https://dx.doi.org/10.24001/ijaems.3.2.1 ISSN : 2454-1311

A Novel IP Traceback Scheme for Spoofing Attack

Dr K Butchi Raju

Professor, Department of CSE, GRIET, Hyderabad, India

Abstract— *Internet has been widely applied in various fields, more and more network security issues emerge and catch people's attention. However, adversaries often hide themselves by spoofing their own IP addresses and then launch attacks. For this reason, researchers have proposed a lot of trace back schemes to trace the source of these attacks. Some use only one packet in their packet logging schemes to achieve IP tracking. Others combine packet marking with packet logging and therefore create hybrid IP trace back schemes demanding less storage but requiring a longer search. In this paper, we propose a new hybrid IP trace back scheme with efficient packet logging aiming to have a fixed storage requirement for each router in packet logging without the need to refresh the logged tracking information and to achieve zero false positive and false negative rates in attack-path reconstruction.*

Keywords— DoS/DDoS attack, hybrid IP traceback, IP spoofing, packet logging, packet marking.

I. INTRODUCTION

A great amount of effort in recent years has been directed to the network security issues. In this paper, we address the problem of identifying the source of the attack. We define the source of the attack to be a device from which the flow of packets, constituting the attack, was initiated. This device can be a zombie, reflector, or a final link in a stepping stone chain. While identifying the device, from which the attack was initiated, as well as the person(s), behind the attack is an ultimate challenge, we limit the problem of identifying the source of the offending packets, whose addresses can be spoofed. This problem is called the IP traceback problem [1]. DOS attack scenario is shown in Fig 1.

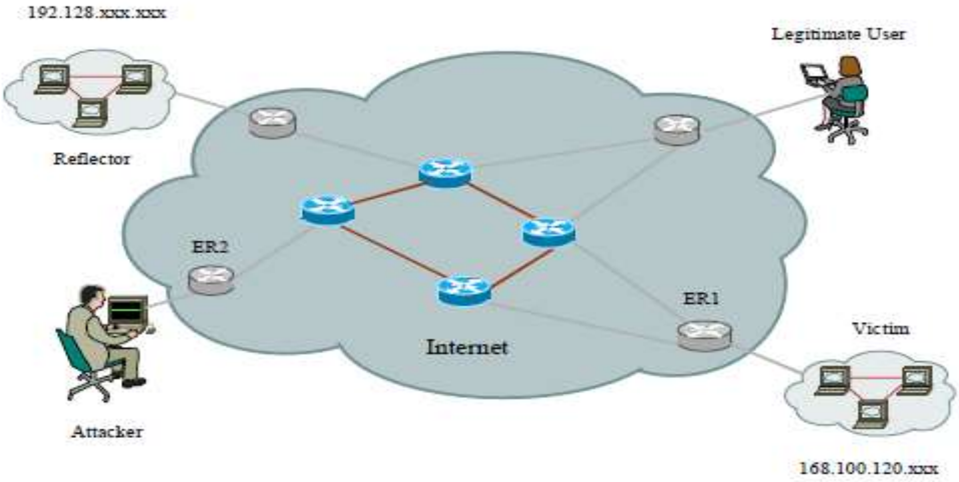


Fig.1: DOS attack scenario

Several solutions to this problem have been proposed. They can be divided in two groups. One group of the solutions relies on the routers in the network to send their identities to the destinations of certain packets, either encoding this information directly in rarely used bits of the IP header, or by generating a new packet to the same destination. The biggest limitation of this type of solutions is that they are focused only on flood-based (Distributed) Denial of Service [DoS] attacks[2], and cannot handle attacks comprised of a small number of packets. The second type of solutions involves centralized management, and logging of packet information on the network. Solutions of this type introduce a large overhead, and are complex and not scalable.

IP traceback [3] is a name given to any method for reliably determining the origin of a packet on the Internet. Due to the trusting nature of the ip protocol, the source IP address of a packet is not authenticated. As a result, the source address in an IP packet can be falsified (IP address spoofing) allowing for Denial Of Service attacks (DoS) or one-way attacks (where the response from the victim host is so well known that return packets need not be received to continue the attack). The problem of finding the source of a packet is called the IP traceback problem. IP Traceback is a critical ability for identifying sources of attacks and instituting protection measures for the Internet. Most existing approaches to this problem have been tailored toward DoS attack detection. Such solutions require high numbers of packets to converge on the attack path(s).

