Flexible Deterministic Router and Interface Marking for IP Traceback

Varsha Mittal
Department of Computer Application,
Graphic Era University,
Dehradun, India

Emmanuel S. Pilli
Department of Computer Science and Engineering,
Graphic Era University,
Dehradun, India

R.C. Joshi
Department of Computer Science and Engineering,
Graphic Era University,
Dehradun, India

ABSTRACT
IP traceback involves identifying the actual source of a packet across the Internet. By identifying the real source address in packets, network security system can smartly protect the victim hosts and mitigate the attacks. Packet marking is the most important method of source identification using IP traceback and there are many variations. In this paper, we propose a modification to our previous capable IP traceback scheme, Deterministic Router and Interface Marking (DRIM), to handle fragmented traffic as well. The modification introduces nominal additional bandwidth overhead, with no additional memory requirements and processing overhead on the DRIM-enabled interface and also reduces the problem of false positives. The proposed technique is compared with similar traceback techniques against various performance metrics and is found to be efficient.

General Terms
Security

Keywords
Traceback, Packet Marking, Router, Interface, Fragmentation.

1. INTRODUCTION
The source identification is a non trivial task as the source address in IP header can be spoofed easily because of the limitation in Internet Protocol (IPv4). The routing infrastructure of the Internet is stateless and packet routing decisions are based on the destination. The source destination can easily be manipulated as there is no mechanism existing to ensure the correctness of the source address. Using any arbitrary source address, malicious IP packets can be generated by the attackers.

IP Traceback is a method for reliably determining the origin of a packet on the Internet. Identifying the source of the offending packets does not necessarily identify the actual attacker [1]. The source of these packets may be a host in a stepping stone chain controlled by the attacker or the packets may have been reflected. IP traceback techniques are used for the identification of the source(s) of the malicious packets while the attack is in progress or after the completion of the attack. However, these methods cannot stop, detect or prevent the attacks. These techniques are also limited as the source address may be behind a firewall or is network address translated. IP traceback is limited to identifying the point where the packets constituting the attack entered the Internet. The router through which the packets entered the network is the closest point of access to the attacker.

IP traceback can be a major component of a network forensic investigation. It is easy for a forensic investigator to narrow down to a particular host / sub network once the source network is identified by the traceback technique. The reconstruction of the path back to the attack origin is a challenging task. Various marking schemes have been proposed to mark the packets and make the reconstruction of the path back to attack origin possible.

Fragmentation is a feature of Internet Protocol (IP) to enable transport of packets across the networks with different Maximum Transfer Unit (MTU) [2]. All networks have the different MTU, whenever a packet enters a network and the MTU of that network is smaller than the packet length, the packet is fragmented. Each packets' payload is divided into many parts and packet fragment refers to a packet containing a portion of the payload. A series of packets which are an ordered collection of fragments are obtained as a result of fragmentation.

Each packet fragment is a valid IP packet with its own header. Almost all the fields of the fragmented packets are same as of the original packet. The fields which are to be considered for fragmentation are the ID field, Flags, and Offset. The value of the ID field is same in all the fragmented packets and the values taken from the original datagram. The ID field of all the fragments, which result from the original packet have same value in the ID field for proper reassembly. The More Fragments (MF) flag is set to '1' in every fragment indicating that more fragments follow. The last fragment has MF set to '0' to indicating that it is the last fragment. Finally, the offset field of the IP header is set to the position of the data in the fragment with respect to the beginning of data in the original datagram.

The fragments may come out of order but reassembly will still be successful because the destination would be able to determine that the fragment belongs to a given series using the ID field, the number of fragments using MF field and its position relative to other fragments using the Offset value. Successful reassembly of the original packet is possible only when the destination gets all the fragments.

