www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 10 Oct. 2016, Page No. 18232-18238

Secured Icmp Based Ip Traceback Scheme To Trace The Spoofed Ip Locations

V. Mariyammal[1], Dr.K.Thamodaran[2]

[1]MPhil. Research Scholar, Dept. of Computer Science,
Marudupandiyar College, Thanjavur,
Tamilnadu, India-613 403.
Mail_id : meet_mariyaa@yahoo.co.in

[2]Professor, Dept. of Computer Science,
Marudupandiyar College, Thanjavur,
Tamilnadu, India-613 403.
Mail_id : k_thamodharan@rediffmail.com

Abstract: ***The Internet Protocol (IP) is the basic protocol for sending data over the Internet and many other computer networks. IP spoofing is the creation of Internet Protocol (IP) packets with a forged source IP address, with the purpose of thrashing the identity of the sender or an attacker can make it appear that the packet was sent by a different machine. The objective of this paper is to devise the passive IP trace back (PIT) scheme using Internet Control Message Protocol(ICMP) to avoid the operational obstacles of IP trace back schemes. PIT investigates ICMP error messages (path backscatter) triggered by spoofing traffic, and tracks the spoofers based on public available information (eg.topology). This scheme(PIT) discover the spoofers without any operational requirement and exhibits the causes, collection, and the statistical results on path backscatter, demonstrates the processes and effectiveness of PIT, and shows the captured locations of spoofers throughout applying PIT on the path backscatter data set. These results are capable of expose the spoofed IP locations.***

Keywords: ICMP, Internet Protocol, IP Spoofing, IP Traceback, Path Backscatter.

1. Introduction

Network Security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers. The protocol that specifies the way data is broken into packets and the way those packets are addressed for transmission. Internet Protocol is a communications protocol for computers connected to a network, especially the Internet, specifying the format for addresses and units of transmitted data. The IP is one of the two most important protocols TCP/IP that makes internet possible. IP divides flow of data into packets (each carrying up to 65,535 eight-bit bytes) and attaches a header containing forwarding address for its correct transmission to the intended receiver. Spoofing of user identity describes a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. Information Disclosure (Privacy violation or Data leak) describes a situation where information, thought as secure, is released in an untrusted environment.

Security system must provide guarantee that no data are disclosed to unauthorized parties. Data should not be modified in illegitimate ways and legitimate user can access the data.
IP Spoofing, which means attackers launching attacks with forged source IP addresses, has been recognized as a serious security problem on the Internet for long [1]. IP spoofing can also be a method of attack used by network intruders to defeat network security measures, such as authentication based on IP addresses. This method of attack on a remote system can be extremely difficult, as it involves modifying thousands of packets at a time. This type of attack is most effective where trust relationships exist between machines. By spoofing a connection from a trusted machine, an attacker on the same network may be able to access the target machine without authentication [3], [4]. IP spoofing is most frequently used in denial-of-service attacks. In such attacks, the goal is to flood the victim with overwhelming amounts of traffic, and the attacker does not care about receiving responses to the attack packets. Packets with spoofed addresses are thus suitable for such attacks. They have additional advantages for this purpose and they are more difficult to filter since each spoofed packet appears to come from a different address, and they hide the true source of the attack [6]. By using addresses that are assigned to others or not assigned at all, attackers can avoid exposing their real locations, or enhance the effect of attacking, or launch reflection based attacks. A number of notorious attacks rely on IP spoofing, including SYN flooding, SMURF, DNS amplification etc. A DNS amplification attack which severely degraded the service of a Top Level Domain (TLD) name server is reported in [12].

Denial of service attacks that use spoofing typically randomly choose addresses from the entire IP address space, though more sophisticated spoofing mechanisms might avoid unroutable addresses or unused portions of the IP address space Backscatter, a technique used to observe denial-of-service attack activity in the Internet, relies on attackers' use of IP spoofing for its effectiveness [11]. Denial of Service (DoS) attack attempts to generate a huge amount of traffic to the victim and thereby disrupting the service or degrading the quality of service, by depleting the resources. Distributed Denial of Service (DDoS) attack is a distributed, co-operative

and large-scale attack. Attackers can launch the attack traffic from various locations of Internet, exhausting bandwidth. The processing capacity or memory of the target machine or network is drained, taking advantage of the vulnerabilities and anonymous nature of Internet [9], [17]. The packets sent will have spoofed IP addresses which makes it practically difficult to identify the real location of attackers. Defending an attacker with spoofed IP address is more complex and this motivates the research on IP traceback, which is a methodology to trace the true origin of spoofed IP packets [2], [4]. IP traceback 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) [10], [13], [15],[16], [18], [20]. The MIT Spoofer Project tries to disclose which networks are able to launch spoofing based attacks. Volunteer participants install a client that tests the spoofing ability of their hosts and networks. The statistic result shows 6700 Ass out of 30205 do not filter spoofing[19].

