UDP based IP Traceback for Flooding DDoS Attack

Vijayalakshmi Murugesan amd MercyShalinie Selvaraj
Department of Computer Science and Engineering, Thiagarajar College of Engineering, India

Abstract: *Distributed denial of service attack has become a challenging threat in today's Internet. The adversaries often use spoofed IP addresses, which in turn makes the defense process very difficult. The sophistication of the attack is increasing due to the difficulty in tracing back the origin of attack. The researchers have contributed many traceback schemes to find out the origin of such attacks. In the majority of the existing methods they either mark the packets or log the hash digest of the packets at the routers in the attack path, which is computational and storage intensive. The proposed IP trace back scheme is an User Datagram Protocolbased (UDP) approach using packet marking which requires computation and storage only at the edge router and victim and hence it does not overload the intermediate routers in the attack path. Unlike existing traceback schemes which requires numerous packets to traceback an attacker, the proposed scheme requires only a single trace information marked packet to identify an attacker. It supports incremental deployment which is a desirable characteristic of a practical traceback scheme. The work was simulated with real time Internet dataset from the* Cooperative Association for Internet Data Analysis (*CAIDA) and found that the storage requirement at the victim is less than 1.2 MB which is nearly 3413 times lesser than the existing related packet marking method. It was also implemented in real time in the experimental DDoS Test Bed the efficacy of the system was evaluated.*

Keywords: *DDoS, Mitigaton, IP Traceback, Packet Marking, Packet logging, Forensics*.

Received May 30, 2014; accepted October 26, 2014

1. Introduction

The Distributed Denial of Service (DDoS) attack is becoming a serious problem with every going day [14]. Major Internet players like CNN, Microsoft, Amazon, Yahoo and eBay are included in the list of DDoS victims. According to the numerous surveys on DDoS attack conducted by Arbor Networks [3], the likelihood of being attacked anonymously is increasing. Denial of service attack is an attempt to affect the availability of resource or network by consuming the limited resources or exploiting the weakness in an application. DDoS attacks can be categorized into flooding attack and software exploit attack based on the amount of attack packets used. In case of flooding attack, the attacker pumps in huge volume of attack traffic to exhaust the server resource and bandwidth. Software exploit attack distress the server by exploiting the vulnerabilities using a few packets.

Most of these DDoS attacks are from anonymous sources or spoofed sources hiding the original identity of the attacker which makes the mitigation of attack and the accountability of the attacker very difficult. Therefore, tracing the attack back to their origin is required to mitigate their adversary effects on the victim host. IP trace back is a technique to identify the attacker who uses spoofed IP address. Lot of researchers has proposed various traceback techniques to identify the origin of flooding based attack and software exploit attack. The traceback scheme applied to trace a flooding based attack is generally dependant on more than one packet [4, 5, 6, 11, 16, 20, 21, 23] and hence the process of reconstructing an IP address is becoming arduous. Consequently IP address reconstruction time is also increased which will in turn delay the mitigation measure.

Later single packet IP traceback schemes [10, 17, 22] were proposed which could trace software exploit attack as well as flooding based attack with a single packet. However most of the single packet traceback requires storage at the routers in the attack path and this log is examined to locate the attacker. In spite of overloading the routers with the traceback aids such as logging or marking algorithm it also demands a heavy storage space at the routers which would in turn degrade the performance of routers.Hence this paper proposes storage free UDP based single packet (trace information marked) IP traceback technique to trace the flooding DDoS attack. The contribution of the paper can be summarized as

- A novel IP traceback scheme is proposed which
  - Incurs no storage or computation overhead at the intermediate routers.
  - Requires minimal computation and storage at the victim.
  - Can be incrementally deployed.
  - Can handle major DDoS attack.
- The proposed system was simulated and analyzed using real world the Cooperative Association for Internet Data Analysis (CAIDA) skitter dataset [7] and implemented in the experimental DDoS test

bed using Click Modular Router (CMR) [8] and it was compared with the existing traceback schemes.

The remainder of this paper is organized as follows: sections 2 discuss on the related work on IP Trace back. The proposed IP traceback technique is detailed in section 3. Section 4 describes the experimental setup, results and analysis. Section 5 draws the conclusion of the entire paper.

2. Related Work

Belenky and Ansari [4, 5] proposes a deterministic packet marking scheme where they utilize the identification field in the IP header to mark the IP address of the border router. Since a 32 bit IP address cannot be marked in a single packet, they fragment it and mark in several packets randomly and in the victim end they reconstruct the IP address from the collection of packets. Xiang *et al*. [24] proposed a flexible mark length strategy which marks either using 16 bits or 19 bits or 24 bits of the IP header. The marking is done based on the usage of IP header fields. They also proposed a flow based marking scheme which is based on random early detection algorithm. These deterministic packet marking approaches can only identify the border router and not the attack path. However it is adequate to filter the attack traffic near the source. Probabilistic packet marking method [2, 11, 16, 21] marked the packets probabilistically and reduced the per packet overhead but this increased the number of packets required to construct the attack path. All these marking algorithms utilize the 16 bit identification field of the IP header overriding its conventional purpose and since the mark information cannot be stored in a single packet, they segment the mark information and store in many packets. Consequently reconstruction procedure becomes long and single packet IP traceback is not possible with these methods.

