS attack. Morris put roughly 5000 machines out of commission for several hours.
- **Mar 1998** - Attackers exploited a problem with Windows NT servers, and successfully drove thousands of NT stations, including ones at NASA, MIT, the U.S. Navy, and UC Berkeley, offline. This DoS attack led to the formation of the FBI's Infrastructure Protection and Computer Intrusion Squad, better known as the Power Rangers.
- **Feb 2000** - DDoS attack caused shutdown of Yahoo, eBay and Amazon for a few hours.
- **Jan 2001** - First major attack involving DNS servers as reflectors. The target was Register.com.
- **Feb 2001** - The Irish Government's Department of Finance server was hit by a denial of service attack carried out as part of a student campaign from NUI Maynooth.
- **May 2001** - Worm Code Red was supposed to attack White House website.
- **Oct 2002** - Attackers performed DNS Backbone DDoS Attacks on the DNS root servers and disrupted service at 9 of the 13 root servers. **Aug 2003** - Worm Blaster attacks Microsoft web pages.
- **Jan 2004** - MyDoom attacked 1 million computers.
- **Feb 2007** - Attackers performed a second set of DNS Backbone DDoS Attacks on the DNS root servers and caused disruptions at two of the root servers.
- **April-May 2007** - A spree of denial-of-service attacks against Estonia's prime minister, banks, and less-trafficked sites run by small schools. (http://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack)
- **July 2008** — A DDoS attack directed at Georgian government sites containing the message: "win+love+in+Rusia" [sic] effectively overloaded and shut down multiple Georgian servers. Websites targeted included the Web site of the Georgian president, Mikhail Saakashvili, rendered inoperable for 24 hours, and the National Bank of Georgia.
- **Mar - Apr 1, 2009** - Cloud computing provider GoGrid is hit by a "large, distributed DDoS attack," which disrupts service to about half of its 1,000 customers."
- **Mar 31, 2009** - A DDoS attack knocks UltraDNS offline for several hours.
- **April 2-5, 2009** - Domain registrar Register.com is hit with a DDoS that causes several days of disruptions for its customers.
- **Apr 6-7, 2009** - Customers of The Planet are hit by web site outages as a result of a DDoS aimed at the huge hosting company.
- **June 2009** - The famous P2P site known as The Pirate Bay was rendered inaccessible due to a DDoS attack.
- **June 2009** - Iranian election protests, foreign activists seeking to help the opposition engaged in DDoS attacks against Iran's government. The official website of the Iranian government was rendered inaccessible on several occasions. Critics claimed that the DDoS attacks also cut off Internet access for protesters inside Iran; activists countered that, while this may have been true, the attacks still hindered President Mahmud Ahmadinejad's government enough to aid the opposition.
- **July 2009** - Multiple waves of cyber attacks targeted a number of major websites in South Korea and the United States: the White House, Department of Transportation, Federal Trade Commission, and the Department of the Treasury. Hit at the same time were the Washington Post and the New York Stock Exchange. The attacker used botnet and file update through Internet is known to assist its spread. Investigation is still underway. (http://www.computerworld.com/s/article/9135274/Online_attack_hits_US_government_Web_sites)
- **Aug 6, 2009** - Several social networking sites, including Twitter, Facebook, Livejournal, and Google blogging pages were hit by DDoS attacks, Although Google came through with only minor set-backs, these attacks left Twitter crippled for hours and Facebook did eventually restore service although some users still experienced trouble.
- **Dec 23, 2009** DNS service provider Neustar Amazon, Wal-mart, and Expedia were affected. 60 min of outage.[1][2][4]
- **Feb 2010** Australian Parliament House website (www.aph.gov.au) Attack was the part of the protest by a group. 50 min of outage
- **Apr 2010** Optus Sourced from china. 4 hours of outage.
- **May 2010** Botnet consisting of web server was discovered Rrather than individual PCs, server were being used. An attackers named "Exeman" has infected around 400 web server with simple 40-line PHP script.
- **May 2010** Vocus Caused connectivity disruption across multiple web site. 80 min of disruption.
- **May 2010** Web24 Caused Connection issues for user of the vocus network More than 12 hours of outage.

