HOP-COUNT SENSITIVE PACKET MARKING IN PROBABILISTIC PACKET MARKING

By

RADHAKRISHNAN GOPALSAMY

Bachelor of Engineering

Bharthidasan University

Trichy, Tamilnadu, India

May 2002

Submitted to the Faculty of the
Graduate College of the
Oklahoma State University
In partial fulfillment of
the requirement for
the Degree of
MASTER OF SCIENCE
July 2005

HOP-COUNT SENSITIVE PACKET MARKING IN PROBABILISTIC PACKET MARKING

Thesis Approved:

Dr. Venkatesh Sarangan
Thesis Adviser

Dr. Debao Chen

Dr. Johnson P.Thomas

Dr. A. Gordon Emslie
Dean of the Graduate College

ACKNOWLEDGMENTS

I wish to express my sincere gratitude and appreciation to my thesis advisor, Dr. Venkatesh Sarangan, for his intelligent supervision, sincere guidance, and friendship. He devoted himself in spending time with all my thesis meetings. His in-depth knowledge in the subject helped me to complete my thesis in an excellent way. Also I like to thank my other committee members, Dr. Johnson P. Thomas and Dr. Debao Chen for their sincere guidance, encouragement, and friendship in completing my thesis.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1: INTRODUCTION:

The Internet is a global network connecting millions of people around the world. More than 100 countries are connected through the Internet to access global data exchange. The Internet architecture looks like this: (see figure below)

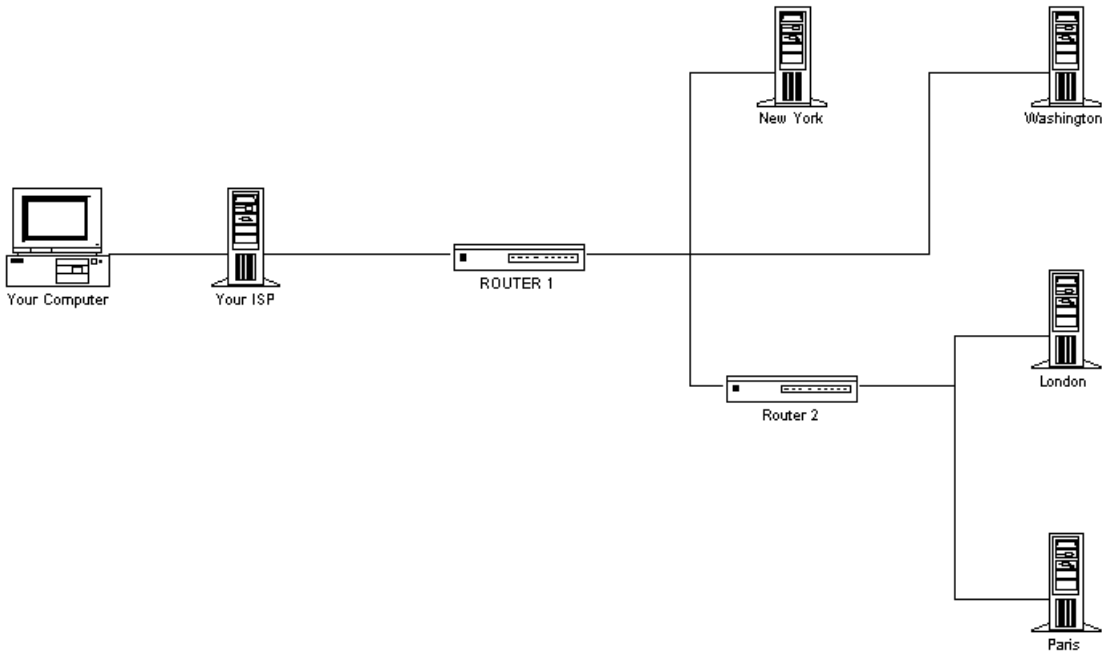

Figure 1: General Internet (reproduced from [1])

So the Internet serves as the backbone for 80% of the world's population. Access to the Internet is gained through ISPs. The Internet has two types of computers, namely HOSTS and CLIENTS. A client is the one which has permanent access to the internet. A client to the internet can access the email and upload or download files and World Wide Web. The size of the internet is being estimated as 27.5 million people in U.S alone [1].

As the Internet grows the threat to the Internet also grows at the same pace. There are varieties of threats to Internets: worms, viruses, and Denial of Service (DoS) attacks.

1.1 WORMS:

A Worm is a program that propagates itself and uses the resources of one machine to attack other machines. The worms get the host address by system tables. Worms consist of 99 line boot strap program written in C language. The activities of worm are divided into attack and defense. In attack mode it will locate a host to penetrate, and it will exploit a security hole in order to pass the copy of the worm and run it. The worms will penetrate to the remote system also. This is achieved in three ways. It will take the advantage of the bug in the finger server that will allow it to download the code as finger request and will execute the code by tricking the server. The second method involves sending mail through a “trap door” in send mail SMTP mail service. In this way, it sends a bug in executing code which will open the command interpreter. Once in the command interpreter it will copy and execute the 99 line boot strap. In the third, the program guesses one of the local accounts and password and tries to get its remote command interpreter; then it copies the code and runs it [2]. Worms will exploit the operating system by bugs which make the operating system inadequate to do normal processes. On the whole, Worms will shut down the whole network.

Protecting the network against worm can be done with several tools. There are two types of protection, namely basic protection and good network security. One type of basic security system is Identification and Authentication. In this, the system will identify the control and authenticate only the legitimate controls to the user. Still, worms will attack if

it is poorly managed. The other method is Add-on tools. There are three types of add-on tools: configuration review tool, check sum–based change detection tool and intrusion detection tool. Wrapper programs are types of network security tools which reject or allow particular connection. The firewall system is another type of network security [3].

1.2 VIRUSES:

The next threat is viruses. A virus is a program that replicates a code segment by attaching copies to existing executables. The main characteristics of viruses are replication, requiring a host program as carrier and activated by external action and replication. These are limited to virtual servers. When the computer program is infected by viruses, then that program has been converted to a Trojan horse. These programs will perform useful functions but they are affected by the side effects of virus programs which perform unintended task. In addition to the unintended tasks, these virus programs perform replication too. The replication begins when the original program tries to execute. The replication of a virus is uncontrollable, which makes a virus so dangerous. Viruses are designed to attack a current platform. A platform is the one which is combination of hardware and operating system. The operating system should be designed for that particular type of hardware. There are two types of viruses, research virus and personal computer virus. The research type of virus is the one that is written for research or study purposes and is not distributed to the public. The first computer viruses were being developed in early 1980s.The first viruses was called APPLE II viruses. All viruses are fond of targeting personal computers. Over the years the viruses have evolved due to the authors making the code more difficult to detect, dissemble and eradicate. Personal computer viruses are those viruses which exploit the controls over these systems. Viruses

can modify files in the operating system itself. These actions are considered a legal action in the operating system. While more stringent rules are there in the multi-user, multi-task operating system due to the loop holes in the configuration and security, it creates the possibility of viruses to get in to these types of systems. In conclusion the viruses can exploit the operating system controls and human patterns of system use/misuse, Destructive viruses are hard to eradicate. Other viruses, which are called innovative viruses, will propagate more windows before being discovered. It is been studied that for multi-user system it is hard to write viruses. Even though it is hard to write the multi-user system viruses there are possibility that viruses can still exist in those systems. The reason is that personal computer systems exchange disks frequently. In those set of personal computers some may be affected by the viruses which leads to the spread of viruses to unaffected systems. In the multi-user systems there exists an administrator which does not exchange the executables but exchanges the source code. In those systems the probability of viruses attacking is much less. These systems are made for copyrighted materials. So they exchange materials with public or local domains. The advent of remote protocols like NFS (Network File Systems) and RFS (Remote File Systems) lead to formation small multi-user systems which can exchange executables. In order to spread, viruses need a set of homogenous systems and executables to exchange software.

