Identifying DOS and DDOS Attack Origin: IP Traceback Methods Comparison and Evaluation for IoT

Brian Cusack[1](✉), Zhuang Tian[1], and Ar Kar Kyaw[1,2]

[1] Digital Forensic Research Laboratory, School of Engineering Computer
and Mathematical Science, Auckland University of Technology,
55 Wellesley Street East, Auckland, New Zealand
{brian.cusack,zhuang.tian}@aut.ac.nz

[2] Facuty of Business and Information Technology, Whitireia Community
Polytechnic – Auckland Campus, 450 Queen Street, Auckland, New Zealand
arkar.kyaw@whitireia.ac.nz

Abstract. Society is faced with the ever more prominent concerns of vulnerabilities including hacking and DoS or DDoS attacks when migrating to new paradigms such as Internet of Things (IoT). These attacks against computer systems result in economic losses for businesses, public organizations and privacy disclosures. The IoT presents a new soft surface for attack. Vulnerability is now found in a multitude of personal and private devices that previously lacked connectivity. The ability to trace back to an attack origin is an important step in locating evidence that may be used to identify and prosecute those responsible. In this theoretical research, IP traceback methods are compared and evaluated for application, and then consolidated into a set of metrics for potential use against attackers.

Keywords: Attack origins · DoS · DDoS · TTL · Traceback · IoT security

1 Introduction

A Denial of Service (DoS) attack can be characterized as an attack with the purpose of preventing legitimate users from using some specific network utilities such as a website, web service or computer system [1]. On the other hand, a Distributed Denial Service (DDoS) attack is a coordinated attack on the availability of the service of a given target system or network. It is launched indirectly through many compromised computing systems. The websites used to launch the attack are often called the '*secondary victims'* [2]. The use of secondary victims in a DDoS attack provides an attacker with the ability to launch a much larger and more disruptive attack than a DoS attack while remaining anonymous since the secondary victims actually complete the attack making it more difficult for the digital forensic investigator (DFI) to track down the original attacker. In general, there are two types of flooding attacks [3]: direct and reflector attacks. In a direct attack, an attacker sends a large number of attack packets directly towards the victims. Attack packets can be of Transmission Control Protocol (TCP), Internet Control Message Protocol (ICMP), User Datagram Protocol (UDP) or a mixture of them,

N. Mitton et al. (Eds.): InterIoT 2016/SaSeIot 2016, LNICST 190, pp. 127–138, 2017.
DOI: 10.1007/978-3-319-52727-7_14

for example Internet Protocol (IP) flooding [4], Synchronization (SYN) flooding [5, 6]. A reflector attack is an indirect attack in those intermediary nodes (routers and various servers), also known as '*reflectors*', are innocently used as attack launchers [7]. An attacker sends packets that require responses to the reflectors with the packets' inscribed source addresses set to a victim's address. Without realizing that the packets are actually address spoofed, the reflectors return response packets to the victim according to the types of the attack packets. As a result, the attack packets are essentially reflected in the form of normal packets towards the victim. Consequently, the reflected packets can flood the victim's network if the number of reflectors is large enough.

One reason that spoofing is often facilitated in these and other DoS or DDoS attacks is that it allows evasion of filters and quotas based on sender IP address, making tracing attackers harder [2, 8] reinforce that tracking back attack origin in DDoS attacks is a difficult and non-trivial problem due to the following reasons. Firstly, it is easy to forge or modify IP address (e.g. IP spoofing). Secondly, the stateless nature of IP routing, where routers normally know only the next hop for forwarding a packet instead of the entire end to end path taken by each packet, makes IP traceback even harder. Moreover, the Internet was originally designed for fast file sharing in a trusted environment and the network security was less important than communications, as it was a secondary consideration. Routers do not verify the source address of IP packets and the entire routing table is constructed on a trust basis. However, the wide adoption of these limitations with the dramatic increase of users, attackers can easily exploit IoT vulnerabilities to launch attacks.

