ISP Identity Based Secure Single Packet IP Traceback

MS Research Dissertation

By

Nabila Akram

(435-FBAS/MSCS/S08)

Supervised By:

Prof. Dr Muhammad Sher

Chairman, Department of Computer Science

International Islamic University

Islamabad

Co-Supervised By:

Mr. Zeeshan Shafi Khan

Department of Computer Science

Faculty of Basic and Applied Sciences,

International Islamic University, Islamabad

2010

1- Internet service provider.

7.3.11

A Dissertation submitted to the

Department of Computer Science

International Islamic University Islamabad

As a partial fulfillment of requirements for the award of

The degree of

MS in Computer Science

International Islamic University, Islamabad

Dated: ----------

Final Approval

It is certified that I have examined the thesis titled "ISP Identity Based Secure Single Packet IP Traceback" submitted by Nabila Akram, Registration No: 435-FBAS/MSCS/S08, and found as per standard. In my judgment, this research project is sufficient to warrant it is acceptance by the International Islamic University, Islamabad for the award of MS Degree in Computer Science.

Committee

External Examiner
Dr Abdul Jalil
Head Department of Computer & Information Sciences
Pakistan Institute of Engineering & Applied Sciences
Islamabad

Internal Examiner
Mr.Qaisar Javaid
Assistant Professor
Department of Computer Science
International Islamic University
Islamabad

Supervisor
Prof. Dr. Muhammad Sher
Chairman, Department of Computer Science
International Islamic University
Islamabad.

Co-Supervisor
Mr. Zeeshan Shafi Khan
Senior Researcher, King Saud University
Riyadh Saudi Arabia

zeeshan shafi

Dedicated to

My respected Teachers, Family Members and Friends

Declaration

I hereby declare that this work, neither as a whole nor as a part has been copied out from any source. It is further declared that I have conducted this research and have accomplished this thesis entirely on the basis of my personal efforts and under the sincere guidance of my supervisor Prof. Dr Muhammad Sher and my Co-Supervisor Mr. Zeeshan Shafi Khan. If any part of this project is proved to be copied out from any source or found to be reproduction of some other project, I shall stand by the consequences. No portion of the work presented in this dissertation has been submitted in support of any application for any other degree or qualification of this or any other university or institute of learning.

nabila

Nabila Akram

(435-FBAS/MSCS/S08)

Acknowledgement

All praise to Almighty Allah who has all the names, and who need no name the most generous, considerate, and compassionate who has blessed mankind with this verdict to think, explore, to learn and discover the hidden secrets of this universe and helped me to broaden the veils of my thought and enabling me to get through the difficulties indulged during this project. Also admiration to our beloved Prophet Muhammad (PBUH) who is always a great source of inspiration of divine devotion and dedication to me.

I would cordially pay my special appreciations and whole heartedly considerations to my reverend supervisors Prof. Dr Muhammad Sher and Co-Supervisor Mr. Zeeshan Shafi Khan for their endless support, guidance and coordination while conducting this research. I owe them a great respect and honor and I am privileged to work under their supervision. It was their efforts, courage, moral support and endeavoring attitude that helped me to get through any problem or difficulty during each step of this project.

I would also like to pay my gratitude to all my respected teachers making me capable of what I am today due to their guidance and help.

Thanking my friends for always being there for me whenever I needed them for their help, generosity and moral support.

Finally my beloved parents and family who deserve the credit more than I could ever express for always being completely supportive to me. They have been a constant source of advice, Love and devotion to me. From moral to financial they have been blessing me with all the support that I have needed up till now in my life.

I express my countless appreciation to all the people who have helped me during achieving this MS degree and hope to have this honor that they would walk along me through out my life

Nabila Akram

Project in Brief

Project Title:	**ISP Identity Based Secure Single Packet IP Traceback**
Undertaken By:	**Nabila Akram**
Supervised By:	**Prof. Dr Muhammad Sher**
Co-Supervised By:	**Mr. Zeeshan Shafi Khan**
Start Date:	**January 2009**
Tools and technologies:	**Network Simulator 2**
Documentation Tools:	**MS Word, EDraw, MS Excel**
Operating System:	**MS Windows XP professional**
System used:	**Pentium 4, 1.73 GHz**

Abbreviations Used

Abbreviations	Acronyms
ISP	Internet Service Provider
IP	Internet Protocol
DDoS	Distributed Denial-of-Service
DoS	Denial of Service
Pi	Path Identification
SIPT	Speedy IP Traceback
ICMP	Internet Message Control Protocol
SYN	Synchronization
NDPM	Novel Deterministic Packet Marking
ADDPM	Across Domain Deterministic Packet Marking
BGP	Border Gateway Protocol
OMNET	Objective Modular Network Tested

AS	Autonomous System
MAC	Media Access Control
LDPM	Logging and Deterministic Packet Marking
ERFIT	Edge Router-Based Fast Internet Traceback
TOS	Type Of Service
TTL	Time to Live
HTTP	Hyper Text Transfer Protocol
NS2	Network Simulator

Abstract

A best effort delivery, unreliable, connectionless protocol that works at the network layer is known as Internet protocol (IP). IP Spoofing is a technique that is used to gain unauthorized access to a computer. Most of the attacks on networks are launched through spoofed IP addresses i.e. Denial of Service attack. Attacker spoofs IP address of legitimate client, sends many useless packets to the victim and acts as a legitimate user. Since the attacks are launched through spoofed IP addresses therefore it is very difficult to identify the source of the attack (Attacker). The researchers introduce a technique to identify the origin of the spoofed user. This technique is known as the IP Traceback. Many Traceback techniques are introduced but all have few drawbacks. Some increases the network load and delay, few requires implantation on all the routers of the world, few compromise on privacy of the user. Many techniques do not guarantee single packet IP traceback.. All the existing IP traceback techniques require an efficient marking technique. We, in this research work, will introduce a new single packet IP tracback technique which will reduce the network delay. Moreover it will not require any marking technique. Private information of the users will remain private. This technique will only be implemented on the ISPs of the world instead of all the routers of the world. Simulation will be done in NS2.

Table of Contents

List of Figures

1: Introduction

1. Introduction

Internet Protocol (IP) is a protocol used for transferring data between computers over the internet using internet protocol suit also called TCP/IP. In the internet layer IP is the primary protocol of the internet protocol suit. Each computer over the internet must have one IP address, used for its identification over the internet. During transmission message is divided into packets, when packet is received by destination it contains both source IP address and destination IP address.

First the packet is sent to the gateway computer that reads the destination address and sent packet to the next gateway. Next one also reads the destination address, same procedure takes place across the internet until one gateway identify that this address is similar to its immediate neighborhood. At the end gateway forward this packet to that computer whose address is similar to this address. IP is a connectionless protocol, used by layer 3 the network layer in OSI model, IP datagram is a heart of the IP.

IP has two versions, IPv4 and IPv6. IPv4s is the most widely used i.e. IP header. IPv6 is the latest version of IP, also called "IPng" (IP Next Generation) designed as an enhancement in IPv4. IPv6 describes rules for unicast addressing; anycast addressing and multicast addressing also includes the capabilities of IPv4. The server that supports IPv6 packet must supports IPv4 packets. A 32 bit address system is offered by IPv6, this address system allows for more than 4 billion unique addresses

IP is the only best effort protocol because it makes best effort to transmit a packet; the service provided by this is characterized as unreliable. Direct link to the recipient is not established itself by IP, however it is established by TCP/IP. To communicate across any interconnected network as well as for LAN and WAN communication IP can be used that is why IP is the world's most popular open system protocol.

Because the nature of the internet and of the business networks is changed according to the time, so the current IP is the backbone of the TCP/IP networking is becoming obsolete. Data is encapsulated as packets from an upper layer protocol.

To resolve IP addresses to data link addresses in every link layer implementation its own method of addressing is used and Address Resolution Protocol (ARP) for IPv4 and Neighbor Discovery Protocol (NDP) for IPv6 is used for handling this address resolution.

Due to lack of reliability data corruption, lost data packets, duplicate arrival and out-of-order packet delivery events can occur. Upper layer protocol is responsible for solution, if any of these reliable issue occurs i.e. upper layer have to cache data until it can be passed to the application in case of in-order delivery.

To ensure that at the routing nodes IP packet header is error free through the computation of a checksum, assistance is provided by IP in version 4 (IPv4). Due to this the packets are discarded with bad headers and no notification is required to be sent to the end node. To resolve this problem Internet Control Message (ICMP) protocol is used.

For the benefit of rapid forwarding through the routing elements IP header checksum is used by IPv6 in the network. During transmission of the packet, a fix size of the packet is very important factor. The packets are transmitted through different route across the internet, so the packets can be reached in different order then the order in which they were sent. IP just delivers the packets; the TCP/IP is responsible to put the packets back in the right order.

1.1 IP Header

IP header is a network layer protocol consists of the information about the packet which is helpful during the transmission of the packet. Length of the IP header is 20 bytes. Using routers a datagram service is used by IP to transfer packets of data between end systems. For added optional bytes an option exists in the IP header which is not normally used.

1.1.1 IP Header Fields

It has 12 fields, each of which is used for multiple purposes.

- **Version**: This field shows that which version of the IP header is used. Both sending and receiving networks must be the same IP version. Normally it represents 4 bits which means IPv4 is used.

- **Type of Service**: This field contains 1 byte. It defines that which type of service is used by data during transmission through a particular network.e.g. Precedence, Delay, Reliability, Throughput, Cost and also defines priorities. A three way tradeoff is a major choice which is between low delay, high reliability and high throughput. The cost of the service may be increased by the use of the delay, through and reliability indications.

- **Header Length**: This field contains 4 bits, represents the length of the IP header which is 32 bit words and the minimum value for the correct header is 5.

- **Total packet Length**: Total packet length is the combination of IP header, TCP header and data. This is measured in octets, length of the packets to be up to 65,535 octets. But all hosts are not able to accept too large packets because they are prepared to accept packets of up to 576 octets, only those hosts are allowed to send packets larger than 576 octets, which have assurance that the destination is also able to accept the larger packets. 576 octets is a reasonable size of the packet, in which 512 octets are of data block and 64

are header octets. A typical internet header is 20 octets and a maximal internet header is 60 octets.

- **Identification**: If the size of the given packet is larger than the normal size then network breaks packet into multiple sub packets then identification number is used to identify each packet. This field contains 2 Bytes. For assembling the fragments of a datagram an identifying value is assigned by the sender. This field is used for multiple purposes e.g. for adding packet tracing information to datagrams which helps to trace back datagrams with spoofed source addresses.

- **Flags**: Flag is a 3 bit field and is used to identify and control fragments, which are in order, from high order to low order. Reserved, Don't Fragment (DF) and More Fragments (MF). The packet will b dropped when to route the packet fragmentation is required and DF flag is set. During packet fragmentation except the last fragment all fragments have MF flag set. Last fragment does not have the MF flag set. An unfragmented packet is its own last fragment, those packets that are not fragmented on those packets the MF flag is not set.

- **Fragmentation offset** : Fragmentation is used for large packets. When fragmentation lost then there is need to retransmit the packet so it is better to avoid fragmentation. In his field 13 bits are used for offset. When these packets are received by the destination then all these sub packets are reassembled using identification number, Flags and the fragmentation offset. This complete packet is then transferred to transport layer .This field specifies the offset of a particular fragment, the fragment which is relative to the beginning of the original unfragmented IP datagram, the first fragment has an offset of zero.

- **Time to Live (TTL):** TTL is decremented at each node to avoid from loops on an internet and in internet header processing it is modified. This is 1 byte field identify the life of packet and limits the lifetime of a packet. When value of the packet reaches to zero

and the packet still not reached to the destination then this packet is discarded. After this an ICMP message is sent back to the sender that it has been discarded. This field is specified in seconds, if time intervals are less than 1 second are rounded up to 1.

- **Header Checksum:** This field is 2 byte long, contains the value which is obtained by calculating the checksum. For error-checking of the header checksum this field is used, the checksum of the header is compared to the value of this field at each hop. If this value is not matched then packet is discarded. The receiver for conformation also use this value and apply checksum by taking the sum of 16 bit words, if digits are greater than 16 bit number add them to the sum. Checksum will have to be recomputed at each hope when TTL is decremented and fragmentation is possible at each hope. The value of the checksum field is zero for computing the checksum.

- **Protocol:** This field contains 1 byte it specifies the next level protocol. In the data portion of the IP datagram the protocol is used. In Internet Assigned Numbers Authority a list of protocol numbers is maintained.

- **Source IP Protocol Address**: This field identifies the IP address of the source. This field contains 4 bytes. The address of the sender is confirmed through network address translation NATing machine and reply packets sent by the receiver are routed to the NATing machine. This translates the destination address to the actual senders address.

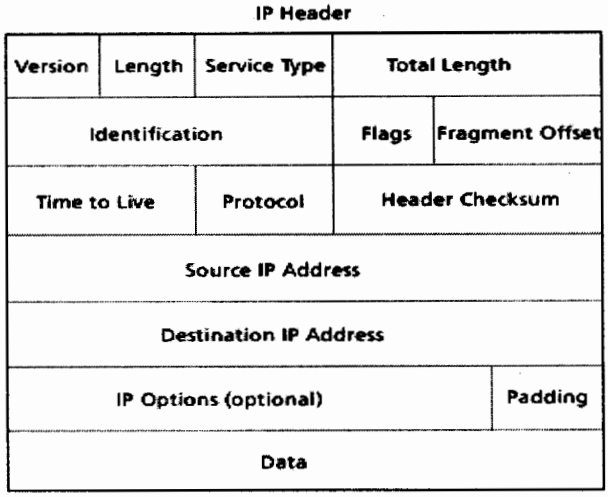

Figure 1.1: IP Header

- **Destination IP address**: This field identifies the IP address of the destination and is similar to the source IP address. Routing is based on the destination address. This field contains 4 bytes.

- **IP Option**: This field is used for testing and debugging and may appear or not in datagrams. IP option is variable in length may be zero or more options. In all datagrams the security options may be required, options must be implemented by all modules e.g. host and gateways. If padding is required make it into 32 bit words. In the format of an option there is a single octet of option type in case one and an option type octet, the actual option data octets and an option length octet in case two.

1.2 IP Spoofing

IP Spoofing is a technique that is used to gain unauthorized access to a computer e.g. source routing, Blind spoofing, Flooding and Man-in-the middle. IP spoofing is also known as IP address forgery or a host file hijack. Hijack is a technique in which cracker (attacker) conceal its

identity acts as a trusted host and spoof a web site then hijack a browser (access a network). Most of the attacks on the internet are launched through spoofed IP addresses of the user. Attacker spoofs IP address and sends messages to the victim and act as a legitimate user [1]. Because the attacker spoofs the IP address so it is very difficult to identify the origin of the attack. Mostly IP spoofing is used to launch Denial of service attacks. In IP spoofing an attacker first access the IP address of the legitimate client by using different techniques then modify the header of the packet and appears as the packets are coming from the true host.

1.2.1 Spoofing of an IP Datagram

A packet which is sent over the internet in a connectionless manner is called IP datagram.IP packets are created for the user behind the scene and are used in application that uses the internet for the communication. IP packets have both source and destination addresses which are must for the communication of the data and there is a header in the operating system for IP datagram. A header in a packet can be modified by inserting a custom header. After inserting a custom header must inform the operating system that packet has no need of the header. To send spoofed IP datagrams raw sockets in UNIX like systems and packet drivers such as WinPcap on windows can be used.

1.2.2 Why spoof the IP Source Address?

When the sender has some malicious packets and he wants to send them without any identification then he send spoofed packets. To trace the location of the sender the source address is used which is present in the header of an IP datagram. To maintain the security some systems keep logs of the internet activity. Due to this when the attacker hides their identity then systems change the source address. The spoofed packets received by the host in return the host replies to the spoofed address. Because the source address is changed so the attacker receives no reply, however attacker can sniffs the reply if spoof address and host are on the same subnet.
There are some reasons to spoof an IP packet.

- **Scanning**

An attacker wants to establish a connection with the host for the purpose of gathering information about the applications on the host e.g. open ports and operating system. When a victim host replies to the source address during this attacker can gather information about the system i.e. open ports, the operating system and some other application running on the open ports.

- **Sequence-Number Prediction**

When a TCP connection is established between two parties and the packets exchanged between these two parties consists of sequence numbers for data and acknowledgments. These sequence numbers helps to determine out-of-order and lost packets. Hence packets are delivered to the application layer reliably. To determine the algorithm which generates these sequence numbers an attacker might send several spoofed packets. Hence using this information attacker gets the information about an existing session.

