Analysis of Various IP Traceback Techniques - A Survey

K. Arun Kumar
Computer Science and Engineering,
CMR Institute of Technology,
Hyderabad, Andhra Pradesh

K. Sai Ashritha
Computer Science and Engineering,
CMR Institute of Technology,
Hyderabad, Andhra Pradesh

ABSTRACT
IP traceback could also be a name given to any methodology for reliably determining the origin of a packet on the net. Because of trusting nature of the IP protocol, the source IP address of a packet is not authenticated. As a result, the source address in an IP packet can be fake allowing for Denial Of Service attacks (DoS) or one-way attacks. IP Traceback may be a important ability for chararcteristics sources of attacks and Starting protection measures for the Internet. This study paper extends many technologies to prevent the secured information from the network issues by using different IP traceback techniques.

Keywords
Denial of service (DOS), packet marking and packet logging.

1. INTRODUCTION
A countless amount of effort in recent years has been targeted within the network security problems. Here, one can statement the problem of detecting the source of the attack to be a device from that the flow of packets, organizing the attack, was initiated. This device are offten a machine, reflector, or a final link in an exceedingly stepping stone chain. Whereas characteristic the device from that the attack was initiated, still because the person(s), behind the attack is an ultimate challenge, limit the matter of characteristics the source of the offending packets, whose addresses are often spoofed is named the IP traceback problem. Let us see a scenario of DOS attack with diagrametic illustration.

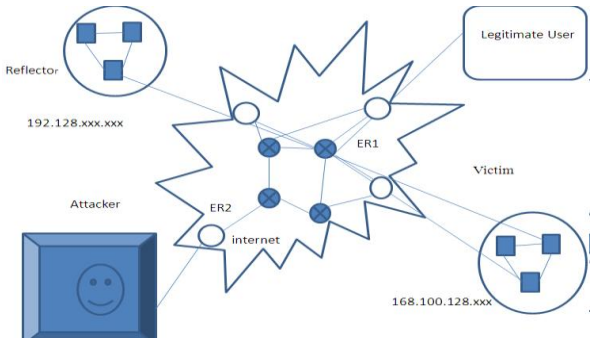

Fig.1. A Scenario of DOS Attack

One of the solutions relies on the routers in the network to send their identities to the destinations of certain packets, either encoding this information directly in rarely used bits of the IP header, or by generating a new packet to the same destination. This mainly focuses only on flood-based (Distributed) Denial of Service [DoS] attacks.

(i) Type of solutions involves centralized management, and logging of packet information on the network. This leads to a large overhead, and are complex and not scalable.

1.1.Classification of Traceback Methods
Trackback methods are generally classified into two types namely, preventive and reactive.

A. Preventive methods are used to prevent DoS attacks. A wide range of solutions has been proposed, however, this problem still remains as an open one.

B. Reactive methods solutions identify the source of the attacks. This is very significant because attackers spoof their addresses, thus techniques are necessary to trace back to the source of the attack.

1.1.1. Reactive Methods
1.1.1.1 Link testing
This Testing starts from the router nearest to the victim and interactively tests its upstream links til they verify that one is utilized to carry the attacker's traffic. Thus this procedure is perennial recursively on the upstream router til the source is reached.

1.1.1.2 Logging
Logging is suggested to log packets at key routers and so use data-mining techniques to see the trail that the packets traversed. It has the valuable property that it will trace an attack long once the attack has completed. This system has drawbacks, and probably huge resource needs and large scale interprovider information integration tough.

1.1.1.3 ICMP traceback
Internet Control Message Protocol (ICMP) in would like of trace out full path of the attacks. Typically this scheme is for each router to come upwith an ICMP traceback message or reach directed to the identical destination because the elite packet. The trace message itself consists of consequent and previous hop data and a time stamp.

1.1.1.4 Packet marking algorithm
During this scheme, every router within the count for forwarding a packet additionally inserts a mark within the packet. This mark could be a distinctive symbol orthodox to the current specific router. As a result the victim will verify all the shift hops for every packet by observant the inserted marks. There are two variants of this marking scheme. Firstly, Deterministic Packet Marking (DPM) scheme in which each router marks all the packets passing through it with its unique identifier. Secondly, probabilistic packet marking (PPM), DoS attacks may be prevented if the spoofed source IP address is traced back to its origin that lets distribution penalties to the wrong party or isolating the compromised hosts and domains from the reminder of the network.