Anti-virus software can be used to protect against viruses. These tools should be available first whenever there is an exchange of software between the systems. These tools are divided in to three categories namely the detection tools, identification tools and removal tools. Examples of detectors are Scanners, modification programs and vulnerability

monitors. Scanners serve as identification tools also. Examples of removal tools are disinfectors.

Scanners and disinfectors rely on the a priori knowledge in the viral code. Scanners will try to find the signature codes or some types of algorithms to detect or identify the existence of known viruses. Where as the disinfectors will look for the size of viruses and type of modifications to restore them. Vulnerability monitors are those that prevent accessibility of viruses to the sensitive parts of the computer. This requires lot of information about the system use. Modification programs are those which do not require any information about viruses. In this technique the check sum information about the clean executables are executed and saved. For each other computation the executables check sum are compared with the original one [4].

1.3 DoS ATTACK:

DoS attack are considered the major threat to the Internet. DoS attack is the concentration of forged traffic in the targeted servers. In DoS attacks useless packets are being sent to the targeted victim, so that the victim gets a multitude of packets which bring the system to halt. Technically the attacker will be sending a large number of requests which may overwhelm the server denying access to legitimate users. These attacks spread through the world by using many computers which take over those networks by hacking. In 2000 DoS attack brought a number of popular sites namely google.com, yahoo.com and hotmail.com to halt. About two to three percent of traffic is by targeted servers; the router used to send to the proper domain name sends to the equivalent address leading to flooding of network. Routers, that direct the traffic, get a DoS attack about 1 to 2 percent. Most important sites like Amazon.com, Aol.com are

targets of DoS attacks. The study about this attack gives the idea that the majority of victims (i.e. 95 % of them) are attacked lesser than 5 times and 65%of the victims are attacked only one time [4]. The interesting thing about the DoS attack is that the attacker will try to spoof the victim by giving spoofed source IP address to the victim. These types of attacks are called hidden attacks, since the attacker will be behind scene and send packets to the victim.

Such attacks are considered to be hardest among the security problem because they are easy to carry out and hard to prevent. In recent years Internet denial of service attacks has increased in frequency, severity and sophistication. DoS are of two type single source Denial of service attacks and distributed source denial of service attacks. In single source only one machine generates packets to the victim where as in distributed DoS, several machine generates packets to the victim. The figure 2 below shows the DDoS attack [8].

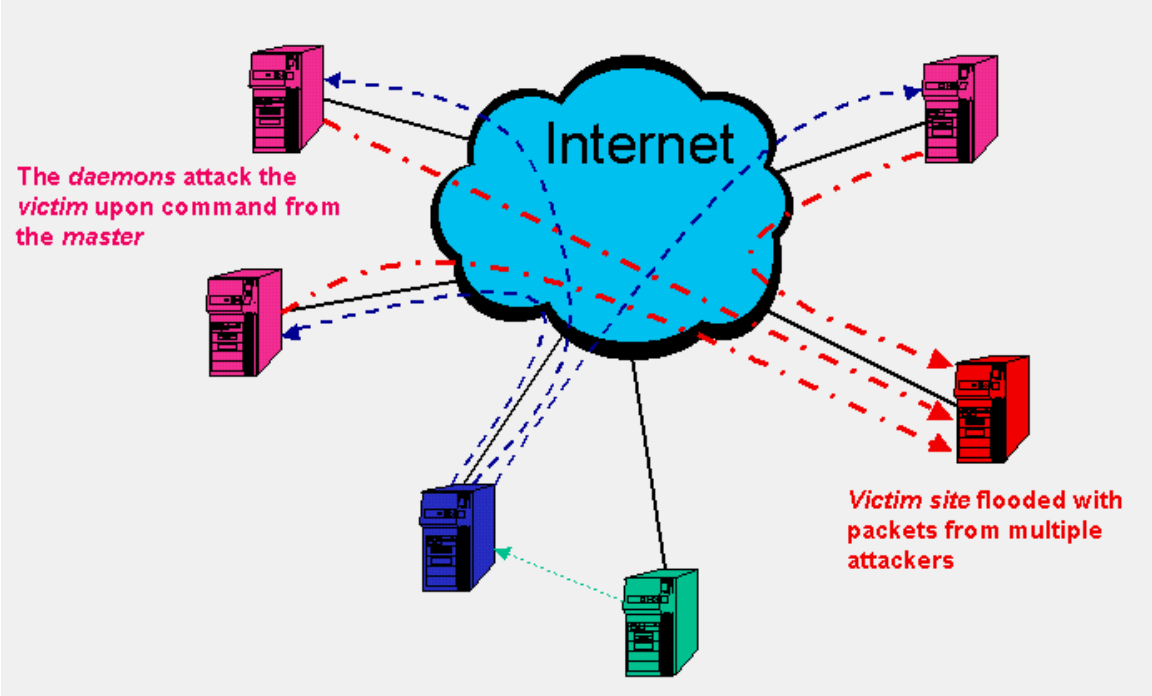

Figure 2: DDoS attack (reproduced from [8])

Some of the common varieties of Denial of service attacks are

a) Syn Flood,

b) ICMP flood,

c) UDP flood,

d) Application Level floods, and

e) Nukes.

1.3.1 SYN FLOOD:

A ***SYN flood*** is a sequence of TCP session initiation packets, often from incorrect (or "spoofed") IP addresses. The result is that the target tries and fails to establish a number of TCP sessions, which consumes resources on the target [14]. The figure 3 shows the model of the SYN attack [5].In this; attacker with IP address 201.10.24.6 sends a SYN packet with the spoofed source address 245.20.26.80. As a result the Net screen device will respond for the SYN request by sending SYN/ACK packets to the spoofed source IP address and waits for a response until the response until the efforts bines out.

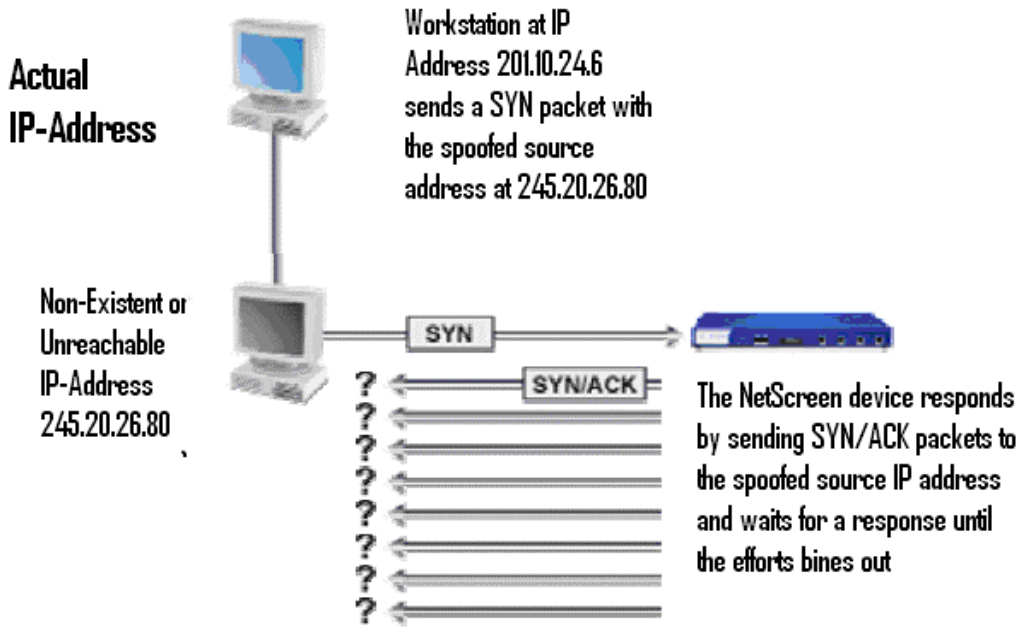

Figure 3: SYN Attack (reproduced from [5])

In SYN flood the attacker will send large amount of SYN request to the server and the server will send ACK to the SYN request. But the attacker will not be responding to those requests so this result in the half open connections in the server. Incoming connections will be still in the handshake phase which is part of the backlog queue. But the backlog queue is really small once these requests start to come in this queue will get full which leads to the half open connection [6]. The attacker will send those SYN request till the server comes to the half connection open. After that the server cannot respond to the new request [17]. If this continues then it halts the entire system. If the target is going to be a SMTP server then legitimate users may not receive any email or if the target is HTTP server then the website will be down.

