IP Traceback Support for Wired and Mobile IP Networks

Adnan Aijaz[1], Syed Raza Mohsin[2] and Mofassir-ul-Haq[3]
Military College of Signals/National University of Sciences and Technology (NUST)
Rawalpindi, Pakistan
{adnanaijaz, razamohsinn}@hotmail.com, mofassir_haque@mcs.edu.pk

Abstract

The Internet has brought a revolution in today's life. Future of Internet is even more promising because of emerging technologies like ubiquitous computing, context sensitive, adaptive and reconfigurable applications. Security is the most important issue concerned with Internet. Internet is exposed to threats like system penetration, financial fraud, theft of proprietary information, Denial of Service (DoS)/Distributed Denial of Service (DDoS) Attacks etc. Currently, DoS/DDoS attacks are the most expensive computer crimes. The attacker launching this type of attacks commonly masks his identity using IP spoofing. It is very difficult to identify the sources of a DoS/DDoS attack. IP traceback methods are used to locate the source of packets causing DoS/DDoS. In this paper we suggest a hybrid IP traceback technique based on TTL identification for both IPv4 and IPv6 networks. We have also extended this technique to be compatible with Mobile IP.

Key words*: Internet, Security, IP traceback, DoS, DDoS, IP spoofing.*

1. INTRODUCTION

The Internet is the basis of number of innovative technologies like the World Wide Web, Email, P2P applications, VOIP etc. It has enabled instant access to vast and diverse resources. But, Internet is also vulnerable to number of attacks from different sources. Major categories of attacks during 2006 were viruses, insider abuse of access, unauthorized access to information, and denial of service (DoS) attacks [1]. It is often much easier to disrupt the operation of a network or system than to actually gain access to a network. There are number of freely available tools on Internet, from covertly exchanged exploit programs to publicly released vulnerability assessment software, to degrade performance or even disable vital network services [2].

1.1 DoS/DDoS

The aim of DoS attack is to prevent legitimate users access to system resources by shutting down or seriously slowing down a service provided by a computer system. DoS first received large scale public attention in February 2000 when major Internet sites including Amazon, Yahoo, CNN and e bay were brought down by DoS attacks. CNN and other victims claimed that the attack caused damages totaling $1.7 billion [3].

DoS attacks are classified as either flooding or logic attacks. In flooding attack the victim is overloaded with a large amount of traffic thus consuming resources. Example of flooding attack is the TCP/SYN flooding [4]. Logic attacks are however, based on exploiting the vulnerabilities in the target system and can be carried out even with a single well crafted packet [5]. Example of logic attack is the LAND attack [4].

In distributed DoS (DDoS) attack, the attacker uses hundreds or thousands of compromised hosts, often residing on different networks, to overload and crash target system [6]. Currently, it is not possible to prevent DoS/DDoS attacks because they are based on exploiting weaknesses in the core internet protocols which are embedded in the underlying network technology.

1.2 IP Traceback

In DoS/DDoS attack, attacker uses fake source IP addresses to make tracing and stopping of DoS difficult. This technique is called IP spoofing. This technique involves the manipulation of the source IP address in the IP header of a transmitted packet. This gives the attacker a form of anonymity. It is difficult to solve problem of IP Spoofing because of lack of security features in TCP/IP specifications. Ingress filtering, Use of cryptographic authentication , IP trace back are some of the approaches used to handle forged IP source addresses [7]. The purpose of IP traceback is to identify the true IP address of a host originating attack packets. IP trace back is vital for quickly restoring normal network functionality and preventing reoccurrences [8].

1.3 Existing IP Traceback Techniques

There is no intrinsic support to identify the real sources of IP packets in the Internet architecture, so different techniques have been proposed to provide traceback capability. Existing trace back schemes can be roughly categorized into three distinct categories viz. traditional, marking and logging. In traditional scheme, victim develops an attack signature, consisting of some data common and unique to the attack traffic. A query including the attack signature is then sent hop-by-hop to each router along the path. Examples of this type of technique are input debugging and controlled flooding [9]. In packet logging, the IP packet

is logged at each router through which it passes. Routers are queried in order to reconstruct the network path. SPIE (Source Path Isolation Engine) is an example of this type of technique [10]. In packet marking [11], the router marks IP packets with its identification information. The network path can be reconstructed by combining packets containing marks. The marking information may be inscribed in the same attack packets called inbound marking or extra ICMP packets called outbound marking. Current traceback schemes based on marking include variants of PPM (Probabilistic Packet Marking), ATA (Algebraic Based Traceback Approach) [12], DPM (Deterministic Packet Marking) [13], and schemes that use ICMP (Internet Control Message) messages, such as iTrace [14].

