Comparative Study of IP Trace back Techniques

Jigneshkumar V Madhad  
Department of Computer Engineering  
Narnarayan Shastri Institute of Technology, Jetalpur, Ahmedabad, GTU-Gujarat, India

Piyush Patel  
Department of Computer Engineering  
Narnarayan Shastri Institute of Technology, Jetalpur, Ahmedabad, GTU-Gujarat, India

Abstract

because so many decades World Wide Web has been used broadly in numerous fields, network safety problems include the main matter. IP traceback is just the actual method to understand the actual purpose, it reconstructs IP packets traversed path inside the World Wide Web to determine their own roots. IP Traceback may be an important ability for characteristics sources of attacks and Starting protection measures for the Internet. This paper discovers different IP Traceback approaches. This comparative paper provides as well as extends many technologies to prevent the secured information from the network issues by using different IP traceback techniques.

Keywords: IP Traceback, Link testing, Packet Marking, ICMP Traceback

I. INTRODUCTION

Internet facilities are generally as well as widely used now-a-days to finish and do each and every task or activity. As Internet is utilized for several tasks, attackers find a method to interrupt the services provided by it. For this reason, right now network safety may be a necessary requirement of Internet World. Even though many security measures are adapted by the security people to ensure security for the customers, still Internet is open for many attacks. The attacks have become so prevalent that no security measure can prevent all of them.

So as to fortify the matter of organizations, they require systems, for example, IP Traceback procedures which will at last decrease the possibilities of misfortunes. IP Traceback is an endeavour to follow the genuine beginning of a packet or a stream of packets. As a result of IP Spoofing, just accepting that the packet was sent by the node indicated as the source address in its IP header is not generally compelling, so different strategies for following packets to their root are required. Thus effective IP Traceback methods must be utilized to discover the genuine source of attacks, with a specific end goal to take any preventive or legitimate activities against the attackers.

IP Traceback is used to find the origins and attacking paths of malicious traffic. The task of identifying the original source of a packet is complex as the source IP address can be fake or spoofed. So IP Traceback techniques neither prevent nor stop the attack, they are used only to identify the source of the packets.

II. EXISTING IP TRACEBACK TECHNIQUES

Existing IP Traceback approaches can be classified into five main categories: (1)

- Link Testing
- Packet marking
- ICMP Traceback
- Logging
- Hybrid tracing.

A. Link Testing (2,3):

Link testing is an approach which determines the upstream of attacking traffic hop-by-hop while the attack is in progress. The majority of active traceback strategies begin as the router best for the target and interactively test their upstream hyperlinks till they will decide which one is used to carry the attacker’s traffic. In a perfect world, this method is rehashed recursively on the upstream router until the source is reached. Below we summarize two varieties of link testing schemes:

1) Input Debugging:

Numerous routers incorporate a component called input debugging. In Input Debugging, the victim needs to perceive that it is being attacked and needs to build up an attack signature that describes a common feature contained in all the attack packets. The most emergent problem with the input debugging approach, even with automated tools, is the management overhead, the coordination from the network admin. If the admin is unavailable or if he lacks the skill to assist the traceback, then the traceback process may be sluggish or its completion could be unattainable.

2) Controlled Flooding:

Another link testing traceback technique called Control Flooding which does not require any support from network operators. This technique tests incoming links of the victim by iteratively flooding each link with large bursts of traffic to see its effect on the incoming traffic. By observing the change in the rate of packets received, the victim can infer from which link the attack...
packets have arrived. This procedure is applied to the next upstream router until the origin of attack is reached. This kind of traceback by itself floods the network. Controlled flooding is also poorly suited for tracing distributed denial-of-service attacks because the link-testing mechanism is inherently noisy and it can be difficult to discern the set of paths being exploited when multiple upstream links are contributing to the attack. Finally, like all link-testing schemes, controlled flooding is only effective at tracing an on-going attack and cannot be used “post-mortem”.

B. Packet Marking
Packet marking methods relies on the routers in the network to send their identities to the destinations either by encoding this information directly in rarely used bits of the IP Header, or by generating a new packet to the same destination. They have the drawback in that they require a large number of attack packets to be collected by the victim to infer the attack paths. [5]

Packet marking methods require routers modify the header of the packet to contain the information of the router and forwarding decision. Hence the receiver of the packet can then reconstruct the path of a packet (or an attacking flow) from the received packets. [1]

As Packet marking methods do not cost storage resource on routers and the link bandwidth resource, they are generally considered to be lightweight. Because however, packet marking is not a widely supported function on routers; thus, it is difficult to enable packet marking traceback in the network.

There are two approaches of packet marking schemes:
- Probabilistic Packet Marking
- Deterministic Packet Marking

1) Probabilistic Packet Marking [3]
Probabilistic packet marking makes use of the Identification field as the marking space and stores the link information. It divides the IP address into eight fragments, 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, and the last 5 bits are enough to show the hop number. If the reported that few packets exceed 25 hops in the forwarding network [9]. When a router decides to mark a packet, it chooses a random fragment of its IP address, and records the fragment offset with the distance field set to 0. The advantage of PPM is that it needs no storage overhead for each router. But the drawback is also apparent. Victim needs a large number of packets to reconstruct the attack path, and PPM does not have the ability to trace a single packet.