1.1.1.5 FDPM traceback
Flexible Deterministic Packet Marking (FDPM) is the enhanced form of DPM that provides more flexible features to trace the IP packets and might acquire higher tracing capabilities over on top of mentioned IP traceback methods.

1.2.Technologies for Preventing Network Attacks
Present technologies for protecting networks against attacks concentrate on access management and attack detection. Even

if some ways will realize the attacker's identity, they are unsuccessful once the attacker's true IP address is hidden or unknown. Few technologies for preventing attacks has been classified below, they are as follows:

1.2.1 Firewalls

Firewalls are generally accustomed shield networks against attacks, particularly those returning from the web. Generally, firewalls management access based on source IP address, destination IP address, protocol type, and source and destination port range.

1.2.2 Intrusion detection

An intrusion detection system (IDS) detects network attacks to a ADP system. It relates the attack signatures, that are structures of famed attacks, with the insides of packets on the network or log information on the host computer.

This paper is organized as follows In section 1 Traceback methods and technologies for preventing network attacks. In section 2 related literature reviews on existing analysis paper. Final conclusion in section 3.

2. LITERATURE SURVEY

A. Yaar et. al.[1] Proposed a replacement packet marking approach i.e., Fast Internet Traceback (FIT), is one of in PPM (Probabilistic Packet Marking) traceback schemes which consists of two major parts: a packet marking scheme to be deployed at routers, and maps and path reconstruction algorithms utilized by end hosts receiving the packet markings. Several extents that improve IP traceback scheme: 1. Victims will determine attack methods with high probability once receiving solely tens of packets, a reduction of 1–3 orders of scale. 2. FIT performs well even within the presence of legacy routers, permitting each FIT-enabled router within the path to be recognized. 3. FIT scales to massive scattered attacks with thousands of attackers. FIT scheme uses each upstream router maps and packet markings with the fragment/number/distance format. It employs unique marking and reconstruction algorithms that dramatically improve its performance. Therefore, a number of the steps to be followed in FIT firstly, it permits the attacker victim to come up with the upstream route map using packet markings. Second, uses node sampling rather than the unremarkably used edge sampling, greatly reducing the number of false positives and also the number of packets needed for attack path reconstruction and lastly FIT uses only 1-bit within the IP ID field to mark the distance from the victim at that the packet was marked. This enables four additional bits to be used for hash fragment marks, that each greatly cut back false positives and will increase the effective marking chance and represents a step forward in performance and deployability.

Shui Yu et al. [2] discussed a novel traceback method for DDoS attacks, based on entropy variations between normal and DDoS attack traffic, which is different from commonly used packet marking techniques. As a basic requirement once a DDoS attack has been identified by the victim via detection algorithms, it initiates the pushback tracing procedure. The traceback algorithm first identifies its upstream routers where the attack flows came from, and then submits the traceback requests to the related upstream routers. This procedure continues until it reaches the discrimination limitation of DDoS attack flows. And some of the advantages compared with existing DDos traceback methods they are: it is memory non-intensive, efficiently scalable, and independent of attack traffic patterns.

Marcelo D. D. Moreira et al. [3] 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.

Qiao Yan et al. [4] outlined an improved dynamic probabilistic packet marking algorithm that can reduce the marking overhead of routers near the attackers and also can locate accurately. In this method, the challenge of weakest node and weakest link is solved with the price of a little more numbers of packets to reconstruct the attack path. The rate of false positive is reduced obviously with the value of F0F1 (01) and hence NS2 testify this approach is feasible and efficient.

Xin Liu et al. [5] proposed a NetFence a secure congestion policing feedback, to enable robust congestion policing inside the network. Bottleneck routers use the congestion policing feedback to signal congestion to access routers, and use it to robustly police senders' traffic and provably guarantees a legitimate sender its fair share of network resources without keeping per-host state at the congested link.

