Hybrid Packet Marking IP Traceback Technique over IPv4, IPv6 and Mobile IPv6

Sukhwinder Singh

School of Engineering & Technology, Centre for Computer Science & Technology,

Central University of Punjab, Bathinda 151001, India

Abstract--*Cyber-attacks are increasing day by day. Each time attackers or malicious users come up with new techniques or methods in order to harm the network system of particular organization. While attacking on any organization, the main focus of the attacker is to successfully launch attack against organization's network system by hiding its own identity under the identity of other legitimate user in order to not to get traceback. This technique is called IP spoofing. This technique is mostly used by the attackers while performing Denial of service (DoS) or Distributed Denial of service (DDoS) attacks. The need of IP traceback technique arises to trace the originator of the DoS and DDoS attacks. There are different kinds of IP traceback technique that are used to successfully traceback origin of the attack. In this research work, the Hybrid packet marking TTL and Hop Limit based identification technique is applied on IPv4 and IPv6 network respectively. In this technique, only the first router in the path marks its identity into the packet. In the IPv4 network, the first router in the path is identified using the TTL value of IPv4 packet header and in IPv6, the hop limit value is used to for the same. In the case of Mobile IP, where the attacking node is movable between the different networks, TTL based identification mechanism and Hop limit based hybrid traceback technique can be used for Mobile IPv4 and Mobile IPv6 respectively. In the mobile IP network, the address of home agent will be marked into the packet both for MIPv4 and MIPv6. In this research work, both the techniques i.e. hybrid TTL based identification and hybrid Hop limit based packet marking technique are simulated for wired and wireless IPv4 and IPv6 networks. The result shows the successful traceback of the nodes through the marking information in IPv4, IPv6 and Mobile IP networks.*

Keywords*--IP, TCP/IP, DoS, DDoS, IP Traceback, PPM, DPM.*

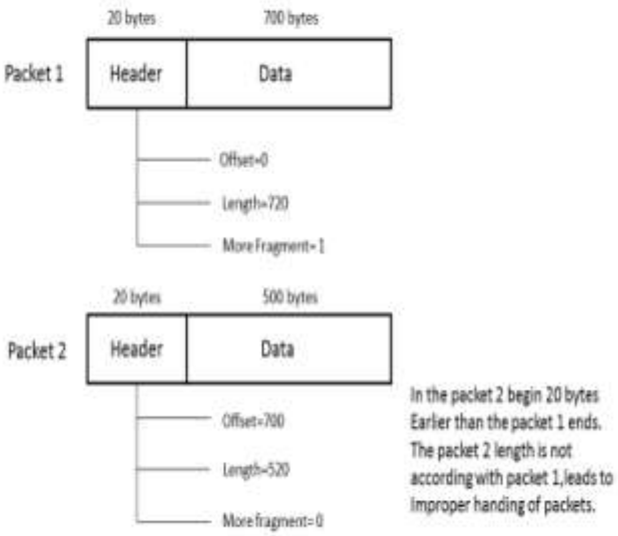
I. INTRODUCTION

With the ease of use and high speed information transfer, the Internet has brought an uprising in today's life. The internet is increasingly becoming the most efficient way of communication nowadays. Anyone can use the services like email, sharing files, browsing information, downloading contents, performing business activities and many more by using the Internet. The various activities like searching information using search engine, online sale and purchase, online education, e-banking etc.are possible through the internet. Besides the various merits of the internet, there are some demerits also. The Internet is vulnerable to various threats like passive attack and active attack. These attacks are performed by exploiting various security vulnerabilities in the target's system. In the **Passive attacks**, attacker or malicious user indulges in eavesdropping or monitoring data during the transmission. In the passive attack, the attacker's primary objective is only to gain information that is in transit. The word passive describes that the malicious user or attacker does not perform any modification to the data. Traffic analysis and release of content are the examples of passive attacks in which malicious user only capture the data and release it publically on web [1]. On the other hand, the **Active Attacks** are based on modification of the content in the original message or creating a false message. Interruption, masquerade, modifications, replay attack, alteration and Denial of Service attack are examples of active attack. These active attacks cannot be prevented easily [1]. Among various passive and active attacks, Denial of Service (DoS) attack is a major attack due to its disruptive nature. The Denial of service (DoS) attack is a malicious attempt by the attacker to make a target system or a network resource unavailable to legitimate users, usually by temporarily interrupting or suspending the services of target system. In DoS attack, a large amount of packets is generated and directed towards the target. The purpose of this attack is to disrupt the normal communication by causing congestion at the target system. DoS attack is hard to detect because attacker may use spoofed address by exploiting the source address spoofing vulnerability in IP header. There are two types of addressing scheme that are used for addressing in Internet Protocol (IP) i.e. IPv4 and IPv6, duringtransmission of the data packet from source to destination. Attacker falsifies the source address in IP packet in order to hide its identity and this makes it difficult to trace out the original source of attack [2].

A. DoS & DDoS Attack

IP spoofing is the primary mechanism that the attacker uses to hide its identity while launching a Denial of service (DoS) attack. IP spoofing means sending packets with a fake source IP address. The main aim of Denial of service (DoS) attacks is to prevent the user's access to a particular web service on a server. DoS can be classified as either flooding attacks or logic attacks. In the flooding attack, a large number of requestsare sent to a victim. As a result, whole network bandwidth gets consumed, and the processing power of victim server is spent on to process unnecessary request [3].

In case of logic attack, the attacker crafts some specific packets that cause the target system crashed, like Teardrop Attack.