Fig. 1: Probabilistic Packet Marking Method

Probabilistic Packet Marking Method [2,9] is shown in Fig. 1. In this technique, each router marks the packet with some probability say $p$ for example $p = 1/100$ which implies marking one packet for every 100 packets received. The marking field uses 16 bits identification field in the header, of which 5 bits are used for marking hop count, which would be useful information during reconstruction of attack path, and the remaining bits are used by the router to send its information. Larger information can be broken into fragments and marked in multiple packets. The marked packets will therefore contain only partial information of the path. This reduces the storage overhead in the packets. The victim has to receive enough number of packets to reconstruct the path. Prior knowledge of the topology does not require in this scheme. The disadvantage of this scheme is that it produces many false positives and the mark field value written by routers far away from victim might be overwritten by the routers closer to the victim and if the attacker is aware of the scheme, then the traceback fails. The marking field is used to hold start, end and distance. The start and end fields store the IP addresses of the routers residing at the two end points making an edge and the distance field registers the number of hops between this edge marked and the victim.
2) Deterministic Packet Marking\(^3\)

Deterministic Packet Marking scheme (DPM) is shown in Fig. 2. This technique overcomes the disadvantages of PPM. Every packet passing through the first ingress edge router is only marked with the IP address of the router. The IP address is divided into two fragments (16 bits each) and each fragment is randomly recorded into each inflowing packet. The entire IP address is recovered by the victim when the victim obtains both the fragments of the same ingress router. This scheme fails when the source address is spoofed and is also false positive. The enhanced schemes\(^{7,8}\) are proposed where the IP address is split into more fragments, and a hash function is used to contain the identity of the ingress router to decrease the false positive. Deterministic packet marking based on redundant decomposition is proposed in\(^{10}\). The knowledge of topology plays a significant role in DPM scheme’s traceback. Consider the DPM scheme suggested in\(^{11}\) where, it is assumed that the topology of the network is known in advance. The packet marking method involves hash of ingress router’s IP address. The hash value is split into chunks and each chunk is marked into the packet randomly. With the topology known, the victim performs traceback of the marked routers. Large numbers of packets are not required for traceback in this scheme but it consumes a longer search time to identify the origin. The traceback scheme is challenged, if the topology is modified.

When an intermediate router goes off, the traceback can be carried out with the topology but might turn to be false positive. If the attacker modifies the mark field, this scheme will fail to traceback. Instead of IP address respective bit fields were marked in\(^{12}\). In Flexible Deterministic Packet Marking (FDPM) scheme\(^{13, 14}\), the marking field length is varied according to the requirement. The length of the marking field is flexible and can be adjusted. Further, the marking rate can also be adaptively changed according to the incoming traffic load on the participating router. FDPM is capable of tracing a large number of real sources with low false positive rate and low resource requirement on routers.

C. ICMP Traceback\(^3\)

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 up with 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.

A traceback scheme utilizing the explicitly generated ICMP Traceback message was proposed in\(^{15}\). Each router samples the forwarding packets with a low probability (e.g. 1/20000) and sends a special ICMP message including the information like neighboring routers (forward and backward links) on the path to the destination and source along with the original (triggering)
Comparative Study of IP Traceback Techniques
(J4R/ Volume 02 / Issue 02 / 007)

packet. Traceback packet also includes an authentication field which guards against spoofed traceback packets sent from attackers. This field can be null authentication, random strings or even HMACs. TTL is set to 255 for computing distance at the receiving end. During DDoS flooding attack, these ICMP traceback messages are used by the victim to reconstruct the path taken by the attacker. The schematic representation of the scheme is shown in Figure 5. The updated version of the previous iTrace (ICMP Traceback) scheme was proposed in [16]. iTrace scheme is considered as an industry standard by IETF. The time taken for path reconstruction by iTrace is minimized in ICMP Traceback with cumulative path (iTrace CP) [17]. This scheme is independent of the attack length. This scheme encodes the entire attack path information (i.e. contains the addresses of all the routers on the attack path) into minimal number of packets, thus minimizing the attack path construction time. This is achieved at the expense of minimal additional overhead in computation, storage and bandwidth. An enhancement to this scheme is suggested in Enhanced ICMP Traceback with Cumulative Path [18], which suggests the exponential increase in the probability of message generation with the distance in hops from the victim. The effectiveness of the scheme relies on selecting the appropriate value for the probability exponent which influences the traceback time for attack paths of different length. The iTrace scheme suffers a serious problem on the resource spent on generating the number of traceback packets which turns out to be neither useful nor informative during traceback and this issue is addressed in Intention-driven ICMP traceback [19] which enhances the probability of the router to generate useful trace messages. This is achieved by adding an additional intention bit to the iTrace message. A modification to Intention driven traceback is provided in [20] to create more effective iTrace packets to detect the origin of attack more accurately.