Fragmented traffic constitutes between 0.25% according to [3] and 0.5% of the total IP traffic according to [4]. Though the amount of fragmented traffic is small, it does exist. Deterministic and Router Interface Marking (DRIM) [5], our previously proposed IP traceback scheme, is scalable and capable of tracing back attacks, which are composed of just a few packets. However, the basic DRIM proposal did not differentiate between fragmented and non-fragmented traffic. The Identification (ID) Field and the Offset field of the IP header were used to store the ingress routers' IP address and the interface on which the packets reach the router.

In this article we present a modification to DRIM to address the problem of fragmented traffic. In the proposed scheme, whenever the packets are being fragmented, the option field of IP header is used to store the information of first ingress routers' IP address and interface number through which the packet enters the Internet. The router marks every incoming packet as in the case of DRIM.

The paper is organized as follows: various techniques used to handle fragmentation in DPM is discussed in Section II, the basic DRIM algorithm and its limitation are described in Section III. Modifications proposed for the basic DRIM to alleviate the problem associated with fragmented traffic are presented in Section IV. Discussion and analysis of proposed model on the evaluation metrics and the comparison of the proposed scheme with other techniques is described in Section V. We conclude in Section VI with future work.

2. RELATED WORK

An important strategy for investigating and attributing network attacks is IP traceback [6, 7]. IP traceback involves identifying the actual source across the Internet and is a tough task because of IP spoofing. If the identity of the attacker can be revealed using IP traceback, the attacker would think twice before performing attack.

IP traceback techniques can be classified into two categories reactive and proactive. Reactive techniques are the one that carries out the IP traceback on the fly once an attack is detected. In reactive scheme, traceback is executed in response to an ongoing attack like a stimuli-response mechanism. Proactive traceback techniques take a different form by proactively recording and logging the traffic packets as they flow through the network. These records are useful for path reconstruction to the actual source.

Packet marking is a technique which inserts marking information within an IP packet and the marking information includes the address of each router along its path. The packets are marked either probabilistically or deterministically. Probabilistic packet marking (PPM) requires many packets for convergence of attacker information. Deterministic packet marking (DPM) techniques need fewer packets for traceback and can be performed post mortem.

The DPM is first proposed by Belenky and Ansari [6, 7] , in which only the ingress edge routers mark packets. To store the marking information DPM splits the IP address into two parts and uses the 1-bit reserved flag to indicate the first and second parts of the IP address. Then Rayanchu and Barua [8] further extended this approach by embedding all the IP information in a single packet. The 16-bit packet ID field is marked with a 16-bit hash of the 32-bit IP address of the edge router.

Another vigorous and scalable DPM scheme is proposed by Lin and Lee [9]. This scheme uses multiple hash functions to reduce the probability of address digest collisions. Their DPM technique uses three bits to distinguish between eight different hash functions; the remaining fourteen bits carry the hashed address information. Another variation of DPM, based on redundant decomposition, was proposed by Jin and Yang [10] where the marking field has two sections: information and index. Every ingress edge router decomposes its corresponding IP address into fragments where the neighbouring fragments have some redundant bits. The IP ID field is marked with one of the fragments.

A flexible DPM scheme is proposed by Xiang, et al [11] to identify the source of attack packets. This scheme adopts the strategy of flexible mark length to have the compatibility with different network environments. Chen, et al. [12] propose router interface marking (RIM) mechanisms which consider a router interface (as opposed to the router itself) as an atomic unit for traceback. RIM-enabled router is used to mark each packet with the identifier of the hardware interface that processed the packet. The mark is a locally-composed string of unique router input IDs that serves as a globally-unique path identifier.

Yi, et al. [13] propose a DPM technique that marks every packet passing through a router with a link signature . Each router participates in marking and the mark changes with each router. The entire path information is available in each packet and single-packet IP traceback is possible. Peng, et al. [14] proposed an enhanced, authenticated DPM that uses path numbering for traceback. DPM-enabled routers mark each packet based on the incoming interface at the edge of a subnet. PPM enabled routers are closest to the packet source and mark each packet with path identifiers that represent the path linking them to the DPM enabled routers. This facilitates attack detection and filtering as well as obtaining accurate information from the authenticated marks.

