Indian Journal of Science and Technology, *Vol 9(47), DOI: 10.17485/ijst/2016/v9i47/95630, December 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A Review on Various DPM Traceback Schemes to Detect DDoS Attacks

S. Suresh[1]* and N. Sankar Ram[2]

[1]Sathyabama University, Jeppiaar Nagar, Chennai - 600119, Tamil Nadu, India;
m.suresh.suresh@gmail.com
[2]Department of Computer Science and Engineering, RMK College of Engineering and Technology, Puduvoyal, Thiruvallur - 601206, Tamil Nadu, India;
n_sankarram@yahoo.com

Abstract

Objectives: Network security deals with the various attacks, in which distributed denial of service (DDoS) is a kind of attacks are thriving every day in networks. The specified users of node or theirs network information's are hidden by Denial of Service (DoS) attack. The aim is to detect the source of attack using improved marking schemes. **Method:** The nodes and networks are very often affected by the Distributed Denial of Service attack (DDoS) from the category of DoS attack. The affected path of DDoS attacks are identified by various IP trace back schemes. Packet marking approach is one type to detect the source of attack from the identified node. **Finding:** PPM and DPM techniques were used to detect the DDoS attack but the performance should be improved in both marking scheme. In DPM marking process done by ingress router to avoid marking process in subsequent egress router. Further DPM is improved with hash functions which is also an overloaded in router. MOD server concepts are used to increase the scalability using Dynamic DPM approach. **Improvement:** To reduce the trace back mechanism procedure and to concern about the memory requirement using Enhanced DPM and DADPM method is considered when detecting the source of attack from the victim node.

Keywords: DADPM, DDoS, DPM, IP Trace back, MOD Server, Source of Attack

1. Introduction

The server process interruption is happening mainly due to DoS (Denial of service) attack. It is strongly reflecting and disturb the legitimate user's valuable services. Intolerable identified node and hiding the information of hackers are two major goals of DoS. The line of attack is required by attacker for using less resources causes also adds more critical step at the victim side. In day today internet services, attacks are unavoidable one in which Distributed denial of service DDoS is very vulnerable attack. DDoS attacks are watchful and complicated to counter, IP networks should be monitored carefully because it is circulated in entire Internet. To differentiate attack traffic from regular traffic is quite complex task, which leads problem[1,2].

Among all types of attack presence in the network, the DDoS attack is one in which detection is a complex process. Three factors of DDoS attacks are not measured which are range, survival and severity. Many methods are existing to detect DDoS attacks and it is found from various sources, paths and flows of network[1,3]. There are different

*Author for correspondence

major types: preventing intrusion, detecting intrusion and intrusion IP trace back. A method to identify the origin of attack packets from the reply from intrusion is called as IP trace back. IP trace back can be classified into two categories: They are 1. DPM-(Deterministic Packet Marking) 2. PPM Probabilistic Packet Marking is considered to be main procedure. Continuous upgraded version of PPM came and changes are analyzed in PPM. The PPM method needs to be updated in several aspects such heavy calculation load, many false results, spoofing etc. The DPM marking introduced to find the attack source better than PPM. The advantages are clearly stated and it is observed in DDoS attacks of big networks[3,4].

The main focus of tracking IP address is finding its sender through the reverse path from victim node. To record the packet digests, to see the transparency of storage and required condition of access time speed router is essential. Tracking the IP address of attack source identified by packet marking scheme adds an additional workload to the router due to heavy flow of packets[5].

Incorrect path can be found in easy manner when an illegitimate user knows the original IP address of legitimate user. Legitimate sender address can be stored by methodology of tracing the reverse for routers at detached WL reserving gadgets, plays out the development of the assault chart inside a narrow space, and gives a connectivity to inter domain assistance to find the system direct closest toward the attack source. There are two different ways to concern with the Non-Intrusive IP Trace back plan namely Network Segmentation Based (NSB) and Strategic Points Based (SPB) schemes. The concentration is separating system with WL device of other portion. The reducing capacity of the routers monitored and inside systems are arranged properly by the second approach[6].