[9] state that there are three types of DDoS defense approach mechanisms depending on their locality of deployment. These are: source-end approach (i.e. the detection approach is implemented in the routers of attacker networks), victim-end approach (i.e. the detection approach is implemented in the routers of victim networks) and in-network approach (i.e. the detection approach is implemented in intermediary routers between victim and attacker networks). Detecting a DDoS attack at the victim-end is easy, but often not useful if it is not a real time detection. In-network solutions are not deployable in real network, unless the whole Internet infrastructure is changed. On the other hand, the source-end detection is a very challenging task as a malicious person can launch attacks from anywhere and anytime. So, the best possible practically deployable solution for DDoS attack detection can be a victim-end detection approach which detects attacks in real time while ensuring high detection accuracy. However, the degree of computational complexity for victim-end scheme has to be low in real-time detection. This might again adversely affect the performance in terms of detection accuracy. The ability to trace back to an attack origin is an important step in locating evidence that may be used to identify and prosecute those responsible. IP traceback is to find the origin of malicious attacking packets [10]. Since routers are the core connectivity devices that direct all traffic in the Internet, most of the IP traceback methods have routers in their design. These traceback methods were developed according to various situations and have their distinct features for tracing back to attack origins. Most of them depend on collecting a large number of packets from routers along the attacking path. Without collecting sufficient packets, tracing back is extremely difficult and sometimes impossible. These methods are also resource costly. The full stream of packets from the routers used to reconstruct the attacking path would be required. The objectives of this paper is to

compare and evaluate existing IP traceback methods, present challenges and provide research directions for future work. This paper is organized into five sections including the "Introduction (Sect. 1)", which is followed by a background literature review of traditional IP traceback methods (Sect. 2) to gain contextual knowledge. Section 3 presents the analysis of a number of recent IP traceback methods and limitations. Afterwards, we propose evaluation metrics for IP traceback methods (Sect. 4), which is followed by the conclusion and future work (Sect. 5).

2 Traditional IP Traceback Methods

IP traceback methods are developed and tested for determining the origin of a packet. Each method attempts to exploit technical possibilities in networks but each runs into difficulties. In general, the ability to consistently connect one network entity to another is lost in the architecture and dynamics of the networks. Multicast routing and many-to-many relationship of communications between networks prevent a single solution to fit all traceback requirements. Each attempt to provide a solution demonstrates the strengths and weaknesses of a preferred approach. Usually, unknown relationships (unicast or one-to-one, multicast or one-to-many, and broadcast or one-to-all) and interaction between network hosts (e.g. a web server and a web client) place limits on the effectiveness of any particular approach. Similarly, most of IP traceback methods developed so far have many serious flaws with falsified IP addresses or spoofing. These traditional traceback methods require an enormous number of packets in order to reconstruct malicious packet paths and demand more computational power, storage, deployment overhead, network throughput and effective response time. Hence, the disadvantages far outweigh the benefits and the overall performance does not seem to be sufficient.

Nowadays, most of IP traceback methods belong to five main categories such as link testing hop-by-hop tracing, ICMP messaging, logging, packet marking and hop count filtering [11]. These traceback methods are developed according to various situations and have their distinct features for tracing back to attack origins. Most of these methods depend on collecting a large number of packets from routers along the attacking path. In fact, a full stream of packets from the routers used to reconstruct the attacking path is required. As a result, these methods are also resource costly (Table 1).

Table 1. Traditional IP traceback methods analysis.

Traceback Scheme	Advantages	Disadvantages
Input Debugging [12]	• Using single packet analysis • Allowing post packet analysis • Can be used to against both DoS or DDoS • Bandwidth overhead is very low	• ISP cooperation is high • Time consuming is high • Not scalable for multiple DoS or DDoS attack at the same time • May require court approval

(*continued*)

Table 1. (*continued*)

Traceback Scheme	Advantages	Disadvantages
	• Storage requirement is very low • Computational overhead is very low • No functions needed to implement	
Controlled Flooding [13]	• ISP cooperation is not required • Easy to implement • Can be used to against DoS attack • Storage requirement is very low	• Time consuming is high • Substantial packets required • Bandwidth overhead i.e. it generates additional network traffics • Potentially, can be considered as a small DoS attack • Legal permission may be required • Can only be used during attack • Cannot distinguish DDoS and genuine flash crowed
ICMP [14–16]	• Compatible with existing protocols • Supporting incremental implementation • Allowing post packet analysis • ISP cooperation is not required • Compatible with existing routers and network infrastructure	• Bandwidth overhead i.e. it generates additional network traffic • Less protective as there is no encryption scheme implemented with key distribution
Logging [19–21]	• Compatible with existing protocols • Medium level of ISP cooperation is required • Allowing post packet analysis • Using single packet to reconstruct attack path • Easy to implement	• Substantial storage required • Have potential hash collision • Depending on data storage size and searching algorithms, extra searching time is required • Path reconstruction need to be completed before stored attacking packet being overwritten • Extra computational resources needed for intermedia routers • Reducing network throughputs
Packet Marking [12, 18]	• Low processing • Suitable for a variety of attacks • It does not have inherent security flaws	• Since every router marks packets probabilistically, some packets will leave the router without being marked • It is too expensive to implement this scheme in terms of memory overhead