- **June 2010** UK-based Jewish Chronicle Website had to shut down its balanced coverage of the "Ashdod flotilla incident" immediately.
- **July and Aug, 2010** Irish Center Application Office server Attack was hit on four different occasions
- **Sep 2010** Fast growing botnet "IMDDOS" was discovered Botnet's motive was to provide commercial service for launching DDOS attacks against any target.
- **Oct 2010** MPPA & Indian tech firm Aiplex software Atleast hundred of 4chan user at once executed attack in Pro-piracy protest. Simple application Low Orbit Ion Cannon (LOIC) was used.
- **Nov 2, 2010** Burma's MAIN Internet provider Disrupted most network traffic in and out of the country for 2 days. Geo political motivated attack. Attack size was 1.09 Gbps (average) & 14.58 Gbps (maximum). Attack vector were TCP Syn/rst 85%, flooding 15%.
- **Nov 12, 2010** domain registrar Register.com Impacted DNS, hosting and webmail client. 24 hours of outage.
- **Nov 28, 2010** whistle blower site Wiki Leaks Attack size was 2-4 Gbps. Attack was launched just after it released confidential US diplomatic cables.
- **Nov 30, 2010** whistleblower site Wiki Leaks Attack size was 10 Gbps. Caused the site unavailable to visitors. Attack was launched to prevent release of secret cables.
- **Dec 8, 2010** MasterCard, PayPal, Visa. And Post Finance Attack was launched in support of WickiLeaks.ch and its founder. Attacks last for more than 16 hour.
- **March 30, 2011** On Blogging Platform Live Journal Experienced serious functionality problems for over 12 Hours and resumed on April 4 and 5, 2011. [3]
- **On Feb 11, 2014** A massive DDoS attack hit EU- and US-based servers, with security companies reporting it to be even more powerful than last year's Spamhaus attacks. While the method of the attack was not new CloudFlare warned there are "ugly things to come." Only scant details about the attack were released by US-based web performance and security firm CloudFlare, which fought back against the distributed denial of service (DDoS) attack early Tuesday. According to CloudFlare CEO Matthew Prince, the attack reached 400 gigabits per second in power – some 100Gbps higher than the notorious Spamhaus cyber-assault of March 2013 that at the time was branded the largest-ever attack in the history of the internet.
- **On May 16, 2014** A massive DNS distributed denial-of-service (DDoS) attack was reported by US security firm Incapsula on one of its clients. This attack came, ironically, from the servers of two providers of anti-DDoS services. The attack originated from servers in China and Canada being targeted against the network of an online gaming firm[15][16][17].

VI. DDoS Defense

There are four approaches to combat with DDoS: Prevention, Detection and Characterization, Trace back and Tolerance and Mitigation. Attack prevention aims to fix security holes, such as insecure protocols, weak authentication schemes and vulnerable computer systems, which can be used **as** stepping stones to launch a DoS attack. Attack detection aim to detect DDOS attacks in the process of an attack and characterization helps to discriminate attack traffic from legitimate traffic. Traceback aims to locate the attack source regardless of the spoofed source IP addresses in either process of attack (active) or after the attack (passive). Tolerance and mitigation aims to eliminate or curtail the affect of an attack and try to maximum the Quality of service (QOS) under attack[1][2].As DDOS is a distributed attack and because of high volume and rate of attack packets distributed instead of centralized defense is the first principle of DDOS defense.

The results and losses due to DDoS attacks are disastrous and unimaginable, therefore it is really important some approaches to defend these attacks. Researchers have been evaluated these defense systems by approaches of Theory and Simulation[2][9][13].

VII. DDOS Impact

The impact of DoS attacks can vary from minor inconvenience to use of a website, to serious financial losses for companies that rely on their on-line availability to do business. DoS attacks generally occur basically in improper system design, insufficient resource. It measure if the legitimate client's receive acceptance service or not during attack. Many solutions have been proposed to require the source networks together with victims[2].

The user must not feel threatened by the system, instead must accept it as a necessity one. In these days, all are equipped with system knowledge and so anybody can access the application easily with less effort. The Proposed system accessing process to solves problems what occurred in existing system. The current day-to-day operations of the organization can be fit into this system. Mainly operational feasibility should include on analysis of how the proposed system will affects the organizational structures and procedures.