Various logging based trace back schemes [12, 13, 18] were proposed based on the first initiative for single packet traceback [17]. In such schemes the hash digest of the packets is stored in a log table at the routers. When the trace back request is issued the log table is looked up and the attacker is identified. Though logging based trace back schemes can trace back even with a single packet they incur prohibitive storage and processing cost at each intermediate router in the attack path affecting the performance of routers. Hybrid traceback schemes [1, 10, 22] reduce the storage overhead to a certain extent by deploying marking as well as logging but it still requires every router to process every packet and the storage overhead still prevails. Incremental deployment is also not possible in any of this single packet traceback schemes.

Internet Engineering Task Force (IETF) has proposed ICMP based traceback as a traceback solution [6] and recently Saurabh and Sairam [15]. has proposed a ICMP based solution to trace reflector attacks But still they have practical difficulties such as it requires support from most of the intermediate routers to construct the attack path and reach the attacker. There is no guarantee that ICMP message packet will take the same route as the attack packet. Most of the routers block the ICMP packets. Unlike the existing approaches, the proposed UDP based IP Traceback Technique (UIT) identifies the ingress router with a single UDP packet. It uses a light weight deterministic packet marking only to store the index without affecting the fragmented packets. It does not require prior knowledge of the topology. It can be incrementally deployed. Most of the existing deterministic techniques[4, 5, 24] require more than one packet to reconstruct the IP address of the attacker's edge router but the proposed technique can traceback each attacker with their respective single packet.

3. Proposed IP Traceback Scheme

The ultimate aim of any IP traceback scheme is to find out the origin of an attack, so that it could be filtered at the place of orgin itself to save the network resources. The proposed UIT is a deterministic packet marking based technique which can identify the ingress router of an attack path. Marking is done only at the edge router and not in any of the intermediate routers. The overview of the proposed IP traceback system is shown in Figure 1. The incoming traffic is monitored at the edge router by the Flow Monitor (FM) to check if it's a normal flow. If it is suspected as an attack flow then it is updated in the Suspicious flow List (SL) and an alert is given to the UDP generator. The UDP generator fetches the data from the SL and generates an UDP packet to the destination about the ingress router.

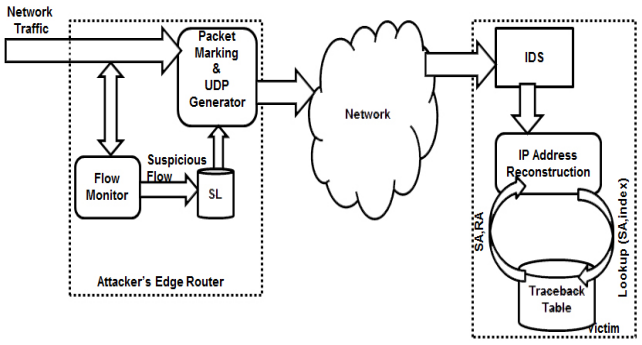

Figure 1. Overview of proposed IP traceback scheme.

Packet marking is performed in all the packets to indicate if the packet forwarded has a corresponding UDP packet generated to the victim. At the victim when an IDS detects an attack the IP address of the attacker's edge router is reconstructed with the help of the traceback table populated with the UDP packets. The reconstruction of IP address is done in the victim

itself. As in the many of the existing approaches the intermediate routers are not burdened in reconstruction of IP address. Each of the components in the proposed framework are detailed in the below section.

3.1. Flow Monitor

The proposed traceback system sends an UDP packet containing the ingress router IP address to the victim. Instead of increasing the computation cost by sending an UDP packet with a fixed probability of packets that the router forwards, it is sent conditionally. An UDP packet is sent only if a packet is considered as suspicious by the FM. The objective of the FM is to observe the traffic passing through the router and update the Suspicious List (SL) with the high rate flows. A flow is represented by $f_i = < s_j, d_k >, i = 1,2,....,n, s_j \in S \text{ and } d_k \in D$, where S is a set of source IP addresses of the packets passing through the edge router and D is a set of destination IP addresses of the packets passing through the edge router. The flow with packet rate above the harmonic mean is updated in the SL.

Harmonic mean is chosen over the other central measures because it is always lesser than arithmetic mean and geometric mean. By choosing the lowest mean, it is ensured that no suspicious flow escape the trace back process. The algorithm used by the FM is shown in Algorithm 1. The traffic flow is observed for a specific time period. After identifying the flows, the packet count in each of the flows is extracted and the harmonic mean is calculated. The flows with the packet rate above the harmonic mean is considered as a suspicious flow and updated to the SL.

