International Journal of Computational Engineering Research||Vol, 04||Issue, 1||

A Survey of Protection Against 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-Services (DoS) attacks cause serious threats to the today internet world. The problem of DoS attacks has become well known, but it has been hard to find out the Denial of Service in the Internet. So the users have to take own effort of a large number of protected system such as Firewall or up-to-date antivirus software. If the system or links are affected from an attack then the legitimate clients may not be able to connect it. There have been a number of solutions and tools to detect the DoS attacks. However there are no end solutions which can protect against the DoS attacks. This paper focuses on techniques used in different DoS attacks and describes the characteristics of tools used in DoS attack network and also presents the proposed solutions.

INDEX TERMS : *Denial-Of-Service, Distributed Dos, DDoS Attack Tools, Traceback Mechanisms, Intrusion Detection and Prevention Method, IP Address Spoofing, IP Address Monitoring, Blocked IP Address, Client-Side Script.*

I. INTRODUCTION

A denial of service (DoS) attack aims to deny access by legitimate users to shared services or resources. This can occur in a wide variety of contexts, from operating systems to network-based services on the Internet. A DoS attack aims to disrupt the service provided by a network or server. On February 9, 2000, Yahoo, eBay, Amazon.com, E*Trade, ZDnet, Buy.com, the FBI, and several other Web sites fell victim to DDoS attacks resulting in substantial damage and inconvenience. More importantly, traditional operations in essential services, such as banking, transportation, power, health, and defense, are being progressively replaced by cheaper, more efficient Internet-based applications. Internet-based attacks can be launched anywhere in the world, and unfortunately any Internet-based service is a potential target for these attacks.This paper presents an overview of the DoS problem in section 2 and it includes classification of DoS attacks and how they are accomplished. In section 3 existing solutions and section 4 follows the problem and proposed solutions. This paper is concluded in section 5.

II. OVERVIEW OF DDOS ATTACKS

One common method of attack involves saturating the target machine with external communications requests, such that it responds so slowly as to be rendered effectively unavailable. Such attacks usually lead to a server overload. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim. A DDoS attack uses many computers to launch a DoS attack against one or more targets. A typical DDoS attack consists of four elements[6].

[1] The real Attacker;
[2] The handler who are capable of controlling multiple agents.
[3] The Zombie hosts who are responsible for generating a stream of packets toward the victim.
[4] The victim or the target host.

The virus-infected computers are called zombies – because they do whatever the DDoSer commands them to do. A large group of zombie computers is called a robot network, or botnet. The computer could be part of a botnet without the knowledge of user. That's because it may be busy participating in a DDoS attack at the same time the user are using it. Or, the user might find out that the computer is infected when the Internet service provider (ISP) drops the user service because of computer is sending an unusually high number of network requests[19].

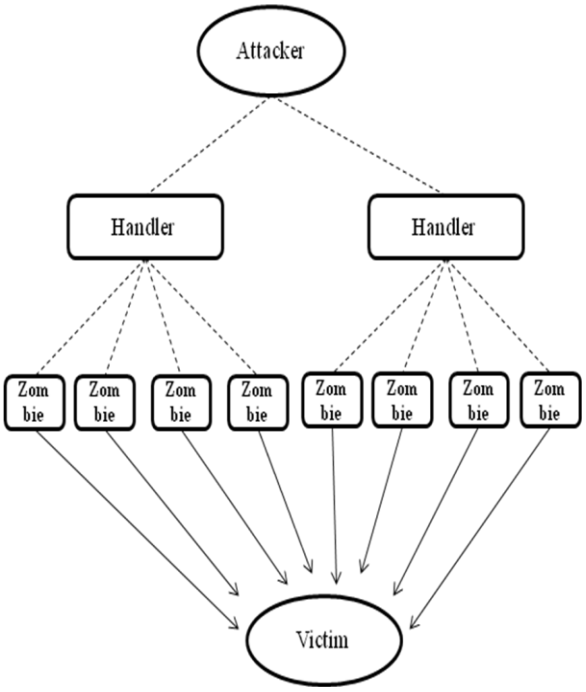

Figure 1: Architecture of DoS attack

Zombie computers in a botnet receive instructions from a command and control server, which is an infected web server. DDoSers who have access to a command and control server can recruit the botnet to launch DDoS attacks

