An Improved IPv6 Trace-Back technique to uncover Denial of Service (DoS) attacks

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering

in

Computer Science and Engineering

Submitted By

Abhishek Jain

(Roll No. 801132001)

Under the supervision of:

Dr. Maninder Singh

Associate Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

July 2013

Certificate

I hereby certify that the work which is being presented in the thesis entitled, **"An Improved IPv6 Trace-Back technique to uncover Denial of Service (DoS) attacks"**, in partial fulfillment of the requirements for the award of degree of Master of Engineering in ***Computer Science and Engineering*** submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of ***Dr. Maninder singh*** and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

(Abhishek Jain)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Maninder Singh)
Associate Professor

Countersigned by:

Maninder Singh, Ph.D
Associate Professor &Head
Computer Science and Engineering Deptt.
Thapar University
Patiala

S. K. Mohapatra, Ph.D
Sr. Professror & Dean of
Academic Affairs
Thapar University
Patiala

Acknowledgement

I would like to express my deep sense of gratitude to my supervisor, **Maninder Singh**, Associate Professor and Head, Computer Science and Engineering Department, Thapar University, Patiala, for his invaluable help and guidance during the course of thesis. I am highly indebted to him for constantly encouraging me by giving his critics on my work. I am grateful to him for giving me the support and confidence that helped me a lot in carrying out the research work in the present form. And for me, it's an honor to work under him.

I would also like to thank my parents and friends for their inspiration and ever encouraging moral support, which went a long way in successful completion of my thesis.

Above all, I would like to thank the almighty God for His blessings and for driving me with faith, hope and courage in the thinnest of the times.

(Abhishek Jain)

Abstract

Due to the rising cyber-attacks like Distributed Denial of Service (DDOS), Reduction of Quality (ROQ) on the networks, IP Trace-backing technique is introduced to provide the internet and network security. IP Trace-backing is one of security techniques associated with identifying the source of attack packets. To tackle new approach has been introduced that is refinement in some of previous packet marking approaches. The proposed approach is scalable, simple to implement, and introduced no bandwidth and practically no processing overhead on the equipment of the network. Tracing thousands of simultaneous attackers during DDoS and ROQ attack can be traced by this approach. All of the processing has been done at the victim. The trace-back process can be executed as post-mortem process, which allows for tracing the attacks that may not have been noticed in initial stage. The contribution and role of the Internet service providers (ISP) is very limited, and changes to the infrastructure and operation required to deploy proposed approach are minimal. Proposed scheme has performed the trace-back without revealing the internal topology of the provider's network, which is a desirable quality of a trace-back scheme.

To check out the source node of the attack, the technique of IP Trace-backing using packet marking and packet logging has been used by us. This technique has been implemented by us to check that upto which level this method is effective in IPv6. We are using IP Trace-backing in IPv6 to check the network from attacks and to find the relevant results from it.

Table of content

List of Figures

Chapter 1
Introduction

1.1 Introduction

Security is always the main issue for any network and there are number of prevention based and detection based approaches to reduce the intruder effect over the network. One of such approach is the packet marking. The packet marking is about to authenticate all the intermediate nodes over the network that participate in data communication. This work is also presented in the same area. . Over the network the active attacks are very common. The proposed approach will provide a reliable packet marking in such network. DDOS attack is one of the biggest threats on the Internet in which a large number of packets are sent to the receiver (victim) machine. It slows down the internet services. DDOS attack uses IP spoofing technique. The source address of the DDOS IP packet attack is spoofed to a random address. It becomes difficult to trace the flow of DDOS. Tracing becomes more difficult when the source address is spoofed. So to trace-back and detect the source address of an attacker IP trace-back technique is used .It traces the attack packets and identify the intruders.

IP trace-backing is the technique with which source of a malicious packet can be identified on internet. Because the IP protocol is of trusting nature, the source IP address of a packet is not authenticated. That is why the source IP address in an IP packet can be manipulated with the help of a technique called IP address Spoofing that allowing the packets for DOS attacks or one way attacks in which response from victim host is so well known that return packets need not be received to continue the attack. IP trace-backing is the problem to find out the source of a packet. Mostly use of this approach is to find out the DOS attack detection because these types of solutions require high number of packets to converge on attack paths. This proposed work is a combination of two probabilistic techniques in one unit along with the authentication process. The complete work includes 3 major algorithms:

- Encode process with Context Model.
- Encode Process with Dictionary Model
- Apply Checksum

Denial of service (DoS) is a prevalent threat in today's networks because DoS attacks are easy to launch, while defending a network resource against them is disproportionately difficult. Despite the extensive research in recent years, DoS attacks continue to harm, as the attackers adapt to the newer protection mechanisms. For this reason, we start our survey with a historical timeline of DoS incidents, where we illustrate the variety of types, targets and motives for such attacks and how they evolved during the last two decades. We then provide an extensive literature review on the existing research on DoS protection with an emphasis on the research of the last years and the most demanding aspects of defense. These include trace-back, detection, classification of incoming traffic, response in the presence of an attack and mathematical modeling of attack and defense mechanisms. Our discussion aims to identify the trends in DoS attacks, the weaknesses of protection approaches and the qualities that modern ones should exhibit, so as to suggest new directions that DoS research can follow. In order to do trace-backing some techniques have been implemented.

1.2 Probabilistic Packet Marking

Savage, who suggested probabilistic packet marking, proposed that router mark the packets with either router's IP address or the edges of path that packet traversed to reach the router. Probabilistic packet marking mark packets with the router's IP address, analysis shows that in order to gain the correct attack path with 95% accuracy as many as 294,000 packets are required. This approach is to XOR each node forming an edge in the path with each other. Node *a* inserts its IP address into the packet and sends it to *b*. Upon being detected at *b* (by detecting a 0 in the distance), *b* XORs its address with the address of *a*. This new data entity is called an edge id and reduces the required state for edge sampling by half. The second approach, edge marking, requires that the two nodes that make up an edge mark the path with their IP addresses along with the distance between them. This approach would require more state information in each packet than simple node marking but would converge much faster. They suggest three ways to reduce the state information of these approaches into something more manageable. Their next approach is to further take this edge id and fragment it into *k* smaller fragments. Then, randomly select a fragment and encode it, along with the fragment offset so that the correct

corresponding fragment is selected from a downstream router for processing. When enough packets are received, the victim can reconstruct all of the edges the series of packets traversed. Due to the high number of combinations required to rebuild a fragmented edge id, the reconstruction of such an attack graph is computationally intensive according to research by Song and Perrig. Further more, the approaches in a large number of false positives. Song and Perrig propose the following trace-back scheme: instead of encoding the IP address interleaved with a hash, they suggest encoding the IP address into an 11 bit hash and maintain a 5 bit hop count, both stored in the 16-bit fragment ID field. This is based on the observation that a 5-bit hop count (32 max hops) is sufficient for almost all Internet routes. Further, they suggest that two different hashing functions be used so that the order of the routers in the markings can be determined. Next, if any given hop decides to mark it first checks the distance field for a 0, which implies that a previous router has already marked it. If this is the case, it generates an 11-bit hash of its own IP address and then XORs it with the previous hop. If it finds a non-zero hop count it inserts its IP-hash, sets the hop count to zero and forwards the packet on. If a router decides not to mark the packet it merely increments the hop count in the overloaded fragment id field. It identifies that this is not robust enough against collisions and thus suggest using a set of independent hash functions, randomly selecting one, and then hashing the IP along with a FID or function id and then encoding this. They state that this approach essentially reduces the probability of collision to (1/(211)m).

1.3 Deterministic packet marking

Belenky and Ansari, outline a deterministic packet marking scheme. They describe a more realistic topology for the Internet that is composed of LANs and ASs with a connective boundary and attempt to put a single mark on inbound packets at the point of network ingress. The idea is to put, with random probability of .5, the upper or lower half of the IP address of the ingress interface into the fragment id field of the packet, and then set a reserve bit indicating which portion of the address is contained in the fragment field. By using this approach they claim to be able to obtain 0 false positives with .99 probabilities after only 7 packets. Rayanchu and Barua provide another spin on this approach. Their approach is similar in that they wish to use and encoded IP address of the input interface in the fragment id field of the packet. Where

they differ from Belenky and Ansari is that they wish to encode the IP address as a 16-bit hash of that IP address. Initially they choose a known hashing function. They state that there would be some collisions if there were greater than 2^16 edge routers doing the marking. They attempt to mitigate the collision problem by introducing a random distributed selection of a hash function from the universal set, and then applying it to the IP address. In either hashing scenario, the source address and the hash are mapped together in a table for later look-up along with a bit indicating which portion of the address they have received. Through a complicated procedure and a random hash selection, this approach capable of reducing addresses collision. By using a deterministic approach they reduce the time for their reconstruction procedure for their mark (the 16 bit hash). However, by encoding that mark through hashing they introduce the probability of collisions, and thus false-positives. Shokri and Varshovi introduced the concepts of Dynamic Marking and Mark-based Detection with "Dynamic Deterministic Packet Marking," (DDPM). In dynamic marking it is possible to find the attack agents in a large scale DDOS network. In the case of a DDoS it enables the victim to trace the attack one step further back to the source, to find a master machine or the real attacker with only a few numbers of packets. The proposed marking procedure increases the possibility of DDoS attack detection at the victim through mark-based detection. In the mark-based method, the detection engine takes into account the marks of the packets to identify varying sources of a single site involved in a DDOS attack. This significantly increases the probability of detection. In order to satisfy the end-to-end arguments approach, fate-sharing and also respect to the need for scalable and applicable schemes, only edge routers implement a simple marking procedure. The fairly negligible amount of delay and bandwidth overhead added to the edge routers make the DDPM implementable. S.Majumdar, D.Kulkarni and C.Ravishankar proposes a new method to trace-back the origin of DHCP packets in ICDCN 2011. Their method adds a new DHCP option that contains the mac-address and the ingress port of the edge switch which had received the DHCP packet. This new option will be added to the DHCP packet by the edge switch. This solution follows DHCP-RFCs. Previous IP-Trace-back mechanisms have overloaded IP header fields with trace-back information and thus are violating IP RFCs. Like other mechanisms, it also assumed that the network is trusted. This presented various performance issues in routers/switches that were considered while designing this practical approach. However, this approach is not applicable to any general IP packet.

Certain approaches have been implemented to get the track of a malicious node and packet which are mentioned below

1.4 Approaches to trace the packet

1.4.1 Router Based Approach

In router based approaches, the router is charged with maintaining information regarding packets that pass through it. Sager proposed log packets and then data mine them later. This has the benefit of being out of band and thus not hindering the fast path. They proposed in their paper is to generate a fingerprint of the packet, based upon the invariant portions of the packet (source, destination, etc.) and the first 8 bytes of payload (which is unique enough to have a low probability of collision). More specifically, m independent simple hash functions each generate an output in the range of 2^{n-1}. A bit is then set at the index generated to create a fingerprint when combined with the output of all other hash functions. All fingerprints are stored in a 2n bit table for later retrieval. They shows a simple family of hash functions suitable for this purpose and presents a hardware implementation of it. The space needed at each router is limited and controllable (2n bits). A small n makes the probability of collision of packet hashes (and false identification) higher. When a packet is to be traced back, it is forwarded to originating routers where fingerprint matches are checked. The fingerprint information is "clobbered" by hashes generated by other packets. Thus, the selectivity of this approach degrades with the time that has passed between the passage of the packet and the trace-back interrogation. Another known take on the router-based schemes comes from Hazeyama et al. In their approach, they wish to integrate the SPIE approach as outlined by Snoeren, with their approach of recording the layer 2 link-id along with the network ID (VLAN or true ID), the MAC address of the layer 2 switch that received the packet and the link id it came in on. This information is then put into two look-up tables both containing the switch (layer 2 router) MAC id for look-up. They rely on the MAC: port tuple as a method of tracing a packet back (even if the MAC address has been spoofed).

1.4.2 Out-Of-Band approaches

The ICMP trace-back scheme Steven M. Bellovin proposes probabilistically sending an ICMP trace-back packet forward to the destination host of an IP packet with some low probability. Thus, the need to maintain state in either the packet or the router is

obviated. Furthermore, the low probability keeps the processing overhead as well as the bandwidth requirement low.

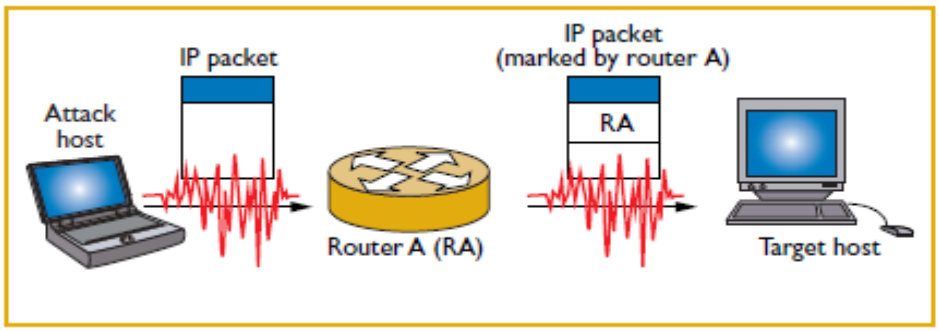

Figure 1.1 Packet marking

Bellovin suggests that the selection also be based on pseudo-random numbers to help block attempts to time attack bursts. The problem with this approach is that routers commonly block ICMP messages because of security issues associated with them.

1.4.3 Trace-back of active attack flows

In this type of solution, an observer tracks an existing attack flow by examining incoming and outgoing ports on routers starting from the host under attack. Thus, such a solution requires having privileged access to routers along the attack path. To bypass this restriction and automate this process, Stone proposes routing suspicious packets on an overlay network using ISP edge routers. By simplifying the topology, suspicious packets can easily be re-routed to a specialized network for further analysis. This is an interesting approach. By nature of DoS, any such attack will be sufficiently long lived for tracking in such a fashion to be possible. Layer-three topology changes, while hard to mask to a determined attacker, have the possibility of alleviating the DoS until the routing change is discovered and subsequently adapted to. Once the attacker has adapted, the re-routing scheme can once again adapt and re-route; causing an oscillation in the DoS attack; granting some ability to absorb the impact of such an attack.

1.4.4 Other Approaches: Hal Burch and William Cheswick proposes a controlled flooding of links to determine how this flooding affects the attack stream. Flooding a link will cause all packets, including packets from the attacker, to be dropped with the same probability. We can conclude from this that if a given link were flooded, and packets from the attacker slowed, then this link must be part of the attack path. Then

recursively upstream routers are “coerced” into performing this test until the attack path is discovered. The trace-back problem is complicated because of spoofed packets. Thus, a related effort is targeted towards preventing spoofed packets; known as ingress filtering. Ingress Filtering restricts spoofed packets at ingress points to the network by tracking the set of legitimate source networks that can use this router. Park and Lee present an extension of Ingress Filtering at layer 3. They present a means of detecting false packets, at least to the subnet, by essentially making use of existing OSPF routing state to have routers make intelligent decisions about whether or not a packet should be routed.

1.5 Types of attacks

1.5.1 DoS Attack

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDOS attack) is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name-servers. This technique has now seen extensive use in certain games, used by server owners, or disgruntled competitors on games such as Minecraft.