As far as the fragmented traffic is concerned, Belenky and Ansari [2] proposed a fragment persistent DPM. The basic DPM marks packets probabilistically, randomly choosing between the first and the last 16 bits of the ingress IP address. This random behavior must be suspended when processing fragments. In order to accomplish this task, DPM has to keep track of the fragments, which pass through. If the first fragment which DPM encounters (which does not have to be the fragment with offset 0) is marked with the first or last 16 bits, then the rest of the fragments of this datagram must be marked with the same bits. This information has to be stored as a table at the DPM enabled interface and checked every time a new fragment arrives.

3. DETERMINISTIC ROUTER AND INTERFACE MARKING (DRIM)

This section provides the general principle behind DRIM [5] as shown in Figure 1 and discusses the most basic implementation of the proposed scheme. DRIM is basically a marking scheme which considers router interface address as a atomic unit. This scheme uses the features of DPM and another scheme called RIM which are already discussed in section 2.

3.1 Review of DRIM

The proposed IP traceback technique deterministically marks each packet with the interface number and the address of the router through which the packet enters the network. Only the first router marks the packet to prevent other routers from overwriting the mark. This makes it possible to perform a traceback beyond the ingress router.

Consider the architecture in Figure 1 with various hosts, switches, routers and interfaces. The attacker connects to the Internet through ingress edge router R_1. Packets reach the first router R_1 through interface I_2. The other interfaces I_1, I_3, I_4 and I_5 of the router R_1 are connected to a switch S_1, a host and two routers R_2 and R_3. The interface number I_2 and a hash value of router R_1's IP address are marked deterministically in each packet on the attack path. No other routers (i.e., R_3 to R_{13}) overwrite the mark. Only packets arriving through the interfaces I_1, I_2 and I_3 are marked by the router R_1.

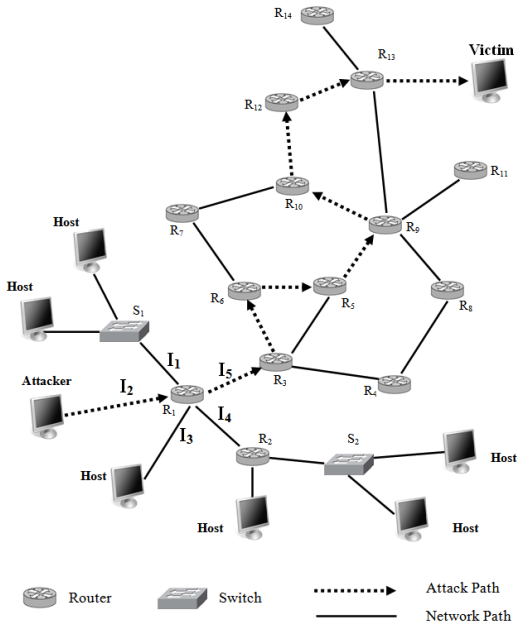

Fig. 1. Proposed Architecture for IP Traceback

Packets arriving through I_4 and I_5 connected to routers R_2 and R_3, respectively, are not marked. Each packet is marked only once with interface number and a hash of the router's IP address.

3.2 Marking Information Encoding

To store the marking information the 16-bit ID field, 3-bit fragment flag field and 13-bit fragment offset field in the IP header is used. The 16 bits of ID field are used to store a 16-bit hash value of the 32-bit IP address of the first ingress edge router. The most significant 12 bits of the 13-bit offset is used to store the interface number. The DF bit is set to 1 and MF bit is set to 0 to indicate that the fields cannot be used for fragmentation. Since the hash function is used for converting the 32-bit IP address into a 16-bit value which may result in some collisions and hence yield some false positives.

