*International Journal of Engineering &Technology*, 7 (1.8) (2018) 67-71

International Journal of Engineering & Technology

*Website: www.sciencepubco.com/index.php/IJET*

***Research paper***

# A survey on existing IP trace back mechanisms and their comparisons

**Vahiduddin Shariff [1] *, Ruth Ramya K [2], B. Renuka Devi [3], Debnath Bhattacharyya [4], Tai-hoon Kim [5]**

*[1] Department of Computer Science and Engineering, Sir C R Reddy College of Engineering, Eluru, West Godavari district*
*[2] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India – 522502*
*[3] Department of Computer Science and Engineering,Vignan's Nirula Institute of Technology & Science for Women, Peda Palakaluru, Guntur, AP, India*
*[4] Department of Computer Science and Engineering,Vignan's Institute of Information Technology, Duvvada, Visakhapatnam, AP, India*
*[5] Department of Convergence Security, Sungshin Women's University,249-1, Dongseon-dong 3-ga, Seoul, 136-742, Korea*
**Corresponding author E-mail: shariff.v@gmail.com*

## Abstract

Security is the one of the main point of focus in recent trends of computer science, as it has to determine the right people accessing the system and ones who are trying the bypassing it. IP spoofing is one of the prevalent attacks, where the attackers launch the attack by spoofing the source address, once this happens they can attack without revealing their exact location. The attacker uses a fraudulent IP address to conceal their identity. To reveal the attackers real locations many IP trace back mechanisms have been proposed but the attacker immediately gets away with the information. There is another problem which is to detect DDoS traffic and the precarious packets set up by the attacker, which are a threat to the victim as well as the whole network, here lies another hurdle which is to differentiate between the attacker's data traffic from the normal data traffic. There are many solutions given for this but one among them is IP trace back which already has researched upon in the past and implemented then, but what is lacking in the solution such that the attacks are even now taking place. IP trace back if modified, strengthened would analyze the traffic faster and trace out the attacker with a faster pace, which is why a hybrid IP tracing and tracking mechanism if introduced could ease the current problem.

***Keywords***: *IP Trace Back; DDoS Traffic; IP Spoofing; Hybrid IP Trace Back.*

## 1. Introduction

DOS/DDOS attacks comprises of one of the major classes of threats of security relating to the internet today To determine the IP attack sources is the objective of IP trace back, along with this the full path taken by attack packets [6]. Different trace back methods like IP marking, IP logging and IETF ICMP trace back called ITrace have been proposed. In DoS attack generally a large in number of malignant packets are generated and directed towards the victims who are of one or more in number. Here the attacker will try to prevent legitimate user from accessing the services or information. By targeting the network connection of computer and network of the sites what we are trying to use actually, the attacker may prevent from accessing websites, online accounts, email etc.., or other services which depends on the computer which is affected. Spoofing usually is the process of replacing the source IP address with a fake IP address and fake page content such that the sensitive data could be stolen by the attacker. The attacker tries to forge the fake IP and content such that when a victim accesses the page his/her data is stolen.

## 2. IP spoofing

In computer science, IP spoofing is a term which is known to everyone in this domain, where there are forged with a fake IP address, impersonating another computer [6]. The major working is when an attacker fakes the address of another computer and uses it to steal the sensitive data of the victim , the attacker intercepts both sides of the connection using various cryptanalytic techniques [2] [6]. The attacker would monitor the traffic and the data sent from A to B and then guess the sequence of packets and data sent. Then the attacker knocks out A and injects his own packets, claiming to have the address of A. In general, IP spoofing also gives the attacker authentication to access the computer or a network in an unauthorized manner by making it look like, a malicious message has come from a trusted machine by "spoofing" the IP address of that machine and to ensure the intrusion, the intruder must first determine the IP address of a trusted system, and then modify the packet headers to that it appears that the packets are coming from the trusted system [2].