2. A HYBRID IP TRACEBACK TECHNIQUE BASED ON TTL IDENTIFICATION

The aim of all the traceback approaches is to identify the sources of attacking traffic but path reconstruction algorithms actually reveal the identity of first router on the path. A better approach would be to find an algorithm that reveals the identity of first router without requiring the participation of all the routers on the path [14].

Since the attacker can forge any field in the IP header, he can't falsify the Time to live (TTL) field. The TTL is an 8-bit field that determines the maximum number of hops a datagram can traverse. Each router decrements the TTL value by 1, after forwarding the datagram. The problem of determining the first router on the path can be solved by using this field.

The TTL field is different for different operating systems and is not universally selected, but all the packets sent by a particular operating system will have the same initial TTL value [16]. Default TTL values for different operating systems are shown in Table 1.

The basic idea behind our technique is to create a TTL vs. operating system table and store it on the routers. The matching of a TTL value with any entry of the table is indicative of the fact that this is the first router on the path. The router should then mark the packet with its IP address. For marking purpose, we select the 'Record Route (RR)' optional field in the IPv4 header. The IP address of the router would be stored in the first 4 bytes of route data in RR field. The router should in fact overwrite the first 4 bytes of route data in RR field if RR is already present. So even if the attacker forges the RR field with wrong IP addresses or unnecessary data, it would still be overwritten with the true IP address of the router. Routers other than the ingress router cannot mark the packet, since TTL value would not match any entry in the TTL vs. operating system table. The minimum required length of RR field is 7 bytes (4 bytes for route data, 1 byte for option type code, 1 byte for option length and 1 byte for pointer into the route data). The remaining space in the optional field can be used for other options like 'Strict Source Route', 'Loose Source Route', 'Stream Identifier' etc, if required.

Table 1: Default initial TTL values for different operating systems [16]

OS	Version	Platform	TTL
Windows	9x/NT	Intel	32
Windows	9x/NT	Intel	128
Windows	2000	Intel	128
Digital Unix	4.0	Alpha	60
Unisys	x	Mainframe	64
Linux	2.2.x	Intel	64
FTX (UNIX)	3.3	STRATUS	64
SCO	R5	Compaq	64
Netware	4.11	Intel	128
AIX	4.3.x	IBM / RS6000	60
AIX	4.2.x	IBM / RS6000	60
Cisco	11.2	7507	60
Cisco	12.0	2514	255
IRIX	6.x	SGI	60
Free BSD	3.x	Intel	64
Open BSD	2.x	Intel	64
Solaris	8	Intel / Sparc	64
Solaris	2.x	Intel / Sparc	255

The flooding DoS attack uses IP spoofing. The problem of this Source address spoofing can be solved by a technique called Ingress Filtering [17], in which the router discards the packets with illegitimate source addresses. The legitimacy of source address can be checked from the network id part of the IP address. A serious limitation of this technique arises when the attacker forges the address to the one that belongs to the same network as the attacker's host.

A more effective solution for IP traceback is to combine Ingress Filtering with this variant of packet marking (based on TTL identification). The packet is first checked for spoofing and is discarded if the source address is forged (doesn't have a valid network id). If the source address has a valid network id, the packet is marked with router's identity. This would obviously reduce the marking overhead of the router. This technique also requires minimum storage requirements at the routers and the present day routers can efficiently execute this marking procedure. The algorithm for this hybrid technique is shown in figure 1.

This hybrid technique is significantly different from the basic Deterministic Packet Marking (DPM) as described in [13, 15] in following respects.

- Reduced marking overhead due to ingress filtering.

- No need of address reconstruction algorithm.
- Faster convergence.
- Usability of 'Identification field' in IPv4 header is retained for fragmentation purposes.
- Reliable approach to identify the ingress router.

```
#define net_id
#define router_ip

struct datagram
{
/*
   this structure contains different fields of IP Header
   e.g, int ttl;
*/

main() {
datagram D;
int ttl_table[18];  /*
                        initial ttl values for different
                        operating systems
                    */
for (each D)
{
 for i=0:17
 {

  if D.ttl==table[i]        // ingress router identified
  {
   y=compute_netid(D.source_address);  /*
                                          compute net id
                                          from source IP
                                          address
                                       */
   if y==net_id
   {
    write router_ip into D.record_route
    forward(D)      // forward the datagram after marking
    }
   else if y!=net_id
    discard(D)       /*
                       discard datagram if invalid source
                       IP address
                     */

   }

   else if D.ttl!=table[i]          // not ingress router
   forward(D)         // forward datagram without marking
   }

  }
 }
```