During the past decade, a lot of attention has been focused on the security of Internet infrastructure in place as being part of transmission, reception and storage of paramount importance within the increasing ecommerce applications. Yet, with high profile Distributed Denial-of Service (DDOS) attacks, numerous ways have been elaborated to identify the source of these attacks and one methodological approach is using IP traceback. The goal of IP traceback is to trace the path of an IP packet to its origin. The most important usage of IP traceback is to deal with certain denial-of-service (DoS) attacks, where the source IP address is spoofed by attackers. Identifying the sources of attack packets is a significant step in making attackers accountable. In addition, figuring out the network path which the attack traffic follows can improve the efficacy of defense measures such as packet filtering as they can be applied further from the victim and closer to the source. Two main kinds of IP traceback techniques have been proposed in two orthogonal dimensions: packet marking and packet logging. In packet marking, the router marks forwarded IP packets with its identification information. Because of the limited space in packet header, routers probabilistically decide to mark packets so that each marked packet carries only partial path information. The network path can be reconstructed by combining a modest number of packets containing mark. This approach is known as probabilistic packet marking (PPM). The PPM approach incurs little overhead at routers. But it can only trace the traffic composed of a number of packets because of its probabilistic nature[4].

In packet logging, the IP packet is logged at each router through which it passes. Historically, packet logging was thought to be impractical because of enormous storage space for packet logs. Hash-based IP traceback approach records packet digests in a space-efficient data structure, bloom filter, to reduce the storage overhead significantly. Routers are queried in order to reconstruct the network path. The information required to achieve traceback is either stored at different points (mostly on routers) along the path that a packet traverses or that path and usually other incidental paths are analyzed to gain information that will be used in traceback. It is this distinction that we employ to further divide network based schemes into packet logging schemes and network analysis schemes. The IP traceback[1,3] categories is shown in Fig 2.

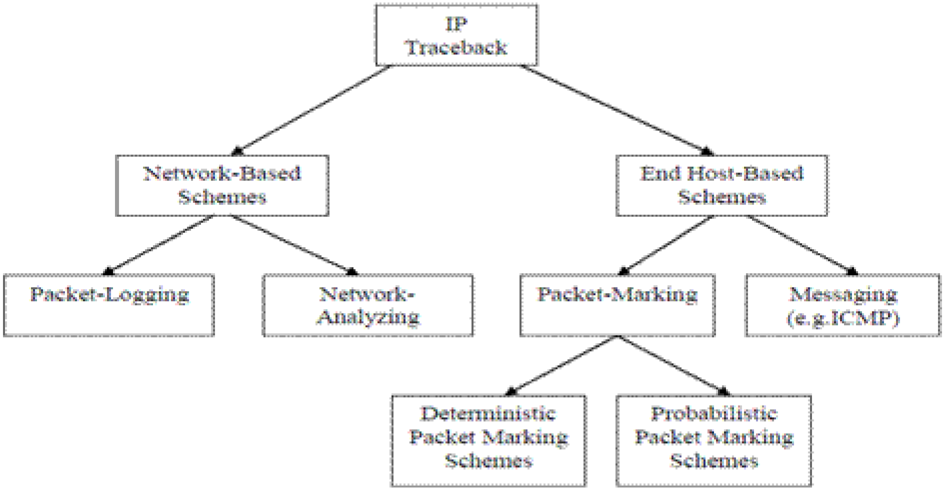


Fig.2: IP Traceback categories

II. LITERATURE SURVEY

A great amount of effort in recent years has been directed to the network security issues. In this paper, we address the problem of identifying the source of the attack.

Snoeren et al. [5] proposed a hash-based IP traceback approach, called Source Path Isolation Engine (SPIE), to realize log-based IP traceback in practice. Their approach reduces the storage overhead significantly through recording packet digests in a space-efficient data structure, a Bloom filter. SPIE has made a significant improvement on the practicality of log-based IP traceback. However, its deployment at high-speed networks has still been a challenging task due to the high storage overhead and access time requirement for recording packet digests.

In (Distributed) Denial of Serviceattack ((D)DoS), attackers send a huge number of packets with spoofed source addresses to disguise themselves toward a target host or network. Various IP traceback techniques such as link testing, marking, and logging to find out the real source of attacking packets have been proposed.