Virandra Patil et al. have offered the passive IP traceback (PIT) that sidesteps the sending challenges of IP traceback strategies. PIT examines Internet Control Message Protocol blunder messages (named way backscatter) activated by mocking movement, and tracks the spoofers in light of open accessible data (e.g., topology).Along these lines, PIT can find the spoofers with no game plan need. This strategy represent the reasons, accumulation, and the authentic results on way backscatter, displays the systems and adequacy of PIT, and shows they got regions of spoofers through applying PIT in transit backscatter data set. These outcomes can assist further with uncovering IP spoofing, which has been examined for long however never surely known. In spite of the fact that PIT can't work in all the spoofing attacks, it might be the most valuable instrument to follow spoofers before an Internet-level traceback framework has been sent in genuine[21].M. Mohammed Imran et al. illustrates the causes, collection, and the statistical results on path backscatter, demonstrates the processes and effectiveness of PIT, and shows the captured locations of spoofers through applying PIT on the path backscatter data set. It may be the most useful mechanism to trace spoofers before an Internet-level trace back system has been deployed in real [22].

The rest of this paper is organized as follows. The Section 2 offers the information about Internet Protocol and Internet Control Message Protocol. The Section 3 describes about the IP Spoofing. The concept of Path Backscatter Messages and Passive IP Traceback is expressed in section 4. Then section 5 illustrates about the proposed secured ICMP based IP Traceback Scheme to trace the spoofed IP locations. The results and discussion are presented in Section 6 and Section 7 concludes this paper.

2. Internet Protocol and Internet Control Message Protocol

2.1 Internet Protocol (IP)

Internet Protocol (IP) is a Network Layer Protocol. The IP protocol defines the basic unit of data transfer (IP datagram) and IP software performs the routing function. IP is consisting of a set of rules that represent the idea of unreliable packet delivery that is i) How hosts and routers should process packets, ii) How and when error messages should be generated, iii) The conditions under which packets can be discarded. The IP relies on several other protocols to perform necessary control and routing functions such as control functions eg. ICMP, multicast signaling eg. IGMP, Setting up routing tables eg. RIP, OSPF, BGP, PIM, etc.

2.2 Internet Control Message Protocol (ICMP)

The Internet Control Message Protocol (ICMP) is a helper protocol that supports IP and all ICMP packets are encapsulated as IP datagram. ICMP messages are divided in to two namely error-reporting messages and query messages. The error reporting messages report problems that a router or a host(destination) may encounter. The query messages get specific information from a router or another host. It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached. ICMP

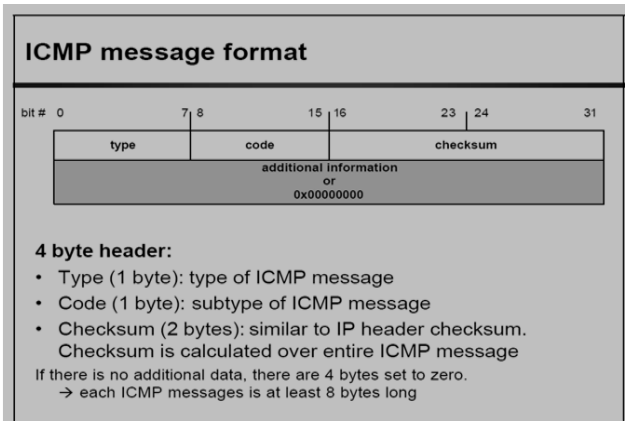

Figure 1: General Format of ICMP Message

can also be used to relay query messages. It is assigned protocol number. The ICMP differs from transport protocols such as TCP and UDP in that it is not typically used to exchange data between systems, nor is it regularly employed by end-user network applications. The figure 1. shows the general format of ICMP messages. The table1. contains the information about categories ICMP messages.