(*continued*)

Table 1. (*continued*)

Traceback Scheme	Advantages	Disadvantages
	• It does not reveal internal topologies of the ISPs • It is scalable	• One important assumption for PPM to work is that DoS attack traffics will have large volume than normal traffic. However this assumption is not valid when attack is highly distributed for example in reflector attacks • High bandwidth overhead • Costing data fragmentation
Hop Count Filtering [23]	• Compatible with existing protocols • Easy to implementation • Compatible with existing routers and network infrastructure • Allowing post packet analysis • ISP cooperation is not required • Can be used to against both DoS or DDoS • It is feasible for wide deployment • It can be used to detect the attack even when it is over • Bandwidth overhead is very low • Storage requirement is very low	• It cannot identify the very first router, rather just give a possible list • It requires pre-generated map of the internet topology

3 Recent IP Traceback Methods

From the above evaluations, the traditional IP traceback methods have their own advantages and disadvantages. Quite often, they are cumbersome to implement. They either require high computational overhead, data storage or even introduce substantial extra packets on the Internet which can significantly reduce the overall network performance. None of the traditional IP traceback methods can provide high-level performance accuracy with cost-effective benefit. In the past decade, researchers [22, 24–26] have tried to invent several new IP traceback methods by combining/merging various traditional methods together in aiming to provide a fast-single packet traceback result. This section will compare and evaluate these IP traceback methods (Table 2).

Table 2. Recent IP traceback methods analysis.

Trace-back scheme	Advantages	Disadvantages
TTL & DPM [22]	• Suitable for a variety of attacks • It does not reveal internal topologies of the ISPs • It is scalable • Allowing post packet analysis • ISP cooperation is not required • It can be used to trace the attack even when it is over	• Resource incentive in terms of processing and storage requirements • Cannot be used to trace DDoS because DDoS may not generate the minimum amount of packets used for DPM • It is not feasible for wide deployment since it requires all the routers to mark the packet in certain percentage • Since every router marks packets probabilistically, some packets will leave the router without being marked • It is too expensive to implement this scheme in terms of memory overhead • Time consuming as extra encryption and decryption steps introduced
Marking & Logging [24]	• Compatible with existing protocols • Supporting incremental implementation • Allowing post packet analysis • Compatible with existing routers and network infrastructure • It is scalable • Provide single packet traceback capability	• Resource incentive in terms of processing and storage requirements • Sharing of logging information among several ISPs leads to logistic and legal issues • Less suitable for DDoS • Since every router logs packets probabilistically, some packets will leave the router without being logged • It is too expensive to implement this scheme in terms of memory overhead • It requires large packets to reconstruct attacking path
Hop Count & Marking [25]	• Suitable for a variety of attacks • It does not reveal internal topologies of the ISPs • It is scalable • Allowing post packet analysis • ISP cooperation is not required • Can be used to against both DoS or DDoS	• Resource incentive in terms of processing and storage requirements • Medium processing overhead is required • Since every router marks packets probabilistically, some packets will

(*continued*)

Table 2. (*continued*)

Trace-back scheme	Advantages	Disadvantages
	• It is feasible for wide deployment • It requires small number of packets to reconstruct attacking path	leave the router without being marked • It is too expensive to implement this scheme in terms of memory overhead
FDDA [26]	• Using features that are out of control of hackers to conduct IP traceback • It does not suffer from the problem of packet pollution • This model can work as an independent software module with the current routing software which helps in ease in implementation	• This technique does not consider the differentiation of DDoS attacks and flash crowds; it may treat flash crowd as DDoS attack resulting in false positive • It is impossible to determine the location of router • Poor performance