Algorithm 1:FlowMonitor (Network Traffic)

```
# s_i is the source IP address of the packet
# d_i is the destination IP address of the packet
#F is the set of flows f_i
#x_i be the number of packets transmitted in flow f_i
identify flows( )
While (true)
{
        While(Δt expires)
        {
          foreach (flow f_i in F)
          {
            calculate packet count (f_i)
          }
          H = n.( Σ_{i=1}^{n} 1/x_i )^{-1}
          foreach (flow f_i in F)
          {
            if ( x_i > H)
            {
            Update Suspicious List (s_i , d_i )
            }
          }
        }
}
```

This SL may contain false positives. Normal flows having the packet rate above the harmonic mean will also be updated in the SL. Since the objective of the SL is to facilitate the traceback of suspicious packets and not to detect the attack, these false positives will not harm the trace back process. In fact, it will minimize the attack packets getting escaped.

3.2. Packet Marking and UDP Generator

Once the FM updates the SL, an UDP packet is generated to the victim and packet is marked accordingly. The process of inscribing the router IP address or partial path information in the rarely used fields of the IP header is called as packet marking. Most of the existing packet marking/hybrid techniques [1, 2, 4, 5, 10, 11, 16, 22, 24] overload the identification field of an IP header to send the path information ignoring its conventional usage by the fragmented traffic. The proposed technique avoids using the identification field so that the fragmented IP packets are not harmed. It is widely accepted in earlier traceback schemes to use reserved flag bit and the Type of Service (TOS) field [1, 11, 24] to mark the trace information. The proposed traceback scheme also uses the reserved one bit flag field and the TOS field for packet marking. The fields used in IP header is shown in Figure 2. The reserved bit is unused field and it's not yet dedicated to any functionality, hence marking in that one bit flag will not harm the existing infrastructure. The TOS has been rarely used in the past and few proposed standards on TOS [9] are still under development, hence overloading the TOS will not harm the existing infrastructure.

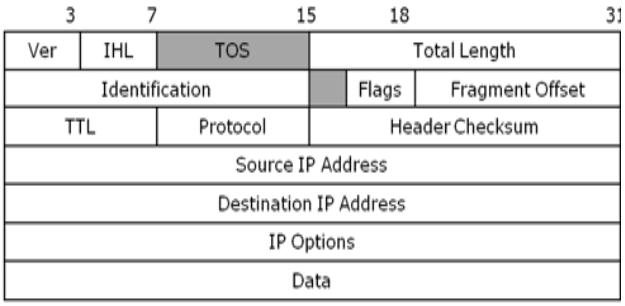

Figure 2. IP header field (darked area) used in marking.

Once a flow is updated to SL, an UDP packet is generated to victim. The UDP packet contains the source IP address, incoming interface address of the router and an index. Source IP address is the original host IP address, incoming interface is the router address and index is an 8 bit hash digest used to differentiate packets from different routers using the same source IP address due to spoofing. Figure 3 illustrates UDP generation and packet marking process. The algorithm used in marking and UDP generation is shown in Algorithm 2. The flow (from

source S1 to destination D1) is updated in the SL by the FM.

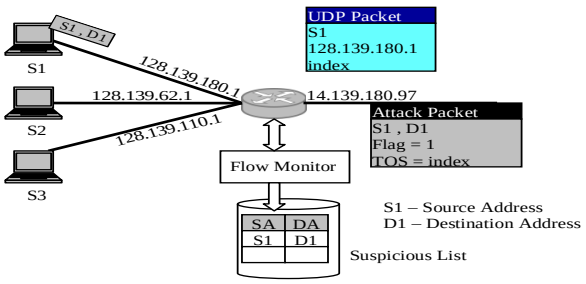

Figure 3. UDP packet generation.

An UDP packet will be created and sent with the details to the victim where 128.139.180.1 is the ingress interface address of the router and index is the hash digest which will also be marked in TOS field of each IP packet belonging to that flow. Hereafter, when packet belonging to that flow(from source S1 to destination D1) arrives at the router, the reserved flag of that packet will be marked as 1 (to indicate an UDP packet has been sent) and the hash digest (index) would be marked in the TOS field and the packet will be forwarded by the router. Reserved flag bit serves as a control bit.

Algorithm 2: PacketMarking(Packet P)

```
#SL is the suspicious list
#I is the incoming interface address
#S is the source IP address of the packet P
#D is the destination IP address of a packet P
for each (packet P)
{
      if (P.S== SL.S)
     {
        index=Hash(I);
        Send UDP Packet N(S, I, index) to
        Destination D's edge router periodically.
        P.ToS = index
        P.flags[0] = 1
      }
      else
     {
        P.flags[0] = 0
     }
}
Forward Packet P
```

It intimates whether an UDP message has been sent to victim for that corresponding IP packet or not. If an UDP message associated with that packet has been sent to the victim then the reserved flag bit will be marked with 1, else it will be marked with 0. The whole IP address is written in a single UDP packet eliminating the chaos in reordering the packets. Every packet passing out of the edge router is marked in the reserved flag bit.