In the packet 2 begin 20 bytes Earlier than the packet 1 ends. The packet 2 length is not according with packet 1,leads to Improper handing of packets.

Fig. 1: Teardrop attack [4]

The teardrop attack is denial of service attack, which exploits the vulnerability in TCP/IP fragmentation reassembly. In this attack, the attacker sends the fragmented packets to the target systemas shown in Fig. 1 and the machine receiving these packets cannot reassemble these packets, thus crashing the target machine.

Denial of service attack can also be carried out (without IP address spoofing) by compromising multiple hosts. The compromised hosts are then used to perform the denial of service attack on network or system called Distributed Denial of service attack (DDoS). The compromised hosts are also known as zombies [5].

B. IP Traceback

The IP Traceback is the technique that is used to find the origin of the packet on the network. It is easy to determining the originating host of a packet, when source IP address is not forged. But in the case of IP Spoofing, it becomes difficult to find originating host. To tackle with this kind of problem, some techniques are needed to trace back the source of the packets.

C. Related Work

Hassan, 2003classified Link Testing IP traceback technique. This technique was devloped to traceback the attacker by testing the uplink stream through two sub types input debugging and controlled flooding. In the input debugging method, the victim communicate attack traffic signature to the internet service provider,and the internet service provider apply filter on the victim's upstream link. Same task is repeated on the upper router nodes until the origin located. In the case of controlled flooding, the upstream links of victim's network are flooded. This will change the flow of incoming packets to victims network. The victim can analyze from which upstream link the attack traffic is coming from chnage the rate of incoming attack traffic. The same proccess is repeated on upper router nodes. The main drawback of these technique is there are lot of network overheads occur. Like there is need to contact the network operator or internet service provider in order to install signature at router incase of input debugging. It becomes difficult to trace when new network boundaries start [6].Savage *et al.*, 2000developed a probabilistic packet marking traceback technique. The previous link testing IP traceback method cannot be used for post-mortum of attack. It can only traceback the on going attack. But in the probablistic packet marking technqiue, the origin of the packets can be located by using the marking information in the packets. It works in two parts makring the packet and traceback algorithm. In this the packets are marked at the router with a constant probablity. Marking information in the packet is either identity of the router or edge from source to next node. During and after the attack traceback method collect the marking information from the packet, which helps to locate the origin of the packet. the main drawback of this technique is that the traceback algorithm requires the large number of the packets to reconstruct the entire path travel by the packets [7]. Snoeren *et al.*, 2001developed Hash based IP-traceback technique. In the previous disscussed probablistic packet marking technique, each nodes mark its identity with some probability into the packet that some times creates the false positives when marking information gets overwritten. To further improve the traceback results author developed hash base ip traceback technique. In this first packet digest is created using the invariant fields of the packet through Source Path Isolation Engine (SPIE) digesting algorithm. After creating the digest, it is stored at the router using a space efficent data structure known as bloom filters. This data structure takes less space to store the 32 bit digest of packet rather than storing the packet as whole. Although it store packet digest in space efficent manner, but still it increases the overhead at router [8].Ansari *et al.*, 2003introduced a new IP traceback technique called Deterministic Packet Marking. The previous disscussed technique, the probablistic packet marking (PPM) has a main drwaback that requires full path traceback to locate the originating host or network. So it becomes difficult to trace when traceback requires to contact from out of boundary of one internet service provider (ISP) to the another. Not all internet service provider will corporate to traceback, because no-one wants to disclose its network topologies to others. In the determinstic packet marking technique, it does not treat router as atomic unit for traceback as in PPM. In this technique, the ingress router will mark the packet with IP address of that interface through which it passes. The IP address is divided into two 16 bits parts. First half is written into the packet and the reserved flag is set to the value' 0'. Second part is written to the another packet by setting the reserved flag bit 1. So address is written into two packet and it requires atleast two packet at receiver side to generate complete address [9]. Aijaz & Mohsin, 2007 proposed a hybrid IP traceback technique based upon time to live (TTL) identification. This technique is also extention to deterministic packet marking (DPM) technique. In the DPM address is divided into two 16 bit parts and is written into two different packets alternativly. But in this hybrid traceback technique, packet is marked with whole 32 bit IP address in the route record optional field of packet header. Only the first router in the path will perform marking. The first router in the path will be located through TTL value of the packet. The TTL value of the packet decrement by one, when the packet traverse the router node. Therefore packet reach to the first router node when ttl value decrement by one from its initial gereated TTL value by operating system. This technique solve the problem of dividing the IP address into two parts and then randomly written into the packets. This technique is called hybrid because ingress filtering technique is applied with the marking technique. In the ingress filtering, the router will first compute and match the net id of packet. If matched, will accept the packet for marking otherwise discard the packet [10].Sun *et al.*, 2011 proposed a modified deterministic packet marking traceback technique for DDoS attack in the IPv6 network. In this method, the marking is performed by ingress edge router based upon the current traffic load upon it. There are two values defined for the traffic load i.e. L_Min and L_Max. If the load on the router is less than L_Min it will not mark the packet. The packet will be marked if load is in between L_Min and L_Max. To mark the IP address of router in the IPv6 packet, the destination option extension header is used. At the receiver side, it checks if there is destination option field in the packet, then information stored it this field is fetched otherwise simply accept packet [11].Parashar & Radhakrishnan, 2014proposed Improved Deterministic Packet marking IP traceback technique for IPv6. This technique is an improved version of deterministic marking, in which hop by hop option field in IPv6 packet header is used to mark the identification of the packet. The marking technique creates a digest of IP address of ingress router and stores it into the hop by hop option field of packet. The intermediate router will process the hop by hop option field, recalculate the digest and compared it with IP digest stored in the packet. If not matched, the packet will be considered spoofed and the intermediate router will discard the packet. But this technique does not specify which intermediate node will recalculate the digest [12]. Paruchuri *et al.*, 2008proposed a TTL based probabilistic packet marking IP traceback technique. This technique is an improved version of probabilistic packet marking technique. In the normal PPM mechanism, the packets are marked with constant probability and the attackers take the advantage of this to create a spoof mark into the packet. So in the improved PPM technique, the routers mark the packets with different probability depend upon the distance travel by a packet. The router computes the marking probability for a packet from time to live value 't' of the packet, where t_p is maximum path length. Therefore router computes probability by 1/h where 'h' is remaining distance calculated as $h \leftarrow t_p\text{-}t$ [13]. Feng & Yusheng, 2014proposed improved probabilistic packet marking (IPPM-v6) IP traceback scheme based on advanced probabilistic packet marking scheme for IPv6 (APPM-v6). In the APPM-v6 scheme, flow label (20 bits) and traffic class (8 bits) field in the basic header is used to store the marking information. In this scheme, 128 bits IPv6 and 32 bits hash value, total 160 bits marking information is divided into 8 blocks of 20 bits each to store into basic IPv6 header. In the improved packet marking scheme (IPPM-v6), the marking space is improved by using the routing extension headers to store the IPv6 address of routers in the path and one bit of hop limit field is used as flag bit. The marking probability 'r' is predetermined. Initially the packet is unmarked and flag bit is 0. If flag bit 0, the router will mark it address with probability 'r' into the routing extension header and change flag bit to 1. If flag bit is 1 in the packet, it means the packet is already marked and the router will add or mark the packet with its IPv6 address without using any probability and forward the packet. At the victim side, one can reconstruct the path back to origin using the marking information [14].