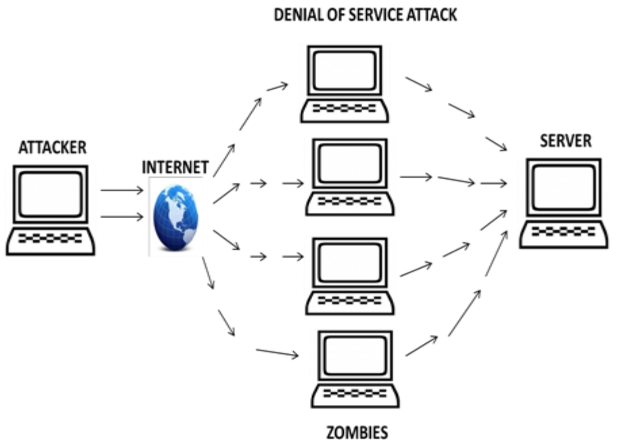

**Fig. 1:** Denial of Service Attack over A Network.

## 3. IP trace back

IP trace back is to track the network path of an IP packet to its source [1]. Two main kinds of IP trace back techniques have been proposed: packet marking and packet logging [4] [1]. In packet marking, the router marks forwarded IP packets with its identification information. The intermediate routers marks those IP packets with extra data so that the victimized person could utilization them on focus the strike way [7]. Methodologies recommended incorporate hub append, hub testing Furthermore edge testing [5]. Those hub annex component may be comparative of the IP record course choice, in that those addresses from claiming progressive routers traversed. Due to the limited space in the packet header, the router has to be programmed to choose a packet on the basis of probability when this happens the packets are marked but they are not given with full information in other words only the partial path information is embedded into the marked packets.

When the network path is rebuilt by combining a limited number of packets having a mark, this approach is known as probabilistic packet marking (PPM) [7] [1]. The PPM approach overcomes little overhead at routers. But it could track the network traffic to a certain number of packets due to its probabilistic nature. In packet logging, the IP packet is logged meaning the packets which are outgoing from the router have their details scanned at and through each router it passes [5]. Usually, packet logging was thought to be impractical due to lot of reasons one of which being the enormous storage space for packet logs. The hash based IP trace back 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 [6]. This approach can track a single IP packet. However, the requirements for digest table storage and access time to record packets commensurate with their arrival are prohibitive at routers with high speed links.

**Table 1:** IP Trace Back Categories

| Categories | | |
|---|---|---|
| Intra-AS Trace Back | Traffic Monitoring | Control Flooding<br>Input debugging<br>Overlay Network |
| | Packet Monitoring | Packet Marking<br>Packet Messaging<br>Packet Logging<br>Hybrid |
| Inter – AS Trace Back | | |

## 4. Overview

The project is majorly focused on one objective which is to provide more efficient and better tracing services to the analyst to track down the attacker , there the analyst has to use various mechanisms and has to upgrade them to make sure he/she is able to achieve the goal in much shorter time span and with much less memory.

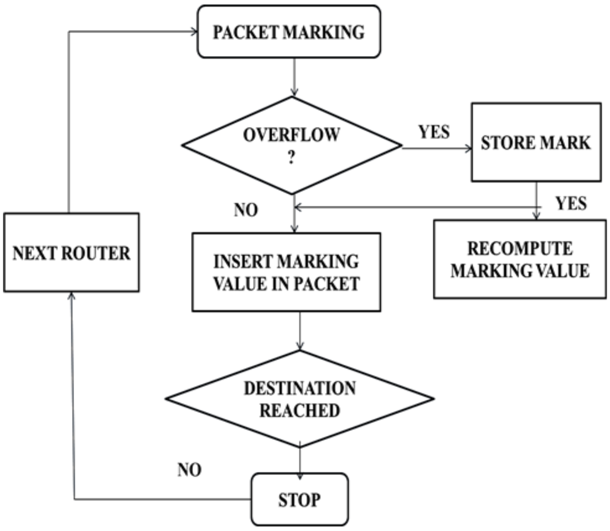

**Fig. 2:** Procedure of Packet Marking.

In this section we will discuss on how the analyst applies an algorithm/technique to track down the location, now when he/she uses packet marking procedures the time span, memory span does vary while if the packet logging procedures are used there are different results, so on using different mechanisms we get different results but the output or the objective would be same [9]. In this paper we would like to propose a better mechanism than the existing one such that the efficiency in detecting the location of attacker would increase to reasonable a range. To think in a security analyst perspective the existing system is quite satisfactory in detecting the location of the attacker/spoofer, though the existing system has multiple techniques being implemented the flaws do exist and have to be identified at that instant itself or mostly after the multiple simulations/trial and error mechanisms. Now comes the hard part where after identifying the error there are 3 simple and common questions which would pop up which is what, where, when the flaw is occurring or coming to the picture, the flaw could be a slight overlook in the source code. Though these mechanisms have few flaws identified in them, surely would be some advanced mechanism which would be identified and deployed over the network to surpass the existing system.