Figure 1: Algorithm for the hybrid IP Traceback technique based on TTL identification

3. PERFORMANCE EVALUATION

This hybrid technique was simulated in the Network Simulator (ns-2.31) [18] at network layer to measure the delay for marked traffic as compared to normal (unmarked) traffic. The simulator was running on an Intel based machine having 1.7 GHz processor and 512 MB of main memory. The internal files of ns-2.31 were modified to incorporate packet marking in it. The simulated topology is shown in figure 2.

The size of the topology doesn't matter because all the delay is incurred at the first router only. Traffic originated from node 7 and was destined for node 3. For this traffic, node 0 acts as the first router on the path. Traffic consisted of TCP packets of 1040 bytes carrying FTP data. The comparison between marked and normal traffic is shown in figure 3. The additional time taken by marked traffic is just 0.8 milliseconds. Similar delay is also observed for traffic from node 13 to node 8 for which node 12 acts as the first router on the path.

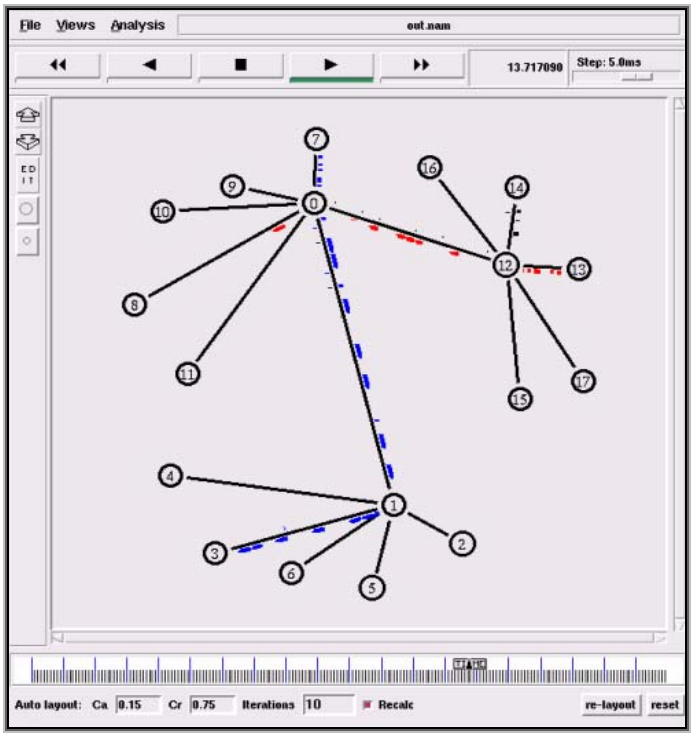

Figure 2: Simulated topology

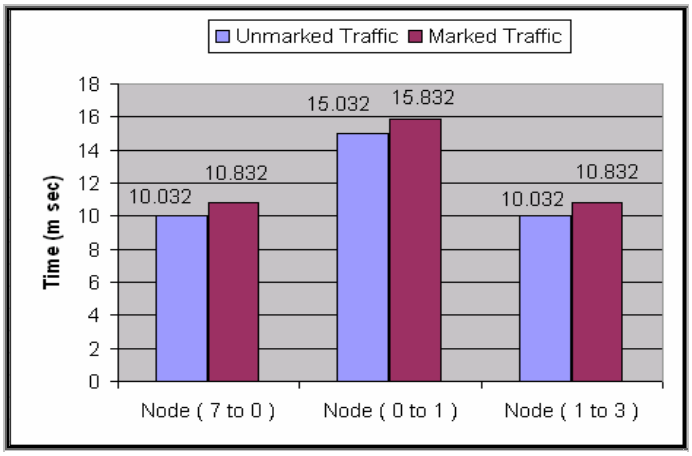

Figure 3: Graph showing the delay for marked traffic as compared to normal traffic

4. IPv6 COMPATIBILITY

IPv6 was proposed to overcome different problems of IPv4 like address depletion, lack of security features, lack of support for real-time audio and video etc. IPv6 addresses are 128 bits long as compared to 32 bit addresses of IPv4 [19].The Hop limit field in IPv6 base header serves the same

purpose as TTL field in case of IPv4. The length of base header is fixed at 40 bytes. However, to achieve greater functionality, extension headers are used. Most of the extension headers are options in IPv4. In this section we describe, how our proposed technique would work with IPv6.