2.1. Denial of Service type

There are many types of DDoS attacks. They target different network components – routers, appliances, firewalls, applications, ISPs, even data centers – in different ways. DDoS attackers use a variety of DDoS attack methods. The malicious hacker group Anonymous, for example, started with a tool that could launch Layer 7 DDoS attacks and Layer 3 DDoS attacks from any computer. These attacks had a common attack signature – that is, common code. As a result, the attacks could be detected and mitigated fairly easily[19].Denial of service can be divided into three forms.

[1] DoS

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[3]. 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.[20]

DDoS attack

A distributed denial of service attack (DDoS) 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[4].

[2] DRDoS

This type of attack is more detrimental than a typical DDoS attack. This is because a DRDoS attack has more machines to share the attack, and hence the attack is more distributed. This is also creates a greater volume of traffic because of its more distributed nature[3].

III. EXISTING SOLUTIONS

3.1 Classification of DDoS Attack

DDoS attacks can be divided into two categories: Bandwidth attack and Resource attack.

- In a bandwidth attack, simply try to generate packets to flood the victim's network so that the legitimate requests cannot go to the victim machine.
- A resource attack aims to send packets that misuse network protocol or malformed packets to tie up network resources so that resources are not available to the legitimate users any more.

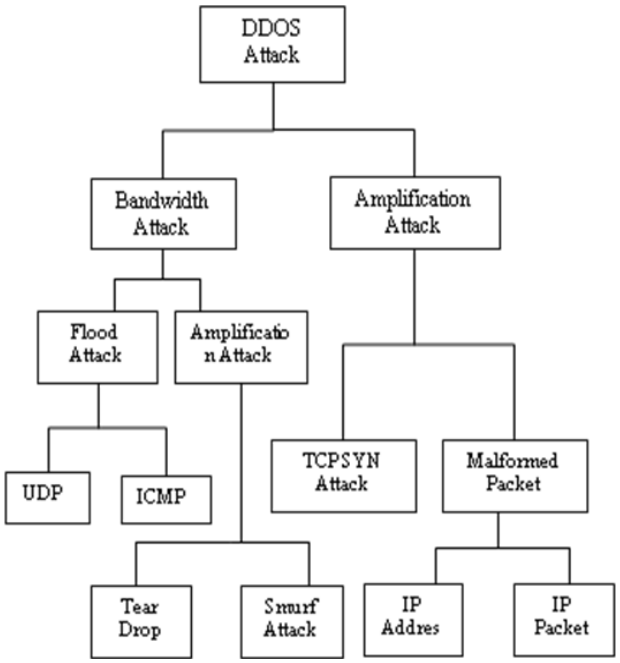

Figure 2.Classification of DDoS Attack

3.1.1 Bandwidth Attacks

- **Flood attack:** This attack 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.Once this buffer is full no further connections can be made, and the result is a Denial of Service.
- **TCP Flood :** 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 Flood: A stream of ICMP packets are sent to a victim IP address.
- **UDP Flood**: A stream of UDP packets are sent to the victim IP address.
- **Teardrop :** This attack creates a stream of IP fragments with their offset field overload. The destination host that tries to reassemble these malformed fragments eventually crashes or reboots.
- **Smurf attack:** The victim is flooded with Internet Control Message Protocol. The attackers sends numerous ICMP "echo-request" packets to the broadcast address of many subnets. These packets contain the victim's address as the source IP address [4][6][10].

