A Survey of Modern IP Trace-back Methods

Chirag Ravat

M.E(I.T) Student,I.T Department,L.D College of engineering Ahmedabad,Gujarat,India.

ABSTRACT

Today network security is significant issue confronted by little organizations as well as large orgs like Samsung and Google. Customary engineering of web is defenseless against DDoS attacks and it gives an open door to an assailant to access an incredible measure of bargained has by utilizing their vulnerabilities to make assault systems or Botnets. In spite of the fact that various safeguard methods and countermeasures against DDoS assaults are built up, the quantity of such assaults is as yet expanding. The fundamental purpose behind that will be that researchers and law authorization organizations are as yet not ready to answer a imperative inquiry: where is the genuine wellspring of DDoS assault? In this paper, I tend to survey different sorts of traceback strategies and systems.

Keyword: - *DDoS Attack, IP Traceback, Link testing, ICMP traceback, Packet Marking, PPM, DPM, FDPM*

1.INTRODUCTION

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are a major threats in the Internet for over a decade. This type of attack is intended to prevent authorized users from accessing a specific network services or resources or degrading the quality of service for this users by sending huge amount of traffic to the attack destination (machines or networks) to deplete services and connection resources. During the last decade the growth of the internet was amazing, but also amazing was the grows of the internet crimes. As a result large amount of vulnerable systems are currently available to attackers. The attacker exploits these systems vulnerabilities by using various hacking techniques so that they become under his control. These vulnerable systems can be hundreds or thousands in numbers and these are commonly termed as 'zombies.' The group of zombies usually formed the 'botnet.' The magnitude of attack is depends on the size of botnet, for larger botnet attack is more massive and disastrous. The major problem with the defense from the DDoS attacks is that packets sent by zombies will have the source address in an IP header falsified (spoofed IP addresses) [1] which makes it practically difficult to identify the real location of attackers. Finding an attacker with spoofed IP address is more complex and this motivates the research on IP traceback, which is a methodology to trace attacking paths and the true origin of spoofed IP packets. In general, IP traceback is not limited only to DDoS it can be used for identifying a source of any packet on the Internet.
In this article we will review Link testing, ICMP traceback**,** PPM, DPM and FDPM techniques.

2. Classification of Traceback Schemes

2.1 Link testing hop-by-hop tracing

The idea of this technique is to checks the network connection between routers to trace the attack origin. If the specific characteristics of the attack traffic's (called the attack signature) are clear for system administrator who controls the router, then he can find the right incoming network link on the router. First the incoming links on the router closest to the attack destination are checked to find out which link caries the attacker's traffic. Process should be repeated on the upstream routers until attack origin is found. See Fig. 1.
Disadvantage: attack should stay ongoing until the trace is finished.
Input debugging [2] and controlled flooding are Link testing approaches.

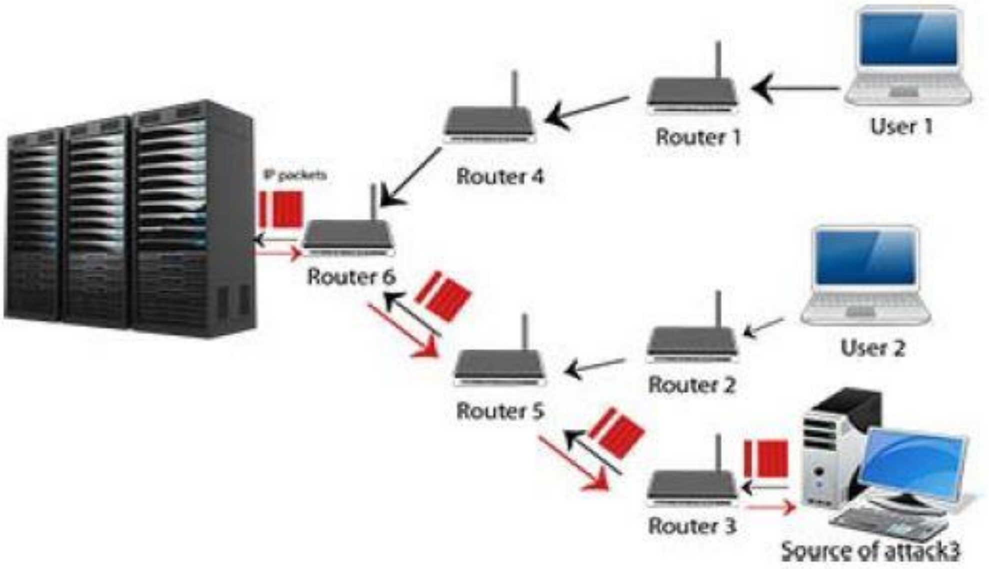

Fig -1: Link-testing traceback. The victim, defines the attack signature and the process starts from the router closest to the attack destination. During the process the upstream links are checked to determine which one carries the attack traffic.