4 Proposed Evaluation Metrics for IP Traceback Methods

The analysis of traceback methods shows that each method uses different techniques to find the original source of attack and the potential location of the attackers. All methods have advantages and disadvantages. To evaluate different traceback methods, the Open Systems Interconnection (OSI) reference model provides an incremental measurement for expectations across the seven layers. The essential task of IP traceback is to find the origin of a particular IP packet traversing the Internet. OSI model can explain the communication expectation through each layer. Protocols serve as the building blocks for the Internet; and different protocols are specifically based on different layers of OSI model. Traceback methods exploit and explore these protocols. Thus, the OSI model also serves as a foundation for benchmarking traceback methods. For example, when data is passed down from layer 7 to layer 1 before being sent to the Internet from source device, each layer encapsulates the data with its header accordingly. These headers contain information about the data as well as the type of protocol being used in accordance with each OSI layer when the data is being passed. Conversely, when the encapsulated data arrives at the destination device, to allow a user to retrieve the information, the data is passed from the lowest layer to the highest layer on OSI model. Moreover, to process the data accordingly, a header will be stripped to enable an appropriated protocol at each layer and pass the remaining data to the level above until it reaches layer 7. The data then will be presented as information understood by user. Therefore, data encapsulated at a lower layer contains more information for traceback exploitation compared with data that has been encapsulated by the layer above. Thus, using the protocols at the lower layer, the more information can be retrieved from the encapsulated data. This also applies to traceback methods. The lower the layer of protocol being used by the traceback method, the more information can be used to find the source of the communication.

On the other hand, the backbone of the Internet consists of routers, switches and physical communication medium connecting all the components of the Internet.

Across different LANs, mostly routers at the Network Layer are processing data. Accordingly, this layer of encapsulated data is known as a packet. Though most proposed traceback methods use different protocols; yet they are all based on the Network Layer. Also, to effectively measure those methods, a set of evaluation metrics should be established. [2] suggest measurement criteria for IP traceback methods, and yet they lack accurate performance evaluation characteristics. Hence, we then propose the following evaluation metrics for IP traceback methods:

- **ISP involvement:** There are no incentives given to the ISPs and enterprise networks to monitor the attack packets and furthermore whether any ISP is involving in traceback method. An ideal traceback scheme should include minimum ISP involvement because the investigation may take longer time and more resources may be required with full co-operation.
- **The number of attacking packets needed for traceback:** IP traceback should able to traceback the attack source based on the packets when the attack has been identified. An ideal traceback scheme should be able to traceback the attacking source with one packet.
- **Processing overhead:** Additional processing overhead for measuring the flow of packets and calculating various statistical parameters are taken placed on the network devices like routers. An ideal traceback method should be able to incur minimal processing overhead during traceback.
- **Storage requirement:** Additional amount of memory is required to store certain information on the network devices to perform IP traceback. An ideal traceback method should be able to acquire a minimum amount of memory in network equipment.
- **Ease of implementation:** IP traceback algorithm is an important part of the solution for stopping DoS and DDoS attacks. These algorithms attempt to approximate the origin of the attack traffic. An ideal traceback method should be designed in such a way that it could be easily implemented at a network layer or application layer.
- **Scalability:** It refers to the amount of extra configuration required on the network devices when implementing a traceback method. An ideal traceback method should be scalable and independent from device manufacturers or vendors.
- **Bandwidth overhead:** Additional traffic that the network must carry for taceback is considered bandwidth overhead. Large bandwidth overhead is undesirable since it may exhaust the capacity of links and routers, forcing the ISP to introduce additional capacity and possibly upgrade or purchase new devices. An ideal scheme should not assume availability of infinite bandwidth.
- **Number of functions needed to implement:** This metric reflects how many different functions a vendor of equipment needs to implement for a given IP traceback method. It is easier for a vendor to implement fewer functions. Ideally, only a single function should be needed for implementation.
- **Ability to handle major DoS or DDoS attacks:** This is an extremely important metric that reflects how well the trackback method can perform the tracing of DoS or DDoS attack under severe circumstances (for instance; many attackers using reflectors or random address spoofing). However, many traceback methods are not able to cope with all types of attacks. An ideal scheme would be able to trace back all malicious attacks (Table 3).

Table 3. IP traceback methods comparison.

Traceback Method	Hop Count Filtering [23]	ICMP [14–16]	Logging [17, 19–21]	Packet Marking [12, 18]	Packet Marking & Logging [24]	TTL & Packet Marking [22]	FDDA [26]
ISP involvement	None	Low	Moderate	Low	None	None	None
No. of attack packets needed for traceback	1	Very Large	1	Very Large	1	Very Large	large
Processing overhead	Very Low	Low	Low	Low	Very Low	Low	High
Storage	Very Low	Low	Low	High	High	High	High
Ease of implementation	Yes	Yes	Yes	No	No	No	No
Scalability	Highest	High	Fair	High	High	Highest	Highest
Bandwidth overhead	None	Low	None	None	None	High	High
No. of functions needed to implement	3	2	3	2	5	5	6
Ability to handle major DDOS attack	Yes	Yes	Yes	Poor	Yes	Yes	Yes
Classification	IDS Based	Proactive	IDS Based	Proactive	IDS Based	Proactive	IDS Based
OSI model layer and protocols	IP, Network Layer	ICMP, Network Layer	IP, Network Layer	IP, Network Layer	IP, Network Layer	IP, Network Layer	IP, Network Layer