- **Hijacking an Authorized Session**

When an attacker who is able to generate a sequence number, sends a message for reset to a party in a session and informs the legitimate party that session has ended. When one party close the session and offline then an attacker use the IP address of that party and connect to the other party which is still online. Hence an attacker can easily attack on that party by sending malicious packets and act as a trusted host.

- **Determining the state of a Firewall**

A firewall is used to protect the network from the different types of attacks. When packets entered into the network are checked by the firewall against an Access Control List (ACL).

1.2.3 How IP Spoofing is carried out

The creation of the TCP/IP packets by using the IP address of anyone is a spoofing. A TCP connection is established between client and server. It is a three step process which is known as three way handshakes. In first step client sends SYN message ask to the server that it wants to establish the connection .Client sets its Initial Sequence Number (ISN) in its TCP header .In

response server also sends its own Initial Sequence Number and acknowledgment of user's first message, then client sends acknowledgment to the server that ISN is being received. After establishment of connection then transformation of data takes place.

To choose a Sequence Number is very important. When a machine boots its ISN initialized it to 1.If no connection occur ISN is incremented by 128,000 every second. If connect () issued counter is incremented by 64,000.

After choosing a sequence number here attacker launch the attack act as legitimate host and disabled legitimate host by SYN flooding attack, made an attempt to establish the connection by guessing the sequence number.

The Packets which are forwarded by the server are received by the attacker, these are forwarded to the host but host is not able to response the server (attacker damage host by DoS attacks), instead of host, attacker response to the server with spoofed packets. If by chance host is able to response to the server then the attacker immediately tear down the connection. To ensure this attacker wait till the host completely down.

1.2.4 Spoofing Attacks

There are a few types of attacks that successfully employ IP spoofing.

- **Non-Blind Spoofing**

When subnet of victim and attacker becomes same then this type of attack takes place. The attacker sniffs the sequence and acknowledgment number and eliminates the power of server to calculate them accurately. During transformation of data between host and server, attackers corrupt the data stream and re-establish the new connection itself.

- **Blind Spoofing**

In blind spoofing there is no need to see responses; it is an integral part of many network attacks. In this attack sequence and acknowledgment number are unreachable to the server. Attacker

sends several packets to the targeted user with sample sequence number. In the past it is easy to detect sequence number but now it is difficult because most operating systems implement random sequence number generation which makes it difficult to detect sequence number. In this attack, attacker add necessary data to a system (i.e. *create* a new connection) act as a legitimate user and easily access to the server.

- **Man in the Middle Attack**

The forms of a common security violation are non blind spoofing and blind spoofing called Man in the Middle (MITM) attack. When two true parties communicate to each other and a malicious party interrupts them in this attack, the communication flow is controlled by a malicious party. Then the data which is sent by a true sender is modified by the malicious party without any knowledge of the original sender or recipient. Hence the attacker spoofs the identity of the actual sender and discloses the confidential data of the victim.

- **Denial of service DOS attacks**

To defend against DOS attack what is currently the most difficult attack, for knowing this IP spoofing is used. Attackers attack with the concern of to waste bandwidth and resources of the server, they flood the victim by sending large amount of packets in a short amount of time. Attackers trace and stop Denial of services by spoofing source IP addresses and maintain the effectiveness of the attack. When multiple attackers send spoofed traffic then it is very difficult to block this traffic immediately.

- **Misconception of IP spoofing**

Session hijacking for host based authentication services and some of other attacks are a bit outdated. In network scanning as well as denial of service floods the IP spoofing is still prevalent. During the use of the internet i.e. during chatting, sending e-mail etc, IP spoofing can hide IP address is a common misconception Due to the forging of source IP address the result will be misdirected and you can't create a normal connection.

- **E-mail address spoofing**

In this type of spoofing the information about the sender is present in the e-mail, which can be easily spoofed by the attacker. In this technique spammers hide the actual e-mail and create the problem e.g e-mail spam backscatter etc.

- **Referer spoofing**

In referer spoofing there are some of the websites commonly pornographic paysites, these websites allow for the access of certain pages which are approved. This technique enforces for checking the referer header of the HTTP request and also allows the users to gain unauthorized access to the materials.

1.2.5 Countermeasures for IP Spoofing

In countermeasures for IP spoofing it is explained that how to detect spoofed IP packets and then how to trace them back to the originating source. In the detection of the spoofed IP packets support of routers, administrative control and host based methods are required. For tracback of IP packets in routers special traceback features are used.

- **Detection of spoofed packets**

Spoofed packet detection is started at layer 2. With the IP source guard feature switches match the MAC address of the host with the Dynamic Host Configuration Protocol (DHCP). Those packets are dropped that don't have the correct IP address for that particular MAC address. Hence the ability of the host through which it is connected to the switch and sends packet to the neighbors is limited. When there is a single IP address for multiple interfaces then IP Guard features works well. When for multiple IP addresses one interface is assigned this may cause a problems, with Network Address Translation (NAT) occurs the same problem. In NAT problem hosts might get different IP addresses several times.

Routers at layer 3 know that a network is connected with which interface. Routers also know that what network addresses can be expected which will come from that network. It is identified that a packet is a spoofed packet when an outgoing packet does not have the network address of that

interface from this it belongs. This packet is stopped by the router at that point. For incoming packet same technique is used, when for an interface a packet is destined and that packet's source address and interface belongs to the same network then it is identified that packet is a spoofed packet. But this technique is not helpful when the IP address of the host is spoofed by the attacker on the same network.

- **Check the Time to Live (TTL) value of the packet**

In this method a request is send to the spoofed host after checking the TTL value of the packet. TTL value of the both packets is compared after the reply. Mostly TTL value is not matched; however it can be matched in some situations.

- **Tracing Spoofed IP packets**

For tracing IP spoofed packets IP traceback technology plays an important role. IP traceback is a technique that is used to trace a spoofed user (source of the attack). There are two methods for tracing IP spoofed packets

1) Hop by hop traceback
2) Logging of suspicious packet

In hop by hop method Internet Service Provider (ISP) involved and is useful only when flood is ongoing. When a node found that it is a victim of the flood attack informs the ISP. The router which is sending this stream to the victim ISP determine from that router, this router determine from next router and so on. Hence this process is reached to the source of the flood attack.

In logging of the suspicious packet method a router maintains a list of those IP addresses which are in interface. When router found the packet which is not belongs to the address range for its interfaces then router logs the packet as a suspicious.

- **Conclusion**

IP spoofing related to IP packet structure so it is very difficult to handle this problem. IP spoofing can be done through different methods and to find the source of the attacker is very difficult because attacker hide the origin.

1.2.6 Defending Against Spoofing

There are a few precautions that can be taken to limit IP spoofing risks on network, such as

- **Filtering at the Router**

To defense against Spoofing attack implement Ingress and Egress filtering on border routers. To block private IP addresses on downstream routers implement ACL (Access Control List). This spoofing technique is used to cheat firewalls and those addresses which are in your internal range should not accepted by this interface as a source. The source addresses which are out of valid range are restricted on the upstream routers. This restriction helps to prevent from sending spoofed traffic on the network.

- **Encryption and Authentication**

Spoofing threats also can be reduced by implementing encryption and authentication techniques. The features of encryption and authentication techniques are included in IPV6 which are used to remove spoofing threats. On the same subnet all host based authentications measures which are common for machines are eliminated. In this technique it is must ensured that all authentication measures are carried out on encrypted channel and are in place.

- **Conclusion**

There is no easy solution for IP spoofing; it is inherent to the design of the TCP/IP suit. Many prevention methods are used which helps to understand how and why spoofing attacks are used, It also helps to prevent from different spoofing techniques.

1.3 Denial of Service Attack (DoS)

DOS attacks takes place on the internet. Attacker attacks on the victim in such a way that resources are unavailable to the legitimate users and the result is Denial of Services (DOS) between client and server. Attacker use spoofed source IP address due to which to find the origin of the attack packet is difficult. In distributed DOS attacks, attackers use multiple machines and send large amount of packets to the victim which greater than its capacity due to which the server is unavailable to response to the legitimate users [1, 4]. In DOS attacks, the attacker use packet floods and consume network bandwidth and server resources, force to the legitimate client to reset the system and prevent you from accessing web sites, e-mail, online accounts and other services .

For example when you want to access any site you must type the URL of that particular site into the browser means you are sending a request to the site's computer server. The server will process certain pages immediately and if an attacker overloads some requests to the server then the server is unable to proceed your requests and you can't access the site which you want. These types of attacks are DOS attacks in which you can't access anything.

1.3.1 Distributed Denial of Service (DDoS) Attacks

In Distributed Denial of Service attack an attacker may use any computer and attack on another computer hence attacker use multiple computers for attack and sends a large amount of data to the victim. Due to the weakness of the security an attacker take control of the computer and force the computer that sends a large amount of data to a particular website or sends spam to the specific e-mail address.

DDOS attacks are classified as follows

1.3.1.1 Network Resource Attack

In this attack attacker sends a large amount of useless packets to the server and waste the network bandwidth which is used to connect the server to the internet. Hence network bandwidth is wasted and packets of the user's are unable to reach to the server and hence there is no service between user and server.

1.3.1.2 Server Resource Attack

Server Resource attacks is classified as:

- **Server processing Attack:**

Like network resource attack, attacker sends many useless packets to the server to greater than its capacity. So the server is not able to process all these packets and force to drop the incoming packets, user's packets also dropped hence service between user and server is failed.

- **Server Memory Attack:**

There are some ambiguities in protocols through which attacker easily consume the server's memory.

1.3.2 Types of DoS Attacks

There are different types of DOS attacks. Which are as follows :

- **Smurf Attack**

Smurf amplifier is a computer network that is used in a smurf attack. Attacker spoof IP address of the victim and uses it as a source address and sends many ICMP echo messages to the IP address that broadcast addresses. Then this IP broadcast this message to all hosts that are in range of this IP address. These all hosts sends echo reply to the victim, because attacker use IP address of victim so it response to all hosts and the result is failure of service between client and server. To avoid this attack configure host and router in such a way that they can't broadcast ICMP echo request or configure router which can't forward the ICMP echo request to broadcast address.

- **Ping Flood**

In this attack attacker sends a large amount of ping requests to the victim. When victim reply these requests the result is no service between host and server. To prevent this problem use Firewall or victim not reply to these requests

- **SYN Flood**

When clients wants to establish a connection with the server, a three way handshake process takes place. Then Attacker sends many SYN messages to the victim and victim reserve resources for every request and sends acknowledgment to the client but client does not sends acknowledgment. The result is denial of services.

- **Nuke Attack**

In this attack attacker sends invalid ICMP packets to the victim and slow down the speed of victim.

- **Teardrop Attack**

In this attack attacker sends packets to the victim which are greater than normal size. When victim receive these packets reassemble them and the result is Operating system crashed.

- **Distributed Denial of service Attack (DDOS)**

An attacker uses multiple machines and sends many flood packets to the victim as a result bandwidth and network resources are consumed in large amount.

- **Bandwidth Attacks**

A host gives a particular amount of bandwidth to its website. When a user wants to load a website, website appears with some images and texts. Due to this it takes certain times to load and consumes some amount of memory. Every site has a particular amount of bandwidth which is given by its host e.g. 100 GB. If more visitors want to access the site and consume all 100 GB bandwidth then the host can ban the site. Similarly attacker can do the same thing. Attacker can access all pages and consumes all the bandwidth.

- **Logic Attacks**

In Logic attacks vulnerabilities in network software can be destroyed i.e. web server.

- **Protocol Attacks**

Protocol attacks exploit the specific features of some protocols at the victim server. They consumes the excess amount of the victim available to its resources that why they are installed at the victim side.

- **Peer to peer Attacks**

Peer to peer attacks are performed on the same network. At one side the client initiates the attack and damages the client which is on another side of the same network. Peer to peer attacks are used to gain sensitive data files, passwords, password files and registry data.

- **Reflected Attacks**

In distributed reflected denial of service attack (DRDoS) attacker's attacks through forged requests .Attackers send forged request in a very large amount to the computer that replies to the requests. In this attack the source address of the victim is set as a target, for this internet protocol spoofing is used. Hence all replies go to the targeted victim.

- **Permanent denial of service Attacks**

  This type of attack damages the system in such a way that it requires reinstallation of hardware or replacement called loosely as phlasing. It is a pure hardware targeted attack so it can be much fast.

1.3.3 Side Effects of DoS attacks

- **Backscatter**

Side-effects of the spoofed denial of service (DoS)attack is a Backscatter in computer network security . In backscatter an attacker spoofs the IP address of the user and sends malicious packets to the victim and act as a legitimate client, the victim can't differentiate between the legitimate packet and the spoofed packet. The victim responds normally and these response packets are called backscatter.

1.3.4 How to prevent DoS Attacks?

There is no way to hundred percent secure from the DoS attacks, but there are some preventions which helps to avoid from DoS attacks

a) Keep yourself updated with the latest security patches.
b) Allow only necessary traffic.
c) Monitor the traffic when there is a sudden rise in traffic. If it is coming from an unauthorized way then block the particular IP.

1.4 Routing of the IP packet

In routing of IP Packets, packets are forwarded from source to destination through a series of routers across multiple networks. When client sends packet to the nearest router, the router puts its own information in the identification field of the packet's IP header and sends packet to the next nearest router. The next router removes the identification field and puts its own information in this field and send to the next router. This process is repeated until the packet reaches to its destination. An attacker can attack by spoofing source address and act as a legitimate client i.e. Denial of service (DOS) attack. It is very difficult to identify the origin of the attack, because the attackers hide their origin.

Whenever a user wants to send some data to another user over the internet, the TCP/IP model plays its role. At the network layer the source and destination IP addresses are attached with the packet. At the data link layer frames are established by associating the MAC address of the source and the next hop. The physical layer converts the data into packets and route it to the next hop. The next hop changes the MAC addresses and TTL value and route it to the next hop and this process continues until the packet reaches its final destination.

To identify the origin of the attacker IP tracback technique is used. A technique that is used to trace a spoofed user (source of the attack) is known as IP traceback technique. If packet is an

attack packet, then the server (victim) reconstructs the path to find the origin of this packet. When a victim found that it's an attack packet then victim ask from its nearest routers that this packet is forwarded by which router. The router which is responsible sends reply to the victim and also asks from its nearest routers and so on. Hence the packet is traversed and reached to the place from where it was forwarded and then IP of the attacker is identified.

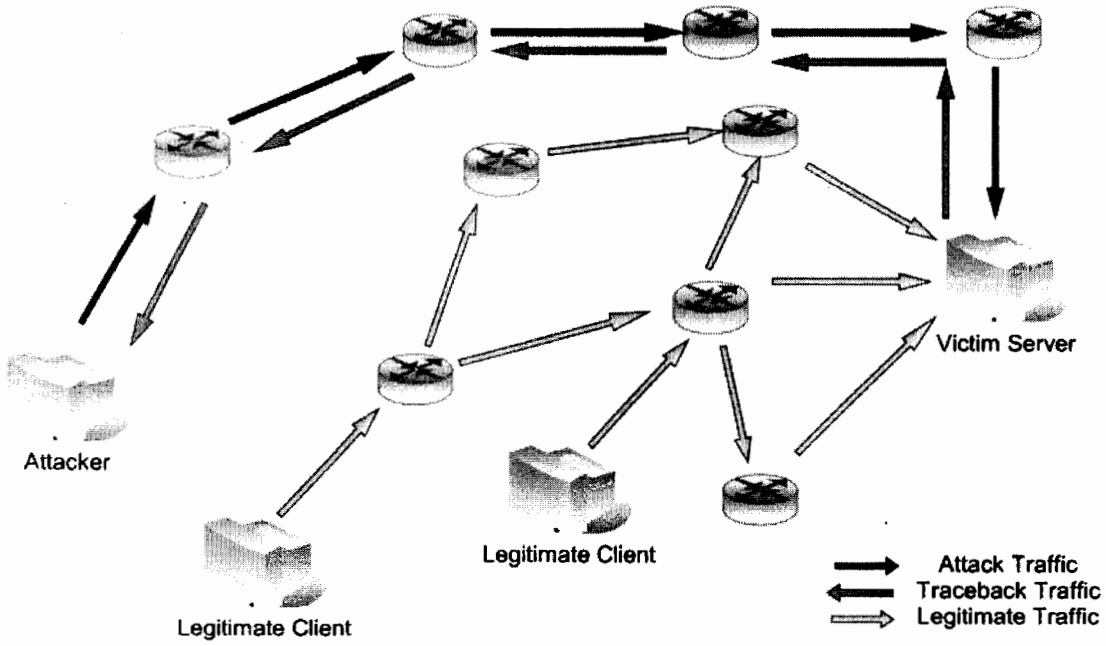

Figure 1.2: Routing of the IP Packet

1.5 Outline of the Thesis

The chapter 1 of this research dissertation is the introduction. In introduction the overview of IP spoofing is discussed in detail also the detailed discussion about the Denial of Service (DoS) attacks is given.