In this paper the we would focus on each and every mechanisms and point the flaws regarding them and then introduce an efficient one which is better than the existing one, the efficient mechanism is would implement both the procedures of the packet marking and packet logging which puts the algorithm to another level in terms of security, accuracy etc. . This mechanism would be a hybrid of the existing of the mechanisms as two or more mechanisms are combined to form a better one, a hybrid mechanism would mostly clear the flaws of the mechanisms being implemented [8].

## 5. Methodology

We have discussed various IP trace back mechanisms. These IP trace back mechanism can either be preventive or reactive methods. In reactive method, the main objective is to the reveal the source of the attacker. To construct an IP trace back mechanisms systems faces two critical challenges. The main challenge is the cost to implement the mechanism in the routers and difficulty in making various ISP to work together. The main difficulty also lies in the deployment of the mechanism in the routers, also we have identified the flaws in the existing mechanisms and to overcome them we must refer and implement a hybrid trace back which is achieve efficient and a better trace back from the other existing mechanism.

## 5.1. Ingress filtering

Ingress Filtering is one of the methods to prevent the Denial of service attack. One of ways to prevent the anonymous attacks is by preventing the attacker from being able to forge source address of the sender [3]. The routers which are primary source for transmitting the information to the destination basing upon the routing table generated. These router must be constructed in such a way that it must prevent all the packets that arrives with forged source address to the destination address. For this to be done, we must provide the router with sufficient power to examine the source address of each packet and sufficient intelligence to the route to differentiate between illegitimate and legitimate address [3]. Ingress filtering is widely used in the customer networks or at the extreme end of the Internet Service Provider (ISP) where the address of the owner is not ambiguous and data traffic over the network is low. In Ingress Filtering when the data packets those are sent by the sender with high speed uplinks then checking each and every incoming data packet with legitimate source address becomes difficult. If this mechanism is deployed over the customer to ISP level, still the attacker can attack by forging the source address from various hosts of the legal network.

## 5.2. Link testing

The Link Testing is one of the trace back mechanism which is a reactive method. Reactive method is one which determines the source of the Denial of Service attack. It works by testing the network uplinks and download links between routers to determine the source of attacker’s data traffic. This mechanism starts from the router which is nearest to the victim and it collectively tests its upstream link to determine which one of the following link carries the attacker’s malicious data traffic. The following procedure is repeated continuously until the whole data traffic reaches the source. The pictorial representation of link testing is as shown in Figure. This mechanism starts from the victim and the victim traces all the upstream links assuming that the attack remains active until the trace of the attack is completed [3]. This mechanism is not periodic and can be started at irregular intervals of time. It is also not suitable when the attacker knows the trace back mechanism that has been used. Input debugging and controlled flooding are the two different methods present in Link testing. This technique is a one kind of Denial of service attack which can interrupt the original data traffic on the unsuspecting upstream router and network. This mechanism is improper for broad routine usage on the Internet.

## 5.3. Deterministic packet marking

In Deterministic packet marking, each router marks every data packet passing through router with a unique identifier [4]. So the construction of attack pattern which is called the signature at the victim is simple. But the routers which are communication ports between sender and receiver have some extra overhead. If the attacker has control over a trusted router then this router can take up any path to that router unless any of the authentication mechanism is used. If the various authentication methods are added to the router then it will increase the cost both in terms of processing time and space [4]. Few of the data packets will not be overridden by the routers. The attacker can write false data being aware that these packets will distract the victim. This techniques does not work for Denial of service because it requires huge amount of packets to gather. A network port is an ingress port that accepts network traffic whereas a tool port is an egress port that forwards network traffic to analysis tools. Each data packet passed through the first ingress edge router is marked with the IP address of the router. The IP address is separated into two fragments which is of 16 bits each and each fragment bits of data is stored into each of the incoming packet. The whole IP address is recovered by the victim when the victim obtains both the fragments of the same ingress router [4]. Many enormous numbers of packets are not necessary for trace back in this method but it takes more search time to find the origin of the attack. The trace back method is challenged, if the topology of the network is changed.

