Volume 4, Issue 3, March-2017, pp. 98-105 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Internet level Traceback System for Identifying the Locations of IP Spoofers from Path Backscatter

Sharada K. Shiaragudikar[1], Nagaraj M. Benakanahalli[2], Pavana Baligar [3]
Arunakumar Joshii[4], JagadeeshMeti[5]

Asst.Prof,Department of Computer/Information Science and Engineering,
S. K. S. V. M. Agadi College of Engineering and Technology,
Laxmeshwar582116,India [1,3,4,5]
Asst.Prof,Department of Automation and Robotics,
B. V. Bhoomaraddi College of Engineering and Technology, Hubl-580031i, India,[2]

Abstract: It is normal that the attackers over the network may use the fake source IP address to conceal their actual locations. This paper proposes a framework that bypasses the deployment challenges of IP Traceback techniques [1]. This system researches Internet Control Message Protocol error messages (named path backscatter) activated by spoofing traffic, and tracks the Spoofers based on the information available by the public(e.g., topology). Along these, the proposed framework can discover the Spoofers with no deployment prerequisite. Despite the fact that the proposed framework can't work in all the spoofing attacks, it might be the most helpful mechanism to trace Spoofers before an Internet-level traceback framework has been deployed in real. The results are got by implementing in the form of simulation using Java platform for understanding the system over the networks.

Keywords : Internet, IPaddress ,traceback mechanism,Spoofer,protocol.

I. Introduction

IP Spoofing is a technique used to gain unauthorized access to machines, whereby an attacker illicitly impersonates another machine by manipulating IP packets. IP Spoofing involves modifying the packet header with a forged (spoofed) source IP address, a checksum, and the order value.

The essential protocol for sending data over the Internet network and many other computer networks is the Net Protocol (IP). The standard protocol specifies that each IP packet should have a header which contains, among other things, the IP address of the sender of the packet. The source IP address can be your address that the packet was sent from, nevertheless the sender's address in the header can be altered, so that to the beneficiary it appears that the packet came from another source. The protocol requires the acquiring computer to send back an answer to the source address, so that spoofing is mainly used when the Fernsehsender can anticipate the network response or does not care about the response.

IP spoofing relating to the use of a trusted Internet protocol address can be employed by network intruders to overcome network security measures, such as authentication based on IP addresses. This type of attack is most effective where trust relationships are present between machines. For example, rather on some business networks to have inside systems trust each other, so that users can log in without a username or password, provided they can be connecting from another machine on the inside network (and so must already be logged in). By spoofing an affiliation from a trusted machine, an attacker on the same network just might gain access to the target machine without authentication.

IP spoofing is quite frequently used in denial-of-service attacks, where the objective is to avalanche the target with a tougher volume of traffic, and the attacker will not care about acquiring responses to the assault packets. Packets with spoofed IP addresses are more challenging to filter since each spoofed packet appears to come from a different sort of address, and they hide the actual source of the assault. Denial of service disorders[2]**.**That use spoofing typically randomly chooses addresses from the complete IP address space, though more complex spoofing mechanisms might avoid unroutable addresses or unused helpings of the IP address space. The proliferation of large botnets makes spoofing less important in refusal of service attacks, but attackers typically have spoofing available as a tool, if they need to use it, so defenses against denial-of-service attacks that rely on the validity of the source IP address in attack packets might have trouble with spoofed bouts. Backscatter, a strategy used to observe denial-of-service attack activity in the Internet, is dependent on the attackers' use of IP spoofing for their effectiveness.

II. Related Work

Though PIT can be used to perform IP traceback, it is quite different from existing IP traceback mechanisms. PIT is inspired by a quantity of IP spoofing remark activities. Thus, the related work is composed of two parts. The first briefly introduces existing IP tracebackmechanisms, and the second introduces the IP spoofing observation activities.

IP traces back mechanisms:

i. Probabilistic Packet Marking

Savagetal [1]. Suggested probabilistically marking bouts as they traverse routers through the Internet. That they propose that the router mark the packet with either the router's IP address or the ends of the path that the packet traversed to reach the router.

ii. Deterministic Packet Marking Scheme

Belenky and Ansari, outline a deterministic packet marking plan. They describe an even more practical topology for the Net - that is made up of LANs and Rear end with a connective border - and make an effort to put a single mark on inbound packets at the actual of network ingress. All their idea is to put, with random probability of. 5, the upper or lower half the IP address of the ingress interface into the écaille id field of the packet, and then collection a reserve bit articulating which portion of the address is contained in the fragment field. Applying this approach they claim to manage to obtain 0 bogus positives with. 99 possibility after only 7 bouts. [3].