The matching of Hop limit value with any entry of Table 1 will identify the first router on the path. This router should then mark the packet with its identification (128 bit IP address). Since Record Route option is not implemented in IPv6, we propose to use 'Destination Option' extension header which is identified by a Next header value of 60. The Destination Option is used when the source needs to pass information to the destination only. Intermediate routers are not permitted to access this information.

The 128 bit Destination address field in IPv6 header is not necessarily the final destination. It contains the address of next hop when source routing is used. It means that the intermediate routers can have access to Destination Option field which is not desired.

This problem can be solved by placing the Destination Option extension header after the routing header and before the upper layer header [19]. In this case only the final destination is allowed to process the Destination Option header.

5. IP TRACEBACK FOR MOBILE IP

With the advent of wireless communications, host computers or PDAs can roam geographically and topologically, which results in change of IP address, thus affecting ongoing connections and higher layer applications. Mobile IP was developed to enable computers to maintain Internet connectivity while moving from one internet attachment point to another [20]. Although Mobile IP can work with wired connections, it is particularly suited to wireless connections.

5.1 Mobile IPv4

In case of Mobile IPv4, a mobile node (MN) is assigned two IP addresses, a home address (HoA) which is static, and a care-of address (CoA) which changes at each new point of attachment. The CoA is the address of the foreign agent (FA), which is a specialized router on the foreign network, and is shared among different mobile nodes. When the mobile node is not attached to its home network, a home agent (HA), which is a specialized router on the home network, tunnels the packets destined for the MN to its current point of attachment (CoA). Since the CoA is shared among different MNs, the FA uses a visitor list (table 2) to deliver the packets to the particular MN [21]. A detailed discussion on Mobile IPv4 can be found in [22].

5.2 DoS Attacks in Mobile IP Networks

DoS attacks in Mobile IP networks can be classified as either authentication-based attacks or flooding-based attacks [23]. In case of authentication-based attacks, an unauthorized node spoofs the identity of a legitimate MN and redirects the packets destined for MN to other network locations. So a service is denied to the legitimate MN.

Flooding-based attacks are similar to flooding attacks in wired IP networks, in which a MN acts as a source of attack traffic. IP Traceback methods can only trace flooding-based attacks in Mobile IP networks. Authentication-based attacks are difficult to trace because the victim (legitimate MN) has no attack traffic to analyze.

5.3 Extending Our Proposed Technique for Mobile IPv4

We consider the following two scenarios in context of Mobile IPv4.

1. When the MN is acting as a source of DoS attack and is residing on the home network.
2. When the MN is acting as a source of DoS attack and residing on the foreign network.

The first case is not specific to Mobile IPv4. It can be treated as a normal attack for IPv4, since the mobile node operates without mobility services, when residing on the home network. So the traffic of the MN is marked in a similar manner as proposed for a wired node.

The second case is specific to Mobile IPv4. The MN uses its HoA as the source address when it sends packets to any other node in the internet. If ingress filtering is enabled on the FA then the traffic of the MN would be discarded [21]. Since ingress filtering is an essential part of our technique as well, we propose conditional ingress filtering i.e., if the packet is not having a valid network id, the source address should be checked in the visitor list. If there is an entry for the source address, the packet should be marked with the HA address, otherwise the packet should be discarded. For marking purposes, the same Record Route field can be used as described in section 2. So even if the MN is roaming among different foreign networks while flooding the victim, the victim can trace the attack's source. It should be noted that in this process, the TTL has to be checked first, to verify the existence of first router (first FA) on the path. The marking scenario of Mobile IPv4, when reverse tunneling [24] is used, changes to the general IPv4 marking scenario but the packet should be marked before encapsulation.

Table 2: Visitor List on the Foreign Agent

HoA	HA Address	Media Address	Lifetime (sec)
100.10.1.9	100.10.1.0	00E166956550	200
200.20.2.18	200.20.2.0	00E166937649	100
----------	----------	----------	----------

6. CONCLUSION

The development of IP traceback techniques is motivated by different DoS attacks in recent years. With the development of Mobile IP, more complex DoS attacks can be launched. However, IP traceback is the first step in identifying the attacker behind the attacks. The effectiveness of any traceback technique depends primarily on its overhead, convergence and the ability to trace any type of DoS attack. The hybrid technique presented here is capable of tracing any type of DoS attack because we can trace even a single packet. Today there is a need of practical implementation of an effective technique so that IP traceback could be carried out in real time across the internet.