The System administrators can use, control and protect the applications on computers in a network or stand alone computer. It describes the system has to be without going to access in the conventional place in the Operating System. Another issue that all-in-one options have with their upgradeability. While most desktop computer cases can be easily opened to upgrade in the System controller. This typically only limits the systems to having their memory upgraded.

The metric are capturing the Unauthorized IP Address who enters into a server. If it identifying the Spam IP and discard them before reaching the victim. The proposed system measure the resource overloading problem. The resource can be bandwidth, memory, cpu performance, File descriptors and buffers etc.,The server resources such as processing capacity, buffer limit are put under the stress by flood of legitimate request generated by DDoS attack zombies. Each request consumes some CPU performance. Once the total request rate is more than the service rate of server the request getting buffered in the server so the incoming requests are dropped because of buffer overflow. The legitimate clients to decrease their rate of sending requests. Thus the service is denied to legitimate clients, filtering traffic of malicious flows become a burden at the target[16][17].

VIII. Comparative Analysis

Collection of Methods techniques is depicted in Table 1 and the definition of the terms used. The comparison of proposed and Existing techniques (some of the techniques) is discussed below.

Attack	Countermeasure Options	Example	Description
Network Level Device	Software patches, packet filtering	Ingress and Egress Filtering	Software upgrades can fix known bugs and packet filtering can prevent attacking traffic from entering a network.
OS Level	SYN Cookies, drop backlog connections, shorten timeout time	SYN Cookies	Shortening the backlog time and dropping backlog connections will free up resources. SYN cookies proactively prevent attacks.
Application Level Attacks	Intrusion Detection System	Guard Dog, other vendors.	Software used to detect illicit activity.
Data Flood (Amplification, Oscillation, Simple Flooding)	Replication and Load Balancing	Akami/Digital Island provide content distribution.	Extend the volume of content under attack makes it more complicated and harder for attackers to identify services to attack and accomplish complete attacks.
Protocol Feature Attacks	Extend protocols to support security.	ITEF standard for itrace, DNSSEC	Trace source/destination packets by a means other than the IP address (blocks against IP address spoofing). DNSSEC would provide authorization and authentication on DNS information.

The Internet Protocol (IP) was designed to support ease of attachment of hosts to networks, and provides little support for verifying the contents of IP packet header fields.

This makes it possible to fake the source address of packets, and hence difficult to identify the source of traffic. Moreover, there is no inherent support in the IP layer to check whether a source is authorized to access a service. Packets are delivered to their destination, and the server at the destination must decide whether to accept and service these packets. The existing problem can be overcome by implementing the local flow monitoring algorithm and the IP trackback algorithm.

The proposed system is to accomplish a denial of service state on systems, flood attacks aim to push limits of system usage to the out of boundaries determined by the normal usage scenarios. There may be a flood attack between the considered normal network traffic and the considered abnormal network traffic. The flood attack name can be determined by the specific protocol that attack is made on. For example, a flood attack on the DNS protocol is called as DNS Flood Attack while a flood attack on the HTTP protocol is called as HTTP Flood Attack. Since every protocol has its own technical architecture and vulnerabilities, flood attacks can differ on the attacking techniques from protocol to protocol.

The main reason of flood attacks is the vulnerability in the protocol. For example, a UDP Flood or SYN Flood attack uses the nature of protocol's design to saturate the network traffic. In a SYN Flood attack, attacker uses the TCP 3 way handshake's first initiation step to spoof IP addresses and to drain server side system/network resources. When the subject comes to the UDP Flood attack, attacker uses the stateless design of the UDP protocol to spoof IP addresses and to drain server side system/network resources. For this reason, to accomplish an effective security solution, every mitigation method for the flood attacks must be implemented in a consideration and perspective of system/protocol design.

There are many situations in the real world scenarios that the HTTP flood attacks are not mitigated properly. Some of them might be related with security configuration weakness of the security device and others might be depending on an absence of a security device. Situations like these might be handled with the other security enhancements at the different level of the information technology architecture. This is where the web application level comes in. Unlike network-layer protection products, an application-layer solution works within the application that it is protecting. Web application is a bunch of technologies which serves for the web service. Before starting a discussion on the web application level approach to the

HTTP flood attacks, it is important to clarify whether the attack I a HTTP flood attack or not. To consider an attack attempt as a HTTP flood attack, a TCP packet which carries a HTTP request payload should be interpreted by the web service. Attack surface for HTTP flood attacks always begins with the web service and its backend infrastructure. A HTTP flood attack attempt, which cannot make it to the web service, is just a TCP DoS attack that saturates the network traffic.