The chapter 2 is Literature survey; it includes the previous work of researchers who have worked in this area.

Chapter 3 is problem definition and research objectives; the problem on which this research focuses is studied in detail, research objective; includes the aims and scope of this research.

Chapter 4 is proposed solution and methodology; in this chapter we have designed the Internet Service Provider (ISP) Identity based IP traceback technique which is an efficient IP traceback technique, it reduces the network load and network delay also provides overall network security as well.

Chapter 5 is simulation results and discussion. In this chapter we have presented the results which we have formulated after implementation in the simulator NS-2.

Chapter 6 is conclusion and future work; in this we conclude our work and some future issues are given for future enhancements in this area.

Chapter 7 is references; it includes the list of those references which have been studied during this research work.

2: Literature Survey

2. Literature Surveys

Before starting a research in any field the survey of the related literature is a must job. So according to this we have also done the same work. By following the earlier work we have introduced a new idea. So for this purpose we have studied articles, research papers, thesis, books etc to determine what has been done in the field in which our problem resides.

Mostly attacks on the internet are launched through spoofing of the IP address called Denial of Service (DOS) attacks. Attacker uses multiple machines and sends the large amount of the data to a victim is known as Distributed Denial of Service (DDOS) attacks. To avoid from the Distributed Denial of Service attacks (DDOS) attacks researcher have introduced many techniques i.e IP Marking technique, IP Logging technique and ICMP trace back technique and many other techniques but still there are many problems i.e. to find the origin of the attacker. There is a lot of IP Traceback techniques have been presented by many authors; those which we have studied during our research are as follows.

Abraham et.al. have proposed a path identification (Pi) mechanism, this Pi mechanism helps to identify the source of the attack packets. During the routing of the IP packet when a packet reaches to a router, every router marks its information in identification field of IP header of the packet. After receiving the packet, if the receiving packet is an attack packet than a victim can use this information to identify the source of the attacker, also can filter incoming packets.

To increase the performance of Pi several methods used: IP address hashing, node omission and edge marking. TTL unwrapping used to protect marking mechanism. A model is established for DDOS attacks, threshold filtering method is used for the performance of marking mechanism by n = 1 bit n =2 bits. Pi is a powerful and flexible mechanism in reducing or removing DDOS attacks.

In this paper a good mechanism is described by the authors but the limitations in this paper are that for the implementation of this technique all routers of the world are involved and if any

single router is missed the solution will not be able to work out. To reconstruct the exact path a large number of the packets required as well as increases the overall delay and also not guaranty about accurate tracing.

Amit et.al. have presented a Speedy IP Traceback (SIPT) approach. In this SIPT approach boundary router picks the MAC address of the user (which may be legitimate client or attacker) and adds its own IP address and sends it to the next non boundary router. The next non boundary router without any change sends packet to the next router. When packet received by the server if it is an attack packet then by using MAC address victim can easily identify the attacker. It is concluded that SIPT approach is faster, has lower overhead on network and operates independently of the attack and continue until attacker traced back.

Limitations of this proposed solution are that privacy of the users is compromised. A good marking technique is required to code 80 bits into16 bits as well as the solution to handle the false claim is not discussed.

Shaoh et.al. have described a new approach called an edge router-based fast internet traceback (ERFIT) for IP trackback, ERFIT reduces the problems of Fast Internet Traceback (FIT) scheme. When packet received by the edge router then it is marked by choosing a fragment number and the relative hash fragment's bit and forwarded. Packet is marked by the all upstream routers.

Victim gathers information about ingress router during TCP connection by collecting unique hash fragment. Then scans all possible IP addresses and if any hash fragment is similar to the unique hash fragment then their IP addresses are added in the ingress router information list. If an attack packet is received by the victim then its hash fragment is compared with the hash fragments of ingress routers from the ingress router information list. If both are same then it will be attack packet and for the traceback procedure only ingress router is involved.

This research concludes that only ingress router involved for the reconstruction procedure and to start the Traceback process the less number of packets required, ERFIT can easily handle spoofing problem of PPM (FIT) approach and has low computational overhead and false positives packets during DDOS attacks.

The drawback of this packet marking scheme is that this scheme will be must implement on all the routers of the world. More packets required to start traceback procedure as well as overall delay increases.

Henry et.al. have proposed an ICMP Traceback technique with Cumulative path (ITrace-CP), which is an enhancement of the ICMP Traceback approach. Entire attack path information is encoded in the ICMP Traceback message. Trace-CP protocol and mechanism described for construction of ITrace-CP messages. To match the IP and ITrace-CP message IP Logging, IP Marking and ICMP Traceback (ITrace) are used. Researchers have concluded that ITrace-CP have marginal overhead in terms of storage and bandwidth and acceptable computational overhead. In simulation highlighted that this research performs well and takes less time to construct the entire attack path.

A good IP traceback technique is presented by the authors to solve the IP spoofing problem but the lack of this traceback technique is that during implementation all routers are involved.

Yi et.al. have introduced a deterministic link signature based DDOS IP traceback algorithm, which reconstructs the attack path immediately whether source addresses are spoofed or not. For validity verification it is implemented under IPv6 using OMNET++ simulation tool. Researchers have concluded that to reconstruct the attack path this algorithm is very efficient and accurate, and to start traceback procedure only single packet is enough.

In this technique the authors have described that to start the reconstruction procedure only single packet is enough but all the routers of the world are involved, so the network delay will be increased due to this. Overall this solution is a complex solution and practically this solution is not implemented in actual IPv6, only examples are described.

Qu et.al. have Presented a Novel Deterministic Packet Marking (NDPM) mechanism, In this method IP addresses and Autonomous systems (AS) are used for packet marking. When packet reaches to the BGP router, the router marks its information and writes 16 bit AS number into the packet. In this mechanism BGP router's information and AS number are combined and results are written in the verification field. This information helps for packet marking as well as packet filtering.

Conclusion of this research shows that it solves the problem of shortage of storage space through Overloading the offset field and TOS field. This proposed scheme has less overhead, all routers are not involved for the reconstruction procedure and this approach is extremely light weight for packet marking and also for packet filtering.

A good marking technique is required to convert 36 bits into 16 bits and this solution implements on all the routers of the world are the limitations of this technique.

Guang et.al. have described an across-domain deterministic packet marking (ADDPM) approach by reserving 30-bit space in IP header for fragmented traffic. The IP addresses of both source domain's ingress router and destination domain's border router are marked, through which victim can easily trace the origin of attack and filter packets. The researchers have concluded that ADDPM is more robust and provides an integrated defense framework for IP traceback and filtering.

The drawbacks of this research are that in IP header 30 bit space is reserved and there is no guaranty that all the ingress routers are safe as well as the attacker can write forged information in the packet.

WANG.et.al heve introduced a novel IP traceback approach which is based on Packet Logging and Deterministic Packet Marking (LDPM) which improves the IP traceback in several aspects. LDPM is easy to implement and this technique stores the complete identification information of a router into a single packet and for this purpose a new IP header encoding scheme is used by this technique, as well as this approach is also able to cope with thousands of attackers. At ingress sites the LDPM approach used as filtering criteria.

The authors have described that this proposed technique after receiving one attack packet starts the traceback procedure and identifies the origin of the attack packet easily. This proposed mechanism provides an integrated defense framework for IP traceback and by comparing this technique with previous techniques the authors have concluded that LDPM is a practical and more effective approach.

The limitations of this technique are that this technique is logging and packet marking based as well as the procedure to handle false claim is not defined in this research.

Andre Castelucio.et.al. have proposed an overlay network that is suitable for large scale networks. In this overlay network border gateway protocol update-message community attribute has extended as well as to remove ambiguities in the traceback path a new sequence marking process is introduced. In this proposed solution the route(s) which are followed by the attack packets are discovered and the traceback procedure operates only on the border routers of the autonomous systems.

The proposed system is autonomous system level traceback system and provides an efficient traceback mechanism during IP traceback procedure as well as also allows an incremental deployment.

The drawbacks of this research are that to implement this solution a marking technique required so also packet delay increased. If a receiver false claims that an attack is launched by a particular IP, so to handle this problem there is no solution in this research.

Macro et. al. have analyzed a light-weight single packet IP traceback system. Author described that this system is stateless and used a Generalized Bloom Filter (BGF) in packet IP header for the storage of traversed router information. Authors have concluded that this research is convenient for high speed network and instead of full IP address packets are marked with node digests during traversing the network. Simulation results show that this system locates the real attack path with high accuracy.

Ahmad et. al. have proposed a scheme which mixes in-band messaging (to include signaling information in forwarded packets) and out-of-band messaging (as a rescue) and used when first one is unusable. Authors have concluded that packet marking is used in this scheme as a primary technique with out-of-band signaling and using real IP traffic, simulation results of this approach are satisfactory.

Michael et. al. have presented a randomize-and-link approach which based on the probabilistic packet marking scheme. The conclusion of the proposed system is that it uses highly scalable large checksum cords to link message fragments. Associative addresses and data integrity verifiers serve for the cord. To produce an 80-bit message a single-phase randomize-and-link scheme is used with 12-bit checksum cord.

Chao et. al. have described a method to improve the scalability of log-based IP traceback by making an intelligent use of packet marking. The conclusion of this research is that a hybrid single-packet IP traceback approach is proposed based on packet logging and packet marking. Purpose of this research is that to collect the information of multiple routers through packet marking and packet logging.

K. Boudaoud. et.al. have proposed an efficient IP traceback scheme that is applicable in the real context of the internet. It is a set of an Autonomous system (AS) under the control of different administrative authorities. The efficiency of the traceback solution depends on the type of collaboration that is used between autonomous systems (ASs). Collaboration can be strong, weak or non-collaboration. Different methods are implemented with weak collaboration in each Autonomous Systems (AS). Simulation indicates that probabilistic logging is efficient when multiple packets coming from same source, with 80% of logging only 4 and with 60% 6 packets were sufficient.

Alireza izaddoost.et.al. have described a Traceback approach known as Intention-driven iTrace. This new approach is the working base of the ICMP traceback, this method provides useful information by introducing a new model through which the victim can easily identify the source of the attack. In this research paper researchers have been identified that when more effective ICMP traceback messages will be generated by the critical routers then the reconstruction procedure can be done easily and the origin of the attacker can be identify more correctly.

Chao Gong.et.al. have presented a new technique in which they have conducted a single packet traceback process in Autonomous System (AS) level under partial deployment of log based IP traceback mechanism and have investigated the effectiveness of single packet traceback. In this research the relationship between the success rate of finding out the attackers and the level of log based IP traceback technique have explored, as well as packet transformation and false positive rate have ignored.

Keisu.et.al have discussed in this research about to recover any failed traceback process by considering serial and parallel control schemes, to improve the end to end traceback success rate IP-TBS control schemes have discussed. Primary performance aspects have analyzed such as success rate load and latency of each control scheme. In this research it is suggested that to achieve a high end to end success rate, on the internet a large number of probes should be installed.

Marios.et.al have presented Connection Oriented Traceback in Switched Ethernet (COTraSE) which is logging based layer 2 system. This system allows for traceback of Ethernet frames. In this research the core algorithm has implemented and the data is used from available WAN traces. Whereas the algorithm establishes the origin switch and port for frames by correlating the MAC address entries and to detect potential errors classifies the return of each table lookup.

Yao Gang.et.al have introduced an efficient pre-traceback architecture for the survivor-path memory unit (SMU) of high constraint length Viterbi Decoder (VD).The target of this proposed architecture is wireless applications, furthermore the architecture is compared to the conventional traceback algorithm. As well as due to this architecture the memory read operations are reduced by 50%, survivor memory size and decoding latency also reduced by 25%.

Basheer.et.al have presented two schemes in this research by adopting a hybrid traceback approach. The idea behind first one scheme is to preserve the marking information at intermediate routers known as Distributed Link-List Traceback (DLLT). So by preserving the marking information can be collected efficiently. The second one is called Probabilistic Pipelined Packet Marking (PPPM) used for propagating packet marking information from one marking router to another, then it reaches to the destination.

Masafumi OE.et.al have proposed a hierarchical IP traceback architecture in which the internet-wide traceback procedure is decomposed into inter-domain traceback and intra-domain traceback, whereas this architecture is independent from a single IP traceback mechanism. Authors have also described in this solution that domain decomposition is based on the existing operational models of the internet. This hierarchical IP traceback architecture is designed as one of the countermeasure to the DDOS attacks, not only used for IPv4 network but also has the ability to used for IPv6 network.

Ken.et.al have described in this approach about the results of large scale demonstration experiments. These experiments were conducted in Japan with fifteen ISPs in 2009. During this all necessary issues have considered e.g. system performance, operational efficiency, management system's validity and system adaptability used to achieve widespread adoption.

2.1 Summary of the Chapter

Tracing the source of the attacker is an important and challenging issue on the internet. Earlier IP Traceback techniques provide different ways to traceback spoofed packets. We also are presenting a new IP traceback technique in this thesis. So before presenting our research we have read about earlier IP traceback techniques in this chapter which were related to our research.

3: Problem Definition

3: Problem Definition

Denial of service (DoS) attacks are carried out by spoofing the IP address of the user, so it is very complicated to detect the origin of the attack. To avoid from these DoS attacks there are multiple solutions presented in the existing IP traceback techniques. After studying and analyzing all these existing IP traceback techniques we have to conclude that there are some limitations.

Few techniques require a set of packets to start the traceback procedure. So they do not provide single IP packet traceback. Few techniques require implementation on all the routers of the world.

Now in this research thesis we have used the SIPT technique as the base to formulate our problem, because it is the latest available IP traceback technique. This technique has lot of limitations.

First it requires a marking technique that on one side marks the 80 bits (48 bits of user's MAC and 32 bits of gateway IP) into 16 bits (Length of the identification field) an on the other side regenerate the 80 bits from these 16 bits. Secondly since it communicates the MAC address of the user, which is the private property of the user so it compromise on the privacy issues. Thirdly it encourages the reflected attacks. A receiver may put a false claim that a user with a particular MAC address tries to launch in it. The author does not discuss any solution to this problem.

3.1 Problem Scenario

Some of the common problems which we have drawn from all the existing IP traceback techniques are as follows.

- ✓ Few techniques require implementation on all the routers of the world.
- ✓ Increase the packet delay.
- ✓ Many techniques do not guarantee single packet traceback.
- ✓ Require efficient marking techniques.
- ✓ Compromise the privacy of the users.

✓ No false claim handling.

3.1.1 Few techniques require Implementation on all the routers of the world

Few techniques require implementation on all the routers of the world [1,5,6].First it is not practical to implement the solution on all the routers of the world as it is very difficult to implement the solution on all the routers. Secondly if it is implemented then involvement of the every intermediate router results in higher network delay and more resources of the network are consumed, also put an extra load on the intermediate routers hence may results in congestion.

3.1.2 Increases the Packet Delay

When marking technique is implemented on all the routers of the world, every router takes some time to mark each of the incoming packets. e.g. If there are 100 routers involved during the communication of one packet and suppose that every router takes one neno second, so in 100 neno seconds one packet will reach to its destination, thus this procedure of marking introduces a great packet delay from source to the destination.

3.1.3 Many Techniques Do Not Guarantee single Packet Traceback

When a victim is attacked and as the attack prolongs to cause more and more damages then the victim tries to get rid off from these attacks. In order to do so the victim makes ways to identify the exact location of the attacker so to prevent the attack from prevailing. For this identification mechanism victim starts a traceback procedure. The existing IP traceback techniques require a set of packets to start the traceback procedure [1,4]. e.g. some of them requires more than two packets and some of them requires ten packets etc.

