Available online at www.worldscientificnews.com

World Scientific News

WSN 40 (2016) 12-22 EISSN 2392-2192

Survey of Several IP Traceback Mechanisms and Path Reconstruction

Dr. M. Newlin Rajkumar[1,a], R. Amsarani[2,b], M. U. Shiny[2,c]

[1]Assistant Professor, Department of CSE, Anna University Regional Centre, Tamil Nadu, India

[2]PG Scholar, Department of CSE, Anna University Regional Centre, Tamil Nadu, India

[a-c]E-mail address: newlin_rajkumar@yahoo.co.in , rk.amsa@gmail.com ,
Sarakrishnan.r@gmail.com

ABSTRACT

In real world the peoples having a lot of attacks troubles in the network. The unauthorized persons or hackers are use the another person’s IP address or use the attackers nearest IP address with in the area. If some kinds attacks such as DOS, DDOS attacks are create a lot of issues in network so difficult to find the spoofers or attackers. In this papper presents the Several IP Traceback Mechanism and Path Reconstruction.

Keywords**:** Dos attack; Packet marking; Packet logging; Probabilistic packet marking; Hash based scheme; reflector attack; ICMP; passive IP traceback; contol flooding; input debugging

1. INTRODUCTION

IP is an INTERNET PROTOCOL each and every system having an unique address. To use this address to communicate to the internet. In world day to day create a lot attacks to network. The attacker spoofing the source address or use nearest address so overcome these kinds of attacks and find the spoofers origin. Section II, section III describes the several mechanism of IP traceback and path reconstruction.

2. SEVERAL MECHANISMS OF IP TRACEBACK

2. 1. Large-Scale IP Traceback in High-Speed Internet and Information-Theoretic Foundation

IP traceback mechanism using two kinds of techniques that are:

i) Probabilistics Packet Marking (ppm) schemes - It is mark the each packet with partial path information, by receiving a number of packets.

ii) Hash based scheme- It having Bloom Filter is store the packet digit and neighbouring routers are iteratively checks the each packet and it is also construct path for attack packets

Issues

i) Ppm based scheme is only suit for small number of attackers ,due to the limited number of bits available for marking the IP header.

ii) Hash based scheme support large scale of IP traceback but it needs only a single packet to trace one attacker.

So overcome these difficulties we proposed a Novel Packet Logging based Traceback Scheme, that is scalable to high link speed and Novel Information Theoretic framework. The a small percentage of packets to be sampled then construct the attack tree using the correlation between the attacks sampled by neighbouring attacks.

Packets to be sampled and its method improved their performance and overall efficiency and to reduce the computational and storage overhead. The novel information theoretic framework provide the fundamental tradeoff between the packets used for traceback, and it also to compute the minimum number of attack packets needed for find the traceback and to study the scalable performance of number of attacks.

2. 2. IP traceback of DPM and DFM methods

2. 2. 1. Deterministic packet marking

DPM is traces the close edge router to the attacker it use the ingress interface to the attacker. DPM uses 17 bits of the IP header, the 16 bits used in Identification field and 1 bit is reserved flag. Each and every packet to be marked and it used 32 bit ingress interface, the IP address is split into two segments. Each segment having 16 bits. The first segment in 0-bit 0 to 15, second segment in 1-bits 16 to 31.

Each packet passed through an edge router, one segment is selected with equal probability of the packet and inserted in the identification field. The victim maintains a table matching the source addresses to the ingress addresses. When the victim receive both segments of an edge router, then it is to reconstruct the routers ingress interface of the IP address.

The reserved flag is used for victim to identify which part of IP address is carried by the current packet. It should be noted only marked incoming packets and not outgoing packets.

DPM has two key features:

1. DPM only marks the closest ingress edge router to the attacker.
2. DPM marks all packets at the ingress interface of the edge routers.