2.2 In Input Debugging

The victim has to acknowledge that it is under attack and has to create an attack pattern (called attack signature) and check that with each of the incoming packets in the upstream routers and identify the corresponding upstream router and proceed further till the attacker.

Advantages:

- Progressive implementation support.
- Small network traffic overhead.
- Existing protocols compatibility
- Existing routers and network infrastructure compatibility.

Disadvantages:

- Along the attack path cooperation of ISPs is needed.
- The attack must stay active during the whole tracing process to succeed.
- Less effective against DDoS attacks.

2.3 Control Flooding

This technique does not require any support from network administrators. It tests incoming links of the victim by iteratively flooding each link with large portions of network traffic to see its influence on the incoming traffic. By observing the change in the speed of incoming packets, the victim can conclude from which link the attack packets have arrived. This procedure is repeated for the next upstream routers until the origin of attack is found.

Advantages:

- Existing protocols compatibility.
- Progressive implementation support.
- Small network traffic overhead.
- Existing routers and network infrastructure compatibility.

Disadvantages:

- This kind of traceback by itself floods the network.
- Knowledge of network topology is required.

- The attack must stay active during the whole tracing process to succeed.
- ISP cooperation might be required.

2.4 ICMP-Based Traceback

A traceback scheme utilizing the explicitly generated ICMP Traceback message was proposed in [3]. ICMP traceback messages generated by the router were used in this technique. The attack destination host receives this messages along with regular network traffic. Partial path information is contained inside this messages, this information includes packet source, time of sending and its authentication. Network managers can trace packets path to its origin by combining the information form ICMP traceback messages. This technique generates additional network traffic, in order to reduce this traffic ICMP traceback messages would be generated with the probability of 0.005 percent. Even such small amount of messages would allow to find the attack origin and will reduce the traffic. Typically a victim host under DoS attack receives thousands packets in a second. ICMP-based traceback is shown in Fig. 2.

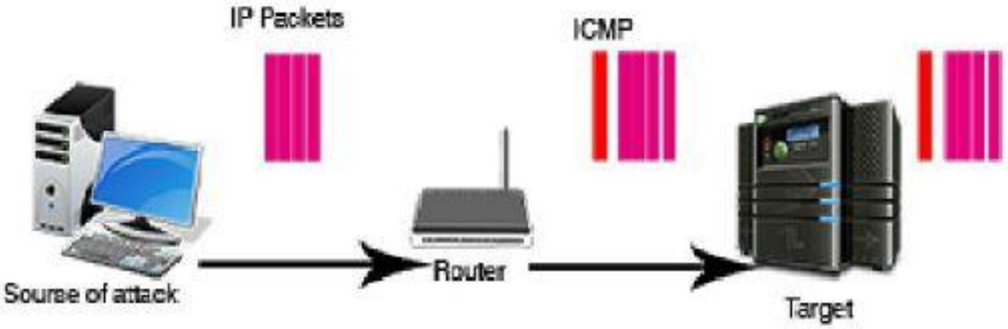

Fig -2: Only one ICMP traceback packet is generated by the Router for every 20,000 packets passing through it.. This ICMP packets Are forwarded to the target after generation.

The updated version of the previous iTrace (ICMP Traceback) scheme was proposed. IETF considers iTrace scheme as an industry standard. The time taken for path reconstruction by iTrace is minimized in ICMP Traceback with cumulative path (iTrace CP). This scheme doesn’t depend on 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 [4], 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 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 [5] to create more effective iTrace packets to detect the origin of attack more accurately.

Advantages:

- Existing protocols compatibility.
- Progressive implementation support.
- Post-attack analysis is possible.
- If encryption and key distribution techniques were used in implementation, presents a very promising and scalable technology for tracing the DoS attacks origin.
- Cooperation with the ISP is not needed.
- Existing routers and network infrastructure compatibility.

Disadvantages:

- Generates additional network traffic, even when probability for traceback messages is 0.005 percent.

- Without using the encryption scheme with key distribution implemented, false ICMP traceback messages can be injected by the attackers into the packet flow to hide the attack traffic's true source.
- ICMP traffic is very often filtered by companies due to its use in several other attack scenarios
- In the case of a DDoS attack very small number of ICMP traceback messages might be received from distant routers (but can be somewhat alleviated by intention-driven).