3.1.4 Require Efficient Marking Technique

The Speedy IP Traceback technique (SIPT) [2] is used to formulate our problem in our research. In this technique when client sends request to the boundary router, the boundary router picks MAC address of the user (which is of 48 bits) and its own IP address (which is of 32 bits) and convert them into 16 bits (Length of an identification field) and on the other side regenerate the

80 bits from these 16 bits. So to convert 80 bits into 16 bits and 16 bits back into 80 bits it requires an efficient, intelligent marking technique to do so.

3.1.5 Compromise the Privacy of the users

In Speedy IP Traceback Technique (SIPT) user's MAC address and boundary router's own IP address is converted into 16 bits which is an identification field in the IP header and forwarded the packet to the next non boundary router and so on. Hence the MAC address of the user is a private property of the user which is compromised on the whole network. Hence a user's privacy is compromised in this technique, which is itself a big drawback.

3.1.6 No False Claim Handling

The SIPT [2] also encourages the reflected attacks, if any receiver puts a false claim that a user with a particular MAC address tries to launch an attack on it. Then by using traceback procedure the suspected MAC address is identified and blocked. Hence in this existing traceback mechanism there is no solution to handle such types of false claims.

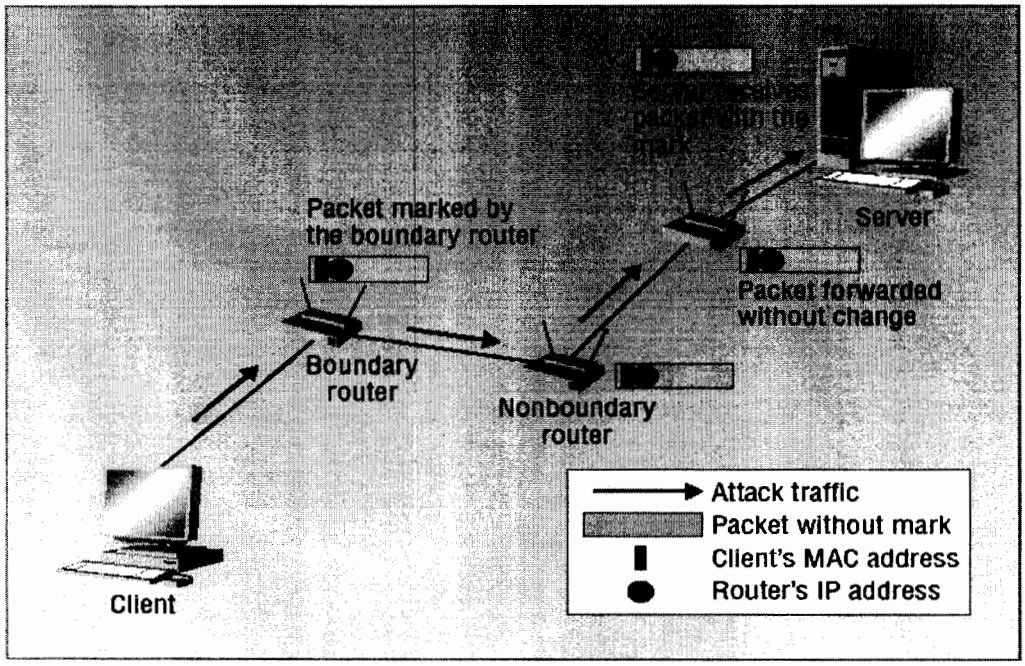

Figure3.1: SIPT approach using MAC address of the source [2]

3.2 Research Objectives

Objectives of the research represent the aim of the research and research may be for solving the problem. Every problem is solved by designing its solution and objectives are the basis of the solution design. The problems which we have discussed above, on the basis of these problems we have set some objectives. These objectives have fulfilled in our proposed solution in the next chapter. These research objectives are as follows.

Increase the packet delay.

- ✓ Increasing the overall Network Security.
- ✓ Providing an Efficient Service.
- ✓ Reducing the Network Load and Network Delay.
- ✓ Eliminate the Need of any Marking Technique.
- ✓ Easy Implementation.
- ✓ Stop Spoofed Routing.
- ✓ Minimizing the Loss.
- ✓ Improving the Network Performance.
- ✓ Occupying Less Network Resources.

3.2.1 Increasing the overall Network Security

The overall network security is increased by using the Internet Service Providers (ISPs). The objective of this research is to provide the complete security to the users during communication. If illegitimate client want to access the data of the legitimate client and attack on the receiver will be detected immediately and panelized by their own Internet Service Provider (ISP), hence the identification of the origin of spoofed users will add up in the overall security of all the networks.

3.2.2 Providing an Efficient Service

To provide an efficient and effective service to the users is the main goal of this research thesis. We have designed such a mechanism which mitigates the effect of Denial of Service (DoS) attacks by identify the origin of the attacker and stop the attacker from many more attacks.

3.2.3 Reducing the Network Load and Network Delay

Another objective of our thesis is to reduce the network load and network delay. We have designed an ISP based IP traceback technique in which only boundary routers (Internet Service Providers) will perform the functionality and intermediate routers just forward the packet without any change in the packet during the routing of IP packet. Hence the result will be less network load and less network delay.

3.2.4 Eliminate the Need of any Marking Technique

The new IP traceback technique which we have present in this thesis is also eliminates the marking and demarking technique. Only a file is maintained by boundary routers which consist about the user's information.

3.2.5 Easy Implementation

Because our proposed solution is eliminating any marking technique from IP traceback procedure, since the implementation of this new IP traceback technique on the ISP routers is an easy procedure.

3.2.6 Stop Spoofed Routing

The proposed solution is also able to stop the spoofed routing. The attackers who spoof the IP address of the users will be controlled by applying this new IP traceback technique and also penalized.

3.2.7 Minimizing the Loss

One of the objectives of our research work is to minimize the loss which is incurred by the spoofed users. In this thesis we are presenting such a solution which will identify the origin of the attacker on receiving first one packet. So on receiving one packet IP traceback procedure will be start and attacker will be controlled from many more attacks.

3.2.8 Improving the network performance

The IP traceback technique which we have designed in this solution is also able to improve the network performance. When attackers will be stopped immediately and no any marking technique will be used, since the performance of the network will be improved during the routing of IP packet.

3.2.9 Occupying Less Network resources

The technique which we are presenting in this thesis occupies less network resources. When Denial of Service (DoS) attacks are controlled, then as a result less network resources will be used and less bandwidth of the network will be wasted.

3.3 Research Scope

As we know there are many types of problems occur during the internet surfing. Attacker can attack on the victim through different ways. It is impossible to get hundred percent securities from these attacks, but by using multiple securing techniques against these attacks we can avoid from the void range of damages and problem. Mostly attacks on the internet are done through spoofing the IP address of the source e.g. Denail of Service (DoS) attack. In DoS attack attacker hides its origin and attacks on victim through different ways i.e. attacker can destroy server memory and consume server bandwidth by sending a large amount of malicious packets which are greater than its capacity and many more similar ways are there. So to avoid these attacks there are different types of IP traceback techniques which are already presented by many authors, but still there are many issues which are left and need to be re-considered. While considering these issues we have drawn the scope of our research i.e. to what an extent our solution is working to cope with above mentioned issues.

In this research a new IP tracback technique is introduced which only works in IPv4. For the implementation of this procedure only IPv4 is used, if IPv6 is used then this technique will not able to do so. The technique which we present in this research is only able to do work when there are ISP routers used, hence this technique is ISP based. Only ISP routers will mark and de-mark

the packet during communication no intermediate routers are involved. Intermediate routers just forward the packet without any change.

3.4 Summary of the Chapter

There are many types of attacks are done on the internet. Denial of Service (DoS) attacks is one of them. In these DoS attacks, attacker spoofs the IP address of any legitimate client. Attacker hides its origin and attacks on the victim from different ways and denies the services to the legitimate clients. Multiple IP traceback techniques are designed by many authors. From these previous IP traceback techniques we have identify some common issues.

The objective of our research is to design a new IP traceback technique which will be more efficient, secure and easy. This IP traceback technique will improve the performance as well as security of the network.

4: Proposed Solution and Methodology

4: Proposed Solution and Methodology

As we have discussed our problems in detail in section [3.1]. These problems have identified from the earlier IP traceback techniques. The Denial of Service (DoS) attacks which are launched on the internet through spoofing the IP address of the user. To identify the origin of these attacks is not so easy task. A lot of research papers have been written and a lot of marking techniques are proposed by the authors to make the traceback procedure more efficient [7, 8, 9], but still there are some issues i.e. some techniques increases network load and packet delay, consumes network bandwidth and so on.

The purpose of our proposed solution is to make the routing of IP packet more efficient on the internet and provide the user a secure and effective IP traceback technique. Our presented solution also has the ability to increase the network security and overall performance of the network.

The solution which we have presented in this research thesis is able to accomplish all those goals and objectives which are discussed in the previous chapter.

In this research thesis we, have introduced a new IP traceback technique, which consumes less network bandwidth and less network resources then the previous mentioned traceback techniques. This technique is more efficient and works more perfect than the earlier IP traceback techniques.

Transferring the MAC addresses to the users will result in un-satisfaction because no one wants to share its private information. So our solution which we have proposed here does not share the MAC address of a user with others. Hence we can say that our proposed solution is not compromising on the privacy of the user.

Our solution also does not require to be implemented on all the routers of the world. It is only implemented on the ISP routers. So we can say that our solution is practical and gives result in lesser network delay and load.

Our proposed solution is Internet Service Provider (ISP) based known as ISP Identity Based Secure Single Packet IP Traceback. As this technique is ISP based, that's why it requires implementing only on the ISP routers.

We, in this research thesis, have designed such a new IP traceback technique. This new IP traceback technique works on single packet IP traceback. Single packet IP traceback means it requires only one packet to start the traceback procedure. When victim receives packet and identify that it's a malicious packet, it may be the first malicious packet. Then victim immediately starts the traceback procedure, by identifying the origin of the attacker and bounding the attacker from commencing more attacks.

Some of the techniques those proved efficient in one scenario, give poor results in another scenario. So our proposed solution totally eliminates the need of any marking technique and is implemented only on the ISP routers. This capability to eliminate the marking technique reduces the load from the routers. This proposed mechanism also reduces the overall packet delay in such a way that it is implemented only on the boundary routers.

The presented solution is more secure and provides complete security to the user's data during the routing of IP packet. In this solution the complete information about the legitimate client is maintained by ISPs and if any illegitimate client wants to have an access of user's data then it is penalized.

In our proposed solution we are using the 16 bit identity. These 16 bits we have taken from the transport layer. Because there is no need of fragmentation at the transport layer, as before these 16 bits were used for fragmentation by this layer. The packets received by the transport layer are

already fragmented now. We have allocates a 16 bit identity to all the ISPs of the world. Against every 16 bit ID of the ISP the IP addresses of that ISP are associated and this list is shared among all the ISPs of the world.

For this proposed solution we have used the IPv4. When IPv4 is used for routing of the IP packet then in the packet's IP header the space of these 16 bits remains free during the routing of IP packet, hence we have used this free space for our solution. As there are 13,000 ISPs in the world and with 16 bits we can easily generate almost 65000 identities. So we have allocated the 16 bit identity to all the ISPs of the world.

According to our survey currently there are 13000 ISPs in the world. With 16 bits we can generate almost 65000 identities, so this 16 bit identification field is enough to accommodate all the ISPs of the world.

Whenever a packet reaches at the ISP gateway it adds its 16 bit identity in the field and keeps the log on the basis of the MAC address of the user.

When this message arrives at the ISP gateway of the receiver, the receiver's ISP removes the 16 bit identity of the sender's ISP and makes its own log file. Therefore the information of the ISPs identity remains only between the ISPs.

If a receiver detects an attack it sends complaints to its ISP that an attack is launched from this particular IP address at this time. The receiver's ISP checks its log and find out the ISP of that particular IP address. After finding out the ISP identity the victim ISP consults the identity list to find the IP address of that ISP, then it forwards the complaint to the attacker's ISP. Upon receiving the complaint the attacker's ISP find out the MAC address of the attacker from their logs file and penalize the attacker according to the nature of the attack.

To handle the wrong complaints also a warning system is implemented in our solution. Since the victim submits an attack complaint to its ISP so the ISP gateway inspects the complaint before forwarding it to the attacker's gateway.

The victim's gateway consults its log file to verify that weather really attack is launched from this IP address at the specified time or the victim is launching a false complaint. If according to the log file an attack detected then the complaint is forwarded to the attacker's ISP. If no attack is detected from the log file then the user who launches the complaint is penalized by its own ISP and complaint is discarded.

We are presenting a general detailed overview of our solution in the next few paragraphs, later on each of the modules is explained separately.

As our proposed solution is ISP based, so when the sender forward its IP packet it will be received by its own ISP known as source ISP gateway. The source ISP maintains the log file on the basis of the MAC address of the user. Upon receiving the IP packet the source ISP gateway note the MAC address of the user, the IP address of the user and the time in its log file. The source ISP gateway does not forward the MAC address of the user; it removes the MAC address from the packet header and adds its own 16 bit identity in the field.

Since in our solution there is no need of any marking technique, as in our base paper an intelligent marking technique is required to convert from 80 bits to 16 bits and from 16 bits to 80 bits.

Then source ISP gateway forward the IP packet to the next router, the next non-boundary router forward the packet without any change, hence the packet is forwarded by the intermediate routers without any change.

When the packet is received by the ISP gateway of the receiver, the receiver's ISP gateway after receiving the IP packet removes the 16 bit identity of the sender's ISP from the IP packet and

copy its own 16 bit identity and makes its own log file. This log file is maintained by the 16 bit identity of the sender's ISP, the IP address of the user and receiving time of the IP packet. After this the receiver's ISP forward the packet to the receiver which is in its domain.

If the receiving packet is an attack packet, then the receiver sends the complaint to its own ISP that an attack is launched through this IP address at this time. The receiver's ISP checks the 16 bit identity of sender's ISP across this IP address from its own log file and find out the ISP of that particular IP address. After finding out the 16 bit identity of the sender's ISP it sends the direct complaint to the attacker's ISP. Then after receiving the complaint the attacker's ISP find out the MAC address against that IP address from its log file and penalize the attacker according to the nature of the attack.

If a receiver false claims to its own ISP that an attack is launched with this particular IP address at this time. The victim's ISP first checks its log file before forwarding the complaint. The victim's ISP checks that particular IP address and the time from its log file and verify, if a victim is launching a false claim then it is penalized by its own ISP. Hence wrong complaints can be handled easily through our solution.

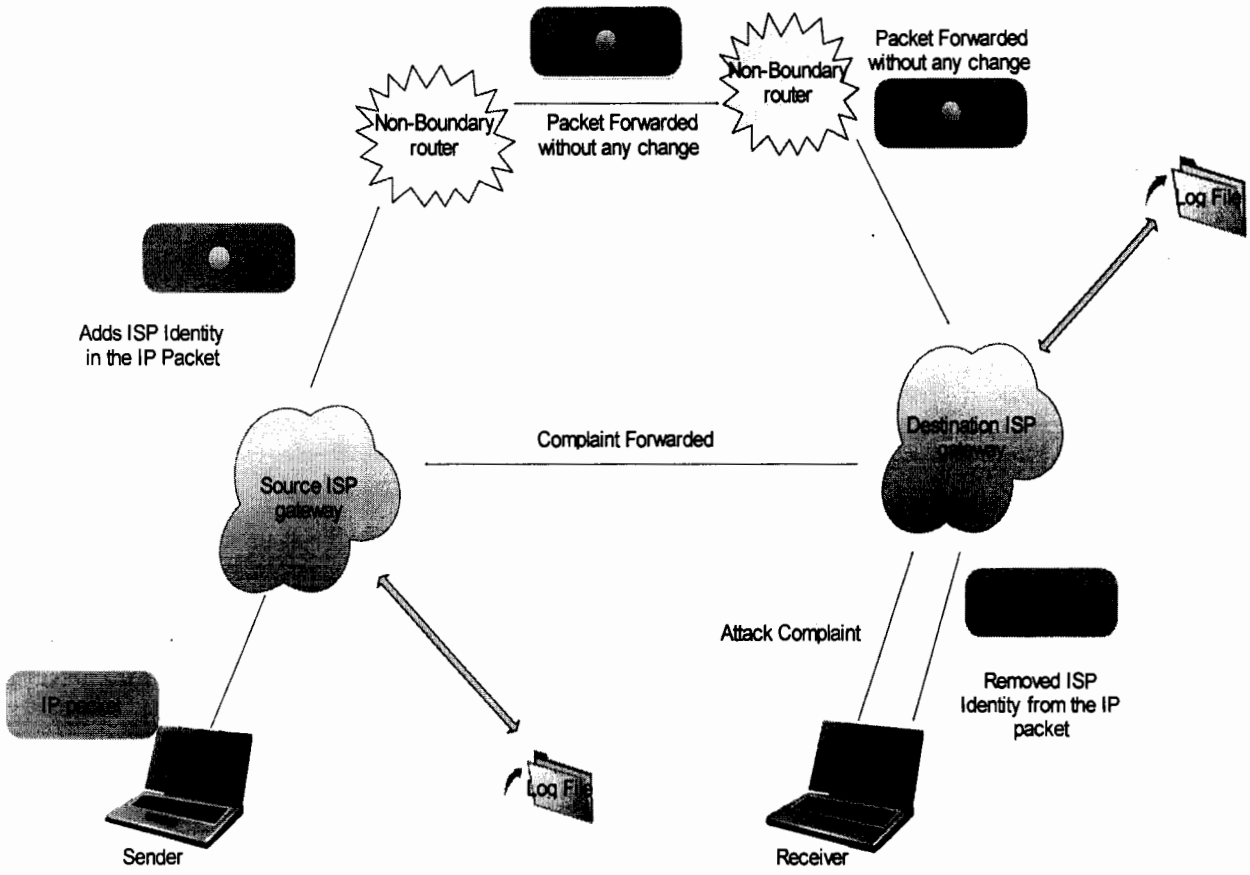

Figure 4.1: ISP Identity Based Traceback

The details of our proposed IP traceback technique are shown in the figure 4.1

Here we are presenting the detailed functionality of our proposed solution step by step.