Various existing techniques for IP traceback have been reported in the literature (Internet Control Message Protocol (ICMP) traceback messages[6], link testing[7], marking[8] and logging[9]).We propose a new technique that uses Huffman codes to mark packets with router's information as packets traverse outers during the journeys to reach their destinations. Simulation results and practical issues are also presented.

III. METHODOLOGY

3.1. Current System

Most of current single packet traceback schemes tend to log packets' information on routers. Most current tracing schemes that are designed for software exploits can be categorized into three groups: single packet, packet logging and hybrid IP traceback . The basic idea of packet logging is to log a packet's information on routers. The methods used in the existing systems include Huffman Code, Modulo/ Reverse modulo Technique (MRT) and MOdulo/REverse modulo (MORE).

These methods use interface numbers of routers, instead of partial IP or link information, to mark a packet's route information. Each of these methods marks routers' interface numbers on a packet's IP header along a route. However, a packet's IP header has rather limited space for marking and therefore cannot always afford to record the full route information. So, they integrate packet logging into their marking schemes by allowing a packet's marking field temporarily logged on routers. From this, it is found that these tracing methods still require high storage on logged routers. Apart from this, also found that, exhaustive searching is quite inefficient in path reconstruction.

Drawbacks

- In the existing system, adversaries often hide themselves by spoofing their own IP addresses and then launch attacks.
- There is a lot of traceback schemes to trace the source of these attacks. Some use only one packet in their packet logging schemes to achieve IP tracking.
- Others combine packet marking with packet logging and therefore create hybrid IP traceback schemes demanding less storage but requiring a longer search.
- Taking longer search time and false positives is the main drawback of the existing system.

3.2. Proposed System and structure

In the proposed system, we provide a new hybrid IP traceback scheme with efficient packet logging aiming to have a fixed storage requirement for each router (under 320 KB, according to CAIDA's skitter data set) in packet logging without the need to refresh the logged tracking information and to achieve zero false positive and false negative rates in attack-path reconstruction. The system structure is shown in Fig 3.

Advantages

- In the proposed system, a new hybrid IP traceback scheme is provided with efficient packet logging
- The aim of packet logging is to have a fixed storage requirement for each router without the need to refresh the logged tracking information and to achieve zero false positive and false negative rates in attack-path reconstruction.
- Packet's marking field is used to censor attack traffic on its upstream routers.
- Possible extension is to explore an alternative approach to packet marking and logging for IP trace back.

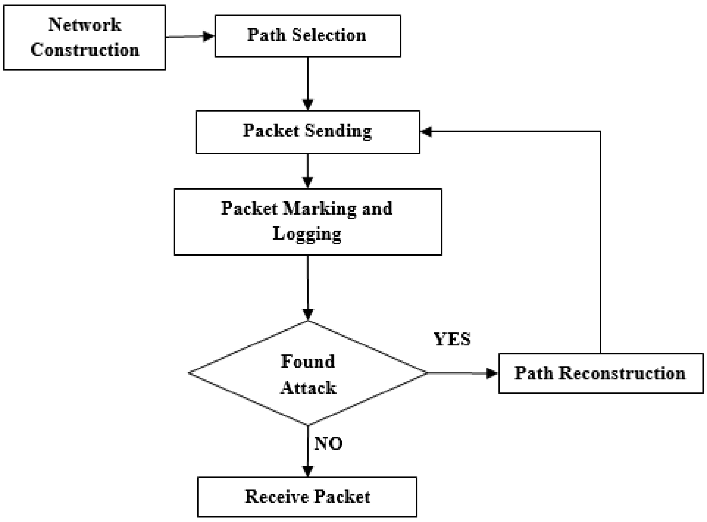


Fig.3: Proposed system structure

IV. MODULE DESCRIPTION AND RESULT ANALYSIS

The entire work of this paper is divided into five different modules. They are:

- Network topology Construction
- Path Selection
- Packet Sending
- Packet Marking and Logging
- Path Reconstruction

Network topology Construction: A Network Topology may consist of the number of routers that are connected with local area networks. Thus, a router can either receive data from the nearer router or from the local area network. A border router receives packets from its local network. A core router receives packets from other routers. The number routers connected to a single router is called as the degree of a router. This is calculated and stored in a table. The Upstream interfaces of each router also have to be found and stored in the interface table. This is shown in Fig 4.