DPM has several advantages:

1. **Computational Overhead:** The CPU overhead of DPM is lower than Probabilistic Packet Marking scheme. DPM reconstructing the edge router ingress interface IP address is more simpler than the ppm attack path reconstruction process of approach.
2. **Memory Overhead:** the victim keeps only a small reconstruction table. DPM needs only *32/a* packets to reconstruct the ingress address.
3. **False Positive Rate:** Multiple attackers to be used a same source IP address at a same time, in this situation the victim can not recognize which marked packet is valid mark, this causes high false positive rates so overcome this problem, we use the method of single hash function to produce hash values of the ingress interface is called Single Digest DPM Technique or use a family of hash functions to produce multiple digest of an ingress address is called Multiple Digest DPM Technique.

2. 2. 2. Deterministic flow marking

DFM allows the victim to trace the origin of the spoofed source addresses up to the attacker node, even if the attack has been originated from a network behind for example a proxy server.

DFM uses three identifiers to mark a flow:

i. The IP address of the output or forwarded interface of the edge router.
ii. The NI-ID, which is an identifier assigned to each interface of having the MAC address of a network interface on the edge router or the VLAN ID of a virtual interface if the edge router uses VLAN interfaces.
iii. Node-ID, which is an identifier assigned to each source MAC address observed on incoming traffic from local networks.

2. 3. Network support for IP traceback

Here we trace the IP Traceback using two method that are Packet Marking and Partial Path. Each packet to be mark with Partial Path Information by routers. In this approach comprise the large number of packets, while each marked packet repents sample of the path it has traversed and it combining by number of packets. The packets in the victim can be reconstruct and it easily find out the source of attack traffic without required from Internet Service Provider (ISP). This approach to overcome the Denial of Service and Flooding Attack.

2. 4. Link testing

Link Test is test the upstream link between the routers. It find the source traffic of the attackers traffic. This approach starts closet router to victim. The router observe the upstream link then it find the attacker traffic. The attack to remain active until it complete a trace. It having two types of link testing approach 1. Input Debugging 2.Controlled Flooding

2. 4. 1. Input Debugging

A network operator or administrator is determine the input port for particular packets. The victim develop an attack signature, it having some kinds of features containing all attack packets. The victim first communicate that signature to a network operator and the upstream routers are determined origin of the traffic and it connects ISP. The ISP tools are automatically trace the attacks. In this system is called Center Track. It improves over hop by hop backtracking by router.

2. 4. 2. Controlled Flooding

It tests the links by large bursts of traffic. In this approach using map of internet topology and it determine how flood affects the attack traffic. The victim connects closet router upstream link. It route into iteratively flooding each incoming link then router buffers to be shared.

2. 5. Marking and logging

IP traceback based on packet marking is referred to as probabilistic packet marking (PPM). The PPM approach packets are marked with partial path information then it forwarded to the destination by routers.

Disadvantages of Probabilistic Packet Marking:

i. Routers overhead.
ii. It can only determine the source of the traffic composed of a number of packets in the path.

IP traceback based on packet logging is referred to as hash-based approach. Here routers to be compute in path and each forwarded packet to be stored with digitest. In this approach requires only an individual packet to trace its corresponding source.

Disadvantages of Hash based Approach:

i. It requires more storage space for packet digest.
ii. It requires more access time for routers.

We propose an IP traceback approach based on both packet marking and packet logging. Compared with the PPM approach, our approach is able to trace individual packets. Compared with the hash-based approach, our approach having less storage overhead with less access time overhead in routers.

Here we introduced a hybrid IP traceback approach based on both packet marking and packet logging. In hashbased IP traceback approach based packet marking is needs only the single packet to trace the IP. Each packet to be mark with information about router identification and it to be forwarded to the destination.

Advantages of Packet Marking:

i. It reduce the storage overhead for packets.
ii. It reduces the access time overheads at routers.

In our approach, each router can commit both marking and logging operations on packets. The logging operation is to record the forwarded packet digest and the marked packet carried by router. The logging operation on a packets are record the current router but it also record the upstream routers on the network path followed by the packet. It record the path of packet and it needs only the logging packet in path and it does not need all routers in the path.

The packet requires only traversed routers in path. The packet refered to be use those information stored in routers. It maintains a different digest table for neighbouring routers with its identification field. Each routers define a table for its neighbouring routers. Each incoming packet to be stored in a neighbouring routers.

