# The Systematic Survey for IP Traceback Methods

Hongcheng Tian[1,2], Jun Bi[2]
1. Information Department, The 309th Hospital of PLA
2. Institute for Network Sciences and Cyberspace, Tsinghua University
2. Department of Computer Science, Tsinghua University
2. Beijing National Research Center for Information Science and Technology (BNRist)
Beijing, China
thc@pku.org.cn, junbi@tsinghua.edu.cn

***Abstract***— Distributed Denial of Service (DDoS) attacks continue to pose major threats to the Internet. IP traceback can identify locations of attackers and attacking paths. This paper classifies existing IP traceback schemes, points out advantages and disadvantages of each category, and summarizes five evaluation indexes for IP traceback to evaluate six representative traceback schemes. In addition, this paper proposes three future research areas of IP traceback. And this paper is an important valuable reference for network researchers to go in for the further study on IP traceback.

***Keywords—IP traceback; network architecture; network security***

## I. Introduction

A packet is forwarded in the Internet, dependent entirely on its destination address. Thus, attacking sources often forge source addresses to escape detection, such as SYN flooding [1], DNS amplification [2], Smurf [3], etc. But it is difficult for victims to block the attack in real time, precisely locate attacking source(s) and pursue legal actions.

To confirm the hosts that directly generate attacking packets and the attacking path that attacking packets follows is called traceback problem [4] (Fig. 1). Traceback is executed with the assistance of a series of routers. Traceback can also collect statistics for packets' forwarding path(s) in the Internet in order to optimize router configuration, benefiting the research in the area of traffic engineering. IP traceback is receiving more and more attentions from the industrial and academic fields.

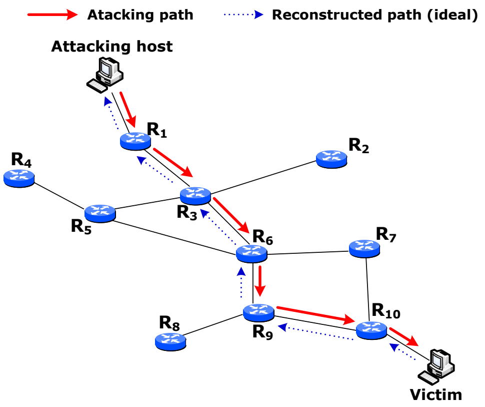

Fig. 1. Traceback problem [4] (to take one attacking host, one victim and the corresponding attacking path for example)

This paper categorizes existing IP traceback methods, points out advantages and disadvantages of each category, summarizes five evaluation indexes for IP traceback in order to evaluate six representative traceback methods, and finally points out three future research areas of IP traceback.

The rest of the paper is organized as follows: In Section II, we present six typical kinds of IP traceback. Section III summarizes five evaluation indexes to compare among six representative methods for IP traceback. In Section IV we discuss three future work about IP traceback. And in Section V, the conclusions are given.

## II. Classification of IP Traceback Methods

Researchers have proposed various approaches to trace attacking traffic back to attacking source(s) and identify attacking path(s). Existing methods for IP traceback can be categorized as the following six types: link testing, packet marking, logging-based schemes, ICMP-based traceback, compounded IP traceback approaches, and overlay network for IP traceback.

The first type, link testing, belongs to real-time approaches for IP traceback. When attacks are in progress, the first type may start up the tracing process. The first type includes the following two subclasses: Ingress filtering [5] and controlled flooding [6].

The remains can trace back not only in real time but also post mortem. It is not necessary that attacks continue until the traceback ends, different from the first type. When packets are forwarded in the Internet, necessary information is recorded in the packets or network devices, and after attacks are discovered, the attacking path(s) will be reconstructed according to the traceback information in the packets or network devices, and then the attacking source(s) will be located.

978-1-5386-4646-5/18/$31.00 ©2018 IEEE

## A. *Link Testing*

Link testing must be conducted when malicious attacks are ongoing, otherwise, IP traceback will not be successfully performed. This type of IP traceback is often used to trace back the attacking path and the attacking source in real time, and is not used post mortem.

