A Survey of Traceback Based on Probabilistic Packet Marking Under DDoS Attacks

Linna Zhou¹, Hui Jiang¹ and Xinli Zhou¹

¹Institute of Information Technology, University of International Relations, Beijing, China

ở Corresponding author: zhoulinna@mail.tsinghua.edu.cn

Abstract. DDoS attacks are mostly adopted by attackers in the network. This attack is malicious on the network protocol, resulting in the object not working properly. At present, the Packet Marking is the main method to trace back the attackers under DDoS attacks, especially the Probabilistic Packet Marking (PPM) of Packet Marking. Therefore, the two main types of Probabilistic Packet Marking are studied in this paper: Advanced Packet Marking and Authenticated Packet Marking (APM) and Adjusted Probabilistic Packet Marking (APPM).

1. Introduction

DDoS attacks are mostly adopted by attackers in the network. This attack is malicious on the network protocol, resulting in the object not working properly. At present, the Packet Marking is the main method to trace back the attackers under DDoS attacks, especially the Probabilistic Packet Marking (PPM) of Packet Marking. The Packet Marking was first proposed by Burch and Cheswick[1] in 2000. It aims to help victims to reconstruct the attack path and finally identify the source of attackers by adding the address information of the router to the IP packet. And this method is verified by Doeppner[2] and Savage et al.[3-4] through experiments. In 2000, the classical Probabilistic Packet Marking (PPM) was first proposed by Savage et al.[3-4] After many experiments, PPM becomes a systematic method which includes node append and node sampling algorithm, edge sampling and compressed edge sampling algorithm. This method can reduce overhead and cut the cost. But, it increases the calculation and attackers easily falsify the identification information. Subsequent improvements to the probabilistic packet marking are based on the classical PPM.

2. Advanced Packet Marking and Authenticated Packet Marking

In 2001, Song et al.[5] improved on Savage’s PPM, and proposed Advanced Packet Marking and Authenticated Packet Marking (APM). They use the Hash Function to reduce the calculation and prevent forgery of information. The Advanced Packet Marking uses edge sampling to reconstruct the path according to the known Network Topology. The traceability is better, but the forged information can not be identified. Therefore, Authenticated Packet Marking is proposed, using the 16-bits of the identification domain to mark, using a secret key at intervals. The secret key is announced later to prevent information forgery. But the required storage space is large, and the response time is relatively long.

In 2005, A Verified Packet Marking (VPM) scheme was proposed by Jinming Li et al.[6] The VPM proposes how to select a new and optimal marker probability. And the VPM uses the edge sampling to reconstruct the attack path and construct a tracking topology tree. The nodes at both ends of the attack
path store the marked routing information for verification to prevent the attacker from forging. The Fast Internet Traceback (FIT), which was improved on the method of Song, was proposed by Yaar et al.\[7\] in the same year. The traceback process is divided into “the construction of the network topology” and “the identification of the intrusion path” in this method. It is proposed that the host constructs the network topology according to the marker information, and then the victims reconstruct the attack path according to the topology structure. Yonghui Li\[8\] proposed a Fast Intra-domain IP Traceback Method based on Dynamic Probabilistic Marking (IDPM) in 2011. This method implements the same process as FIT. IDPM has the advantage that the router can dynamically adjust the packet marking probability with the optimal marking probability.

In 2009, Zhiyong Yuan\[9\] improved on the basis of the classical PPM and expanded the marking space of the IP header. He proposes a packet domain to group each router in the attack path to reduce the number of fragment combinations and the time of reconstructing the path. It improves efficiency and easily distinguishes which router the tag packet comes from. In 2016, Yan Tang et al.\[10\] proposed an advanced packet marking scheme algorithm based on multidimensional pseudo-random sequences, which was improved on the basis of the Song’s APM. On the one hand, the hardware is used to implement of the edge sampling matrix instead of the Hash Function. And the marking packet is verified. On the other hand, the weight of the introduced edge is used for the qualitative and quantitative analysis on the reconstructed path result, which increases the credibility.