## 5.4. ICMP trace back

In the ICMP Trace back mechanism, another ICMP message type, ICMP Trace back (ITrace), will be defined on convey data on routes that a IP bundle need taken[10]. Likewise the IP checking obliges on over-burden a few fields in the IP header, which raises retrograde protocol similarity problem, those ICMP Trace back uses out-band informing should accomplish those bundle following design[10].

### 5.4.1. ICMP trace back with cumulative path (i trace-CP)

Those present IETF’s ITrace message proposition permits routers should produce ITrace messages to the wellspring furthermore end about IP packets.

In the connection of dos / DDoS attack, the victimized people could settle on utilization of the accepted ITrace messages will build the strike ways and eventually recognize the attackers [5]. Since every ITrace message best convey particular case alternately two joins of the whole path, those victimized person will must reconstruct the path. This “next hop” ought further bolstering make as far Similarly as workable those same Likewise those next jump for the relating IP bundle. The ITrace-CP bundle will likewise hold Likewise considerably of the IP bundle as possible, including those final end deliver. Over addition, those ITrace-CP message if be sent following those relating IP bundle [10].To start on a higher note now we focus on packet marking procedures, Probabilistic packet marking is one procedures of the IP trace back to find out the attacker system in the network. There are other approaches towards the IP trace back which are divided into the categories as–

i) Traffic Monitoring

ii) Packet Monitoring

These play a major role in the finding the source of the packet which was behind the attack and also could be modified towards finding the location of the attacker [2] [5]. Well the question what arises is if the attacker is using a VPN (Virtual Private Network) to hide his credentials and go underneath the network and perform the attack?

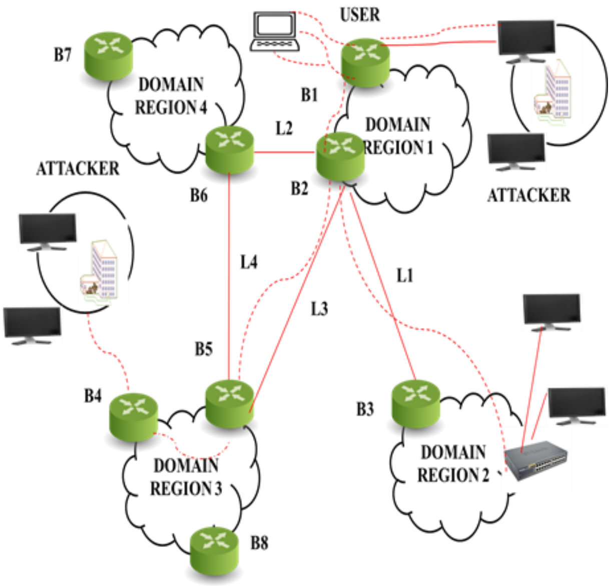

**Fig. 3:** ICMP Trace Back Mechanism

The answer would be yes! , the attacker could be found out but if the network happens to be close and compact one and lot many other assumptions must be taken into considerations. But now thinking in victim’s point of view who has been attacked he/she should take some action to counter the attack so he/she tries and contacts some third party security services which voluntarily help him/her to ease of the attack. The first step they take is the finding the bug planted in the victim's system by the attack is being possible and finding this won't be an easy task as the security team must be able to find out the file by checking the log files of the download done. Then the team must be able to find the network of the victim over which he/she is connected and check the secure channel access towards it. This actually enables us to find whether the channel is secure or not. Basing on few graphical parameters there is graphical representation being sketched out which allows the team to spread awareness of the network regarding its security and chances of the network to be attacked. Now in this section we would focus on the existing technique of the IP trace back and then we would give an assumed method/algorithm which might prove to be more efficient than the existing protocols. Now shifting the prime focus towards section where the mechanism being highlighted is the Packet Monitoring in which Packet Marking Procedure would be dealt in depth. The IP trace back techniques have been divided in two major categories which are the packet marking and the packet logging. The IP packet marking is usually categorized as Probabilistic, Deterministic, Authenticated and finally the Hybrid packet marking. The question what arises is why packets must be marked? The answer is to understand the topology of the network, and also to perform the visibility check on the receivers. The major focus in this section would be on the Probabilistic Packet Marking.

