# Tracing the True Source of an IPv6 Datagram Using Policy Based Management System*

Syed Obaid Amin[1], Choong Seon Hong[2,**], and Ki Young Kim[3]

[1,2] School of Electronics and Information, Kyung Hee University,
1 Seocheon, Giheung, Yongin, Gyeonggi, 449-701 Korea
obaid@networking.khu.ac.kr, cshong@khu.ac.kr
[3] Electornics and Telecommunications Research Institute,
161 Gajeong-dong,Yusung-gu, Daejeon, 350-700, Korea
kykim@etri.re.kr

**Abstract.** In any (D)DoS attack, invaders may use incorrect or spoofed IP addresses in the attacking packets and thus disguise the factual origin of the attacks. Due to the stateless nature of the internet, it is an intricate problem to determine the source of these spoofed IP packets. This is where; we need the IP traceback mechanism i.e. identifying the true source of an IP datagram in internet. While many IP traceback techniques have been proposed, but most of the previous studies focus and offer solutions for DDoS attacks done on IPv4 environment. Significant differences exist between the IPv4 and IPv6 Networks for instance, absence of option in basic IPv6 header. Thus, the mechanisms of IP Traceback for IPv4 networks may not be applied to IPv6 networks. In this paper, we extended our previous work i.e. PPM for IPv6 and removed its drawback by using Policy Based IP Traceback (PBIT) mechanism. We also discussed problems related to previously proposed IPv4 traceback schemes and practical subtleties in implementing traceback techniques for IPv6 networks.

**Keywords:** DDoS, Traceback, IPv6, Network Security.

## 1 Introduction

To deter (D)DoS attacks, technologies like Intrusion Detection System (IDS) [13], Intrusion Prevention System (IPS) [14] and the Firewalls [15] are good solutions. However, in reality, prevention of all attacks on the internet is nearly impossible and the situation gets worse due to anonymous nature of IP protocol i.e. an attacker may hide its identity if he wants to. Moreover, the routing decisions are taken on destination addresses and none of the network unit makes sure the legitimacy of source address. Therefore, when prevention fails, a mechanism to identify the source(s) of the attack is needed to at least ensure accountability for these attacks and here we need the traceback techniques.

The elements that were threatening for IPv4 networks can also be intimidating for the future IPv6 network. To cope with IPv6 networks, we need to modify IPv4's

* This work was supported by MIC and ITRC Project.
** Corresponding author.

Y.-T. Kim and M. Takano (Eds.): APNOMS 2006, LNCS 4238, pp. 263 – 272, 2006.

traceback technologies to be suited to IPv6 network. The reasons behind this amendment are the technological differences between these two network-layer protocols for instance, change in header size or fragmentation mechanism.

As mentioned before, the goal of traceback scheme is to identify the true source of a datagram. To achieve this task we try to pass the info of a packet or a path taken by a packet to the victim. One of the ways is that routers probabilistically or deterministically mark path information in packets as they travel through the Internet. Victims reconstruct attack paths from path information embedded in received packets. Packet marking techniques can be subdivided in Deterministic Packet Marking (DPM) [10] and Probabilistic Packet Marking (PPM) [2, 3, 4, 9]. In messaging routers probabilistically send ICMP messages, which contain the information of forwarding nodes the packet travels through, to the destination node. Victims reconstruct attack paths from received ICMP messages [1]. Another way of tracking the source of a packet is Packet Digesting in which routers probabilistically or deterministically store audit logs of forwarded packets to support tracing attack flows. Victims consult upstream routers to reconstruct attack paths [5, 8].

In this paper, we start our discussion with our previous work i.e. PPM algorithm for IPv6 networks [17]. Later on, to eliminate the deficiency of IPv6 PPM, we propose an IP traceback mechanism using Policy Based Management System. The rest of this paper is articulated as follows: In section 2, we describe related work. Section 3 outlines our previously proposed technique [17]. Section 4 covers the IP traceback technique using Policy Based Management System. Section 5 provides the simulation results and finally, we summarize our findings in Section 6.