Only the flow with heavy traffic is updated to suspicious list, and hence an UDP message is sent to the victim only about the details of packets belonging to that suspicious flow. This UDP traceback message is differentiated from other UDP packets by using dedicated unused UDP source and destination port.

The existing deterministic packet marking methods [4, 5, 24] fragment the IP address into several segments and mark the IP address of the edge router. Hence those methods take longer time to reconstruct the IP address. In the proposed method, IP address is stored in a single UDP packet. Consequently the packet reconstruction time and false positives are reduced.

3.3. IP Address Reconstruction

The forwarded UDP packets are identified as the UDP traceback messages since it will be collected by the victim at the dedicated port. The traceback table is populated with the UDP packets received from different edge routers. The table contains:
<Source IP address | In Interface|Index>

The source IP address is the original host source IP address, incoming interface is the attacker's edge router address and the index helps to differentiate hosts using the same source IP address due to spoofing.

It is assumed that an Intrusion Detection System (IDS) is running on the victim machine. When an IDS detects an attack, IP address reconstruction procedure is initiated. The IP address reconstruction is a simple technique involving very less computation. The victim checks the attack packet's reserved flag field, if it is marked '1' then there will be an entry in traceback table for that corresponding packet. The attacker edge router can be identified by looking into the traceback table with the source address found in the packet. By looking up the traceback table with the source address and index, the IP address of the edge router of an attacker can be retrieved. Due to spoofing if hosts from different network uses the same source address, it will cause confusion by returning two different edge router addresses. To circumvent this, hash digests and source address pair is searched in the traceback table which would return a single IP address. The algorithm is given in Algorithm 3.

Since the entire IP address is put in a single field of a single UDP packet, the IP address reconstruction involves only the search time in the traceback table and the false positives are greatly reduced. Since there is no segmentation of IP address or reorganization of IP address like the existing methods, the false positive is reduced and the number of packets required to reconstruct is only one. This traceback table is refreshed periodically to reduce the storage overhead at the router.

Algorithm 3: IPAddress_Reconstruction (Alert File A)

```
#S is the source IP addresses
#R is the attacker's edge  router address
#TTble is the traceback table
for each (packet P in A)
{
      if(P.flags[0]==1)
     {
        if((TTble.index==P.ToS)&&(TTble.S==P.S))
       {
          R=TTble.incoming interface
       }
     }
   }
   return R
```

4. Experimental Results and Analysis

4.1. Experimental Setup

The proposed work is simulated as well as implemented in real time. Most of the existing traceback techniques are either simulated or theoretically validated because of the restricted access to the routers. To understand the practical difficulties the proposed UDP based Traceback (UIT) was implemented in real system using CMR [8].CMR is a programmable router which would make a PC to function like a router and user logic could be added as elements. The topology that was implemented is shown in Figure.4.The victim was connected to a DDoS experimental test bed. The test bed interconnects the geographically distributed collaborative working nodes through MPLS-VPN cloud. The routers connecting the network were CMR. TCPDUMP [19] is used to capture the packets. The captured packets are further examined and processed to identify the IP address of the edge router. It was also simulated using the real Internet Skitter dataset from CAIDA [7]. Using the real time experiments, hosted on DDoS Experimental test bed, programmable routers and simulations using CAIDA, the potency of the system was evaluated in terms of computation, storage and accuracy.

Since the proposed method focuses on tracing flood attack with a single marked packet, the proposed system is analyzed and compared with traceback scheme which is capable of tracing back flood attack with a single packet as well as multiple packets. Since the proposed method marks deterministically, it is compared with DPM [4], a representative method of deterministic packet marking and since it can trace back with a single trace information marked packet it is compared with the state of art single packet IP traceback, HIT [10].It is also compared with ICMP based traceback [6] because it is considered as the most feasible traceback approach.

4.2. Packet Marking Overhead

The packet marking overhead is analyzed in terms of number of packet involved in marking and the marking bits overloaded in an IP header.

The proposed approach deterministically marks the status in every packet and conditionally marks the index value before it forwards but it does not involve any heavy computation for marking. It either marks 0 or 1 based on SL.A hash digest is marked only if a source address is found in the SL. The hash digest of the ingress router addresses are computed in advance and the respective hash digest is just copied into the UDP packet and the TOS field of the IP header. Hence heavy computation is avoided in the proposed method. Let n be the number of packets passing through a router r. Then the overall marking overhead in the proposed system is 'n'. The marking overhead in DPM is also 'n' whereas the marking overhead in HIT is $\left(\frac{h}{2}\right)n$ where h represents the total number of routers in the attack path. It requires marking at every alternative router in the attack path.