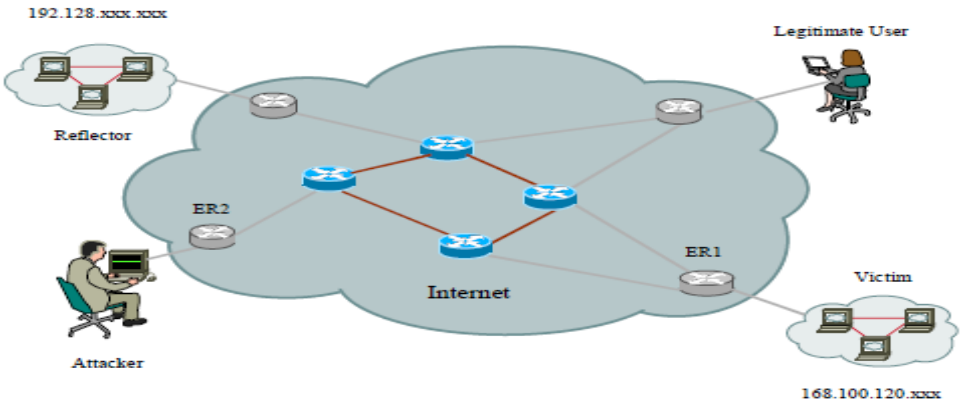

Figure 1.2 A Scenario of DOS Attack

Increasingly, DoS attacks have also been used as a form of resistance. Richard Stallman has stated that DoS is a form of 'Internet Street Protests. The term is generally used relating to computer networks, but is not limited to this field; for

example, it is also used in reference to CPU resource management One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately. Denial-of-service attacks are considered violations of the Internet Architecture Board's Internet proper use policy and also violate the acceptable use policies of virtually all Internet service providers.

Denial-of-service attacks are considered violations of the Internet Architecture Board's Internet proper use policy and also violate the acceptable use policies of virtually all Internet service providers. They also commonly constitute violations of the laws of individual nations.

1.5.2 Methods of DoS Attacks

A denial-of-service attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. There are two general forms of DoS attacks: those that crash services and those that flood services. DoS attack can be done in a number of ways. The five basic types of attack are:

- Consumption of computational resources, such as bandwidth, disk space, or processor time.
- Disruption of configuration information, such as routing information.
- Disruption of state information, such as unsolicited resetting of TCP sessions.
- Disruption of physical network components.
- Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

In most cases DoS attacks involve forging of IP sender addresses (IP address spoofing) so that the location of the attacking machines cannot easily be identified and to prevent filtering of the packets based on the source address. Low-rate Denial-of-Service attacks: The Low-rate DoS (LDoS) attack exploits TCP’s slow-time-scale dynamics of retransmission time-out (RTO) mechanisms to reduce TCP throughput.

Basically, an attacker can cause a TCP flow to repeatedly enter a RTO state by sending high-rate, but short-duration bursts, and repeating periodically at slower RTO time-scales. The TCP throughput at the attacked node will be significantly reduced while the attacker will have low average rate making it difficult to be detected**.**

1.5.3 Peer-to-Peer attacks

Attackers have found a way to exploit a number of bugs in peer-to-peer servers to initiate DDOS attacks. The most aggressive of these peer-to-peer-DDOS attacks exploits DC++. Peer-to-peer attacks are different from regular botnet-based attacks. With peer-to-peer there is no botnet and the attacker does not have to communicate with the clients it subverts. Instead, the attacker acts as a "puppet master," instructing clients of large peer-to-peer file sharing hubs to disconnect from their peer-to-peer network and to connect to the victim's website instead. As a result, several thousand computers may aggressively try to connect to a target website. While a typical web server can handle a few hundred connections per second before performance begins to degrade, most web servers fail almost instantly under five or six thousand connections per second. With a moderately large peer-to-peer attack, a site could potentially be hit with up to 750,000 connections in short order. The targeted web server will be plugged up by the incoming connections. While peer-to-peer attacks are easy to identify with signatures, the large number of IP addresses that need to be blocked (often over 250,000 during the course of a large-scale attack) means that this type of attack can overwhelm mitigation defenses. Even if a mitigation device can keep blocking IP addresses, there are other problems to consider. For instance, there is a brief moment where the connection is opened on the server side before the signature itself comes through. Only once the connection is opened to the server can the identifying signature be sent and detected, and the connection torn down. Even tearing down connections takes server resources and can harm the server. This method of attack can be prevented by specifying in the peer-to-peer protocol which ports are allowed or not. If port 80 is not allowed, the possibilities for attack on websites can be very limited. Wide array of programs are used to launch DoS-attacks. Most of these programs are completely focused on performing DoS-attacks, while others are also true Packet injectors, thus able to perform other tasks as well. Such tools are intended for benign use, but they can also be utilized in launching attacks on victim networks.

1.6 ROQ attacks

Reduction of Quality (RoQ) attacks are a new breed of attacks that target adaptation Mechanisms employed in current computing systems and networks. RoQ is pronounced as in "rock". RoQ attacks keep an adaptive mechanism oscillating between over-load and under-load conditions, all the time.

ROQ is different form Denial of Service (DoS). DoS attacks rely on overwhelming the victim with load that constantly exceeds its capacity. RoQ attacks, on the other hand, optimize the attack traffic to produce the maximum damage, while keeping a low profile to avoid detection. RoQ attacks do not necessarily result in a complete denial of service. RoQ attacks target the transients of a system's adaptive behavior as opposed to its limited steady-state capacity.

1.7 IP spoofing

The internet protocol is the main protocol used to route information across the Internet. IP provides best-effort services for the delivery of information to its destination. IP works on upper-level TCP/IP suite layers and provides accountability and reliability. The heart of IP is the IP datagram, a packet sent over the Internet in a connectionless manner. An IP datagram carries enough information about the network to get forwarded to its destination. It consists of a header followed by bytes of data. The header contains information about the type of IP datagram. But Spoofing IP datagrams is a well-known problem that has been addressed in various research papers. Generally spoofing is done for illegitimate purposes. Attacker hides their own identity and somehow damages the IP packet destination.

1.7.1 Spoof the IP Source Address

Most systems keep logs of Internet activity, so if attackers want to hide their identity, they need to change the source address. The host receiving the spoofed packet responds to the spoofed address, so the attacker receives no reply back from the victim host. But if the spoofed address belongs to a host on the same subnet as the attacker, then the attacker can "sniff" the reply. You can use IP spoofing for several purposes. For some scenarios an attacker might want to inspect the response from the target victim (called "non-blind spoofing"), whereas in other cases the attacker might not care (blind spoofing).

1.7.2 Tracing Spoofed IP Packets

IP Trace-back technology plays an important role in discovering the source of spoofed packets. Hop-by-hop Trace-back and logging of suspicious packets in routers are the two main methods for tracing the spoofed IP packets back to their source. When a node detects that it is a victim of flood attack, it can inform the Internet Service Provider (ISP). In flood attacks the ISP can determine the router that is sending this stream to the victim, and then it can determine the next router, and so on. It reaches either to the source of the flood attack or the end of its administrative domain. For this case it can ask the ISP for the next domain to do the same thing. This technique is useful only if the flood is ongoing.

1.8 Packet logging

The packet log collects information about the IP network traffic. By default, the packet logging is turned off. Packet logging is mainly aimed at experienced users who are familiar with computer networks. You can turn the packet logging on if you have created your own set of firewall rules, and want to check how they block traffic. You can also do this if you suspect malicious network activity. Information is gathered into 10 files (packetlog.0-packetlog.9). Each time you turn on the logging, the packet log is collected into a new file. After the tenth file becomes full, the next log is collected again to the first file. In this way, you can view the previous logs while a new log is generated.

In addition to the IP traffic, the packet log also collects information about other types of network traffic, for example, about the protocols needed by your Local Area Network (LAN). This information includes, for example, routing information. The packet log is in hexadecimal format and supports tcpdump format. This allows you to open the log files also in a packet logging program other than the default packet log viewer. You can also use a network protocol analyzer program to analyze the contents further.

Chapter 2
Literature survey

DoS attacks have become very popular. So demand is to design proper mechanisms to protect systems from such attacks. Mechanisms has been developed and deployed to prevent such attacks. But DDoS is still a problem as it is difficult to trace DDoS attackers and its effect is too bad. So development towards defending DDoS is very important. Some schemes are present which very well defends such attacks, but without the cooperation of ISPs it will be difficult to deploy any scheme. Though RFC asks to deploy ingress filtering, still very less number of ISPs have deployed that. Mechanisms like hash based traceback leads to many management issues, which in current scenario doesn't seem to be working. Mechanisms are there which talks about single packet trace-back, but there are lots of overheads for such methods.

(2003), U. Tupakula and V. Varadharaja: described us about two main kinds of IP trace-back techniques have been proposed in two dimensions: packet marking and packet logging. IP trace-back based on packet marking is often referred to as probabilistic packet marking (PPM) approach where packets are probabilistically marked with partial path information as they are forwarded by routers. This approach incurred little overhead at routers. But due to its probabilistic nature, it can only determine the source of the traffic composed of a number of packets. IP trace-back based on packet logging is often referred to as hash-based approach where routers compute and store digest for each forwarded packet. This approach can trace an individual packet to its source. However, the storage space requirement for packet digests and the access time requirement for recording packets commensurate with their arriving rate are prohibitive at routers with high speed links.

It proposed an IP trace-back approach based on both packet marking and packet logging. Compared with the PPM approach, this approach is able to track individual packets. Compared with the hash-based approach, approach in this incurred less storage overhead and less access time overhead at routers. Specifically, the storage overhead is reduced to roughly one half, and the access time requirement is decreased by a factor of the number of neighbor routers [21]. It proposed to develop a hybrid IP trace-back approach based on both packet marking and packet logging. The

motivation is to develop an IP trace-back approach that has advantages of both packet marking and packet logging.

(2003), Andrey Belenky and Nirwan Ansari: Described about the rising threat of cyber-attacks especially distributed denial-of-service (DDOS), makes the IP Trace-back problem very relevant to today's Internet security. IP Trace-back is one of the security problems associated with identifying the source of the attack packets. This work presents a novel approach to IP trace-back Deterministic Packet Marking (DPM) [9]. The proposed approach is scalable, simple to implement, and introduces no bandwidth and practically no processing overhead on the network equipment. It is capable of tracing thousands of simultaneous attackers during DDOS attack. All of the processing is done at the victim. The trace-back process can be performed post-mortem, which allows for tracing the attacks that may not have been noticed initially. The involvement of the Internet service providers (ISP) is very limited, and changes to the infrastructure and operation required to deploy DPM are minimal. DPM performs the trace-back without revealing the internal topology of the provider's network, which is a desirable quality of a trace-back scheme. DPM is a packet marking algorithm. The 16-bit Packet ID field and 1-bit Reserved Flag (RF) in the IP header will be used to mark packets. Each packet is marked when it enters the network. This mark remains unchanged for as long as the packet traverses the network. The interface makes a distinction between incoming and outgoing packets. Incoming packets are marked; outgoing packets are not marked. This ensures that the egress router will not overwrite the mark in a packet placed by an ingress router [9].

(2005), BasheerAl-Duwairi, and G.Manimaran: Mentioned about Tracing DoS attacks that employ source address spoofing is an important and challenging problem. Traditional trace-back schemes provide spoofed packets trace-back capability either by augmenting the packets with partial path information (i.e., packet marking), or by storing packet digests or signatures at intermediate routers (i.e., packet logging). Such approaches require either a large number of attack packets to be collected by the victim to infer the paths (packet marking), or a significant amount of resources to be reserved at intermediate routers (packet logging). It adopted a hybrid trace-back approach in which packet marking and packet logging are integrated in a novel manner, so as to achieve the best of both worlds, that is, to achieve small number of attack packets to conduct the trace-back process and small amount of resources to be

allocated at intermediate routers for packet logging purposes. Based on this notion, two novel trace-back schemes were presented. The first scheme, called Distributed Link-List Trace-back (DLLT), is based on the idea of preserving the marking information at intermediate routers in such a way that it can be collected using a link list based approach. The second scheme, called Probabilistic Pipelined Packet Marking (PPPM), employs the concept of a "pipeline" for propagating marking information from one marking router to another so that it eventually reaches the destination [8]. This thesis evaluated the effectiveness of the proposed schemes against various performance metrics through a combination of analytical and simulation studies. Our studies shows that the proposed schemes offer a drastic reduction in the number of packets required to conduct the trace-back process and a reasonable saving in the storage requirement.

(2006), Chao Gong, Kamil Sarac: Described us about tracing IP packets back to their origins is an important step in defending the Internet against denial-of-service (DoS) attacks. Two kinds of IP trace-back techniques have been proposed as packet marking and packet logging approaches. In packet marking, routers probabilistically write their identification information into the forwarded packets. This approach incurred little overhead but requires a large flow of packets to collect the complete path information. In packet logging, routers record the digests of the forwarded packets. This approach made it possible to trace even a single packet and, hence, is considered more powerful. At routers forwarding a large volume of traffic, however, the high storage overhead and access time requirement for recording packet digests introduce practicality problems. This approach presented a novel scheme to improve the practicality of log-based IP trace-back by reducing its overhead on routers. Approach in paper makes an intelligent use of packet marking to help improve the scalability of log-based IP trace-back. This approach used mathematical analysis and simulations to evaluate our approach. Approach considered maintains the ability to trace a single IP packet while reducing the storage overhead by half and the access time overhead by a factor of the number of neighboring routers.This approach referred to a router with high speed links as a high-speed router and also term a packet of interest an attack packet. Similarly, the source and destination of an attack packet is an attacker and a victim respectively [1]. The sequence of routers traversed by an attack packet on its way from source to destination make up an attack path. The attack

path from the attacker to the victim is represented as an ordered list of routers (R1; R2; : : : ; Rm). The objective of IP trace-back is to figure out this ordered list of routers. The process of constructing attack paths is called trace-back process.

(2006), Minho Sung, Jason Chiang, and Jun (Jim) Xu: Described that Recent surveys show that DDOS attack is still one of the major threats to the Internet security. Many techniques have been proposed to trace the origin of attacking packets, known as IP trace-back problem, using either hash-based packet logging or probabilistic packet marking. However, both approaches have scalability problems under the heavy DDOS attacks in terms of the space and computational overheads. This thesis proposed a novel scalable IP Trace-back scheme by utilizing the advantage of both packet logging and marking to balance the overheads at routers and at the victim, hence scalable for both sides. The baseline idea of our approach is to sample a very small percentage (e.g., 1%) of packets at the routers, and save the digests of only sampled packets. At the same time, the routers mark their signature using very simple marking scheme into the marking field of sampled IP packets to send out the "information of logging" to the victim in probabilistic way to help the trace-back procedure. It also proposed a heuristic technique to improve the performance of the marking scheme. In the result, the number of attacking packets the victim should collect for the trace-back procedure to achieve high level of trace-back accuracy is much less than the numbers in previous PPM schemes, and also the computational and storage overhead in routers are much less than previous packet logging approaches [5].