Table 1 : The Categories of ICMP Messages

Category	Type	Message
Error-Reorting Messages	3	Destination Unreachable
	4	Source Quench
	11	Time Exceeded
	12	Parameter Problem
	5	Redirection
Query Messages	8 Or 0	Echo Request Or Reply
	13 Or 14	Timestamp Request Or Reply
	17 Or 18	Address Mask Request Or Reply
	10 Or 9	Router Solicitation Or Advertisement

3. IP Spoofing

IP spoofing, which means attackers launching attacks with forged source IP addresses, has been identified as a severe security issue on the Internet. By using addresses that are assigned to others or not assigned at all, attackers can avoid finding their original locations, or enhance the effect of attacking, or launch reflection based attacks. IP spoofing can also be a method of attack used by network intruders to defeat network security measures, such as authentication based on IP addresses. This method of attack on a remote system can be extremely difficult, as it involves modifying thousands of packets at a time. This type of attack is most effective where trust relationships exist between machines[7].

The concept of IP spoofing, was initially discussed in academic circles in the 1980's. While known about for some time, it was primarily theoretical until Robert Morris, whose son wrote the first Internet Worm, discovered a security weakness in the TCP protocol known as sequence prediction. Stephen Bellovin discussed the problem in-depth in Security Problems in the TCP/IP Protocol Suite, a paper that addressed design problems with the TCP/IP protocol suite. Another infamous attack, Kevin Mitnick's Christmas Day crack of Tsutomu Shimomura's machine, employed the IP spoofing and TCP sequence prediction techniques. While the popularity of such cracks has decreased due to the demise of the services they exploited, spoofing can still be used and needs to be addressed by all security administrators.

IP spoofing is most frequently used in denial-of-service attacks. In such attacks, the goal is to flood the victim with overwhelming amounts of traffic, and the attacker does not care about receiving responses to the attack packets. Packets with spoofed addresses are thus suitable for such attacks. They have additional advantages for this purpose and they are more difficult to filter since each spoofed packet appears to come from a different address, and they hide the true source of the attack. Denial of service attacks that use spoofing typically randomly choose addresses from the entire IP address space, though more sophisticated spoofing mechanisms might avoid unroutable addresses or unused portions of the IP address space[8], [14].

The process of detaining the origins of IP spoofing traffic is a tough job. Provided that the real locations of spoofers are not revealed, they cannot be deterred from launching further attacks. Even just approaching the spoofers, for example, determining the ASes or networks they reside in, attackers can be located in a smaller area, and filters can be placed closer to the attacker before attacking traffic get aggregated. The last but not the least, identifying the origins of spoofing traffic can help build a reputation system for ASes, which would be helpful to push the corresponding ISPs to verify IP source address.

3.1 Categories of Spoofing Attacks

The spoofing attacks are classified in to various categories which are effectively employed in IP spoofing by the attackers.

i.) **Non-Blind Spoofing :** This type of attack takes place when the attacker is on the same subnet as the victim. The sequence and acknowledgement numbers can be sniffed, eliminating the potential difficulty of calculating them accurately. The biggest threat of spoofing in this instance would be session hijacking. This is accomplished by corrupting the data stream of an established connection, then re-establishing it based on correct sequence and acknowledgement numbers with the attack machine.

ii.) **Blind Spoofing :** This is a more sophisticated attack, because the sequence and acknowledgement numbers are unreachable.. It was relatively easy to discover the exact formula by studying packets and TCP sessions. Now a day's most OSs are implementing random sequence number generation, making it difficult to predict them accurately. A properly crafted attack could add the requisite data to a system (i.e. a new user account), blindly, enabling full access for the attacker who was impersonating a trusted host.

iii.) **Man In the Middle Attack :** Both types of spoofing are forms of a common security violation known as a man in the middle (MITM) attack. In these attacks, a malicious party intercepts a legitimate communication between two friendly parties. The malicious host then controls the flow of communication and can eliminate or alter the information sent by one of the original participants without the knowledge of either the original sender or the recipient. In this way, an attacker can fool a victim into disclosing confidential information by "spoofing" the identity of the original sender, who is presumably trusted by the recipient.