1.3.2 ICMP FLOOD:

An ***ICMP flood*** is another attack mechanism wherein a sequence of ICMP echo request packets from spoofed IP addresses is sent to a server. Echo requests are usually answered by an echo reply packet if the target is operational, so such an attack will consume resources on the target. This attack will also consume resources on the spoofed source IP addresses as they will receive a number of ICMP echo replies [16].An example of this attack is that in the figure 4 shown below [7]. In this the attacker sends the spoofed ICMP request to IP addresses 192.168.1.255 and 10.1.2.255. This in turn sends those requests to the victim. As a result the system hangs [7]. There are actually three players in this attack namely the attacker, the intermediary victim and the victim. The attacker sends the request with spoofing its IP address as IP address of intermediary network address. As a result the intermediary network replies to those requests which cause the victim flooding [7].

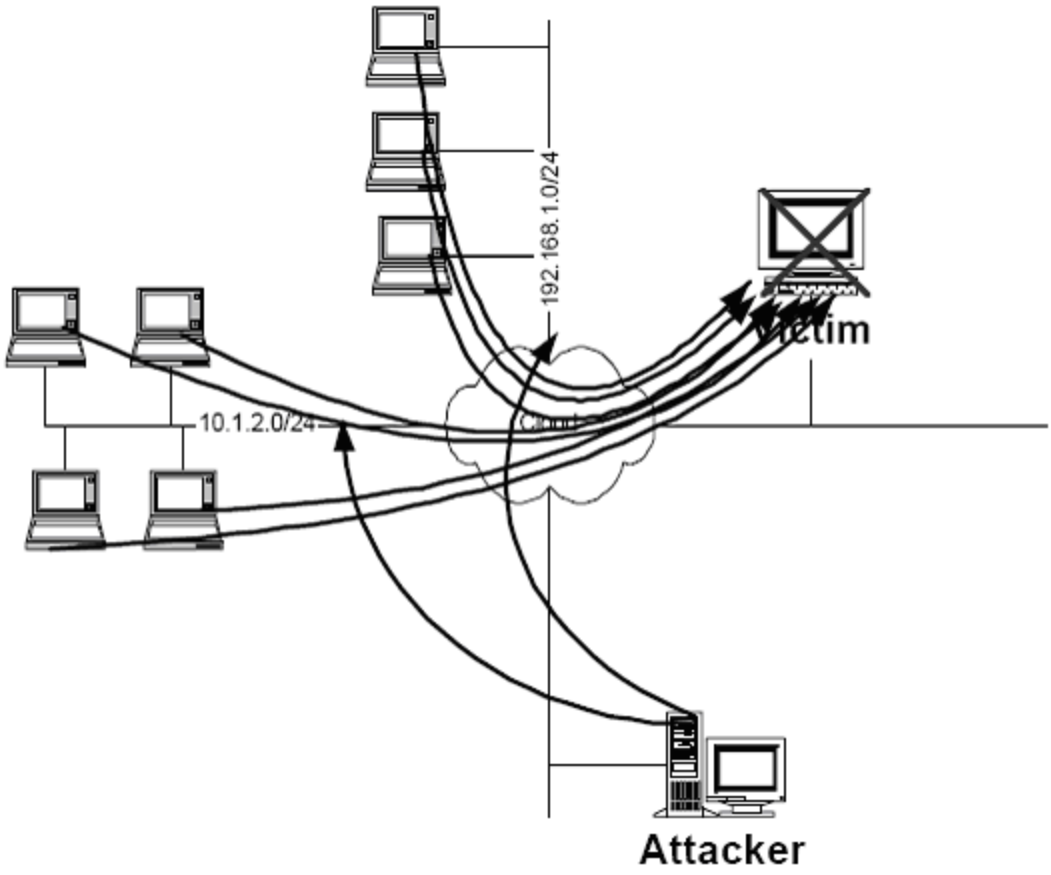

Figure 4: ICMP attack (reproduced from [7])

1.3.3 UDP FLOOD:

The same idea is used in a ***UDP flood*** where a sequence of UDP packets, often from spoofed IP addresses, is sent to UDP ports. Smurf and Fraggle attacks exploit the fact that a source IP address sending an ICMP or UDP flood will be flooded with reply traffic, by flooding the broadcast address of a target network with ICMP or UDP packets [16].UDP is a type of protocol which does not use any hand shake signals. So this makes the attacker to easily abuse victim. One common type of attack in UDP is called as “Pepsi attack.” In this attack the attacker sends large number of forged UDP packets to the random diagnostic port on the target host. The CPU time, resource and the bandwidth

required for processing these packets makes the network unavailable for providing access to the legitimate users [9].

1.3.4 APPLICATION LEVEL FLOOD:

An application Level flood is the flooding of various applications. The common application level flood is multiple requests to a particular web server and sending large email attachments to the victim [16].The main target of application level flood is to disable and damage application process. These attacks can be identified by deep packet filtering. Also these attacks cannot be identified by layer 3-4 parameters since these attacks uses legitimate parameters and performs malicious functions [10].

1.3.5 Nukes:

Nukes are a method of crashing out the remote systems. A common example of a Nuke attack is the IP packet with same source and destination address [16]. Nukes will exploit bugs in the operating system (OS). The main idea of nukes is to send packets to OS such that, the OS may not be able to recognize those packets. In this attack the attacker will send message stating that particular system had dropped the connection with the server, so the server will drop that particular connection. But the victim has not sent those messages. So the result is that the particular victim will be disconnected with the server. These attacks are carried out mainly to crash windows 32/95/NT systems. Technically this attack carried out by sending OOB (Out Of Band) used to establish connection with the windows user.Net bios is effective in this attack, whichever port listens to that data can be attacked.Net bios is used as communication link between computer hardware and network hardware. When it receives OOB data, it asks the computer hardware, which one wants the OOB data but the OOB data is been faked by the attacker. As a result of this all

the hardware will respond as “I don’t know.” In the mean time computer says it could not respond, leading the computer to hang. Tear drop attack and smurf attack are types of Nuke attacks.

Tear Drop attack is the one that happens when TCP/IP protocols handle data larger than 1024 bytes. TCP/IP protocol handles these large amounts of data by dividing them into fragments and putting an offset number at the beginning of the packet. At the receiving side the receiver must reassemble these fragments in order to get the whole data. So in this attack, the attacker puts a confusing offset number. For the receiver, if there is no plan to handle this situation the system will crash [11].

Smurf Attack is the one in which the attacker sends ping requests to a receiving site. These ping requests represent it have to be broadcasted to all of the local networks sites. Also this request will represent that it is from some spoofed host. As a result the spoof will receive lot of replies flooding the innocent host [11].

CHAPTER 2: BACKGROUND

This chapter is to give some of the background information about the packet marking and trace back scheme. In this chapter we are going to study about various kinds of other methods carried out by others, what are all drawbacks with those schemes and why we need to go for the new scheme.