### *1) Ingress Filtering [5]*

Ingress filtering utilizes a router function, which can confirm the input physical link of output attacking packets according to their certain features. The attack features come from attacking packets and are used to confirm input port of attacking packets at the victim's upstream router. In the same way, the input port of further upstream router can be identified. This process is repeated recursively over hop-by-hop upstream routers. Accordingly, the attacking path can be reconstructed and the attacker can be located.

For ingress filtering, it is not necessary to modify existing network protocols and this method is easy to be implemented. But the management overhead is high. Network administrators are needed to work co-operatively to trace back attack(s). If the attacking path transits multiple ISPs, the coordination among multiple ISPs is difficult. And It is required that the duration time of the attack is long enough for ingress filtering to trace back.

### *2) Controlled Flooding [6]*

Controlled flooding submerges relative physical links of a router with the bursts of traffic and watches changes of the velocity in which attacking packets reach the victim. When the reaching velocity decreases, the input physical link of the attacking packets at the router may be confirmed. Similar to Ingress filtering, this process is repeated recursively over hop-by-hop further upstream routers, and the attacking path and attacking source can be found.

In controlled flooding, it is not necessary to change existing protocols at routers and this method is intuitive.

However, network administrators must know the network topology of controlled flooding region. The weakness of controlled flooding is that it is actually a denial of service (DoS) attack that occupies the precious network bandwidth, and the bandwidth overhead in tracing is high. Thus, controlled flooding should not be widely used. Furthermore, if the velocity of the attack traffic, which the victim is receiving, is irregularly changing, it is difficult to trace the attacking sources accurately.

## B. *Packet Marking [7-23]*

The working process of packet marking methods consists of two sub-processes: marking sub-process at routers and path reconstruction sub-process at a victim.

Marking sub-process at routers is described in the following: when an attacking packet is sent to the network and reaches a router, the router marks information related to its partial (or entire) address into the attacking packet with a certain probability. Subsequently, the attacking packet is forwarded by the downstream routers hop by hop. In the same way, many attacking packets are marked and forwarded in the network.

Path reconstruction sub-process at a victim is presented below: when a victim receives the attacking packets, it can extract path information from the attacking packets and reconstruct the attacking path along which the attacking packets transits according to the path reconstructed algorithm.

Packet marking schemes only uses the information embedded in packets, not generating additional traffic. And packets with the marking information are not filtered by firewall or security strategy. In addition, packet marking methods do not need the cooperation from ISPs, different from Ingress filtering.

However, the protocols running at routers are required to be modified. And packet marking schemes cannot be used on packets which are fragmented or encrypted.

### *1) Deterministic Packet Marking Technologies [12-13]*

These technologies require that routers mark every packet which transits the routers, and every packet must store addresses of all routers that the packet transits. It is required that the packet can supply enough marking space but it cannot in fact. So far, existing deterministic packet marking technologies mainly comprise the following three methods: node adding algorithm, node sampling algorithm and edge sampling algorithm.

### *2) Probabilistic Packet Marking Technologies [14-16][21]*

These technologies require that a router marks a packet with the partial (or entire) address at a certain probability, reducing the computing overhead of routers and the requirement of marking space. So far, existing probabilistic packet marking technologies mainly consist of the following two schemes: probabilistic packet marking scheme based on fragments [14], and algebraic approach for IP traceback [15].

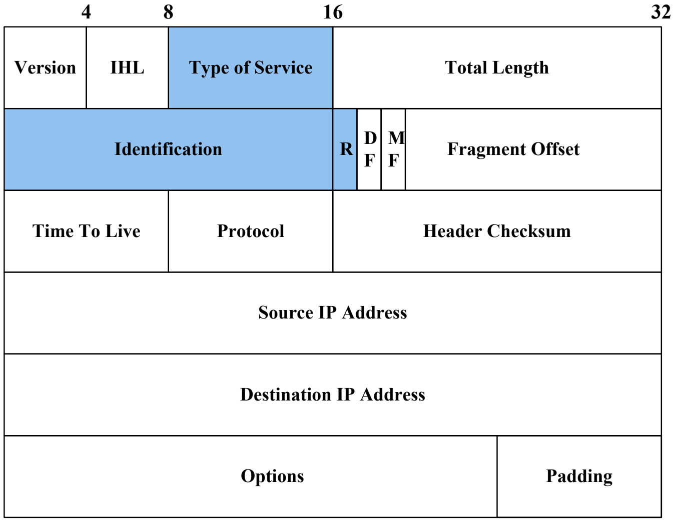

Fig. 2. Light blue fields are often occupied by packet marking methods, for example, [4] and [7] occupy Identification field, [12] takes up Identification field and Reserved Flag (R), [10] occupies Identification field, Reserved Flag (R) and Type of Service field.