iv.) **Denial of Service Attack :** IP spoofing is almost always used in what is currently one of the most difficult attacks to defend against – denial of service attacks, or DoS. Since crackers are concerned only with consuming bandwidth and resources, they need not worry about properly completing handshakes and transactions. Rather, they wish to flood the victim with as many packets as possible in a short amount of time. In order to prolong the effectiveness of the attack, they spoof source IP addresses to make tracing and stopping the DoS as difficult as possible. When multiple compromised hosts are participating in the attack, all sending spoofed traffic, it is very challenging to quickly block traffic.

v.) **Misconceptions of IP Spoofing :** While some of the attacks described above are a bit outdated, such as session hijacking for host-based authentication services, IP spoofing is still prevalent in network scanning and probes, as well as denial of service floods. However, the technique does not allow for anonymous Internet access, which is a common misconception for those unfamiliar with the practice. Any sort of spoofing beyond simple floods is relatively advanced and used in very specific instances such as evasion and connection hijacking.

3.2 Security Against Spoofing

There are a few precautions that can be taken to limit IP spoofing risks on network, such as:

i.)**Filtering at the Router :** Implementing ingress and egress filtering at the border routers is a great place to start your spoofing defense. An implementation of an ACL (access control list) that blocks private IP addresses on your downstream interface. Additionally, this interface should not

accept addresses with your internal range as the source, as this is a common spoofing technique used to circumvent firewalls. On the upstream interface, you should restrict source addresses outside of your valid range, which will prevent someone on your network from sending spoofed traffic to the Internet.

ii.) **Encryption and Authentication :** Implementing encryption and authentication will also reduce spoofing threats. Both of these features are included in Ipv6, which will eliminate current spoofing threats. Additionally, you should eliminate all host-based authentication measures, which are sometimes common for machines on the same subnet. Ensure that the proper authentication measures are in place and carried out over a secure (encrypted) channel [8], [14].

3.3 Observation of IP Spoofing

It is a elementary technique for passive observation of spoofing activities on the internet. Network telescope [23] captures non-solicited messages, which are mainly generated by victim attacked by traffic with source prefix set in the scope owned by the telescope. Then, it can be determined a part of nodes which are attacked by spoofing traffic. Currently, the largest scale telescope is the CAIDA UCSD telescope, which owns 1/256 of all the IP addresses and is mainly used to observe DDOS activities and worms. Moore el at. [10] Presented a technique named "backscatter analysis" which infers characteristics of dos attacks based on traces collected by the network telescope. Though ICMP error messages are mentioned in the paper, it does not further investigate these messages to trace spoofers. CAIDA provides publicly accessible data. The main analysis and experimental work of this article are performed on the data supplied by CAIDA. The MIT spoofer project tries to disclose which networks are able to launch spoofing based attacks. Volunteer participants install a client that tests the spoofing ability of their hosts and networks. The statistic result shows 6700 ass out of 30205 do not filter spoofing. The figure2 shows the network telescope captures path backscatter in random spoofing attacks.

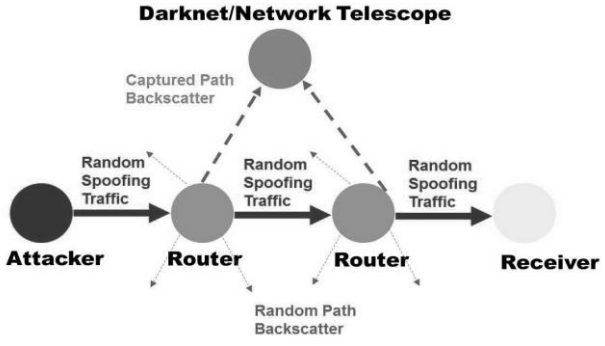

Figure 2: Network telescope captures path backscatter in random spoofing attacks

4. Path Backscatter

4.1 Path Backscatter Messages

In network transmission, many packets are not delivered in their intended destination. A router may fail to forward a packet due to various factors. It may produce path backscatter message (ICMP error message) under some circumstances. The source IP address indicated in the original packet will receive the path backscatter messages. If the source address is spoofed, then the messages will be sent to the node who actually owns the address. This means that the victims of reflection based attacks, and hosts whose addresses are used by spoofers, may collect such information [10]. The Figure 3. shows the process of Path Backscatter Generation and Collection.