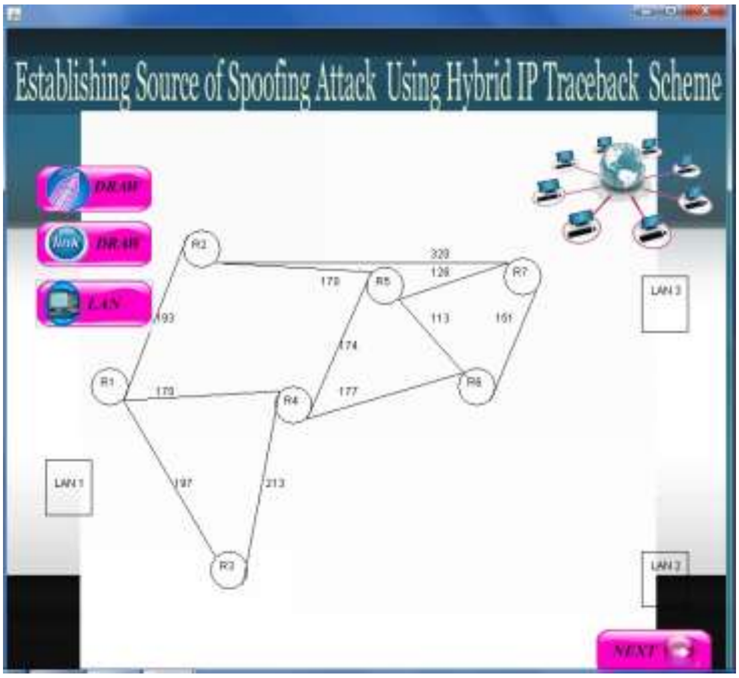
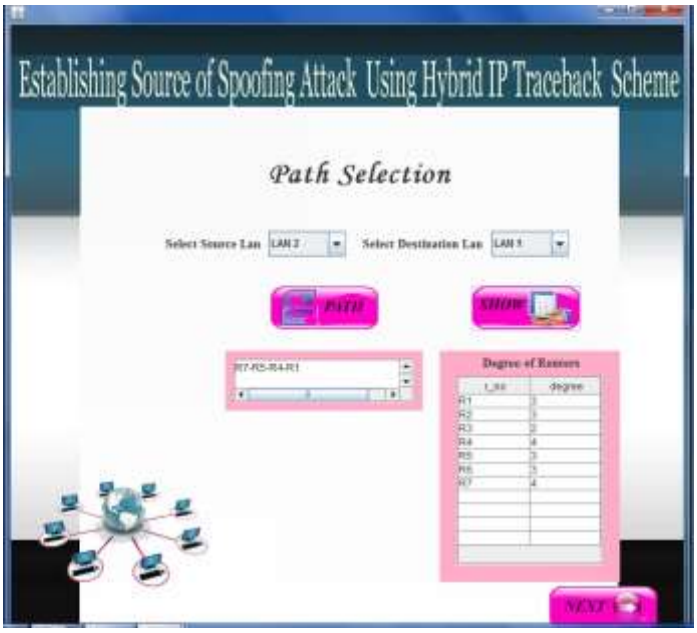


Fig.4: Network topology construction

Path Selection

The path is said to be the way in which the selected packet or file has to be sent from the source to the destination**.** The Upstream interfaces of each router have to be found and it is stored in the interface table. With the help of that interface table, the desired path between the selected source and destination can be defined. This is shown in Fig 5.


Establishing Source of Spoofing Attack Using Hybrid IP Traceback Scheme
Path Selection
PATH
SHOW
NEXT