2.1 TRACE BACK:

In order to trace the attacker from all attacks mentioned in the previous chapter IP trace back scheme is used. IP trace back in general is defined as the method of tracing back the path traversed by packets using the IP header from source to destination, where the source is the attacker and destination is the victim. The trace back process from an attacker to victim is shown in the figure [12].In this, attacker is traversing the path Router3, Router5 and Router6.So the path is traced back in order to find out the attacker.

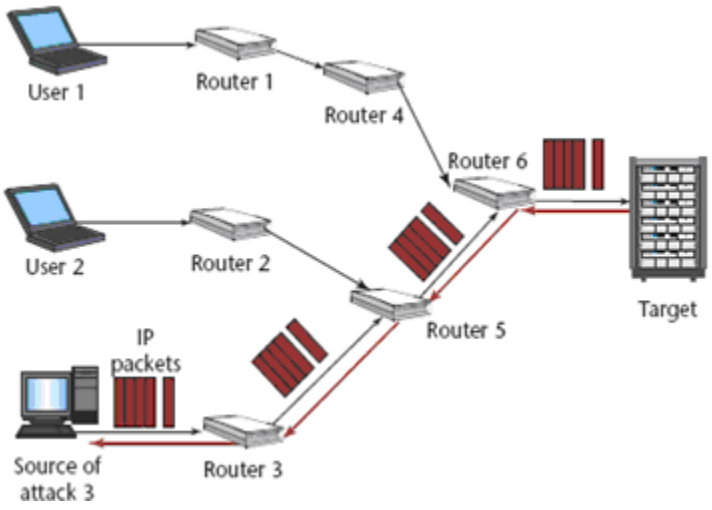

Figure5: IP trace back (reproduced from [12])

The trace back process is carried out in the network layer with the help of routers and gateways. The challenge in IP trace back processes is to find a scalable and efficient way to track the source of the arbitrary IP packet [17]. Another objective of IP trace back is to minimize router overload and the time required to get the trace [17].To carry out IP trace back we need to mark the illegitimate packets that are passing through the routers. IP marking is the technique used to get the information of the router through which the packet had passed through the network. All the routers are enabled with some marking technique by which, if a router decides to mark a packet it gives its IP information to the destination router through the packet. When the victim receives a sufficient number of packets, it traces the path traversed by the packet from the attacker to the victim.

2.2 NODE APPENDING, NODE SAMPLING AND EDGE SAMPLING:

Savage et. al. in ref [17] discussed three basic marking scheme namely node appending, node sampling and edge sampling. In Node Appending, a router's address is appended to a packet traveling through the network from the attacker to the victim. At the victim side the packet carries all the routers address with that it gets the trace. The main draw back of node appending is Router over load that happens when appending the IP address during packet marking. Also, since the length of the path is not known a priori, it is impossible to use all the unused space in the packet for the complete list. This leads to unwanted fragmentation of packets and bad interaction with the services.

In node sampling on receiving a packet the router chooses to write its address with some probability. So by receiving certain number of packets the victim can get its trace. The main draw back of node sampling is the routers that are far away from the victim

contribute only few samples for path construction. Interfacing the total router order from the distribution of samples is a slow process. This technique is not robust against multiple attacks.

The third scheme that is proposed is called as Edge sampling. In Edge sampling two static address fields “start” and “end” and a distance field are reserved. Whenever a router R decides to mark the packet, it writes its own address in the start field and marks the distance field as zero. Otherwise if the distance field is already zero then this shows that some other router R1 had already marked the packet. Hence in this case router R writes its own address in the end field. The distance field is incremented in each hop as long as packet is forwarded in the network. The main draw back of edge sampling is that it requires larger IP packet header sizes; there by it is not backward compatible. Consequently less information is available for the path reconstruction.

2.3 PROBABILISTIC PACKET MARKING:

Park et. al. in ref [18] discussed the probabilistic packet marking. Probabilistic packet marking is the method in which the packet is marked based on some probability called the marking probability. In probabilistic packet marking packets are chosen randomly with low marking probability for example 1/25. So the packets that are marked are a subset of total traffic. Each router will calculate a marking probability by which the router takes a decision to mark the packet or not. If the router decides to mark the packet it writes its IP address to the packet and forwards the packet. The simple model of probabilistic packet marking is shown in the figure 5 [19].In this, attacker is source x. Which takes the attack path R1, R2 and R3.All the routers in the attack path will mark the

packet with some marking probability. With the marked packets the victim gets the attacker information.

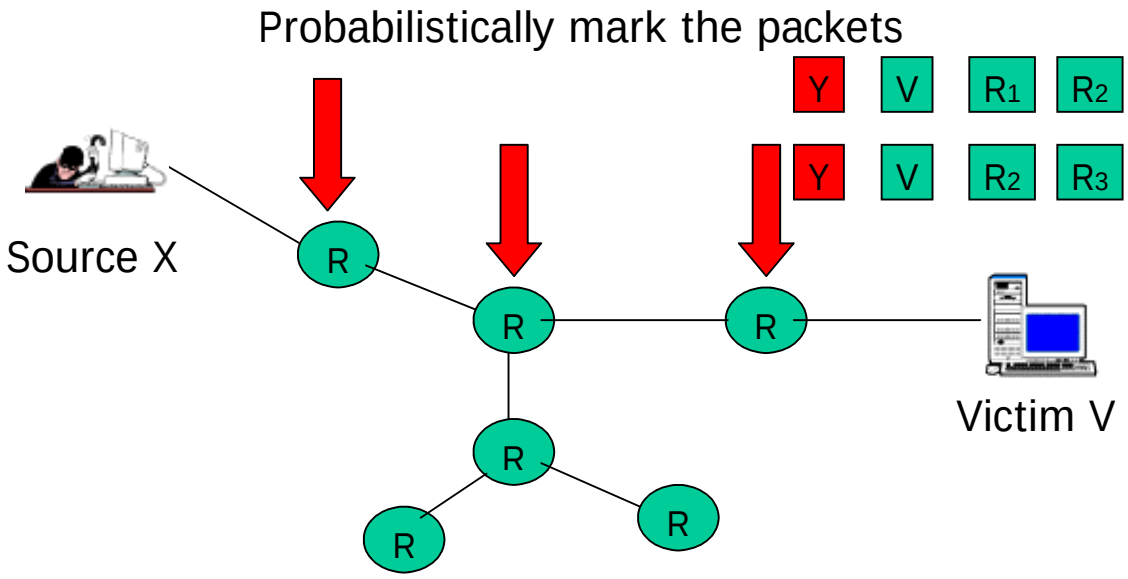

Figure 6: Probabilistic Packet Marking (reproduced from [15])

In probabilistic packet marking, two methods are carried out namely packet marking and path reconstruction. Packet marking is done by the method said above and the packet information are stored and handled by edge sampling method. The marked packets are used for the path reconstruction. The main draw back of probabilistic packet marking is the number of packets required for reconstruction is more. The reason is ppm uses underutilized space in IP packets to send information which is not enough to get information. So we need more packets to get entire path.