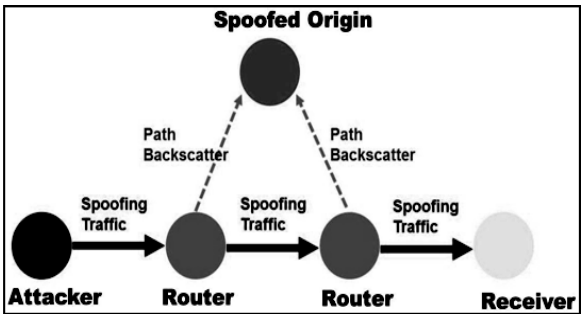

Figure 3: The Path Backscatter Generation and Collection

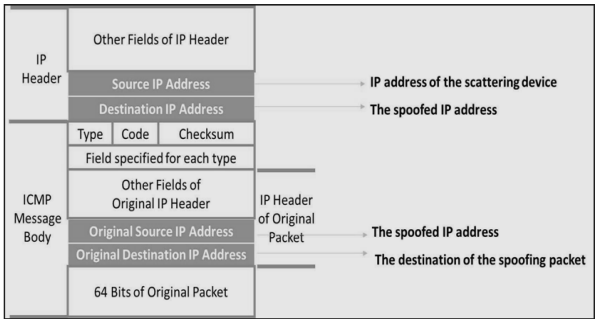

Figure 4: The Format of the Path Backscatter Messages

The structure of the path backscatter message is shown in figure 4. Each message contains mainly two parts: IP header and ICMP message body. The IP header part contains

i.) The IP address of the scattering device i.e. router, which is on the path from the attacker to the destination of the spoofing packet;
ii.) The spoofed IP address i.e. the victim.

The ICMP message body part contains
i.) The spoofed IP address;
ii.) The original destination of the spoofing packet.

The original IP header also contains the remaining TTL of the spoofing packet.

The table 2. contains the information about the path Backscatter Classes. The figure 5 shows **t**he victim captures path backscatter in reflection attacks.

Table 2 : The Path Backscatter Classes

Type	Class
Time Exceeded	TIMXCEED_INTRANS
Destination Unreachable	UNREACH_FILTER_PROHIB UNREACH_NET_PROHIB UNREACH_HOST_PROHIB UNREACH_HOST UNREACH_NET UNREACH_NEEDFRAG
Source Quench	SOURCEQUENCH
Redirect	REDIRECT_HOST, REDIRECT_NET
Parameter Problem	PARAMPROB

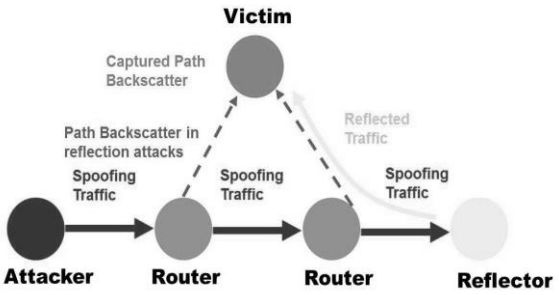

Figure 5: The victim captures path backscatter in reflection attacks

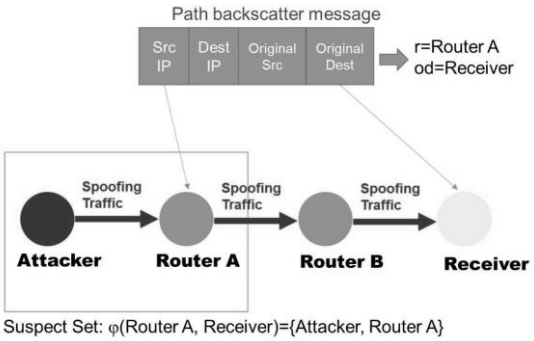

Figure 6: The suspect set determined by a path backscatter message

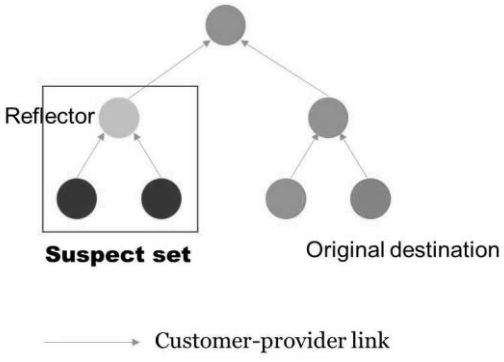

Figure 7: The suspect set determined by a path backscatter message with valley-free Assumption