II. HYBRID PACKET MARKING IP TRACEBACK TECHNIQUE OVER IPv4, IPv6 and MOBILE IP

A. IP Traceback in IPv6

IPv6 was developed to overcome the problems in the IPv4 like address depletion, lack of security etc. Aijaz et al., 2007 [10]proposed hybrid technique for IPv4 [15]and is compatible with IPv6 also. This technique is not simulated for IPv6 and Mobile IPv6. In the IPv6 the IP address is 128 bit long as compared to the 32 bits address of IPv4. The hop limit field in the IPv6 [16] base header is used for the same purpose as time to live field in IPv4.

Table 1: Initial Hop Limit/TTL values of Different operating systems

Operating System	Version	Platform	Default TTL/Hop Limit Values
Windows	7	Intel	128
Digital Unix	4.0	Alpha	60
Linux	2.2x	Intel	64
Z/OS	2.1.0	IBM	255
PC-BSD	10	X86-64	64
Cisco	5.0x	7000	64

Therefore the similar technique as used for the IPv4 can be simulated for IPv6 by using the hop limit field, serving the same purpose as TTL field in IPv4. The table 1 shows the default hop limit values of different operating system. The hop limit field can be used to find the first router in the path as the time to live field does as discussed above. The route record field is not implemented in the IPv6 packet header. So Aijaz et al., 2007 [10] suggest the destination option extension field to store the marking information about the router. The value 60 in the next header field of IPv6 base header shows that it is using destination option [16] extension header. The destination option field contains the address of next hop when source routing is used. It means that intermediate router can access this field. To make use of this field in marking technique the destination option field is placed after the routing header.

Step 1: In the Fig. 3, the host 4 at router 1 sends packet to host H3 at router 3.

Step 2: As the packet arrives at router 1, it will match TTL/Hop limit value of the packet to the stored value. If match found, it will mark its identity R1 into the router.

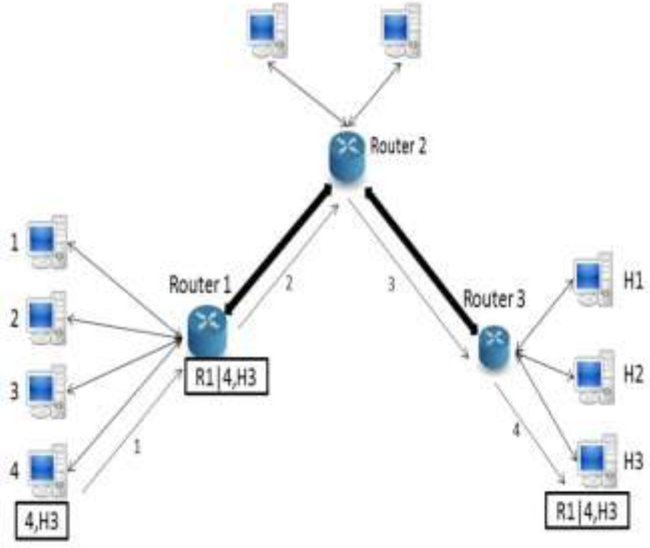


Fig. 2: Packet marking in the wired network

Step 3: The router will not mark the packet as packet is already marked and forwards to next node.

Step 4: The packet will be reached at the destination with the marking information of router node 1.

B. IP Traceback in Mobile IPv6

In the case of mobile network [17], the device connected to the network is movable, means device can move from one point of attachment to another.When the mobile node is connected to home agent in its home network, the technique is implemented same as does in wired IPv4 and IPv6 on the router. When the packet received at the router it match the TTL/Hop limit value in the packet with stored table value. If matched then it marks address of home agent will be marked into the packet.