RIHT is a hybrid trace back mechanism which deals with logging and marking process by marking router's interface number and it contains logging of packet with a hash table. To reach the given properties, the various types of IP trace back combined to form RIHT trace back procedure: 1) Each router must have storage together the different paths to the router, and Renew logged tracking information process is not necessary by entire routers involved in network 2) There is no false positive and false negative rates achieved in path of reconstruction 3) Reconstruction of path has better competence in RIHT 4) Attack traffic is easily suppressed by this marking scheme[7].

Edge router packet marking process to be done by Deterministic Packet Marking (DPM). IP header includes 16 bit of Packet Identity Field and 1 bit of Reserved Flag for packet marking process in this DPM scheme. This scheme marks all the packets which are passing into the network[8]. Arranging the various nodes presence in the network plays an important role by DPM trace back procedure. It always to be considers that the node arrangement is moving forward in the network. Hash function is applied to the IP address of incoming routers whenever packet marking process is done. Hash value generated by the hash function is segregated and splits into different value and it is marked to packets by randomly. The topology structure is known by the victim node then it becomes easy procedure to tracking back to the origin. The less number of packets are used for trace back procedure but searching of source takes more time to detect it in this procedure. Trace back will become difficult when sudden changes in arrangement of nodes[9].

DPM is an easiest mechanism to track the source of attack than other schemes, due to considering the characteristics of scalability DPM method is not suitable for trace back procedure. Instead of marking entire resources are available in the network only less number of nodes and routers marked which are participated in attack session as mentioned in current scheme. The above circumstance leads a further improved decision; The new DPM scheme named as MOD (novel marking on demand) trace back procedure. MOD server represents one type of marking reacting to the urgent needs. The online database of MOD server, which stores the imprint data for possible data recovery[10].

2. Organization

The information of this paper is structured in following manner: Section 3 deals about Methodology which describes about the various techniques of marking schemes. Section 4 deals with the comparison on DDoS detection and packet marking scheme. Finally, Section 5 analyzes the various deterministic packet marking schemes. Finally, Section 6 concludes the paper.

3. Methodology

The motivation behind the mechanism of tracking back IP address is used to identify the origin of attack from the specified node in network. DDoS attacks very much vulnerable in the current internet. With the assistances

of IP trace back methodology, it is simple to discover the source of DDoS attack[11]. DDoS attacks can be tracked to use three approaches namely the mechanism of Proactive, Reactive and Survival. IP Trace back is the method under the Reactive Mechanism. Identifying the origin of attacks from victim node once it is involved in the existing network is known as Reactive mechanism. Packet Marking Scheme is a solution based method to identify the illegitimate sender address[12,13].

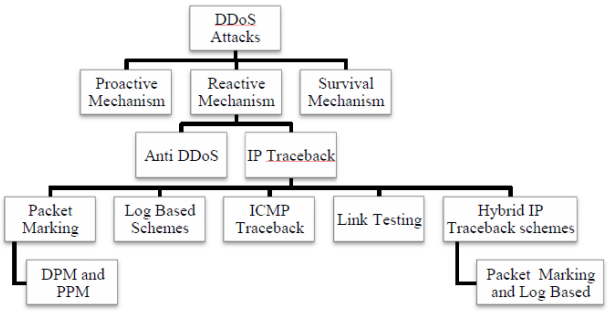
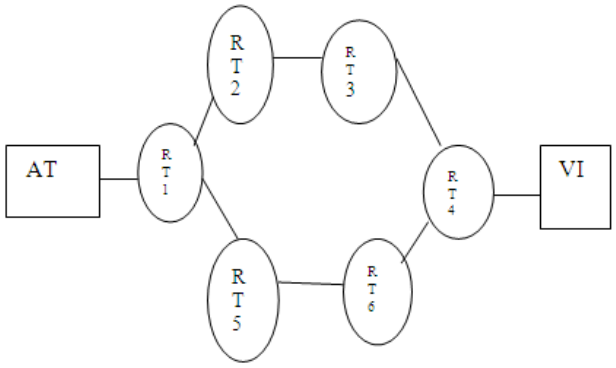


Figure 1. Various traceback schemes.