3.1.2 Reflected attack

A distributed reflected denial of service attack (DRDoS) involves sending forged requests of some type to a very large number of computers that will reply to the requests. Using Internet Protocol address spoofing, the source address is set to that of the targeted victim, which means all the replies will go to the target.ICMP Echo Request attacks (Smurf Attack) can be considered one form of reflected attack, as the flooding host(s) sends Echo Requests to the broadcast addresses of miss-configured networks, thereby enticing many hosts to send Echo Reply packets to the victim. Some early DDoS programs implemented a distributed form of this attack[16].

- **TCP SYN Attack :** This attack occurs during the three-way handshake that marks the onset of a TCP connection. If an attack occurs, the attacker sends an abundance of TCP SYN packets to the victim.
- M**alformed Packet Attack :** A ping of death is a type of attack on a computer that involves sending a malformed or otherwise malicious ping to a computer.

3.2 DDoS Attack Tools

There are many security problems in today's Internet. But none of these problems have been completely solved; some of the tools and technical solutions have been helped to reduce the danger from the intrusions [9]. There are several DDoS attack tools are available. But some of the well known DDoS tools are given below :

[1] Trinoo
[2] Tribe Flood Network(TFN),
[3] Tribe Flood Network 2000 (TFN2K),
[4] Stacheldraht,
[5] Mstream and
[6] Shaft
[7] Trinity
[8] Knight
[9] Kaiten

Trinoo is one of DDoS attack tool and is able to launch packet flooding attacks. It has the ability to control the duration of the attack as well as the size of the flooding packets .Trinoo is the first DDoS attack tool. This is the first DDoS attack tool. It has been able to achieve bandwidth depletion and can be used to launch UDP flood attacks against one or many addresses. The trinoo was the first attempt at client-server programming by its author and was designed and implemented in a period of monthsTribe Flood Network (TFN) is able to perform bandwidth depletion and resource depletion attacks. It is able to implement Smurf, UDP fl ood, TCP SYN flood, ICMP echo request flood, and ICMP directed broadcast. TFN2K is a derivative of TFN and is able to implement Smurf, SYN, UDP, and ICMP flood attacksTribe Flood Network 2000 (TFN2K) has the special feature of being able to add encrypted messages between all attack components. Stacheldraht is based on early versions of TFN attempts to eliminate some of its weak points and implement Smurf, SYN flood, UDP flood, and ICMP flood attacks. Mstream **is** a simple point-to-point TCP ACK flooding tool that is able to overwhelm the tables used by fast routing routines in some switches.Shaft is a DDoS tool similar to Trinoo and is able to launch packet flooding attacks. It has the ability to control the duration of the attack as well as the size of the flooding packets [2][6]Trinit is the first DDoS tool that is controlled via IRC. Trinity is capable of launching several types of flooding attacks on a victim site, including UDP, IP fragment, TCP SYN, TCP RST, TCP ACK, and other floods[7].Knight is IRC based DDoS attack tool. It provides SYN attacks, UDP flood attacks, and an urgent pointer. This is designed to run Windows Operating systems.Kaiten is another IRC based DDoS attack tool. It includes code for UDP and TCP flooding attacks, for SYN attacks, It also randomizes the 32 bits of its source address[8].