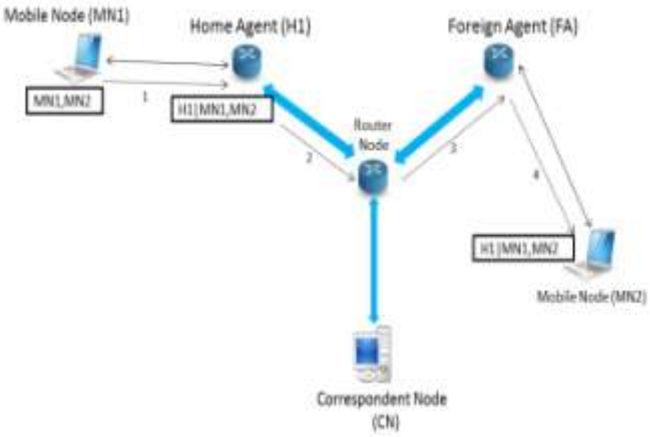


Fig. 3: IP traceback in Mobile IP

Step 1: In the Fig. 3, the mobile node MN1 wants to send data to another mobile node MN2 on another network (FA). The mobile node forwards the packet to home agent

Step 2: The home agent mark its identity H1 in the packet header and forward to the next router node.

Step 3: The packet is forwarded to the FA. No node in the path will mark the packet again.

Step 4: The destination mobile node MN2 receive the packet with marked information about the home agent of the source mobile node in the packet header.

III. SIMULATION AND ANALYSIS OF RESULTS

The hybrid IP traceback technique for IPv4,IPv6 and Mobile IPv6 has been simulated as shown in figure 4. The results are discussed as following. The network simulator (NS2) tool is used for the simulation.

A. *Simulation for wired network scenario*

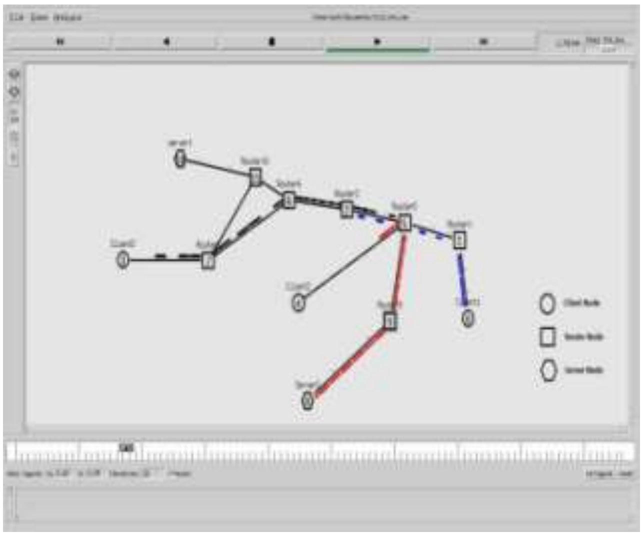


Fig. 4: wired network scenario for IPv4 and IPv6

- In this wired simulation scenario, the client nodes as source and server nodes as destination are defined.
- All the source and destination nodes are connected through multiple intermediate router nodes
- TCP connections are made from client to server nodes to send FTP type application traffic on it.
- On run the simulation, when the packets will arrive at router node 1, 5 and 7 from the respective clients as shown in figure 4.1, all the three router nodes will mark the packets with their own identity and forward the packet to next node.

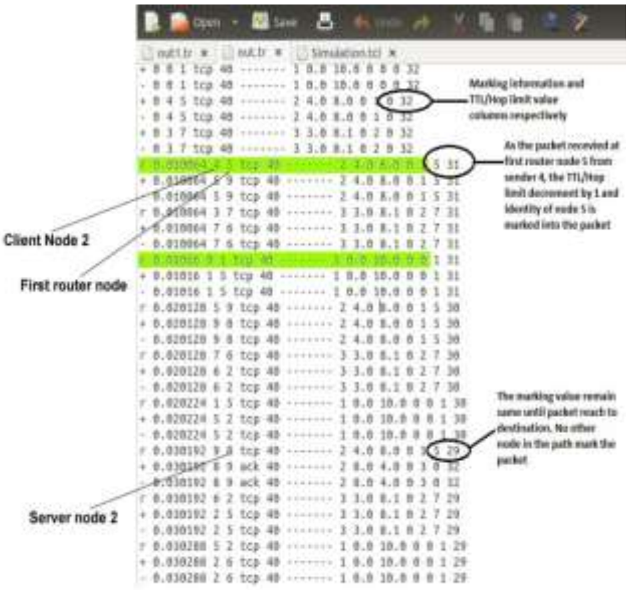
The table 2 shows three type of TTL/Hop limit values of the packets from clients to server nodes captured in the trace file generated after running the wired network simulation shown in figure 4.

Table 2: TTL/Hop limit values in the packet from client to server

Source Node	Default TTL/Hop limit value	TTL/Hop limit value when packet is marked $(\text{TTL/Hop limit})_M$	TTL/Hop limit value when packet received $(\text{TTL/Hop limit})_R$	Destination Node
Client 1	32	31	26	Server 1
Client 2	32	31	29	Server 2
Client 3	32	31	26	Server 2

From the TTL/Hop limit values shown in the table one can calculate that number nodes need to traverse back to trace the origin of the packets. Like for the traceback from client 1 to server 1, the $(\text{TTL/Hop limit})_M$when packet is marked 31 and $(\text{TTL/Hop limit})_R$ when the packet received is 26. From $(\text{TTL/Hop limit})_M$ - $(\text{TTL/Hop limit})_R$ gives the value 5 i.e. number nodes need to traverse back. After traversed back, the marking information in the packet reveal the identity of the first router node.