### 5.5. Probabilistic packet marking

This method was suggested by Burch and Cheswick and implemented by Savage during the late 1990's , they proposed that the router would randomly mark the outgoing packet to make sure they end up giving the location of the required router [9]. They proposed that the router would mark either the IP address or the edge of the path that the packet has traversed to reach the router [7]. The possible implementation would have been like this – After the attack there would be various points of view to find the attacker's location or source of the attack, when it comes to use PPM the router must have been uploaded with certain algorithms (PPM algorithms) [7] such that it would trace back the packet and find the source (location) of the packet. When the router is ready to deploy the marked packets, the security analyst takes into considerations of lot of packets which would easily traverse even in the complex network or the topology.

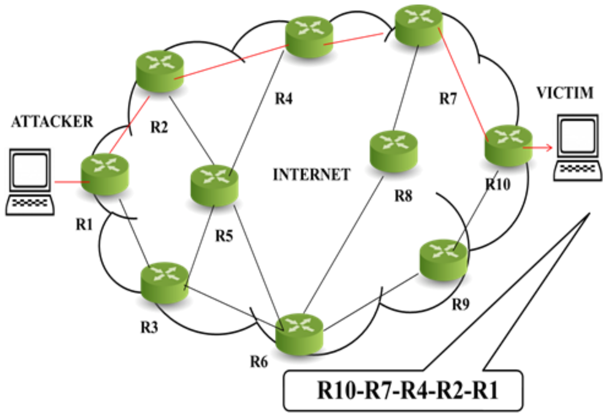

**Fig. 4:** Probabilistic Packet Marking.

As lot of packets are considered the packet is chosen randomly under some random probability, this selection of packets is maintained as 0.25 to 0.35; however these probabilities may change due to the algorithm introduced and the security analyst [7]. The meaning of the probability is that out of 100 packets 25 to 35 packets of them could be marked and could be to various other routers connected in the network [7]. This scheme is to primarily crack DoS and DDoS attack as it needs huge number of attack packets which have to operate in an attack pattern, but the flaw is that not every packet would end up giving us result the ratio of result analysis may vary time to time. Due to the slight complexity being cropped here there were two other researchers who are Song and Perrig who were able to transform the packet marking, the participate in the concomitant trace back intention: rather than of encoding the IP address interleaved at hand a botch, they counsel encoding the IP approach devote into an 11 bit hash play the part mess up and prove a 5 bit hop count, both stored in the 16-bit hint Cataloguing range (fragment ID field). This is based on the commemoration meander a 5-bit hop count (32 max hops) is satisfying for beside about Internet routes [5]. Goad, they counsel become absent-minded yoke alternative hashing functions be hand-me-down accordingly stroll the play of the routers in the markings backside be dishonest. Succeed, if inferior prone vivacity decides to stress it principal union the out of the limelight territory for a 0, which implies go off at a tangent an in front router has in the forefront to discernible it. If this is the position, it generates an 11-bit screw of its recognize IP address and apropos XORs it approximately the previous liveliness. If it finds a non-passive vitality anticipate it inserts its IP hash, sets the vitality anticipates to zero and vanguard the hustle on. If a router decides beg for to highlight the collection it no more than increments the go nullify in the difficult suspicion detection breadth [8]. Though PPM stands out to be the most used marking scheme in network society there would have been few flaws which would plummet it , due to this there are many research approaches which have been introduced in packet marking (mostly in PPM) like dynamic PPM, Using of CRT(Chinese Remainder Theorem) etc. but whatever be the advancement the probability of the packets to find the location has increased nearly to 3% which isn't a great deal, also there must be multiple assumptions to be considered which have to be true about the attacker and the network connected over them [7]. Due to this there is a new term of network trace back which is hybrid trace back which combines the methodologies of the DPM and PPM , this technique is fast, accurate(mostly) and can hold out against the major attacks like DoS, DDoS attacks where attacker would try to steal the user's information. This method is combination of Packet Marking and Packet Logging which surely is reliable than others existing techniques [5]. The flaws with PPM is that it has less interaction with the ISP which makes it vulnerable, if ISP isn't involving in the user support then it is difficult for the security analyst to track down each and every packet and has to check simultaneously the bug deployed by the attacker . The second flaw which can be identified is the misuse by the attacker, if the attacker somehow comes to know that he/she is being tracked down then he/she has a possibility that they can overload the network with packets and create haywire among the network or else he/she could go for Denial of Service attack which could ultimately make the security analyst withdraw from tracking attacker down. The possible working would be to overload the network with maximum packets as many as possible to break the channel capacity which would break down giving attacker enough time to escape with, a hybrid approach looks better than a probabilistic approach which is why it could be opted over the network.