3.3 Limitations of DRIM

The Deterministic Router and Interface Marking (DRIM) technique can trace an attacker from the ingress edge router using a single packet, meeting the basic requirement of network forensics. It traces an attacker more closely than other techniques by identifying the interface from which the attack packet arrived at the router. But it cannot handle fragmented packets while facilitating router and interface marking.

In the case of fragmentation, a datagram is fragmented by a router or a host before it reaches the DRIM-enabled interface. In this case, a series of fragments of the original datagram will reach the DRIM-enabled interface. Since the basic DRIM does not distinguish between fragments and non-fragments, the scheme will randomly replace the ID field of all the fragments with the router hash address. This will cause fragments to have different ID fields when they arrive to the destination. Fragments with different ID fields will be considered to be parts of different datagrams. The reassemblies will eventually "timeout" since the destination will never get all the fragments necessary for the reassembly of what it considers to be from different series. The probability of all fragments in a series of two fragments having the same ID field after marking is 0.5, for a series of three fragments, 0.25, and so on. Clearly, the rate of reassembly errors caused by fragmentation is unacceptable. To avoid this situation, the modification to the basic DRIM is introduced.

4. FLEXIBLE DRIM

In the IPv4 header the option field is often empty and generally is not used. In the proposed scheme to handle the fragmented traffic the option filed of IP header is used to store the information of router IP address and router interface number of the first ingress router where the every incoming packet is marked.

4.1 FDRIM Principle

The Flexible Deterministic and Router Interface Marking technique deterministically marks each packet with the interface number and the address of the router through which the packet enters the network. Only the first router marks the packet to prevent other routers from overwriting the mark. This makes it possible to perform a traceback beyond the ingress router. While marking a packet the algorithm will treat the fragmented packet in a way so that the packet can be reassemble at destination without the time out.

Ver 4 bits	HLEN 4 bits	Service 8 bits	Total Length 16 bits
Identification 16 bits			D F | M F | R F | Fragment Offset 13 bits
Time to Live 8 bits	Protocol 8 bits		Header Checksum 16 bits
Source IP Address 32 bits			
Destination IP Address 32 bits			
Option Variable Length			

Figure 2 IPV4 Header

4.2 Marking Information Encoding

Before considering how the marking is done lets recall the actual IPV4 header as shown in Figure 2. In FDRIM, a 16-bit hash value of the 32-bit IP address of router is required to store. An enterprise network grade Cisco router that connects to a maximum number of 4,096 interfaces would use a maximum of twelve bits in the mark. The total bits we require to store is 16 bits + 12 bits ie 28 bits. When the packet is not fragmented these 28 bits can be easily stored in the Identification field and fragmentation offset field. Figure 3 shows the mapping between the IP header fields and the marking fields when the packet is not fragmented.

In this case the IP header will have the structure as given in Figure 3 and the average size of the packet will not be more than 1500 bytes. Now when the packet is fragmented along with padding of 4 bits the total required bits will be 32 bits i.e 4 bytes (32 bits). These 4 bytes of option field [2] is used to store the marking information if the packet is fragmented.

Figure 4 shows the mapping of the IP header fields when the

Ver 4 bits	HLEN 4 bits	Service 8 bits	Total Length 16 bits
Hash of Routers IP Address **16 bits**			1 | 0 | R F | **Interface Number** **12 bits**
Time to Live 8 bits	Protocol 8 bits		Header Checksum 16 bits
Source IP Address 32 bits			
Destination IP Address 32 bits			
Option **(Empty)** Variable Length			

Figure 3 Marking of Router Address and Interface Number when packet *is not* fragmented

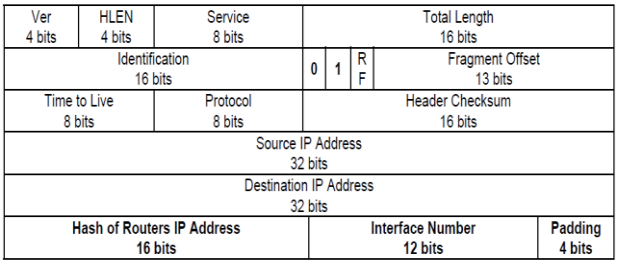

Figure 4 Marking of Router's Hashed Address and Interface Number when packet *is* fragmented

packet is fragmented. In this case the option field is used to store the information of router IP address & the router interface number. When the packet is fragmented, the average size of the packet increases to 1504 bytes.