5 Conclusion

The review and analysis of traceback methods have been consolidated into a set of metrics that may be applied to enhance and improve the development of IP traceback methods. Many traditional traceback methods demonstrate limitations for practice. The theoretical deduction of solutions has not been enough to address practical problems that are found (for example, potential poor cooperation amongst ISPs). Other methods simply involve too much data that requires excessive storage and processing capabilities. Consequently, further research is required into the development of better algorithms and methodologies for optimizing the trace back to an attack origin. Attempts to mix and merge methods have been successful at reducing the overhead costs and approaching the origin more economically. However even with these more recent attempts at methodology improvement the ideal solution is not yet been established.

The wide adoption of IoT connectivity into people's daily lives everywhere has motivated the necessity of maintaining the integrity of communications. Initially, the Internet was designed for file sharing in a trusted environment. Security was of a lesser concern. Routers were designed so that they did not have to verify a sender's source IP address and the utility value of the internetworks was functionality. The more recent problem has been the exploitation of these global communication channels for criminal and terrorist purposes. Many of the advantages developed for efficient communication have been hijacked and are easy to exploit. For example, the vulnerability exploitation of DoS or DDoS attacks and the hiding of true IP addresses. These matters impact the integrity of IoT developments.

Another challenge is that most of the existing IP traceback methods are specifically designed for an Internet Protocol version 4 (IPv4) environment. However, IPv4 will become unsustainable in 2017 or 2018, and cannot meet the demand of IoT. IPv6 is capable for IoT and supports an IP address demand of 2^{128}. Currently, IPv6 packets are accounting for less than 2% of all Internet traffic. By far, only a few of research reports [27–30] are reported in IPv6 environment using the packet marking method. These proposed methods inherit the fundamental design flaws from the packet marking method reviewed in this paper. Thus, to design better performing traceback methods is urgent and a challenge for researchers for future work. This paper has contributed a consolidation of current literature and proposed a metric basis for further study.

References

1. Specht, S., Lee, R.: Distributed denial of service: taxonomies of attacks, tools and countermeasures. In: International Conference on Parallel and Distributed Computing Systems, pp. 543–550. San Francisco, CA, USA: CiteSeerX (2004)
2. Kumar, K., Sngal, A., Bhandari, A.: Traceback techniques against DDoS attacks: a comprehensive review. In: 2011 2nd International Conference on Computer and Communication Technology (ICCCT), pp. 491–498. IEEE, Allahabad, India (2011)
3. CERT Coordination Center.: Cert Advisories: CA-2000-01 denial of service developments. CERT Software Engineering Institute. http://www.cert.org/historical/advisories/ca-2000-01.cfm (2015)
4. Chen, T., Tsai, J., Gerla, M.: QoS routing performance in multihop, multimedia, wireless networks. In: IEEE 96th International Conference on Universal Personal Communications Record, vol. 2, pp. 557–561. IEEE, San Diego (1997)
5. Eddy, W.: TCP SYN flooding attacks and common mitigations, RFC4987. IETF: https://tools.ietf.org/html/rfc4987 (2007)
6. Lemon, J.: Resisting SYN flood DoS attacks with a SYN cache. In: 2nd European BSD Conference, pp. 89–98. Amsterdam, The Netherlands: USENIX (2002)
7. Paxson, V.: An analysis of using reflectors for distributed denial-of-service attacks. ACM SIGCOMM Comput. Commun. Rev. **31**(3), 38–47 (2001)
8. Gilad, Y., Herzberg, A.: LOT: a defense against IP spoofing and flooding attacks. ACM Trans. Inf. Syst. Secur. **15**(2), 6 (2012)