K. H. Choi et al. [6] discussed a new marking scheme with marking and tracing back algorithms during which a router marks a packet with a link that the packet came through. Therefore the links of a router are represented by Huffman codes according to the traffic distribution among the links. Generally this marking scheme needs:

(i) Once a router marks a packet with address information, the data is not on the router that is marking however of a router that is sent the packet to this router.

(ii) It uses a special table known as link table, that shows all the links between the router and its adjacent routers. The router joins to the marking field of a Huffman code word representing the link variety of the link through which the packet arrived. Once the marking field of a packet converts short of space left to join the corresponding Huffman code word for the link number, the router stores the content of the marking field with a message digest of the packet into the router's local memory, and so clears the field and appends the code word. The stored link sequence may be retrieved via the message digest of the packet from the intermediate router. Additionally it needs so much of less amount of memory compared to logging methods and is strong just in case of Distributed Denial of Service (DDoS). However this IP header is not applicable for marking, using either the Identification field or the choice field of the IP header has its own limitation.

C. Gong et al. [7] proposed a novel scheme to enhance the usefulness of log-based IP trace back by reducing its overhead on routers and makes an intelligent use of packet marking to improve the scalability of log-based IP trace back. This methodology is counting on the availability of free space within the marking field of the forwarded packets; routers decide whereever to record network path data. If there is free space available in the marking field, routers write their identification data in the packets; otherwise, routers calculate and record the packet digests, and so clears the marking field.

A number of the expansions of this approach to the state-of-the-art log-based approach called as Source Path Isolation Engine (SPIE). It reduces the storage overhead of packet digests to atleast one and second reduces the time interval demand by an element of the quantity of neighboring routers.

S. Malliga et al. [8] mentioned a packet marking technique, that follows the hybrid marking scheme to resolve IP trace back problem where ever the packets travel through the network, and they are marked with router data using modulo technique which is primarily based upon trace back request to reconstruct the path traversed by the packets one needs to use reverse modulo. Particularly, this method reconstructs the attack path with one packet and acquires terribly less overhead on the network and router. It needs work at routers, that the storage overhead on the routers is also significantly reduced. It stores the entire path traversed in a very single packet and so results in less convergence time to seek out the attack path at the victim.

L. Zhang et al. [9] outlined a way of technique called Bloom filter-based topology- where single packet IP trace back system, specifically TOPO, that utilizes routers native topology information, i.e., its immediate predecessor information to trace back. It will considerably cut back the quantity and scope of unnecessary queries and so decreases the false attributions to innocent nodes. Partial deployment could be a vital and desired property once designing and implementing IP trace back systems. Once Bloom filters are applied in IP trace back systems, it's troublesome to make a decision and their optimal control parameters a priori and so accomplish all time low false positive rate. Here designing a k-adaptive mechanism to dynamically alter parameters of Bloom filters in such a way that, IP trace back system can do the most effective performance in terms of false attribution rates, storage space required and reduce the number of unnecessary queries.

A. C. Snoeren et al. [10] developed a hash-based technique for IP trace back that generates review trails for traffic inside the network. Source Path Isolation Engine (SPIE) is employed to enable IP trace back, the flexibility to spot the single IP packet to be derived, its destination, and an approximate time of receipt. Tracing individual packets have needed prohibitory amounts of memory. One amongst SPIE's key innovations is to reduce the memory demand through the utilizations of Bloom filters. By storing only packet digests, and not the packets themselves, SPIE additionally does not increase a network's status to eavesdropping. Thus it permits routers to efficiently determine if they forwarded a selected packet inside a fixed interval whereas maintaining the privacy of unrelated traffic. During this methodology it supports trace-back of enormous packet flows for extended periods of your time in an exceedingly fashion the same as probabilistic marking schemes instead of discarding packet digests as they expire.