3. Adjusted Probabilistic Packet Marking

In 2002, Peng et al.\[11\] presented a Adjusted Probabilistic Packet Marking (APPM), which was designed to address the “weakest chain” problem of the probabilistic packet marking. The problem is that the victims collect little information on the nearest edge or node from the attackers when reconstruct the path and can not determine the final source of the attack. The previous fixed probability is replaced by the adaptive probability, so that the router dynamically determines the probability of the marking packet based on its location at the attack path. However, Dequan Li\[12\] believed that the scheme proposed by Peng was unfeasible in 2004. He believes that this method is time-consuming and large computation and impracticable. Therefore, he proposes an adaptive packet marking scheme to mark the router with a better probability after re-encoding, which reduces the false alarm rate of the traceback and computation.

In 2006, Yinan Jing\[13\] proposed the Adaptive Edge Marking Scheme (AEMS) based on reverse recognition. The development of this scheme inherits the advantage of the APM to prevent the forgery of information. The probability of covering the data packet is small, if the data packet has been marked in the router. The attack path can be confirmed only by the upstream router, so the network burden is small and the labeling probability is less affected. An IP Traceback scheme bases on the Marking in order is proposed by Haipeng Qu et al.\[14\] This scheme orderly sends the fragment of data packet by storing the tag state of each target IP address. The victims receive the required marking packets more quickly and accurately, improving the speed of the reconstructed attack path and the accuracy of the traceback, when attacked by DDoS.

In 2015, Peng Sun et al.\[15\] proposed a self—adaptive packet—marking algorithm based on path length. The algorithm designs two kinds of marker data: (1) When the path length does not exceed 32, the forwarded data packets are not repeatedly marked, that is, the data is not covered again; (2) When the path length exceeds 32, an overlay mark algorithm is adopted. In addition, they applies to the reflection node by designing a reflection mark algorithm with storage marks and copy marks. The storage marks store the router information in the reflector. The copy marks are the marks in the proposed reflector and are copied into the response header.

In 2017, Li Weiyue\[16\] proposed an improved dynamic probabilistic packet marking scheme based on fragment association, which was based on the classical PPM. The number of IP fragments is reduced by the method. The IP fragments and the Hash fragments are combined in the same data packet to prevent the forged information from being processed in the TTL domain. The victims reconstruct the path after hash matching of each data fragment. It reduces the complexity of the
operation, and the time required for traceback. It also proposes to verify and reorganize to prevent forgery information from affecting the final traceback result.

4. Analysis and Comparison of two types of Probabilistic Packet Marking Traceback Algorithms

The above two types of probabilistic packet marking traceback algorithms have their own advantages and disadvantages. Under the DDoS attacks, the traceback ability of the two algorithms are compared from the following five aspects:

1. Do it need a network topology map?
   According to the network topology map, the attack path can be reconstructed well through the topology map structure, and the time required for traceback is less. But the network topology structure needs to be known in advance.

2. The speed of reconstructing the attack path
   Can it respond quickly and trace the source of the attack, after the victim is attacked. Tracking during the attack, is it time-sensitive?

3. Router overhead
   The router needs to mark its address information into the transmitted data packet, and also needs to record some data packet information. Therefore, the router needs to have certain marking functions, and the router needs extra overhead in addition to normal packet forwarding.

4. Algorithm complexity
   How much time and space resources are needed, when the probabilistic packet marking algorithm is actually used? Usually, the complexity of algorithm is determined by the amount of the input data.

5. False alarm rate
   Whether it can identify and authenticate the packet information forged by the attackers, thereby reducing the certain false positive rate?

As can be seen from the table, APM and APPM algorithms have different advantages in different aspects. APM algorithm reduces the false alarm rate and router overhead, but need to know the network topology map in advance to build and determine the attack source for the attack path. APPM algorithm uses a variable probabilistic method. When the router marks the information, it can adaptively change the marking probability according to a certain setting rule. Therefore, the speed of tracking is much faster, and it is not necessary to know the network topology in advance for reconstructing the attack path. However, the router overhead is large and the algorithm complexity is high.

|                      | Do it need network topology map? | The speed of reconstructing the attack path | Router overhead | Algorithm Complexity | False alarm rate |
|----------------------|----------------------------------|--------------------------------------------|-----------------|---------------------|-----------------|
| APM                  | yes                              | slow                                       | smaller         | low                 | low             |
| APPM                 | no                               | fast                                       | larger          | high                | high            |