Advantages of Packet Logging:

i. It reduce the storage overheads in routers.
ii. It reduce the access time for recording packets by neighbouring routers.

2. 6. Reflector attack

A reflector attack is an indirect attack in that intermediary nodes such as routers and various server as known as reflectors. Some major reflector attacks such as smurfing, SYN flooding, RST flooding, ICMP flooding and DNS reply flooding. For Example a smurfing attack spoofing a number of ICMP ping packets with the victim's Source IP address it directly broadcast the message to the destination address. It consume a lot of network issues and host resources with few packets as spoofed. There are three components in a reflector attack 1. The attacker, 2. The amplifying subnet, 3. The victim. The attacker sends ICMP ping packets with the using the victim's source IP address to the broadcast address of an amplifying the destination address. So the destination address assumes the packet was sent by the victim. Since it sent to a broadcast address of a local network, and all the hosts, each packet will responds that message but except those whose configuration has been specified not to respond to ICMP broadcast packets, in the local network. So we found the smurf is a kind of amplified DoS attack. This amplifying effect is able to determine an individual reflector attacker can send the packets at a lower rate compared to the packet rates created by attacker of the victim. To provide some solutions to against the reflector attacks. For example smurfing attack: solution is invisible the translation of layer 3 broadcasts packets into layer 2 broadcasts at the border router; that is, the router was filtered any packet with a broadcast source address. This disable of layer having many useful services such as ARP, audio sharing. Another solution is configuring the not respond host to broadcast ping packets or to ignore all ping packets. We use this approach the ICMP functionality to be loss.

2. 6. 1. Reflective marking scheme

Figure 1, describe the victim map the upstream routers. We use *V-victim*, *R-router*, and *A- attacker* to denote respectively. An upstream routers map is map the topology of the upstream routers of a single host. The upstream routers map define the upstream routers IP addresses. For ex, *R*9 and *R*10 are the upstream routers of *A*2. In this graph, there are two attack paths that are represented , one is (*A*1 *R*6 *R*3 *R*2 *R*1), and the other is (*A*2 *R*3 *R*2 *R*1). To meaure the distance between two hosts it means the number of routers in the attack path between them.

For example, in the attack path (*A*1 *R*6 *R*3 *R*2 *R*1), it measures the distance between router *R*6 with victim and the victim is 3. some routers to be failed by the attacker and the marking packets may be forged. Some kinds of the traceback problem to finding a source attack path it contains a suffix of the original attack path, and such a suffix is called a valid suffix of that path. For example, path (*R*6 *R*3 *R*2 *R*1) is a valid suffix of the original attack path (*A*1 *R*6 *R*3 *R*2 *R*1). Here we finding the real attack path where compare to source path as valid suffix path. We define a router false positive it is reconstructed the attack path.

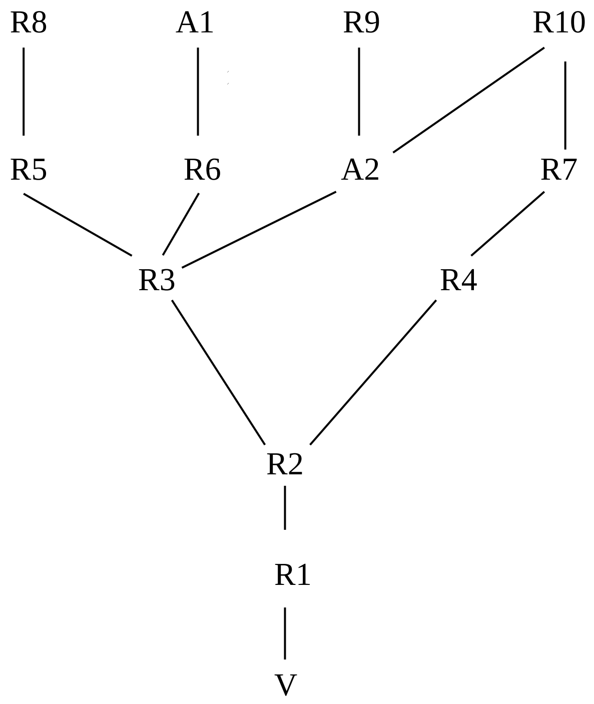

Fig 1. The upstream routers map from victim with attackers.