The main shortcomings of the packet marking methods are that the computation cost is high, and the reconstructed path has more false positives [41]. Since the marking fields of various packet marking methods are customizable by the designers, some packet header fields defined by RFC 791 [39] is often occupied, such as Identification, Type of Service, Reserved Flag and so on (Fig. 2). If a packet is not marked by routers and reaches the victim, its header may carry the original semantic information or the forged mark from an attacker. But the victim cannot distinguish among a legitimate mark, a forged mark and the original semantic information in the marking fields. And the forged mark or the original semantic information is improperly regarded as the legal mark to be used for attacking path reconstruction. Thus, on the one hand, the computing overhead of the attack path reconstruction increases, on the other hand, the reconstructed path has more false positives.

### C. *Logging-based Schemes [24-29]*

Routers log characteristics of the traffic in the network facilities (such as routers, servers or dedicated network storage devices). Generally, characteristic information is compressed and stored. For example, commonly-used compressed technology is Bloom Filter (BF) [40]. When traceback is launched, the log records can be queried over hop-by-hop upstream routers. The routers along the attacking path will be identified gradually and at last the router nearest to the attacking source can be located. As said before, logging-based schemes can trace the attacking paths and sources not only in real time but also post mortem.

Source Path Isolation Engine (SPIE) [24] is a typical logging-based method for IP traceback, providing a single-packet traceback service that can trace DDoS attacks. In SPIE, each router uses a BF to record the feature information of each transiting packet, and when tracing, the attack path is reconstructed through querying the log records of routers.

The main problem of logging-based schemes is that the storage and computing overheads are high. In the Internet architecture, the main function of the router is to forward packets, and the computing and storage functions of the router are relatively weaker. If a logging-based scheme is deployed, the computing and storage costs of the router are so heavy that the forwarding function of the router is seriously affected, and it will have a serious impact on the main business of ISPs.

### D. *ICMP-Based Technologies [30-31]*

Routers generate ICMP messages for transiting packets at a very low probability. ICMP messages, including router information and information of transiting packets, are sent to the source host (this is to deal with reflecting attacks) or the destination host. When the host receives these ICMP messages, it extracts useful information and reconstructs attacking path according to the path reconstructed algorithm.

In ICMP-based technologies, computing overheads of routers do not increase much. The additional traffic that ICMP-based technologies generate is few.

But ICMP messages may be filtered by routers along the way and false negatives [41] of traceback results increases. The host needs to receive ICMP messages as many as possible for path reconstruction. If the number of ICMP messages is not enough, the complete attacking path cannot be reconstructed successfully.

### E. *Compounded IP Traceback [32-35]*

Packet marking and logging-based schemes have their own virtues and vices. Thus, some researchers combine them together (known as the compounded IP traceback) and make good use of the advantages and bypass the disadvantages. That is to say, computation and storage overheads can be reduced. In compounded IP traceback, every router should mark or log a packet which transits the router. Generally speaking, when one scheme solves one or more problems, it produces other problems simultaneously.

HIT [32], as a compounded IP traceback, is similar to SPIE [24], and has the capability of the single-packet traceability. Furthermore, HIT causes less overhead at routers than SPIE, because HIT marks information into the transiting packet and do not need to log the packet at every router.

Compared with SPIE, HIT reduces the storage overhead of 1/2. And the storage speed of the BF in SPIE needs to match the total data arrival rate of the router while the BF in HIT only needs to match the data arrival rate of each interface, reducing the demand for the storage speed of the BF in HIT. The disadvantage of HIT is that [32] does not describe how to number neighbor routers.