1) Analysis of trace file:The Fig. 5 shows the trace file generated after the running the simulation. The trace file shows the marking information of first node. In the normal trace file format, the last two columns are not present. So the trace file format has been modified to get the mark information about the router node.



```
+ 0 0 1 tcp 40 ------- 1 0.0 10.0 0 0 0 32
- 0 0 1 tcp 40 ------- 1 0.0 10.0 0 0 0 32
+ 0 4 5 tcp 40 ------- 2 4.0 8.0 0 1 0 32
- 0 4 5 tcp 40 ------- 2 4.0 8.0 0 1 0 32
+ 0 3 7 tcp 40 ------- 3 3.0 8.1 0 2 0 32
- 0 3 7 tcp 40 ------- 3 3.0 8.1 0 2 0 32
r 0.010064 4 5 tcp 40 ------- 2 4.0 8.0 0 1 5 31
+ 0.010064 5 9 tcp 40 ------- 2 4.0 8.0 0 1 5 31
- 0.010064 5 9 tcp 40 ------- 2 4.0 8.0 0 1 5 31
r 0.010064 3 7 tcp 40 ------- 3 3.0 8.1 0 2 7 31
+ 0.010064 7 6 tcp 40 ------- 3 3.0 8.1 0 2 7 31
- 0.010064 7 6 tcp 40 ------- 3 3.0 8.1 0 2 7 31
r 0.01016 0 1 tcp 40 ------- 1 0.0 10.0 0 0 1 31
+ 0.01016 1 5 tcp 40 ------- 1 0.0 10.0 0 0 1 31
- 0.01016 1 5 tcp 40 ------- 1 0.0 10.0 0 0 1 31
r 0.020128 5 9 tcp 40 ------- 2 4.0 8.0 0 1 5 30
+ 0.020128 9 8 tcp 40 ------- 2 4.0 8.0 0 1 5 30
- 0.020128 9 8 tcp 40 ------- 2 4.0 8.0 0 1 5 30
r 0.020128 7 6 tcp 40 ------- 3 3.0 8.1 0 2 7 30
+ 0.020128 6 2 tcp 40 ------- 3 3.0 8.1 0 2 7 30
- 0.020128 6 2 tcp 40 ------- 3 3.0 8.1 0 2 7 30
r 0.020224 1 5 tcp 40 ------- 1 0.0 10.0 0 0 1 30
+ 0.020224 5 2 tcp 40 ------- 1 0.0 10.0 0 0 1 30
- 0.020224 5 2 tcp 40 ------- 1 0.0 10.0 0 0 1 30
r 0.030192 9 8 tcp 40 ------- 2 4.0 8.0 0 1 5 29
+ 0.030192 8 9 ack 40 ------- 2 8.0 4.0 0 3 0 32
- 0.030192 8 9 ack 40 ------- 2 8.0 4.0 0 3 0 32
r 0.030192 6 2 tcp 40 ------- 3 3.0 8.1 0 2 7 29
+ 0.030192 2 5 tcp 40 ------- 3 3.0 8.1 0 2 7 29
- 0.030192 2 5 tcp 40 ------- 3 3.0 8.1 0 2 7 29
r 0.030288 5 2 tcp 40 ------- 1 0.0 10.0 0 0 1 29
+ 0.030288 2 6 tcp 40 ------- 1 0.0 10.0 0 0 1 29
- 0.030288 2 6 tcp 40 ------- 1 0.0 10.0 0 0 1 29
```

Marking information and TTL/Hop limit value columns respectively

As the packet received at first router node 5 from sender 4, the TTL/Hop limit decrement by 1 and identity of node 5 is marked into the packet

Client Node 2

First router node

The marking value remain same until packet reach to destination. No other node in the path mark the packet

Server node 2

Fig. 5:Analysis of trace file of wired network simulation

- By analyzing the trace file in figure 5 one can see that in the last two, when the TTL/Hop limit value is 32 there is no value in the marking column.

- The first highlighted line in the trace file in figure 5 shows that the TCP type packet destined from node 4 and port number 0 to node 8 and port 0 has been successfully received at first router node 5. On receiving packet at node 5, the identification of node 5 has been written into the packet and TTL/Hop limit value decrements by 1.
- The TTL/Hop limit value in packet is 29, when the packet is received at node8. So one can see that, marking value in the packet remains same up to the destination node and no other intermediate router performs the marking.
- On receiver side this marking information will help to trace back to the source of traffic generated.