2.4 DETERMINISTIC PACKET MARKING:

Belenky et. al. in ref [7] discussed about the deterministic packet marking .In deterministic packet marking all the packet that enters the network is been marked (i.e.

whenever a packet enters the network the packet is marked by the ingress router[1] and the marking remain unchanged as long as the packet stays in the network). The model for Deterministic Packet Marking is shown in figure 6 below

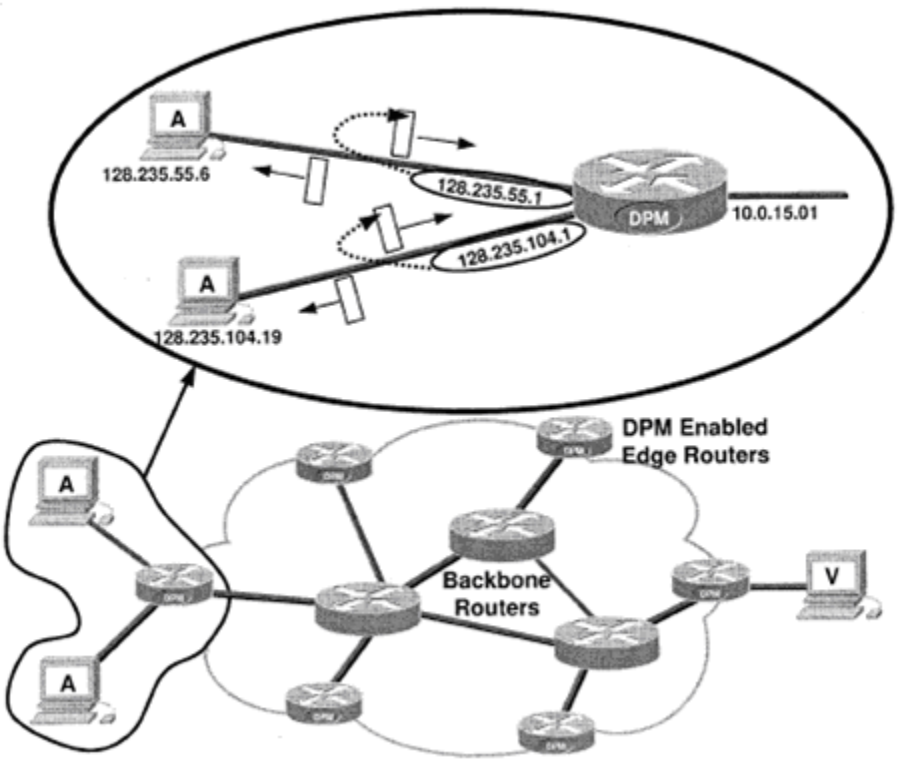

Figure 7: Deterministic Packet Marking (reproduced from [17])

There are only 17 bits available for carrying the marked information. So the marked information is carried in a field of17 bits. The 32 bit marked information is split into two parts of each 16 bits, we use the 16 bit for the address and one bit to represent which part of the address (i.e.) if the flag field is '0' then it is first half or if it is '1' then it is second half. Hence the marked information is carried through two packets. The main draw back of Deterministic packet marking is packet overhead. This technique requires two packets to get the information of one router; it doubles the number of packets required for the

[1] Ingress router is the router through which the packet enters the network.

victim to get the attacker information. Also as we have the reserved flag for getting which part of the IP address, there is a very good chance of getting the wrong IP address.

2.5 DISTRIBUTED LINK LIST MARKING:

Duwairi et. al. in ref [8] discussed the distributed link list (DLL) concept. The basic idea behind DLL is “store, mark and forward.” Each packet has a single marking field. Whenever the router decides to mark the packet it stores the current IP address along with packet id in the marking field to the special data structure called the marking table. Then it writes its IP address to the marking field and forwards the packet. Link list is inherently implemented since the marking table in each router has the pointer to the previous router. The marking strategy carried out in this method is that when ever a router marks a packet, it tries to enforce the subsequent router to mark the same packet; there exists a marking flag in the packet if the flag is on then the next router deterministically marks the packet and resets the flag. The next router along the way then marks the packet in a probabilistic fashion. The main draw back of DLL is router overhead. More routers store the packet information. This happens if high marking probability is used. In order to reduce router head, the marking probability is decreased. Then the time taken to get the trace is high.

2.6 PROBABILISTIC PIPELINED PACKET MARKING:

Basheer et. al. in ref [9] discussed with Probabilistic pipelined packet marking .The main aim of this research is to reduce the number of packets required for the trace back process. The idea in this research is that the marking information is sent through the subsequent packets heading to the same destination. In this approach each of the pipelined probabilistic packet marking enabled router has a buffer of its own. The marking strategy carried out is that, when ever router decides to mark a packet it stores the packet information into its buffer and rewrites the packet information. For example let three routers be R1, R2, and R3 with the attacker being R1 and the victim being R3. We assume that all the routers mark the packet. When packet p1 reaches router R1 it marks the packet and stores the old information into its buffer when the packet p1 reaches R2, R2 will mark the packet and stores R1 information to its buffer. At last the victim R3 will get R2 information through packet p1.When packet p2 is also heading to same destination as p1 does, p2 is not marked by any of the router but p2 is used to carry information of the marked packet. When p2 reaches R3 it has information of R1, so the victim can get all the path information. The main draw back of pipelined probabilistic packet marking is constant marking probability. When the marking probability is kept as constant two things happen. If the marking probability is high then router overhead is high. If the marking probability is low then the time required to get the trace is high.

CHAPTER 3: PROPOSED SCHEME

The imminent threats imposed by the Internet Denial of Service attacks imply that there is need for fast and efficient trace back scheme. A good trace back scheme should have the following features [9]

1. Recognition and exclusion of false information injected by the attacker;
2. Avoiding the use of large amount of packets to construct the trace back path;
3. Low processing and storage overhead at the intermediate routers;
4. If the packet information is stored at the intermediate routers then collecting this information must be efficient.

In order to achieve the above, a new approach called “Hop count Sensitive marking probability in Probabilistic packet marking” is proposed.

3.1 DRAW BACK WITH EXISTING SCHEMES:

The main draw back of node appending is Router over load that happens when appending the IP address during packet marking. Also, since the length of the path is not known a priori, it is impossible to use all the unused space in the packet for the complete list. This leads to unwanted fragmentation of packets and bad interaction with the services. The main draw back of probabilistic packet marking is the number of packets required for reconstruction is more. The reason is ppm uses underutilized space in IP packets to send information which is not enough to get information. So we need more packets to get the entire path. The main draw back of Deterministic packet marking is packet overhead. This technique requires two packets to get the information of one router it doubles the

number of packets required for the victim to get the attacker information. Also as we have the reserved flag for getting which part of the IP address, there is a very good chance of getting the wrong IP address. The main draw back of DLL is router overhead. More routers store the packet information. This happens if high marking probability is used. In order to reduce router head if the marking probability is decreased. Then the time taken to get the trace is high. The main draw back of pipelined probabilistic packet marking is constant marking probability. When the marking probability is kept as constant two things happen. If the marking probability is high then router overhead is high. If the marking probability is low then the time required to get the trace is high.

3.2 PROPOSED SCHEME:

The proposed scheme is ***Hop count Sensitive Probabilistic Packet Marking.*** In this approach marking of the packets is carried out based on the hop count where by the router overload is minimized without compromising on the speed of detection. Each router has a buffer as in [8]. When ever packet enters the network the ingress router marks the packet, stores the packet information in to the buffer, remarks the packet with its information and forwards the packet. Each packet has a hop count field. When the first router in the network marks the packet it sets the hop count field as one. Each router along the path increases the hop count field. The packet is marked by the method discussed earlier. That is, when the router decides to mark the packet it marks based on some constant marking probability.

When number of hops traversed by a packet is greater than threshold then the method of marking is carried out by the following. The marking probability is calculated as

$$p = f(d)$$

Where $f()$ is the monotonically increasing function of *d*,

p is the marking probability,

and *d* is the hop count.

So routers after the threshold are going to mark the packets. When the router marks the packet it stores the previously marked information in its buffer and remarks the packet. The marking probability is going to increase with each hop. The trace back is carried out same as in Pipelined Probabilistic packet marking [8]. The marked router information is sent through the packets that are heading to the same destination.