Reference [33] proposes a precise and practical IP traceback approach (PPIT) to improve HIT. Specifically, (a) HIT cannot distinguish the upstream and downstream relationships among the routers along the forwarding path of attacking packet when tracing back. Aiming at this issue, in PPIT, when a router logs a packet, the current TTL value of the packet is also used as the log item. (b) Along the forwarding path of each packet, HIT records the packet once every 2 routers while PPIT does every 3 routers, thus reducing the total storage overhead in the network. In addition, since PPIT is improved from HIT, it also has shortages of HIT.

### F. *Overlay Network for IP Traceback [36]*

CenterTrack [36] uses the overlay network and the existing technologies (such as tunnels, input debugging, etc.) to implement IP traceback. In CenterTrack, there are a central traceback router and some border routers. Tunnels are configured between the central traceback router and the border routers, forming an overlay network. In the overlay network, the core is the central traceback router.

Border routers can selectively reroute interesting packets (or all transiting packets) to the central traceback router. And the central traceback router can observe which tunnel a packet comes from by means of Sniffer or other tools, identifying which border router the packet comes from. The central traceback router checks the packet, and directly discards or forwards it to the appropriate router. According to the scale of the network, more than one central traceback router may be deployed. Among these central traceback routers, there are of full mesh.

In CenterTrack, the central traceback router builds tunnels with multiple border routers and bears heavy computing overhead. The central traceback router is the performance bottleneck of the whole system for IP traceback.

## III. Evaluation Indexes and Evaluation on Representative IP Traceback Methods

So far, there exist many different IP traceback approaches, and every approach has its own characteristics. It is necessary to evaluate these approaches using a series of normative indexes. Thus, we summarize five evaluation indexes for IP traceback, and we evaluate six representative approaches for IP traceback on the basis of the five evaluation indexes.

### *A. Evaluation Indexes*

We make an analysis of different methods for IP traceback, and get five evaluation indexes: computing overhead, storage overhead, false positive ratio (FPR), false negative ratio (FNR) and traceback time. In the following, we will explain the above five evaluation indexes.

#### *1) Computing Overhead*

The index, computing overhead, indicates the computing costs of the router or the victim when the tracing scheme works. Computing overhead is measured in terms of the computing time in the environment of the same hardware and system software. The computing overhead is lower, the performance of the traceback scheme is better.

#### *2) Storage Overhead*

The index, storage overhead, shows the amount of storage space that the router or the victim needs when the tracing scheme works. The storage overhead is lower, the performance of the traceback scheme is better.

#### *3) False Positive Ratio*

False Positive Ratio (FPR) is defined as the ratio of the false positive number ($N_{FP}$) to the checking positive number ($N_{CP}$) (1). FPR indicates the wrong proportion of the traceback result.

$$FPR = \frac{N_{FP}}{N_{CP}} = \frac{N_{FP}}{N_{TP} + N_{FP}} \tag{1}$$

$N_{FP}$ is the number of routers that the traceback result shows they are in the attacking path but actually not. $N_{CP}$ is the number of routers that the traceback result shows they are in the attacking path. And $N_{CP}$ is the sum of $N_{TP}$ and $N_{FP}$. Thereinto, $N_{TP}$ is the number of routers that the traceback result shows they are in the attacking path and actually they are indeed. FPR is lower, the performance of the traceback scheme is better.

TABLE I. THE COMPARISON AMONG SIX REPRESENTATIVE IP TRACEBACK METHODS

| | | **Controlled Flooding** | **PPM** | **SPIE** | **iTrace** | **HIT** | **Centertrack** |
|---|---|---|---|---|---|---|---|
| **Computing Overhead** | **router** | low | low | high | low | high | high |
| | **victim** | low | high | low | low | low | low |
| **Storage Overhead** | **router** | none | none | high | none | high | none |
| | **victim** | none | high | low | low | low | none |
| **False Positive Ratio (FPR)** | | high | high | low | high | low | low |
| **False Negative Ratio (FNR)** | | low | low | low | high | low | low |
| **Traceback Time** | | long | long | middle | long | middle | short |

*4) False Negative Ratio*

False Negative Ratio (FNR) is defined as the ratio of the false negative number ($N_{FN}$) to the actual positive number ($N_{AP}$) (2). FNR indicates the proportion that the routers succeed in escaping traceback.

$$FNR = \frac{N_{FN}}{N_{AP}} = \frac{N_{FN}}{N_{TP} + N_{FN}} \qquad (2)$$

$N_{FN}$ is the number of routers that traceback result shows they are not in the attacking path but they actually are. $N_{AP}$ is the number of routers that they are in the attacking path in fact. And $N_{AP}$ is the sum of $N_{TP}$ and $N_{FN}$. Thereinto, $N_{TP}$ is the same as (1). $N_{FN}$ is the number of routers that the traceback result shows they are not in the attacking path but actually they are. FNR is lower, the performance of the traceback scheme is better.