4.1 Step 1:

In the first step of the ISP identity Based Secure Single Packet IP Traceback during the routing of the IP packet the sender sends the IP packet to its own Internet Service

Provider (ISP) gateway known as the source ISP gateway. The IP packet contains the IP address of the sender, MAC address of the sender and the data.

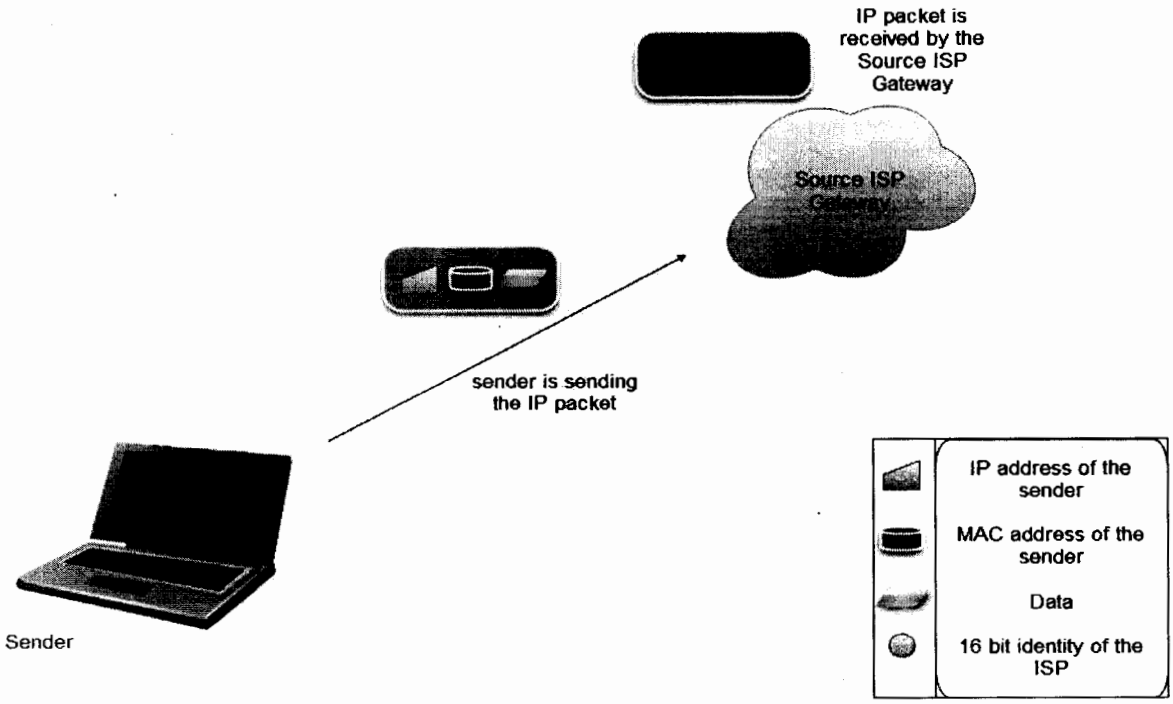

Figure 4.2: Step 1: ISP Identity Based Traceback

4.2 Step 2:

When IP packet is received by the source ISP gateway, the source ISP gateway maintains its own log file and copy the IP address of the sender in the log file and removes the MAC address of the sender from IP packet and note it in the log file and adds its own 16 bit identity in place of the MAC address in IP packet's header and also note down the receiving time of the IP packet in its log file and forward the IP packet to the next router.

By removing the MAC address of the sender from the IP packet and note it in the log file maintains the security of the sender. As the MAC address is the confidential data of the user and in our solution the privacy of the sender/user remains intact, because the MAC

address of the user is not transferred in our presented IP traceback technique as transferred in previous IP traceback techniques. Hence the privacy of the user is not compromised.

As our solution maintains the log file and keeps the record of the sender; hence our solution totally eliminates the need of the marking technique and works without any marking technique. By eliminating the need of the marking technique increases the network efficiency and also reduces the packet delay.

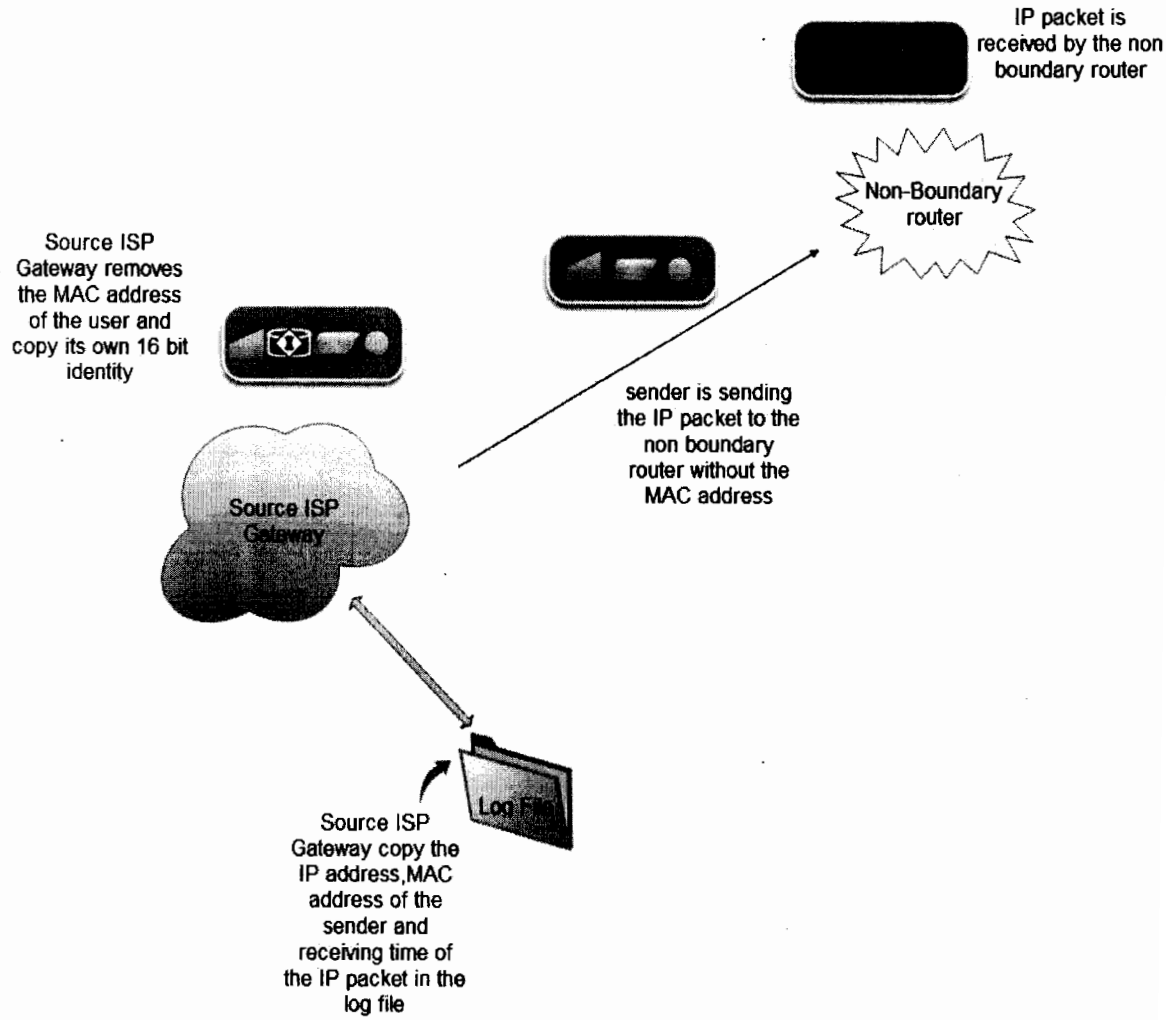

Figure 4.3 step2.: ISP Identity Based Trace

4.3 Step 3:

In the next step when the IP packet is forwarded to the non boundary router, the non boundary router forwards the IP packet to another non boundary router without any change. Similarly the IP packet is forwarded by the all intermediate routers without any change, at last the IP packet reaches to the destination ISP gateway. Hence our proposed solution is implemented only on the boundary routers and our solution also reduces the network load as well as increases the network efficiency because the intermediate routers do not perform any functionality just forwards the IP packets.

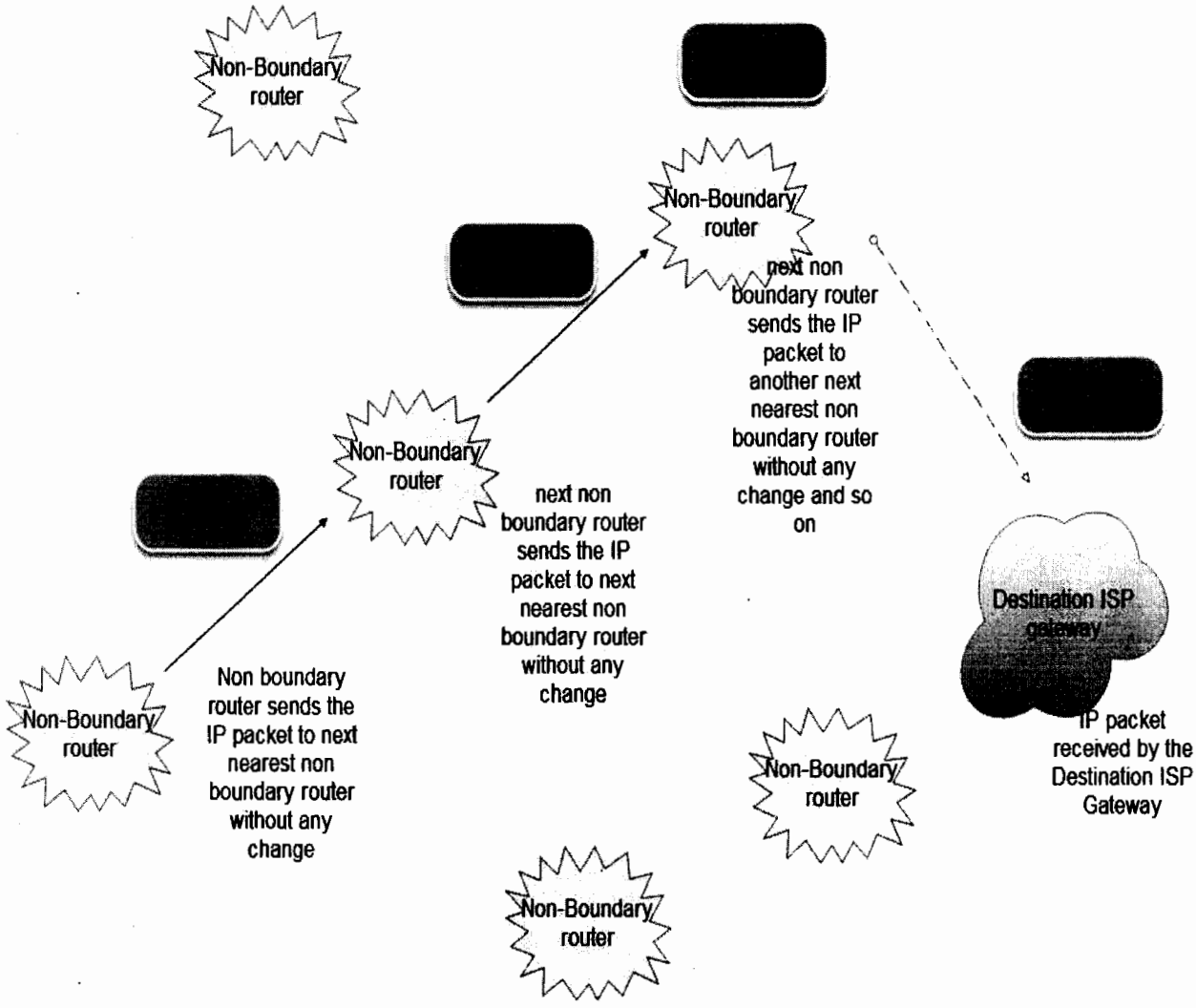

Figure 4.4.step 3: ISP Identity Based Traceback

4.4 Step 4:

In the forth step when IP packet received by the destination ISP gateway, the destination ISP gateway removes the 16 bit identity of the sender's ISP and copy in its own log file. Hence the information of the ISP's identity remains only between the ISPs.

After this the IP address of the IP packet and the receiving time of IP packet also recorded in the log file by the destination ISP gateway.

After maintaining the log file and attaching its own 16 bit identity, the destination ISP gateway forward the IP packet to the receiver. So the destination ISP gateway sends its own information to the receiver instead of the source ISP gateway and keeps the sender's ISP information in its own log file.