2. 7. ICMP approach for IP traceback

This approach is based on routers, the router generated ICMP traceback maessage when hacker hacking the packets. The every router to be sample with low probability, the packets to be forwarding and copy the contents into a some special ICMP Traceback message including information about the adjacent routers with destination path. For example flooding attack is involes, the victim host can use these messages to reconstruct an entire path back to the attacker. ICMP message traffic itself be filtered in a network under attack; the ICMP Traceback message having an input debugging capability such as the able to associate a packets with the input port and/or MAC address. some router architectures not having these special ability as arrived informations to the victim. It is difficult to connect the traceback messages from participating routers separated by comparing a nonparticipating router and The victim requires a key distribution from destination and the attackers sending false ICMP Traceback messages to the victim. So easily found the attacker. In this approach is widely used for traceback mechanisms.

2. 8. Passive IP traceback mechanism

Passive IP Traceback techniques are designed to disclose the original origin of IP traffic or track the path of the spoofers. An Existing IP traceback approaches can be classified into five categories that are packet marking, ICMP traceback, logging on the router, link testing, overlay, and hybrid tracing.

1. In **Packet marking** methods require routers to modifying the packets header to containing the information about router and forwarding decision about paths. The receiver of the packet can then reconstruct the received packets path or an attackers path. There are two methods for packet marking schemes.

i. probabilistic packet marking *ii.* deterministic packet marking. Packet marking methods are lightweight because it do not having routers resource of cost storage and the link bandwidth resource. But packet marking is not suitable for all function on routers; so, packet marking is harder to traceback in the network.

2. The **ICMP traceback** routers generates ICMP messages to the destination. The ICMP messages can be used to reconstruct the attacking path in the network. Here we maintain a log record for routers information with forwarding packets path. Suppose the attacker attacks the path , we use this log record. The Bloom filter is used to less bits to store a packet. It achieve a low collision probability in current high-speed networks, But the storage cost is higher for commodity routers.

***3.* Link Test** is test the upstream link between the routers. It find the source traffic of the attackers traffic. This approach starts closet router to victim. The router observe the upstream link then it find the attacker traffic. A controlled flooding mechanism based on performing tests the links by large bursts of traffic. In this approach using map of network topology and it dertermine how flood affects the attack traffic. The victim connects closet router upstream link. It route into iteratively flooding each incoming link then router buffers to be shared. But, In this approach is hard to perform at the Internet level.

4. The **overlay network** can reduce the edge routers requirements but the overlay network will be significantly increase overhead of network management. Here we use building an AS-level overlay to trace spoofers. The overlay network combine the hundreds of ASes so we found the accurate location of spoofers. The challenge in this approach is how to make the cooperate of ASes. But the intra-domain version can avoid this problem, but OSPF requires necessary to update the routers modifications. The above all mechanisms to be combined to achieve better tracing capacity and reduce the cost.

5. The **hybrid mechanisms** employ both packet marking and logging. It reduce routers overhead, Both mechanism support to router; But it barrier to adopt is higher than adopting a single mechanism.

The Passive IP Traceback (PIT), to bypass the challenges in deployment, Suppose Routers may fail to forward an IP spoofing packet due to various reasons that are TTL exceeding, packet was lossed. In such cases, the routers may generate an ICMP error message as named path backscatter and send the message to the spoofed source address.

WHEN PATH SCATTER MESSAGE TO BE GENERATED:

A network device may fail to forward a packet due to various reasons. Under certain conditions, it may generate an ICMP error message, The path backscatter messages will be sent to the source IP address indicated in the original packet. The path scatter message contaning some formats suppose If the source address is forged, the messages will be sent to the original node At the victims collects message of reflection based attacks, and the neighbouring host addresses are used by spoofers. Each message in packets contains the source address of the reflecting device, and the IP header of the original packet. The reflecting device which is on the path from the attacker to the destination of the spoofing packet. the IP address of the *original* destination of the spoofing packet. The original IP header also contains other valuable information, the remaining TTL of the spoofing packet and which information to be sent.