*5) Traceback Time*

Traceback time is defined as the time that the traceback process lasts from the beginning to the end, indicating that how much time we spend to get the traceback result after the traceback request is launched. This index is directly related to the traceback speed. Traceback time is shorter, the performance of the traceback scheme is better.

### *B. Evaluation on Representative Traceback Methods*

According to the above five evaluation indexes, we compare the six representative traceback schemes with each other (controlled flooding [6], PPM [4], SPIE [24], iTrace [30], HIT [32] and Centertrack [36]). The comparison results are listed above(Table I).

According to Table I, There is no method, whose five evaluation indexes are all the best or all the worst. Thereinto, SPIE and HIT have higher computation and storage overhead at routers, while PPM has higher computation and storage overhead at victims. And Control Flooding, PPM and iTrace have higher false positive ratios, while iTrace has higher false negative ratios.

Although the computing overhead of Centertrack at routers is high and its other evaluation indexes are good, Centertrack can only trace attacking traffic back to the border routers of the deployment region and its central traceback router bears heavy computing overhead.

Basically speaking, the pros and cons of a method depend on the method itself and the requirements of end-users.

## IV. Future Study About IP Traceback

IP traceback faces many challenges because of the following main reasons: (a) the stateless characteristic of Internet; (b) no source address validating on IP packets; (c) commonly-used network proxies and Network Address Translation (NAT) [37-38]. Although researchers have had much study on various schemes for IP traceback, there exist some shortcomings in the aspects of incremental deployment, traceback overhead, traceback accuracy, traceback time and so on. Furthermore, the traceback field lacks an evaluation model to evaluate different schemes. It is required that more research should be done on IP traceback. The future research areas are proposed but not limited to:

### *A. The Study to Combine IP Traceback Approaches with Intrusion Detection Systems (IDS)*

Existing IP traceback methods mark or log packets, not distinguishing legitimate packets from attacking ones. The traceback information, generated from legitimate packets, is not useful to trace back attacking traffic, but brings addition computing and storage overhead. In the next step, combined with IDS, traceback information is only generated from attacking traffic. The advance in this area relies on the breakthrough at IDS.

### *B. The Study on New Packet Marking Methods for IP Traceback*

Packet marking methods mark path information into the packet. The ideal marking information includes: the identity of attacking path, the hop number away from victim(s) or attacker(s), the router address fragments, the group identity of different fragments from the same router, checksum, and so on. However, there is not enough space in the packet to mark information. All possible combinations must be traversed in the process of the path reconstruction at victim(s). Thus, the traceback speed is slow, the computing overhead is heavy, and the traceback result is not accurate enough. In the future, the study on the packet marking will be attributed to the encoding method combined with the characteristics of Internet to a great extent. That is to say, how do we efficiently encode path information in order to reconstruct the attacking path quickly and accurately? In this respect, we can use research findings on source encoding and channel encoding of information theory.

### *C. The Study to Establish the Evaluation Model Based on the Analytic Hierarchy Process (AHP)*

So far, there is no evaluation model in the field of IP traceback to comprehensively evaluate representative traceback methods. It is seemingly difficult to evaluate various methods for IP traceback, because there are many evaluation indexes, and the requirements of end-users are varied. Fortunately, AHP can solve this problem. By means of AHP, the evaluation model can be set up based on multiple evaluation indexes, and the AHP-based evaluation model can be used to quantitatively evaluate various methods for IP traceback according to various requirements of different end-users, and then the relative advantages and disadvantages of these methods can be obtained.