2.5 Packet Marking

Traceback data is inserted into the IP packet in packet marking scheme [1] by the routers on the path to the victim. Identification field of IP header is used to store the audit trail where the field size used for marking. The marking utilizes the rarely used fields of IP header, to store the audit trail where the field size used for marking varies from scheme to scheme. Each method emerged with the purpose to overcome the difficulties faced by the other. Figure 3 shows the general concept of packet marking.

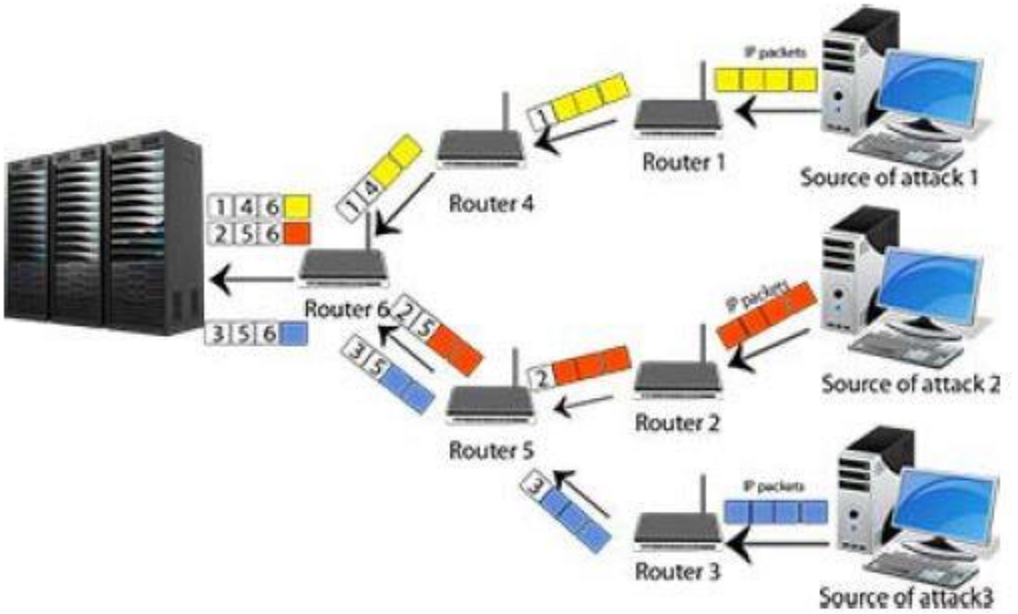

Fig -3: Packet marking. During the process of packets passing through the router probabilistically marks them (by inserting an indication of the router IP address). The marking process depends on the method chosen.

There are the following packet marking types: Probabilistic Packet Marking (PPM), Deterministic Packet Marking (DPM) and Flexible Deterministic Packet Marking (FDPM).

Probabilistic Packet Marking(PPM):

This technique [1, 6] concentrates on reconstructing the full path of attacker's traffic. Stamps are inserted into packets by the router with a fixed probability to allow victim to reconstructs full attack path using these stamps. The marking field uses 16 bits identification field in the header, of which 5 bits are used for marking hop count, which would be a useful information during reconstruction of attack path, and the bits that remain are used by the router to send its information. After arrival at the routers packets are marked with partial path information. The victim has to receive enough number of packets to re-construct the path. This scheme does not require prior knowledge of the topology.

Advantages:

- Possibility of approximate attack source allocation without the ISP cooperation.

- The attack source location can be done after the attack has stopped.

Disadvantages:

- This technique produces many false positives.
- The mark field value written by distanced routers might be overwritten by the routers closer to the victim.
- If the attacker is aware of the scheme, then the traceback fails.
- Traceback process requires large number of packets.

Deterministic Packet Marking (DPM):

This technique was first proposed [7] to overcome the disadvantages of PPM, it concentrates on the sources of the attacker's packets only, it doesn't depend on the attacker's packets path to the victim. 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. During the packets pass through the network this mark stays not changed.

Advantages:

Traceback process requires small number of packets.

Disadvantages:

- This techniques fails when the source address is spoofed and is also false positive.
- No overload prevention and Increase in packet header size.
- Consumes a longer search time to identify the origin.
- Scalability problem.

Flexible Deterministic Packet Marking (FDPM):

It is optimized version of DPM. In this technique [8], the marking field length is flexible and is adjusted according to the network protocols deployed. 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.