B. Simulation for wireless network scenario

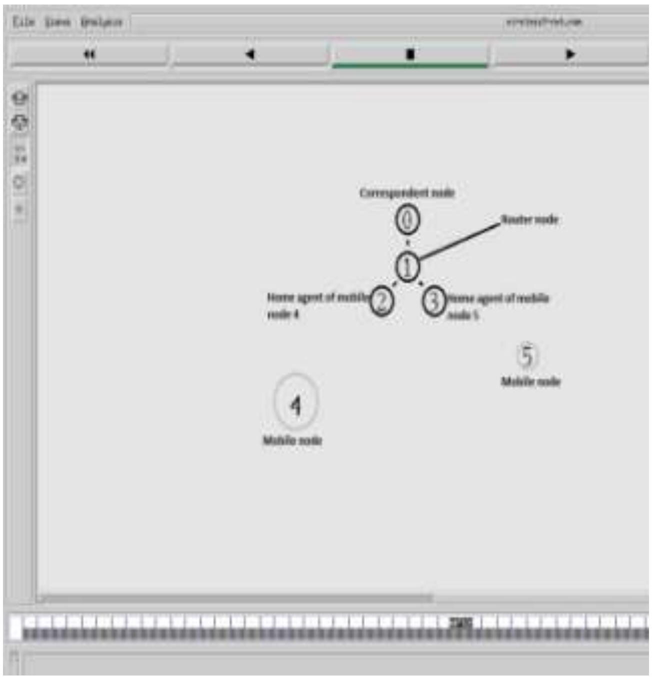


Fig. 6: wireless network simulation scenario

- In the wireless scenario, the source and destination node are the mobile nodes connected to their respective home agents.
- Node 2 and node 3 are two home agents, configured with hierarchical address format.
- The correspondent node shown in the Fig. 6 is connected to the wireless nodes through intermediate router node.
- A TCP connection is setup between the mobile node 4 and node 5 to send FTP type traffic on it.
- When the node 4 will send the data packet, it will first go to its home agent and from there the data packet will direct to the home agent of node 5 through intermediate router node. The home agent of node 5 will forward the packet to it.

The table 3 shows three types of TTL/Hop limit values of the packets from source mobile node to destination mobile node captured in the trace file generated after running the wireless network simulation shown in Fig. 6.

Table 3: TTL/Hop limit values in the packet for the mobile nodes

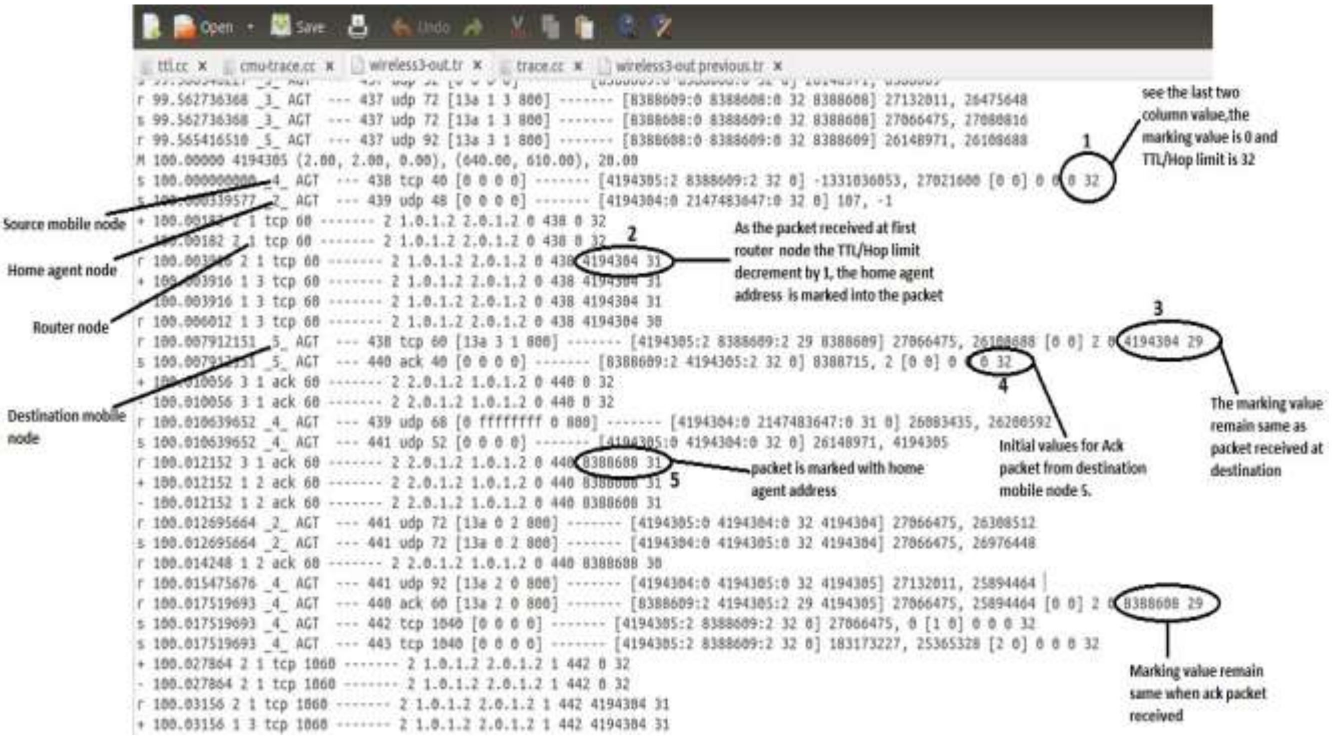
Source Node	Default TTL/Hop limit value	TTL/Hop limit value when packet is marked (TTL/Hop limit)$_M$	TTL/Hop limit value when packet received (TTL/Hop limit)$_R$	Destination Node
Mobile node 4 (TCP packet)	32	31	29	Mobile Node 5
Mobile node 5 (Ack packet)	32	31	29	Mobile Node 4

In the table 3 (TTL/Hop limit)$_M$ value in a packet when it is marked with the identification of home agent is 31. The (TTL/Hop limit)$_R$ value is 29 when packet received at the receiver. Now one can calculate the value of no. nodes need to traceback from (TTL/Hop limit)$_M$-(TTL/Hop limit)$_{R.}$ In this case 31-29= 2, only two nodes need to traverse back (excluding itself) and the marking information in packet 2 nodes back reveals the identity of first router node in the path.

1) Analysis of trace file:The Fig. 7 shows the trace file generated after running the wireless simulation. The highlighted area labeled as 1 show the marking value field and initial TTL/Hop limit value of a packet. In the normal trace file format these fields are not shown. The trace file format is modified to print the new fields of packet header. One need to examine the packet header to get information stored into the packet.