3.2.1 ADVANTAGES:

Earlier approaches have a constant probability of marking, so the router overload is going to increase if the marking probability is high. Also if the marking probability is low then the time taken for trace back process is high, because the number of routers along the attack path that are going to mark the packets are going to be less. Hence this leads to increase in number of packets to get the trace. In order to reduce the router load and increase the time taken for trace back process this scheme of having variable marking probability based on hop count is of great advantage. Another advantage is that most of the critical websites takes more than 15 hop counts shown in figure 9, also the general internet takes less than 10 hops shown in the figure 8; therefore the proposed Hop count

Sensitive Probabilistic Packet Marking will enable faster detection of Dos attacks on the critical websites without overloading the Internet routers.

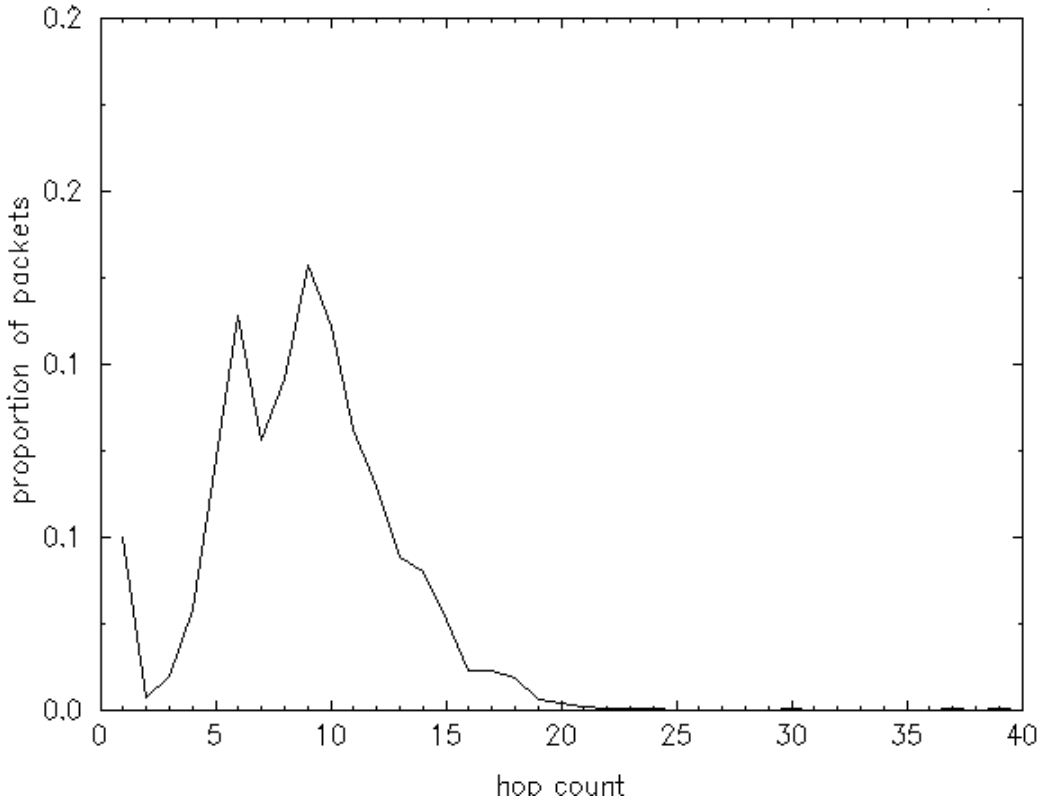

Figure 8: General Internet Traffic (reproduced from [23])

This figure below shows the hop count distribution of popular websites namely yahoo.com and Stanford .com. The distribution shows that it takes more than 15 hop count in order to get access to those sites.

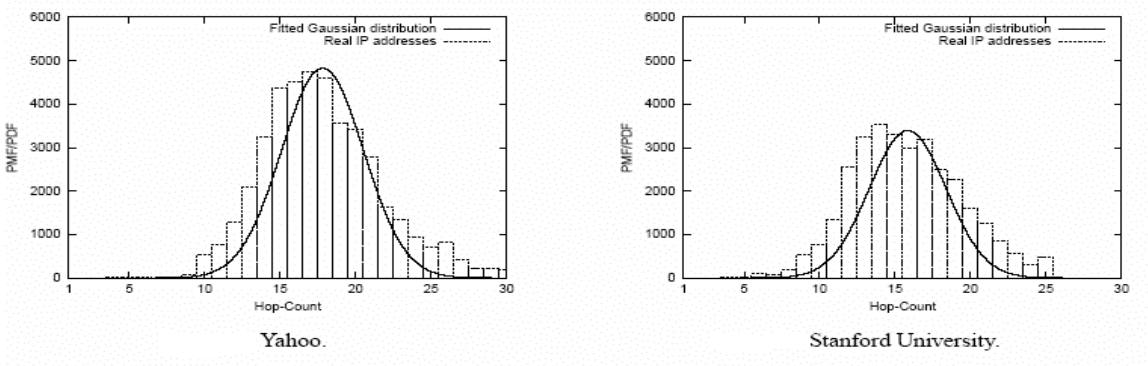

Figure 9: Internet Traffic for Popular sites (reproduced from [24])

3.2.2 SIMULATION:

The simulation is carried out in C language. The assumptions that are made during simulation are as follows the network topology that considered is Line, the attack length is 15, threshold is 10 and number of attackers is 50.In the simulation the performance are studied for following categories.

Case i:

The marking probability with number of packets and router overload are measured. In this the number of packets to get the complete path is less compared to the existing schemes (as shown in the figure 10) this makes the faster scheme for detecting DoS attack, also the router overload looks more in the proposed scheme but it is low for that particular speed. The performance graph is shown in the figure 11.

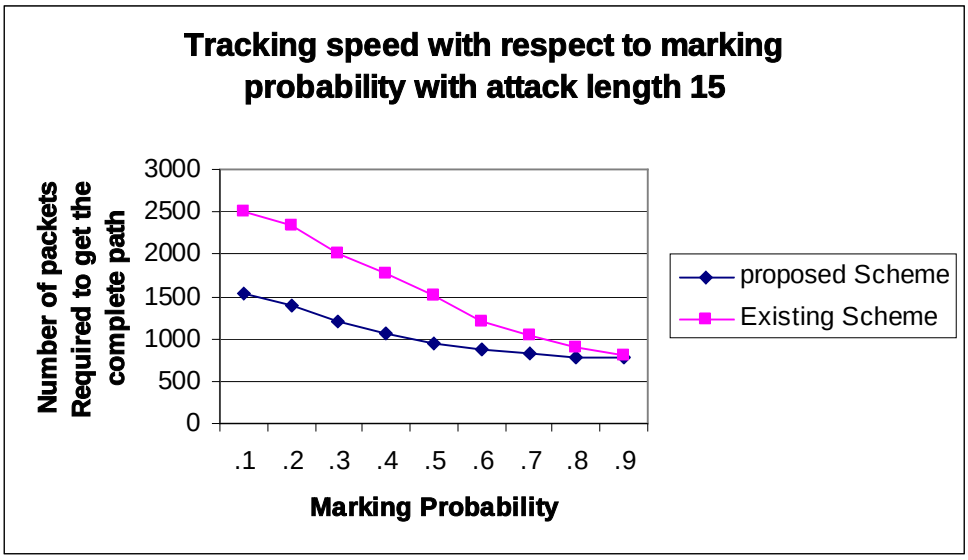

Figure 10: Tracking speed with respect to Marking Probability.