4.2 TIME-TO-LIVE (TTL)

Time-to-live (TTL) is a value in an Internet Protocol (IP) packet that informs a router whether or not the packet has been in the network for too long and should be discarded. A packet may not reach its destination, in a reasonable time frame due to several reasons. Such packets may loop endlessly on the network. To avoid this situation, the packet may be discarded after certain time and send a message to the originator, who can decide whether to resend the packet. The initial TTL value is set, usually by a system default, in an 8 bit field of the packet header. The original concept of TTL was that it would specify a certain time frame in seconds that, when exhausted, would cause the packet to be discarded.

4.3 Passive IP Traceback

The Distributed Denial of Service (DDoS) attacks are launched synchronously from multiple locations and they are extremely harder to detect and stop. Identifying the true origin of the attacker along with the necessary preventive measures helps in blocking further occurrences these types of attacks. The issue of tracing the source of the attack deals with the problem of IP traceback.

5. Proposed ICMP based IP Traceback Scheme

In this proposed ICMP based IP Traceback Scheme Passive IP Traceback (PIT) security system is developed to bypass the challenges in deployment. Routers may fail to forward an IP spoofing packet due to various reasons, e.g., TTL exceeding. In such cases, the routers may generate an ICMP error message and send the message to the spoofed source address. Because the routers can be close to the spoofers, the path backscatter messages may potentially disclose the locations of the spoofers. PIT exploits these path backscatter messages to find the location of the spoofers. With the locations of the spoofers known, the victim can seek help from the corresponding ISP to filter out the attacking packets, or take other counterattacks. PIT is especially useful for the victims in reflection based spoofing attacks, e.g., DNS amplification attacks. The victims can find the locations of the spoofers directly from the attacking traffic. Profoundly explores way backscatter messages. These messages are profitable to help comprehend with spoofinging exercises. All the way through applying PIT on the path backscatter dataset, a number of locations of spoofers are captured and presented. PIT exploits these way backscatter messages to discover the spoofers' area. With the spoofers' areas known, the casualty can look for assistance from the relating ISP to filters through the attackers packets, or take different counterattack. PIT is particularly valuable for the victims in reflection based spoofing attack, e.g., DNS amplification attack. The casualties can discover the spoofers' areas specifically from the attacking movement. The figure 8. shows the architecture of passive IP traceback system.

5.1 Procedure for IP Traceback Mechanism

Step 1. Find the shortest path from source (s) node to destination (d) node.

Step 2. The message can be send from r to d through many intermediate nodes i.e. routers (r).

Step 3. There may any spoofer origin available in between the path

Assume, that 'SP' is the spoofer node in the network. There are two assumptions for locating such spoofing origin while routing the packets in the network.

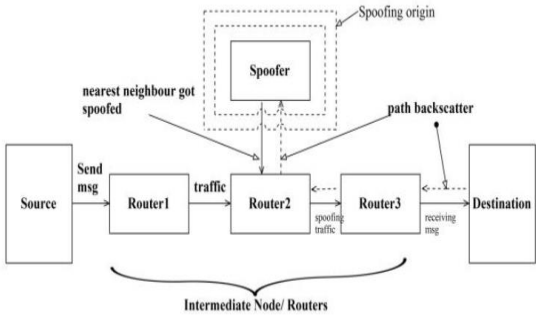

Figure 8: Architecture of Passive IP Traceback System

A. Loop-Free Assumption: This assumption states there is no-loop in the paths. This assumption always holds unless misconfiguration or the routing has not converged.

B. Valley-Free Assumption: This assumption states there should be no valley in the some node level network paths. Though the increased complexity of node relationship has reduced the universality of this assumption, it is still the most common model of intermediate network level routing.

The table 3. contains the datasets for the proposed method. The table 4. having the algorithm to determine the suspect set based on Valley free assumption. The table 5. contains the algorithm to determine suspect set based on Loop-free assumption.