## 2 Related Work

### 2.1 Packet Marking

Packet Marking [1][3][4][10] algorithms are based on the idea that intermediate routers mark packets that pass through them with their addresses or a part of their addresses. Packets can be marked randomly with any given probability or deterministically. The victim can reconstruct the full path with given mark packets, even though the IP address of the attacker is spoofed. This scheme was improved in several different ways; some of them introduced improved coding methods and security. All of the IPv4 marking algorithms suffered by the space limitation of IPv4 header. Therefore they have to utilize encoding or fragmentation of intermediate router's address. The encoding of each and every packet of course degrades the routing performance while fragmentation of address in small chunks may lead to state explosion problem that is discussed in [7]. As a result, none of the packet marking traceback techniques has been adapted for the practical work or implementation so far. In our previous work, we presented a PPM algorithm for IPv6 environment which is discussed in Section 3.

### 2.2 ICMP Traceback

ICMP traceback [1] scheme lies under the messaging category. Every router on the network is configured to pick a packet statistically (1 in every 20,000 packets

recommended) and generate an ICMP traceback message or iTrace directed to the same destination as the selected packet. The iTrace message itself consists of the next and previous hop information, and a timestamp. As many bytes of the traced packet as possible are also copied in the payload of iTrace. The time to live (TTL) field is set to 255, and is then used to identify the actual path of the attack.

This scheme can also be deployed on IPv6 networks and presents a very expandable technology if implemented with encryption and key distribution schemes. However, the additional traffic generated consumes a lot of bandwidth even with very low frequency (1/20,000). Without encryption, an attacker can inject false ICMP tra ceback messages. In addition, ICMP traffic is filtered in many organization to avoid several attack scenarios which make iTrace not that much useful.

### 2.3 Hash Based IP Traceback

It comes under packet digesting technique. In Hash-based traceback [5][6], officially called Source Path Isolation Engine(SPIE), specialized router confines partial information of every packet that passes through them in the form of hash, to be able in the future to determine if that packet passed through it. In this scheme such routers are called data generation agents (DGAs). DGA functionality is implemented on the routers. The network is logically divided into regions. In every region SPIE Collection and Reduction Agents (SCARs) connect to all DGAs, and are able to query them for necessary information. The SPIE Traceback Manager (STM) is a central management unit that communicates to IDSs of the victims and SCARs.

This technique is very effective and capable of identifying a single packet source as well as, according to best of our knowledge, the only scheme that also has solution for IPv6 networks [8]. This scheme, on the other hand, is very computational and resource intensive because tens of thousands of packets can traverse a router every second, the digested data can grow quickly to an enormous size, which is especially problematic for high-speed links.

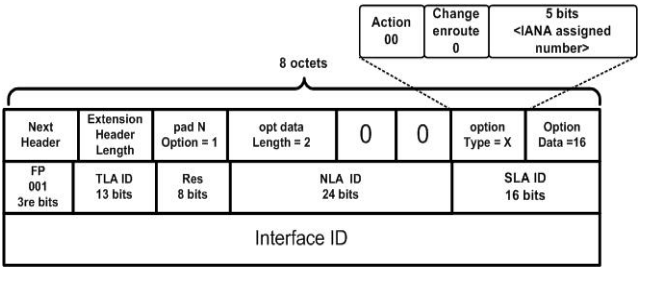


**Fig. 1.** Proposed Marking Field

## 3 Probabilistic Packet Marking (PPM) for IPv6 Traceback

This section will briefly discuss our previous work i.e. PPM for IPv6. In PPM for IPv6, router en route probabilistically marks the incoming packets with the Global unicast IPv6 address of that router. We used Hop-by-Hop Header [16] to store a mark

the reasons were two folds; first, the Hop-by-Hop option is processed by every router en-route. Second, it provides the larger space to store a mark. Proposed option in Hop by hop option header is shown in Figure 1.

Use of extension headers gave us great flexibility to pass the information to the victim. As we marked the packet with complete address, our scheme is not vulnerable to state explosion problem [7]. We used these marked packets to construct the reverse routing table from victim to attackers. For this purpose, on victim side, we proposed a data structure called Reverse Lookup Table (RLT). Following steps were taken to complete the traceback.