## V. Conclusions

This paper categorizes and describes existing IP traceback approaches, and presents advantages and disadvantages of every category. In addition, this paper induces five evaluation indexes for IP traceback and evaluates six representative traceback schemes. At last, this paper discusses three future research areas on IP traceback.

## Acknowledgement

This work is supported by National Key R&D Program of China (2017YFB0801701), the National Science Foundation of China (No.61472213) and China Postdoctoral Science Foundation under Grant 2015M572723. Jun Bi (junbi@tsinghua.edu.cn) is the corresponding author.

## References

[1] W. Eddy and Verizon, “TCP SYN Flooding Attacks and Common Mitigations,” RFC 4987, August 2007.

[2] R. Vaughn and G. Evron, DNS Amplification Attacks, http://www.isotf.org/news/DNS-Amplification-Attacks.pdf, March 2006.

[3] CERT, Cyber Lightning Case Study, https://www.sei.cmu.edu/research-capabilities/all-work/display.cfm?customel_datapageid_4050=25905, Dec. 2017.

[4] S. Savage, D.Wetherall, A. R. Karlin and T. Anderson, “Practical network support for IP traceback,” Proc. ACM SIGCOMM, pp.295-306, Stockholm, Sweden, August 2000.

[5] P. Ferguson and D. Senie, “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing,” RFC 2827, May 2000.

[6] H. Burch and B. Cheswick, “Tracing anonymous packets to their approximate source,” In Proceedings of 14th Systems Administration Conference, 2000.

[7] D. X. Song and A. Perrig, “Advanced and Authenticated Marking Schemes for IP Traceback,” In Proc. Infocom, 2001.

[8] M. Ma, “Tabu marking scheme to speedup IP traceback,” Computer Networks, vol.50, pp.3536-3549, March 2006.

[9] A. Yaar, A. Perrig and D. Song, “FIT: Fast Internet Traceback,” In Proceedings of IEEE Infocom, 2005.

[10] M.T. Goodrich, “Probabilistic packet marking for large-scale IP traceback,” IEEE/ACM Transactions on Networking, vol.16, pp.15-24, February 2008.

[11] Y. Xiang, WL. Zhou, and MY. Guo, “Flexible Deterministic Packet Marking: An IP Traceback System to Find the Real Source of Attacks,” IEEE Transaction on Parallel and Distributed Systems, vol.20, pp.567-580, April 2009.

[12] A. Belenky and N. Ansari, “Tracing multiple attackers with deterministic packet marking (DPM),” In Proc. IEEE Pacific Rim Conference on Communications, Computers and signal Processing, pp.49-52, August 2003.

[13] V Aghaei-Foroushani and AN Zincir-Heywood, “Deterministic flow marking for IPv6 traceback (DFM6),” Proceedings of the 11th International Conference on Network and Service Management, pp.270-273, Barcelona Spain, Germany, November 2015.

[14] B. Al-Duwairi and G. Manimaran, “A Novel Packet Marking Scheme for IP Traceback,” In Proc. 10th International Conference on Parallel and Distributed Systems, pp.719, July 2004.

[15] D. Dean, M. Franklin and A. Stublefield, "An Algebraic Approach to IP Traceback," ACM Transactions on Information and System Security, vol.5, No. 2, pp.120-137, February 2002.

[16] V Aghaei-Foroushani and AN Zincir-Heywood, “Probabilistic flow marking for IP traceback (PFM),” Proceedings of 2015 7th International Workshop on Reliable Networks Design and Modeling, pp.229-236, November 2015.

[17] Shui Yu, Wanlei Zhou, Song Guo and Minyi Guo, “A Feasible IP Traceback Framework through Dynamic Deterministic Packet Marking,” IEEE Transactions on Computers, vol.65, pp.1418-1427, May 2016.

[18] M Vijayalakshmi, N Nithya and SM Shalinie, “A novel algorithm on IP traceback to find the real source of spoofed IP packets,” Advances in Intelligent Systems and Computing, vol.325, pp.79-87, 2015.

[19] Sangita Roy and Ashok Singh Sairam, “Distributed star coloring of network for IP traceback,” International Journal of Information Security, pp.1-12, March 2017.