As the average packet size is 1500 bytes, for each fragmented packet we have an overhead of 4 bytes and we will shift the 4 bytes of the current packet to next fragmented packet to accommodate this overhead. It may finally increase the overhead of one packet at max. Figure 4 shows the header structure when it carries the information of marking in option field. Figure 5 shows the structure of IP header when the complete router address is marked. However, the maximum size cannot exceed more than 1508 bytes.

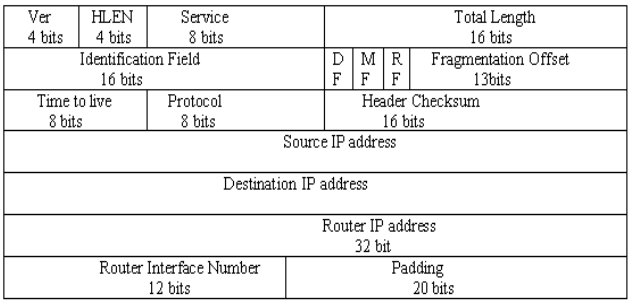

Figure 5 Marking of Router Address and Interface Number when packet *is* fragmented

Algorithm 1 lists the steps used to encode and mark the IP address and the interface number of the router in each packet. It checks whether the packet is fragmented and marks the fields accordingly based on the DF flag.

4.3 Traceback Operation

The traceback operation (Algorithm 2) is simple because each packet holds the information required to identify the first ingress router and the interface through which the packet reached the router. The 16 bit identification field in the IP header gives the 16-bit hash value of the router's 32-bit IP address. The 12-bit value in the offset field indicates the interface number. The identification of the interface through which the attack packet entered the network places the attacker closer than other traceback techniques that only identify the first ingress edge router. Since each packet has all the marker information, the traceback operation requires only a packet.

5. Discussion and Analysis

The metrics used to evaluate the traceback schemes originally suggested by Belenky and Ansari [1] are analyzed accordingly for the proposed technique FDRIM.

Algorithm 1 : Marking the address and interface number of router *Ri*.

```
for each outbound packet P reaching router Ri
     through interfaces Ij ⊂ Ilocal do
    if (DF is set or packet is not fragmented)
      Write  HashIP16(Ri) into P.Identification
      Write Ij into P.offset[0..11]
      Set P.DF = 1
      Set P.MF = 0
    Else
      Write HashIP16(Ri) into P.option[1..16]
      Write Ij into P.option[17..28]
      P.IPHL = 4bits
    end if
end for
```

Algorithm 2 : Reconstruction at victim *V* .

```
for each attack packet P reaching victim do
    if (DF is set or packet is  not fragmented)
       Read  HashIP16(Ri) from P.Identification
       Extract IP from HashIP16(Ri)
       Read Ij from P.offset[0..11]
    else
       Read HashIP16(Ri) from P.option[1..16]
       Read Ij from P.option[17..28]
    end if
       IN = Ij
       return(IP,IN)
end for
```

5.1 Performance Metrics

The following metrics are analyzed for FDRIM:

5.1.1 Bandwidth overhead

Using the above mentioned algorithm a nominal bandwidth overhead will increase. Out of the total internet traffic the fragmented traffic is only 0.25%. to 0.5% Suppose the entire traffic is of 1000 packets then the fragmented traffic is 0.5% of 1000 i.e.5 packets at most.