Using this path scatter message to find the attacker location but it requires separate router storage and high bandwidth requirements .

This approach used three special types of path backscatter messages which are more useful for tracing spoofers:

1. The path backscatter messages source original hop count is 0 or 1. Such messages are generated 1 or 2 hops from the spoofer.
2. The path backscatter messages whose type is ‘Redirect’. Such messages must be from a gateway of the spoofer.
3. The path backscatter messages are typically generated by DFZ router on the path from the spoofer to the original destination.

2. 9. Fast internet traceback (FIT)

The Fast Internet Traceback (FIT) is uses a probabilistic packet marking schemes and it consists of two major methods that are 1. packet marking scheme to be deployed at routers 2. path reconstruction algorithms used by victim. The victim receiving the markings packets with identity. The fast internet traceback scheme improves the traceback methodology to identifying the attack path with high probability, it find only with two or three attack packets in path and it also improves routers information it maintains an interface of packets table and it can determine large scattered attacks. FIT scheme uses this upstream router map information with packet markings of that fragment. The marking packets and reconstruction algorithms which improves its performance. The fast internet traceback scheme contains three steps:

1. FIT generate the upstream router map using packet markings from attack victim.
2. FIT is allows the node or victim to be sampled, this method is more effectively reducing the number of false positives and it reconstruct the number of packets required for attack path.
3. FIT uses only 1-bit for IP id field to mark the distance from the victim at which the packet was marked.

Fast Internet Traceback Scheme is more reliable than hash based tracing method and it use few bits compare than hash based traceback method and it increase performance and accurability.

2. 10. Advanced and authenticated packet marking (AAPM)

Advanced and Authenticated Packet Marking (AAPM) uses hash functions to reduce the requirement storage space for augmenting router information in the IP header. The attacker uses a compromised router in the victims path.it attack packets or it can forge that packets, so we can determine and prevent the marking packets in victim from the compromised router. To solve this problem to introduced a mechanism to authenticate the packet marking. The process is the marking of packets to be digitally sign in the router. But digital signatures having two disadvantages, that are its computation is very expensive and its space overhead is larger. So, it's an reliable technique to authenticate the packet marking. The packet making use this AAPM technique only uses one cryptographic MAC (Message Authentication Code). So, it is more efficient to compute than others and can be easily adaptable to packets because it requires the 16-bit overloaded IP identification field for storage.

2. 11. A practical approach for single-packet IP traceback

Here We using packet marking and logging, that is called Hybrid Single-Packet IP Traceback (HIT) Approach has been introduced. In this approach in compared to SPIE method is used to trace a single IP packet with reducing the storage overhead by half and the access time overhead by the number of neighbouring routers. In this approach the routers can uses both packet marking and packet logging operations. Router will mark and log each packets and it to be forwarded to the destination through it depending upon the space availability in packets in path buffer. In packet logging, to log the current router by router with it provide the alternate router in its path. The marking field of a packet resides the identification information of a single router. The packets to be traversing in the network, the routers marks the each packet in the path but log the packets are alternately. In HIT, router is assigned a 15 bit ID number. The remaining 15 bits are used to store a router ID number. If the logging flag is set to 0, the router define to process to both packet logging and marking, if logging flag is set to 1 then the router define to process only a marking operation. In this approach is effectively managed by traceback servers apparelled with the network topology information. Suppose the attacker attacks the packets in path then the server to inform to Victim with an attack packets and its time if attack. Each and every packet containing a value of the logging flag bit, so the traceback server can determine whether the last router logged the packet. And also the traceback server will inform to the router which in turn checks all packet digests and also checks the time provided by sever. If an any other additional entry in the packet then that router is dertermined to be on the attack path, and it consist collecting of routing ID which states the upstream routers on the path.