(2008),S.Karthik, Dr. V.P. Arunachalam,Dr.T.Ravichandra: Distributed denial-of-service (DDOS) is a rapidly growing problem. The multitude and variety of both the attacks and the defense approaches is overwhelming. IP trace-back the ability to trace IP packets from source to destination is a significant step toward identifying and, thus, stopping, attackers. The IP trace-back is an important mechanism in defending against distributed denial-of-service (DDOS) attacks. This constructed a simulation environment via extending ns2, setting attacking topology and traffic, which can be used to evaluate and compare the effectiveness of different trace-back schemes. A comparison among some of the Packet Marking schemes is presented with several metrics, including the received packet number required for reconstructing the attacking path, computation complexity and false positive etc. The simulation

approach also can be used to test the performing effects of different marking schemes in large-scale DDOS attacks. Based on the simulation and evaluation results, more efficient and effective algorithms, techniques and procedures to combat these attacks may be developed [27].

(2010), S.mallinga, A. Tamilarasi: Explained that IP trace-back is a mechanism for tracing IP packets back to their sources. Tracing mechanisms include packet marking and logging. Log based trace-back has the ability to backtrack a single packet by logging each packet at intermediate nodes in the networks. Marking based trace-back helps to embed the path information of the intermediate nodes in the packets and the embedded information is used by a victim to reconstruct the attack path. Recent researches showed that the performance of hybrid methods comprising logging and marking are appreciable as they help to trace-back a single attack packet with less storage overhead on routers. In this study, we use a hybrid approach based on marking and logging to trace-back single attack packet with less storage and trace-back overhead on routers. It has been shown this through a mathematical analysis. It also evaluated the trace-back accuracy of our system and other hybrid approaches. Additionally, the simulation results are also presented to verify the effectiveness of the proposed system [23].

2011, R. Sravani, J. Swami Naik: Told about Internet Protocol (IP) trace-back is the enabling technology to control Internet crime. This paper presents a practical IP trace-back system called Flexible Deterministic Packet Marking (FDPM) which provides a defense system with the ability to find out the real sources of attacking packets that traverse through the network. While a number of other trace-back schemes exist, FDPM provides innovative features to trace the source of IP packets and can obtain better tracing capability than others [2]. FDPM adopts a flexible mark length strategy to make it compatible to different network environments; it also adaptively changes its marking rate according to the load of the participating router by a flexible flow-based marking scheme. Evaluations on both simulation and real system implementation demonstrate that FDPM requires a moderately small number of packets to complete the trace-back process; add little additional load to routers and can trace a large number of sources in one trace-back process with low false positive rates. The motivation of this trace-back system is from DDOS defense.

2011, Jun Xu, Xuehai Zhou, Feng Yang: Described that In a hostile environment, sensor nodes may be compromised and then be used to launch various attacks. One

severe attack is false data injection which is becoming a serious threat to wireless sensor networks. An attacker uses the compromised node to flood the network and exhaust network resources by injecting a large number of bogus packets. In this paper, we study how to locate the attack node using a framework of packet marking and packet logging. Proposal of a combined packet marking and logging scheme for trace-back (CPMLT) has been done by us . In CPMLT, one packet can be marked by up to *M* nodes, each node marks a packet with certain probability. When one packet is marked by *M* nodes, the next marking node will log this packet. Through combining packet marking and logging, we can reconstruct the entire attack path to locate the attack node by collecting enough packets. In our simulation, CPMLT achieves fast trace-back with little logging overhead [24].

2011, A.Parvathi and G.L.N.JayaPradha: Presented the idea that Internet Protocol (IP) trace-back is the enabling technology to control Internet crime. In this paper, we present a novel and practical IP trace-back system called Flexible Deterministic Packet Marking (FDPM) which provides a defense system with the ability to find out the real sources of attacking packets that traverse through the network. While a number of other trace-back schemes exist, FDPM provides innovative features to trace the source of IP packets and can obtain better tracing capability than others. In particular, FDPM adopts a flexible mark length strategy to make it compatible to different network environments; it also adaptively changes its marking rate according to the load of the participating router by a flexible flow-based marking scheme. Evaluations on both simulation and real system implementation demonstrate that FDPM requires a moderately small number of packets to complete the trace-back process add little additional load to routers and can trace a large number of sources in one trace-back process with low false positive rates. The built-in overload prevention mechanism makes this system capable of achieving a satisfactory trace-back result even when the router is heavily loaded. The motivation of this trace-back system is from DDOS defense. It has been used to not only trace DDOS attacking packets but also enhance filtering attacking traffic. It has a wide array of applications for other security systems [26].

2011, Yang Xiang, Member, Ke Li, and Wanlei Zhou: Defined that this paper introduce new information metrics one is generalized entropy metrics and information distance metric to detect low rate DDOS attacks by measuring difference between legitimate traffic and attack traffic. The proposed generalized entropy metric can

detect attacks several hops earlier (three hops earlier while the order) than the traditional Shannon metric. The proposed information distance metric outperforms (six hops earlier while the order) the popular Kullback–Leibler divergence approach as it can clearly enlarge the adjudication distance and then obtain the optimal detection sensitivity. The experimental results showed that the proposed information metrics can effectively detect low-rate DDOS attacks and clearly reduce the false positive rate. Furthermore, the proposed IP trace-back algorithm can find all attacks as well as attackers from their own local area networks (LANs) and discard attack traffic [14].

2012, Dong yan, Yulong wang, Sen su and Fangchun yang: Mentioned about tracing malicious packets back to their source is important to defend the Internet against Denial of Service (DoS) intrusion. IP trace-back is just the technique to realize the goal, it reconstructs IP packets traversed path in the Internet to determine their origins. There are two major kinds of IP trace-back techniques, which have been proposed as packet marking and packet logging. In packet marking, it incurs little overhead, but requires a large number of packets to get the complete path. In packet logging, it requires plenty of storage space to record packet digests information, but has the capability to trace even a single packet. Therefore, it is a new idea to draw on both advantages to get the intrusion source. HIT (Hybrid IP Trace-back) is a representative hybrid IP trace-back approach, but it has some vulnerabilities. It may return incorrect path in the trace-back process, and its storage overhead remains high. This thesis proposed a precise IP trace-back approach with low storage overhead, which improves accuracy and practicality greatly. In the end, the feasibility and effectiveness are evaluated by mathematical analysis and simulations. Packet logging scheme makes routers record the state information of packets, and it has the capability to trace a single packet. Therefore it can provide the straightforward evidence for trace-back. It becomes practical when SPIE appeared, but it still needs great storage space. Packet marking approach makes routers write ID information into packet IP header, and reconstruct the complete path in the victim node. It does not increase storage burden on routers [4].

2013, Vahid Aghaei-Foroushani,A. Nur Zincir-Heywood: Explained an evaluation of two promising schemes for tracing cyber-attacks, the well-known Deterministic Packet Marking, DPM, and a novel marking scheme for IP trace-back, Deterministic Flow Marking, DFM. First of all paper explore the DPM in detail and then by

investigating the DFM, paper analyze the pros and cons of both approaches in depth in terms of practicality and feasibility, so that shortcomings of each scheme are highlighted. This evaluation is based on CAIDA Internet traces October 2012 dataset. The results show that using DFM may reduce as many as 90% of marked packets on average required for tracing attacks with no false positives, while it eliminates the spoofed marking embedded by the attacker as well as compromised routers in the attack path. Moreover, unlike DPM that traces the attack up to the ingress interface of the edge router close to the attacker, DFM allows the victim to trace the origin of incorrect or spoofed source addresses up to the attacker node, even if the attack has been originated from a network behind a network address translation (NAT), firewall, or a proxy server. According to classification by the basic principle, Most of the existing trace-back methods categorize into Logging and Marking groups. In logging methods, the routers keep some specific information of travelling packets. For example, Snoeren et al have suggested generating a fingerprint of the packet, based upon the invariant portions of the packet (source, destination, etc.) and the first 8 bytes of payload. During the trace-back, the routers can verify if a suspicious packet has been forwarded or not [3].

2013, Chaitanya kumar singh, Srinivas koppu, V madhu viswanatham: Presented that Internet is a worldwide network and used in almost every field of work such as industrial, educational, military etc. Based on the use, its security needs differ. Few applications may need less security and few may need high security. Today various internet attacks are being developed every day, such as viruses, DoS (Denial of Service), spoofing, etc. Spoofing is a kind of attack in which attacker masks itself under some other user's IP address. Thus, it is difficult to find the original attacker. Proposed scheme is termed as E-RIHT (Enhanced Routers Interface Hybrid Trace-back) [25].

2013, S.pratusha, M.v sruthi, S.anjali Prasad: Detailed that computer network attacks are on the increase and are more sophisticated in today's network environment than ever before. One step in tackling the increasing spate of attacks is the availability of a system that can trace attack packets back to their original sources irrespective of invalid or manipulated source addresses. Most of these schemes require very large number of packets to conduct the trace-back process, which results in lengthy and complicated procedure [22].

Chapter 3
Related work

There are some survey papers discussing the tradeoffs of different IP trace-back schemes. Current IP trace-back schemes can be classified into five categories: link testing, messaging, logging, packet marking, and hybrid schemes.

3.1 IP trace-back schemes

3.1.1 Link testing

The main idea of the link testing scheme is to start from the victim to trace the attack to upstream links, and then determine which one carries the attack traffic [2].

Disadvantage: It consumes huge amount of resources, introduces additional traffic, and possibly causes denial of service when the number of sources needed to be traced increases.

3.1.2 Messaging

Messaging schemes use routers to send ICMP messages from the participating routers to destinations. For a high volume flow, the victim will eventually receive ICMP packets from all the routers along the path back to the source, revealing its location.

Disadvantage:

The disadvantages of messaging schemes are that the additional ICMP traffic would possibly be filtered by some routers, and huge number of packets is required by the victim to identify the sources.

- Logging schemes include probabilistic sampling and storing transformed information [2]. Logging schemes maintain a database for all the traffic at every router within the domain and to query the database to identify the sources of an IP packet. Hash function or Bloom filter is used to reduce the data stored.
- The main disadvantage of logging schemes is that they heavily overload the participating routers by requiring them to log information about every packet passing by, although it is claimed that it needs only a single packet to find its origin.

Some trace-backing schemes are there which are mentioned below.

3.1.3 Hybrid trace-back scheme

A hybrid trace-back scheme combining logging and packet marking is presented to achieve the small number of packet needed to trace a single source and the small amount of resources to be allocated to the participating routers. Although the hybrid schemes try to overcome the disadvantages of each trace-back scheme, the complexity of such combination and the practicability of their implementation still need more research.

3.1.4 Packet marking schemes

Packet marking schemes insert trace-back data into an IP packet header to mark the packet on its way through the various routers from the attack source to the destination; then the marks in the packets can be used to deduce the sources of packets or the paths of the traffic [26] .

As this method overwrites some rarely used fields in IP header, it does not require modification of the current Internet infrastructure. This property makes it a promising trace-back scheme to be part of DDOS defense systems. However, the space in IP header that can be utilized is limited. Thus, the information that one packet can carry is also limited.

Therefore, many challenges for this category of trace-back schemes are raised. For example, the number of sources that can be traced could be limited, the number of packets required to find one source could be large, and the load of the trace-back router could be heavy.

3.1.5 Probabilistic Packet Marking Schemes

Probabilistic Packet Marking (PPM) is one stream of the packet marking methods. The assumption of PPM is that packets are much more frequent than the normal packets. It marks the packets with path information in a probabilistic manner and enables the victim to reconstruct the attack path by using the marked packets. PPM encodes the information in rarely used 16-bit Fragment ID field in the IP header. To reduce the data that is to be stored in 16 bits, the compressed edge fragment sampling algorithm is used. Although PPM is simple and can support incremental deployment, it has many shortcomings that can seriously prevent it from being widely used.

3.1.6 Deterministic Packet Marking Schemes

Another stream of packet marking methods, which does not use the above probabilistic assumption and stores the source address in the marking field, is in the category known as the deterministic approaches, such as Deterministic Packet Marking (DPM).The DPM scheme was modified to reduce false positive rates by adding redundant information into the marking fields. Unlike PPM, deterministic approaches only keep the first ingress edge router's information in the marks (but not the whole path). Moreover, they record marks in a deterministic manner (but not a probabilistic manner as in PPM).

- Tracing Capability is less.
- The path reconstruction process requires high computational work, especially when there are many sources. For example, a 25-source path reconstruction will take days, and thousands of false positives could happen.
- When there are a large number of attack sources, the possible rebuilt path branches are actually useless to the victim because of the high false positives.

3.1.7 Flexible deterministic packet parking approach

The FDPM scheme utilizes various bits (called marks) in the IP header. The mark has flexible lengths depending on the network protocols used, which is called flexible mark length strategy. When an IP packet enters the protected network, it is marked by the interface close to the source of the packet on an edge ingress router. The source IP addresses are stored in the marking fields. The mark will not be overwritten by intermediate routers when the packet traverses the network. At any point within the network, e.g., the victim host, the source IP addresses can be reconstructed when required [7]. Processing packets consume resources such as memory and CPU time of a participating router. Therefore, it is possible for a router to be overloaded when there are a large number of arrival packets waiting for FDPM to mark them. The flow-based marking scheme is proposed to solve the overload problem. When the load of a router exceeds a threshold, the router will discern the most possible attacking packets from other packets then selectively mark these packets. The aim is to alleviate the load of the router while still maintaining the marking function. The flexibility of FDPM is twofold. First, it can use flexible mark length according to the

network protocols that are used in the network. This characteristic of FDPM gives it much adaptability to current heterogeneous networks. Second, FDPM can adaptively adjust its marking process to obtain a flexible marking rate. This characteristic prevents a trace back router from the overload problems.

Advantages:

- Easy to find out packet loss and Duplicate packets.
- Reduces the network traffic.
- Bandwidth consumption is less.
- Flexible mark length: The length of marking field can be adjusted according to the network protocols deployed.
- Flexible mark rate: The marking rate can be changed adaptively according to the load of the participating router.
- Low false Positive rate.
- Number of packets required is comparatively less.
- Better Tracing Capability.
- It has Different probabilities that a router marks the attack packets.

3.2 Encoding in FDPM

Before the FDPM mark can be generated, the length of the mark must be determined based on the network protocols deployed within the network to be protected. According to different situations, the mark length could be 24 bits long at most, 19 bits at middle, and 16 bits at least. Therefore, the flexible length of the marks results in three variations of the encoding scheme, which are named as FDPM-24, FDPM-19, and FDPM-16. FDPM encoding scheme is shown in Fig. 1. The ingress IP address is divided into k segments and stored into k IP packets. The padding is used to divide the source IP address evenly into k parts. For example, if k = 6, the source address is added with 4 bits of 0, making it 36 bits long, then each segment will be 6 bits long. The segment number is used to arrange the address bits into a correct order. The address digest enables the reconstruction process to recognize that the packets being analyzed are from the same source. Without this part, the reconstruction process cannot identify packets coming from different sources, thus will not be able to trace multiple IP packets.

