ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

Establishing Source of Spoofing Attack Using IP Hybrid Traceback Scheme

Durgarani Basireddy[1], Sreekanth.K[2]

Department of CSE & JNTUH Department of CSE & JNTUH[1,2]

Abstract- Distributed Denial of Service (DoS) attacks are widely known attacks on networks that deny service over network. When such attacks use source address spoofing it is not easy to trace the source of attack. This is an open problem to be addressed. The existing traceback scheme employed either packet marking or packet logging approaches. However, for successful traceback, these schemes need large number of attack packets. To overcome this drawback Al-Duwairi and Manimaran presented hybrid traceback schemes which combine both approaches. The schemes include Distributed Link-List Traceback (DLLT) and Probabilistic Pipelined Packet Marking (PPPM). In this paper we implement the hybrid traceback schemes presented by them using a prototype application which demonstrates the proof of concept. The empirical results revealed that the proposed system traces back the source of attack effectively.

Index Terms –IP Traceback, address spoofing, Denial of Service attacks

I. INTRODUCTION

Adversaries make attacks by hiding their identity. Being at a remote place they can make attacks through some intermediate nodes. It does mean that they employ source address spoofing while making a Denial of Service attack [1], [2]. The advanced version of DoS is known as DDoS which takes advantage of address spoofing. When such attacks are made, tracingthesource of attack is difficult. These are the attacks that deny regular services being rendered over a network thus causing problems to genuine users. The aim of attackers is to hide their identity while causing problems to the victim. History shows many such attacks and the impact of them. Many root DNS server were under this attack in October 2002 [1]. The process of identification of source of attack packets is known as IP traceback. The traceback will help to control such attacks. By isolating attack sources it is possible to prevent DoS attacks and also help in making intelligent packet filtering techniques [3]. Due to the anonymous and distributed nature of the attack, the DDoS is very complex and difficult to traceback.

Generally, the traceback schemes put partial path information into spoofed packets which is known as packet marking. Another way the traceback schemes follow is known as packet logging which stores packet digests in the routers encountered on the way. The problem with these schemes is that they do need large number of attack packets and more resources to trace back. Al-Duwairi and Manimaran [4] proposed a novel traceback scheme that combines the both approaches. They have built two new schemes known as DLLT and PPPM. In DDLT hash based trace back [5] and PPM [6] are combined. In PPPM pipelines concept is used. These two approaches overcome the drawbacks of traditional approaches.

In this paper we implemented the trace back methods proposed in [4] using a custom simulator application. The application demonstrates the proof of concept of IP trackback. The remainder of the application is organized into the following sections. Section II reviews literature. Section III provides details of proposed scheme. Section IV provides implementation details. Section V presents experimental results while section VI concludes the paper.

II. PROPOSED TRACEBACK SCHEME

This section provides details about the proposed traceback scheme including problem statement, and algorithm for two typesof schemes namely Distributed Link List Traceback (DLLT) and Probabilistic Pipelined Packet Marking (PPPM). These concepts are briefly described here. However, detailed information of DLLT and PPPM can be found in [4]. The traceback problem is described here as illustrated in figure 1.

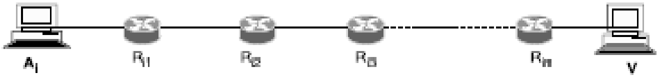


Fig. 1 –Traceback Problem Instance (excerpt from [4])

As can be seen in fig. 1, between the source and destination there are many routers found. Ai denotes attacker and V denotes victim. Between the victim and attacker there are ordered list of routers which are denoted as Ri1, Ri2, Ri3,and Rin. These routers are used to define the attack path. Some assumptions are made which are similar to the ones presented in [7], [6] and [8]. Two schemes have been proposed namely DLLT and PPPM.

III. DISTRIBUTED LINK LIST TRACEBACK (DLLT)

"Store, mark and forward" is the approach followed by DLLT. This scheme keeps track of the routers which are involved in forwarding packets. This is achieved by establishingtemporary links between the routers in distributed fashion. Every router generally marks the packet and forwards it. There may be a case where a router may not be willing to mark packet and forward it directly. With all the details a linked list is created and maintained. This process is illustrated in figure 2.