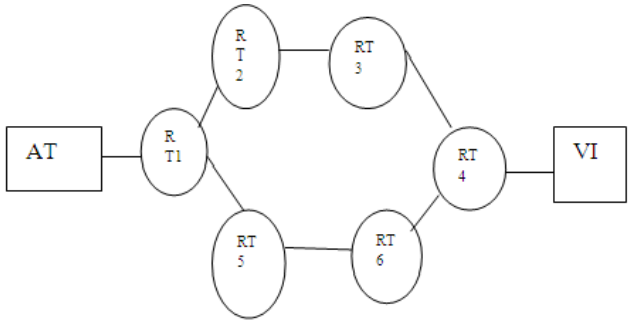
There are 2 categories in scheme of Packet Marking. They are 1. PPM –Probabilistic Packet Marking scheme. 2. DPM- Deterministic Packet Marking scheme. The following Figure 2 represents the concept of PPM



AT-Attacker VI-Victim Reconstructed path **RT4-RT3-RT2-RT1** from marked packets of each router.

Figure 2. PPM-marking scheme.

The router is marking all the packets that go through the with their locations and a portion of its locations or edge. Those changed packets are dissected at the casualty path for way recreation. The PPM introduced to identify DoS and DDoS attack because it requires various attack packets from the victim node to regenerate the complete path in network[14].



AT-Attacker VI-Victim Marking all packets in ingress router **RT1, RT4.**

Figure 3. Deterministic Packet Marking (DPM).

To overcome the problems arises in PPM, marking process is done only at incoming router present in first alone marked by the deterministic packet marking scheme[14]. In random manner the entire incoming packet stores the detail and IP address is split by two different 16 bits segments each. When an identified node receives two 16 bits of the same incoming router, IP address detection is possible by victim node[15].

DPM procedure was unsuccessful the IP address of origin node is spoofed and when it is set false positive. When an IP address is located more number of pieces, the given plan is expected improvement and the character of entry router will lead productive false reduction by a capacity of hash function. For repeated break down DPM is further improved and it is named as FDPM. The knowledge of node arrangement plays an important role in DPM scheme's trace back. Flexible Deterministic Packet Marking (FDPM) scheme, the marking field length is changed depends on the requirement and it is adjustable. The marking rate is modified and acceptable depends on current router flow of traffic. The minimum resource requirements and less rate of false positive produced by FDPM are used to trace back highest number of resources.

Another improved method of marking procedure of IP trace back is DFM. DFM mean all the stream, (All streams K first packets), as replace for every group, to concentrate on connecting of "DPM method clarity on huge trace back " and "verifying the combined packets" of PPM. The trace back of attack origin node from the LAN followed by edge router is the key focus of DFM procedure. Finally, DFM method consists three IDs to check the flow (i) IP address of egress interface in Edge

router (ii)Network interface identifier which identifies to use the entire interface of both device and VLAN interface of the MAC locality on the border router or the edge router virtual interface identifier of VLAN (iii) An identifier(Node-ID) represents to all the source MAC address saw on forthcoming movement from nearby systems[15,16].

The unique marks will be given to corresponding needs by Global MOD server and the MOD server also maintains a database in the web, which recovers information of marking details. The possible attack may not be monitored by R_k router because of threshold value or finding reaction. Router R_j can be able to identify uncertain flows but attack verification is not possible because it is coming from different attack) So Rj considers this flow as doubtful flows, and it starts packet marking procedure with sets off the alarm. With the sudden increase amount of attack flows, finally, router Ri discovers the attack mentioned in Figure 4[10].