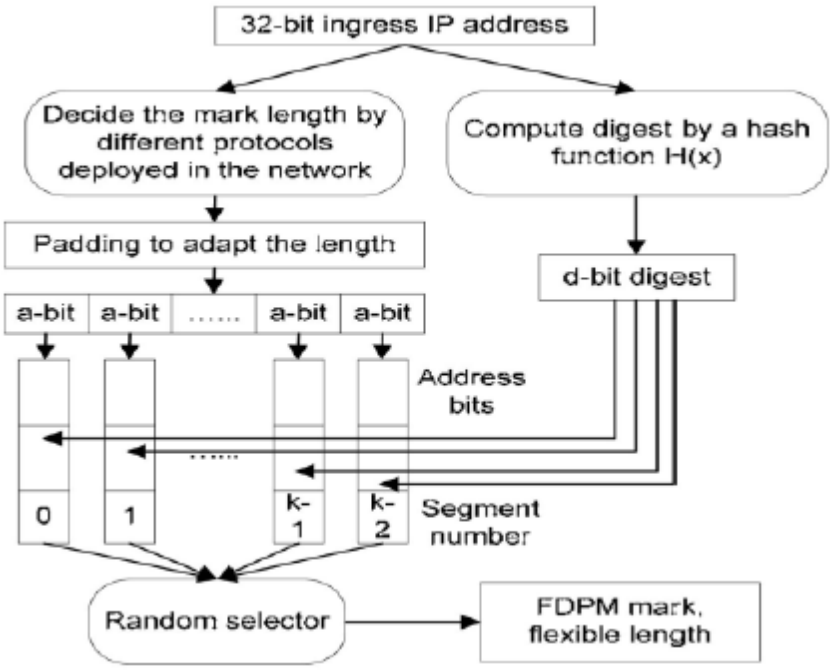

Figure 3.1 FDPM encoding Scheme [2]

In FDPM, before the encoding process begins, the length of the mark must be calculated. If the TOS field in the IP packet is not used by the protected network, the 1-bit Reserved Flag in the header is set to 0, and the length of mark is set to 24. Under other situations, the length of mark will be 19 or 16, with relevant bit(s) in TOS marked. If the network supports TOS Precedence but not TOS Priority, fourth to sixth bits of TOS are utilized for marking; and if the network supports TOS Priority but not TOS Precedence, first to third bits of TOS are utilized for marking.

3.3 Basic deterministic packet marking (DPM)

The basic DPM is a packet marking algorithm, which was first introduced in this section provides the general principle behind DPM and discusses the most basic implementation of the proposed scheme

3.3.1 DPM Principle

As mentioned above, DPM is a packet marking algorithm. The 16-bit Packet ID field and 1-bit Reserved Flag (RF) in the IP header will be used to mark packets. Each packet is marked when it enters the network. This mark remains unchanged for as long as the packet traverses the network.

The packet is marked by the interface closest to the source of the packet on an edge ingress router. The mark is partial address information of this interface. The interface makes a distinction between incoming and outgoing packets. Incoming packets are marked; outgoing packets are not marked. This ensures that the egress router will not overwrite the mark in a packet placed by an ingress router. For illustrative purposes, assume that the Internet is a network with a single administration. In this case, only interfaces closest to the customers on the edge routers will participate in packet marking. Every incoming packet will be marked. Should an attacker attempt to spoof the mark in order to deceive the victim, this spoofed mark will be overwritten with a correct mark by the very first router the packet traverses.

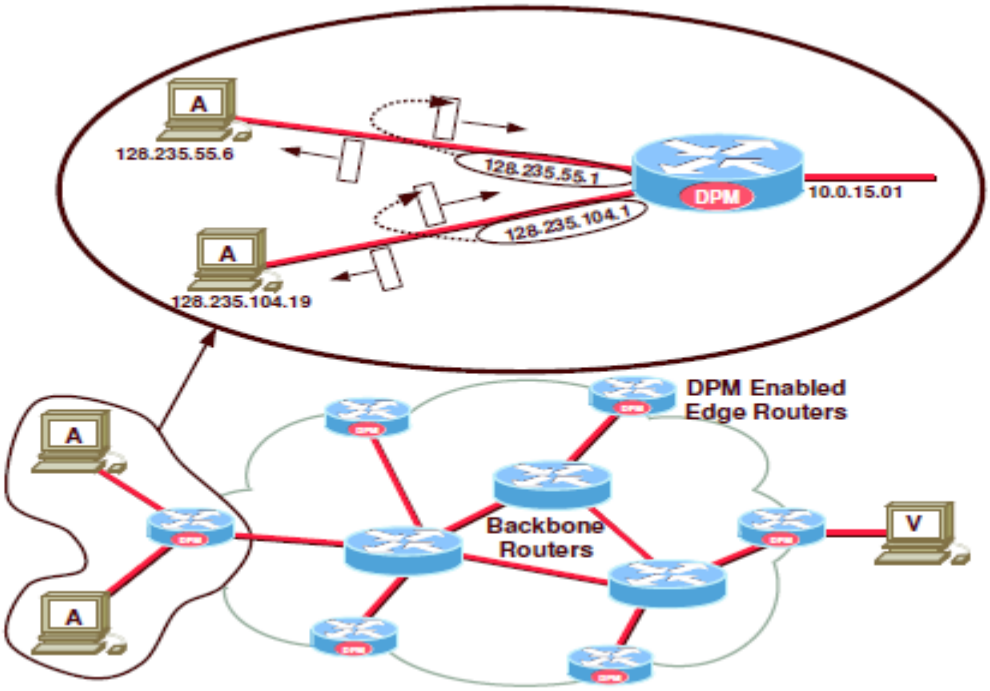

Figure 3.2 Deterministic packet marking [9]

3.3.2 Shortcomings of basic DPM with respect to DDOS

The problem with the basic DPM, which causes the inability to handle a certain type of DDOS attacks, lies in the fact that the destination would associate segments of the ingress address with the source address of the attacker. If it could be guaranteed that only one host participating in the attack has a given source address, even though it might have been spoofed, and that the attacker would not change its address during the attack, there would be no problems. There are two situations when the

reconstruction procedure of the basic DPM will fail. First, consider the situation when two hosts with the same Source Address (SA) attack the victim. The ingress addresses corresponding to these two attackers are A0 and A1, respectively. The victim would receive four address segments: A0[0], A0[1], A1[0], and A1[1]. The victim, not being equipped to handle such attack would eventually reconstruct four ingress addresses, since four permutations are ultimately possible: A0[0]**.**A0[1], A0[0]**.**A1[1], A1[0]**.**A0[1], and A1[0]**.**A1[1], where `**.**' denotes concatenation. Only two of the four would be valid. A typical metric of evaluation of the trace-back schemes for DDOS attacks is the rate of false positives or false positive rate. In the context of DPM, a false positive is denied as an incorrectly identified ingress address. The rate of false positives refers to the ratio of the incorrectly identified ingress addresses to the total number of identified ingress addresses. In the example described above, the false positive rate for that particular attack is 50%. Clearly, the false positive rate would increase even further if the number of attackers, with the same SA, was larger. Second, consider a (D)DoS attack, where the attackers change their source addresses for every packet they send. The basic DPM will be unable to reconstruct any valid ingress addresses, since none of the entries in the Ingress table would have a complete ingress address.

3.3.3 Hash-Based DDOS modification to DPM

The scheme described in this section utilizes a hash function, H(x). To simplify the performance analysis, the hash function is assumed to be ideal. An ideal hash function minimizes the chances of collision, an occurrence when two different ingress addresses result in the same hash value. In other words, H(x) is assumed to produce a collision only after all possible hash values have been produced. It is also assumed that the hash function is known to everybody, including all DPM-enabled interfaces, all destinations, which intend to utilize DPM marks for trace-back, and the attackers. The constraint of 17 bits still remains, so a longer digest would result in fewer bits of the actual address transmitted in each mark, and consequently, the higher number of packets required for trace-back. Mark Encoding Recall that in the basic DPM, the ingress address was divided in two segments. In this modified scheme, the ingress address is divided in k segments. Also, more bits would be required to identify the segment. Instead of a single bit required for two segments in the basic DPM, log2(k) would be required for this scheme. The remaining bits would be used for the digest.

Independently of what segment of the address is being sent to the victim, the digest portion of the mark will always remain the same for a given DPM interface. This would enable the victim to associate the segments of the ingress address with each other to reconstruct the whole address.

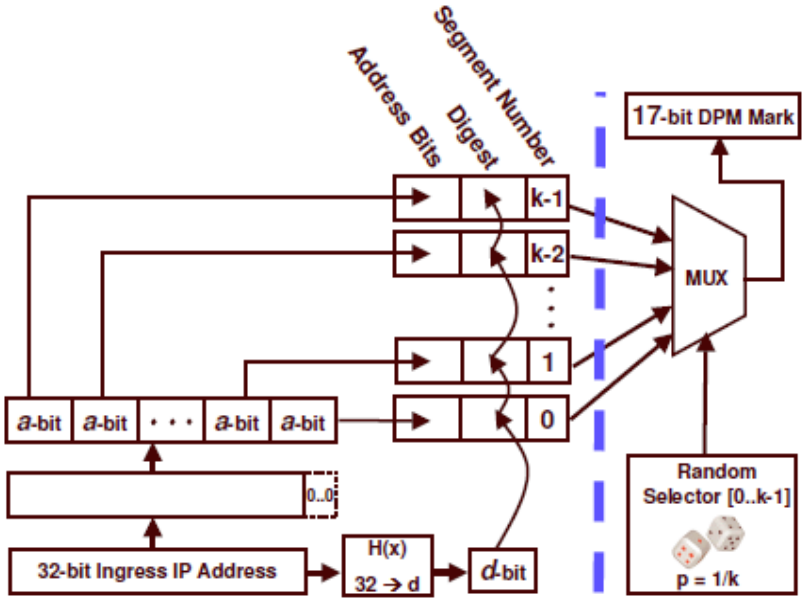

Figure 3.3 Single digest DDOS Modification [9]

The DPM mark consists of three fields: a-bit address bits field, d-bit digest field, and s-bit segment number field. Some padding may be required so that the address is split into segments with equal length. For example if the ingress address is divided in 5 segments, it would be necessary to pad it with `000' to make it 35-bit long. At startup the DPM-enabled interface prepares k marks for all segments of the address. A d-bit hash value, or digest, of the ingress address is calculated once and then inserted in the digest field of every mark. Each of k marks will have address bits set to a different segment of the ingress address. The segment number field will be set to the appropriate value. These operations are shown to the left of the bold dotted line in The processing required for every packet will be limited to generating a small random number from 0 to k – 1 and inserting a corresponding mark into the packet header. According to classification by the basic principle, Most of the existing trace-back methods categorize into Logging and Marking groups. In logging methods, the routers keep some specific information of travelling packets. For example, Snoeren have suggested generating a fingerprint of the packet, based upon the invariant portions of the packet (source, destination, etc.) and the first 8 bytes of payload. During the trace-

back, the routers can verify if a suspicious packet has been forwarded or not Further improvement in terms of logging only a small portion of each travelling packet at the transient routers have been proposed. One of the major problems of the logging method is the requirement for high amount of memory and CPU usage on the routers in the attack paths.

In marking methods, some or all routers in an attack path send specific information along with traveling packets. The destination may use this information to trace the attacker even if the source IP has been spoofed. This information could be either embedded in the packet's IP header or sent by generating new packets and consume extra bandwidth. In particular, Savage have described a technique for tracing anonymous packet flooding attacks on the Internet back toward their source. This trace-back can be performed after an attack is identified. While each marked packet represents only a sample of the path it has traversed, by combining a modest number of such packets, a victim can reconstruct the entire attack path. Dean have presented a scheme for providing trace-back data by having routers embedding specific information into packets randomly. This is similar to the technique used by Savage with the major difference being that it is based on algebraic techniques. On the other hand, Song presents two new IP marking techniques to solve the IP trace-back problem: The Advanced Marking Scheme and the Authenticated Marking Scheme. The Authenticated Marking Scheme supports authentication of routers' markings. This prevents a compromised router from forging other uncompromised routers markings. Doeppner identify the source of Denial of Service attacks, provided that a significant percentage of packets are sent from one subnet. In this method, each router marks its own IP address to the travelling packet with a determinable probability. Moreover, Tseng have proposed a modification to the PPM to ensure that the probability of receiving the mark is equal to the original marking probability. Yaar have proposed a method of encoding path identification by marking packets with path fingerprints. They have also another research based on the PPM with further improvements such as 1-bit distance. Victims can identify attack paths after receiving tens of packets encoding. It detects the distance of the attacker by changing the TTL field and storing 1 bit in the IP header. Goodric have proposed to use relatively large, randomized messages to encode router information. The main idea is to have each router fragment its message into several words, then include a large checksum cord on the entire message randomly in the reusable bits of such a word fragment. Instead of

the recovery of the full paths, Belenky proposed to only record the IP addresses of ingress edge routers. Their scheme, Deterministic Packet Marking (DPM), is simple and easy to implement, and has a little overhead on routers and the victim. Aghaei-Foroushani proposed the Deterministic Flow Marking (DFM) approach, which allows the victim to trace-back the origin of an incorrect or spoofed source IP address up to the attacker node, even if the attack has been originated from a network behind a NAT or a proxy server. This scheme has low processing and memory overhead at the victim machines and edge routers. Additionally, DFM provides an optional authentication, so that a compromised router cannot forge markings of other uncompromised routers. Yan take advantage of both marking and logging methods and combines both approaches at routers in an attack path. Most marking methods use 16 bits of identification field. However, some other works propose to use 17 bits (identification field and reserved flag) bits (identification and TOS fields plus reserved flag) 25 or 32 bits (identification field, flag and fragment offset

In deterministic methods, regardless of the marking or logging, every packet should be processed at both the source and the destination end. In comparison to the probabilistic methods, these methods require more processing overhead but higher accuracy. For example, Belenky embed the upper or the lower half of the IP address of the ingress interface into the fragment id field of the packet with a probability of 0.5. Then, they set a reserve bit indicating which portion of the address is contained in the fragment field. Some well-known examples of probabilistic methods are PPM and many of its variants. From the perspective of the location based classification, existing trace-back methods are divided into two types: those that send trace-back information by the edge routers closest to the source (source group), and those that send trace-back information by some or all routers in the attack path on the network (network group), respectively. Most of the current trace-back methods belong to the network group. The purpose of these methods is to identify the attack path entirely or partially. The drawbacks of these methods are the requirement of involvement of all the routers along the paths and high resource consumption in terms of the processing time and memory. While the goal of source group methods is to identify the attack source, they do not identify the attack path.