Rayanchu and Barua provide another spin on this approach (called DERM). Their approach is similar in that they wish to use and protected IP address of the input interface in the fragment id field of the packet. Where they differ from Belenky and Ansari is that they wish to encode the IP address as a 16-bit hash of that Internet protocol address. Primarily they choose a known hashing function. They express that there would be some collisions if there were greater than 2^16 edge routers doing the marking.

iii. Route Based Approach

With router-based approaches, the router is charged with maintaining information regarding bouts that pass through it. For instance, Sager suggests to log packets and then data mine them later. It has the good thing about being out of the band and so not blocking the fast path.

iv. Out of Band Approach

The ICMP traceback scheme Steven M. Bellovin proposes probabilistically sending an ICMP traceback packet forward to the destination host of an IP packet with some low probability. Thus, the need to maintain point out in either the bundle or the router is obviated. Furthermore, the low probability keeps the finalizing overhead as well as the bandwidth requirement low. Bellovin shows that the selection also be centered on pseudo-random numbers to help block attempts to time attack bursts. The problem with this method is that routers commonly block ICMP messages because of security issues associated with them.

v. Traceback of active attack flows

Through this type of solution, an observer tracks an existing attack flow by evaluating incoming and outgoing slots on routers starting from the host under assault. Thus, such a remedy requires having privileged entry to routers along the attack course.

To bypass this constraint and automate this process, Stone proposes routing suspect packets on an contribution network using ISP border routers. By simplifying the topology, suspicious packets can certainly be re-routed to a specialized network for further analysis.This is an unique approach. By nature of DoS, any such strike will be sufficiently long lived for tracking in such a fashion to be possible. Layer-three topology changes, while hard to mask to an identified attacker, have the likelihood of alleviating the 2 before the routing change is uncovered and therefore adapted to. Once the attacker has adapted, the re-routing scheme can once again adapt and re-route; creating an oscillation in the DoS attack; giving some ability to absorb the effect of such an attack.

IP spoofing observation activities:

Only some the packets reach their spots. A network device may fail to forward a packet due to various reasons. Under certain conditions, it may well generate an ICMP error message, i. elizabeth., path backscatter messages. The path backscatter messages will be delivered to the source IP address indicated in the original packet. In the event that the source address is forged, the messages will be provided for the client who actually owns the address. This implies the affected individuals of reflection based problems, and the hosts in whose addresses are being used by spoofers, are possibly to accumulate such messages.

The format of the way backscatter emails, is illustrated in Figure 2. Each message includes the source address of the reflecting device, and the IP header of the original packet. Hence, from each path backscatter, we can get 1) the Internet protocol address of the reflecting device which is on the road from the attacker to the destination of the spoofing packet; 2) the IP address of the original destination of the spoofing packet. The original IP header also is made up of other valuable information, elizabeth. g., the remaining TTL of the spoofing box. Note that due to some network devices may perform address rewrite (e. g., NAT), the original source address and the destination address may be different.