The packet marking

After entering the protected network an IP packet will be marked by the interface closest to the packet source on an edge entrance router. During packet passing through the network the mark will stay unchanged. The marks would contain the source IP addresses. When source ip addresses are need they can be aggregated at any point of network. One o this scheme advantages is that mark spoofing is not effective because all the packets are marked by the entrance router. Packet marks have length limits, because of that 2 packets are needed for transferring one source IP address. The mark contains also the segment number which is necessary for the reconstruction process. Router computing resources are used for the packet processing, therefore when the number of arriving packets is high, this resources may be depleted during the process and router will become overloaded. In order to fix this issue Flow-based marking is proposed. In the case of router overloading the packets with the most possible attacking packets will be distinguished from other packets and marked afterwards. This would allow to reduce the load of the router while still allowing to get the marking function.

The reconstruction

The reconstruction process is made in two steps:

1) Mark recognition

2) Address recovery

The process is much simpler and comfortable compared to DPM. After arrival to the attack destination each packet used for reconstruction is put into a cache in some cases it causes the difference between the processing speed and the incoming packets arrival speed. Different process units can get packet information from the cache that allows to use and compare different reconstruction methods by distinguishing the fields in the IP header, the length of the mark and the list of fields in the IP header which might be recognized.

Advantages

- Good scalability.
- Low false positive rate.

Disadvantage

- Packet processing consumes more resources.

This technique offers more flexible features for tracing the IP packets to its origin compared to other IP traceback schemas viewed in this article. Comparison of IP traceback techniques is displayed in Table I.

TABLE-1: COMPARISON OF IP TRACEBACK TECHNIQUES

Categories	**Link Testing input debugging**	**Link Testing Controlled flooding**	**PPM**	**DPM**	**FDMP**
Number of packets needed for traceback	N/A	N/A	10^3	10^2	10^2
Sources can be traced	N/A	N/A	10^2	10^3	10^5
Compatibility	High	Low	Low	Low	Moderate
Implementation	Easy	Fair	Easy	Difficult	Difficult
Router overhead	Low	High	Low	Low	Low
Post mortem Capability	N/A	N/A	Excellent	Excellent	Excellent
Network overhead	Low	High	Low	Very High	High
Network Topology	No	No	Yes	Yes	No

3. Conclusion

The IP traceback techniques proposed in this article have their specific advantages and disadvantages. Some of proposed schemas cannot be used for post attack analysis are resource intensive, can cause network overload and might be not effective against DDoS attacks. But FDPM technique requires relatively small amount of packets to finish the traceback process and uses not much computing resources so this method is a more powerful way to defend against large-scale DDoS attacks then other techniques proposed in this article.

4. REFERENCES

[1] N. Gupta, M. Dhiman, "A study of DDOS attacks, tools and DDOS defense mechanisms," International Journal of Engineering Reasearch and Application, vol. 1, issue 3, 2011

[2] A. John, T. Sivakumar, "DDoS: survey of traceback methods," International Journal of Recent Trends in Engineering, vol. 1, no. 2, May 2009.

[3] A. Parvathi and G. L. N. JayaPradh, "An IP trace back system to find the real source of attacks," International Journal of Computer Trends and Technology, vol. 2, issue 1, 2011.

[4] V. L. L. Thing, H. C. J. Lee, M. Sloman and J. Zhou, "Enhanced ICMP traceback with cumulative path," in Proceedings of the 61st IEEE Veh. Technology Conference, 2005.

[5] A. Mankin, D. Massey, C.-L. Wu, S. F. Wu, L. Zhang, "On design and evaluation of 'intention-driven' ICMP traceback, in Proceedings of the Tenth IEEE International Conference on Computer Communications and Networks, Scottsdale, AZ, 15-17 October 2001.

[6] M. T. Goodrich, "Probabilistic packet marking for large scale IP traceback," IEEE/ACM Transactions on Networking, vol. 16, no. 1, 2008.
.

[7] A. Belenky and N. Ansari, “Tracing multiple attackers with deterministic packet marking (DPM),” in Proceedings of the IEEE PACRIM’03, Victoria, BC, Canada, August 2003.

[8] Y. Xiang, W. Zhou and M. Gu, “Flexible deterministic packet marking: An IP traceback system to find the real source of attacks,” IEEE Transactions on Parallel and Distributed System, vol. 20, issue 4, April 2009.

BIOGRAPHIES

	Chirag Ravat has received his B.E. Degree from L.D. College of Engineering, Ahmedabad, Gujarat. And now pursuing M.E. Degree from same college, L.D. College of Engineering, Ahmedabad, Gujarat, India.