Chapter 4
Problem statement

4.1 Gaps in Study

The previous work adopted a hybrid trace-back approach in which packet marking and packet logging are integrated to achieve the best of both worlds (i.e., small number of attack packets to conduct the trace-back process, and small amount of resources to be allocated at intermediate routers for packet logging purposes). Based on this notion, two trace-back schemes were proposed. The first scheme, called Distributed Link-List Trace-back (DLLT), is based on the idea of preserving the marking information at intermediate routers in such a way that it can be collected in an efficient manner. The second scheme, called probabilistic pipelined packet marking (PPPM), employed the concept of "pipeline" for propagating marking information from one marking router to another so that it eventually reaches the destination. Their probabilistic nature of marking and storage offers the advantage of minimizing router's processing and storage overhead. Also, both schemes eliminate attacker's ability to mislead the victim. This is achieved in DLLT by storing the packet digests at intermediate routers, which provides an authentic way to verify that a given router has actually forwarded certain packet. In PPPM, spoofed marking information written by the attacker can be discarded by observing that the distance associated with it is always the largest among distances obtained for marking information that correspond to the same packet. Marking information is collected from intermediate routers efficiently. For example, DLLT collects relevant marking information from specific routers in a predetermined manner using the link list approach. PPPM collects the marking information by loading them into packets going to the same destination. It is not claimed by us that DLLT and PPPM are perfect IP trace-back schemes. In general, for such schemes to be practically efficient they must be secure, backward compatible and requires low storage. A study in terms of saving information for "selective packet flows" instead of "per packet information" may improve the scalability of the proposed hybrid IP trace-back schemes. Probabilistic packet marking has been proposed for tracing the source i.e., origin of an DoS attack. While PPM has the advantages of efficiency and implements ability over deterministic packet marking and router based logging/messaging, it has the potential

drawback that an attacker may impede trace-back by sending packets with spoofed marking field values as well as spoofed source IP addresses. This thesis analyzed the effectiveness of PPM in a mini max adversarial context where the attacker is allowed to spoof the marking field to achieve maximum confusion at the victim. Previous analysis showed that, while it is always possible for an attacker to impede exact trace-back by the victim, the attacker's ability to affect uncertainty is limited in internetworks with bounded diameters similar to the Internet, when a suitable marking probability is chosen. Thus, for single source attacks PPM is effective at localizing the attack origin. In a distributed DoS attack, however, as the number of attack sources mounted increases, trace-back is rendered more difficult due to an uncertainty amplification effect above and beyond the distribution factor M. In this work, an evaluation and a comparison of two IP trace-back techniques has been proposed by us, the well-known Deterministic Packet Marking (DPM), and a novel marking scheme for IP trace-back proposed by the authors, Deterministic Flow Marking (DFM), from the perspective of practicality and feasibility. Vahid Aghaei-Foroushani IEEE Security and Privacy authors employed the CAIDA Internet traces October 2012 dataset, and used a number of metrics to evaluate the performance of disparate trace-back schemes, including the computational overhead, the memory overhead, the bandwidth overhead, the trace-back rate, the false positive rate, mark spoofing by attackers or subverted routers in the attack path, the number of required packets for trace-back, the percentage of marked packets, ISP involvement, the ability to handle fragmentation, the ability to handle major DDoS attacks, and the maximum trace-back ability [3].

In this work we will be evaluating IP trace-backing scheme on IPv6 by embedding it on existing security systems and framework.

Chapter 5
Implementation

5.1 NS2

NS (Network Simulator) is a discrete event simulator targeted at networking research. NS provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks. NS2 is an open-source event-driven simulator designed specifically for research in computer communication networks. Since its inception in 1989, NS2 has continuously gained tremendous interest from industry, academia, and government. Having been under constant investigation and enhancement for years, NS2 now contains modules for numerous network components such as routing, transport layer protocol, application, etc. To investigate network performance, researchers can simply use an easy-to-use scripting language to configure a network, and observe results generated by NS2. Undoubtedly, NS2 has become the most widely used open source network simulator, and one of the most widely used network simulators. Network Simulator (Version 2), widely known as NS2, is simply an event driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done using NS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors. Due to its flexibility and modular nature, NS2 has gained constant popularity in the networking research community since its birth in 1989. Ever since, several revolutions and revisions have marked the growing maturity of the tool, thanks to substantial contributions from the players in the field. Among these are the University of California and Cornell University who developed the REAL network simulator, the foundation which NS is based on. Since 1995 the Defense Advanced Research Projects Agency (DARPA) supported development of NS through the Virtual Inter-Network Test-bed (VINT). Currently the National Science Foundation (NSF) has joined the ride in development. Last but not the least, the group of researchers and developers in the community are constantly working to keep NS2 strong and versatile.

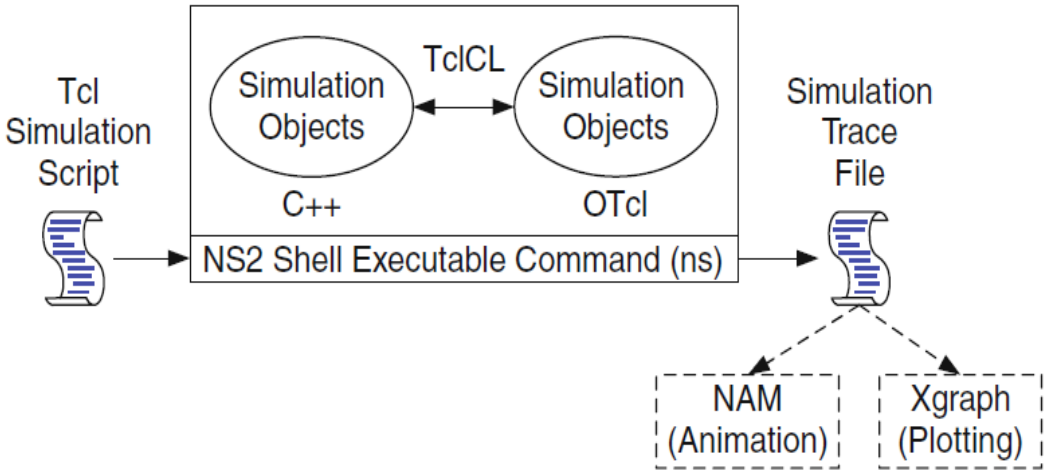

Figure 5.1 Basic architecture of NS.

Figure 5.1 shows the basic architecture of NS2. NS2 provides users with executable command ns which take on input argument, the name of a Tcl simulation scripting file. Users are feeding the name of a Tcl simulation script (which sets up a simulation) as an input argument of an NS2 executable command ns. In most cases, a simulation trace file is created, and is used to plot graph and/or to create animation. NS2 consists of two key languages: C++ and Object-oriented Tool Command Language (OTcl). While the C++ defines the internal mechanism of the simulation objects, the OTcl sets up simulation by assembling and configuring the objects as well as scheduling discrete events (i.e., a frontend). The C++ and the OTcl are linked together using TclCL. Mapped to a C++ object, variables in the OTcl domains are sometimes referred to as handles. Conceptually, a handle (e.g., n as a Node handle) is just a string in the OTcl domain, and does not contain any functionality. Instead, the functionality (e.g., receiving a packet) is defined in the mapped C++ object (e.g., of class Connector). In the OTcl domain, a handle acts as a frontend which interacts with users and other OTcl objects. It may defines its own procedures and variables to facilitate the interaction. Note that the member procedures and variables in the OTcl domain are called instance procedures NS2 provides a large number of built-in C++ objects. It is advisable to use these C++ objects to set up a simulation using a Tcl simulation script. However, advance users may find these objects insufficient. They need to develop their own C++ objects, and use a OTcl configuration interface to put together these objects.

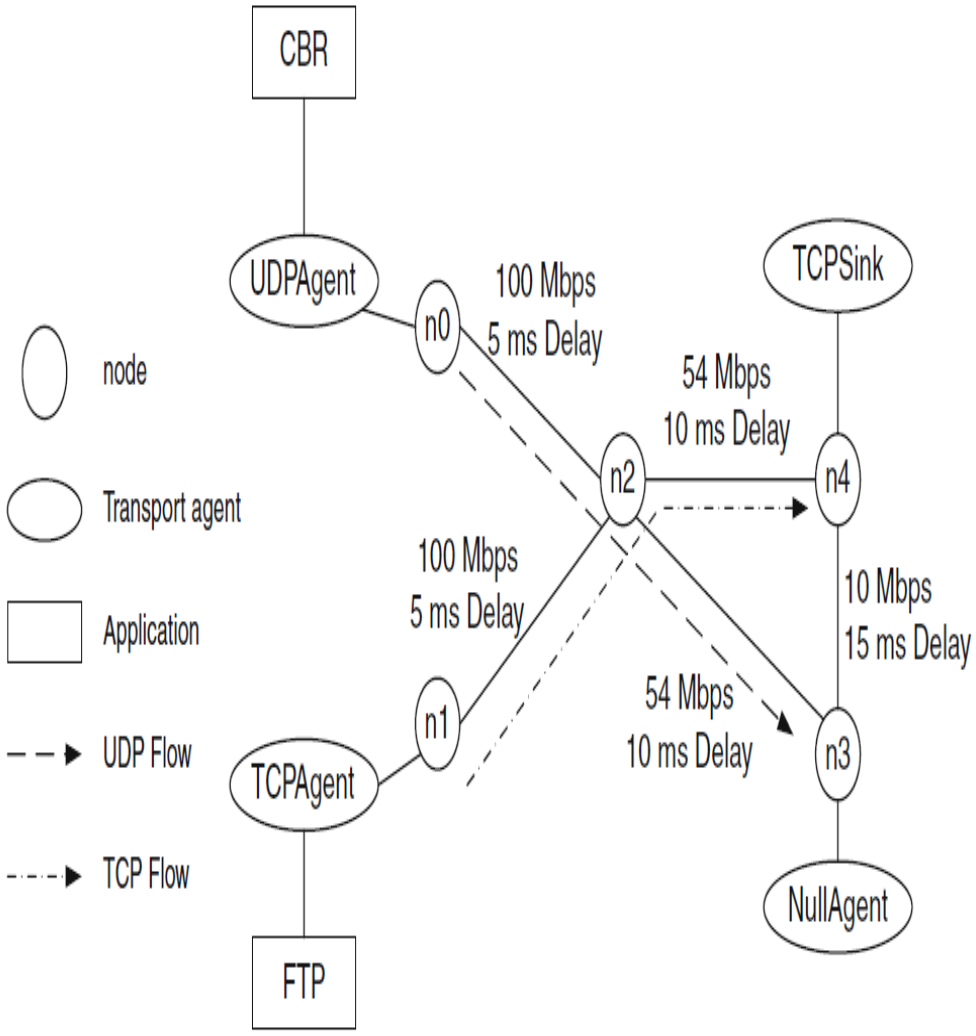

Figure 5.2 Working of NS2

5.1.1 Features of NS2

- Protocols: TCP, UDP, HTTP, Routing algorithms etc
- Traffic Models: CBR, VBR, Web etc
- Error Models: Uniform, bursty etc
- Radio propagation, Mobility models
- Energy Models
- Topology Generation tools
- Visualization tools
- Extensibility

5.2 Flow chart of implementation:

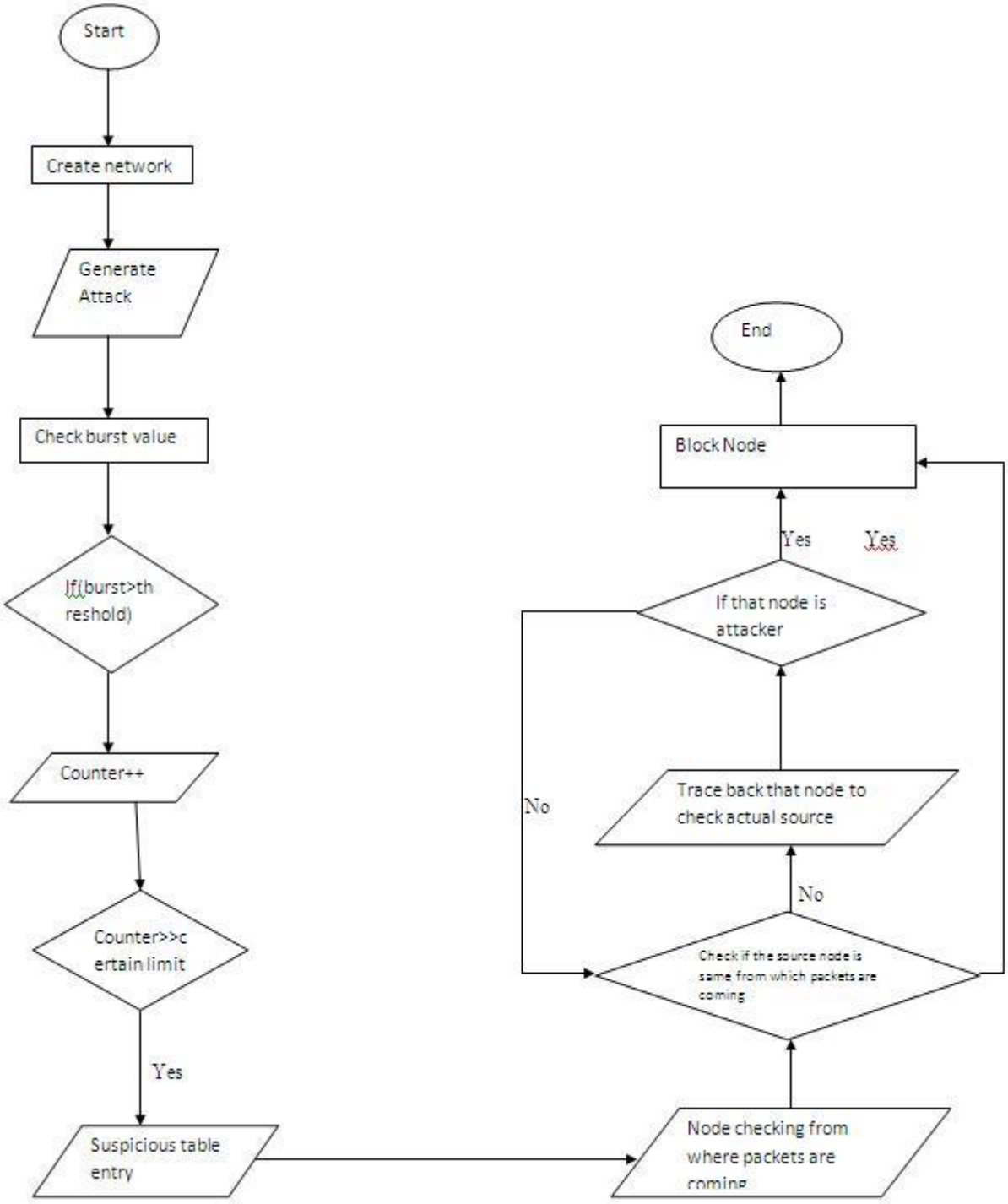

Figure 5.3 Flow diagram for Trace-Back

As shown in the flow chart if attacker attacks on the network it will take the following steps.

- If the traffic that is received, during the burst, by receiver is same as that of sender node, then it will be placed in the suspicious list and all nodes in that list will be supervised by the network admin in every unit time.
- If the burst is in the regular pattern then put nodes will be put together in the temporary table and also will add a counter with it.
- If counter is greater than a certain limit that is assumed as 3 then put that node in the blocking list and trace-back the source node.
- If the source node is the same as that in network it will be completely blocked otherwise trace-back to previous node to reach to the source node.
- At last attacking node will be discovered and will be blocked it completely.

5.3 Assumptions

In order to make our marking scheme more practical and effective, the following assumptions have been made in devising our proposed IP Trace-back method.

1. Attackers are able to generate any packets
2. Multiple attack paths may exist
3. Packets may be reordered or lost
4. Routes between the attacker and the victim are fairly stable
5. The resources of the routers are limited so that the routers cannot perform too much processing per packet.
6. Attackers might be aware that they are being traced
7. Attackers may send a large number of packets
8. Routers might be compromised; but the nearest routers should not be compromised in big proportion.