9. Kashyap, H., Bhattacharyya, D.: A DDos attack detection mechanism based on protocol specific traffic features. In: Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology, CCSEIT 2012, pp. 194–200. ACM, New York (2012)
10. Yao, G., Bi, J., Vasilakos, A.: Passive IP traceback: disclosing the locations of IP spoofers from path backscatter. IEEE Trans. Inf. Forensics Secur. **10**(3), 471–484 (2015)
11. Ho, C.: Email forensics: tracing and mapping digital evidence from my address. Unpublished Master's Thesis (2010)
12. Savage, S., Wetherall, D., Karlin, A., Anderson, T.: Network support for IP tracback. IEEE/ACM Trans. Netw. **9**(3), 226–237 (2001)
13. Burch, H., Cheswick, B.: Tracing anonymous packets to their approximate source. In: Proceedings of the 14th USENIX conference on System Administration, LISA 2000, pp. 319–328. Berkeley, CA, USA: USENIX Association Berkeley (2002)
14. Bellovin, S.: ICMP Traceback Messages. Internet Draft: draft-bellovin-itrace-00.txt (2002)
15. Lee, H.C.J., Thing, V.L.L., Xu, Y., Ma, M.: ICMP traceback with cumulative path, an efficient solution for IP traceback. In: Qing, S., Gollmann, D., Zhou, J. (eds.) ICICS 2003. LNCS, vol. 2836, pp. 124–135. Springer, Heidelberg (2003). doi:10.1007/978-3-540-39927-8_12
16. Izaddoost, A., Othman, M, Rasid, M.: Accurate ICMP traceback model under DoS/DDoS attack. In: Proceedings of the 15th International Conference on Advanced Computing and Communications, ADCOM 2007, pp. 441–446. IEEE Computer Society, Washington, DC, USA (2007)
17. Sager, G.: Security fun with OCxmon and cflowd. Presentation at the Internet 2 Working Group (1998)
18. Song, D., Perrig, A.: Advanced and authenticated marking schemes for IP traceback. In: Proceedings of Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM 2001, vol. 2, pp. 878–886. IEEE, Anchorage, AK, USA (2001)
19. Snoeren, A., Partridge, C., Sanchez, L., Jones, S., Tchakountio, F., Schwartz, B., Kent, S., Strayer, W.: Single-packet IP traceback. IEEE/ACM Trans. Netw. **10**(6), 721–734 (2002)
20. Ponec, M., Giura,P., Brönnimann, H., Wein, J.: Highly efficient techniques for network forensics. In: Proceedings of the 14th ACM Conference on Computer and Communication Security, CCS 2007, pp. 150–160. ACM, New York (2007)
21. Sung, M., Xu, J.J., Li, J., Li, L.E.: Large-scale IP traceback in high-speed internet: practical techniques and information-theoretic foundation. http://www.cc.gatech.edu/∼mhsung/pub/ddos_sp.pdf (2008)
22. Devasundaram, S.: Performance evaluation of a TTL-based dynamic marking scheme in IP traceback. University of Akron, Akron (2006)
23. Wang, H., Jin, C., Shin, K.: Defense against spoofed IP traffic using hop-count filtering. IEEE/ACM Trans. Netw. **15**(1), 40–53 (2007)
24. KrishnaKumar, B., Kumar, P., Sukanesh.: Hop count based packet processing approach to counter DDoS attacks. In: International Conference on Recent Trends in Information, Telecommunication and Computing (ITC), pp. 271–273. IEEE, Kochi (2010)
25. Yang, M., Luo, J.: High accuracy and low storage hybrid IP traceback. In: 2014 International Conference on Computer, Information and Telecommunication Systems (CITS), pp. 1–5. IEEE, Jeju (2014)
26. Park, P., Yi. H., Hong, S., Ryu, J.: An effective defense mechanism against DoS/DDoS attacks in flow-based routers. In: The 8th International Conference on Advances in Mobile Computing and Multimedia, pp. 442–446. ACM, Paris (2010)

27. Dang, X., Albright, E., Abonamah, A.: Performance analysis of probabilistic packet marking in IPv6. Comput. Commun. **30**(16), 3193–3202 (2007)
28. Michiko, H., Naoyuki, K., Daisaku, T.: Implementation of probabilistic packet marking for IPv6 traceback. IPSI BgD Trans. Internet Res. **1**(1), 54–58 (2005)
29. Amin, S., Hong, C., Kwak, D., Lee, J.: IPv6 traceback using policy based management system. Korean Netw. Oper. Manag. **9**(2), 1–7 (2006)
30. Yan, Q., He, X., Ning, T.: An improved dynamic probabilistic packet marking for IP traceback. Int. J. Comput. Netw. Inf. Secur. **2**(2), 47–53 (2010)