3. PATH RECONSTRUCTION

In this method using two approach for findind the attacker that are Packet Marking and Packet Logging.

1. The **Packet Marking** -is stored information about path in the packet, each packet to be marked and it contains the source address with destination address and to be forwarded the packets to destination address, the destination receives the packet with network path information in packet header.
2. The **Packet Logging** -is stored information about path in the router. here we used the log based IP Traceback method the packets are logged by router with network path information in router.

In existing system router maintain the router interface table it contain the information about number of routers and maintain a hash table for making packet values. The IP header using 32 bit marking field. The corner routers receives the packets from local network and it forwarded to the next router is marking the packet as zero field.

The next router marks the packet as new mark value. The overflow's marking packets are logged in router and this process to be continues until reach their destination address. The marked packets value in router are stored by hash table suppose the packet was spoofed, we refer the hash table mark packets value and we find the origin attacker during this process of path reconstruction .In proposed system use the link state routing approach the router contains the information about network topology with connectivity in the network. Once the packet to be forwarded it performs the Qos routing by computing path is based on number of multiple Qos constraints is called multiple constrained path. If suppose the router 2 failed and router choose nearest router or next router, here we use the next router information having one hop count from its corresponding router. This process to be continues until it reaches the destination.

3. 1. Process of alternate path

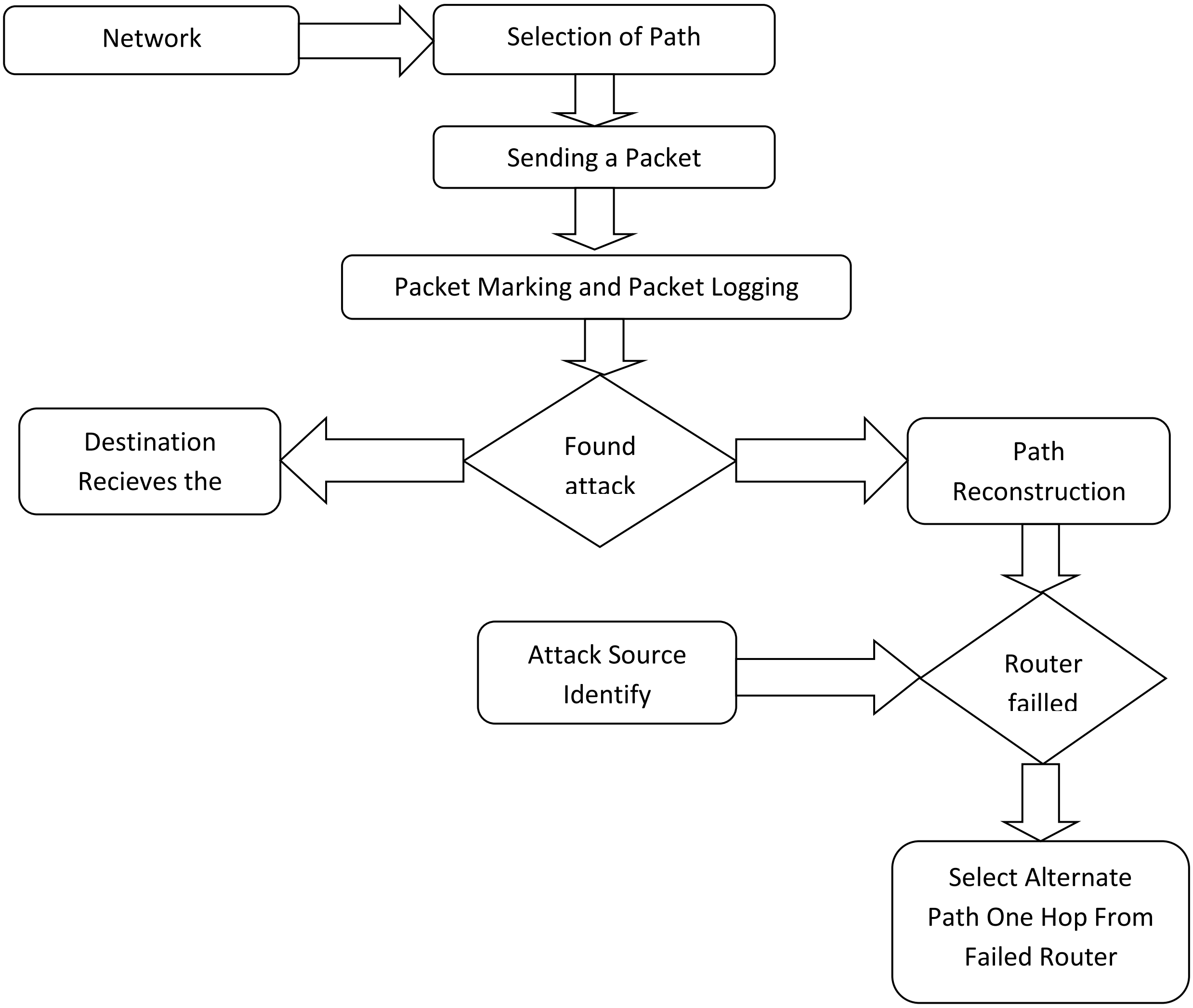

Fig. 2. Process of Alternate Path.

4. CONCLUSION