Table 3: Datasets

Dataset	Source
Path Backscatter dataset	CAIDA 2008 Backscatter dataset
AS Level Internet topology	Route View BGP data
AS relationship	Inferred AS relationship from CAIDA
IP-to-AS Mapping	RouteView BGP Data
AS topologies	Topology zoo
IP geolocation	IP Info

Table 4. : Function Getsupsectset_Valleyfree

```
function
GETSUSPECTSET_VALLEYFREE(G,r,od)
  if od Є C one(r) then
      return G,nodes()
   else
      return C one(r)
   end if
   end function
```

Table 5. : Function Getsuspectset_Loopfree

```
functionGETSUPSECTSET_LOOP FREE(G,r,od)
 suspect set ← 0
    c← null
 p← shortest path from r to od
for Vertex v in p do
if v==r then
   Continue
   end if
   G'← G. remove (r)
   if r and od are disconnected in G' then
   c←v
   break
   end if
end for
 SG← G, remove (c)
for Vertex v in SG do
   if v and r are connected in SG then
   Suspect Set ←suspectSet +v
   end if
   end for
   return SuspectSet
   end function
```

Step 1. I
f suppose any intermediate node has being spoofed by spoofer node then the destination node will send the path backscatter message to all intermediate node indicating that spoofing has occurred at somewhere in the network.

Step 2. Then each node in network will send the acknowledgment for that path backscatter message. The node which fails to give back acknowledgment that will be assumed as spoofer node.

6. Results and Discussion

The ICMP based passive IP traceback (PIT) system has been developed . The proposed system is used to capture the spoofed locations. The results are observed through combining the pathbackscatter mechanism. Initially for each path backscatter check the message whether it belongs to the special classes listed in table 2 of section 5. If yes, the reflector should be near the attacker. Thensimply use the source as of the message as the location of the spoofer. If the message does not belong to the types, it is mapped into an as tuple. Determine whether the as tuple can accurately locate the source as of the attacker based on the mechanisms proposed in section 5. Because the system perform tracking at the as level, we only use the valley free assumption which results in better tracking capability than the loop-free assumption. Then if the as tuple can accurately locate the source as of the message, the source as of the spoofer is just this as. Then we also use the source as the location of the spoofer. We do not further investigate the location of the spoofers inside the ash because we do not know the inner structure and address allocation in the ases.

On the other hand, at least the messages of the special classes listed in table 2 of section 5 can help locate the network of the spoofer. The security system has observed 2788 ases in which there are spoofers 914 of them are located by the tracking mechanisms, and 2148 are located based on the special classes of path backscatter messages. There are 274

ases located by both mechanisms. The full list of the ases can be fetched from http://tinyurl.com/lp959y4. The captured ases are only a small portion of all the ases. We believe this result underestimated the total number of ases with spoofers reside in. Considering the limitation of the backscatter collection capability of the CAIDA network telescope, the uncertainness of path backscatter generation and the available datasets produce the results at the maximum. This paper produces the partial result to illustrate the effectiveness of the proposed tracking mechanism. It can be the basis for further potential works. Besides, it should be noted that the ases with spoofers in are not the ases which indulge spoofing. Actually, there are a number of path backscatter messages are generated because of the filtering performed by the assessment.

7. Conclusion

The proposed ICMP based passive IP traceback (PIT) system is offered the results to scatter the mist on the locations of spoofers based on investigating the path backscatter messages. Passive IP Traceback (PIT) tracks spoofers based on path backscatter messages and public available information. Specified how to apply PIT when the topology and routing are both known, or the routing is unknown, or neither of them are known. An effective algorithm is used to apply PIT in large scale networks and proofed their correctness. The proposed system showed the captured locations of spoofers through applying PIT on the path backscatter dataset.

References

[1] S. M. Bellovin, "Security problems in the TCP/IP protocol suite,"ACM SIGCOMM Comput. Commun. Rev., vol. 19, no. 2, pp. 32–48,Apr. 1989.

[2] R. Stone, "Center Track: An IP overlay network for tracking DoS floods," in Proc. 9th USENIX Secur. Symp., vol. 9. 2000, pp. 199–212.

[3] A. C. Snoeren et al., "Hash-based IP traceback," SIGCOMM Comput. Commun. Rev., vol. 31, no. 4, pp. 3–14, Aug. 2001.