With the proposed system the web application firewall can avoid DoS attacks because it inspects HTTP traffic and checks their packets against rules such as to allow or deny protocols, ports, or IP addresses to stop web applications from being exploited. Architected as plug & play software, The proposed system provides optimal out-of-the-box protection against DoS threats, Cross-site scripting, SQL Injection attacks, Path traversal and many other web attack techniques.

The proposed system have the following comprehensive solutions are

- Easy installation on Apache and IIS servers.
- Strong security against known and emerging hacking attacks.
- Best-of-breed predefined security rules for instant protection.
- Interface and API for managing multiple servers with ease
- Requires no additional hardware, and easily scales with your business.

The proposed system is used to monitor all traffic entering and leaving the network. The user who enters into a server will be monitored by this method.

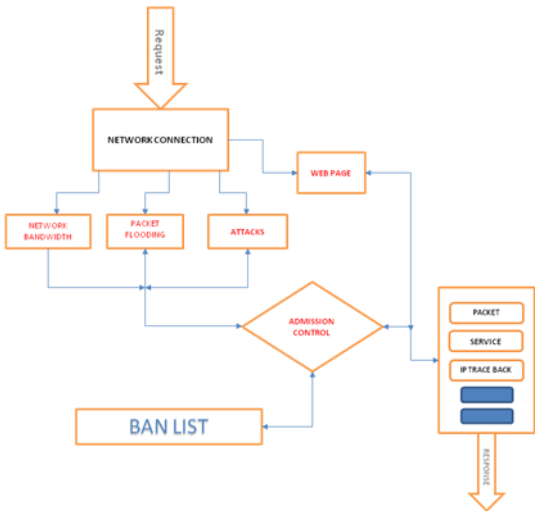

Figure 2: Architecture Diagram for Proposed Method

IX. Testing Approaches

Network simulator (Version2) known as NS2, is very helpful in understanding the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocol can be done using NS2. It provides users with a way of specifying such network protocols and simulating their corresponding behaviors. Due to flexibility and modular nature.Ns2 outputs either text-based or animation-based simulation results. To interpret these results graphically and interactively, tools such as NAM(Network Animator) and Xgraph are used. Ns2 is event simulator where the advance of time depends on the timing of events which are maintained by a scheduler[5].

In the proposed system , Seven nodes have been taken for problem formulation. Node number 0,1,2,and 3 are wired nodes. Node number 4 and 5 are base station nodes. Traffic is moving between these nodes. Node 6 is taken as movable node. Node 6 moves towards the base station nodes and create the unnecessary traffic causing the denial of service attack.