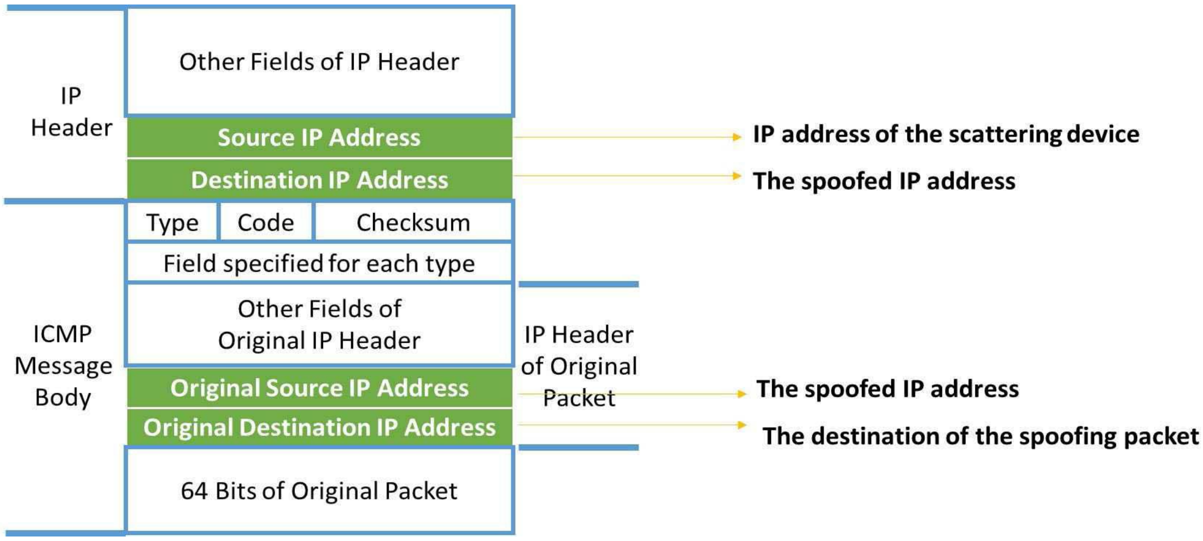

IP Header
Other Fields of IP Header
Source IP Address
Destination IP Address
IP address of the scattering device
The spoofed IP address
ICMP Message Body
Type
Code
Checksum
Field specified for each type
Other Fields of Original IP Header
Original Source IP Address
Original Destination IP Address
IP Header of Original Packet
The spoofed IP address
The destination of the spoofing packet
64 Bits of Original Packet

Figure1:The format of a path backscatter messages

III. Existing System

Existing IP traceback methodologies can be ordered into five fundamental classes: packet marking, ICMP traceback, logging on the router, link testing, overlay, and hybrid tracing. Packet marking strategies require routers modify the header of the packet to contain the data of the router and forwarding decision. Not the same as package checking techniques, ICMP traceback creates expansion ICMP messages to a collector or the destination. Attacking path can be remade from log on the router when router makes a record on the packets forwarded. Link testing is a procedure which decides the upstream of attacking traffic hop by hop while the attack is in progress. Center Track proposes offloading the suspect traffic From edge routers to special tracking routers through an overlay network.

Disadvantages of Existing System:

- Based on the captured backscatter messages from UCSD Network Telescopes, spoofing activities are still frequently observed.
- To build an IP traceback system on the Internet faces at least two critical challenges. The first one is the cost to adopt a traceback mechanism in the routing system. Existing traceback mechanisms are

either not widely supported by current commodity routers, or will introduce considerable overhead to the routers (Internet Control Message Protocol (ICMP) generation, packet logging, especially in high-performance networks. The second one is the difficulty to make Internet service providers (ISPs) collaborate.

- Since the spoofers could spread over every corner of the world, a single ISP to deploy its own traceback system is almost meaningless.
- However, ISPs, which are commercial entities with competitive relationships, are generally lacking of explicit economic incentive to help clients of the others to trace attacker in their managed ASes.
- Since the deployment of traceback mechanisms is not about clear gains but apparently high overhead, to the best knowledge of authors, there has been no deployed Internet-scale IP traceback system till now.
- Despite that there are a lot of IP traceback mechanisms proposed and a large number of spoofing activities observed, the real locations of spoofers still remain a mystery.

IV. Proposed System

We propose an internet level solution, to bypass the issues in deployment. There are many reasons for the routers to fail in forwarding IP spoofing packet e.g., TTL exceeding. In such cases, the ICMP error message (named path backscatter) is generated by the router and sends the message to the spoofed source address. While the routers can be close to the spoofers, the path backscatter messages may potentially disclose the locations of the spoofers. The system exploits these messages to find the location of the spoofers. Passive IP traceback is especially useful for the victims in reflection based spoofing attacks, e.g., DNS amplification attack as 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.