1. The victim will sort the RLT by distance field; as shown in figure 2.
2. Observe the discontinuity in distance field and apply the error correction algorithm (ECA) to find the missing nodes.
3. Finally, victim will resolve the last hop field to complete the RLT.

The resultant sorted tuples of routers can provide a complete path from Victim to attacker.

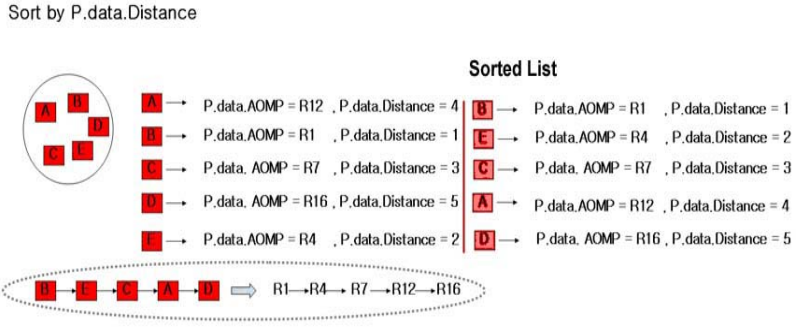


**Fig. 2.** Reconstructed path using AOMP value and Distance value

This algorithm worked under the assumption that victim is in DDoS attack so the number of evading packets would be sufficient to provide the information of all routes. However, it is quite practical the victim does not have complete route information of the attacker. For this purpose, we also introduced the Error Correction Algorithm [17]. Marking the packet with extra 20 bytes might increases the size of packet than PMTU, and since intermediate routers cannot do fragmentation, the packets will be dropped. Therefore, we also proposed a modified Path MTU (PMTU) discovery algorithm discussed in detail in [17].

## 4 Policy Based IP Traceback (PBIT)

### 4.1 Motivation of Another Traceback Technique

Thousands of packets traverse through one router in a second and marking of every packet, even probabilistically, may affect routing performance. Therefore, the

cooperation in implementing the traceback algorithm will not be tempting for ISPs. Because it is obvious, none of the ISP provides security to other networks by sacrificing their own customers' satisfaction. To cope with these problems, there should be a mechanism to minimize the burden of packet marking and initiate packet marking only when a victim is under (D)DoS attack.

One of the ways to accomplish this is to deploy IDS on victim side and once this IDS detects an attack it sends message to intermediate routers to initiate marking. However, since we do not have any information of path (because we are not using PPM here that is discussed above) we cannot send the message to desired routers to start marking. The other option left is to multicast the message to all backbone routers that is quite impractical due to many reason such as increase in network traffic that may lead to network congestion. Moreover, if going along with standards, we will have to use ICMP to send these messages and ICMP traffic is mainly filtered in many ISPs. Therefore, there are much greater chances that these messages will be dropped by most of the ISPs.

Another possible way is that IDSs are deployed on intermediate routers and starts marking packets, once they detect congestion or high packet rate on any specific interface. This scheme seems appealing by keeping in mind that most of the routers now come with IDS functionality or we may plug-in the IDS functionality in a router as a separate module (if this feature is present in router). The problem with this architecture that these types of router or routers with IDS are normally deployed on the edges of network due to the fact that adding IDS support to backbone routers will degrade the routing performance as IDS requires high end processing to infer something about attacks.

### 4.2 PBIT Mechanism

To mitigate the above problems we utilized the power of Policy Based Management System [12]. Policy-based management is an administrative approach that is used to simplify the management of a given endeavor by establishing policies to deal with situations that are likely to occur. The description of Policy Based Management is out of scope of this paper but it would be worthy to mention two basic building blocks of Policy Based Management architecture i.e. Policy Decision Point (PDP) and Policy Enforcement Point (PEP). PDP is a resource manager or policy server that is accountable for handling events and making decisions based on those events (for instance; at time *t* do *x*), and updating the PEP configuration appropriately. While the PEP exists in network nodes such as hosts, routers and firewall. It enforces the policies based on the "if condition then action" rule sets given by the PDP. Both PDP and PEP communicates with each other through COPS (Common Open Policy Service) that is a typical protocol [12], although DIAMETER or even SNMP may be used.