3.3 Trceback Solutions

Dos attacks are easy to generate but very hard to detect. In denial of service attacks, the packets are routed correctly but the destination becomes the target of the attackers. Once the target system is attacked, the detection mechanisms are necessary to detect an attack with less false positive rate and more accuracy rate ICMP Traceback method involves every router on the network pick a packet probabilistically and generate an ICMP traceback message directed to the same destination as the selected packet.. The IP Trace is used to identify the actual path of the attack[9] Algebric approach to IP Traceback scheme is based on algebraic techniques.It generate traceback data using polynomial function and storing data in unused bits of IP header. Fast Internet Traceback a new packet marking approach. FIT is scalable to vast scattered attacks with thousands of attackers. It uses path reconstruction algorithm with node marking instead of link marking at the end user side. Performance and deployment ability of FIT is better than other packet marking schemes. It will take minimal processing time of router to track very small number of attack packet. But it goes through the false positive and negative rate[11].Advance and Authenticated Marking approach is more efficient and accurate for the attacker path reconstruction within the seconds and has low false positive rate. Traces the origin of spoofed IP packets[12].Hash Based IP Traceback has been proposed by Snoeren et al. In this method a Source Path Isolation Engine (SPIE) is used which produces review track of traffic and it can trace origin of single IP packet. The data (8 bytes) and the IP header (20 byte) both are logged on intermediate routers. This operation uses 28 byte data in hashing. The main advantages of this method are low storage of data and it ignores eavesdropping but it create overhead to generate 28 byte hash[13]

Another packet marking scheme is Deterministic Packet Marking. In this method each packet is marked and they are used to find out the source of a traffic flow. It will include all size of packets whether it is small or big. And due to this computation work and packet header size both increases. Also there is no overload prevention method exist [14].Probabilistic packet marking scheme is somewhat similar like DPM. In this, router mark packet with all its path details probabilistically and victim machine recreate the graph. It is more efficient than Deterministic packet marking scheme. But the same drawback applies to this scheme as in DPM have. Also in this scheme more number of packets gets involved in trace back processes which increase the computational time[15].

IV. Proposed Solutions

There are many problems in DoS attacks and there exists no easy way to solve DoS problem. DDoS attacks are among the hardest security problems to address because they are difficult to prevent and very difficult to trace out.To overcome these problems a novel method is propsed in this system This system is known as **PSYADoS**(**P**rotection **Sy**stem **A**gainst **DoS** attack). This system gives an solution to solve the following problems.

4.1 Intrusion Detection and Prevention Method

An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or a system attack from some one attempting to break into a system. There are a number of hacking and intrusion incidents increasing year on year as technology rolls out, it may be exposed to a variety of intruder threats. Intrusion Detection Systems detect unauthorized access attempts. There are basically two main types of IDS being used today: Network based, and Host based (looking for instance at system logs for evidence of malicious or suspicious application activity in real time).
The existing Network-Based Intrusion Detection system have the following disadvantages:

- Intrusion detection becomes more difficult on modern switched networks
- Current network-based monitoring approaches cannot efficiently handle high-speed networks
- Most of Network-based systems are based on predefined attack signatures--signatures that will always be a step behind the latest underground exploits

The proposed system introduces a new Network based Intrusion detection method. It can monitor all traffic entering and leaving the network. The proposed IDS protects a system from attack, misuse, and compromise. The user who enters into a server will be monitored by this method.

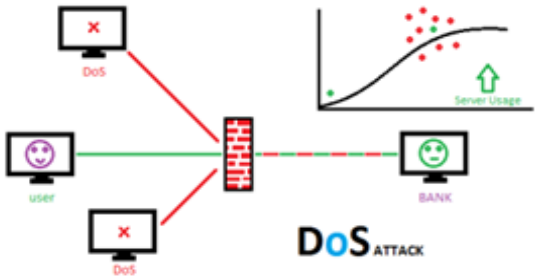

Figure 3: CPU Performance

In the above graph CPU performance is figured. Depending upon the graph the X axis shows the performance of the system and Y axis shows no of uesr working in it. It reveals that number of users comes at many times, the system becomes slow. At this moment we may know that the server is aimed for an attack. So the above graph is useful to monitor the CPU Performance.

4.2 IP Address Spoofing

IP address spoofing is the creation of forged source IP address for the purpose of the identify of the sender or impersonating another computer system. IP address spoofing mostly used in Denial-of-Service attacks. In such attacks, the aim is to flood the victim with overwhelming amounts of traffic, and attacker does not care about receiving response of attack. IP address blocking is commonly used to protect against the attacks. On a website, an IP address ban is often used to prevent a disruptive member from access. In Existing system, IP address banning is used to limit the content to a specific region. The proposed method is used to detect the attackers IP address(that is a source IP address) and it identify that the user is unauthorized user. This system can store all the IP addresses in list which is called an admin list. Even a single user IP address can also store by this method until the user logout from the server.