Table 1 summarizes marking overhead in terms of number of bits overloaded in an IP header in different traceback schemes.

Table 1. Summary of marking overhead.

	DPM	**HIT**	**UIT (Proposed)**
No. of bits used in IP header	17	16	9
Fields Used in IP header	Identification field – 16 bits	Identification field – 16 bits	TOS – 8 bits
	Reserved Flag – 1 bit		Reserved Flag – 1 bit

4.3. Reconstruction Time

The time taken to identify the attacker edge router is computed by deploying UIT and DPM in the implementation set up shown in Figure 4. Figure 5 depicts the reconstruction time in proposed UIT and DPM. It is found that the UIT scheme is faster compared to DPM. DPM requires the minimum of number of packets to trace back the attacker and it forms a table and identifies the attacker router from it. It is time consuming, whereas in UIT the reconstruction time is simply the search time in the pre built traceback table.

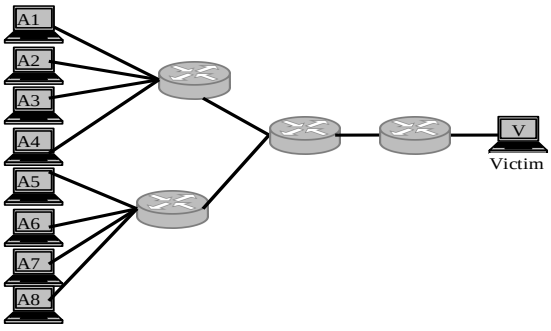

Figure 4. Implementation setup.

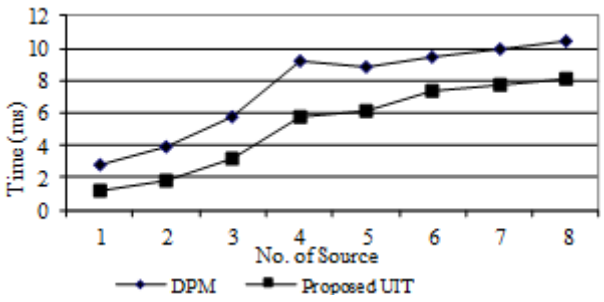

Figure. 5. IP address reconstruction time.

Likewise ICMP based traceback also takes longer time to identify the attacker as it is dependent on multiple packets. The reconstruction time in HIT will be obviously higher than the proposed scheme as it has to traverse back along the attack path to find the attacker.

4.4. Number of Packets Required to Traceback

The number of packets required to traceback is an important metric to analyze the efficiency of the trace back scheme. Most of the traceback scheme which concentrates on tracing flooding attacks requires more number of packets to reconstruct the attacker's edge router.

The expected number of packets to reconstruct the attack path in an ICMP based trace back is given by (1)

$$\frac{nH_n}{q} \tag{1}$$

Where, n is the number of attackers, q is the probability at which the ICMP packet is sent which is normally 1/20,000 and H_n is the nth harmonic number. DPM also requires more than one packet to traceback the attacker since a single ingress router address is stored in multiple packets. The expected number of packets to trace back an attacker in HIT is 1.

In the proposed UDP based traceback scheme single trace information marked packet is adequate to traceback an attacker. The IP packet can differentiate if the trace information is available in the traceback table or not by examining the reserved flag bit. If the flag bit is set 1 then it can traceback with that one packet itself else it has to wait for the packet which is marked 1.However before the IDS detects a flooding attack an IP packet which are marked 1 will reach the victim.

FM is used at the attacker edge router to minimize the marking overhead if that is eliminated then the proposed UDP based trace back scheme will mark each and every packet at the edge router which will enable the scheme to trace back every single packet received by the victim.

4.5. Number of Routers Required to Traceback

When the traceback scheme overloads the routers with additional task the primary functionality of the router will be degraded.

ICMP involves the routers only during the first phase and not in the traceback. In DPM and the proposed UIT only the victim is involved in the traceback process. It does not involve any routers for trace back, whereas the schemes which are able to traceback even a single attack packet (HIT and SPIE [17]) requires the support of routers and their neighbors in the attack path to find the attacker. The number of routers involved in the traceback process of HIT is given by (2)

$$(n-1)h/2 \tag{2}$$

Where (n-1) refers to the neighbors of each router in attack path excluding the downstream router and h denotes the number of hops. The number of routers involved in SPIE [17] is given by (3)

$$(n-1)h \tag{3}$$

According to CAIDA dataset [7] the average degree of a router (neighbours) is 3.8.Assuming n is 4 the number of routers involved in traceback of an attacker with different path length is shown in Figure 6.

