THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

# An Effective Detection of Real Source Attack Using Extended IP Traceback Mechanism

**G.D. Dhanalakshmi**
Research Scholar, Department of Computer Science,
Quaid-E-Millath Govt. College for Women Chennai, TamilNadu, India
**Dr. G.Velmayil**
Assistant Professor, Department of Computer Science,
Quaid-E-Millath Govt. College for Women, Chennai, TamilNadu, India

***Abstract:***
*Network becomes an essential part of everyone's life. Sophisticated network security technologies are being developed to protect data and preserve privacy. As the Internet has been widely applied in various domains, additional network security is the most important issue concerned with Internet. The internet is exposed to threats like System penetration, Data modification, Denial of service (DoS) attacks etc. DoS attack is the most expensive computer crimes. This paper proposes a new Extended IP Traceback mechanism with efficient packet marking to censor attack traffic on its upstream routers. In this process the key challenge is to reduce the number of packets that are involved in the traceback of these attacks. The proposed Traceback mechanism is the most successful implementation towards preventing DoS attacks and it can trace back the source of the attack based on Time to Live (TTL) value. In addition, it uses the (Network Address Translation and Port Address Translation (NAT/PAT) data extraction and considering in the Packet matching process to avoid the path reconstruction and thus to achieve zero false positive and false negative rates in attack-path reconstruction.*

***Keywords:*** *IP traceback,packet marking,DoS attack,TTL, path reconstruction,Query request,NAT/PAT transaction.*

## 1. Introduction

DoS attack render a computer or network incapable of providing service to legitimate users DoS attacks are classified as either direct or reflector attacks. In Direct attack, attacker generates huge amount of packets which are directly sent to the victim. A Reflector attack is an indirect attack in that intermediary node (routers and various servers), known as reflectors, is innocently used as attack launchers. DoS attack consist of an overwhelming quantity of packets being sent to a victim - these packets arrive in such high quantities that some key resource at the victim (network bandwidth, memory or I/O buffers, and CPU time to compute responses) is quickly exhausted [5]. Therefore it requires large storage space and has a false positive problem. The victim subsequently either crashes or spends so much time handling the attack traffic that it exceeds the TTL value [3], thereby depriving legitimate client's access to the system or resources.

The Extended IP traceback scheme designed to defend indirect or reflective attack and to perform the traceback from a single attack packet without requiring state storage in the network infrastructure. Here the paths of incoming packets are traced by using IP-Traceback scheme. The router will mark the incoming packet by packet marking technique and using this technique one can identify the network through which that packets are coming. The router has to modify the packet header and it has to insert the identity of intermediate router in the packet header. This packet marking scheme allows to reconstruct the network path from the victim to the attackers.Often the attackers use incorrect or spoofed IP addresses in the attack packets, hence the true origin is lost. No verification method to check IP addresses and key marking and therefore reduction in accuracy of finding DoS type attack. To avoid this kind of problem, newly implemented Novel NAT/PAT Packet Marking (NNPM) can serve as an efficient and secure scheme for extended IP traceback.This paper is organized as follows. In Section 2 surveys related research on IP traceback, NAT/PAT and packet marking/packet logging schemes. Section 3 introduces proposed method. Section 4 presents experimental results of our work. Finally section 5 describes conclusion and future scope of the work.

## 2. Previous Work on IP Traceback

IP traceback is a successful technique to find the source of the attacks and determine the path travelled by the packets to perform the attack. This technique can be used in such scenarios to find the source of the attacks and the path taken by the packets from the attacker to the victim.

*2.1. Hybrid IP Traceback (HIT) Scheme*

Ming-Hour Yang et al. [1] proposed a new novel hybrid IP traceback scheme comes under the domain network security. HIT uses packet marking to reduce the number of routers required for logging. Packet logging and Packet marking algorithm are considered in this hybrid traceback scheme. In this technique packet logging is assumed to have a fixed storage space for each router. Since it has fixed storage space there is no need for refreshing the table. However, this method does not give better solution for the problem caused by packet fragmentation.Other researchers have proposed new schemes to further reduce the storage requirement for router logging and to decrease the number of routers required for logging, e.g., Huffman codes, modulo/Reverse modulo Technique (MRT) and Modulo / REverse modulo (MORE). 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.