4.3 IP Address Monitoring

The PYSADOS tool is used to monitor the IP address also. The user press F5(refresh) more than once, automatically this tool will be capture and store the user IP address into the database with the user's details and the time of their login. The Algorithm in the below is used to capture and store the unauthorized IP address into the database.

4.3.1 Algorithm for Monitoring Unknown IP address

```
vip=getip("address");
If (Ip!=ValidIp(vip)&& Ip<=proxy("vip"))Then
{
        time=30;
        gtime=refr("time");
        If(rEcap("StrVal")==getstr("vstr")&& gtime>=1) Then
{
        ready->work;
        get(login)=siteurl->vip;
}
        else
{
    banfile=fopen("$file_location_banlist","w")
    setbanlist=add(vip);
    print(banfile,"Str",gettime());
   }
}
```

Figure 4:Screenshot of a IP Address Monitoring

4.4 Blocked IP address

Many users operate from shared IP addresses, often those belonging to proxies used by large networks or home users with their Internet service providers. Since it is impossible to distinguish between individual users operating from shared IP addresses, blocking one may affect a very large number of legitimate users (ranging up to millions). Users operating from dynamic IP addresses change IP addresses periodically. This can compound the auto block problem, particularly when they are also shared, because a block targeted at a malicious user may shift to a legitimate user while the target shifts to an unblocked IP address. This proposed system is used to store the blocked spam IP address. This address will be added to the Admin List.

Figure 5 ; Screenshot of Blocked IP Address

4.4.1 Algorithm for storing Spam IP Address

```
Vip=getip("address");
function validip()
{
$pattern = "/^([1]?\d{1,2}|2[0-4]{1}\d{1}|25[0-5]{1})(\.([1]?\d{1,2}|2[0-4]{1}\d{1}|25[0-5]{1})){3}$/";
return (preg_match($pattern, $ip) > 0) ? true : false;
      }
if(rEcap()->fail)
{
//move ip to banlist
block("vip")
        }
else //if it Ok
{
banfile=fopen("$file_location_banlist","w")
setbanlist=add(vip);
while(Ip==EoF)
{
record=FETCH("Banlistfile");
if(record==vip)
{
DELETE("Record");
            }
else
{
Print("Spam IP");
                        }
            }
}
```

Symbols used in description

Vip= user ip
rEcap=recatch Google Api
Proxy=Proxy ip Checker Function
vstr=users Replay String
gtime=gettime refresh "seconds">(aprox_value="30sec")

4.5.Client-Side Script

Security on the web is based on a variety of mechanisms, including an underlying concept of trust known as the same origin policy. This essentially states that if content from one site is granted permission to access resources on the system, then any content from that site will share these permissions, while content from another site will have to be granted permissions separately. Cross side scripting vulnerabilities have been reported and exploited since the 1990s. Prominent sites affected in the past include the social-networking sites Twitter, Facebook, MySpace, YouTube and Orkut. In recent years, cross-site scripting flaws surpassed buffer overflows to become the most common publicly reported security vulnerability, with some researchers in viewing as many as 68% of websites as likely open to Cross side scripting attacks. Cross-site scripting uses the known vulnerabilities in web-based applications, their servers, or plug-in systems. On which they rely. Exploiting the fold malicious content into the content being delivered from the compromised site. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user. The expression "cross-site scripting" originally referred to the act of loading the attacked, third-party web application from an unrelated attack site, in a manner that executes a fragment of JavaScript prepared by the attacker in the security context of the targeted domain. These are held in the existing client-side-script.