To go with policy based management framework, of course due to standard, we slightly modified our architecture. Instead of probabilistically marking of every packet by intermediate routers, we maintain a list of participating edge routers (the router closest to the sender) on PDP and placed an IDS along with traceback agent near to the victim as shown in Fig. 3.

Once the IDS detects a (D)DoS attack on victim, it generates the request to PDP to enforce policy which in turns, send message to all participating routers (i.e. PEP) found in the list to initiate packet marking *deterministically*. Most of the IDSs detect an attack after observing a huge traffic volume, and if we start probabilistic packet marking after this point, we might not have large amount of marked packets to construct the complete path. Therefore, in PBIT, we deterministically mark the packets so one packet would be enough to get the entire path. Actually, through this algorithm, we are not getting the entire path of an attack instead; we will be able to get only the injection point of an attack but finding the address of an ingress point is as good as full path traceback.

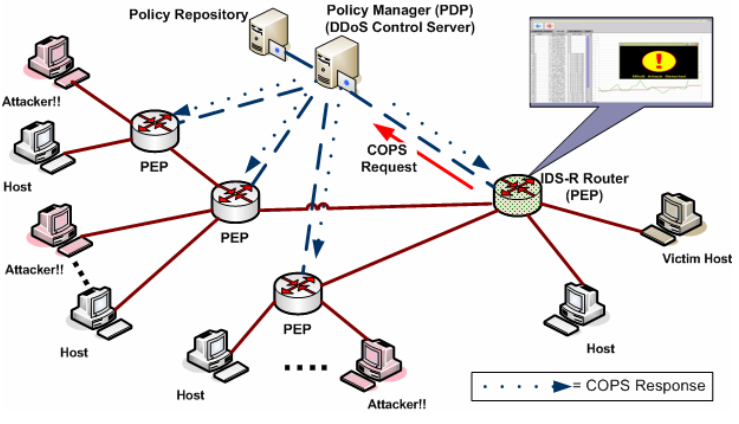


**Fig. 3.** Network architecture of policy based traceback system

The foremost improvement through this modification is obviously the lesser burden on intermediate routers of marking packets even they are not under (D)DoS attack hence will not affect the routing performance. Moreover, by using COPS, we are not deviating ourselves from standards else we could have a specialized server which maintains the list of participating routers and signal them to start packet marking after getting an indication from IDS. The complete pseudo code of PBIT is given below.

**At source:**

```
M = max (PMTU, 1280) - 26 bytes;
for every packet p{
    if p.size > M{
          fp[i]=fragment(p,M);
                send(fp[i]);
          }else
                send(p);
    }
```

**At edge routers (PEP):**

```
Marking procedure at edge router R:
Let attack is set to 1 when R got a signal from PDP:
    for every packet p{
          if (attack=1)
                mark_packet(p);
          forward(p);
    }
```

**At Victim:**

*For traffic logging:*

```
          for every marked packet pm
          if (pm.interface_addr is in RLT)
              incr_packetcount(if_addr,current_time);
             else{
              add_in_RLT(if_addr);
              set_packet_count(if_addr,1,current_time);
             }
```

*For Traceback:*

```
          If packet qm is given
           If_addr=Get_ifaddrr(qm);
          Else
           If_addrr=max_count(RLT,time_period);
```

## 5 Implementation and Evaluation

In this paper, we presented both of our architectures for IPv6 traceback i.e. PPM and PBIT. In case of PPM, we were interested in the number of packets required to get the full path to the victim. For this, we developed a simulator in Java, as there is no good support for IPv6 networks in current network simulators. On the other hand, the efficiency of PBIT depends on the IDS that how accurately and quickly it detects an attack. For PBIT evaluation, we integrated our traceback agent to IDS as shown in Fig. 4 developed by our lab. The performance of this IDS system has already been evaluated in [11].