D. Logging [3]

This solution involves storing packet digests or signatures at intermediate routers. The drawbacks of this technique include significant amount of resources have to be reserved at intermediate routers and hence large overhead on the network, complexity, centralized management.

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.

Logging scheme for IP traceback stores the information like packet’s digest, signature, and fields of IP header on all or few routers which forward packets within the domain. It is shown in Figure 6. When an attack is detected, the victim requests the upstream router to gather information about attack packet. If the information is found, then the router is counted as a hop in the attack path and the process is repeated.

E. Hybrid Traceback [3]

This solution achieves the best of both the worlds: small number of attack packets to conduct the traceback process and small number of resources to be allocated at intermediate routers for packet logging purposes.

The idea of hybrid scheme combining marking and logging has been conceived to overcome the disadvantage of individual marking and logging schemes as stated above and a drastic improvement in traceback has been achieved. In [21], two hybrid schemes of IP traceback are proposed – Distributed Linked List Traceback (DLLT) and Probabilistic Pipeline Packet Marking (PPPM). The first scheme preserves the marking information at the core routers in a precise way such that it can be collected using a linked-list based approach. The second scheme aims at passing the IP addresses of the routers that were involved in marking particular packets by stuffing them into the packets going to the same destination. This mechanism avoids the need for long-term storage at the core routers. This scheme can fail if IP marking field value is spoofed by the adversary but can be
identified with the help of restrictions imposed on TTL field. When compared to IP logging schemes, processing and storage overhead at the routers are significantly minimized using this Hybrid Scheme.

III. PASSIVE IP TRACEBACK

Here natural Internet-scale Passive IP traceback (PIT) approach that requires no ISP deployment. PIT analyzes packets collected from network telescopes, and infers the locations of spoofed traffic. The intuition behind PIT is that spoofing flows may trigger ICMP error messages at routers on the path to victim. These ICMP messages are sent to the spoofed nodes. Under the assumption that attackers use randomly forged addresses, some of these ICMP messages will be received by the network telescopes. The addresses of routers sending the message can be combined with an Internet route model to re-construct the attack path and find the locations of the spoofer.

IV. COMPARISON OF VARIOUS IP TRACEBACK TECHNIQUES

<table>
<thead>
<tr>
<th>Link Testing</th>
<th>Packet Marking</th>
<th>Packet Logging</th>
<th>ICMP Traceback</th>
<th>Hybrid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployability</td>
<td>PPM</td>
<td>DPM</td>
<td>Poor</td>
<td>Good</td>
</tr>
<tr>
<td>Scalability</td>
<td>Poor</td>
<td>Poor</td>
<td>Fair</td>
<td>Good</td>
</tr>
<tr>
<td>Memory Requirement (Network)</td>
<td>Not Required</td>
<td>Not Required</td>
<td>Very High</td>
<td>Not Required</td>
</tr>
<tr>
<td>Memory Requirement (Victim)</td>
<td>Not Required</td>
<td>Very High</td>
<td>Medium</td>
<td>Not Required</td>
</tr>
<tr>
<td>Router Processing overhead</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Reliability</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
<td>Poor</td>
</tr>
<tr>
<td>Parameter needed for traceback</td>
<td>Attack pattern and large number of packets</td>
<td>Minimum number of packets compared to PPM</td>
<td>One Packet</td>
<td>One Packet</td>
</tr>
<tr>
<td>Prior knowledge of different topology</td>
<td>Needed</td>
<td>Not needed. Faster traceback and low false positive if known</td>
<td>Not needed. Faster traceback and low false positive if known</td>
<td>Not Needed</td>
</tr>
<tr>
<td>Accuracy</td>
<td>Medium</td>
<td>Medium, huge false positive rate in case of DDOS attack</td>
<td>Good</td>
<td>Good for less number of attackers</td>
</tr>
</tbody>
</table>

Fig. 5: Passive IP traceback
V. CONCLUSION

The comparing traceback mechanism by considering different categories like Deployability, Router Involvement during Traceback, Parameter needed for traceback, Router Processing overhead, Memory Requirement (Network), Memory Requirement(Victim), Reliability. the advantages and disadvantages of the all mechanisms are described.

REFERENCES

[4] DONG YAN, YULONG WANG, SEN SU and FANGCHUN YANG A Precise and Practical IP Traceback Technique Based on Packet Marking and Logging State Key Laboratory of Networking and Switching Technology Beijing University of Posts and Telecommunications Beijing, 100876 P.R. China

<table>
<thead>
<tr>
<th>Post Attack Analysis</th>
<th>Not Possible</th>
<th>Possible</th>
<th>Possible</th>
<th>Possible</th>
<th>Possible</th>
<th>Possible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attacker challenge vs. Scheme's survival</td>
<td>Poor</td>
<td>Poor</td>
<td>Poor</td>
<td>Poor</td>
<td>Poor</td>
<td>Poor</td>
</tr>
<tr>
<td>Router Involvement during Traceback</td>
<td>High</td>
<td>Nil</td>
<td>Nil</td>
<td>High</td>
<td>Nil</td>
<td>High</td>
</tr>
</tbody>
</table>