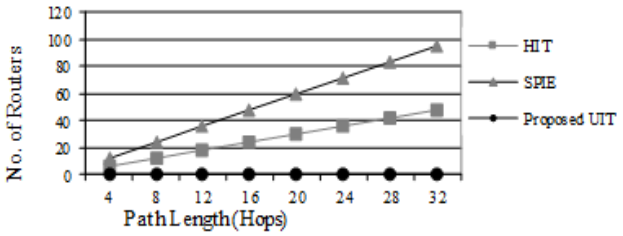

Figure 6. Number of routers involved in traceback.

It is evident from Figure 6 that both HIT and SPIE involves computational intensive trace back process and incurs overhead at routers as well as their neighbor routers in attack path even though it can trace back with a single packet, whereas the proposed scheme can identify the attacker from the victim itself without involving any router with a single trace information marked packet.

4.6. Storage Over Head

IP traceback scheme is considered as efficient if it does not cause additional storage overhead at the routers because overloading routers with additional storage and computation for each packet it forwards will decrease the throughput of the router.

Even though HIT is able to traceback with a single packet they require prohibitive storage at the routers in the attack path. Consider a router with b packets/unit time with memory efficiency factor r. The storage overhead of HIT at routers is given by (4)

$$S = P_l \times b \times \frac{1}{r} \tag{4}$$

P_l denotes the logging probability.ICMP based traceback, DPM and the proposed UIT needs storage

only at victim does not need additional storage at the routers.

In DPM several segments constitute a single border router IP address, so it requires 32 KB of storage at victim, 16 KB for RecTbl and 16KB for StatTbl for every new source address from which it receives the packet whereas the UDP based scheme requires only 72 bits for each flow.32 bit to store the host IP address and 32 bits to store the ingress router IP address and 8 bits to store the index value. It is illustrated in Figure 7.

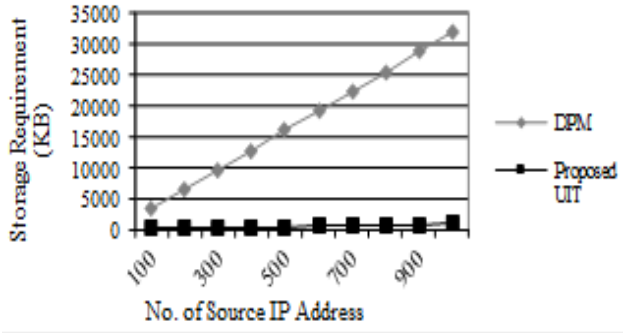

Figure 7. Storage requirement to identify the attackers.

To analyze the storage requirement the proposed UIT and DPM was simulated using CAIDA skitter dataset. It is a trace route dataset from a monitor of CAIDA to 131203 destinations. 186642 complete paths were found. It was assumed that the monitor was the victim and 131203 nodes were edge routers and each of these routers is directly connected to the attack host. Suppose the edge router of each of these 131203 nodes sends an UDP packet to the victim. Then the total size of the Traceback table at the victim will be less than 1.2 MB whereas DPM requires 4 GB of memory at the victim, 2 GB of storage for StatTbl and 2 GB for RecTbl. The storage requirement of DPM is nearly 3413 times higher than the proposed UIT.

4.7. Accuracy

The accuracy of the traceback scheme can be determined by analyzing the false positive and false negative. A false positive is the incorrectly identified source as an attacker. A false negative is incorrectly ignoring an attacker as legitimate user.

To test the accuracy an experiment was conducted in real network set up shown in Figure.4. Each of this attack host sent ‘n’ number of spoofed packets. By varying the number of packets depending on the number of different IP addresses the traceback was repeated to note the number of correctly identified source addresses. It is shown in Figure 8.

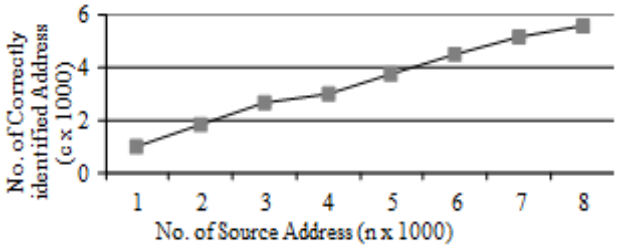

Figure 8. No. of source vs No. of correctly identified sources.

In the proposed scheme accuracy will be high if there is an entry in the traceback table for every attacker. To prove that every attacker has an entry in traceback table an experiment was conducted in the experimental DDoS test bed to analyze the normal and attack traffic characteristics with respect to the harmonic mean. In flooding attack huge volume of data is pumped in with the intention of exhausting the bandwidth or server resource. Hence the number of packets flowing through the attack traffic is always higher than the normal traffic. The harmonic mean of the traffic is computed for every time instance.Figure.9 shows that the attack rate is always above the harmonic mean. It shows the packet count in three different flows of which two of them are normal flows and one is an attack flow. It can be noted that the attack flow is always above the harmonic mean. By this way it ensures that the packets in the attack flow is always updated in the SL which leads to the corresponding UDP packet generation followed by traceback table updation. During the second and third epoch, normal flow 2 also falls above the harmonic mean, and the packet belonging to that flow is also updated to SL.So this harmonic mean cannot be used in detecting an attack but the objective of this FM is only to segregate potential attack traffic from normal traffic to reduce the marking overhead at the router and hence it does not affect the traceback process. It is evident from the graph that although normal flows are updated in SL occasionally, attack flows can never escape from the FM. Hence every attacker will have an entry in the traceback table.