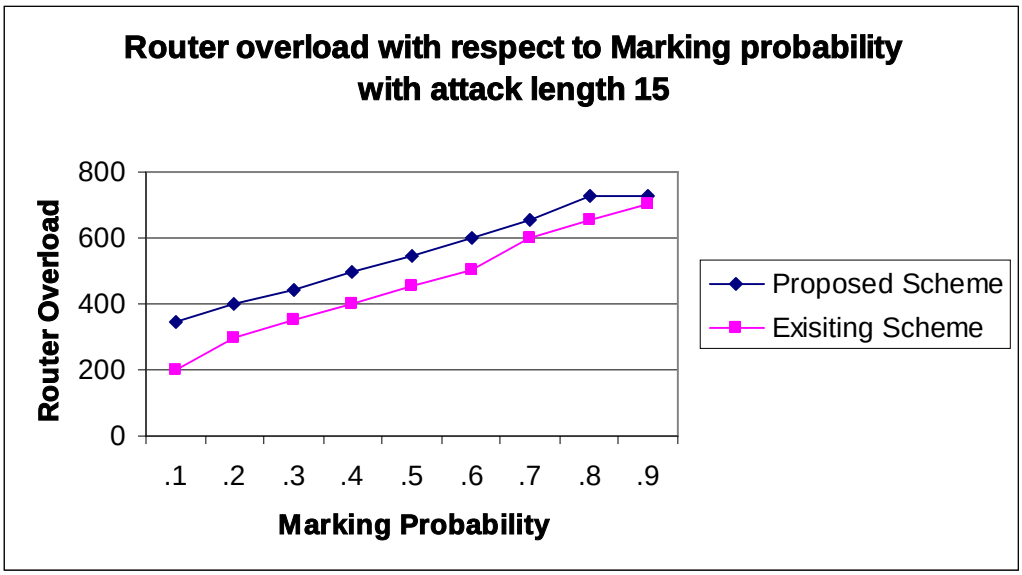

Figure11: Router Overload with respect to Marking Probability.

In proposed scheme the speed of detection is ***Sp*** and the speed of detection in existing scheme is ***Se***. Also it is found that ***Sp < Se***. And from the figure 11 it is found that If ***Op*** is the router overload for proposed scheme and ***Oe*** is the router overload for the existing scheme then ***Oe < Op***. If we need to achieve the speed (i.e. ***Sp= Se***) then from the figure 10 and figure 11 we can see that the router overload is more in existing than in proposed,

(i.e. if the router overload of the increasing speed in existing scheme is ***ΔOe*** then ***ΔOe >Op***).Hence the proposed scheme gives the Faster detection also with less router overload.

Case ii:

The performance studies are Number of packets with the number of attackers and Router Overload with Number of attackers. The performance is good because as the number of attacker is going to increase the performance also going to increase as per the above two graphs. The two graphs are shown in figure 12 and figure 13 below.

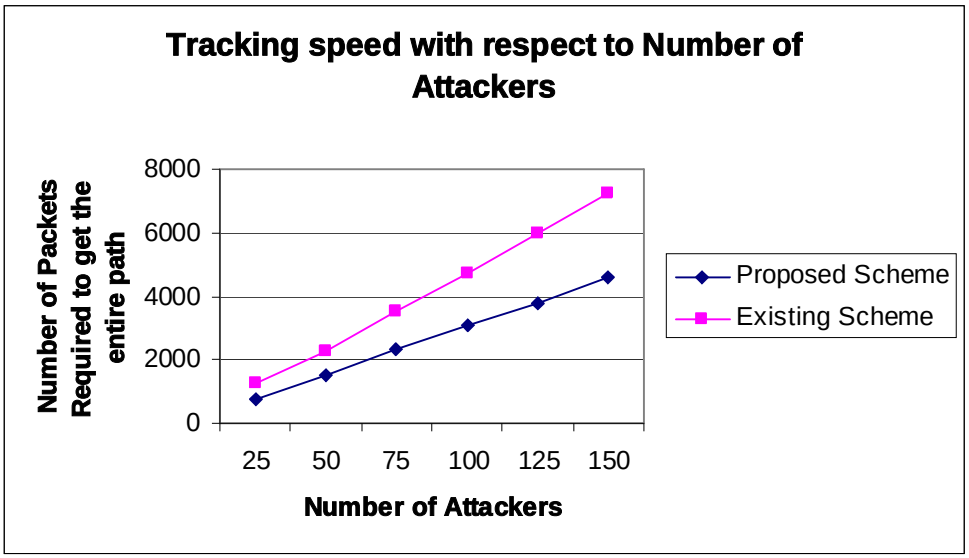

Figure 12: Tracking speed with respect to Number of attackers.

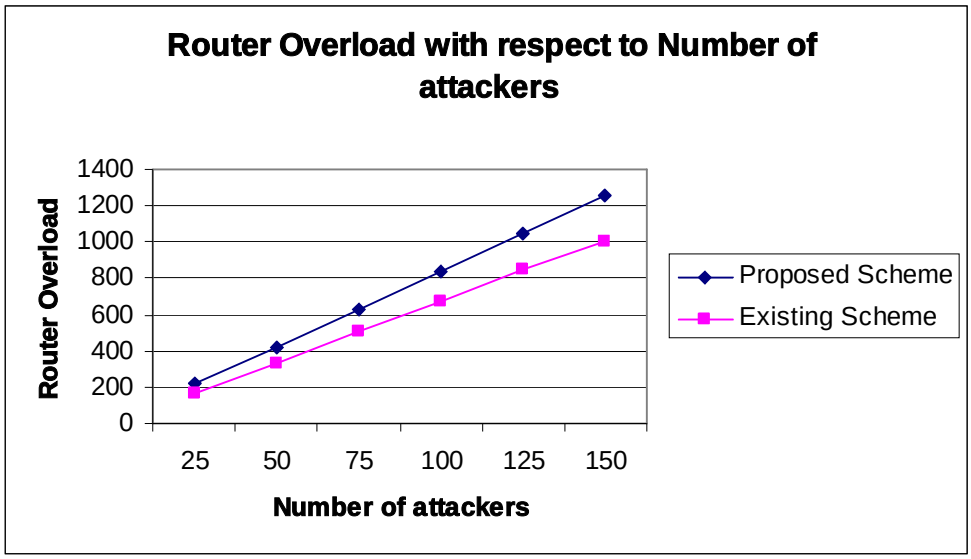

Figure 13: Router overload with respect to Number of attackers.

Case iii:

The final performance is studied based on the proportion of attackers with number of packets to get the trace and router overload. The proportion is divided, based on the general internet traffic and the performance is good compared to the existing scheme. The performance is shown in figure 14 and figure 15.

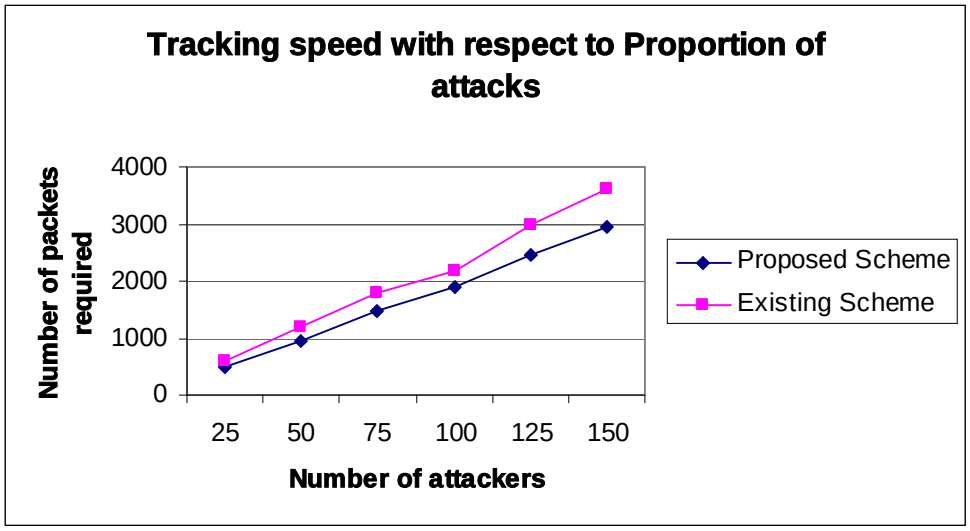

Figure 14: Tracking speed with respect to Proportion of attackers.