REFERENCES

[1]. Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Robert Richardson, CSI/FBI Computer Crime and Security Survey, 2006.

[2]. Computer Emergency Response Team. CERT advisory CA-1999- 17 denial of service tools. http://www.cert.org/advisories/CA-1999-17.html.

[3]. Computer Emergency Response Team. CERT advisory CA-2000- 01: denial of service developments. http://www.cert.org/advisories/CA-2000-01.html, 2000.

[4]. M. Handley and E. Rescorla, "*Internet Denial-of-Service Considerations"*, Request for Comments 4732, Internet Engineering Task Force, Nov 2006.

[5]. D.Moore, G. M. Voelker and S. Savage, "*Inferring Internet Denial of Service activity*" ACM Trans. Comput. Syst., vol. 24, no. 2, pp. 115-139, May 2006.

[6]. Matthew Hutchinson, "*Study of Denial of Service*", MS Dissertation, Queen's University of Belfast, Aug 2003.

[7]. J. Li, J. Mirkovic, M. Wang, P. Reiher and L. Zhang, "*SAVE: Source Address Validity Enforcement Protocol*", in Proc IEEE INFOCOM, 2002, pp 1557-1566.

[8]. S.C. Lee and C. Shields, "*Tracing the Source of Network Attack: A Technical, Legal and Societal Problem*", Proc. 2001, IEEE Workshop on Information Assurance and Security, IEEE Press, 2001, pp. 239-246.

[9]. Hassan Aljifri, "*IP Traceback: A New Denial of Service Deterrent*", IEEE Computer Society, 2003.

[10]. A.C. Snoeren, C Patriage, L. A. Sanchez and S. Kent, "*Hash-based IP Traceback*", Proc. of ACM SIGCOMM conference, 2001, San Diego, CA, Computer Communication Review vol 31, no 24, Oct 2001, pp. 3-14.

[11]. Chao Gong and Kamil Sarac, "*IP Traceback based on Packet Marking and logging"*, Proc. of International Conference on Communication, 2005, Seoul, Korea, IEEE Communications Magazine, vol 2, May 2005, pp 1043-1047.

[12]. D. Dean, M. Franklin and A. Stubblefield, "*An Algebraic Approach to IP Traceback"*, ACM Trans. Info. and Sys. Sec., vol 5, May 2002, pp. 119-137.

[13]. Zhiqiang Gao and Nirwan Ansari, "*Tracing Cyber Attacks from Practical Perspective*", IEEE Communications Magazine, 2005.

[14]. Vadim Kuznetsov, Andrei Simkin and Helena Standstorm, "*An evaluation of different IP Traceback Approaches*", Proc. of 4th International Conference on Information and Communication Security, Singapore, 2002, pp 37-48.

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

[16]. Ankit Fadia, "*Network Security: A Hacker's Perspective*", pp. 125-127, Course Technology Inc, 2006. ISBN 1598631632.

[17]. S. Savage, D. Wetherall, A. Karlin and T. Anderson, "*Practical Network Support for IP Traceback*", Proc ACM SIGCOMM Conference, Aug 2000, Stockholm, Sweden, Computer Communication Review, vol 30, no 4, pp. 295-306, Oct 2000.

[18]. The Network Simulator – ns-2 http://www.isi.edu/nsnam/ns

[19]. S. Deering and R. Hinden, "*Internet Protocol, Version 6 (IPv6) Specification*", Request for Comments 2460, Internet Engineering Task Force, Dec 1998.

[20]. Henry C.J. Lee et al, "*On the Issues of IP Traceback for IPv6 and Mobile IPv6*", Proc. of 8th IEEE International Symposium on Computers and Communications (ISCC) 2003.

[21]. C. Perkins, "*Mobile Networking through Mobile IP*,"IEEE Internet Computing, Jan-Feb 1998.

[22]. C. Perkins, "*IP Mobility Support for IPv4*", Request for Comments 3344, Internet Engineering Task Force, Aug 2002.

[23]. Tarik Taleb et al, "*Securing Hybrid Wired/Mobile IP Networks from TCP-Flooding Based Denial-of-Service Attacks*", IEEE GLOBECOM, 2005, pp 2907-2911.

[24]. G. Montenegro, "*Reverse Tunneling for Mobile IP*" Request for Comments 3024, Internet Engineering Task Force, Jan 2001.