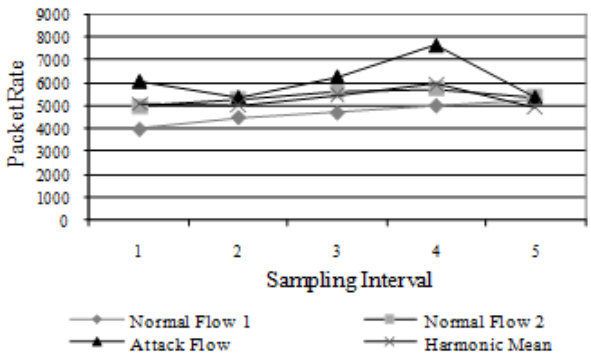

Figure 9. Comparison of normal packet rate and attack packet rate with respect to harmonic mean.

This scheme can produce inaccurate results in one of the following situations.

- UDP packet is lost on the way to victim and hence there is no entry in the Traceback table.
- Source address and index pair occur more than once in the victim's Traceback table.

As far as the first case is concerned this is a rare situation and even in that case if the first UDP packet is lost then the consequent UDP packet could be used to update the Traceback table. As far as the second case is concerned, the false positive will be zero when no two different hosts from different ingress router with same digest use the same source address or if no two ingress router shares the same digest. DPM matches only with the digests. The accuracy of UIT is higher than DPM because it not only matches the digest to identify the attacker it also matches an additional key, source IP address of the attack packet. Hence by that way false positive is reduced. HIT and ICMP also tend to provide higher false positive because it is dependent on multiple logs at multiple routers and multiple packets respectively.

4.8. Comparison with other Traceback Schemes

Table 2 compares the proposed traceback with the exiting approaches. As for partial deployment issues, it is not required to deploy the proposed method in each and every router spread across the network. It is enough if it is deployed only in the edge routers. So the ISP involvement is very low and hence allows incremental deployment. The number of hops taken by the packet to reach the victim also does not affect the traceback process as it is completed in the victim itself.

It is scalable, incrementally deployable and consumes negligible bandwidth in sending the notification packet. It requires very less storage at the victim and zero storage at the intermediate routers.

5. Conclusions and Future Work

A simple and practical UDP based trace back scheme is proposed. It requires zero storage at the core routers but still it retains the capability of tracing single trace information marked packet. Although ICMP is considered as a feasible approach it requires millions of packets to traceback 1000 attackers but in the proposed UIT single trace information marked packet is adequate to identify an attacker. It requires minimal storage (1.2 MB for CAIDA skitter dataset) at the victim to traceback the attacker which is nearly 3413 times lesser then the existing method. It does not burden the routers in the attack path with additional storage and computation as in the existing single packet traceback approaches. The traceback time is lesser than the existing approaches as it is not dependant on more number of packets or routers. The accuracy of the traceback is also higher compared to the existing approaches. It does not require prior knowledge about the topology of the network. It is incrementally deployable with lesser ISP involvement.

Few issues in the proposed system are not discussed in the paper and it will be handled in the future work. FM marks normal flow packets also occasionally, which can be narrowed down further by using a better algorithm. However by removing the FM, the proposed system can be used to trace back the software exploit attack as well. An efficient data structure can be used for Traceback table so that the reconstruction of IP address can be even faster.

Table 2. Comparison with existing traceback methods.

Traceback Method	Number of Packets needed to identify 1000 attackers	No. of bits overloaded in IP packet	Storage overhead at the routers	Storage overhead at the victim	Firewall Issues	Process Overhead at the intermediate routers in attack path
ICMP	138 million	0	NIL	HIGH	YES	HIGH
DPM	10000	17	NIL	HIGH	NO	NIL
HIT	1	16	HIGH	NIL	NO	HIGH
UIT (proposed)	1 trace information marked packet.	9	NIL	VERY LOW	NO	NIL

References

[1] Al-Duwairi B. and Govindarasu M., "Novel Hybrid Schemes Employing Packet Marking and Logging for IP Traceback, *IEEE Transactions on Parallel and Distributed Systems*, vol. 17, no. 5, pp. 403-418, 2006.

[2] Alenezi M. and Reed M., "Uniform DoS traceback," *Computers and Security*, vol. 45, pp. 17- 26, 2014.

[3] ArborNetworks, "DDoS Attacks and the Ostrich Mentality," http://www.arbornetworks.com, Last Visited 2017.