The different packet marking schemes were discussed to find the source of attack. The PPM, DPM, FDPM, DFM and marking on insist to discover the DDoS attack using trace back mechanism. Like round robin method MOD scheme rotation based marking by considering the scalability constraint problem in DPM and FDPM when tracing more number of resources. It requires 32 marked attack packets for finalizing source of attack from victim node to find all possible sources of attack in DPM and the FDPM trace back scheme. MOD scheme helps with one packet to trace back to the source.

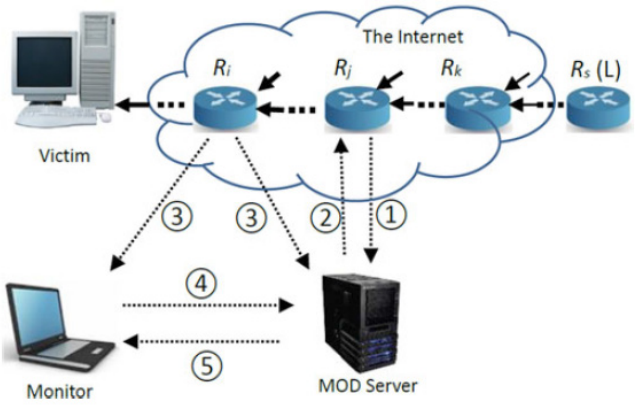


Figure 4. Marking on demand scheme traceback.

4. Comparisons on Various DDOS Detection Method, Packet Marking Scheme

The Comparisons on various method of trace back scheme gives an idea from by following evaluation metrics. The evaluation metrics considered are scalability, memory requirement, router processing overhead, parameter required in trace back[12,17,18].

The Table1 speaks to the comparison examination of various schemes. The scalability and router processing overhead can be improved in various marking scheme. scalability and memory requirement are the very important factors in network[19]. If we add more number of nodes in existing network performance can be degraded than

Table 1. Evalaution based metrics for different schemes of trace back

Measurement criteria for evaluation	Result of testing link	Process of packet marking	Packet Log	Tracing ICMP	other combined schemes
Scalability constraint	No expected result	No expected result	Fair expected result	Good expected result	Fair expected result
memory necessity of Network and Victim	Not Required	Not Required	Very High	Not Required	Low
	Not Required	Medium	Not Required	Medium	Not Required
router processing overhead	High	Medium	High	Low	Low
parameter required	Huge packets and attack pattern	Less and high number in packets mapped	1 packet	Numbers of ICMP messages and high attack packets.	Only 1 packet

previous performance[12]. The comparisons of two basic marking schemes are PPM and DPM[20,18].

Table 2. Comparison over PPM with DPM

PPM	DPM
Packets marking in each router by random probability	Packets marking in edge router by fixed probability
Large no of packets are need for reconstruction	Less no of packets are need for reconstruction
More burden in infrastructure	Less burden in infrastructure
Memory requirement is high	Memory requirement is less

The scalability and memory requirement in router processing are improved in DPM. Further these two evaluation metrics are considered to improve the performance in tracking the sender of attack from the victim node.

5. Analysis on Different DPM

Marking and recovery algorithm are two key factors to differentiate DPM-RD (DPM Redundant and Decomposition) with DPM. The marking field in earliest DPM technique includes address section, processing value and key value is used to store information. It is diminished into two sections which are called as information and key value in DPM-RD procedure. Information section can be able to store address fragment or values of correlation function. All incoming edge router Rin splits n section of its IP address and IP identity field takes at random and marks one of them[3,21].