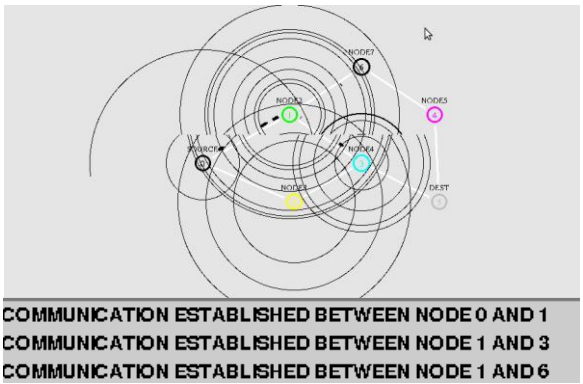

Figure 3 Communications Established between Node 0 to 6

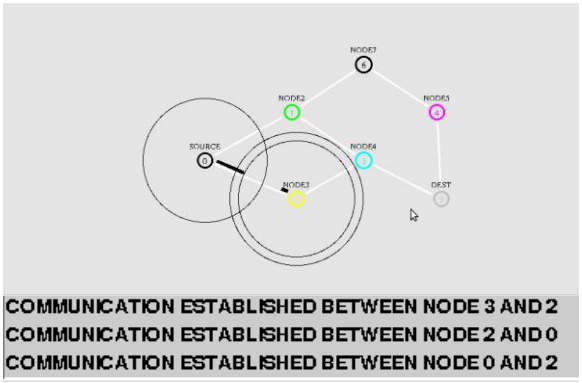

Figure 4 Communications Established between node 0 to 3

----- Lines represents the data to be shared between the nodes

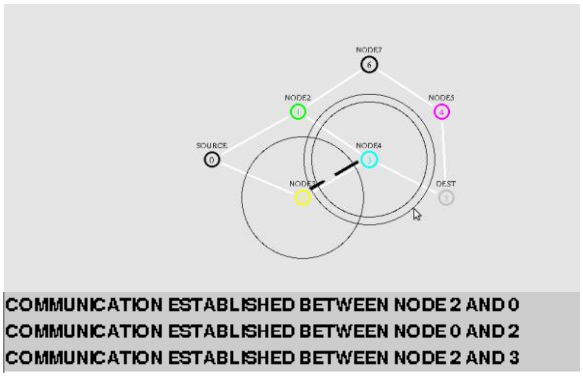

Figure 5

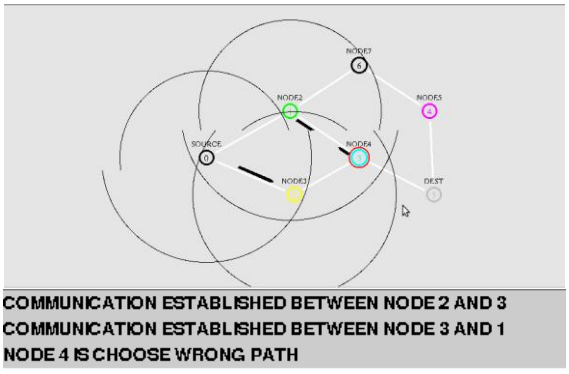

Figure 6

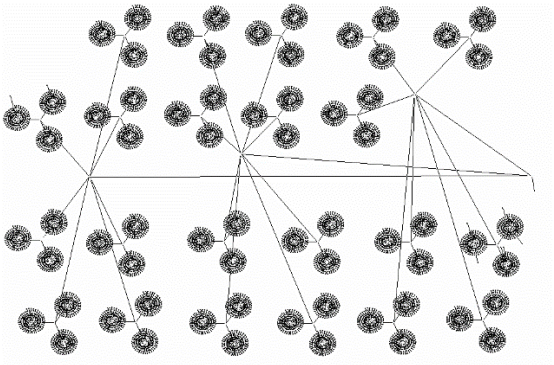

Figure 7 Communications Established between n number of Nodes

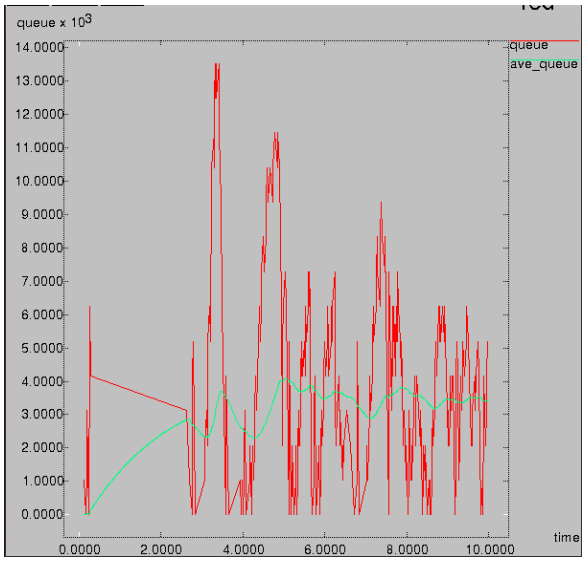

Figure 8 –Graphical Visualization

The above graph is an Graphical Visualization raw or processed data collected in a simulation can be graphed using tools XGRAPH. Red color represents scenario n number of IPs in the queue. Green color represents the scenario number of IPs is in average queue length.