The proposed system aims to overcome the existing client side scripting. This system can check not only the client side malicious content but also check the server side script of Code Execution, Command Execution, Header Injection, File Disclosure, File inclusion, File Manipulation, LDAP Injection, SQL Injection. It can display how long it has been scanned and how many numbers of files have been scanned. It can produce the graph to identify where the errors are and how to replace the errors. It can also identify how much it has been injured and can edit easily wherever the errors occurred. We can check to find out the errors by using two methods of Top-Down and Bottom-Up approach.

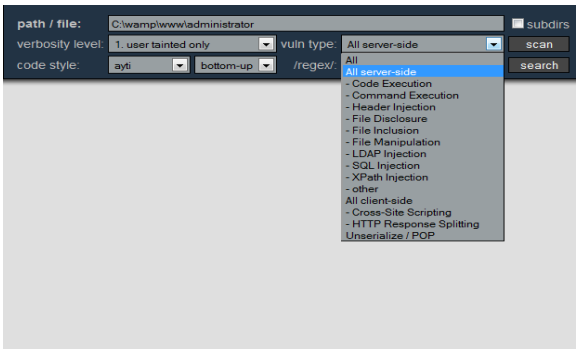

Figure 8: Types of Files to be scanned in this System

The above figure is shows how to check the vulnerable type injections both in the Client side and Server Side

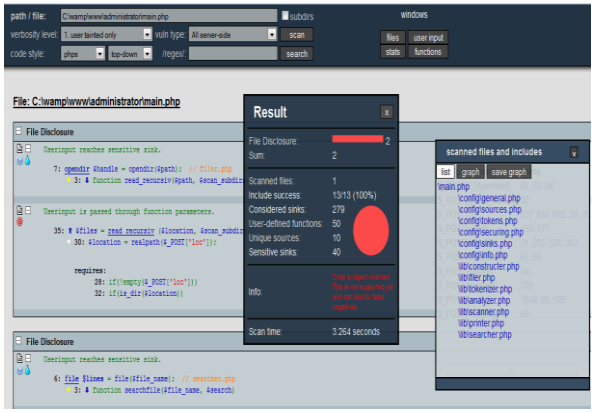

Figure 9: Result of Script Scanning

4.6 Mathematical Model

This system is used to stop a DoS attack by identifying the Spam IP and discard them before reaching the victim. The web surfer might surf the source code programs also. This system could check the client side and the server side scripting to avoid the harmful attackers. So this system is also examine the malicious content into the content being delivered from the compromised site by applying the following equations

$$if\ c \leq \propto then\ goto\ Check$$

Where **c** can scan the script to find out the errors in the **α** coding.

$$t * c * C = n\ value$$

C can check the malicious content of the Coding, **t** is to calculate the timings of **C** and **n** is the total timing calculated by the **c&C** and also **t.**

$$bug = \alpha$$

α finding out the errors in the script

$$val = \beta$$

β finding out the vulnerable coding and

$$exploit = \gamma$$

Y rectifying the infected coding.

$$if\ \alpha \rightarrow \propto \&\ \beta \rightarrow \propto \&\ \gamma \rightarrow \propto \&\ then$$

$$\alpha \uparrow_{= safe} \downarrow$$

If **α, β, Y** are correct then the script will be in safe.

4.7 Graphical Model

The graphical model shows the scanning of script wherever it has the errors in it and also it shows the modification of error code. In its scanning if the white color displays there is no error and if the orange color indicates there is changes made in it. If the red color is indicated the code must be completely modified.The developers must be careful to be safe in the codings. This type of code is called the vulnerable code. The graph model is useful to keep the script in safe.