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

[5] Belenky A. and Ansari N., "On Deterministic Packet Marking," *Computer Networks*, vol. 51, no. 10, pp. 2677-2700, 2007.

[6] Bellovin SM. ICMP Traceback Messages. *Internet Draft: draft-bellovin-itrace-00.txt*, Last Visited 2000.

[7] CAIDA's Skitter Project CAIDA, http://www.caida.org/tools/measurement/skitter/ Last Visited 2017.

[8] Click Modular Router: www.read.cs.ucla.edu/click/click, Last Visited 2014.
[9] Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, *RFC2474*, Network Working Group, 1998, https://tools.ietf.org/html/rfc2474, Last Visited 2017.
[10] Gong C. and Sarac K., "A More Practical Approach for Single-Packet IPTraceback Using Packet Logging and Marking," *IEEE Transactions on Parallel and Distributed Systems*, vol. 19, no. 10, pp. 1310 -1324, 2008.
[11] Goodrich MT., "Probabilistic Packet Marking for Large-Scale IP Traceback," *IEEE/ACM Transactions on Networking*, vol. 16, no. 1, pp. 15-24, 2008.
[12] Jeonga E. and Lee B., "An IP Traceback Protocol Using a Compressed Hash Table, a Sinkhole Router and Data Mining Based on Network Forensics against Network Attacks," *Future Generation Computer Systems*, vol. 33, pp 42 -52, 2014.
[13] Lu N., Wang Y., Su S. and Yang F., "A Novel Path-Based Approach for Single-Packet IP Traceback," *Security Communication. Networks*, vol. 7, no. 2, pp. 309-321, 2014.
[14] Sachdeva M., Singh G., Kumar K., and Singh K., "DDoS Incidents and their Impact: A Review," *The International Arab Journal of Information Technology*, vol. 7, no. 1, pp. 14 - 20, 2010.
[15] Saurabh S. and Sairam AS., "ICMP Based IP Traceback with Negligible Overhead for Highly Distributed Reflector Attack Using Bloom Filters," *Computer Communications*, vol. 42, no 1, pp 60-69, 2014.
[16] Savage S., Wetherall D., Karlin A., and Anderson T., "Network Support for IP Traceback," *IEEE/ACM Transactions on Networking*, vol. 9, no. 3, pp. 226-237, 2001.
[17] Snoeren A., Partridge C., Sanchez L., Jones C., Tchakountio F., Schwartz B., Kent S., and Strayer W., "Single-packet IP Traceback," *IEEE/ACM Transactions on Networking*, vol. 10, no. 6, pp. 721-734, 2002.
[18] Sung M., Jun X., Jun L., and Li L., "Large-Scale IP Traceback in High-Speed Internet: Practical Techniques and Information-Theoretic Foundation," *IEEE/ACM Transactions on Networking*, vol. 16, no. 6, pp. 1253-1266, 2008.
[19] TCPDUMP: www.tcpdump.org, Last Visited 2017.
[20] Tian H. and Bi J., "An Incrementally Deployable Flow-Based Scheme for IP Traceback," *IEEE Communications Letters*, vol. 16, no. 7, pp. 1140-1143, 2012.
[21] Tseng Y., Chen H., and Hsieh W., "Probabilistic Packet Marking with Non-Preemptive Compensation," *IEEE Communications Letters*, vol. 8, no. 6, pp. 359-361, 2004.
[22] Yang M. and Yang M., "RIHT: A Novel Hybrid IP Traceback Scheme," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 789- 797, 2012.
[23] Xiang Y., Li K., and Zhou W., "Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 42 -437, 2011.
[24] Xiang Y., Zhou W., and Guo M., "Flexible Deterministic Packet Marking: An IP Traceback System to Find the Real Source of Attacks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 4, pp. 567-580, 2009.

Vijayalakshmi Murugesan received the Ph.D. degree in information andcommunication engineering at Anna University, India. She is currently inDepartment of Computer Science and Engineering, Thiagarajar College ofEngineering, India. She serves as a reviewer to several journals including IET Information Security, Wiley Security and Communication Networks.Her research interests include network security, Digital Forensics andInternet of Things.

MercyShalinie Selvaraj is currently an Associate Professor and Head of the Department of Computer Science and Engineering, Thiagarajar College of Engineering, Madurai, India. Her research interest includes AI, Machine Learning and Information Security. She has the distinction of publishing over 75 research papers in refereed International and National Journals and Conferences. Her sustained research interest has made her complete sponsored R&D projects from DRDO, AICTE, DeitY, DST, NTRO, Honeywell and Yahoo. Her passion to work in Free/Open Source Software has lead to the development of ICT Framework for Thiagarajar College of Engineering which has received National level accolades. She received her Ph.D. (Computer Science and Engineering) in 2000 from Madurai Kamaraj University. She has Post Doctoral Research experience at University of California, Irvine, USA and Monash University, Melbourne, Australia.