Advantages of Proposed System:

This is the first article known which deeply investigates path backscatter messages. These messages are valuable to help understand spoofing activities. Though Moore has exploited backscatter messages, which are generated by the targets of spoofing messages, to study Denial of Services (DoS), path backscatter messages, which are sent by intermediate devices rather than the targets, have not been used in traceback. A practical and effective IP traceback solution based on path backscatter messages, i.e., PIT, is proposed. PIT bypasses the deployment difficulties of existing IP traceback mechanisms and actually is already in force. Though given the limitation that path backscatter messages are not generated with stable possibility, PIT cannot work in all the attacks, but it does work in a number of spoofing activities. At least it may be the most useful traceback mechanism before an AS-level traceback system has been deployed in real. Through applying PIT on the path backscatter dataset, a number of locations of spoofers are captured and presented. Though this is not a complete list, it is the first known list disclosing the locations of spoofers.

V. System Architecture

A network device may fail to forward a packet due to various reasons. And hence not all the packets reach their destinations. It may generate an ICMP error message, i.e., path backscatter messages under certain conditions. The path backscatter messages will be sent to the source IP address indicated in the original packet. The messages will be sent to the node who actually owns the address if the source address is forged. This means through the victims of reflection based attacks, and the hosts whose addresses are used by, the spoofers are possibly to collecting such messages.

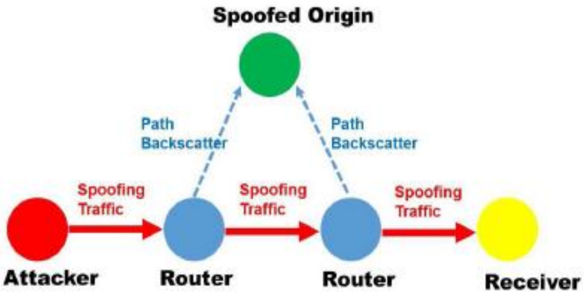


Figure2: The path backscatter generation and collection

VI. Algorithm of Path Backscatter

We consider r (named reflector) as a path backscatter message whose source is router and od as the original destination , the most direct inference is that the packet from attacker to od should bypass r. We have used a simple technique in detecting origin tracking. We consider the network as a graph G(V, E) abstracted , here V is the set of all the network nodes. A network node can be a router, depending on the tracking scenario. From each path backscatter message,the node r, r ∈ V which generates the packet and the original destination od, od ∈ V of the spoofing packet can be considered.

The algorithm is given below.

```
Function Get suspect_loopfree(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(v)
        If r &od are disconnected in g' then
            C<-v
        End if
    End for
    Sg<-g.remove(c)
    For vertex v in sg do
        If v and r areconncetd in sg then
            Suspect set <-suspect set+v
        End if
    End for
    Return suspect set
End function
```

VII. Methodology

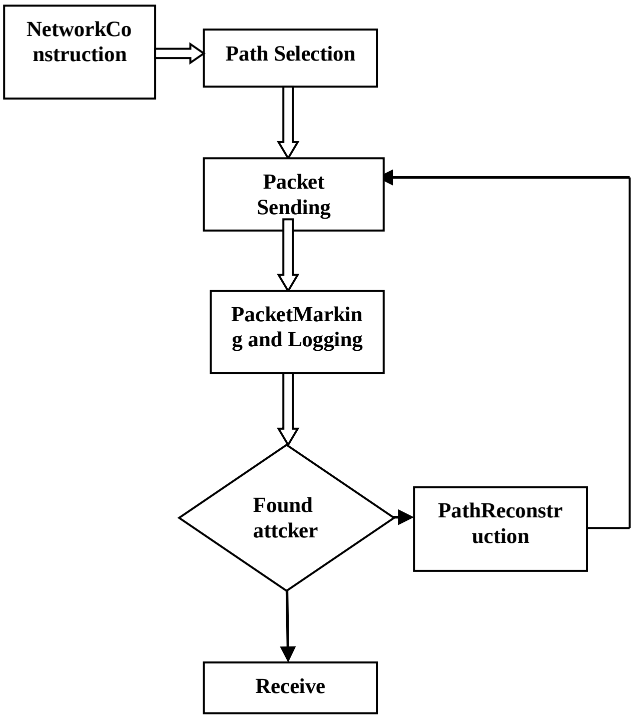


Figure 3:Flow diagram of path back scatter.