5. Conclusion

At present, the DDoS attacks are growing threats in the Internet security. Because the DDoS attacks are simple to implement and the scope of the attacks is large. The victims will bear unbearable losses, once the attacks are launched. The traceback of the DDoS attacks have become a major study. This paper studies the traceback technology of the probabilistic packet marking algorithm, which is the mainstream method used in DDoS attacks in recent years. The development of packet marking traceback technology is mainly based on advanced packet marking and authentication packet marking algorithm and adaptive probability packet marking algorithm. Both of them have better effects on anti-counterfeiting and reducing storage space. But currently there are still some incompatible issues.
between them. The next step of this paper will continue to conduct in-depth research on them to find a more suitable method for complementing the two, further improving the accuracy and efficiency of traceback.

Acknowledgement
The work is supported by the National Natural Science Foundation of China (NSFC) under Grant no.U1536207, the National Key Research and Development Program of China under no.2016QY08D1600 and the the National Key Research and Development Project of China under no. 2016YFB0801405 and Research on Network Security Discipline Construction under the Framework of National Security Science First Class Discipline in the 2018 Annual Basic Research Service Expense Project of the University of International Relations under no.3262018T02.

References
[1] Burch H, Cheswick B. Tracing Anonymous Packets to Their Approximate Source[C]/Proceedings of the 14th Conference on Systems Administration. Usenix Assoc: [s.n.], (2000)
[2] Doeppner T W, Klein P N, Koyfman A. Using router stamping to identify the source of IP packets[C]/ CCS 2000, Proceedings of the, ACM Conference on Computer and Communications Security, Athens, Greece, November. DBLP,184-189, (2000).
[3] Savage Stefan, David Wetherall, Anna Karlin, Tom Anderson. Practical network support for IP traceback[J]. ACM SIGCOMM Computer Communication Review. (2000)
[4] Stefan Savage, David Wetherall, Anna Karlin, Tom Anderson. Network support for IP traceback[J]. IEEE/ACM Transactions on Networking (TON). 3 (2001)
[5] Song D X, Perrig A. Advanced and authenticated marking schemes for IP traceback[M]. (2001).
[6] Yaar A, Perrig A, Song D. FIT: fast Internet traceback[C]/ INFOCOM 2005. Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE. IEEE, 1395-1406 vol. 2, (2005).
[7] Jinming Li, Weichuan Wang. A New Packet Marking Scheme for DDoS Attack Source Tracking[J]. Journal of Communications, (11): 22-27+33, (2005).
[8] Zhiyong Yuan. Research on attack source tracking technology for distributed denial of service attacks[D]. Central South University, (2009).
[9] Yan Tang, Guo-nian Lv, Hong Zhang. Advanced packet marking strategy algorithm based on multi-dimensional pseudo-random sequence[J]. Journal of Computer Applications, 36(11): 3093-3097+3102, 2016.
[10] Peng T, Leckie C, Ramamohanarao K. Adjusted Probabilistic Packet Marking for IP Traceback[M]// NETWORKING 2002: Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications. Springer Berlin Heidelberg, 697-708, (2002).
[11] Dequan Li, Yiding Xu, Yurui Su, Dengguo Feng. Adaptive Packet Marking in IP Tracking[J]. Chinese Journal of Electronics, (08): 1334-1337, (2004).
[12] Yinan Jing. Research on attack source tracking in distributed denial of service attacks[D]. Fudan University, (2006).
[13] Haipeng Ou, Dengguo Feng, Yurui Su. IP packet tracking scheme based on ordered labeling[J]. Chinese Journal of Electronics. (01),2006
[14] Yonghui Li. Research on traceability method based on packet marking in IP network [D]. Beijing University of Posts and Telecommunications, (2011).
[15] Peng Sun, Qing Wu. Research on RDDoS Attack Source Tracing Technology Based on Adaptive Packet Marking[J]. Communication Technology,48(04):478-483, (2015).
[16] Weiyue Li. Research and implementation of data source tag marking based denial of service attack traceback technology [D]. Beijing University of Posts and Telecommunications, (2017).