Marcelo D. D. Moreira et al. [2] proposed a stateless IP traceback mechanism that identifies the source network of each individual packet. And it is the only one that scales with the number of attackers and also satisfies practical requirements, such as no state stored at routers and a header overhead (25 bits) that can be allocated in IPv4 header. These method implements two nodes at Autonomous system level, first a customer provider hierarchy of the web at separate system level and second presents idea of check points. Thus, it allows tracing the origin AS with high accuracy, despite the marking space limitation.

S. Malliga et al. [4] discussed a packet marking algorithm, which follows hybrid marking scheme to solve IP traceback problem where the packets travel through the network, and they are marked with router information using modulo technique. Upon traceback request, to reconstruct the path traversed by the packets we use reverse modulo. In particular, this method reconstructs the attack path with one packet and acquires very less overhead on the network and router. It requires logging at routers, so the storage overhead on the routers is also significantly reduced. And stores the entire path traversed in a single packet and thus leads to less convergence time to find the attack path at the victim.

Tao Peng et al. [12] proposed a new adjusted marking scheme to increase the probability of receiving packets from distant routers. In this technique, the marking probability at every router is computed by using the distance from itself to the destination. The marking probability is computed using the formula 1/ (31-d) where d is the distance from the current router to the victim. The drawback with this scheme is that the router is dependent on the underlying protocol to compute the distance from itself to the victim. This is a router overhead, which considerably slows down the packet marking.

*2.2. Packet Logging Schemes*

Alex C. Snoeren et al. [6] developed a hash-based technique for IP traceback that generates audit trails for traffic within the network. Source Path Isolation Engine (SPIE) is used to enable IP traceback, the ability to identify the single IP packet to be traced, its destination, and an approximate time of receipt. Tracing individual packets have required prohibitive amounts of memory. The major drawback of this method is that they put a heavy burden on routers by requiring them to log information about every forwarded packet. Moreover, there is a need to download and search all this information looking for specific packet footprints, which results in a tedious and an unnecessary process.

Goodrich [7] proposed DPM is light, secure, scalable, and suitable for many types of attacks. Another modification to the basic approach will be aiming to address the fact that an IP source address can be changed by the attacker during the attack. Though the marks in DPM cannot be spoofed, frequent spoofing/changes of the source address with a different value by an attacker may void the DPM’s effectiveness. This problem can be solved by making the destination rely only on the marks, which cannot be spoofed. By using a globally known hash function, the destination can verify that the two halves of the ingress address, received in the marks, do indeed belong to the same ingress address without relying on the source address of the packet. This solution will require sending additional marks with hash values, and will somewhat raise the expected number of packets needed for reconstruction of the ingress address

*2.3. Packet Marking Schemes*

Unlike packet logging scheme, in packet marking scheme, routers do not record packets digests, but note their ID information into IP header. When the victim gets sufficient packets, it can reconstruct the full attack path. Savage et al. [8] proposed the classic probabilistic packet marking (PPM) method. PPM makes use of the Identification field as the marking space and stores the link information. It divides the IP address into eight fragments block of 4 bits each. This IP address fragment and the same offset fragment of the next router compose the edge fragment with 8 bits. The offset flag needs 3 bits for eight fragments block, and the last 5 bits are sufficient to show the hop number. It is reported that few packets exceed 25 hops in the forwarding network when a router decides to mark a packet, it selects an arbitrary fragment of its IP address, and records the fragment offset with the distance field set to 0. The benefit of PPM is that it desires no storage overhead for each router. But the weaknesses are also noticeable. The victim requires a large number of packets to reconstruct the attack path, and PPM does not have the ability to trace a single packet.Burch and Cheswick [9] introduce the concept of network traceback. They identify attack paths by selectively flooding network links and monitoring the changes caused in the attack traffic. This approach requires substantial network resources to send the additional packets for high bandwidth network links, which does not satisfy our requirement for low overhead on the victim. The victim uses the information in the marked packets to trace an attack back to its source. This approach has not been previously explored in any depth, but has many potential advantages. It does not require interactive cooperation with ISPs and therefore avoids the high management overhead of input debugging. Unlike controlled flooding, it does not require significant additional network traffic and can potentially be used to track multiple attacks.