Module Description:

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

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

Network topology Construction

A router can either receive data from the nearby router or from the local area network as the network topology may consist of the number of routers that are connected to local area networks. Thus, a border router receives packets from its local network. A core router receives packets from other routers. The degree of a router is defined as the number of routers connected to a single router. The degree of a router is calculated and stored in a table. And also the interface table is stored with Upstream interfaces of each router and it has to be used for the further process.

Path Selection

The way in which the selected packet or file has to be sent from the source to the destination is called as path. From the interface table the upstream interfaces of each router have to be found. The desired path between the selected source and destination can be defined with the help of that interface table.

Packet Sending

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

Packet Marking and Logging

The efficient Packet Marking algorithm is applied at each router along the defined path in this phase of Paket marking. The Pmark value is calculated and stored in the hash table. The packet is sent to the next router if the Pmark value is not more than the capacity of the router. Otherwise, it refers the hash table and the algorithm is repeatedly applied.

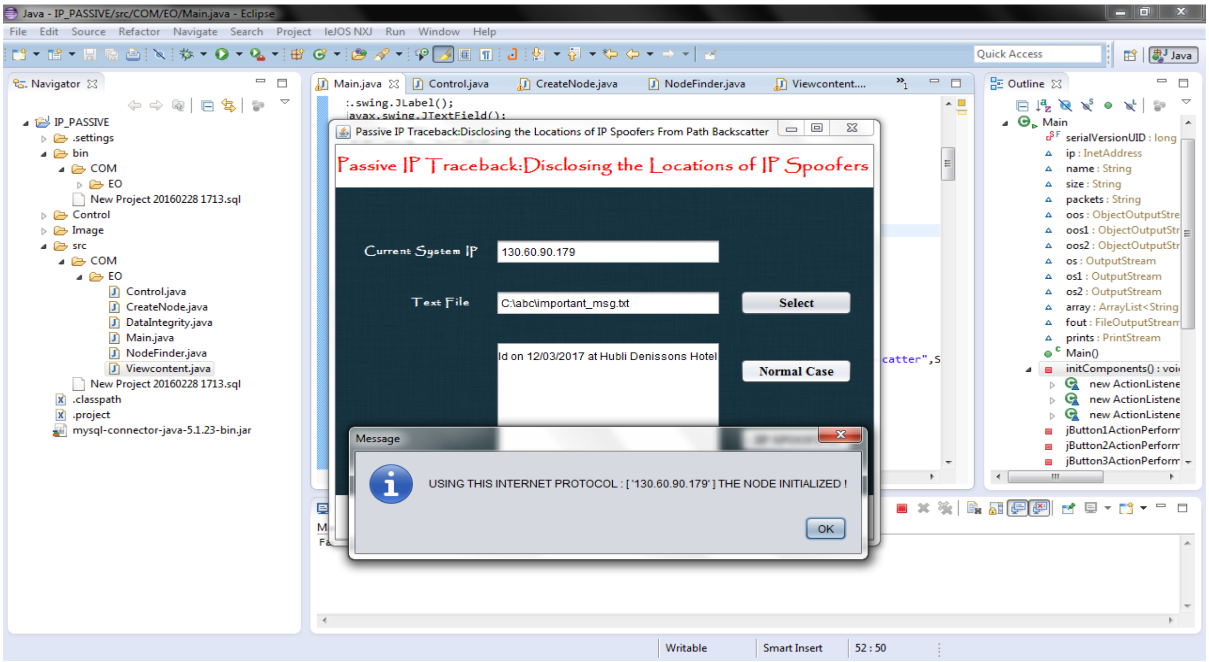
Path Reconstruction

After applying the algorithm, the Packet has to reach the destination,the condition would be checked whether it has sent from the correct upstream interfaces or not. Path Reconstruction is the Process of finding the new path for the same source and the destination in which no attack can be made. The request for the path reconstruction would be sent if any of the attack is found.