Below we are comparing the efficiency of implemented scheme with key evaluation metrics discussed in [1]; this paper gave several evaluation metrics but here we are judging our scheme to only those attributes that can be affected by proposed algorithm. The detail comparison is shown in Table 1.

**Processing Overhead:** The processing can take place either at victim side or at intermediate nodes. For an ideal traceback scheme, the processing overhead of traceback should be minimum. Although the Figure 4 represents the traceback agent as an integrated part but in fact it is acting as a separate component. Therefore, in PBIT the processing overhead at intermediate nodes and victim side is almost none. Although during traceback intermediate nodes will consume a little processing power

to mark a packet however, this kind of processing can be seen in *Time To Live (TTL)* and *Hop Limit* calculations in IPv4 and IPv6 networks respectively. Furthermore; it is apparent; the proposed scheme does not require any calculation of hash values or message digests, encoding/decoding or any other computational intensive job either on intermediate routers or at victim side.

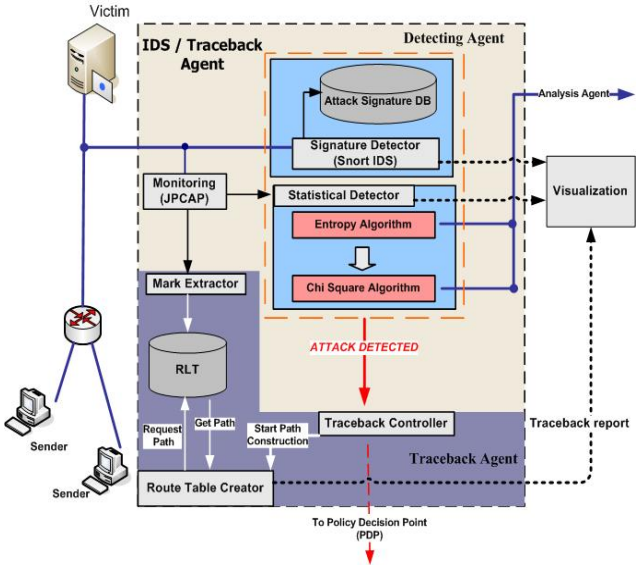


**Fig. 4.** Block diagram of overall architecture on victim side

**Number of Attacking Packets:** In PBIT, after (D)DoS attack detection, only one packet is enough to complete traceback which also eliminates the path reconstruction problem; one of the major weakness of PPM techniques.

**ISP Involvement:** As discussed above the traceback scheme should be tempting enough for ISPs because none of the ISP will compromise on quality of service and provide accountability of its user to other ISPs. If you ponder, you may realize that this is the motivation of PBIT. If any of the edge routers is not participating in traceback it can sincerely inform others ISPs or an ISP can also examine by observing the absence of the traceback option in this case the ISP which is not implementing PBIT would be considered as potential hacker and marking should be implemented on the interface(s) connected to that client ISP. It is pertinent to mention that for other IP traceback mechanism if intermediate nodes don't participate than it's nearly impossible to trace back an attack path.

**Bandwidth Overhead:** During traceback, we might need to slightly compromise on bandwidth consumption due to addition of one option header but this is acceptable as we already have much bigger routing header in IPv6 specification.

**Table 1.** Comparison of PBIT with other Traceback schemes

| | | iTrace | Hash-based | PPM | PBIT |
|---|---|---|---|---|---|
| | | | | | |
| Number of attacking packets | | Thousands | 1 | Thousands | **1** |
| ISP involvement | | Low | Fair | Low | **Low** |
| Network processing overhead | Every packet | Low | Low | Low | **None** |
| | During Traceback | None | Low | None | **Low** |
| Victim processing overhead | Every packet | None | None | None | **None**† |
| | During Traceback | High | None | High | **Low** |
| Bandwidth overhead | Every packet | Low | None | None | **None** |
| | During Traceback | None | Low | None | **Very Low** |
| Memory requirement | Network | Low | Fair | None | **None** |
| | Victim | High | None | High | **Low** |
| Ease of Evasion | | High | Low | Low | **Low** |
| Protection | | High | Fair | High | **High** |
| Can handle attacks other then DDoS | | No | Yes | No | **No** |

**Ease of Evasion:** Refers how easily an attacker can circumvent the traceback technique. In the case of PBIT we assume that edge routers are not compromised. For such instances, PPM algorithm will work best due to its distributed nature.