We know the maximum packet size is 1500 bytes. Now for each fragmented packet we have a overhead of 4 bytes. To accommodate this overhead we will shift the 4 bytes of the current packet to next fragmented packet. It may finally increase the overhead of one packet at max if the last packet in fragmented packet is of exactly 1500 bytes otherwise no overhead will be increased. So at most the overhead will be of maximum of one packet on every 5 fragmented packets.

5.1.2 False Positives:

The false positives is almost reduced to zero if the complete router IP address is stored without hashing ,in that case the header size will be of 28 bytes and the actual packet size will be of 1508 bytes. Again to accommodate this overhead of 8 bytes the 8 bytes will be shifted to next fragmented packet which will only increase the overhead of maximum of one packet.

5.1.3 Number of Packets for Traceback:

Every packet provides information about the attacker. The information includes the ingress router IP address and interface number from which the attack packet entered the network. The technique works for any number of distributed attackers working in coordination.

Table 1. Comparison of FDRIM with related techniques

Techniques Evaluation Metric	**DPM**	**Fragmentation Persistent DPM**	**RIM**	**DRIM**	**FDRIM**
Number of packets	Seven Packets	44 fragmented packets	Single packet	Single packet	Single packet
Processing overhead	Packets marked only once with the first or last sixteen bits of edge router's address	Each packet has to marked only once	Packets probabilistically marked with XOR and interface ID values or XOR value is updated	Packets assigned two marks by the first ingress edge router	Packets assigned two marks by the first ingress edge router
Storage overhead	Table used for matching source and ingress addresses	Table for matching source with ingress addresses at the victim	Trace table maintains hop count, interface id and XOR value	Hash value of router's address is precomputed and stored	No storage required at router or victim.
Marking field length	34 bits in two consecutive packets	34 bits in 2 packets	17 bits (handling 64 interfaces)	31 bits (handling 4,096 interfaces)	31 bits (handling 4,096 interfaces)
Infrastructural changes	One function added to network devices	Marking function involves to store the value of RF corresponding to(SA,DA,P,ID)	One function added to network devices	One function added to network devices	One function added to network devices
False Positives	Two packets carry the router's address and may yield errors	44 Packets carry the router address so may yield to error	Few errors as router interface IDs may not be unique	Hashing the router's address yields few errors	No Hashing will reduce False positive to almost zero
Scalability	Thousands of attackers can be traced	Any number of packets can be traced	False positive errors increase with number of attackers	Any number of attackers can be traced	Any number of attackers can be traced

5.1.4 *Storage Overhead:*
The technique requires no additional storage beyond the hash value of the router.

5.1.5 Infrastructure Changes:
Infrastructure changes are minimal because the technique requires the implementation of only one additional function in the routers. The function to reconstruct the traceback is only required at the victim's end.

5.1.6 Scalability:
The technique is scalable and can handle multiple attackers because information about the attacker is in each packet.

5.1.7 *ISP Involvement:*
Considerable interaction with an ISP is required to implement the *marking* function in all routers.

5.1.8 *Effect of Partial Deployment:*
Incremental deployment is limited because the marking is done only once. If the attacker's ingress routers do not perform the marking, then the technique may yield more false positive errors. The assumption that marking occurs in the attacker's network ensures that every packet that reaches the first ingress edge router is marked.

5.2 Comparison with other Schemes
As well-known, the usage of fragmentation is decided by MTU size [3]. Fragmentation will degrade the efficiency and performance of Internet. In order to improve the performance of whole network, RFC1191 specifies a path MTU discovery protocol. At present this protocol is widely using in Internet, so majority of traffic do not experience fragmentation and normally DF is set. But there still has exception. FDRIM has several advantages over the other techniques. It can trace the attacker using a single packet and does not require additional memory at the router or at the victim. The marking operation is simple, easily implemented and overcomes mark spoofing. Because the entire marking information is available in a single packet, with false positive errors almost reduces to zero. FDRIM goes one step beyond other related techniques by identifying the interface from which a packet reached the ingress router handling both fragmented and non-fragmented traffic in a efficient way with a very nominal bandwidth overhead. This increases the possibility of tracing an attacker beyond the router, which the other techniques are unable to accomplish. As compared with other marking schemes, FDRIM posses the advantages.