The first five assumptions are quite easy to understand with the knowledge of current network infrastructure. The sixth one is a conservative evaluation of the abilities of the attackers. The sophisticated attackers should be aware that they are being traced and may send fake packets to make the victim confused. So the Trace-back method proposed must consider such an ability of the attackers. Like the probabilistic marking scheme, our marking scheme marks packets with a very low probability; so it requires a certain number of packets, sent by the attacker, to reconstruct the attack paths. If some routers are compromised, then only reconstruct the attack paths to the corresponding relevant comprised routers since a compromised router could tamper

the information marked by its upstream routers. Therefore a valid suffix instead of the entire attack path to assess the robust of a Trace-back technique is being used . One thing to remind is that the nearest routers should not be compromised; otherwise they can tamper any messages the upstream routers have marked, so that the victim might reconstruct totally wrong paths.

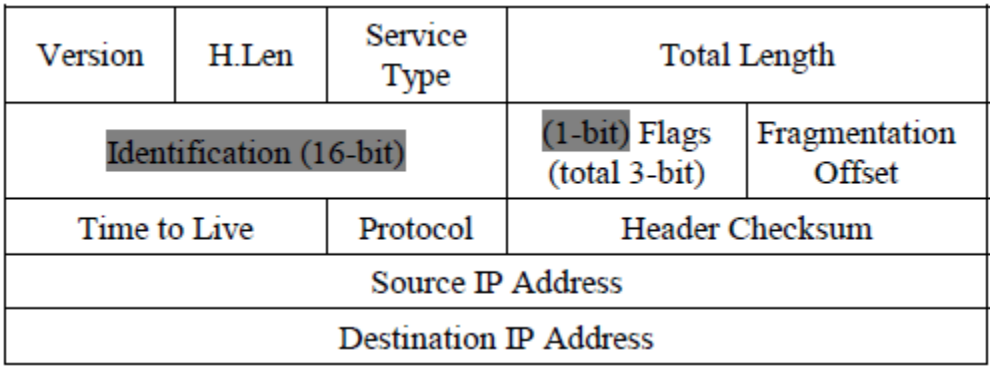

Figure 5.4 IP header

Figure 5.4 shows the structure of the IP header. The 16-bit Identification field allows the destination host to determine which datagram a newly arrived fragment belongs to. Stoica and Zhang pointed out that less than 0.25% of the entire network traffic is fragmented, so the bits for the identification field can be overloaded with the marking information. In addition, one out of three bits in the Flags field is of little use in the current version of IP protocol. Thus up to 17 bits has been used by us to store marking information. The total number of bits *b* needed to store the marking information can be estimated as $b = \log2(p) + \log2(d) + \log2(n)$. The first term estimated the bits needed to store Full path, which has a value less than *p*. The second term estimated the bits needed to store distance, and the third term estimates the bits needed to store *x*. Letting $c = 4$, $d = 32$, $p = 257$, and $n = 2c = 8$, the above expression for b can be computed to a value no more than 17. The reason for setting $n = 2c$ is that each full path is related to $2c$ fragments of two IP addresses as long as we provide $2c$ distinct values of *x*, the two IP addresses can be uniquely identified. Thus 3 bits would be needed to store 8 distinct values of *x*. There is a tradeoff between the number of packets required for reconstruction and the number of bits needed. A smaller value for *c* implies a smaller number of packets and a shorter reconstruction time. However, the total number of bits in the IP header that can be used to store the marking information is quite limited, so eclectically c = 4 has been chosen by us in this implementation. In

general, a packet can reach its destination by passing no more than 32 hops. For reflector attacks, it can be assumed that the distance field of a packet is less than 64. Therefore, 6 bits would be sufficient for the distance field. Then there would be only 8 (17 – 3 – 6) bits left for storing the full path value, which ranges from 0 to 256. Thus two of the values will be in collision. In this implementation, if the full path value calculated by the router is 256, the router would write 0 to the full path field. While doing the attack paths reconstruction, if the path value calculated by the victim is 256, the victim would convert it to 0. With this simple technique employed to handle the collision of two different values, the probability of reconstructing a false positive would be extremely low. In thousands of attack paths reconstruction experiments, no false positives were generated.

5.4 Packet marking procedure in router R

Algorithm 5.1 Packet Marking Algorithm

Procedure Packet_Marking ()

```
1.    for a packet do
2.        generate a counter ctr
3.        if ctr ≤ q then
4.            /* q is the certain limit */
5.            P.distance ← 0
6.            Increment counter integer x
7.            P.x ← x
8.            Fullpath ← (A1,1 + A1,2x + A1,3x2 +A1,4x3) mod p
9.        else if P.distance = 0 then
10.           Fullpath ← (Fullpath + A1,1x4+ A1,2x5+A1,3x6 +A1,4x7) mod p
11.           // x is recorded in the packet to be used for blocking list
12.           P.distance ← P.distance + 1
13.       else if P.distance > 0 then
14.           P.distance ← P.distance + 1
15.       else call error_handler
```

Packet Marking Procedure [9]

```
Marking procedure at router R, edge interface I:
  for each incoming packet w
    let x be a random number from [0, 1)
    if x < 0.5 then
      write I_{0-15} into w.ID_field
      write '0' into w.flags[0]
    else
      write I_{16-31} into w.ID_field
      write '1' into w.flags[0]

Ingress address reconstruction procedure at victim V:
  for each packet w from source S_x
    if IngressTbl[S_x] == NIL then
      create IngressTbl[S_x]
    if w.flags[0] == '0' then
      IngressTbl[S_x]_{0-15} := w.ID_field
    else
      IngressTbl[S_x]_{16-31} := w.ID_field
```

Pseudo code for packet marking [9]

5.5 Marking Algorithm

To resolve the information loss problem caused by attacker. Marked information in each incoming request packet to the outgoing reply packet is being copied. This operation has been carried out through the reflection procedure by each reflector. Note that the number of request packets and the number of reply packets are asymmetric. For example, the number of packets in a GET request message of FTP is small, but those in the reply message may be large. For this reason, a simple copy operation for the marked information may not work. One possible method is to use a table to store the marked information. The reflector simply collects the marked information in the table and copies the relevant marked information to outgoing packets.

5.6 Results

The generation of the simulation scenarios for this network model is shown below. Considering the initial assumptions, here 22 nodes has been taken up in the network with 100Mbps LAN and generating CBR type of traffic in these mobile nodes. Here are some of the screen shots that depict the network simulations.

5.6.1 Simulation:

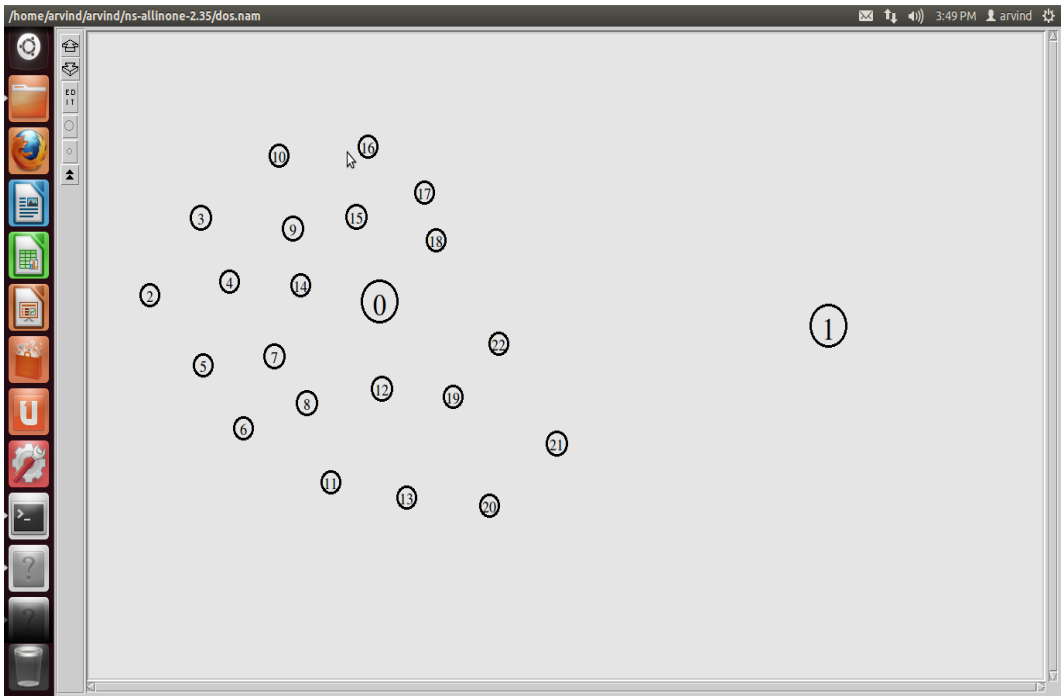

Figure 5.5 Initially all nodes with routers 0 and 1

Figure 5.5 depicts about the initial configuration of the network and the architecture of the network. In this network scenario we have 2 routers those do have mobility will communicate in the network. When the network will initialize or when it will start generating traffic packets will flow in the network as shown in Figure 5.6 and in 5.7. Those 2 graphs depicting about the flow of packets in the network and are communicating with each other.