*2.4. Network Address Translation and Port Address Translation (NAT/PAT)*

Network address translation is a feature by which IP addresses are mapped from one group to another. When the address mapping is N-to-N, it is called static network address translation. When the mapping is M-to-N it is called dynamic network address translation. Network address, port translation is an extension to basic NAT, in that many network address and their TCP/UDP ports are translated to a single network address and its TCP/UDP ports. The advantage of NAT is that real servers can run any operating system that supports TCP/UDP protocol. NAT can meet the performance request of many servers.

Xie et al. presented a model of network reachability in their seminal work [10], however they give no algorithms for computing reachability (and of course no experimental results). Xie *et al.*'s network reachability model does not address IP tunneling, dynamic NAT, and PAT and does not consider whether transport layer protocols are connectionless or connection-oriented. Furthermore, Xie et al.'s model is limited to describing the networks where each subnet connects to only one router because they model a network as a graph over only routers.

T. Korkmaz et al. [11] suggested that the design of the IP protocol makes it difficult to reliably identify the originator of an IP packet. Even in the absence of any deliberate attempt to disguise a packet's origin, wide-spread packet forwarding techniques such as NAT and encapsulation may obscure the packet's true source. Techniques have been developed to determine the source of large packet flows, but, to date, no system has been presented to track individual packets in an efficient, scalable fashion.

## 3. Proposed Method

### *3.1. Novel Nat/Pat Packet Marking (NNPM)*

Along with packet marking TTL based technique called Novel NAT/PAT packet marking (NNPM) is proposed to detect the real source of attack packets in the network. This method not only identifies the real source of attack but also detects the DoS attack.NNPM accurately verifies the key matching process, path reconstruction process and aiming to control the attack traffic.

The contribution of this approach is (1) to verify whether the packets are from the correct source by checking the key marking and TTL value; (2) to reduce the storage overhead at routers and (3) to reduce the access time requirement for recording packets by a factor of the number of neighboring routers.

### *3.2. Utilization of IP Header*

NNPM is based on IPv4. Possible IPv6 implementation of NNPM will involve adding an extension header in IPv6 packets, which is different with the IPv4 design.The TTL field is an 8-bit field in the IP header is used for marking. Time to Live (TTL) value depicts the life of the packet on a network in terms of hops. It is known that every router decrements the TTL value (TTL value=Path length) of the packet before forwarding the packet to the next router.

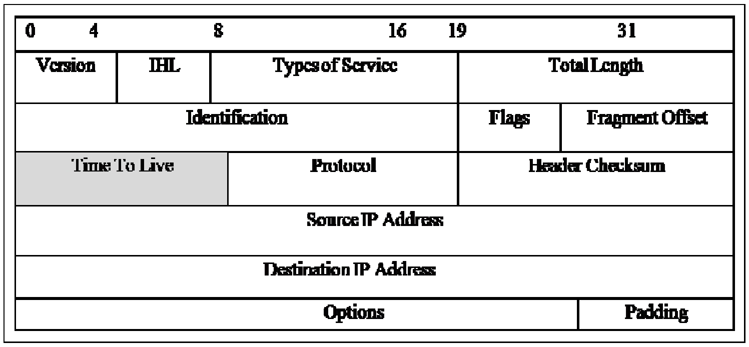

<table>
<tr><td>0</td><td>4</td><td>8</td><td>16</td><td>19</td><td>31</td></tr>
<tr><td>Version</td><td>IHL</td><td colspan="2">Types of Service</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="4">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time To Live</td><td colspan="2">Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="6">Source IP Address</td></tr>
<tr><td colspan="6">Destination IP Address</td></tr>
<tr><td colspan="5">Options</td><td>Padding</td></tr>
</table>

