ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
June 2017,
Vol. 10, No. (2):
Pgs. 507-512

Survey on Packet Marking Algorithms for IP Traceback

Y. BHAVANI[1]*, V. JANAKI [2] and R. SRIDEVI[3]

[1]Dept of Information Technology, Kakatiya Institute of Technology and Science, Warangal, Telangana, India
[2]Dept of Computer Science, Vaagdevi College of Engineering, Warangal, Telangana, India
[3]Dept of Computer Science, Jawaharlal Nehru Technological University, Hyderabad, Telangana, India
*Corresponding author E-mail: yerram.bh@gmail.com

http://dx.doi.org/10.13005/ojcst/10.02.36

(Received: March 17, 2017; Accepted: May 05, 2017)

ABSTRACT

Distributed Denial of Service (DDoS) attack is an unavoidable attack. Among various attacks on the network, DDoS attacks are difficult to detect because of IP spoofing. The IP traceback is the only technique to identify DDoS attacks. The path affected by DDoS attack is identified by IP traceback approaches like Probabilistic Packet marking algorithm (PPM) and Deterministic Packet Marking algorithm (DPM). The PPM approach finds the complete attack path from victim to the source where as DPM finds only the source of the attacker. Using DPM algorithm finding the source of the attacker is difficult, if the router get compromised. Using PPM algorithm we construct the complete attack path, so the compromised router can be identified. In this paper, we review PPM and DPM techniques and compare the strengths and weaknesses of each proposal.

Keywords: Distributed Denial of Service, Deterministic Packet Marking, IP traceback, packet marking, Probabilistic Packet Marking.

INTRODUCTION

Distributed Denial of service (DDoS) attacks are becoming a major problem now a days. This type of attacks not only allows the authorized users from accessing the specific network services or resources but also propel a large amount of traffic on the network. There is a huge growth of internet users day to day. As the number of users are growing, the crime is also growing. Many techniques like input debugging, controlled flooding and ICMP messaging have been developed to identify attackers[1,4] but none of these techniques have been succeeded. To find the DDoS attackers the only method is IP traceback because the source address can be spoofed. IP traceback is the process

of finding the source router of the attacker who created a heavy traffic by sending spoofed packets. The IP traceback can be done in two ways using Probabilistic Packet Marking algorithm (PPM) and Deterministic Packet Marking algorithm (DPM). In both techniques the routers on the path to the victim stores the traceback data in the identification field of IPv4 and may also use fields like Type of Service and Reserve flag fields shown in fig.1. The victim after receiving the marked packets using the traceback data finds the source router of the attacker. In this paper we will review the PPM and DPM techniques.

Probabilistic Packet Marking(PPM)

Probabilistic Packet Marking algorithm helps in reconstructing the attack path from victim to the source. In this technique each router in the attack path as shown in fig.2 marks the packet with the partial IP address information called the marking information. This marking information is placed into the IP packet with a fixed probability[5,12]. After receiving the partial path information from the marked packets the victim reconstructs the attack path. Some of the Probabilistic Packet Marking techniques are discussed hereafter.

Practical network support for IP Traceback schemes by Savage, Wetherall, Karlin, Anderson

Savage et. al[4]. in their method proposed two components, marking procedure and path reconstruction procedure. In marking procedure each router in the attack path generates a random number *X*. If the random number *X* is less than the marking probability P_m then the router marks the packet with the part (fragment) of the marking information, if not the upstream routers' marking information is exclusive 'OR'ed with its corresponding part of the marking information. The marking information consists of IP address (32 bits) and a random hash value (32 bits) which is Bit interleaved (72 bits). The receiver after receiving this marking information constructs the attack path.

The expected number of packets needed to reconstruct the attack path with probability q is

$$E(X) = \frac{\ln(d)}{q(1-q)^{d-1}}$$

where d is the distance

Advantages

- ISP support not required.
- Less overhead at the router

Disadvantages

- High false positive rate
- Requires large number of packets
- The identity of edges being far away from victim is very less or may be zero due to overwriting.
- Due to overwriting some new edges which are not in the attack path may be formed, and result in erroneous construction of constructed graph.