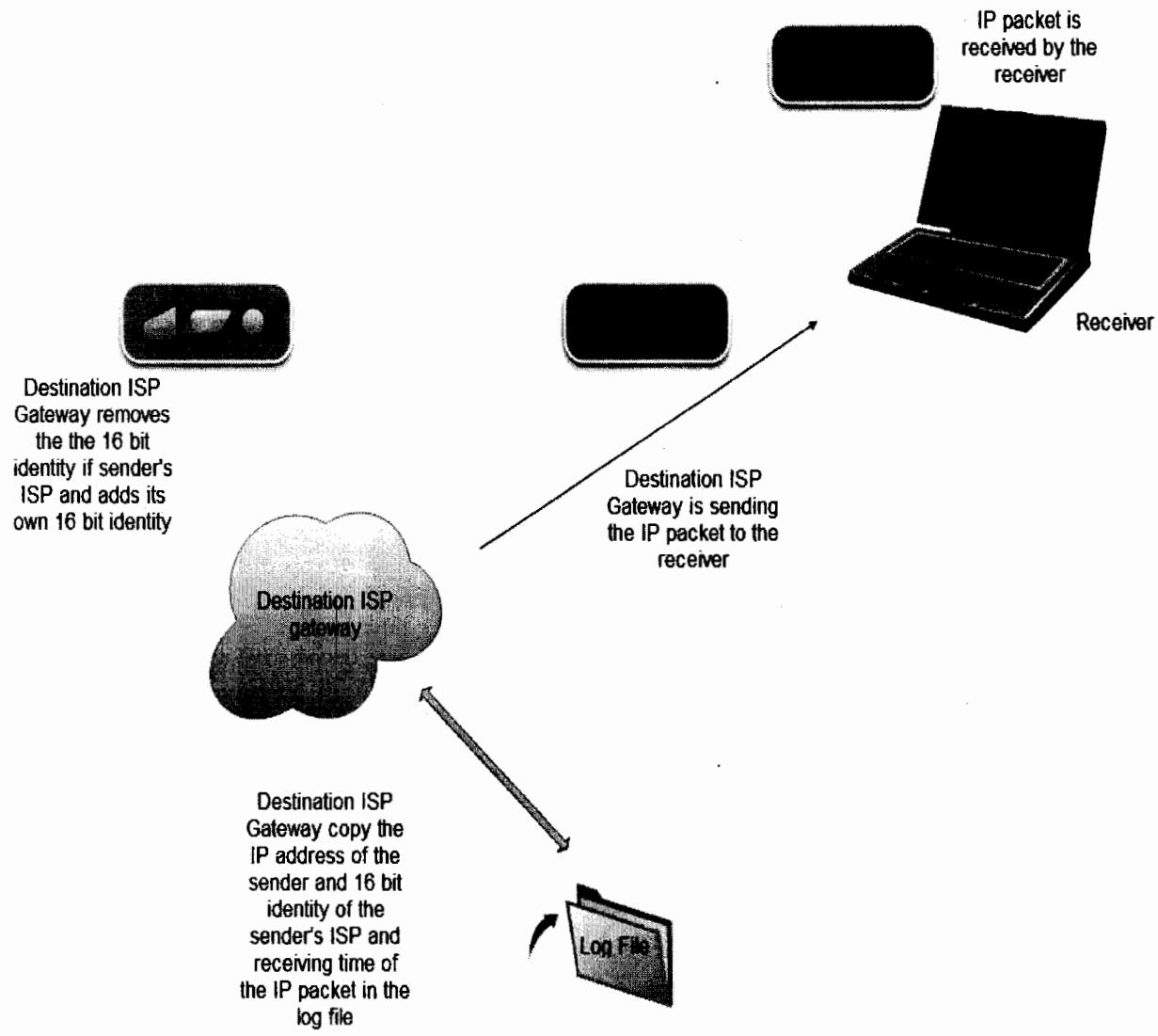

Figure 4.5: step 4: ISP Identity Based Traceback

4.5 Step 5:

In the next step the IP packet is received by the receiver, if the receiving packet disturbs the normal functionality of the receiver e.g. corrupt the windows, restart the operating system etc and the receiver detects that the receiving packet was an attack packet then it sends the complaint to its own ISP that an attack is launched with this IP address at that time. Hence at receiving single packet the victim can detect that the receiving packet is an attack packet and IP traceback procedure is started to identify the origin of the attacker.

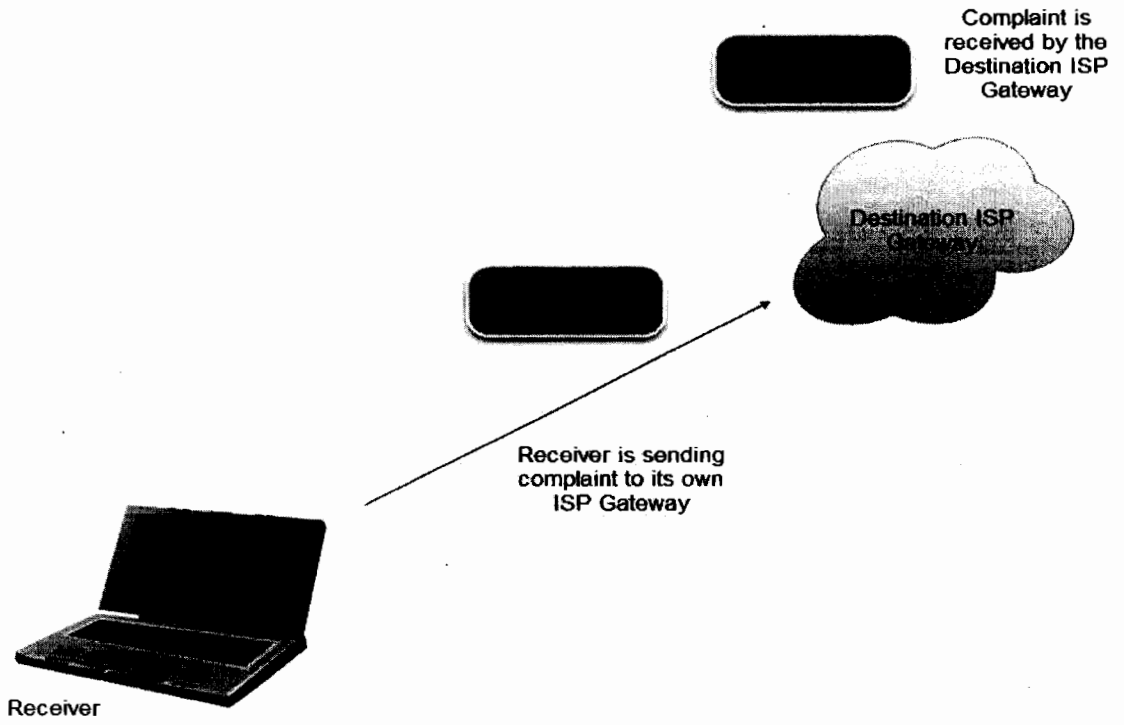

Figure 4.6: step 5: ISP Identity Based Traceback

4.6 Step 5.1:

In this step after receiving the complaint the destination ISP gateway checks its own log file and find out the ISP identity of that particular IP address and the sending time from its own log file. After finding out the ISP identity, the victim's ISP consults the identity list and find out the IP address of that ISP and forward the complaint.

This proposed solution also handles false claim, as when a victim forwards a complaint to its own ISP that an attack is launched with this particular IP address, then the victim's ISP gateway before forwarding the complaint to the attacker's ISP gateway inspects the complaint from its own log file to verify that whether really attack is launched from this IP address at the specified time or the victim is launching a false complaint.

If that particular IP address is found from the log file, then an attack is detected and the complaint is forwarded to the attacker's ISP. If that particular IP address is not found

4.7 Step 6:

In the case when a true attack has been launched a complaint is directly forwarded to the attacker's ISP by the destination ISP gateway that an attack is launched with this particular IP address at this time from your destination. By forwarding the direct complaint to the attacker's ISP the network load is decreased as well as less network resources are consumed.

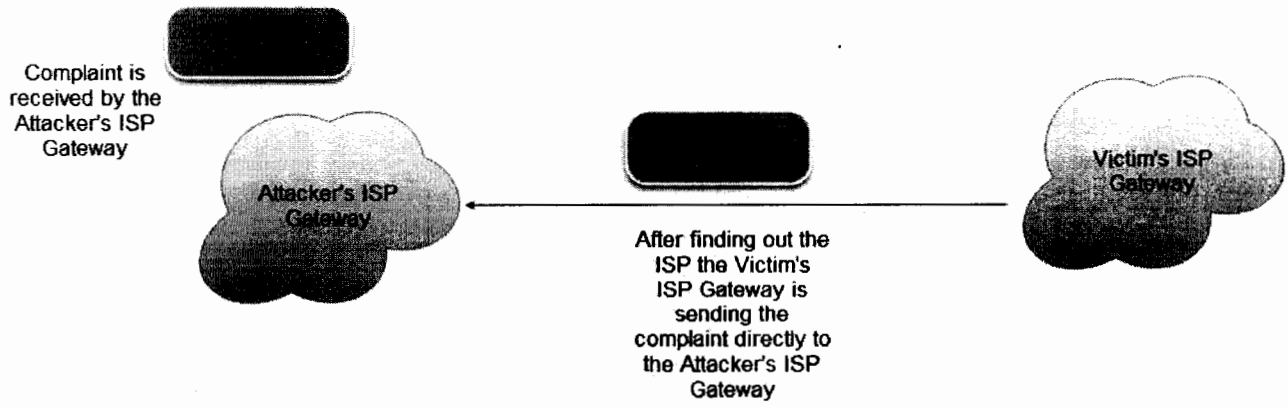

Figure 4.8: step 6: ISP Identity Based Traceback

4.8 Step 7:

After receiving the complaint the attacker's ISP gateway checks its own log file and find out the MAC address of the attacker and sending time from its own log file. The attacker's ISP finds out the MAC address of the attacker and penalizes the attacker according to the nature of the attack and thus with the propagation of a single packet only

our traceback mechanism is activated and with the consumption of only few resources it achieves its desired output.

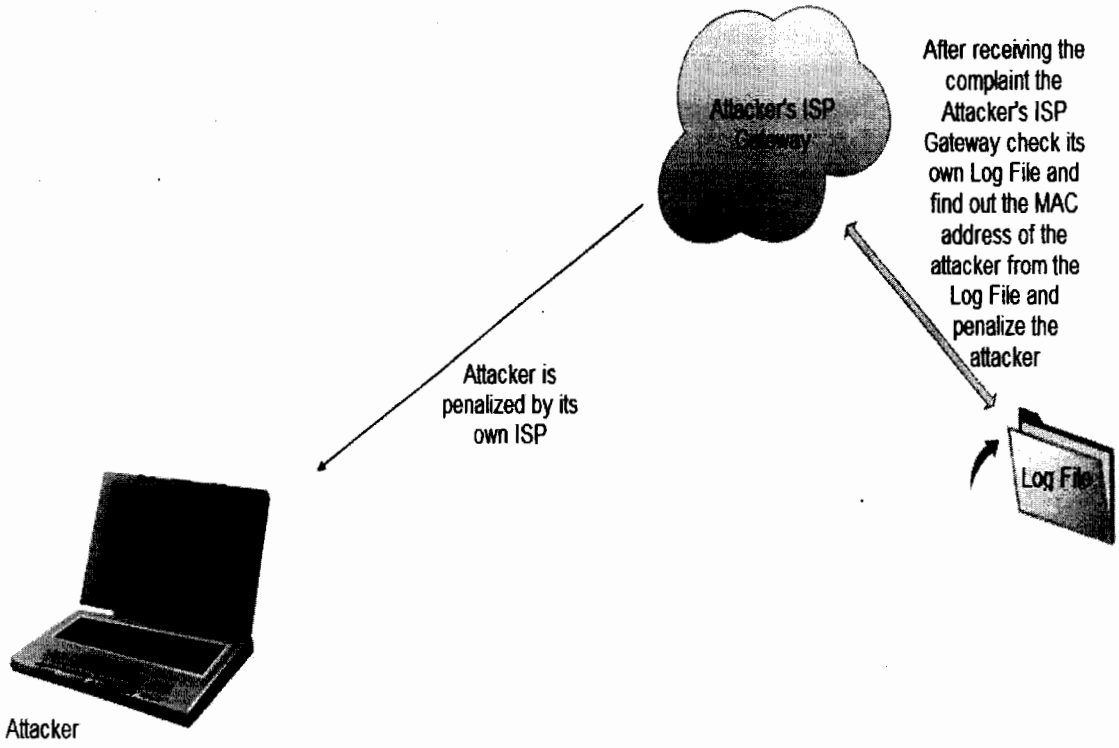

Figure 4.9: step 7: ISP Identity Based Traceback

All the existing IP trace back techniques need to be fully implemented on all of the routers of the world in order to operate and function properly. While this proposed trace back solution need not to be implemented on all the routers, instead it is necessary to be implemented on ISP's routers only hence partial implementation can also efficiently work here.

4.9 Comparison of PI and SIPT with our proposed solution

Traceback Mechanism/Parameters	**PI**	**SIPT**	**SSPITM (Our proposed solution)**
Packet Marking	Required (For adding router's information)	Required (For converting bits)	**Not Required (Only 16 bits are replaced)**
Load on the Intermediate Routers	High (All routers adds their own information)	Normal (Only boundary routers adds their own information)	**Normal (Simply forward the packets)**
Privacy of the Legitimate User	Remains intact (only router's information is added)	Compromised (MAC of the user is added)	**Remains Intact (Only ISP's IDs are added)**
Reflected Attacks	Possible (if a receiver claims false will be entertained)	Possible (If a receiver claims false will be entertained)	**Not Possible (If a receiver claims false will be penalized)**
Implementation	Complex (Marking technique required on all the routers)	Moderate (Marking technique required only on the boundary routers)	**Easy (No marking technique required)**
Packet Delay	Maximum (Packet marked by all the routers)	Moderate (Packet marked by the boundary routers)	**Minimum (Only 16 bits are replaced)**

4.10 Summary of the chapter

To solve the problems of the existing IP Traceback techniques a new ISP based secure single packet IP Traceback technique is presented to identify the source of the attack. A 16 bit's identity is assigned to every ISP in the world. Our presented solution is implemented only on the ISPs and non boundary routers just forward the IP packet without any change. A log file is maintained by the ISPs to keep the record of the sender. In case of the attack this record is helpful to identify the origin of the source.

5: Simulation, Results and Discussion

5: Simulation, Results and Discussion

We have carried out our simulation, to analyze the performance of Transport Protocols using different performance parameters in different scenarios using NS-2 (version 2.27) simulator.

5.1 NS-2 Simulators

NS-2 is a simulator tool used to simulate different network protocols. Using object oriented technique. NS is implemented, written in C++, at the front end OTcl parser is used. The simulator contains a chain of class hierarchy in C++ and a similar chain of class hierarchy is followed in the OTcl parser. From the user prospective two hierarchies have a close relation with each other, in interpret and compile hierarchy one to one correspondence is there. The root of hierarchy is Tcl object. As for as end user is concerned the end user have to create new objects in the predictor; the new objects are surrounded within the predictor, which are in compiled hierarchy are mirror by relevant object.

To work for two different tasks, NS has two languages first to deal with simulation of protocols it required a system language to work with bytes, packet headers and after powerful processing these are put into algorithm to run over bulky data. Run time for these tasks is more significant than turnaround time. Second in the network simulation scenarios require quick configuration of some parameters in these situations iteration time is more considerable than run time. So NS provides the structure in which we can run simulations for real time networks for analysis of different scenarios and different parameters.

Figure 5.1 describes the simplified view from user perspective.

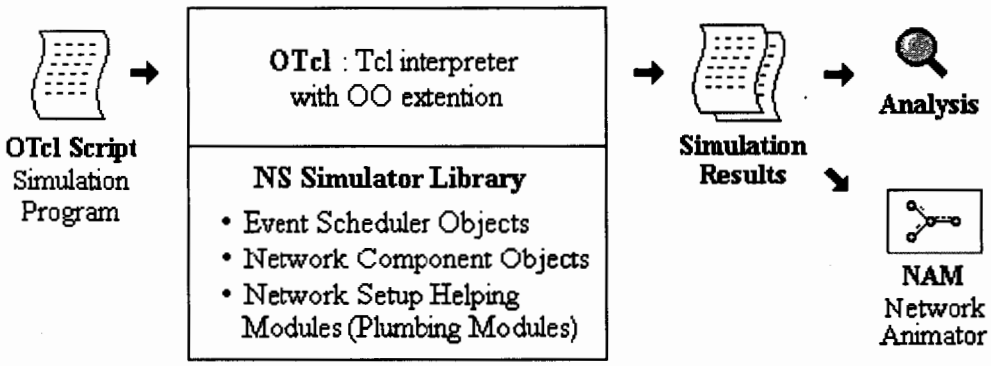

Figure 5.1: Simplified User's View of NS-2

5.1.1 TCL interpreter

Ns-2 uses two languages which are entirely different from each other to make the two languages understandable for each other some sort of parser is required which could make possible the communication of the two languages. TCL interpreter is used for this purpose TclCL is used between the communication of OTcl and C++. Toolkit Command scripts are designed to solve the different topologies. The objects in C++ that do not need to be controlled in a simulation or internally used by another object do not need to be linked to OTcl. Likewise, an object (not in the data path) can be entirely implemented in OTcl. Figure [4.2] shows an object hierarchy example in C++ and OTcl. One thing to note in the figure is that for C++ objects that have an OTcl linkage forming a hierarchy, there is a matching OTcl object hierarchy very similar to that of C++ as shown in fig 5.2.

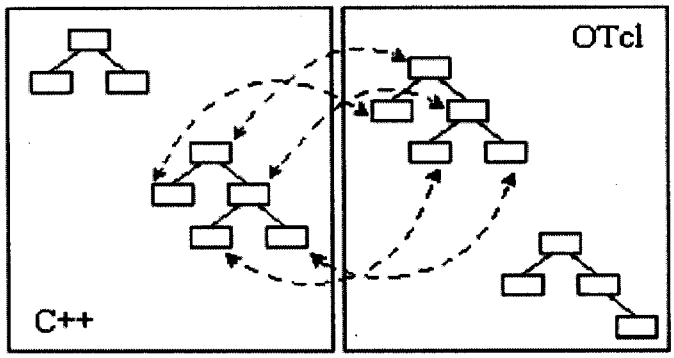

Figure 5.2: C++ and OTcl: The Duality [24]

5.1.2 Network Animator (NAM)

It is used as graphical visualization of different network scenarios which are created by user. It provides visual image of packet flows with different colors, node movements, packet queues, link between nodes, wireless nodes transmission range, drop packets and etc. NAM is a tool to visualize the imitations and traces for real world packets which is based on Tcl/TK. The theme to build NAM was to take the imitation and traces so that these results could be used in different visualization situations. The NAM when runs generate a file which could be used later if required. The advantage of NAM is that the generated file is of some significant size for some large simulations.