[4] A. Snoeren, C. Partridge, L. Sanchez, C. Jones, F. Tchakountio, S. Kent, and W. Strayer, "Hash-based IP traceback," in Proc. of ACM SIGCOMM,(San Diego, CA, USA), August 2001.

[5] S. Savage, D. Wetherall, A. R. Karlin, T. E. Anderson: Network Support for IP Traceback, IEEE/ACM Transactions on Networking, Vol. 9, No. 3, 2001, pp. 226-237.

[6] Belenky.A., N. Ansari: On IP Traceback, IEEE Commun. Mag. Vol. 41, No. 7, 2003, pp. 142-153.

[7] Belenky.A. and N. Ansari, "IP traceback with deterministic packet marking," IEEE Commun. Lett., vol. 7, no. 4, pp. 162–164, Apr. 2003.

[8] IP Spoofing: An Introduction by Matthew Tanase, 2003.

[9] J. Mirkovic, J. Martin, P. Reiher: A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms, Computer Communication Review, Vol. 34, No. 2, 2004, pp. 39-53.

[10] Belenky, Andrey; Nirwan Ansari (2007). "On deterministic packet marking". Computer Networks: the International Journal of Computer and Telecommunications Networking 51 (10): 2677–2700. doi:10.1016/j.comnet.2006.11.020.

[11] D. Moore, C. Shannon, D. Brown, G. Voelker, S. Savage: Inferring Internet Denial-of-Service Activity, ACM Transactions on Computer Systems, Vol. 42, No. 2, 2006, pp.115-139.

[12] ICANN Security and Stability Advisory Committee, "Distributed denial of service (DDOS) attacks," SSAC, Tech. Rep. SSAC Advisory SAC008, Mar. 2006.

[13] J.Liu, Z.-J. Lee, and Y.-C. Chung, "Dynamic probabilistic packet marking for efficient IP traceback," Comput. Netw., vol. 51, no. 3, pp. 866–882, 2007.

[14] Forouzan, Behrouz A., Data Communications and Networking, 4th Edition, Boston: McGraw-Hill,2007.

[15] 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.

[16] Savage, Stefan; D. Wetherall, A. Karlin, and T. Anderson (2000). "Practical Network Support for IP Traceback" (PDF). ACM SIGCOMM. Stockholm, Sweden. Retrieved 2008-11-18.

[17] C. Labovitz, "Bots, DDoS and ground truth," presented at the 50th NANOG, Oct. 2010.

[18] A. Castelucio, A. T. A. Gomes, A. Ziviani, and R. M. Salles, "Intradomain IP traceback using OSPF," Comput. Commun., vol. 35, no. 5, pp. 554–564, 2012.

[19] M.-H. Yang and M.-C. Yang, "Riht: A novel hybrid IP traceback scheme," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 789–797, Apr. 2012.

[20] Guang Yao, Jun Bi, Senior Member, IEEE, and Athanasios V. Vasilakos, Senior Member, IEEE, "Passive IP Traceback: Disclosing the Locations of IP Spoofers From Path Backscatter", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 3, March 2015.

[21] Virandra Patil, Pritish Deshpande, Mahesh Talekar, Swapnil Tapkir, Dhanajay Khade, Prof.Nitin Hambir, "Spoofer Location Detection Using Passive IP Traceback", Multidisciplinary Journal Of Research in Engineering and Technology, Volume 3, Issue 1, 2016,Pg.903-910.

[22] M. Mohammed Imran, B. Sivaranjini, L.Govindhasamy, P. Gunasekaran, "IP Spoofing Identification", South Asian Journal of Engineering and Technology Vol.2, No.17, 2016, pp18–23.

[23] The UCSD Network Telescope. [Online]. Available:http://www.caida.org/projects/network_ telescope/

Author's Biography

V.Marriyammal is a M.Phil research scholar in the Department of Computer Science, Marudupandiyar College, Thanjavur, Tamilnadu, India. She has received her B.Sc(CS) degree and MCA degree from Bharathidasan University, Trichy, TamilNadu, India. She also finished her B.Ed in Haji S.M.S B.Ed College. She is having more than 2 years of teaching experience and also having 3 years experience in software development such as Creating Websites and project works. Her areas of research interest are Computer Networks and Network Security.