VIII. Results

The proposed system is implemented using Eclipse Kepler and MYSQL with Java Language environment and produced the following results.

i) NORMAL CASE



```
:.swing.JLabel();
avax.swing.JTextField();
```

Passive IP Traceback:Disclosing the Locations of IP Spoofers From Path Backscatter

Passive IP Traceback:Disclosing the Locations of IP Spoofers

Current System IP: 130.60.90.179

Text File: C:\abc\important_msg.txt

Select

ld on 12/03/2017 at Hubli Denissons Hotel

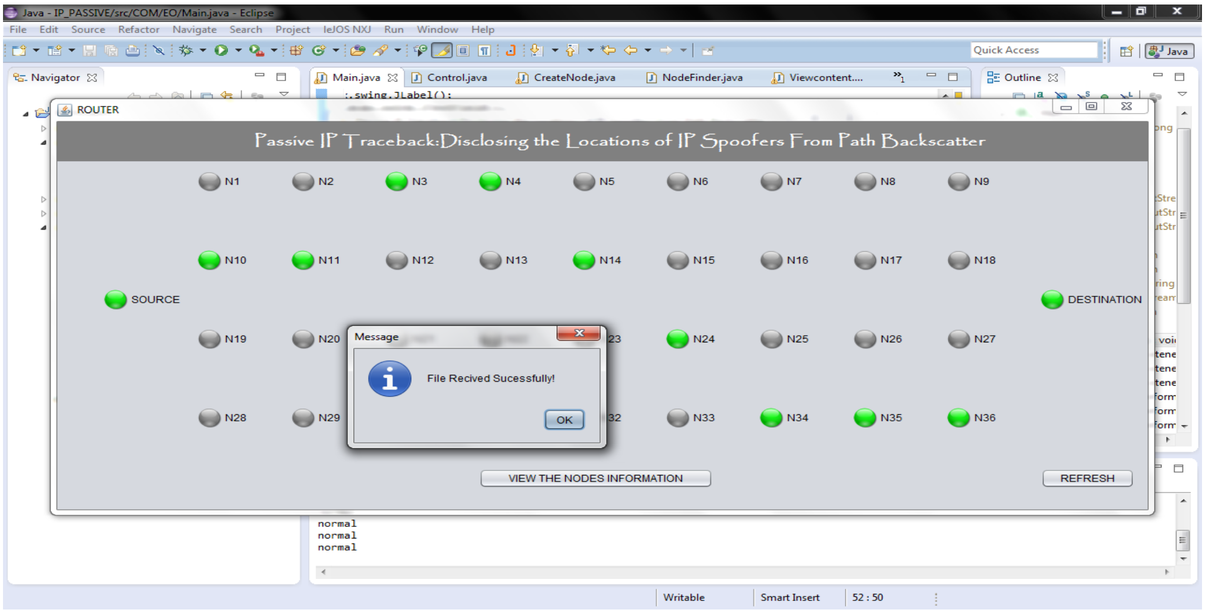
Normal Case

Message

USING THIS INTERNET PROTOCOL : ['130.60.90.179'] THE NODE INITIALIZED !

OK

Figure4: Normal Case- selecting the input file to be sent to the destination over the network



Passive IP Traceback:Disclosing the Locations of IP Spoofers From Path Backscatter