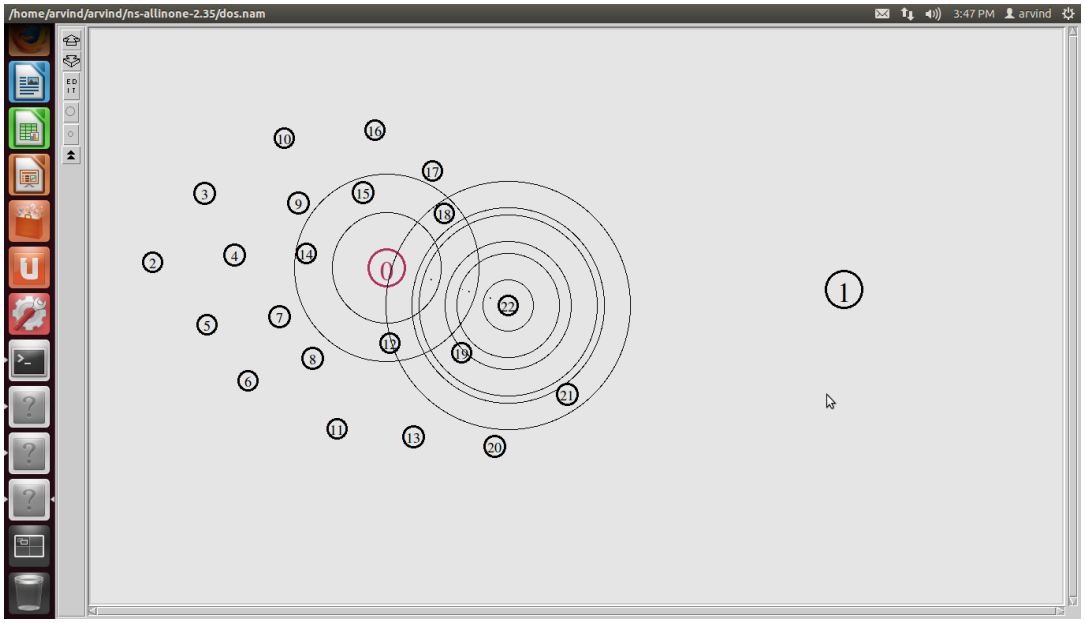

Figure 5.6 Transferring packets

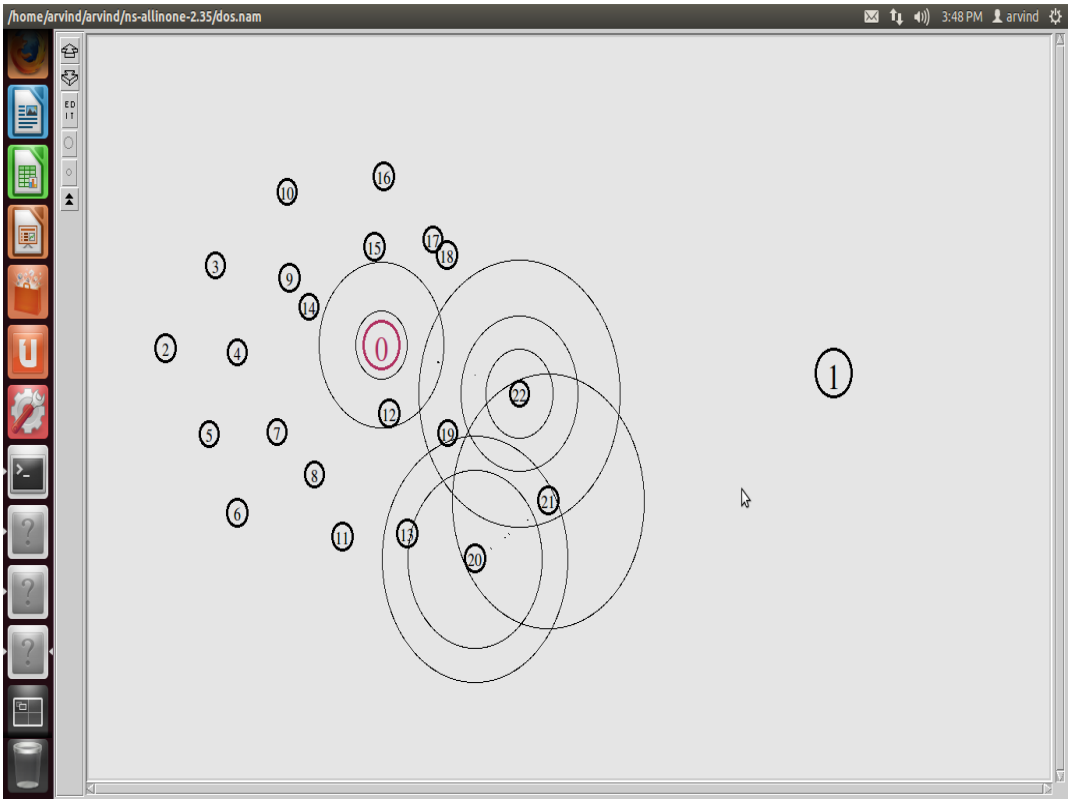

Figure 5.7 Packet received

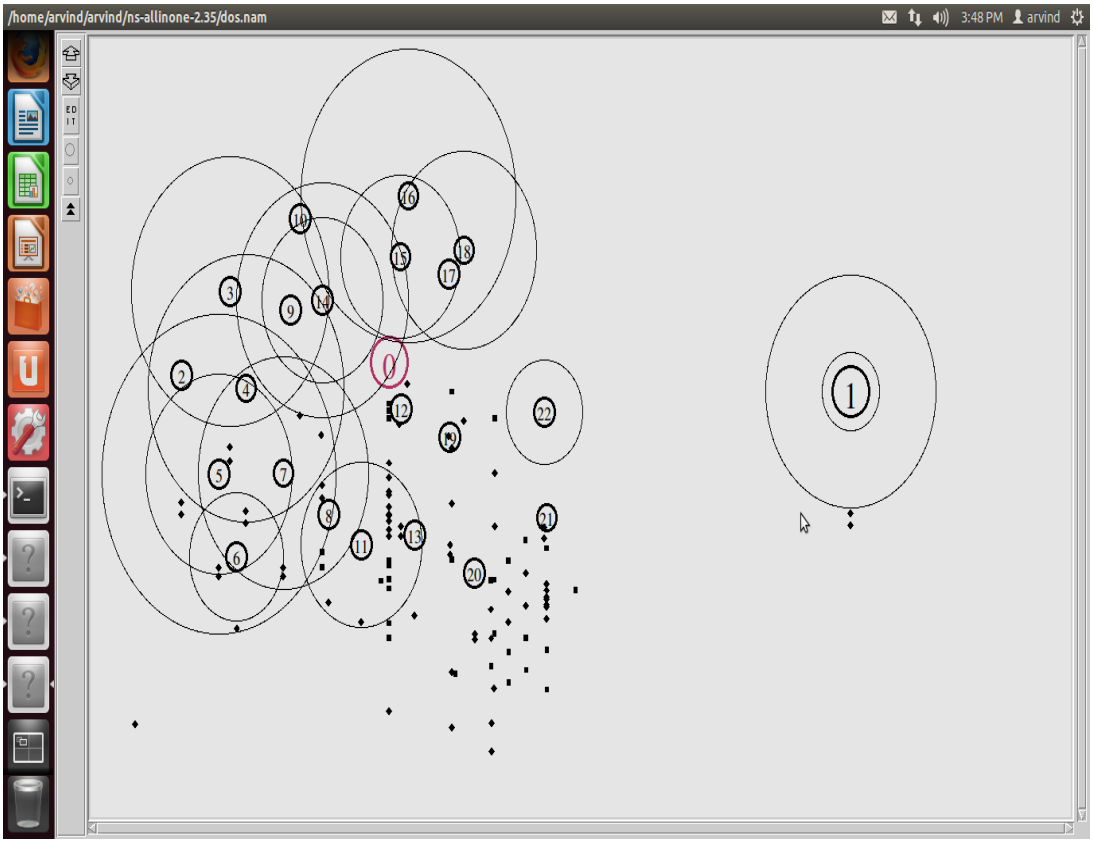

Figure 5.8 Packet dropped

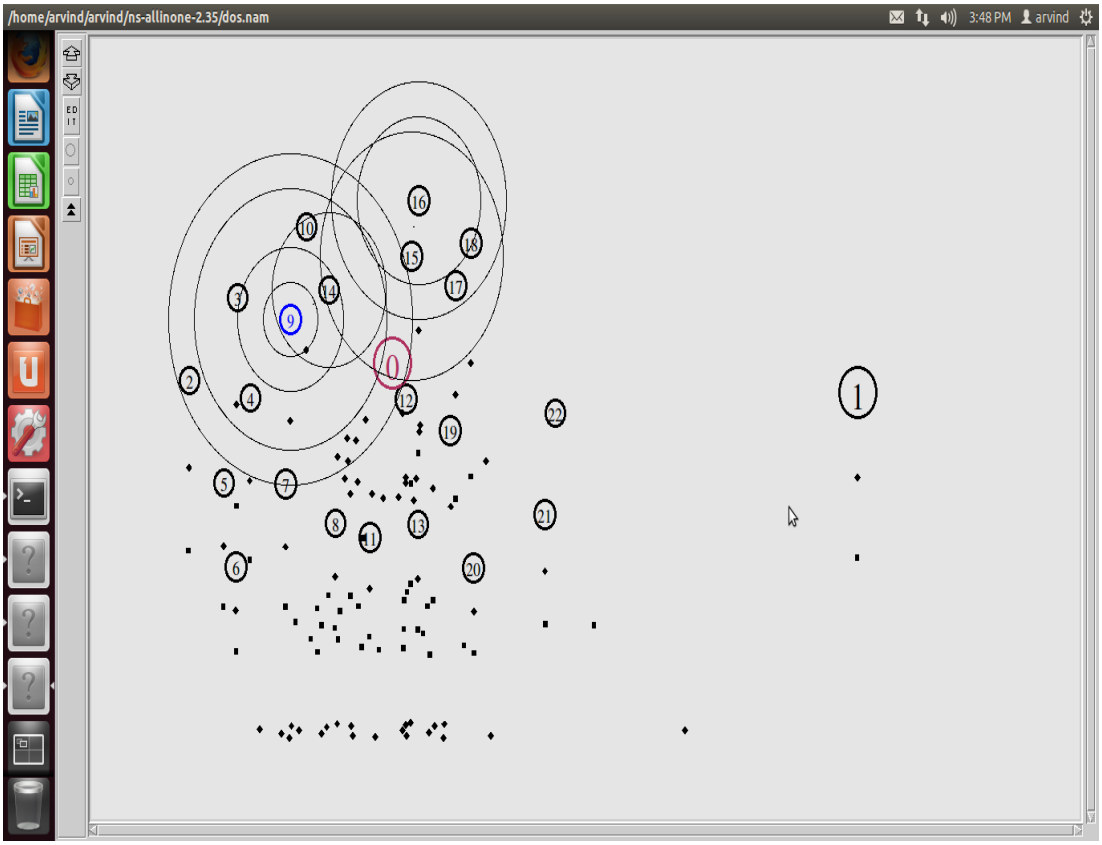

Figure 5.9 Identification of suspicious node

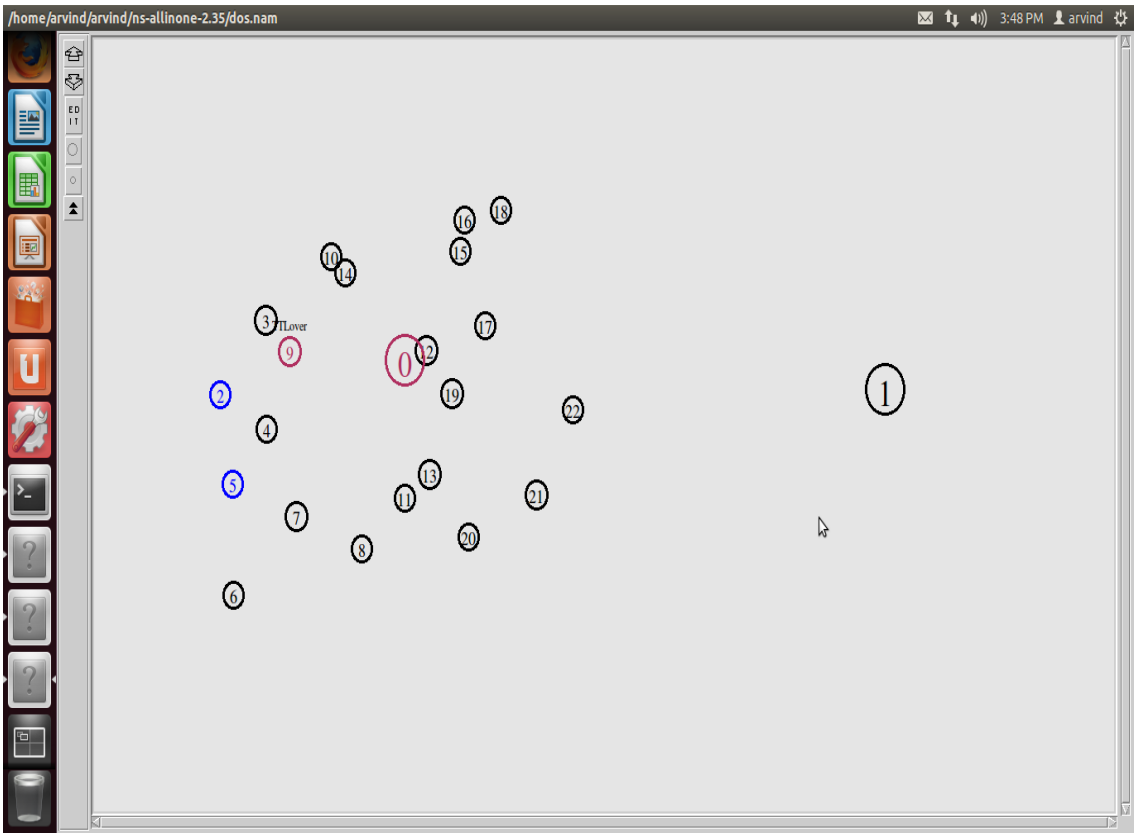

Figure 5.10 Identification of suspicious node (ii)

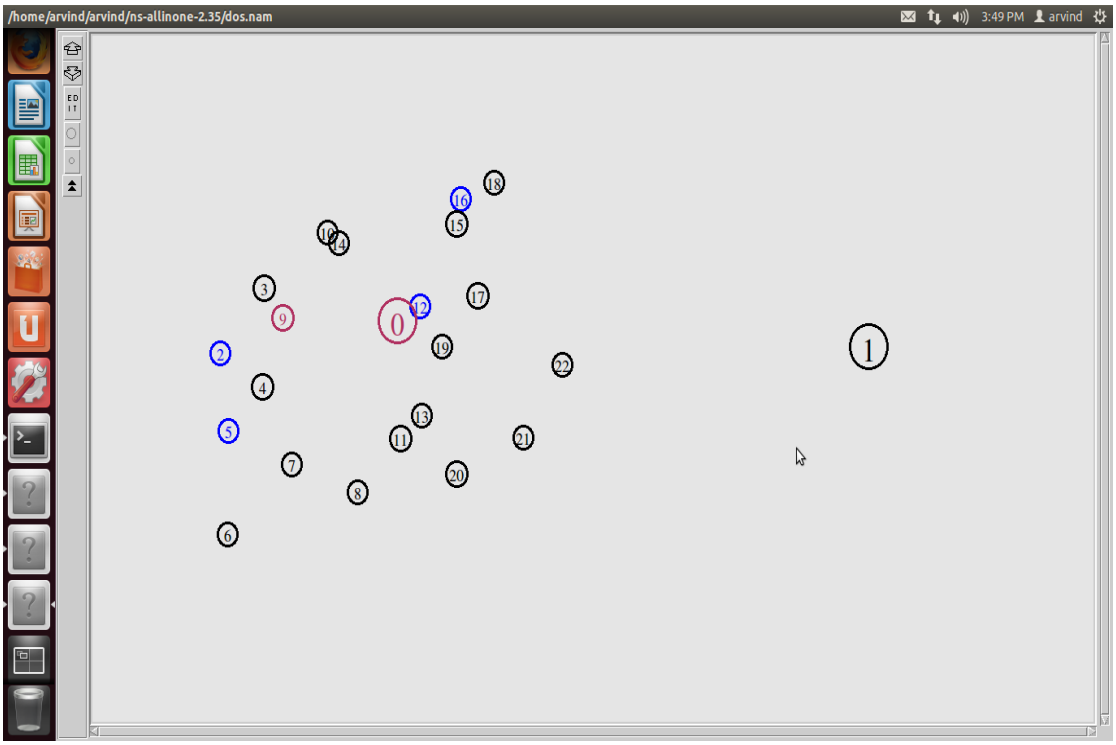

Figure 5.11 Suspicious nodes identified

During the simulation when attacker attacks on the network packet flow will be disturbed and packets will be dropped in the network. There will be packet loss and congestion will be occurring in the network. So on the extreme condition the link will be down and any other path will have to be chosen. Due to the above condition the network will down if all attacks will occurred. To avoid these kinds of conditions we shall detect the attack and mitigate attack. To check out the source node of the attack the technique of IP Trace-backing using packet marking and packet logging has been used by us. This technique has been implemented by us to check that upto which level this method is effective in IPv6. We are using IP Trace-backing in IPv6 to check the network from attacks and to find the relevant results from it

4.6.2 Graphs:

After the simulation of the network, followings graphs were generated with the parameters of bandwidth v/s time, ratio v/s time and traffic received v/s time.

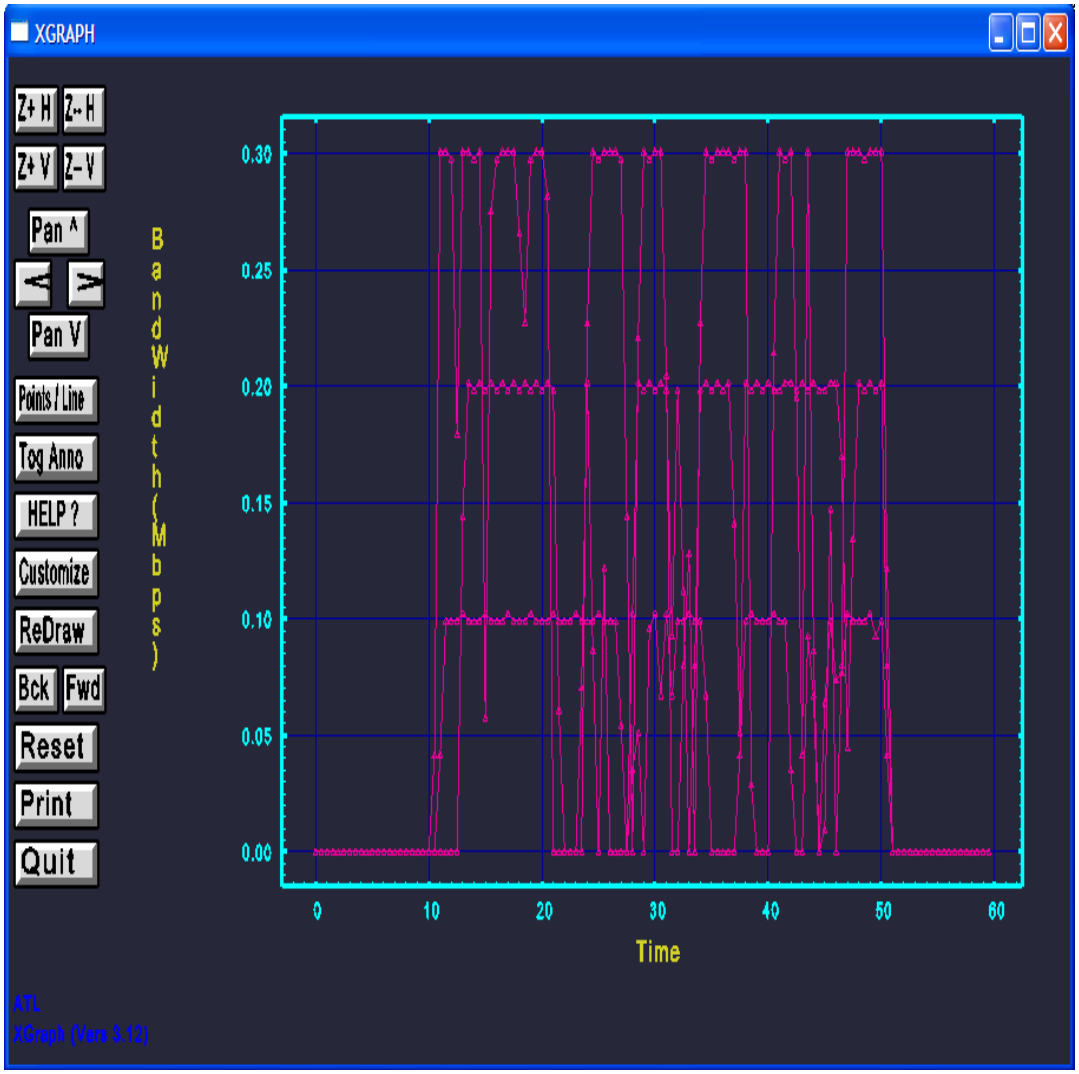

Figure 5.12 Bandwidth vs. time graph

In the bandwidth time graph we are plotting depicts the bandwidth usage of network in our 3 cases when we are using not any detection model and when we are using proposed detection model in our network. As we shown in the graph in our model the bandwidth which is using by attacker on the initial phase of is approximately 2.5 times less than that of not using any kind of detection model in IPv6.