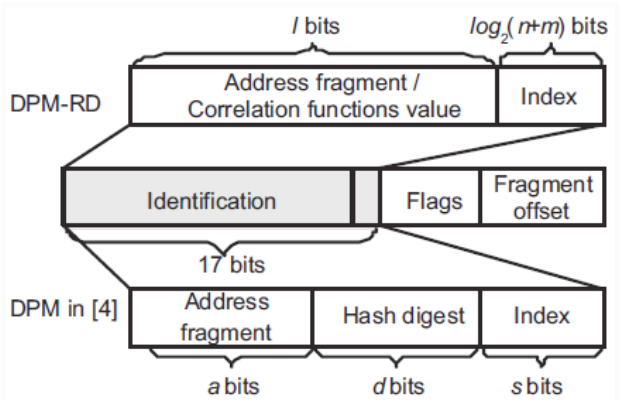


Figure 5. DPM and DPM-RD marking fields

IP header of the FDPM (Flexible DPM) trace back mechanism uses a scope of bits (called marks). Adaptable marking length procedure is used to mark flexible lengths depend upon the system conventions utilized. An interface nearby origin packet of router in the edge separates the packets of IP which are entering into the network system. The origin of IP address is always segregates from Checking fields. When the packet arrivals into the system marking process won't be composed again by routers which are located in intermediate and target process has, the IP address of sender locations can be remade inside the system when its required at all time. Memory and CPU takes more time in process of packet handling[22].

In Figure 6, the adaptability of FDPM has two significances. The flexible mark length is mentioned in the internet by the system conventions that are utilized as a part is considered first.

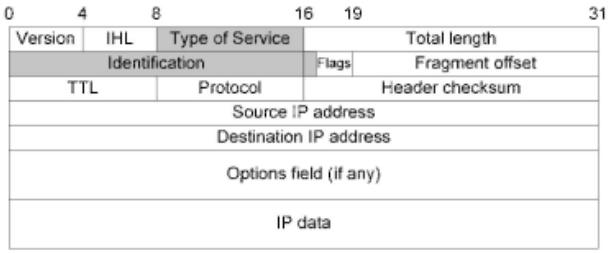


Figure 6. Marking field in FDPM.

It leads a result in heterogeneous network can be facilitated by the FDPM trace back procedure. Second, FDPM can adaptively confirm its monitoring technique to gather an adaptable marking rate. These above procedures solve the issues of trace back procedure better than other schemes[22].

When router encounters a problem with sudden surge flow traffic a FDPM (flow based marking) is mainly mark the packets mentioned in the flow. Trace back mechanism monitors the processor available in router[19]. The packet marking process in router will attempt to reduce it at the same moment it monitors the marking and trace back function[22].

When the router exceeds the current load, the router should slow down rate of marking so as to change its capacity with another. Always most of the time that the packets are lay down apart in an arbitrary way (If not mentioning the possible attack packets then all packet have the similar probability to be noted), to differentiate

various flow based packet marking process the victim node which regenerate the path of source takes more number of packets.

FDPM is appropriate methodology to follow and identify the illegitimate users IP address of DDoS attack and DDoS detection FDPM suitable than other tracking procedure. The standard normal for DDoS is to utilize the various attacking sources to assault a private casualty (the growth trademark). If sudden increase in flow of packets with the same destination address in this manner, anytime and the same collection of digest marks, it denotes the possible identification of a DDoS attack. Subtler elements can be found in[2,23].

Minimum number of packets is needed to trace back procedure in DFM when compare to other schemes.DFM procedure determines the percentage of packet marking by edge router from calculated number of packets of both trace back procedures to find the result calculation. DFM trace back scheme totally eradicate the risk of IP spoofing and attacker involved in spoofed marking process. It is also not concern attack path of compromised routers. It depicts that it can be using optional authenticated marking flow of network. In large scale network, the performance of DFM is better than DPM to deal with DDoS attack, because DPM is limiting the surge flow in number of sequence attackers, Whereas DFM does not have these limitations[15,16]. The comparisons of DPM and DFM is given in the following Table 3[15].