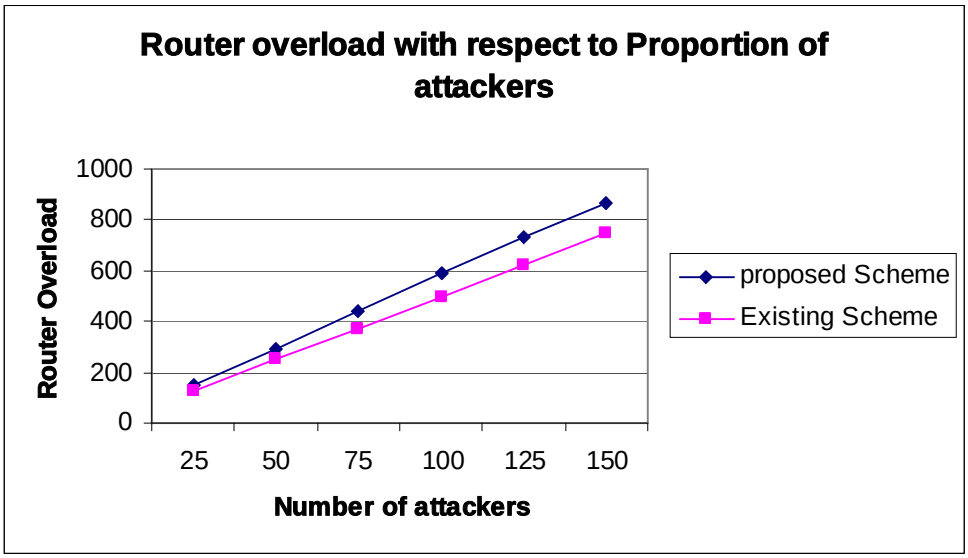

Figure 15: Router overload with respect to Proportion of attackers

The same sets of experiments are going to be carried out in future with different probability function and performances are going to be studied.

CHAPTER 4: CONCLUSIONS

The approach was implemented with various set of functions and hop-counts to compare the number of packets required to get the trace and the router overload. The results from the simulation are shown in the graphs. From the graphs shown the proposed approach is of high advantage with less number of packets to get the trace and the router overload for that speed of detection is much less than the existing schemes. As a future work, optimization of the probability function needs to be studied in order to increase the performance more.

REFERENCES:

[1] http://www.northernwebs.com/bc/bc10.html#_Toc375028391 date accessed May 15, 2005.

[2] http://world.std.com/~franl/worm.html date accessed May 15, 2005.

[3] http://csrc.nist.gov/publications/nistir/threats/subsubsection3_3_2_1.html #SECTION00321000000000000000 date accessed May 15, 2005.

[4]http://iwsun4.infoworld.com/articles/hn/xml/01/05/23/010523hndosrep.htmldate accessed May 15, 2005.

[5] http://www.juniper.net/products/integrated/dos.pdf date accessed May 15, 2005.

[6]http://security.ittoolbox.com/browse.asp?c=SecurityPeerPublishing&r=%2Fpub%2FDN052603.pdf date accessed May 15, 2005.

[7] http://ee.tamu.edu/~reddy/ee689_04/lec2.pdf date accessed May 15, 2005.

[8] http://www.garykessler.net/library/ddos.html date accessed May 15, 2005.

[9] http://www.techexams.net/technotes/securityplus/attacks-DDOS.shtml#udpflood date accessed May 15, 2005.

[10] http://www.peapod.co.uk/radware-defensepro-faqs.htm date accessed May 15, 2005.

[11] http://support.loxinfo.co.th/security.asp?where=security/nukes date accessed May 15, 2005.

[12]http://dslab.csie.ncu.edu.tw/93html/paper/pdf/IP%20Traceback:A%20New%20Denial-of-Service%20Deterrent.pdf date accessed May 15, 2005.

[13]https://users.cs.jmu.edu/aboutams/Public/IP%20TraceBack/Background%20on%20traceback.pdf date accessed March 08, 2005

[14]. http://www.niscc.gov.uk/niscc/docs/re-20021025-00481.pdf?lang=en date accessed March 08, 2005

[15]. http://www.windowsitpro.com/Article/ArticleID/20559/20559.html date accessed March 13, 2005.

[16].http://www.i2r.astar.edu.sg/icsd/publications/HenryLee_2003_iscc_ip_traceback.pdf date accessed May 15, 2005.

[17]S. Savage, D. Wetherall, A. Karlin and T. Anderson, "Practical network support for IP traceback," in *Proc. of ACM SIGCOMM*, Aug.2000, pp. 295-306.

[18] K. Park and H. Lee, "On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack," in *Proc.of IEEE INFOCOM 2001*, Mar. 2001. pp. 338-347

[19]http://www.cs.mu.oz.au/~tpeng/mudguard/research/pisa-conference.ppt#301,7, Probabilistic Packet Marking [Savage 00]

[20] A. Belenky and N. Ansari, .IP traceback with deterministic packet marking, *IEEE Communications Letters*, vol. 7, no. 4, pp. 162.164,April 2003.

[21] B. Duwairi, A. Chakrabarti, and G. Manimaran, "An Efficient Packet Marking Scheme for IP Trace back," *in Proc. of Networking 2004*, Athens, Greece. pp. 1263–1269

[22] D. Basheer and G. Manimaran, "A novel packet marking scheme for IP traceback", in Proc. 10th IEEE *Intl. Conf. on Parallel and Distributed Systems, Newport Beach (CA), USA*, July 2004.pp 195-204

[23] http://www.nlanr.net/NA/Learn/wingspan.html date accessed March 10, 2005.

[24] http://www.eecs.umich.edu/techreports/cse/2003/CSE-TR-473-03.pdf date accessed March 10, 2005.

VITA

RADHAKRISHNAN GOPALSAMY

Candidate for the Degree of

Master of Science

Thesis: HOP-COUNT SENSITIVE MARKING PROBABILITY IN PROBABILISTIC PACKET MARKING
Major Field: Computer Science

Biographical:

Personal Data: Born in Tamilnadu, India.

Education: Received Bachelor of Engineering in Information Technology from Sastra University, Thanjavur India in may 2002.Completed the requirements for the Master of Science degree with a major in computer Science at Oklahoma State University in July 2005

Name: Radhakrishnan Gopalsamy Date of Degree: July 2005

Institution: Oklahoma State University Location: Stillwater, Oklahoma

Title of Study: HOP-COUNT SENSITIVE PACKET MARKING IN PROBABILISTIC PACKET MARKING

Pages in Study: 32 Candidate for the Degree of Master of Science

Major Field: Computer Science

Scope and Method of Study:

The scope of the finding has more efficiency in terms of cost and time. Various other methods are studied in order to achieve the proposed scheme.

Findings and Conclusions:

Denial-of –Service attack has emerged as a great threat to the Internet. Trace back is the scheme that is used to get Denial of Service attacker. Various trace back schemes have been proposed by others. The draw back in the existing schemes is router overload and takes a long time to get the trace. This happens because of maintaining constant marking probability. The new scheme proposed is "Hop count sensitive marking probability in probabilistic packet marking." In this approach marking probability is calculated based on the Hop count. So a variable marking probability is maintained. Having variable marking probability minimizes router overload and fastens the trace back process. This method is of great advantage to the critical services. The performance of the method is studied by simulation.

ADVISER'S APPROVAL: Dr.Venkatesh Sarangan