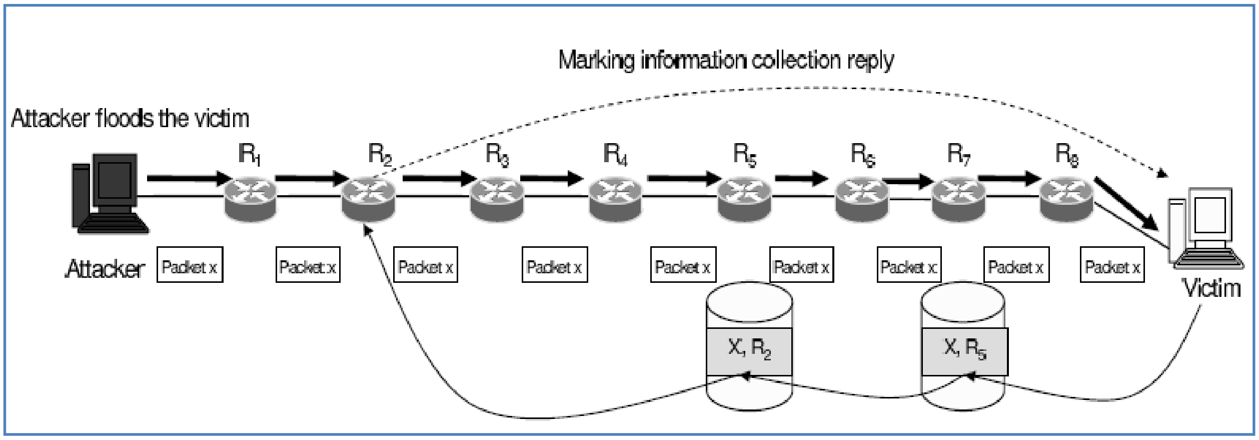
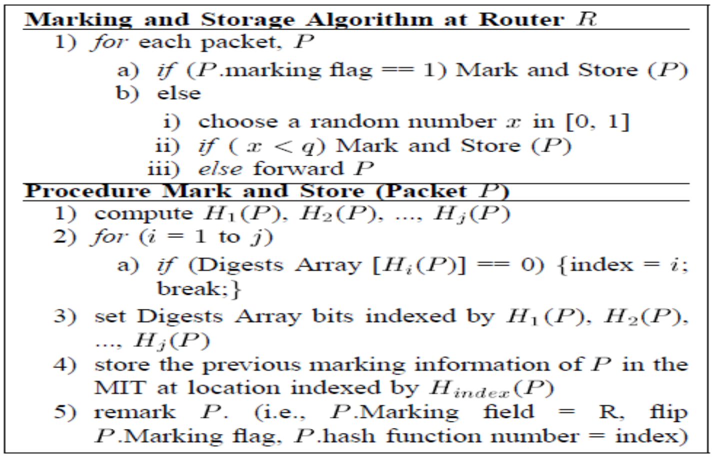


Fig. 2 – Illustrates distributed linked list marking (excerpt from [4])

As seen in fig. 2, the routers R2, R5 and R7 have marked the packet x. The figure also shows the victim making marking information collection request and also corresponding response. Here the linked list plays an important role in obtaining all makers about packet. A probabilistic marking and storage approach is followed by DLLT scheme. Packet digests are used to verify the forwarding of packets by routers. The digests of packets are mapped to specific storage locations. The algorithm for this scheme is as given in fig. 3.



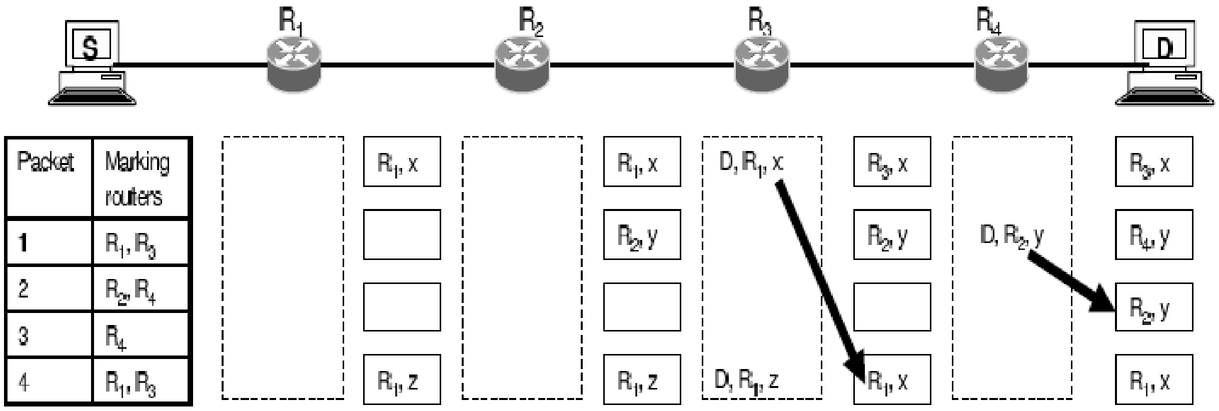
```
Marking and Storage Algorithm at Router $R$
  1) for each packet, $P$
        a) if ($P$.marking flag == 1) Mark and Store ($P$)
        b) else
            i) choose a random number $x$ in $[0, 1]$
           ii) if ( $x < q$) Mark and Store ($P$)
          iii) else forward $P$
Procedure Mark and Store (Packet $P$)
  1) compute $H_1(P)$, $H_2(P)$, ..., $H_j(P)$
  2) for ($i = 1$ to $j$)
        a) if (Digests Array [$H_i(P)$] == 0) {index = $i$;
           break;}
  3) set Digests Array bits indexed by $H_1(P)$, $H_2(P)$,
     ..., $H_j(P)$
  4) store the previous marking information of $P$ in the
     MIT at location indexed by $H_{index}(P)$
  5) remark $P$. (i.e., $P$.Marking field = R, flip
     $P$.Marking flag, $P$.hash function number = index)
```