Table 3. Comparisions on DPM and DFM

Evaluation metrics	DPM	DFM
Mark Spoofing in router	Available	Not available
Routers and victim computational overhead	Less	Normal
Routers and victim Memory Overhead	Less	Less
Trace back required packets	8	2 or 5
DDoS attacks handling	Normal only, The Maximum Number of parallel Attackers is limited	It can handle effectively

To consider scalability constraint factor in mind, the various DPM based trace back schemes are not practical[24]. We observed an another factor that only very limited number of devices and routers are involved while in attack session of DDPM (Dynamic DDPM) a novel Marking On Demand (MOD) trace back method on the DPM[10]. In order to trace back to involved attack source, there is a need to mark these concerned ingress routers using the traditional DPM trace back mechanism. The various existing schemes stated that require concerned routers to establish a traffic monitor. The following Figure 7 represents the various fields in MOD

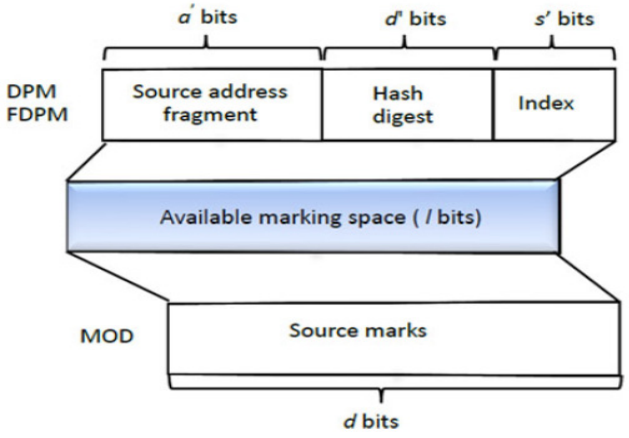


Figure 7. Marking field in MOD.

When a monitor identifies a sudden data forward of distrustful network flows, it will appeal a unique mark from a commonly shared MOD server in the network, and mark the distrustful flows with the unique marks. Simultaneously, the MOD server start records the information of the marks and their connected requesting IP addresses. If DDoS attack is confirmed in the network, the victim can obtain the attack source to the MOD server with the marks taken from attack packets. The marking field is represented in above Figure 6[10].

Table 4. Comparisons on DPM, FDPM and DDPM

Evaluation metrics	DPM	FDPM	DDPM
Scalability	Extremely limited	Very limited	Unlimited
Maximum traceable resources	Extremely limited	Very limited	Unlimited
Working Mode	Individual	Individual	Global
Storage	High	High	Low
False positive	Inherent	Inherent	Non-Inherent

Marking on demand based DPM scheme performs better than all above mentioned various deterministic marking scheme in some of evaluation metrics.

6. Conclusions

In PPM the packet marking process is done in probability based and the all routers are involved in marking process.DPM is introduced to mark all packets and ingress routers are involved in marking process rather than other routers. We observed that many evaluation metrics can be improved in aspects of performance when we trace back of attack source from victim.

Further many improved versions of DPM discussed like DPM-RD, FDPM, DDPM and Flow based DPM. All above mentioned marking schemes were given better performance than the previous scheme. Finally, DDPM is improving the scalability ratio when compared to other schemes. Since we are doing marking process and hash function in edge router, it gives additional over load to the routers. When number of nodes increased and involved in breaking the network, it is quite difficult to deal in IP trace back. We are going to implement the DADPM algorithm in edge routers to reduce the memory overhead problem and simplify the trace back procedure in simple manner.