Advanced and Authenticated marking schemes for IP Traceback by Song, Perrig

Song and Perrig[5] in their Advanced scheme-I marks the packet with the hash value of the IP address instead of the IP address itself. A 11 bit hash value is calculated to each IP address in the attack path. In this technique two independent hash functions are used to distinguish the order of two routers in the XOR result. The advanced marking scheme-II technique uses many number of hash functions. This approach uses flag field to indicate which hash function is used for the marking. If the FID is known then the R_i is simply calculated using h(<FID, R_i>). Thus different FIDs indicated different independent hash functions. In authenticated marking scheme, Song and Perrig proposed a technique to authenticate the packet marking so that the victim can detect the compromised routers.

Advantages

- Low network and router overhead
- Lower computation overhead
- Authenticated marking scheme provides efficient authentication of routers' markings.

Disadvantages

- In this technique the 11 bit hash value is not sufficient to avoid collision (i.e., the different router address may encode the same hash value).
- Though efficient and accurate than savage et al technique, still gives many false positives in DDoS attacks.
- Network map is needed to reconstruct the attack path.

Hash–Based IP Traceback by Snoeren, Partridge, Sanchez, Jones, Tchakountio, Kent

Snoeren et al[6]. proposed a Source Path Isolation Engine (SPIE) to trace the source of a particular IP packet. Packet's destination and time of receipt is provided to the routers to trace the path.

Advantages

Traceback is performed by using just a single packet.

Disadvantages

- Requires large amount of storage space and hardware changes for packet logging at router.
- High memory requirements.

A precise termination condition of the probabilistic packet marking algorithm by Wong Tsz-Yeung, Wong Man-Hon, Lui Chi-Shing

This algorithm[7] uses the savage et. al. marking procedure but uses a precise termination condition while constructing the attack graph. It takes less number of packets and guarantees that the constructed graph is correct.

Advantages

- Does not require any prior knowledge about the network topology.
- Upon termination of the algorithm the constructed graph is the attack graph.

Disadvantages

- Because it is using the PPM algorithm, all the disadvantages of PPM algorithm are brought into this method also.

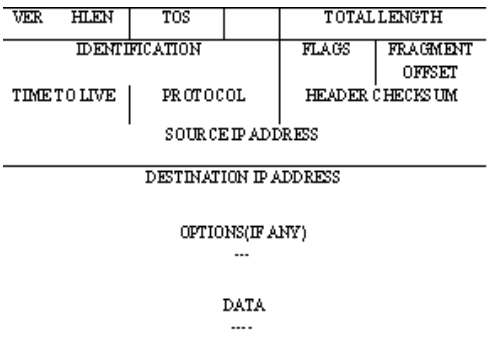

Fig. 1: IPv4 packet format

IP Traceback based on Chinese Remainder Theorem by Lih-Chyau, Liu Tzong-Jye, Yang Jyun-Yan

In Lih-Chyau Wuu et. al[8]. technique the characteristic of the IP address is passed with the IP address inorder to reduce the false combination. The IP address characteristic is calculated using the Chinese Remainder Theorem. The marking information is divided into five fragments. The victim after receiving the IP address parts combines them and finds the characteristic of the combined IP address. If the calculated IP address characteristic is equal to the received IP address characteristic then that IP address is considered as valid.

Advantages

- This technique has reduced the number of combinations and hence the number of false positives.
- It takes less number of packets to reconstruct the attack path.

Disadvantages

- It cannot be applied directly to IPv6.

IP Traceback through Modified Probabilistic Packet Marking algorithm using Chinese Remainder Theorem by Bhavani, Janaki, Sridevi

In this technique[9] a unique X value calculated using Chinese remainder theorem is

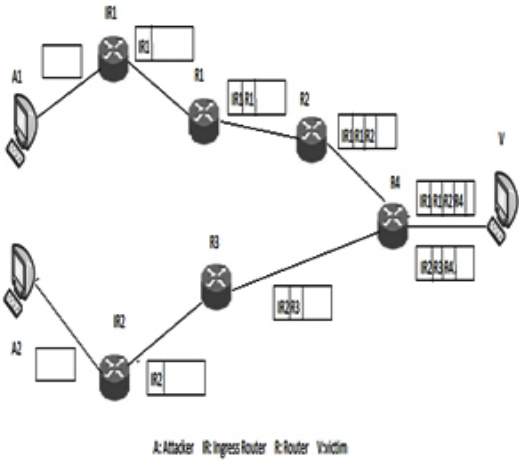

Fig. 2: Probabilistic Packet Marking. Packets are marked by the routers probabilistically with the routers IP address information as they pass through them

marked instead of the IP address itself. The X value is calculated as

$$X \equiv IP_i \bmod m_k$$

This X value is divided into four fragments. The victim after receiving this X value fragments combines them by checking the successive fragments. This combined X value is converted into IP address by using the Chinese remainder theorem as

$$IP_i \equiv X \bmod m_k$$

Advantages

- This technique has reduced more number of combinations and hence the number of false positives than in[8].
- It takes less number of packets to reconstruct the attack path.
- The far away routers have enough chance to pass their identity to the victim because the usage of flag eliminates overwriting of information by intermediate routers[12]
- It can be applied to IPv6.