*Figure 1: The IP header field (darkened) utilized in NNPM*

### *3.3. Block Diagram for Detection of Real Source Attack*

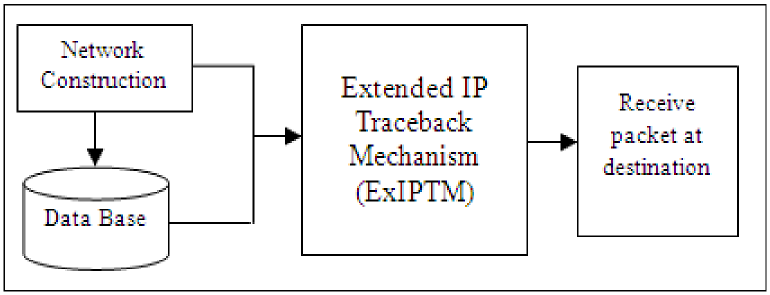

Network Construction
Data Base
Extended IP Traceback Mechanism (ExIPTM)
Receive packet at destination

*Figure 2: Detection of attack under DoS*

Here the path selection is based on open shortest path and the network construction and the node details are stored in the database. Thus the first step in the proposed methodology is to construct the network with intermediate nodes. Then get the value for n where 'n' is the distance and assign the 'n' value as TTL value i.e. Path length. In order to detect the attacker the entry of all users and their details are stored in the database.The details also contain the information about the users with their corresponding IP address, port address and user id. Routing values (i.e.) the distance between each node is displayed in the routing table and the user list are stored in the database. With the help of this database the destination node can easily determine the correct source.

That is, if the entry of the user is found in the database means, they are considered to be a trusted source. Otherwise, they are considered to be an attacked source.

### *3.4. Packet Marking and Path Reconstruction*

The network consists of nodes interconnected to each other. The Source node can be selected according to the user's choice. Every intermediate node between the source and destination acts as a router. Packet is marked at the router by giving sample message. Packet marking is nothing but in each router along the path the packet is marked by applying the packet marking algorithm and its information is stored and sent to the neighboring nodes.This mark is a unique identifier corresponding to this particular router. As a result the victim can determine all the intermediate hops for each packet by observing the inserted marks. In this process the key challenge is to reduce the number of packets that are involved in the traceback of these attacks. Once the transmission starts, the source node starts sending the packets to the destination node.The generated packet is passed through NAT/PAT transaction where it extracts the packet information. The source will then request the query to the destination and the destination verifies whether the packet is from a trusted source by checking the key marking and TTL value and finally forwards the result for the query. Once the verification is true, the packet will reach the correct destination, while after reaching the destination the packet is checked whether it is attacked or not.However, if any attack is found or the attacker may enter into the network with the help of some other router the destination will request for path reconstruction. Path reconstruction is a process of finding the new path for the same source and destination in which no attack can be made.

### *3.5. Flow Chart*

The diagrammatic representation of the flow of the Extended IP Traceback mechanism is given as a flowchart below:

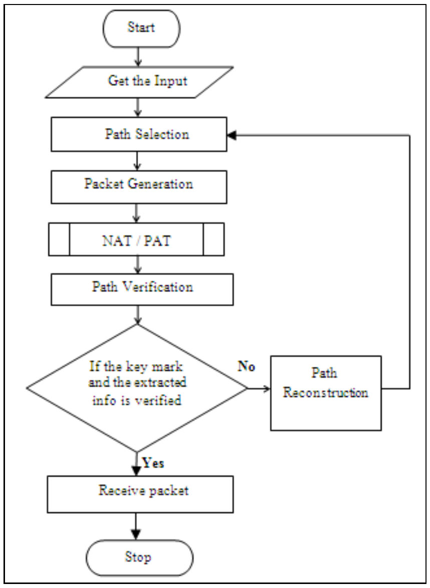


*Figure 3: Process flow of the proposed method*

Get the input (i.e.) choose the source and destination node. Then the message is marked on the packet. The packet is generated and traceback the flow of the packet. If find NAT & PAT transaction and if valid IP and Port address is present forward the packet to next hop, then TTL value will be decremented and the packet reaches the correct destination. Otherwise, if any attack is found the destination will request for path reconstruction and alternate path is determined.Then the packet is selected and passed through NAT/PAT transaction where the source will request and forward the input query and the result for the query is obtained at the destination. Thus, this method provides a better solution to trace back the real source of attack and identifies the attacker efficiently based on Novel NAT/PAT packet marking (NNPM) and TTL value.