Fig. 3 –Marking and storage algorithm as per DLLT (excerpt from [4])

As seen in fig. 3, the algorithm for marking and storage is presented. This algorithm runs at router. The algorithm invokes a procedure for mark and store.

Probabilistic Pipelined Packet Marking (PPPM)

DDLT needs long time storage by intermediary routers. This is its drawback. To overcome this drawback PPPM is introduced which makes use of pipeline based packet marking scheme. The idea behind this scheme is to transfer packet information from one router another router using the packets that follow the preceding packet. The scenario is as illustrated in fig. 4.



Packet	Marking routers
1	R1, R3
2	R2, R4
3	R4
4	R1, R3

Fig. 4 –Pipelined-based packet marking (excerpt from [4])

As can be seen in fig. 2, it is evident that the marking scheme is changed here. There is buffer associated with each router. Marking information associated with each packet is also shown.

IV. EXPERIMENTAL RESULTS

We built a prototype application in Java platform. The application is a custom simulator that demonstrates the proof of concept. The experiments are made with two marking schemes by name DLLT and PPPM. The environment used for the experiments is a PC with 4 GB RAM, Core 2 dual processor running Windows 7 operating system. The experimental results are presented as series of graphs below.

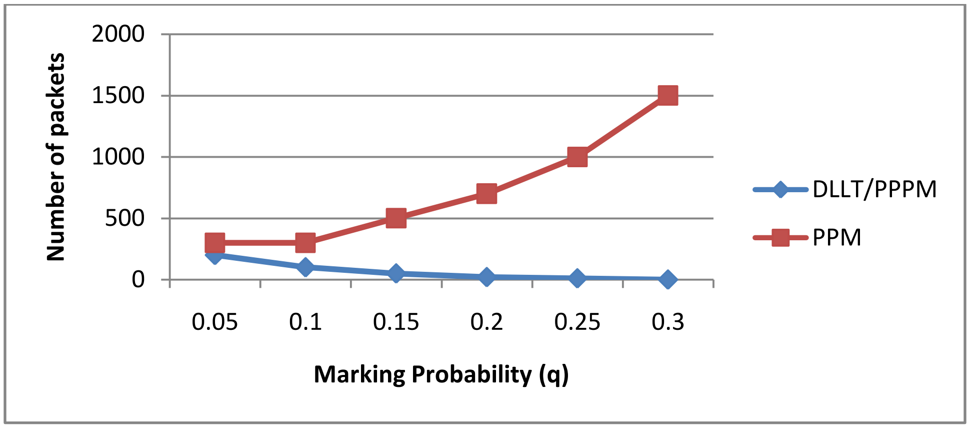


Fig. 5- A comparison between the number of packets required by DLLT/PPPM and that required by PPM Effect of marking probability, Attack path length

As shown in the above figure 5 represents the horizontal axis represents marking probability while vertical axis represents number of packets.