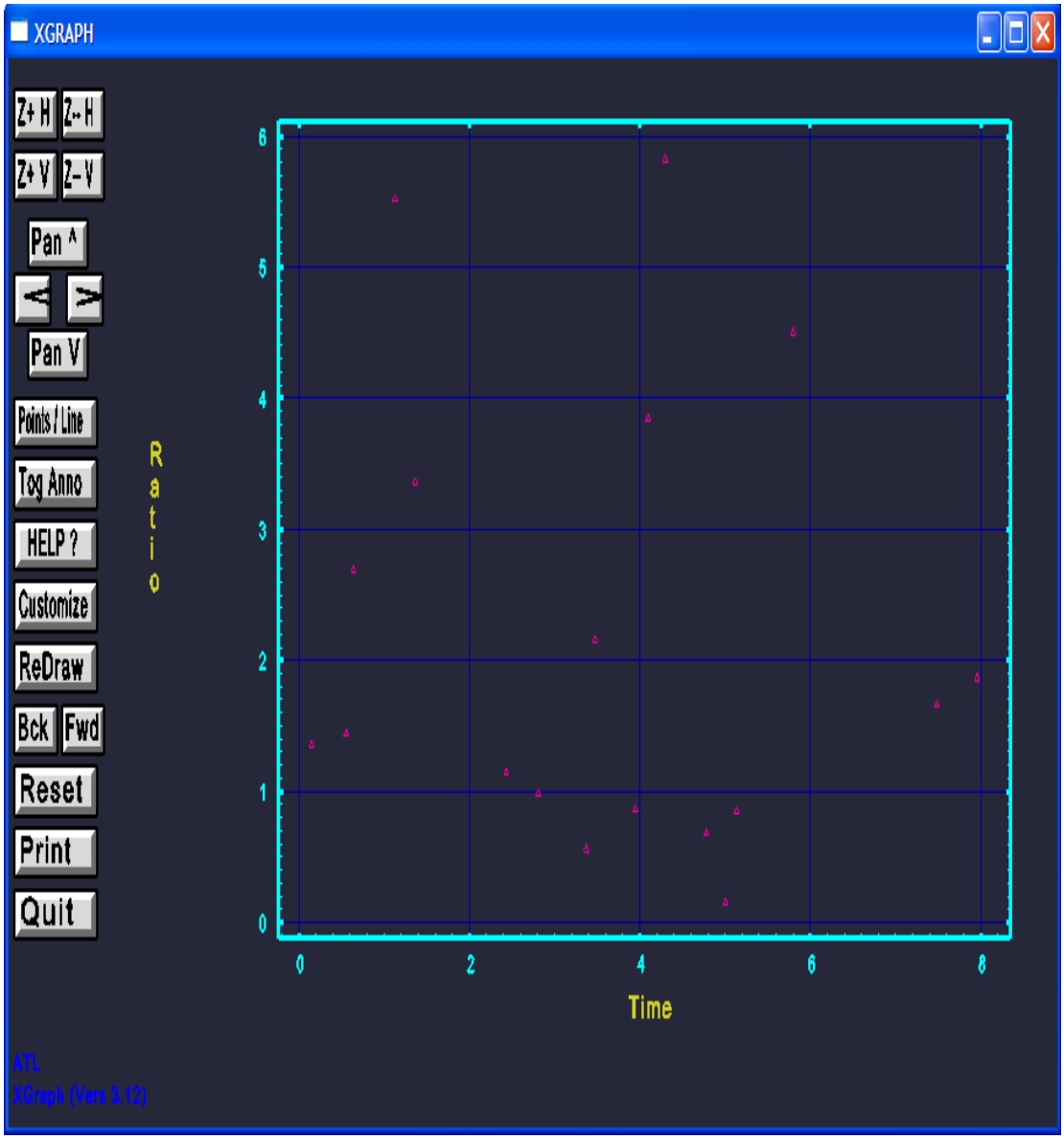

Figure 5.13 Ratio v/s time

In the ratio vs time graph we are depicting the ratio of experimental value over the expected value. In this graph to check out the results we are using chi square technique to extract the results. We are not getting many variations in our results of expected value and experimental value. So our model is validating here.

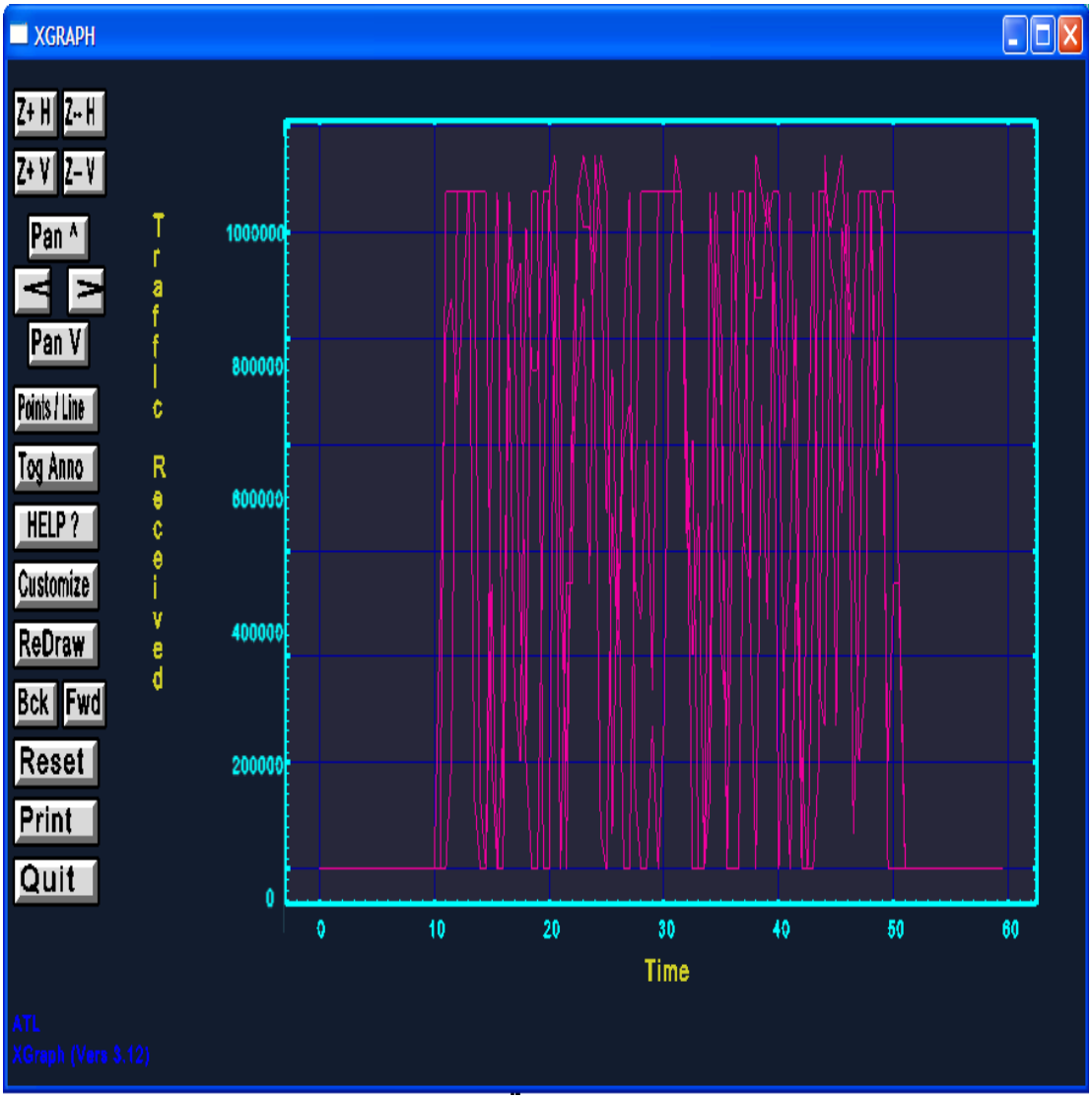

Figure 5.14 Traffic received v/s. time

In the Figure 5.14, we are presenting the traffic vs time graph which depicts the amount of traffic send in the network vs time of simulation.

This approach of detect the source address for tracing the attacker, reduces time and also memory of our network. If we talk in terms of time, then the time taken to calculate or detect both the attacks is less than that of the previous approaches because we can detect both the attacks to high extent by using our technique to mitigate attack

This technique illustrates the feasibility of tracing individual packets with packet logging. However, the storage overhead and access time requirement for recording packet digests are fairly high at high-speed routers.

Chapter 5
Conclusion & Future Scope

An efficient trace-back scheme is necessary to identify the sources of DoS attacks which impose an imminent threat to the availability of Internet services. The work presented in this thesis adopted a hybrid trace-back approach in which packet marking and packet logging are integrated to achieve the best of both worlds. The main characteristic of DDoS is to use multiple attacking sources to attack a single victim (the aggregation characteristic). Therefore, at any point in the network, if there is a sudden surge in the number of packets with the same destination address and with the same group of digest marks, it can be a sign of a DDoS attack.

By using this approach to detect the source address for tracing the attacker reduce time and also memory of our network in IPv6. Memory management is done by generating a bit of RED which is inside the packet to tell that if packet is sent by attacker or the actual node. We shall generate a bit in RED if attacker is sending packets otherwise bit is 0. If we talk in terms of time than the time taken to calculate or detect both the attacks is less than that of the previous approaches because we can detect both the attacks to high extent by using our technique to mitigate attack. Now tracing a single IP packet back to its origin is the ultimate goal of IP trace-back in IPv6. Our technique illustrates the feasibility of tracing individual packets with packet logging. However, the storage overhead and access time requirement for recording packet digests are fairly high at high-speed routers.

References

[1] Chao gong, Kamil sarac, "A more practical approach for single-packet IP trace-back using packet logging and marking" (2006)

[2] R. sravani, J. swami naik, "A study on flexible deterministic packet marking: an ip trace-back system" *International journal of advanced engineering sciences and technologies* vol no. 9, issue no. 1 ,(2011)

[3] Vahid Aghaei-Foroushani, A. nur zincir-heywood, "On evaluating IP trace-back schemes: a practical perspective" *IEEE security and privacy workshops*, (2013)

[4] Dong yan, Yulong wang, Sen su and Fangchun yang ," A precise and practical IP trace-back technique based on packet marking and logging" *Journal of information science and engineering* 28, (2012)

[5] Minho sung, Jason chiang, and Jun (jim) xu, "Scalable hash-based IP trace-back using rate-limited probabilistic packet marking" *Technical report, college of computing, georgia institute of technology*, (2006)

[6] A.parvathi and G.l.n.jayapradha," An IP trace back system to find the real source of attacks" I- volume 2 issue 1- (2011).

[7] R. sravani, J. swami naik, "A study on flexible deterministic packet marking: an IP trace-back system" *International journal of advanced engineering sciences and technologies* vol no. 9, issue no. 1.

[8] Basheer al-Duwairi, and G. manimaran,"Novel hybrid schemes employing packet marking and logging for IP trace-back" (2005).

[9] Andrey belenky and Nirwan ansari, "Tracing multiple attackers with deterministic packet marking (DPM)" (2003).

[10] Amey shevtekar, Nirwan ansari, "A router-based technique to mitigate reduction of quality (roq) attacks" received 21 february 2007, received in revised form 3 november 2007; accepted 22 november 2007 available online 4 december (2007).

[11] Mina guirguis,Oshua, Tharp azer bestavros, Ibrahim matta, "Assessment of vulnerability of content adaptation mechanisms to roq attacks" (2009).

[12] Jatinder singh, "A mac layer based defense architecture for reduction-of-quality (roq) attacks in wireless lan" (2010).

[13] Mina guirguis, Azer bestavros, Ibrahim matta, "Exploiting the transients of adaptation for roq attacks on internet resources" (2004).

[14] Yang xian, Ke li and Wanlei zhou, senior, "low-rate ddos attacks detection and trace-back by using new information metrics" *IEEE transactions on information forensics and security*, vol. 6, no. 2, june (2011).

[15] Yu chen and Kai hwang, " Spectral analysis of tcp flows for defense against reduction-of-quality attacks" (2007).

[16] Wei ren, Dit-yan, Yeung, Hai jin, and Mei yang, "Pulsing roq ddos attack and defense scheme in mobile ad hoc networks" (2007).

[17] Mina guirguis, Azer bestavros, Ibrahim matta, "Bandwidth stealing via link-targeted roq attacks" *International conference on communication and computer networks* (ccn'04).

[18] Andrey belenky and Nirwan ansari, " Tracing multiple attackers with deterministic packet marking (DPM)" advanced networking laboratory, ECE department, njit, newark, nj 07102, usa

[19] Minho sung, Jason chiang, and jun (jim) xu, "scalable hash-based ip trace-back using rate-limited probabilistic packet marking" *Technical report, college of computing, georgia institute of technology.*

[20] Sager, "security fun with ocxmon and cflowd," in internet 2 working group meeting, november (1998).

[21] U. tupakula and V. varadharajan, "A practical method to counteract denial of service attacks," *in proc. of the 26th australasian computer science conference*, february (2003).

[22] S.prathyusha,M.v.sruthi, S.anjani prasad, "A novel attack path reconstruction based on packet logging & marking scheme" *International journal of advanced research in electrical, electronics and instrumentation engineering* vol. 2, issue 2, February(2013).

[23] S.mallinga, A. tamilarasi, "A hybrid scheme using packet marking and logging for Ip traceback" *International journal of internet protocol technology* volume 5 issue 1/2, april (2010).

[24] Jun xu, Xuehai zhou, Feng yang, "Traceback in wireless sensor networks with packet marking and logging" frontiers of computer science in china september 2011, volume 5, issue 3

[25] Chaitanya kumar singh, Srinivas koppu, , V madhu viswanatham, "E-RIHT: enhanced hybrid ip traceback scheme with 16-bit marking field", *International journal of engineering and technology (ijet)* vol 5 no 3 jun-jul 2013

[26] A.parvathi and G l.n.jayapradha, "An ip trace back system to find the real source of attacks" *International journal of computer trends and technology*- volume 2 issue 1- 2011

[27] S.Karthik, Dr. V.P. Arunachalam, Dr.T.Ravichandran, "An Investigation about Simulation of IP Trace-back and Various IP Trace-back Strategies, IJCSNS *International Journal of Computer Science and Network Security*, VOL.8 No.12, December 2008

List of Publications

[1] "IP traceback technique to uncover intruders" *National Conference on Security Issues in Network Technologies"* (NCSI – 2013) srcem/ncsi-2013/152 [communicated].