Trace file is required before one can NAM to visualize the simulations. More often trace file is produced by NS however many application can generate NAM trace file. When one run the NAM file one can see the topology design flow of packets in different direction depending upon the topology packets which are dropped due to some reasons can also be visualized from NAM visualization. All this can be seen in a separate window.

5.1.3 User Interface

When starting with network animator, firstly it will create the NAM console window as shown in figure 5.3. You can have more than one animations running under the one NAM instance. At the top of NAM windows, there is a menu bar. That have 'File' and 'Help' menus. Under the 'File'

menu, a command of 'New' used for creating a ns topology using this NAM editor , and also have an 'Open' command which permit you to open existing trace files, and a 'WinList' command that popup a window, that have the list of all recently opened trace files, and a 'Quit' command which close NAM file. The 'Help' menu have a very small number of popup help screen and a command to show copyright and version information.

When a trace file loads into NAM, an animation window will show. It has a 'Save layout' command which saves the existent layout into a file and a 'Print' command which allow prints the current layout.

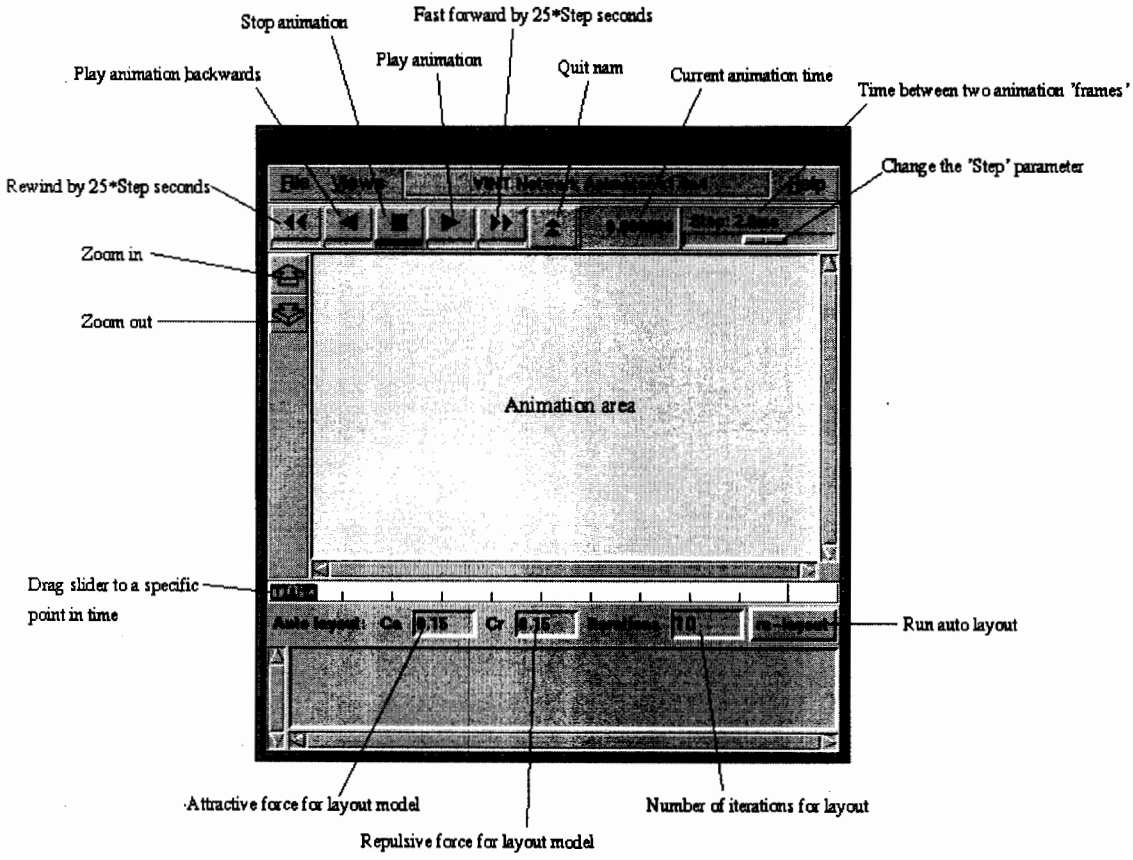

Figure 5.3: User Interface

5.2 Simulation Setup

We create a network of 100 nodes out of which 50 are routers and 50 belong to end stations. OSPF is used as routing protocol. Each node is capable of sending and receiving packets. 6 ISPs are created and one router per ISP is designated as gateway. A normal node sends maximum 5 packets per second while an attacker sends more than 5 packets per second.

We divide our validation phase into two different modules named as Fixed and Intelligent. In Fixed Mechanism user is in learning phase and it is fixed that which one is an attack packet and which one is legitimate. So as soon as the attack packet is received a traceback mechanism is initiated.

In contrast in Intelligent Mechanism the receiving ISP is not aware that what is an attack and what it is not an attack. As soon as it receives the attack complaint from any of its user it first checks its log to decide whether the complaint is genuine or it is a false complaint. If the complaint is genuine a traceback mechanism is initiated else false alarm is initiated.

5.2.1 Packet Marking

Packet marking technique is root of almost all the traceback techniques developed till today. An efficient packet marking technique is required in successful implementation of the traceback mechanism. A more efficient technique will provide more accurate results. In Pi [1] author proposed that each of the router will mark n bits of the identification field of the IP header. Now the first question is about deciding n. a smaller value of n provides very weak traceback results, and a large value provides better results but at the cost of high overhead. Second question is how to mark n bits, what mechanism or marking technique should be used to mark n bits. To answer these questions Pi mechanism required an efficient marking technique. So success of Pi is totally dependent on strength of the marking technique.

In SIPT [2] MAC address of the sender and IP address of the gateway is marked into 16 bit identification field of the IP header. MAC address is of 48 bits while IP address is of 32 bits, so totally it comprise on 80 bits. Marking 80 bits into 16 bits identification field is again required an

efficient reversible packet marking technique. So SIPT is again dependent on an efficient packet marking technique.

In our proposed solution we designed a marking technique in which a 16 bit ID is allocated to each ISP. As soon as ISP receives a packet from any attached end user it adds its 16 bit ID to the identification field of IP header. Since the size of the ISP ID and IP identification field is same so we don't need any other efficient packet marking technique. 16 bits are embedded into 16 bit field. Therefore our proposed marking technique is more efficient and simple as compared to other solutions.

5.2.2 Load on Intermediate Routers

In Pi [1] every router is involved in packet marking. A packet that travels from sender to receiver is marked by every intermediate router. It increases the load on intermediate routers that can results in congestion. In our proposed solution, intermediate routers have nothing to do with traceback. They are totally unaware from any of the traceback mechanism. Load on the intermediate routers, in our proposed solution, is remains same as it was in the absence of traceback mechanism.

5.2.3 Privacy of Legitimate Users

In Pi every router marks the n bits of every packet. So when a receiver receives a packet it contains information about the network i.e. load on intermediate routers, network topology etc. This information can help an attacker to launch different types of attacks on the network. Sharing the private information of the network introduces new security threats to the network.

In SIPT, MAC address of every user is embedded into identification field of IP header. Transferring MAC of the sender towards receiver is a compromise on privacy. Sender may not be willing to share its MAC address with receiver.

In our proposed solution ISP IDs are marked into the identification field of IP header at the sender's ISP. On the receiver's ISP that ID is removed. So end users got no private information either about the network or about the sender. Therefore we can claim that our proposed solution in more efficient in keeping the privacy of the users and network.

5.2.4 Packet Acceptance Ratio

Once an attacker is identified, it will be blocked for certain period of time depending upon the severity of the attack. Blocked users will not allow sending any packet, so their packets will be dropped at source ISP. Here we measure the packet acceptance ratio by setting different number of attackers. Out of 50 nodes first we got the results by assuming all the nodes as legitimate and we find that in both mechanisms, fixed and intelligent, packet acceptance ratio was 100%. After that we start to increase the number of attackers. As we increased the number of attackers the packet acceptance ratio starts decreasing. We repeat the experiment by setting 5, 10, 15, 20, and 25 nodes as attacker. We find that when there are 25 attack nodes the packet acceptance ratio is 31% in case of fixed mechanism. As in intelligent mechanism it is little complex to identify an attacker so packet acceptance ratio in intelligent mechanism was 38% with 25 attack nodes.

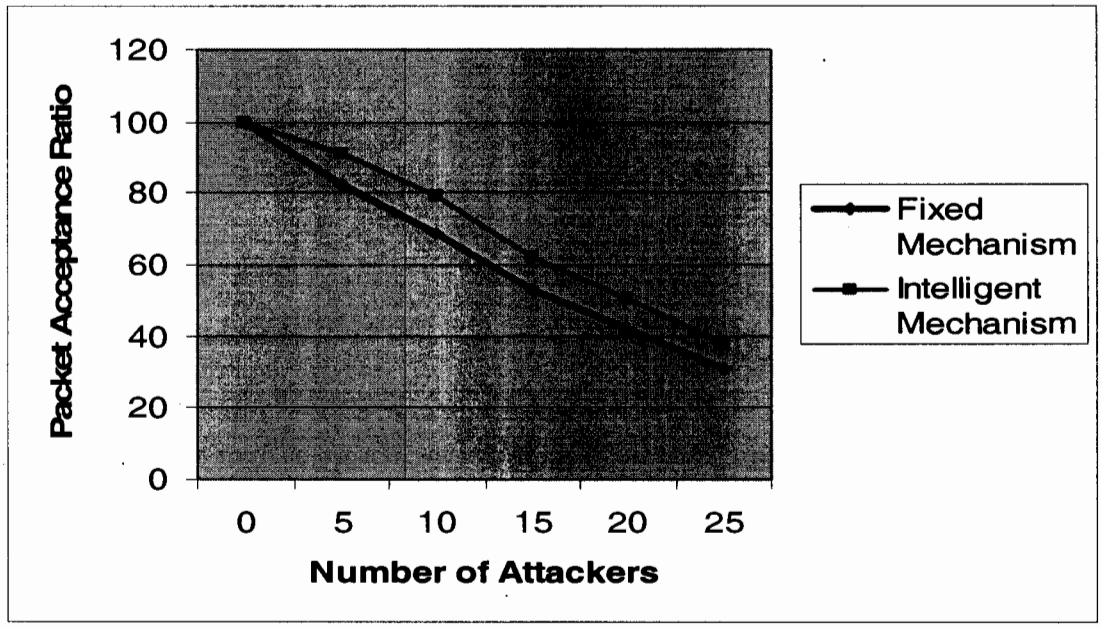

Figure 5.4: Packet Acceptance Ratio

5.2.5 Topology Independence

In Pi [1] since every intermediate router is involved in traceback mechanism so results may vary from topology to topology. While in our proposed solution in doesn't matter that what type of topology network have. Our solution is independent from network topology because intermediate routers are not involved in it.

5.2.6 False Attack Claims

A receiver may claim that an attack is launched from a particular or group of senders. Now whether an attack is really launched or not is difficult to decide. Existing solutions ignored this point and traceback mechanism is stared whenever an attack claim is launched without considering whether really an attack is launched or not. We, in our proposed solution, developed a mechanism to identify the false claims. Whenever a receiver claims that an attack is launched first its request is verified. We have conducted number of experiments for this purpose.

In the first experiment we launched 25 false claims and we find that Pi and SIPT start traceback for all these 25 false claims. Fixed mechanism of our proposed solution detects that all the claims are false so it entertain none of them. Intelligent mechanism also tries to detect the false claims and it serves only 6 claims and successfully blocks the remaining 19 false claims. By improving the set of rules these 6 can also be reduced. Results are shown in the figure.

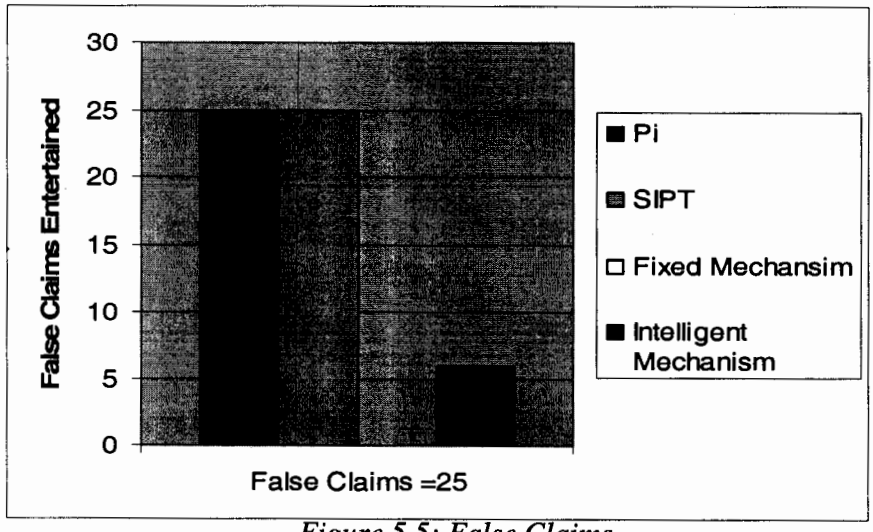

Figure 5.5: False Claims

In the next set of experiments we launched different number of false claims and measure how many of them are entertained by Pi, SIPT, Fixed mechanism and Intelligent Mechanism. Fixed mechanism provides the best results by not entertaining any of the false claims, intelligent mechanism identified maximum of the false claims while Pi and SIPT totally failed to detect any of the false claim. Results are shown in the figure below.

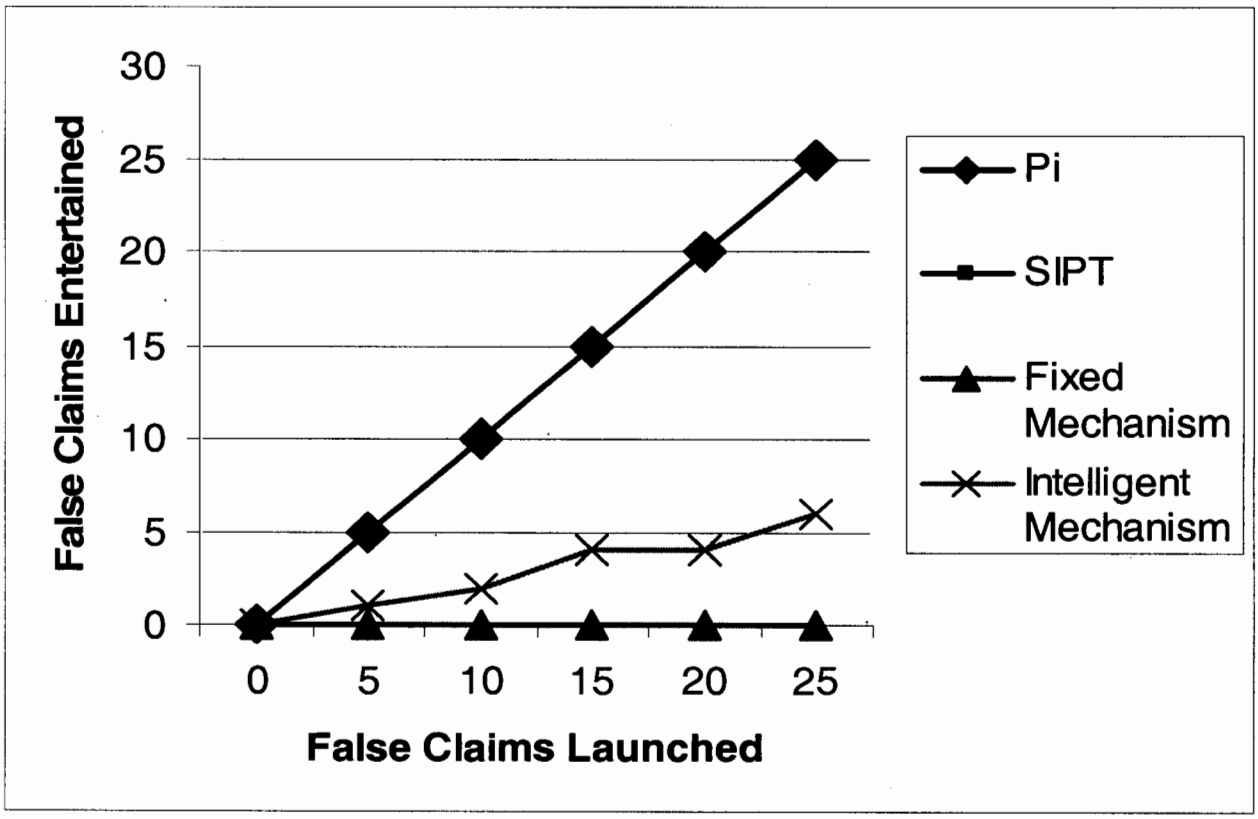

Figure 5.6: False Claims with Multiple Attackers

5.2.7 Packet Delay

Packet delay is one of the most important features in the network performance. We measure the packet delay in case of our proposed solution and compare it with the existing solutions. We find that the delay in our proposed solution is lesser as compared to other solutions. Delay is more in Pi because processing is required on intermediate router, delay in case of SIPT is average because an algorithm works to convert 80 bits into 16, and in our proposed solution delay is lesser. It is the delay caused by marking 16 bit ISP ID into 16 bit identification field of IP header.