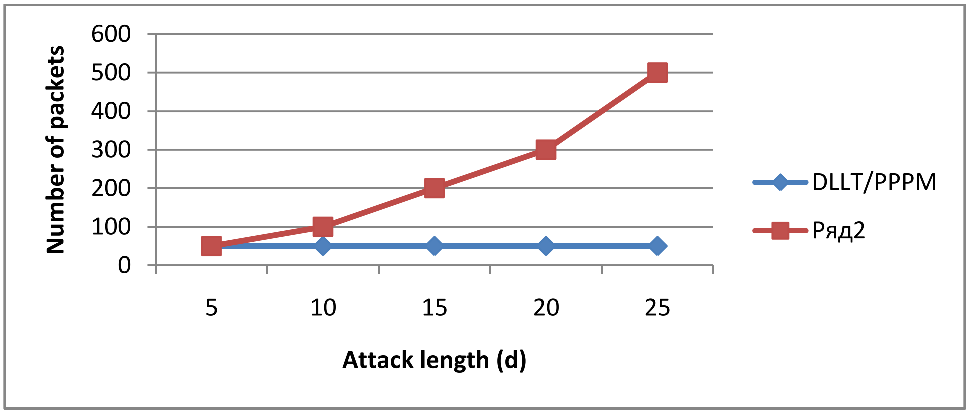


Fig. 6 - A comparison between the number of packets required by DLLT/PPPM and that required by PPM Effect of attack path length.Marking probability was fixed to 0.2

As shown in the above figure 6 represents the horizontal axis represents attack length while vertical axis represents number of packets.

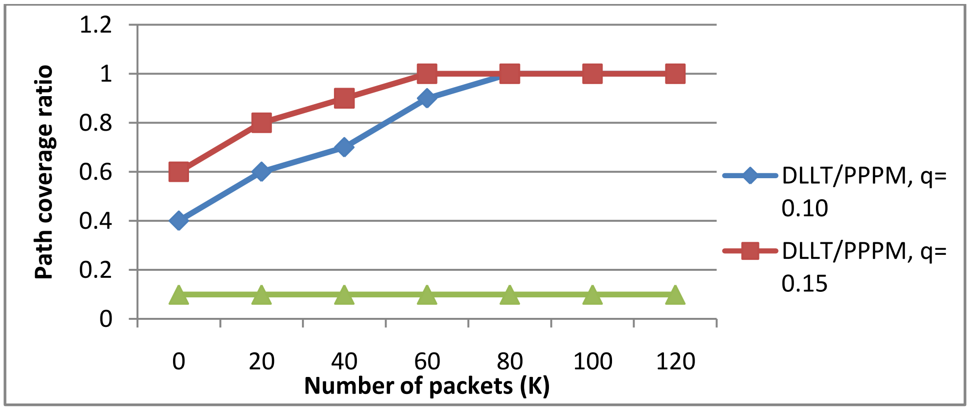


Fig. 7 - Comparison between DLLT/PPPM and PPM in terms of Path coverage ratio.

As shown in the above figure 7 represents the horizontal axis represents number of packets while vertical axis represents path coverage ratio.

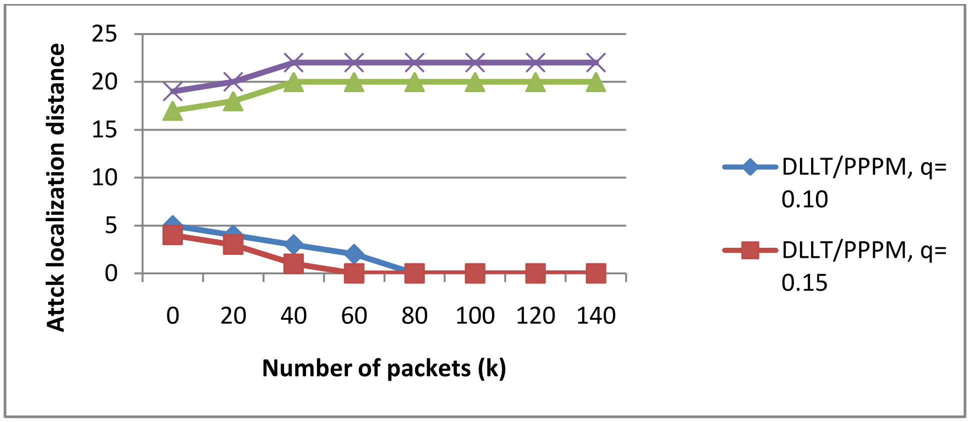


Fig .8- Comparisons between DLLT/PPPM and PPM in terms of Average attack localization distance.

As shown in the above figure 8 represents the horizontal axis represents number of packets while vertical axis represents attack localization distance.