### *3.6. Novel Nat/Pat Packet Marking (NNPM) algorithm*

- STEP 1: Construct the network using intermediate nodes.
- STEP 2: Select the Source and Destination node in the network.
- STEP 3: Make the marking in the packet during transmission.
- STEP 4: Verify whether NAT/PAT transaction has been taken place.
- STEP 5: Packet is forwarded.
- STEP 6: for packet with valid IP address and port number
- STEP 7: Next hop takes place.
- STEP 8: Decrement the TTL value immediately after hop.
- STEP 9: If the IP address differs
- STEP 10: Decrement the TTL value immediately without reaching destination.
- STEP 11: If found same IP address and Key marking

- STEP 12: Verify with NAT/PAT transaction
- STEP 13: Receive the packet at the correct destination.
- STEP 14: End

## 4. Result and Evaluation

The Extended IP Traceback Mechanism (ExIPTM) is implemented using JavaNetbean and the reconstruction of path in this scheme is perceptibly quicker than that in MRT and MORE. In ExIPTM, the marks in packets do not increase their size; therefore, no additional bandwidth is consumed.Moreover, with the overload prevention capability, ExIPTM can maintain the traceback process when the router is heavily loaded, whereas most current traceback schemes do not have this overload prevention capability.This section shows that the number of attack packets required to identify the attack sources .The Convergence time and Computational overhead on marking are analyzed as follows:

### *4.1. Number of Attack Packets Required to Identify the Attacker*

An Effective Detection of Real source attack using IP Traceback mechanism (ExIPTM) is substantially less than that required by PPM. The objective is to find a bound on the minimum number of packets that has to be received by the victim such that every router on the path from attacker to victim is involved in marking at least one of these packets with high confidence probability u. Let y represent this lower bound. Let the marking probability at router R be q. Let Pf be the probability that R fails to mark any packet out of the y packets. Clearly, $P_f = (1\text{-}q)^{\,y}$: Therefore, the probability that R will succeed in marking at least one packet is given by:

$$P_s=1-P_f=1-(1-q)^y \qquad (4.1.1)$$

The probability marking in packet for the proposed method (NNPM) is:

$$\text{Pmark} \qquad = \frac{Cp}{Tp} \qquad (4.1.2)$$

Here,
$C_p$= Current packets in transmission
$T_p$= Total number of packets

### *4.2. Traceback Process Overhead*

During the traceback process, the total number of the digest tables examined is an index reflecting the overhead on the traceback server and the speed of the traceback process. Suppose time synchronization is maintained between adjacent routers, and each router has n neighbors on average. Then, during the traceback process, the ratio of the number of digest tables examined in the hybrid approach to that in the hash-based approach is between n/2 and 1 /2 , depending on the average link latency between routers.The mathematical deduction under is based on average values of parameters and omits small value constants. Suppose each router has n (n >= 2) neighbor routers on average, and the traffic load at the router is from each neighbors equally. Let the average time interval covered by one digest table in the hash-base approach be $t_h$, and the average time interval covered by one digest table in the hybrid approach be $t_c$. The average time interval for adding TTL value $t_v$ is:

$$t_c = t_v + t_h \times n \qquad (4.2.1)$$

Suppose the attack path is m hops long from the attacker to the victim. Let the average link latency between routers be l. If the average link latency between routers is larger than the average time interval covered by one digest table, multiple digest tables covering continuous time periods at one router or one interface will be examined during the traceback process. Suppose the average time interval covered by one digest table is t, then l/t tables need to be examined in order to locate the digest of attack packet. In the hash-based approach, in order to move one hop upstream along the attack path from the current router during the traceback process, the digest tables at n neighbor routers need to be examined (actually n -1, omit that constant for simplicity). The number of digest tables and the average time interval for TTL value ($t_v$) examined is:

$$N_h = m \times n \times [l/t_h] =[\, m \times n \times [l\times n]/t_c\, ] + t_v \qquad (4.2.2)$$