We have conducted number of experiments to check the packet delay in existing techniques and in our proposed solution. In the first experiment we sent 1014 packets and the total delay in these packets while using Pi technique was 102, while using SIPT technique was 85, and with our proposed solution it was 80, while normal delay should be 72.05. This clearly shows that our proposed solution is better than the existing techniques. In another experiment when we sent 533280 packets then the delay in Pi technique was 53000, in SIPT technique was 49990, and in our proposed solution the delay was 48500, while normal delay should be 47997.5. Hence this shows that our proposed solution is better then Pi and SIPT.

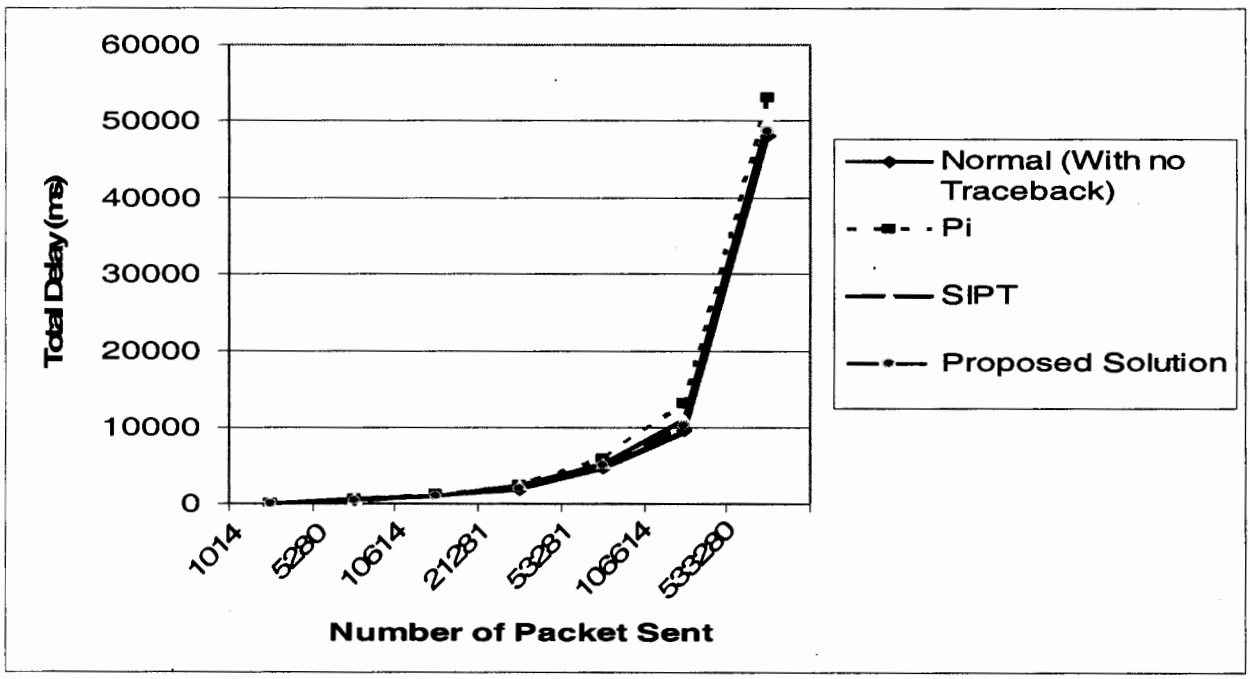

Figure 5.7: Total Delay

Here we have calculated the Average packet delay. When we sent 1014 packets then while using Pi technique the average packet delay was 0.094, while using SIPT technique was 0.087 while with our proposed solution it was 0.081 and normal average delay should be 0.076. This shows that our proposed solution is better then Pi and SIPT techniques.

When 533280 packets were sent then the average delay in Pi technique was 0.109, in SIPT technique was 0.102, while in our proposed solution average delay was 0.096 while the normal average delay should be 0.096. This shows that the working of our proposed solution is better then Pi and SIPT techniques.

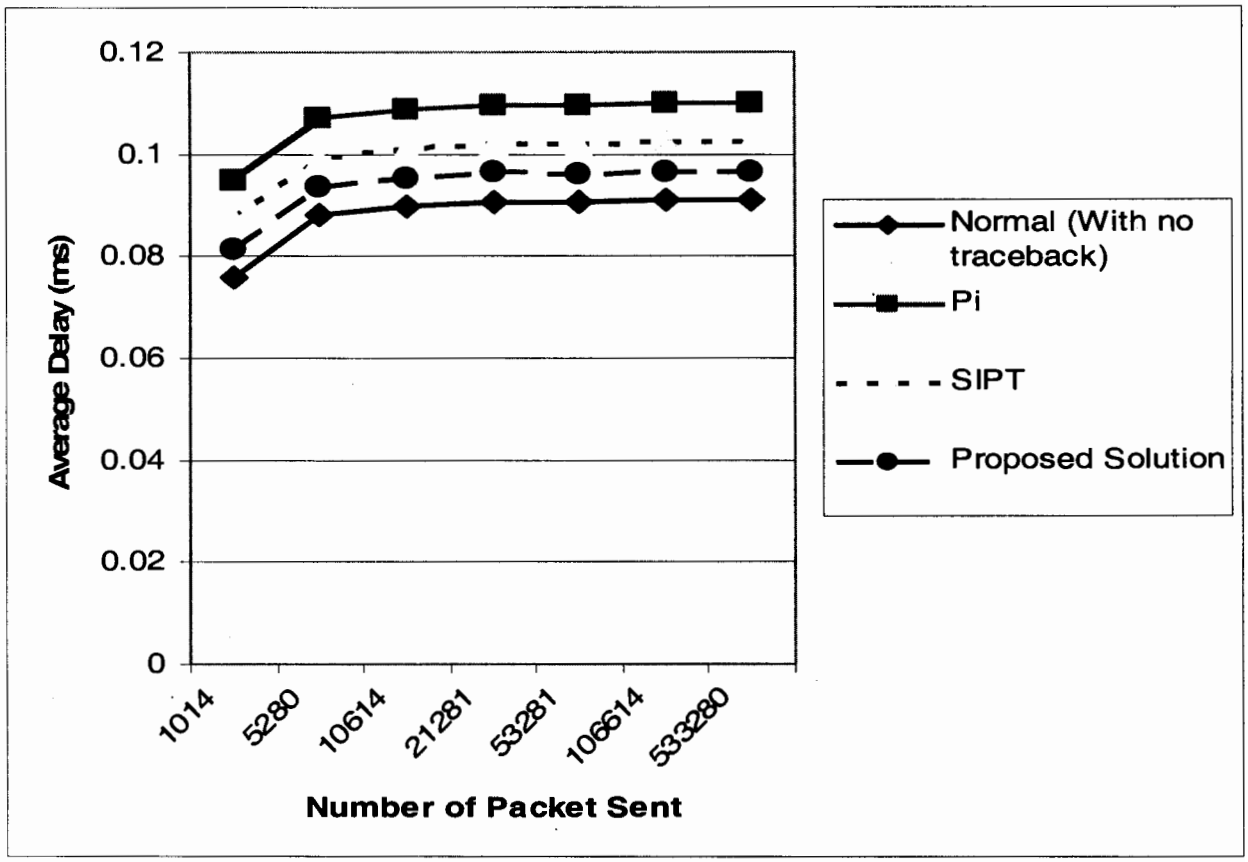

Figure 5.8: Average Delay

5.3 Summary of the Chapter

In this chapter we set a network of 100 nodes and conducted various numbers of experiments. We find that our proposed solution provides better results as compared to the existing solutions. We compare our results with Pi and SIPT. Our proposed solution is better in handling false claims, marinating privacy, reducing packet delay, providing better packet acceptance ratio, reducing load on intermediate routers etc. We select NS-2 to conduct the simulation.

6: Conclusion and Future Work

6: Conclusion and Future Work

Finally our dissertation is concluded here, giving the essence of our research.

6.1 Conclusion

The proposed IP traceback technique requires implementation on only the ISPs. The source ISP gateway adds its own 16 bit identity on receiving the every IP packet which is received only by the destination ISP gateway. The whole functionality is performed by the ISPs on both sides and the non boundary routers are just used to forward the IP packets without any change. Hence identity of the ISPs remains only among ISPs. MAC address of the sender is not transferred. So privacy of the user is not compromised.

Marking technique is no more required. So less network resources are consumed and packet delay is decreased because our solution removes the need of any marking technique. Therefore the efficiency problems arise due to the inefficiency of the marking techniques which no more disturb the traceback mechanism.

Single packet ensures the accurate traceback. On receiving the single attack packet the traceback procedure is started by the victim and hence immediately the attacker is stopped from launching the more attacks. Log files are maintained by the ISPs to keep the record about the users which are helpful in the identification of the source of the attack.

Presented solution also discourages the attacker from more attacks. In case of the attack the victim's ISP gateway sends complaint directly to the attacker's ISP gateway and hence the attacker is penalized by its own ISP through identifying its MAC address from the log file. If a receiver false claims about the attack then it is also properly checked by its own ISP, if the claim is not true then the receiver is also penalized by its own ISP. In short this is the best traceback technique to identify the source.

6.2 Future Work

In this thesis we have focused some problems related to IP spoofing and also we have solved these problems through the Internet Service Provider based technique that occurred during the routing of the IP packet. Achievement in any area is always welcomed. Still there are some issues which we have not discussed in this thesis and can be solvable in the future which are as follows.

In our thesis we have used Internet Service Providers (ISPs) for the identification of the attacker. Our presented solution works very well in the presence of IPv4, implementation of this technique by using the IPv6 can be discussed in the future.

According to our research the source of the attacker can be identified easily, but if an attacker sends a message to the ISP and acts like an ISP, the way to handle this kind of situation also can be discussed later.

References

[1]Abraham Yaar, Adrian Perrig, Dawn Song, "Pi: A Path Identification Mechanism to Defend against DDOS Attacks", IEEE Computer Society, Washington, DC, USA, Carnegie Mellon University, 2004

[2] Vaarun Vijairaghavan, Darshak Shah and Pallavi Galgali, Amit Shah and Nikhil Shah, Venkatesh Srinivasan, Lokesh Bhatia, "Marking Technique to Isolate Boundary Router and Attacker", IBM India Software Labs, IBM India System and Technology Labs, Synygy India, Zensar Technologies, February 2008

[3] Shaoh-Chen Ke, and Yen-Wen Chen, "An Edge Router-Based Fast Internet Traceback", Department of Communication Engineering, National Central University, Taiwan, ROC, 2007

[4] Henry C.J. Lee,Vrizlynn L.L. Thing, Yi Xu, and Miao Ma, "ICMP Traceback with Cumulative Path, An Efficient Solution for IP Traceback", Institute for Infocomm Research, 21 Heng Mui Keng Terrace, Singapore 119613

[5] Yi Shi, Yong Qi, BinXia Yang, "Deterministic link signature based IP traceback algorithm under IPv6", Department of Computer Science & Technology, Xi' an Jiaotong University, Xi' an 710049, P.R.China, February 2008

[6] Qu Zhaoyang, Huang Chunfeng, "A novel Deterministic Packet Marking Scheme for IP Traceback", School of Information Enginerring, Northeast Dianli University, Jilin City, Jilin Province, China, 2008

[7] Guang Jin, Jiangang Yang, Wei and Yabo Dong, "Across-Domain Deterministic Packet Marking for IP Traceback", College of Computer Science and Technology,

Zhejiang University, Hangzhou, China, 310027, College of Information Science and Engineering, Ningbo University, Ningbo, China, 315211

[8] WANG Xiao-jing, XIAO You-lin, "IP Traceback based on Deterministic Packet Marking and Logging", Lab of Computer Network Defense Technology, Beijing Institute of Technology, Beijing, China, Beijing Militry Representative of the General, armaments Department, Beijing, China, 2009

[9]Andre Castelucio and Artur Ziviani, " An AS-Level Overlay Network for IP Traceback" National Laboratory for scientific computing, Ronaldo M.Salles, Military Institute of Engineering, 2009

[10] Rafael P. Laufer, Pedro B, Velloso, Daniel de O. Cunha, Igor M. Moraes, Macro D. D. Bicudo, Marcelo D. D. Moreira, and Otto Carlos M. B. Duarte, "Towards Stateless Single-Packet IP Traceback", University of California at Los Angeles, USA, Universite Pierre et Marie Curie – Paris VI, France, Universidade Federal do Rio de Janeiro , Brazil, 2007

[11] Ahmad Fadlallah, Ahmed Serhrouchni, Youcef Begriche, Farid Nait-Abdesselam, "A Hybrid Messaging-based Scheme for IP Traceback", TELECOM Paris Tech, Telecom Institute Paris, France, Univ. of Science & Technologies of Lille, Lille, France

[12] Michael T. Goodrich, Senior Member, "Probabilistic Packet Marking for Large-Scale IP Traceback", IEEE, 2008

[13] Chao Gong, Student Member, and Kamil Sarac, Member, "A more practical Approach for Single-Packet IP Traceback Using Packet Logging and Marking", IEEE, 2008

[14] K. Boundaoud, F. LeBorgne, "Towards an Efficient Implementation of Traceback Mechanisms in Autonomous Systems", University of Nice Sophia Antipolis – 13S-Laboratory – CNRP, 2008

[15] Alireza izaddoost, Mohamed Othman, Mohd Fadlee A Rasid "Accurate ICMP Traceback Model under Dos/DDos attack", Department of Communication Technology and Network, Universti Putra Malaysia, 2007

[16] Chao Gang, Trinh Le, Turgay Korkmaz, Kamil Sarac, "Single Packet IP Traceback in AS- Level Partial Deployment Scenario", Department of Computer Science, University of Texas at San Antonio USA, 2005

[17] Keisuke Takemori, Shoichi Endo, "Performance Analysis of IP Traceback Systems with Serial and Parallel Control Schemes", Information Security Development Group, 2007

[18] Marios Andreou, Aad Van Moorsel,"COTrase: Connection Oriented Traceback in Switched Ethernet", New Castle University, School of Computing Science, 2008

[19] Yao Gang, Ahmet T.Erdogan, and Tughrul Arslan, "An Efficient Pre-Traceback Architecture for the Viterbi Decoder Targeting Wireless Communication Applications" Member, IEEE, 2006

[20] Basheer Al Duwairi, Manimaran Govindarasu, "Novel Hybrid Schemes Employing Packet Marking and Logging for IP Traceback", Member IEEE, 2006

[21] Masafumi OE, Youki KADOBAYASHI, Suguru YAMAGUCHI, "An Implementation of a Hierarchical IP Traceback Architecture", Graduate School of Information Science, Nara Institute Science and Technology Ikoma, 630-0192, Japan.

[22] Ken Wakasa, Hiroaki Hazeyama, "Large Scale Demonstration Experiments Towards achieving practical Traceback on the internet", Japan Data Communication Association, Nara Institute of Science and Technology, 2010