- Initially, the TTL/Hop limit value is 32 there is no value in the marking column.
- As TTL/Hop limit value decrement by one, it means that the packet arrive at first router (see the area labeled as 2). The router will mark the home agent identification (as in this simulation MAC id is taken as identification) in the packet.
- No other router node will mark the packet in path. The marking information will remain same until reach to the destination mobile 5 as highlighted in the label 3.
- On receiver side this marking information will help to trace back to the source of traffic generated.

- In the label 4 the mobile 5 reply back with Ack packets to the mobile node 4.


Open
Save
Undo
ttl.cc
cmu-trace.cc
wireless3-out.tr
trace.cc
wireless3-out previous.tr
Source mobile node
Home agent node
Router node
Destination mobile node
1
see the last two column value,the marking value is 0 and TTL/Hop limit is 32
2
As the packet received at first router node the TTL/Hop limit decrement by 1, the home agent address is marked into the packet
3
The marking value remain same as packet received at destination
4
Initial values for Ack packet from destination mobile node 5.
5
packet is marked with home agent address
Marking value remain same when ack packet received

```
r 99.562736368 _3_ AGT  --- 437 udp 72 [13a 1 3 800] ------- [8388609:0 8388608:0 32 8388608] 27132011, 26475648
s 99.562736368 _3_ AGT  --- 437 udp 72 [13a 1 3 800] ------- [8388608:0 8388609:0 32 8388608] 27066475, 27080816
r 99.565416510 _5_ AGT  --- 437 udp 92 [13a 3 1 800] ------- [8388608:0 8388609:0 32 8388609] 26148971, 26108688
M 100.00000 4194305 (2.00, 2.00, 0.00), (640.00, 610.00), 20.00
s 100.000000000 _4_ AGT  --- 438 tcp 40 [0 0 0 0] ------- [4194305:2 8388609:2 32 0] -1331036053, 27021600 [0 0] 0 0 0 32
s 100.000339577 _2_ AGT  --- 439 udp 48 [0 0 0 0] ------- [4194304:0 2147483647:0 32 0] 107, -1
+ 100.00182 2 1 tcp 60 ------- 2 1.0.1.2 2.0.1.2 0 438 0 32
- 100.00182 2 1 tcp 60 ------- 2 1.0.1.2 2.0.1.2 0 438 0 32
r 100.003916 2 1 tcp 60 ------- 2 1.0.1.2 2.0.1.2 0 438 4194304 31
+ 100.003916 1 3 tcp 60 ------- 2 1.0.1.2 2.0.1.2 0 438 4194304 31
- 100.003916 1 3 tcp 60 ------- 2 1.0.1.2 2.0.1.2 0 438 4194304 31
r 100.006012 1 3 tcp 60 ------- 2 1.0.1.2 2.0.1.2 0 438 4194304 30
r 100.007912151 _5_ AGT  --- 438 tcp 60 [13a 3 1 800] ------- [4194305:2 8388609:2 29 8388609] 27066475, 26108688 [0 0] 2 0 4194304 29
s 100.007912151 _5_ AGT  --- 440 ack 40 [0 0 0 0] ------- [8388609:2 4194305:2 32 0] 8388715, 2 [0 0] 0 0 0 32
+ 100.010056 3 1 ack 60 ------- 2 2.0.1.2 1.0.1.2 0 440 0 32
- 100.010056 3 1 ack 60 ------- 2 2.0.1.2 1.0.1.2 0 440 0 32
r 100.010639652 _4_ AGT  --- 439 udp 60 [0 ffffffff 0 800] ------- [4194304:0 2147483647:0 31 0] 26083435, 26200592
s 100.010639652 _4_ AGT  --- 441 udp 52 [0 0 0 0] ------- [4194305:0 4194304:0 32 0] 26148971, 4194305
r 100.012152 3 1 ack 60 ------- 2 2.0.1.2 1.0.1.2 0 440 8388608 31
+ 100.012152 1 2 ack 60 ------- 2 2.0.1.2 1.0.1.2 0 440 8388608 31
- 100.012152 1 2 ack 60 ------- 2 2.0.1.2 1.0.1.2 0 440 8388608 31
r 100.012695664 _2_ AGT  --- 441 udp 72 [13a 0 2 800] ------- [4194305:0 4194304:0 32 4194304] 27066475, 26308512
s 100.012695664 _2_ AGT  --- 441 udp 72 [13a 0 2 800] ------- [4194304:0 4194305:0 32 4194304] 27066475, 26976448
r 100.014248 1 2 ack 60 ------- 2 2.0.1.2 1.0.1.2 0 440 8388608 30
r 100.015475676 _4_ AGT  --- 441 udp 92 [13a 2 0 800] ------- [4194304:0 4194305:0 32 4194305] 27132011, 25894464
r 100.017519693 _4_ AGT  --- 440 ack 60 [13a 2 0 800] ------- [8388609:2 4194305:2 29 4194305] 27066475, 25894464 [0 0] 2 0 8388608 29
s 100.017519693 _4_ AGT  --- 442 tcp 1040 [0 0 0 0] ------- [4194305:2 8388609:2 32 0] 27066475, 0 [1 0] 0 0 0 32
s 100.017519693 _4_ AGT  --- 443 tcp 1040 [0 0 0 0] ------- [4194305:2 8388609:2 32 0] 183173227, 25365328 [2 0] 0 0 0 32
+ 100.027864 2 1 tcp 1060 ------- 2 1.0.1.2 2.0.1.2 1 442 0 32
- 100.027864 2 1 tcp 1060 ------- 2 1.0.1.2 2.0.1.2 1 442 0 32
r 100.03156 2 1 tcp 1060 ------- 2 1.0.1.2 2.0.1.2 1 442 4194304 31
+ 100.03156 1 3 tcp 1060 ------- 2 1.0.1.2 2.0.1.2 1 442 4194304 31
```

Fig. 7: Analysis of trace file of wireless network simulation

- As the TTL/Hop Limit value decrements by 1, the address of home agent (node 3) of mobile node 5 is marked into the packet and forwarded.
- The Ack packet with the marking information about home agent of node 5 is received at the mobile node 4.
- Using the marking information one can trace mobile node through its home agent.