In this method, in order to move from the current router which marked attack packet to the upstream marking router which is 2 hops away, the digest tables at all interface of n neighbor routers need to be examined, there are $n^2$ interfaces totally $(n\text{ -}1)^2$. The number of digest tables examined is:

$$N_c = m/2 \times n^2 \times [\frac{l}{tc}] \qquad (4.2.3)$$

Hence the ratio of the number of digest tables examined in the hybrid approach to that in the hash-based approach during the traceback process is:

$$r = \frac{Nc}{Nh} = \frac{n}{2} \times [\frac{l}{tc}] \qquad (4.2.4)$$

$$[\frac{l}{th}]$$

Here l/tc, where $t_c$ value is calculated based on the new added TTL value ($t_v$).
Parameters for evaluation of various traceback approaches include the following:

- Convergence time (i.e.) the number of packets needed to reconstruct the full attack path and estimated time taken by the routers to do so.
- The estimated time for marking by every router (i.e.) the computational overhead in a router due to marking.
- Storage overhead in a router due to logging.
- Robustness of the traceback mechanism.
- Average size of the marking information.

The first two parameters determine the fastness in response to the attack and reducing its strength. The third parameter represents the amount memory required at the routers as a result of logging while marking. The last two parameters depict the false positive rate and sufficiency of the marking field on average case of the proposed method.For the qualitative analysis, use the following notations.

$(CT)_{sys}$ - convergence time for the given system 'sys'
p - probability of marking
d - length of the attack path
EMS - Edge Marking Scheme
AMS - Advanced Marking Scheme
DLLT - Distributed Link List Traceback
PPPM - Pipelined Probabilistic Packet Marking
MDADF - Marking-based Detection And Filtering
Huff - Huffman Code for marking

### 4.3. Convergence Time Analysis

Convergence time is the time taken to reconstruct the attack graph. Given the packets marked by PPM, it is important to know the number of packets needed and time taken to find the IP addresses of all the routers along the attack path. The purpose of reconstruction is to determine the address of the host involved in attack or at least the address of the edge router nearest to the attacking host. Approximately the time taken by a packet in the Novel NAT/PAT Packet marking (NNPM) to traverse from one node to another node (T) is 2 ns.Hence the path constructed from source to destination through ($D_n$) no of times and the value is calculated by,

$$E_t = \frac{T \times D_n}{T_p} \qquad (4.3.1)$$

Here,

- $E_t$ ---->Averege Estimated time.
- T----->Time taken by a packet.
- $D_n$--->The path distance through which packet is transmitted from source to destination.
- $T_p$--->Total number of packets in transmission.

It is necessary to verify that the path reconstructed is correct and complete. But it has been found that none of the PPM approaches provide a mechanism to verify the completeness of the reconstructed path. To verify, a large number of packets need to be collected. This method compared the convergence time required by various traceback approaches and presented below.

The Edge Marking scheme by Savage et.al. uses the edges sampled in the marked packets to construct the path of attack. Here the probability of receiving marked packets from the furthest routers is smaller than the routers nearer to the victim and hence the time to receive the samples from the furthest router is given by $1/p\,(1-p)^{d-1}$ for a router which is'd' hops away.

The factor ln (d) accounts for the small probability for the marked packets from furthest router than the nearer ones. Thus the number of packets needed to reconstruct the attack path of length'd' is given by,

$$(CT)_{EMS} < \frac{\ln(d)}{p\,(1-p)^{d-1}} \qquad (4.3.2)$$

For the DLLT and PPPM u is a parameter that helps in choosing the success probability of routers (i.e.) p(x-d) ≥ u, where x is a random variable that represents the number of routers out of'd' that succeeded in marking.