Disadvantages

- Network map is needed to reconstruct the attack path.

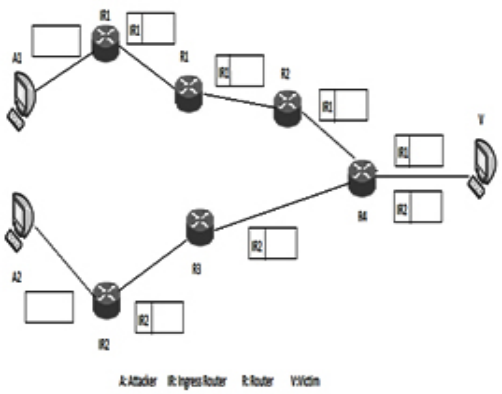

Fig. 3: Deterministic Packet Marking process. Packets are marked by only the ingress routers deterministically with their IP address information as they pass through them

Deterministic Packet Marking (DPM)

Deterministic Packet Marking helps in finding the source router of an attacker's packet but it will not find the attack path from victim to attacker as done in PPM. In this technique only the ingress router as shown in fig.3 marks the packet with its IP address[13,16].

IP Traceback with Deterministic Packet Marking

Andrey Belenky and Nirwan Ansari[13] proposed a technique where the ingress router marks the packet with its IP address parts. The IP address is divided into two parts. When the first part is sent the reserved flag is set to "0" and to "1" if the second part is sent. At the victim the two parts are combined to find the attacker.

Advantages

- It is easy to implement.
- It is suitable to find other types of attacks than DDOS attacks.
- Number of packets to reconstruct the attack path is very less.

Disadvantages

- Requires knowledge about ingress routers.
- If the ingress router is compromised then attacker is not found.

Improved Deterministic Packet Marking Algorithm

IDPM technique[14] is effective in finding the spoof packets. In this technique the ingress router will deterministically mark the packets with the IP address and the hash value of the IP address. The intermediate routers will calculate the hash value of the IP address in Identification field. If the calculated hash value is not equal to the hash value in identification field then it is assumed as a spoofed packet and it is dropped.

Advantages

- It is simple and scalable.
- It is suitable to find other types of attacks than DDOS attacks.

Disadvantages

- Requires knowledge about ingress routers.
- False positives may be more.

A Feasible IP Traceback Framework through Dynamic Deterministic Packet Marking

Yu S, et. al[15]. technique depends on the current router flow of traffic. When the Router identifies a doubtful flow, it passes a request to Mark on Demand (MOD) server for a unique mark. The MOD server identifies the unique mark and stores the mark, source address and time stamp into its database. With the sudden increase amount of attack flows, finally, the other router may discover the attack and intimate MOD server. The MOD server will store this information in its database. When the victim performs the traceback process it requests the MOD server about the IP addresses related to this unique marks. In this way the victim is able to find the source attacker.

Advantages

- It is simple and scalable.
- Number of packets to reconstruct the attack path is very less.

Disadvantages

- MOD server is a bottleneck.
- All packets will be enlarged, which will increase the network overhead.

Table 1: Comparison of PPM and DPM techniques

PPM	DPM
Less overhead because all the routers participate in marking with some probability.	As attackers send enormous number of packets marking all the packets is time consuming and overhead at ingress router.
Network overhead is less than that of in DPM, because only some packets are marked at each router.	All packets will be enlarged, which will increase the network overhead.
If the router gets compromised then it can be identified while constructing the path back.	If the ingress router gets compromised then it is impossible to find the attacker
The number of packets needed to reconstruct the attack path is very large.	The number of packets needed to find the ingress router (source router) is very less
Finds complete attack path.	Finds only the source router

Flexible Deterministic Packet Marking: An IP Traceback system to find the real source of attacks

FDPM technique[15] is effective in finding the real sources of the attackers. In this technique the marking of packets depend on the load of the router. If the load of the router exceeds some threshold value then that router differentiates between the normal packets and the attack packets. Only the attack packets are marked.