[20] Vijayalakshmi Murugesan and MercyShalinie Selvaraj, "UDP based IP Traceback for Flooding DDoS Attack," International Arab Journal of Information Technology, vol.15, pp.103-111, January 2018.

[21] Abdullah Yasin Nur and Mehmet Engin Tozal, "Record route IP traceback: Combating DoS attacks and the variants," Computers & Security, vol.72, pp.13-25, January 2018.

[22] Long Cheng, Dinil Mon Divakaran and Wee Yong Lim, "Opportunistic Piggyback Marking for IP Traceback," IEEE Transactions on Information Forensics and Security, vol.11, pp.273-288, February 2016.

[23] Vahid Aghaei-Foroushani and A. Nur Zincir-Heywood, "Autonomous System based Flow Marking Scheme for IP-Traceback," IEEE/IFIP Network Operations and Management Symposium (NOMS), pp.121-128, 2016.

[24] A.C. Snoeren, C. Alex, C. Partridge, L. A. Sanchez, C. E. Jones, F.Tchakountio, B. Schwartz, S. T. Kent and W. T. Strayer, “Single-packet IP traceback,” IEEE/ACM Transactions on Networking, vol.10, pp.721–734, December 2008.

[25] H. Egon, D. E. P. Jr. and M. Glenn, “Extensions to the source path isolation engine for precise and efficient log-based IP traceback,” Computers & Security, vol.29, pp.383-392, Jun.2010.

[26] L.Zhang and Y. Guan, “TOPO: A Topology-aware Single Packet Attack Traceback Scheme,” Securecomm and Workshops, 2006.

[27] M. S. Andreou and A. Van Moorsel, “Logging based IP Traceback in switched ethernets,” In Pro. European Workshop on System Security, pp.1-7, April 2008.

[28] MM Fadel, AI Eldesoky, AY Haikel and LM Labib, “A low-storage precise IP traceback technique based on packet marking and logging,” Computer Journal, vol.59, pp.1581-1592, November 2016.

[29] S Malliga, CSK Selvi and SV Kogilavani, “Low storage and traceback overhead IP traceback system,” Journal of Information Science and Engineering, vol.32, pp.27-45, January 2016.

[30] A. Mankin, D. Massey and C. Wu, “On Design and Evaluation of Intension-driven ICMP Traceback,” IEEE International Conference on Computer Communications and networks, pp.159-165, October 2001.

[31] Steve Bellovin, Marcus Leech and Tom Taylor, “ICMP Traceback Messages,” Internet Draft, February 2003.

[32] C. Gong and K. Sarac, “A more practical approach for single-packet IP traceback using packet logging and marking,” IEEE Transaction on Parallel and Distributed Systems, vol.19, pp.1310-1324, October 2008.

[33] Yan Dong, Wang Yulong, et al, “A Precise and Pratical IP Traceback Technique Based on Packet Marking and Logging,” Journal of Information Science and Engineering, vol.28, pp.453-470, 2012.

[34] C Shuai, X Ouyang, J Jiang and S Li, “P-CCBFF: A lightweight cooperative detection and traceback framework of DDoS/DoS attacks,” Journal of Internet Technology, vol.18, pp.1147-1158, 2017.

[35] Kamaldeep, Manisha Malik and Maitreyee Dutta, "Implementation of single-packet hybrid IP traceback for IPv4 and IPv6 networks," IET Information Security, vol.12, pp.1-6, January 2018.

[36] R. Stone, “Centertrack: An IP Overlay Network for Tracking DoS Floods,” In Proc. 9th USENIX Sec. Symp., 2000.

[37] F. Audet and C. Jennings, “Network Address Translation (NAT) Behavioral Requirements for Unicast UDP,” RFC 4787, January 2007.

[38] D. Wing and T. Eckert, “IP Multicast Requirements for a Network Address Translator (NAT) and a Network Address Port Translator (NAPT),” RFC 5135, February 2008.

[39] J.Postel, “Internet Protocol,” RFC 791, 1981.

[40] B. H. Bloom, “Space/time trade-offs in hash coding with allowable errors,” Commun. ACM, vol.13, pp.422–426, 1970.

[41] Wikipedia, “False positives and false negatives,” https://en.wikipedia.org/wiki/False_positives_and_false_negatives, January 2018.