$$(CT)_{DLLT} \geq \frac{\log_{10}(1-u^{1/d})}{\log_{10}(1-p)} \qquad (4.3.3)$$

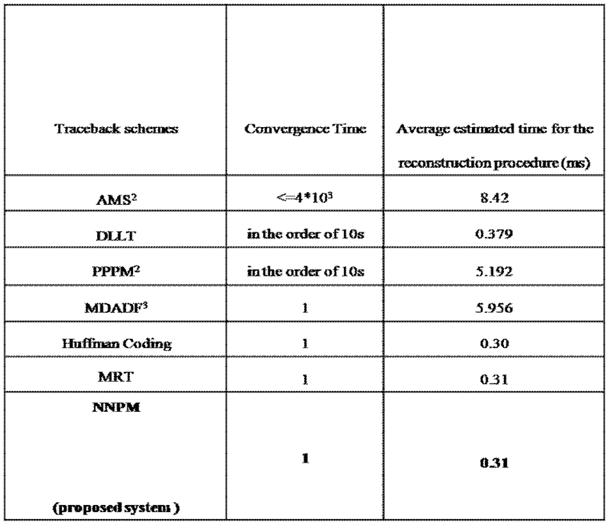
$$(CT)_{PPPM} \geq \frac{\log_{10}(1-u^{1/d})}{\log_{10}(1-p\,(1-p)^{d-1})} \qquad (4.3.4)$$

For the schemes in Detecting and preventing IP- Spoofed distributed DoS attacks and A Marking Scheme using Huffman Codes for IP Traceback, the convergence time is:

$$(CT)_{MDADF} = (CT)_{Huff} = 1 \qquad (4.3.5)$$

Since the above two schemes are of DPM in nature, they require one packet to traceback to the true source of the attack. The convergence time for the NNPM method is:

$$(CT)_{NNPM} = 1 \quad (4.3.6)$$



| Traceback schemes | Convergence Time | Average estimated time for the reconstruction procedure (ms) |
|---|---|---|
| AMS[2] | <=4*10[3] | 8.42 |
| DLLT | in the order of 10s | 0.379 |
| PPPM[2] | in the order of 10s | 5.192 |
| MDADF[3] | 1 | 5.956 |
| Huffman Coding | 1 | 0.30 |
| MRT | 1 | 0.31 |
| NNPM<br>(proposed system) | 1 | 0.31 |

*Table 1: Average estimated time for reconstruction*

The estimated time for reconstruction is represented in a graph as shown below:

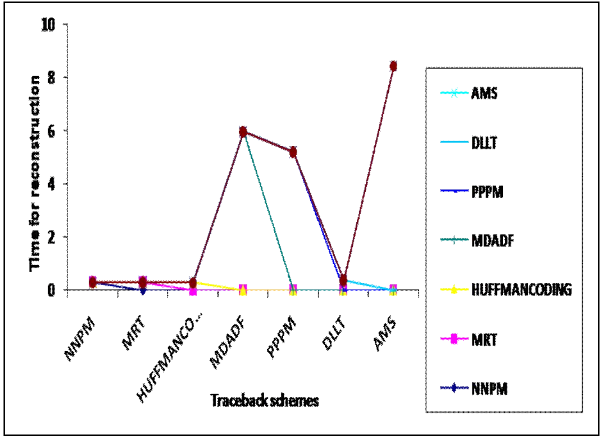


*Figure 4: Average Estimated time for reconstruction*

This shows that, when compared with PPM approaches, the proposed system has less time to converge. But the estimated time needed for marking and reconstruction procedure is small in this system.

### 4.4. Computational Overhead on Marking

This parameter defines the estimated time needed for marking by the routers along the path towards the destination.The path reconstruction is determined using number of packets of varying lengths. The result shows that NNPM (Novel NAT/PAT packet marking) reconstruct the path efficiently, irrespective of number of packets in transmission. Existing method likes Modulo / Reverse modulo Technique (MRT) and Hybrid IP Traceback (HIT) can reconstruct only few number of packets.