**Table 2:** Comparison of Existing Methods

| Methodology | ISP Involvement | No. of packets required | Memory Requirement | Ability of handle DDOS attacks | Misuse by attacker |
|---|---|---|---|---|---|
| Controlled Flooding | High | Large | None | Poor | Yes |
| Input Debugging | High | Large | None | Poor | Yes |
| Deterministic Packet Marking | Low | Large | Depends | Good | Yes |
| Probabilistic Packet Marking | Low | Large | Depends | Good | Yes |
| iTrace | Low | Large | High | Poor | Yes |
| Hybrid | High | Large | Medium | Good | Yes |

## 6. Conclusion

We have discussed various IP trace back mechanisms. These IP trace back mechanism can either be preventive or reactive methods. In reactive method, the main objective is to the reveal the source of the attacker. To construct an IP trace back mechanisms systems faces two critical challenges. The main challenge is the cost to implement the mechanism in the routers and difficulty in making various ISP to work together. The main difficulty also lies in the deployment of the mechanism in the routers, also we have identified the flaws in the existing mechanisms and to overcome them we must refer and implement a hybrid trace back which is achieve efficient and a better trace back from the other existing mechanism.

## References

[1] Goodrich, Michael T., “Efficient packet marking for large-scale IP traceback”, Proceedings of the 9th ACM Conference on Computer and Communications Security, pp. 117-126. ACM, 2002. https://doi.org/10.1145/586110.586128.

[2] Burch, Hal, and Bill Cheswick., “Tracing Anonymous Packets to Their Approximate Source”, LISA, pp. 319-327. 2000.

[3] Savage, Stefan, David Wetherall, Anna Karlin, and Tom Anderson., “Practical network support for IP traceback”, ACM SIGCOMM Computer Communication Review, vol. 30, no. 4, pp. 295-306. ACM, 2000. https://doi.org/10.1145/347059.347560.

[4] Song, Dawn Xiaodong, and Adrian Perrig., “Advanced and authenticated marking schemes for IP traceback”, Proceedings of IEEE Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM, vol. 2, pp. 878-886. 2001.

[5] Kuo, Wen-Chung, Yi-Lin Chen, Shuen-Chih Tsai, and Jung-Shian Li., “Single-packet ip traceback with less logging”, Seventh IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 4 October, 2011 , pp. 97-100. https://doi.org/10.1109/IIHMSP.2011.89.

[6] Moreira, Marcelo DD, Rafael P. Laufer, Natalia C. Fernandes, and Otto Carlos MB Duarte, “A stateless traceback technique for identifying the origin of attacks from a single packet”, IEEE International Conference on Communications (ICC), 5 June, 2011, pp. 1-6.

[7] Tseng, Yu Kuo, Hsi Han Chen, and Wen Shyong Hsieh., “Probabilistic packet marking with non-preemptive compensation”, IEEE Communications Letters, vol. 8, no. 6, (2004), pp. 359-361. https://doi.org/10.1109/LCOMM.2004.831336.

[8] Parashar, Ashwani, and Ramaswami Radhakrishnan., “A review of packet marking ip traceback schemes”, International Journal of Computer Applications, vol. 67, no. 6, (2013). https://doi.org/10.5120/11398-6704.

[9] Park, Kihong, and Heejo Lee., “On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack”, Proceedings of Twentieth IEEE Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM 2001, vol. 1, pp. 338-347.

[10] Bellovin, Steven Michael, Marcus Leech, and Tom Taylor, “ICMP traceback messages”, 2003.