S. Savage et al. [11] discusses a completely unique strategy that tracing anonymous packet flooding attacks in net back towards their source. It is driven by the increased frequency and sophistication of Denial-of-Service (DoS) attacks and by the difficulty in tracing packet(s) with incorrect, or "spoofed" source addresses. Here a general probabilistic packet marking technique within the network is employed and performs a "post-mortem" – after an attack has completed. Later on trace attacks back towards their origin and ideally stopping an attacker at the source. Crucial the source generating attack traffic is surprisingly tough because of the stateless nature of net routing. As these packets traverse the web their true origin is lost and a victim is left and it does not require interactive cooperation with ISPs and thus avoids the high management overhead of input debugging. Therefore reuse the IP identification field must address issues with backward compatibility for IP fragment traffic.

K. Sarac [12] proposed a new Probabilistic Packet Marking (PPM) approach which improves the present state of the art in two directions: First it improves the efficiency and accuracy of IP trace-back and second it provides incentives for ISPs to deploy IP trace-back in their networks. This approach employs a new IP header encoding scheme to store the whole identification data of a router into a single packet thus eliminates the computation overhead and false positives as a result of router identification fragmentation. Here is a problem delaying the deployment of PPM approaches within the web and has restricted potency and accuracy in tracing large-scale Distributed DoS (DDoS) attacks, so as to avoid this problem an accurate and secure PPM (ASPPM) has been used that addresses the above-mentioned problem. ASPPM uses a new IP header encoding scheme to store the entire router identification data into one packet. In general, if a marked packet is to be forwarded to a client not purchasing an IP trace-back service, the marking data within the packet are going to be removed. Hence, it is suitable to deploy by ISPs as a value- added service whereever it stores the entire identification data of a router in a single packet and so the router does not have to be compelled to split its identification data into multiple fragments.

3. CONCLUSION

In this paper, different methods and technologies of IP traceback mechanisms discussed as a survey which firmly plays a vital role to transfer the information over the network. However, hackers generally hide themselves by spoofing their own IP addresses and then blast off attacks. To overcome these attacks a novel hybrid IP traceback scheme has been introduced which might be attempting within the course work.

4. REFERENCES

[1] A. Yaar, A. Perrig, and D. Song, "FIT: Fast internet traceback," in *Proc. IEEE INFOCOM2005*, Miami, FL, Mar. 2005, pp. 1395–1406.

[2] Shui Yu, Wanlei Zhou, Robin Doss and Weijia Jia, "Traceback of DDoS Attacks UsingEntropy Variations" in proc *IEEE* transactions on parallel and distributed systems, vol. 22, no. 3, march 2011.

[3] 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.

[4] Qiao Yan and Xiaoming He and Tuwen Ning," An Improved Dynamic Probabilistic Packet Marking for IP Traceback", I.J.Computer Network and Information Security, 2010, 2, 47-53.

[5] X. Liu, X. Yang, and Y. Xia, "NetFence: Preventing Internet Denial of Service from Inside Out," in ACM SIGCOMM. ACM, 2010.

[6] K. H. Choi and H. K. Dai, "A marking scheme using Huffman codes for IP traceback," in Proc. 7th Int. Symp. Parallel Architectures, Algorithms Networks (SPAN'04), Hong Kong, China, May 2004, pp. 421–428.

[7] C. Gong and K. Sarac, "A more practical approach for single-packet IP traceback using packet logging and marking," IEEE Trans. Parallel Distributed Syst., vol. 19, no. 10, pp. 1310–1324, Oct. 2008.

[8] S. Malliga and A. Tamilarasi, "A proposal for new marking scheme with its performance evaluation for IP traceback,"WSEAS Trans. Computer Res., vol. 3, no. 4, pp. 259–272, Apr. 2008.

[9] L. Zhang and Y. Guan, "TOPO: A topology-aware single packet attack traceback scheme," in Proc. IEEE In. Conf. Security Privacy Communication Networks (SecureComm 2006*)*, Baltimore, MD, Aug. 2006, pp. 1–10.

[10] 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 trace back," IEEE/ACM Trans. Networking, vol. 10, no. 6, pp. 721–734, Dec. 2002.

[11] 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.

[12] K. Sarac and C. Gong, "Toward a practical packet marking approach for IP traceback," *Int. J. Network Security*, vol. 8, no. 3, pp. 271–281, Mar. 2009.