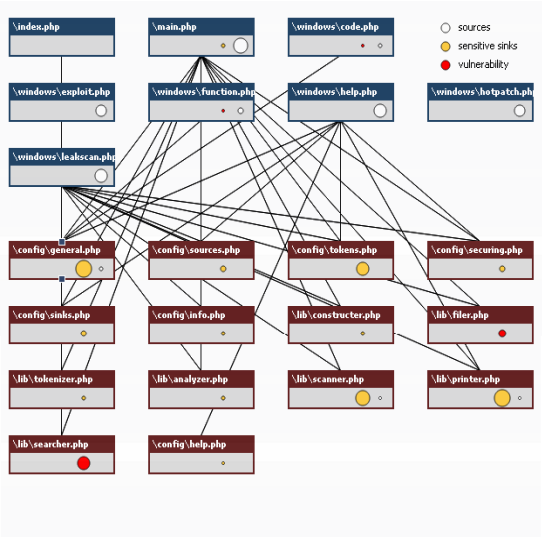

Figure 10 : Graph Model

III. CONCLUSIONS

DoS and DDoS attacks are advanced and powerful methods of attacking a network system to make it either unusable to the legitimate users or downgrade its performance. This survey indicates that an overall DoS detection mechanism by combing different detectors in order to provide robust and effective detection. Since Dos attacks are complex and difficult to combat till now. There is no single point solution, everyone is vulnerable. This survey examines the possible solutions to this problem.

We cannot separate good traffic system from the more attacks. This Proposed system is used to show the Flood IP address and also it proves that the users are authentication user by using recapturing techniques. It can defend against blocking,based on the analysis of existing solutions, the proposed desirable solutions are to defend DDoS.

REFERENCES :

[1] David karig and Ruby Le, "Remote Denial of Service Attacks and Countermeasures," Princeton University Department of Electrical Engineering Technical Report CE-L2001-02

[2] Helna Sandstrom, "A Survey of the Denial of Service Problem," Lulea University of Technology,Sweden.

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

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

[5] Georgios Loukas and Gulay Oke, "Protection against Denial of Service attacks: A Survey," Intelligent Systems and Networks Group, Imperial College, London.

[6] Shibia Lin Chiueh, , "ASurvey on solutions to Distribuited Denial of Service Attacks," Stony Brook University, Stony Brook.

[7] http://users.atw.hu/denialofservice/ch04lev1sec4.html.

[8] http://www.scribd.com/doc//DDoS-Tool-Knight-and-Kaiten

[9] A.John,T.Sivakumar,Ramanujam, "DDoS Survey of Traceback Methods," International Journal of Recent Trends in Engineering, Vol.1,No.2,May 2009

[10] Arun Raj Kumar,P and S.Selvakumar, "Distributed-Denial-of-Service(DDoS) Threat in Collaborativem Environment-A Survey on DDoS AttackTools and Traceback Mechanisms," IEEE International Advance Computing Conference(IACC 2009).

[11] Abraham Yaar,Adrian Perring, Dawn Song, "Fast Internet Traceback,"Carnegie Mellon University.

[12] Dawn Xiaodong Song & Adrian Perrg, "Advanced And Authenticated Marking Schemes For IP Traceback," IEEE INFOCOM 2001.

[13] A.Snoeren,C.Partidge,L.Sanchez,C.Jones,F.Tchakountio,B.Schwartz,S.Kent and W.Strayer, "Single-Packet IP TracEkback," IEEE/ACM Trans. Networking, Vol 10, no.6,PP.721-734,2002.

[14] Andrey Belenky, Nirwan Ansar, "On deterministic packet marking," Computer Networks, Volume 51, Issue 10, 11 July 2007, Pages 2677–2700.

[15] Pegah Sattari, Minas Gjoka, Athina Markopoulou, "A Network Coding Approach to IP Traceback," University of California, Irvine

[16] Randal Vaughn and Gadi Evron, "Dns amplification attacks preliminary release," March 17,2006.

[17] http://www.ddosmitigation.biz/

[18] http://www.watchguard.com/infocenter/editorial/41649.asp

[19] http://www.prolexic.com/knowledge-center-what-is-ddos-denial-of-service.html

[20] Aleksei Zaitsenkov, Dos Attack