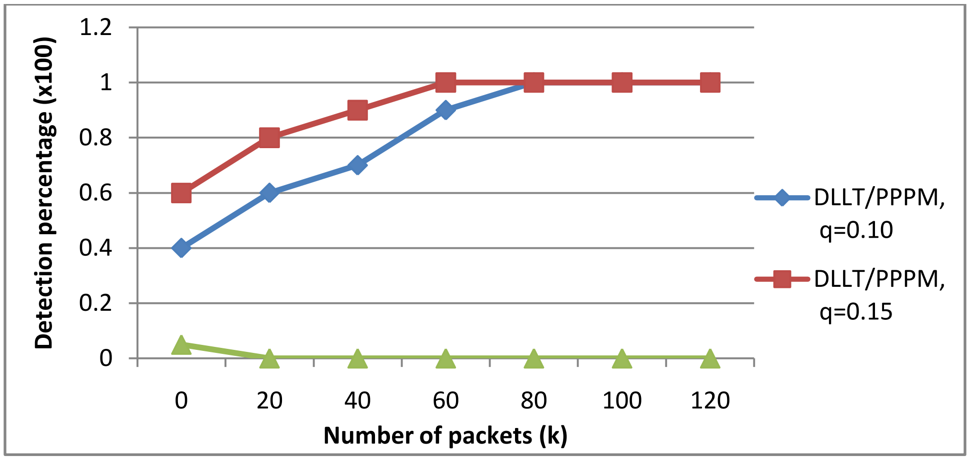


Fig. 9 - Comparison between DLLT/PPPM and PPM [6] in terms of Attack source identification percentage.

As shown in the above figure 9 represents the horizontal axis represents number of packets while vertical axis represents detection percentage.

V. CONCLUSION

When DoS attacks employ source address spoofing method, it is difficult to traceback the source of attack. To identify such source of attack more efficient tracebackschemes are required. The existing IP traceback techniques follow either packet logging or packet marking that cause overhead besides the need for large number of attack packets. To overcome this drawback Al-Duwairi and Manimaran[4] proposed a hybrid model which provides better performance in traceback. In this paper we implemented the hybrid model using a prototype application that demonstrates the proof of concept. The experimental results revealed that the hybrid traceback approach is effective inaccurately finding the source of attack.

REFERENCES

[1] D. McGuire and B.Krebs,“Attack on Internet calledlargestever,”in www.washingtonpost.com,Oct.2002. http://www.washingtonpost.com/wp-dyn/articles/A828-2002Oct22.html.

[2] C.Meadows,“AFormalFrameworkand Evaluation MethodforNet-workDenialofService,”inProc.IEEEComputerSecurityFoundations Workshop,June1999,pp.4-13.

[3] M.SungandJ.Xu,“IPTraceback-basedIntelligent PacketFiltering:ANovelTechniqueforDefending AgainstInternetDDoSAttacks,”in Proc.ofIEEETransactionsonParallelandDistributedSystems,Vol.14,No.9,pp.

861-872,Sep2003.

[4] Basheer Al-Duwairi and G. Manimaran, "Novel Hybrid Schemes Employing Packet Marking and Logging for IP Traceback", pp. 1-14

[5] A.C.Snoeren, C.Partiridge,L.A.Sanchez,C.E.Jones,F.Tchhakoun-tio,S.T.Kent,andW.T.Strayer,"Hash-BasedIPTraceBack,"inProc.ofACMSIGCOMM,Aug.2001.

[6] S.Savage,D.Wetherall, A.Karlin andT.Anderson,"Practicalnetwork supportforIPtraceback,"inProc.ofACMSIGCOMM,Aug.2000,pp. 295-306.

[7] D.Song and A.Perrig, "Advancedand authenticatedmarkingschemes forIPtraceback,"inProc.ofIEEEINFOCOMM2001,April2001.

[8] D.Dean,M.Franklin,andA.Stubblefield,"Analgebraicapproachto IP traceback,"inNetworkandDistributedSystemSecuritySymposium (NDSS'01),Feb.2001.

BIOGRAPHIES

Durgarani.B is student of MallaReddy College of Engineering and Technology, Hyderabad, AP, INDIA.

She has received B.Tech Degree Computer Science and Engineering and M.Tech Degree in Computer Science and Engineering. Her main research interest includes Networking and Datamining.

Sreekanth.K is working as an Assistant Professor in MallaReddy College of Engineering and Technology, JNTUH, Hyderabad, Andhra Pradesh, India. He has completed M.Tech (CN&IS) from JNTUH. His main research interest includes InformationSecurity and Computer Ad-HocNetworks.