This paper describes survey of several IP Traceback mechanism for several attacks and it is also define the path reconstruction method. Different IP Traceback mechanisms are available for identify such kinds of Dos attacks. In real world difficult to provide a security to corresponding authorized persons and difficult to trace the attackers origin, so we motivate work on ICMP Traceback mechanism with less computation storage and cost overhead

References

[1] Sung M, Jun (Jim) Xu, Jun Li (2004). ‘Large-Scale IP Traceback in High-Speed Internet: Practical Techniques and Information-Theoretic Foundation‘, Vol. 7.

[2] Vahid A and Nur Zincir-Heywood A (2013). ‘On Evaluating IP Traceback Schemes: A Practical Perspective’, Vol. 8, No. 2.

[3] Savage S, David Wetherall, Anna K, and Tom Anderson (2001). ‘Network Support for IP Traceback‘, pp. 295-306.

[4] Savage S, David Wetherall, Anna Karlin and Tom Anderson (2000). ‘Practical Network Support for IP Traceback’, Vol. 29, No. 9.

[5] 3Cheng J, Haining, Kang G. Shine (2008). ’Hop Count Filtering: An Effective Defense Against Filtering Spoofed Traffic’. Vol. 9, No.1.

[6] Gong C and Kamil Sarac (2009). ‘IP Traceback based on Packet Marking and Logging‘, Vol. 9, No.6.

[7] Chen Z, Moon-Chuen Lee (2003). ‘An IP Traceback Technique against Denial-of-Service Attacks’, Vol. 40, No.10.

[8] H.C. Lee, V.L. Thing, Y. Xu and M. Ma (2003). ’Icmp Traceback with Cumulative Path Efficient Solution for Ip Traceback’ ,pp. 124-135.

[9] Guang Yao, Jun Bi Athanasios, V. Vasilakos (2015). Passive IP Traceback: Disclosing the Locations of IP Spoofers From Path Backscatter Vol 10,No 2.

[10] K. Jeeva, N. Duraipandian (2014). Hybrid IP Traceback Involving Path Reconstruction Using Qos. ISSN 1990-9233.

[11] Yaar, A. Perrig, and D. Song, “FIT: Fast internet traceback,” in Proc. IEEE 24th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM), vol. 2. Mar. 2005, pp. 1395-1406.

[12] C. Gong and K. Sarac, “A more practical approach for single-packet IP traceback using packet logging and marking,” IEEE Trans. Parallel Distrib. Syst., Vol. 19, no. 10, pp. 1310-1324, Oct. 2008.

[13] D. X. Song and A. Perrig, “Advanced and authenticated markingschemes for IP traceback,” in Proc. IEEE 20th Annu. Joint Conf. IEEE. Comput. Commun. Soc. (INFOCOM), Vol. 2. Apr. 2001, pp. 878-886.

(Received 24 January 2016; accepted 04 February 2016)