Advantages

- Requires a small number of packets to complete the traceback process.
- Traces a large number of sources in one traceback process.
- Low false positive rate.

Disadvantages

- All packets will be enlarged, which will increase the network overhead.
- If the ingress router is compromised then attacker is not found.

CONCLUSIONS

Many packet marking techniques have been studied. These mechanisms differ in their working principle but are used to detect source of the attacker. In this paper, the advantages and disadvantages of PPM and DPM techniques have been discussed. The comparative study of these techniques is shown in Table1. Scope of the future work is to reduce the number of packets to reconstruct the attack path using PPM.

REFERENCES

1. Marion Vasseur, Xiuzhen Chen, Rida Khatoun, Ahmed Serhrouchni, Survey on Packet Marking Fields and Information for IP Traceback, In *Proc. Int. Conf. on Cyber Security of Smart cities, Industrial Control System and Communications (SSIC)*, 2015.
2. R. Kiremire Ankunda, R. Brust Matthias, V. Phoha Vir, Using network motifs to investigate the influence of network topology on PPM based IP traceback schemes. *Computer Network*, 2014; 14–32.
3. Anatolii Balyk, Uliana Latsykovska, Mikolaj Karpinski, Yuliia Khokhlachova, Aigul Shaikhanova, Lesia Korkishko, A Survey of Modern IP Traceback Methodologies. In *Proc. 8th IEEE Int. Conf. on Intelligent Data Acquisition and Advanced Computing Systems*, 2015: pp. 484-488.
4. S. Savage, D. Wetherall, A. Karlin, T. Anderson, Practical network support for IP Traceback. In *Proc. ACM SIGCOMM conference*, 2000; pp. 295-306.
5. DX Song, A. Perrig, Advanced and authenticated marking schemes for IP Traceback. In *Proc. IEEE INFOCOM*, 2001; pp. 878–86.
6. Snoeren AC, Partridge C, Sanchez LA, Jones CE, Tchakountio F, Kent ST, Hash-based IP Traceback. In *Proc. ACM SIGCOMM*, 2001.
7. Wong Tsz-Yeung, Wong Man-Hon, Lui Chi-Shing, A precise termination condition of the probabilistic packet marking algorithm. *IEEE Transactions on Dependable Secure Computing*, 2008; 5: 6–21.
8. Lih-Chyau, Liu Tzong-Jye, Yang Jyun-Yan, IP traceback based on Chinese Remainder Theorem. In *Proc. 6th IASTED Int. Conf. on Communications, Internet, and Information Technology*, 2007, pp. 214–219.
9. Y. Bhavani, V. Janaki, R. Sridevi, IP traceback through modified probabilistic packet marking algorithm using Chinese remainder theorem, *Ain Shams Engineering Journal*, 2015; 6: 715–722.
10. D. Dean, M. Franklin, A. Stubblefield, An algebraic approach to IP Traceback. *ACM Transactions on Information and System Security*, 2002; 5: 119–137.
11. K. Park, H. Lee, On the effectiveness of probabilistic packet marking for IP Traceback under denial-of-service attacks, In *Proc. IEEE INFOCOM*, 2001.
12. Y. Bhavani, V. Janaki, R. Sridevi, IP Traceback through modified probabilistic packet marking algorithm. In *Proc. IEEE Region10 conference TENCON*, 2013, pp.1565-1569.
13. Andrey Belenky and Nirwan Ansari, IP Traceback with Deterministic Packet Marking. *IEEE Communications Letters* 7, 2003; 162-164.
14. Ashwani Parashar, Dr. Ramaswami Radhakrishnan, Improved Deterministic Packet Marking Algorithm. In *Proc. of 15th Int. Conf. on Advanced Computing Technologies*, 2013.
15. Yang Xiang , Wanlei Zhou , Minyi Guo, Flexible Deterministic Packet Marking: An IP Traceback System to Find the Real Source of Attacks. *IEEE Transactions on Parallel and Distributed Systems*, 2009; 20: 567 – 580.
16. S. Yu, W. Zhou, S. Guo, M. Guo, A feasible IP traceback framework through dynamic deterministic packet marking. *IEEE Transactions on Computers,* 2016; 65: 1418–1427.