Select Source Lan: LAN 2 Select Destination Lan: LAN 1

R7-R5-R4-R1

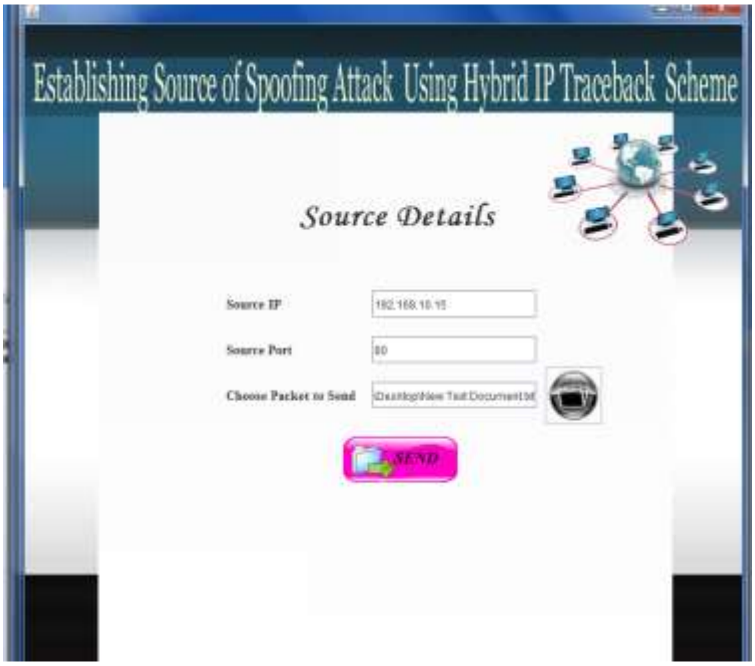
Degree of Routers

r_no	degree
R1	3
R2	3
R3	2
R4	4
R5	3
R6	3
R7	4

Fig.5: Path selection

Packet Sending

One of the Packet or file is to be selected for the transformation process. The packet is sent along the defined path from the source LAN to destination LAN. The destination LAN receives the packet and checks whether that it has been sent along the defined path or not. This is shown in Fig 6.


Establishing Source of Spoofing Attack Using Hybrid IP Traceback Scheme
Source Details
SEND

Source IP: 192.168.10.15

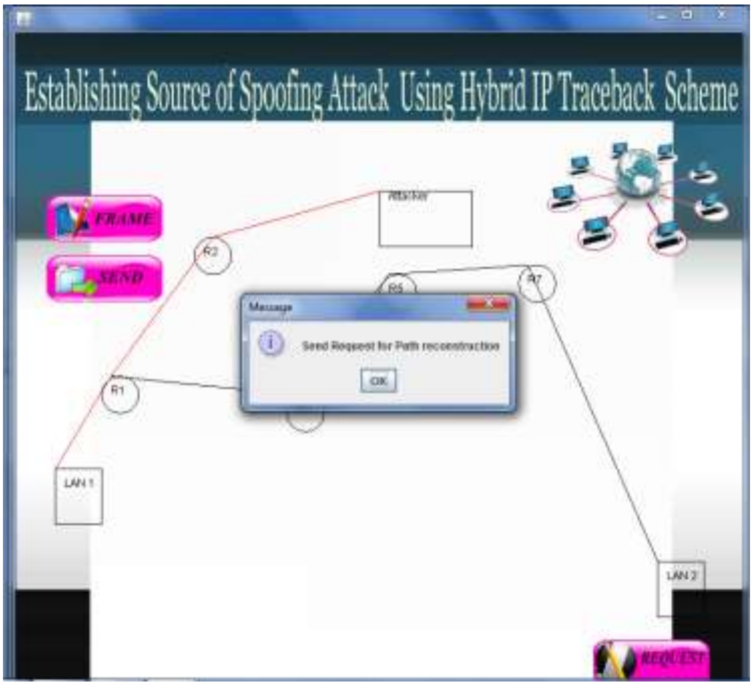
Source Port: 80

Choose Packet to Send: \Desktop\New Text Document.txt

Fig.6: packet sourcing

Packet Marking and Logging

Packet Marking is the phase, where the efficient Packet Marking algorithm is applied at each router along the defined path. It calculates the Pmark value and stores in the hash table. If the Pmark is not overflow than the capacity of the router, then it is sent to the next router. Otherwise it refers the hash table and again applies the algorithm. This is shown in Fig 7.


Establishing Source of Spoofing Attack Using Hybrid IP Traceback Scheme
FRAME
SEND
R2
Attacker
R5
R7
R1
LAN 1
LAN 2
REQUEST