Table 1 compares the various marking techniques with the proposed Flexible deterministic router and interface marking (FDRIM) technique.

6. Conclusion

In this article we present the modification to the DRIM. With this modification the DRIM traceback scheme will handle the fragmented traffic also with a very nominal bandwidth increase and no processing and storage overhead will be increased also the false positive is also almost reduced to zero. Future research includes the simulation of the proposed technique using the appropriate simulator and moreover some more improvements which will facilitate the incremental deployment of FDRIM enabled routers and reduce ISP interaction.

7. REFERENCES

[1] Belenky, A. and Ansari, N. 2003. On IP traceback. *IEEE Communications Magazine*, *41* (7). 142-153.

[2] Belenky, A. and Ansari, N. 2003. Accommodating fragmentation in deterministic packet marking for IP traceback. in *IEEE Global Telecommunications Conference (GLOBECOM '03)*, (San Francisco, California, USA). 1374-1378.

[3] Savage, S., Wetherall, D., Karlin, A. and Anderson, T. 2001. Network support for IP traceback. *IEEE/ACM Transactions on Networking*, *9* (3). 226-237.

[4] Shannon, C., Moore, D. and Claffy, K. C. 2002. Beyond folklore: observations on fragmented traffic. *IEEE/ACM Transactions on Networking (TON)*, *10* (6). 709-720.

[5] Pilli, E. S., Joshi, R. C. and Niyogi, R. 2011. Router and Interface Marking for Network Forensics. in *Advances in Digital Forensics VII*, (Florida, USA). 209-220.

[6] Belenky, A. and Ansari, N. 2003. IP traceback with deterministic packet marking. *IEEE Communications Letters*, *7* (4). 162-164.

[7] Belenky, A. and Ansari, N. 2007. On deterministic packet marking. *Computer Networks*, *51* (10). 2677–2700.

[8] Rayanchu, S. and Barua, G. 2005. Tracing attackers with deterministic edge router marking (DERM). in *First International Conference on Distributed Computing and Internet Technology (ICDCIT '04)*, (Bhubaneswar, India). 400-409.

[9] Lin, I. and Lee, T. H. 2006. Robust and scalable deterministic packet marking scheme for IP traceback. in *IEEE Global Telecommunications Conf. (GLOBECOM '06)*, (San Francisco, California, USA). 1-6.

[10] Jin, G. and Yang, J. 2006. Deterministic packet marking based on redundant decomposition for IP traceback. *IEEE Communications Letters*, *10* (3). 204-206.

[11] Xiang, Y., Zhou, W. and Guo, M. 2009. Flexible deterministic packet marking: an IP traceback system to find the real source of attacks. *IEEE Transactions on Parallel and Distributed Systems*, *20* (4). 567-580.

[12] Chen, R., Park, J. M. and Marchany, R. 2006. RIM: Router Interface Marking for IP Traceback. in *IEEE Global Telecommunications Conference (GLOBECOM '06)*, (San Francisco, California, USA). 1-5.

[13] Yi, S., Xinyu, Y., Ning, L. and Yong, Q. 2006. Deterministic packet marking with link signatures for IP traceback. in *Second SKLOIS Conference on Information Security and Cryptology (Inscrypt '06)*, (Beijing, China). Springer. 144-152.

[14] Peng, D., Shi, Z., Tao, L. and Ma, W. 2007. "Enhanced and authenticated deterministic packet marking for IP traceback," in *7th International Conference on Advanced Parallel Processing Technologies (APPT 2007)*, (Guangzhou, China), Springer-Verlag, 2007, 508-517.