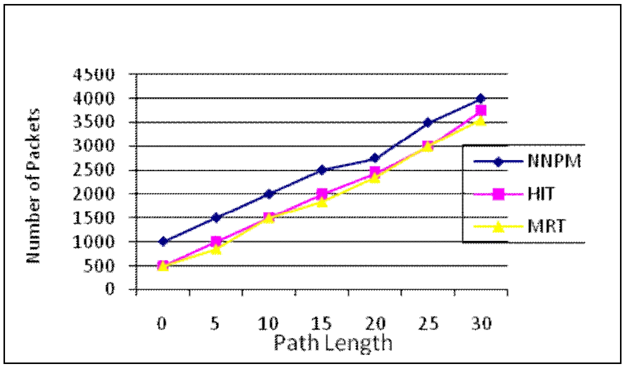


*Figure 5: Number of Packets needed to reconstruct the path of varying length*

## 5. Conclusion and Future Work

The Extended IP Traceback Mechanism (ExIPTM) efficiently detects the real source of attack and traces the path of an IP packet to its origin. The new NAT/ PAT method is implemented to verify the key matching process. It finds the attack node and applies the path reconstruction process. This method possesses several advantageous features such as easy traversing to the attacker and improves the efficiency of tracing the attacker system.Tracing a single IP packet back to its origin is the ultimate goal of IP traceback. The Extended Traceback mechanism presented here is capable of tracing any type of DoS attack during transmission irrespective of number of packets. It can even trace beyond the corporate firewalls which is a challenge faced by most of the existing traceback techniques. Since the attacker is detected earlier before reaching the destination, this method provide more reliable network and enhance the performance of the network.

The proposed system works well when none of the routers participating in the scheme are compromised, the authenticity of the markings cannot be verified in case a router itself is participating in the DoS attack. An authentication mechanism needs to be introduced into this scheme to make it more robust against compromised routers.However the proposed method is not a complete solution against DoS attacks. It needs to be used in conjunction with other filtering mechanisms to give better solution. It can be enhanced from single autonomous server to multiple autonomous servers. In future real time IP traceback mechanism which uses a 16-bit marking field is developed and identified within the network and also implement this proposed method on large scale i.e. actual internet to detect multiple attacks.

## 6. References.

1. Ming-Hour Yang and Ming-Chien Yang, “RIHT: A Novel Hybrid IP Traceback Scheme”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012.
2. M.D.D. Moreira, R. P. Laufer, N. C. Fernandes and O. C. M. B. Duarte, “A Stateless Traceback Technique for Identifying the Origin of Attacks from a Single Packet,”, ICC 2011, pp. 1-6, June 2011.
3. Yan Fen, Zhu Hui , Chen Shuang-shuang , Yin Xin-chun “A Lightweight IP Traceback Scheme Depending on TTL” International Workshop on Information and Electronics Engineering (IWIEE), 2012.
4. S. Malliga and A. Tamilarasi, “A hybrid scheme using packet marking and logging for IP traceback,” Int. J.Internet Protocol Technol., vol. 5 no. 1/2, pp. 81–91,Apr. 2010.
5. William Stallings, Network security Essentials Applications and standards, Fourth Edition, Pearson Education.
6. A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, B. Schwartz, S. T. Kent, and W. T. Strayer, “Single-packet IP traceback,” IEEE/ACM Trans. Networking, vol. 10, no. 6, pp. 721–734, Dec. 2002.
7. M.T.Goodrich (2002), “Efficient Packet Marking for Large-Scale IP Trace back, ”Proc. Ninth ACM Conf.Computer and Comm. Security (CCS ’02), pp.117-126,2002.
8. S. Savage, D. Wetherall, A. Karlin, and T. Anderson, “Practical network support for IP traceback,” in Proc. ACM SIGCOMM2000, Stockholm, Sweden, Aug. 2000, pp. 295–306.
9. H. Burch and B. Cheswick, “Tracing anonymous packets to their approximate source,” Proceedings of 2000 USENIX LISA Conference, pp. 319-327, Dec 2000.
10. G. G. Xie, J.Zhan, D.A.Maltz, H. Zhang, A.Greenberg, G. Hjalmtysson, and J. Rexford, “On static reachability analysis of IP networks,” Proc. IEEE INFOCOM, vol. 3, pp. 2170–2183, Mar. 2005.
11. T. Korkmaz, C. Gong, K. Sarac, and S. G. Dykes, “Single packet IP traceback in AS-level partial deployment scenario,” Int.J. Security Networks, vol.2, no. 1/2, pp. 95–108, 2007.
12. T. Peng, C.Leckie, and K. Ramamohanarao, “Adjusted probabilistic packet marking for IP traceback,” in Networking 2002, Pisa,Italy,May2002,pp. 697–708.