Message

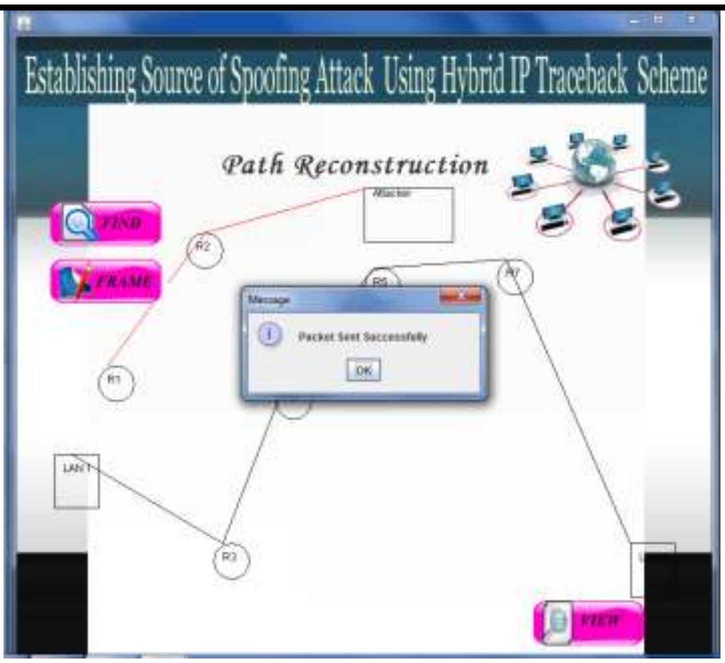
Send Request for Path reconstruction

OK

Fig.7: packet marking and logging

Path Reconstruction

Once the Packet has reached the destination after applying the Algorithm, there it checks whether it has sent from the correct upstream interfaces. If any of the attack is found, it request for the Path Reconstruction. To reconstruct the path of a packet and identify the source of the attack, the victim requires a map of the routers. This is shown in Fig 8.


Establishing Source of Spoofing Attack Using Hybrid IP Traceback Scheme
Path Reconstruction
FIND
FRAME
VIEW
Attacker
R2
R5
R7
R1
R3
LAN 1

Message

Packet Sent Successfully

OK

Fig.8: Path reconstruction

V. CONCLUSIONS

In this paper, we propose a new hybrid IP traceback scheme (RIHT) for efficient packet logging aiming to have a fixed storage requirement in packet logging without the need to refresh the logged tracking information. Also, the proposed scheme has zero false positive and false negative rates in an attack-path reconstruction. Apart from these properties, our scheme can also deploy a marking field as a packet identity to filter malicious traffic and secure against DoS/DDoS attacks. Consequently, with high accuracy, a low storage requirement, and fast computation, RIHT can serve as an efficient and secure scheme for hybrid IP traceback.

REFERENCES

[1] Cheng L, Divakaran DM, Lim WY, Thing VL. Opportunistic Piggyback Marking for IP Traceback. IEEE Transactions on Information Forensics and Security. 2016 Feb;11(2):273-88.

[2] Patel S, Gupta B, Sharma V. Throughput analysis of AQM schemes under low-rate Denial of service attacks. InComputing, Communication and Automation (ICCCA), 2016 International Conference on 2016 Apr 29 (pp. 551-554). IEEE.

[3] Cheng L, Divakaran DM, Ang AW, Lim WY, Thing VL. FACT: A Framework for Authentication in Cloud-Based IP Traceback. IEEE Transactions on Information Forensics and Security. 2016 Nov 3.

[4] Zhao Y, Dong Q. Anomaly detection for DOS routing attack by a attack source location method. InGuidance, Navigation and Control Conference (CGNCC), 2016 IEEE Chinese 2016 Aug 12 (pp. 25-29). IEEE.

[5] Snoeren, A. C., Partridge, C., Sanchez, L.A., Jones, C. E. HashBased IP Traceback. In: Proceeding in ACM. SIGCOMM, pp 3– 14, 2001

[6] Cheng L, Divakaran DM, Lim WY, Thing VL. Opportunistic Piggyback Marking for IP Traceback. IEEE Transactions on Information Forensics and Security. 2016 Feb;11(2):273-88.

[7] Liu X, Huo L, Wen XM, Paige R. A link-free approach for testing common indices for three or more multi-index models. Journal of Multivariate Analysis. 2017 Jan 31;153:236-45.

[8] Li P, Feng Y, Kawamoto J, Sakurai K. A Proposal for Cyber-Attack Trace-back Using Packet Marking and Logging. InInnovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2016 10th International Conference on 2016 Jul 6 (pp. 603-607). IEEE.

[9] Li P, Feng Y, Kawamoto J, Sakurai K. A Proposal for Cyber-Attack Trace-back Using Packet Marking and Logging. InInnovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2016 10th International Conference on 2016 Jul 6 (pp. 603-607). IEEE.