7. References

1. Chen S, Song Q. Perimeter-based defense against high bandwidth DDoS attacks, IEEE Transactions On Parallel and Distributed Systems. 2005 Jun; 16(6):526–37.
2. Achar RK, Babu MS, Arun M. Border gateway protocol performance and its protection against disturbed denial of service attack. Indian Journal of Science and Technology. 2015 Jan; 8(S2). DOI: 10.17485/ijst/2015/v8iS2/59169.
3. Jin G, Yang J. Deterministic packet marking based on redundant decomposition for IP traceback. IEEE Communications Letters. 2006 Mar; 10(3):204–6.
4. Uddin M, Alsaqour R, Abdelhaq M. Intrusion detection system to detect DDoS attack in Gnutella hybrid P2P network. Indian Journal of Science and Technology. 2013 Feb; 6(2). DOI: 10.17485/ijst/2013/v6i2/30585.
5. Gong C, Sarac K. A more practical approach for single packet ip traceback using packet logging and marking. IEEE Transactions on Parallel and Distributed Systems. 2008 Oct; 19(10):1310–24.
6. Thing VLL, Sloman M, Dulay N. Locating network domain entry and exit point/path for DDoS attack traffic. IEEE Transactions on Network and Service. 2009 Sep; 6(3).
7. Yang M-H, Yang M-C. RIHT: A novel hybrid IP traceback scheme. IEEE Transactions on Information Forensics and Security. 2012 Apr, 7(2):789–97.
8. Florance G. Survey of IP traceback methods in Distributed Denial of Service (DDoS) attacks. International Journal of Innovative Research in Science, Engineering and Technology. 2015 Jul; 4(7):6319–25.
9. Gibish S, Babu PU. Survey of IP traceback mechanisms to overcome DoS attacks. International Journal of Advanced Research in Computer and Communication Engineering. 2015 Dec; 4(12):427–30.
10. Yu S, Zhou W, Guo S, Guo M. A feasible IP traceback framework through dynamic deterministic packet marking. IEEE Transactions on Computers. 2016 May; 65(5):1418–27.
11. Ahamad T, Aljumah A. Detection and defense mechanism against DDoS in MANET. Indian Journal of Science and Technology. 2015 Dec; 8(33). DOI: 10.17485/ijst/2015/v8i33/80152.
12. Murugesan V, Shalinie M, Neethimani N. A brief survey of IP traceback methodologies. 2014; 11(9):197–216.
13. Sharifi AM, Amirgholipour SK, Alirezanejad M, Aski BS, Ghiami M. Availability challenge of cloud system under DDOS Attack. Indian Journal of Science and Technology. 2012 Jun; 5(6). DOI: 10.17485/ijst/2012/v5i6/30488.
14. Youm H-Y. Overview of traceback mechanism and their ability. IEICE Transactions on Information and Systems. 2011; E94.D(11):2077–86.
15. Aghaei-Foroushani V, Zincir-Heywood AN. On evaluating IP traceback schemes: A practical perspective. 2013 IEEE Security and Privacy Workshops; 2013. p. 127–34. DOI 10.1109/SPW.2013.13.
16. Aghaei-Foroushani V, Zincir-Heywood AN. IP traceback through (authenticated) deterministic flow marking: An empirical evaluation. EURASIP Journal on Information Security. 2013; 5:1–24.
17. Singh K, Singh P, Kumar K. A systematic review of IP traceback schemes for denial of service attacks. Elsevier Computers and Security. 2016; 56:111–39.
18. Kiremire AR, Brust MR, Phoha VV. Using network motifs to investigate the influence of network topology on PPM-based IP traceback schemes. Computer Networks. 2014; 72(2014):14–32.
19. Srinath SL, Pillai AS. Adaptive interplay of DVS and DPM for power consumption reduction in real-time embedded processors. Indian Journal of Science and Technology. 2016 Aug; 9(30). DOI: 10.17485/ijst/2016/v9i30/99038.

20. Parashar A, Radhakrishnan R. A review of packet marking IP trace back schemes. International Journal of Computer Applications. 2013 Apr; 67(6):15–20.
21. Belenky A, Ansari N. Tracing multiple attackers with Deterministic Packet Marking (DPM). Proceeding IEEE IEEE Pacific Rim Conference on Communications, Computers and Signal Processing; 2003 Aug. p. 49–52.
22. Xiang Y, Zhou W, Guo M. Flexible deterministic packet marking: An IP traceback system to find the real source of attacks. IEEE Transactions on Parallel and Distributed Systems. 2009 Apr; 20(4):567–80.
23. Xiang Y, Zhou W. Mark-aided distributed filtering by using neural network for DDoS defense. Proceeding IEEE Global Telecommunications Conference (GLOBECOM); 2005.
24. Devi BSK, Subbulakshmi T. A comparative analysis of security methods for DDoS attacks in the cloud computing environment. Indian Journal of Science and Technology. 2016 Sep; 9(34).