IV. CONCLUSION

The demand of internet is increasing day by day. Although it provides services to the user, but at the same time some malicious users take the advantage of the ease and high speed communication of the internet in order to perform the malicious activities. These malicious users are sometimes hard to detect as they hide their identity under the identity of other legitimate user (called IP spoofing). This is the main drawback in IP protocol that it does not provide any mechanism to authenticate the source address in IPv4 packet header. So the need of IP traceback technique arises to trace the malicious user in the network. There different type of IP traceback techniques developed and implemented to trace the attacker over IPv4 networks. The IP traceback technique is effective, if it is capable of traceback the attacking host with minimum overheads like processing at router nodes, easy reconstruction of the path etc. The IPv6 version of IP protocol was designed to cover the various security flaws in IPv4 version, but still attacks are possible on IPv6 networks also like Distributed denial of service attack. The IPv4 networks are getting replaced with IP version 6. The technique proposed and implemented in this research work is capable of traceback even a single packet for IPv4, IPv6 and Mobile IPv6 networks. The simulation and analysis of the results show that one can traceback the packet by using the marked information provided in the packet header. In the wired IPv4 and IPv6, the first router identity marked in the packet helps to trace the origin of the packets. In the case of mobile node, where the mobile node is moving, the home agent address marked in the packet is used to find out theorigin of the packets.

Future Work: In this research work the hybrid IP traceback techniques haven't used the path reconstruction algorithm to reconstruct the exact attack path. To get the more efficient traceback result, these techniques can be used with a path reconstruction algorithm like ant based traceback. It is an efficient algorithm for path reconstruction during the attack.

REFERENCES

[1] Atul Kahate, *Cryptography and Network security.*: Tata McGraw-Hill Education, 2013.

[2] Incapsula. (2010) www.incapsula.com. [Online]. https://www.incapsula.com/ddos/ddos-attacks/denial-of-

service.html

[3] B. Xiaoa, W. Chenb, and Y. Hec, "An autonomous defense against SYN flooding attacks: Detect and throttle," *Journal of parallel and distributing computing*, vol. 68, no. 4, pp. 456-470, July 2007.

[4] Jupiner. (2010) Understanding Teardrop attack. [Online]. https://www.juniper.net/techpubs/software/junos-es/junos-es92/junos-es-swconfig-security/understanding-teardrop-attacks.html

[5] Incapsula. (2010, May) www.incapsula.com. [Online]. https://www.incapsula.com/ddos/attack-glossary/ntp-amplification.html

[6] Aljifri Hassan, "IP traceback: a new denial-of-service deterrent," *IEEE Security & Privacy*, vol. 1, no. 3, pp. 24-31, June 2003.

[7] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical Network Support for IP Traceback," in *In Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*, vol. 30, New York, USA, August 2000, pp. 295-306.

[8] A. C. Snoeren, C. Partridge, L. A. Sanchez, and C. E. Jones, "Hash Based IP Traceback," in *Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications*, vol. 31, San Diego, August 2001, pp. 3-14.

[9] N. Ansari, A. Belenky, and Nirwan, "IP Traceback With Deterministic Packet Marking," *IEEE Communications Letters*, vol. 7, no. 4, pp. 162-164, April 2003.

[10] A. Aijaz and S. R., & Mofassir-Ul-Haque Mohsin, "IP trace back techniques to ferret out denial of service attack source," in *Proceedings of the 6th WSEAS international conference on Information security and privacy*, Wisconsin, USA, 2007, pp. 135-140.

[11] Y. Sun, C. Zhang, S. Meng, and K. Lu, "Modified deterministic packet marking for DDoS attack traceback in IPv6 network.," in *In IEEE 11th International Conference on Computer and Information Technology (CIT)*, Pafos, 2011, pp. 245-248.

[12] A.i, Parashar and R. Radhakrishnan, "Improved deterministic packet marking algorithm for IPv6 traceback.," in *In International Conference on Electronics and Communication Systems (ICECS)*, Coimbatore, 2014, pp. 1-4.

[13] V. Paruchuri, A. Durresi, and S. Chellappan, "TTL based packet marking for IP traceback.," in *In IEEE Global Telecommunications Conference*, New Orleans, LO, 2008, pp. 1-5.

[14] B. Feng and H. Yusheng, "Improved probabilistic packet marking scheme based on APPM-V6," in *In IEEE 7th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, NanChang, China, 2014, pp. 380-386.

[15] Andrew S. Tanenbaum, *Computer networks, 4-th edition.*, 4th ed.: Pearson Prentice Hall, 2003.

[16] A. Behrouz. Forouzan, *Data Communications & Networking*, 4th ed.: Tata McGraw-Hill Education., 2006.

[17] Charles E. Perkins, "Mobile networking through Mobile IP," *IEEE Internet Computing*, vol. 2, no. 1, pp. 58-69, Feb 1998.