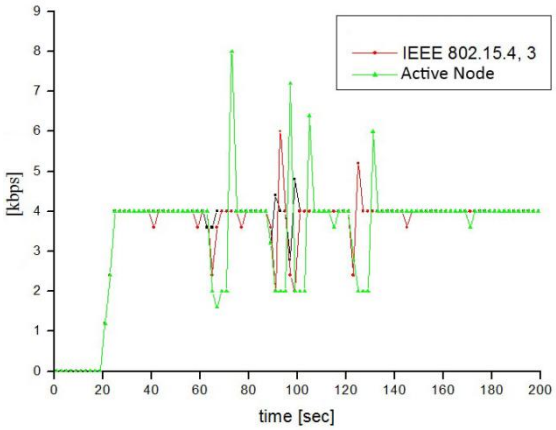

Figure 9 –Graphical Representation

In the above graph dead node and active node is figured. Depending upon the graph the X axis shows the Speed level of the system and Y axis shows the time of the user on it. It reveals when the users comes at a time in many numbers with speed. Red color represents scenario n number of nodes in the queue with WIFI connection. Green color represents the scenario number of nodes in active mode and black color represents number of nodes in dead state which is an blocked node.

X. Conclusions

DoS attack are a serious problem on the internet and their rate of growth and wide acceptance challenge the general public. It is clear that the wave of DoS attacks will continue to pose significant threat.A network infrastructure enough to survive direct DoS attacks. There are number of DDoS attack incidents. Not only DDOs incidents are growing day by day but the technique to attack, btnet size, and attack traffic are also attaining new heights.

The major contribution of this paper are :

- It gives a deep DDoS problem and its orgin.
- It gives overview of DoS and DDoS problem.
- DDoS defence challenges and requirements are explained.
- Choronological information about DDoS incidents are provided
- DDoS incidents on various sites are explored.

References

[1]. Daljeet Kaur , Monika Sachdeva., "Study of Recent DDoS Attacks and Defense Evaluation Approaches", International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459,ISO 9001:2008 Certified Journal, Volume 3, Issue 1, January 2013)

[2]. Monika Sachdev, Guruvinder Singh, Krishnan Kumar And Kuldip Singh.,

[3]. "DDoS Incidents and their Impact :overview", The Internatonal Arab Journal of Information Technology, Vol.7, No.1, January 2010.

[4]. Daljeet Kaur, Monika Sachdeva Department of Computer Science and Engineering, SBS Stat Technical Campus, Ferozepur – 152004, Punjab, India

[5]. Jake Stein, "DoS Attacks Trend Toward Politics".

[6]. Shiva kumar , Ritika singal, priyadharshini , "Mitigate the Impact of DOS Attack by Verifying Packet Structure", "ECE Department LCET Katani, Kalan, India.

[7]. Ketki Arora, Krishan kumar, Monika Sachdev, "Impact Analysis of DDOS Attacks", "International Journal on Computer Science and Engineering(IJCSE).

[8]. Sarika Agarwal, Saumya Agarwal, Bryon Gloden, "DDOS Attack Simulation Monitoring, and Analysis"

[9]. Igino Corona, Giorgia Giancinto, "Detection of Service-Side Web Attacks"

[10]. Jelena Mirkovic, Sonia Fahmy, Peter Reiher, "Measuring Impact of DDOS Attacks".

[11]. Barlow j., "TFN2K: An Analysis," http://packetstormsecurity.org/distributed/TFN2K_Analysis-1.3.txt, 2007.

[12]. Peng, T., Leckie, C., and Ramamohanarao, K.(2007) Survey of network-based defense mechanisms countering DOS and DDOS problems. ACM computing survey,39,3:1-3:42.

[13]. Garg, A., Narasimhma Reddy A.L. "Mitigation of DOS attack through QOS regulation" in Proc. Quality of Service,2002.pp:45-53.

[14]. Li. J, Mirkovic. J, Wang.M, Reiher.P, and Zhang.L "SAVE:source address validity enforcement protocol" in Proc. INFOCOM 2002, Vol.3,pp1557-156.

[15]. J.Howard, and T. Longstaff,"a common language for computer security incident,"[online].Available:www.cert.org/research/taxanomy_988667.pdf.

[16]. M.Robinson, J.Mirkovic,M.Schaider, S.Michel,and P.Reiher, "Challenge and principle of the defense," Computer Journel of ACM SIGCOMM, vol.5,no.2,pp.148-152,2003.

[17]. Damiano Bolzoni and Sandro Etalle. Boosting web intrusion detection system by inferring positive signature. In OTM Conference (2), pages 938-955,2008.

[18]. Monowar H.Bhuyan,H.J.Kashiyap, D.K. Bhattacharya and J.K.Kalita, "Detecting Distributed Denial of Service Attacks :Methods,Tool and Future Directions.