**Protection:** Relates to produce the meaningful traces if some of the devices included in traceback are undermined. PBIT is highly protective as intermediate routers don't participate in traceback and the single point of consideration is the router interface closest to the attacker if this interface or a router is down then there would be no way for an attacker to invade.

## 6 Conclusion

In this paper, we gave an introduction of IP traceback and a brief overview of current IP traceback trends. These schemes were not adapted widely for IPv4 networks. One of the main reasons was degradation in routing performance, as encoding should be applied to pass the path information through a limited space IPv4 header.

In this paper, we discussed two Packet Marking algorithms for IPv6 network. The extension header gave us great flexibility to pass the path information to the victim

† Considering IDS as an external component.

and since in both of our algorithms, information of routers are not distributed in different fragments as proposed in [3], our schemes are not affected by the state explosion problem that is discussed in [7]. We believe that PBIT is more appealing than PPM as it requires minimum ISP intervention and doesn't harm the routing performance. However, in the case of PBIT we assume that edge routers are not compromised. For such instances, PPM algorithm will work best due to its distributed nature.

## References:

[1] Belenky, A. and Ansari, N. "On IP Traceback," IEEE Communications Magazine, Volume 41, Issue 7, July 2003
[2] S. Savage et al., "Network Support for IP Traceback," IEEE/ACM Trans. Net., vol. 9, no. 3, June 2001, pp. 226-37.
[3] Dawn X. Song and Adrian Perrig, "Advanced and authenticated marking schemes for IP traceback," in Proceedings IEEE Infocomm 2001, April 2001
[4] K. Park and H. Lee, "On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack," Tech. Rep. CSD-00-013, Department of Computer Sciences, Purdue University, June 2000.
[5] A. Snoeren, C. Partridge, L. Sanchez, C. Jones, F. Tchakountio, B. Schwartz, S. Kent, and W. Strayer. Single-packet IP traceback. ACM/IEEE Transactions on Networking, Dec.2002.
[6] Aljifri, H. "IP traceback: a new denial-of-service deterrent" Security & Privacy Magazine, IEEE , Volume: 1 , Issue: 3 , May-June 2003 Pages : 24 - 31
[7] Marcel Waldvogel, "GOSSIB vs. IP Traceback Rumors", 18th Annual Computer Security Applications Conference (ACSAC '02).
[8] W. Timothy Strayer, Christine E. Jones, Fabrice Tchakountio, and Regina Rosales Hain, SPIE-IPv6: Single IPv6 Packet Traceback, Local Computer Networks, 2004. 29th Annual IEEE International Conference on 16-18 Nov. 2004 Page(s):118 – 125.
[9] Micah Adler, "Tradeoffs in probabilistic packet marking for IP traceback," in Proceedings of 34th ACM Symposium on Theory of Computing (STOC), 2002.
[10] A. Belenky and N. Ansari, .On IP traceback,. IEEE Communications Magazine, vol. 41, no. 7, July 2003.
[11] Choong Seon Hong , Pil Yong Park, Wei Jiang, " DDoS Attack Defense Architecture Using Statistical Mechanism on Active Network Environment ", Applied Cryptography and Network Security , pp. 47-56, June 2004
[12] A. Westerinen et al, "Terminology for Policy-Based Management", RFC3198, IETF, November 2001.
[13] http://en.wikipedia.org/wiki/Intrusion-detection_system
[14] http://en.wikipedia.org/wiki/Intrusion_prevention_system
[15] http://en.wikipedia.org/wiki/Firewall_%28networking%29
[16] S. Deering, R. Hinden, Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, IETF, December 1998.
[17] Syed Obaid Amin, Myung Su Kang and Choong Seon Hong, "A Lightweight IP Traceback Mechanism on IPv6", EUC Workshops 2006, LNCS 4097, pp. 671 – 680, 2006.