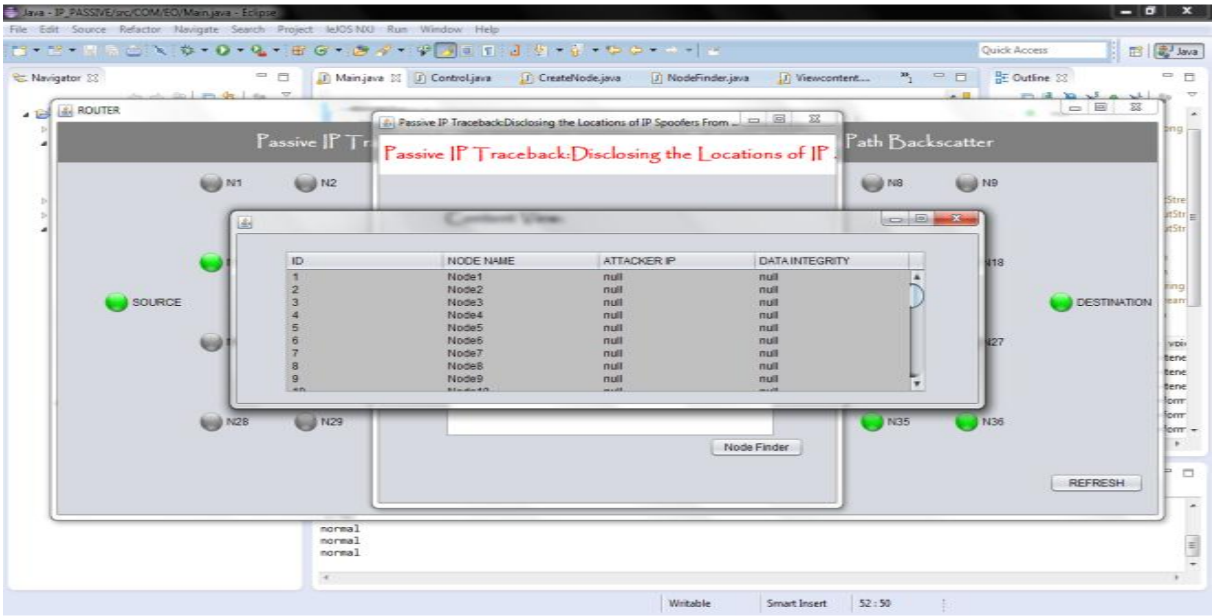
Message

File Recived Sucessfully!

OK

```
normal
normal
normal
```

Figure5: Normal case – Node path-- File received to the destination

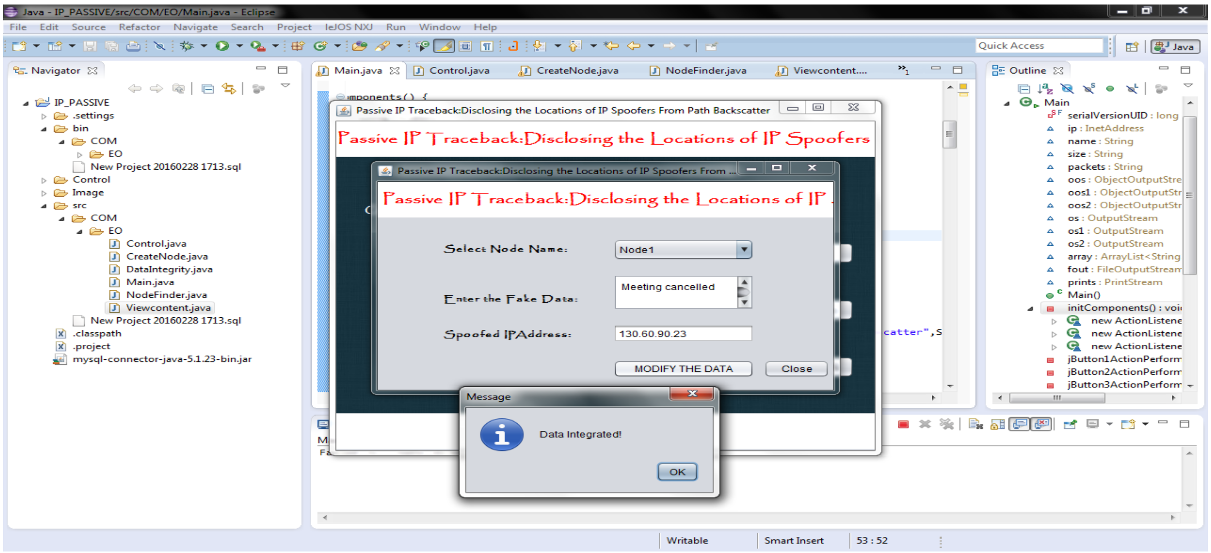

Java - IP_PASSIVE/src/COM/EO/Main.java - Eclipse
File Edit Source Refactor Navigate Search Project leJOS NXJ Run Window Help
Navigator
Main.java
Control.java
CreateNode.java
NodeFinder.java
Viewcontent....
Outline
ROUTER
Passive IP Tr
Path Backscatter
Passive IP Traceback:Disclosing the Locations of IP Spoofers From ...
Passive IP Traceback:Disclosing the Locations of IP
N1
N2
N8
N9
SOURCE
DESTINATION
N18
N27
N28
N29
N35
N36
Node Finder
REFRESH
Writable
Smart Insert
52 : 50

ID	NODE NAME	ATTACKER IP	DATA INTEGRITY
1	Node1	null	null
2	Node2	null	null
3	Node3	null	null
4	Node4	null	null
5	Node5	null	null
6	Node6	null	null
7	Node7	null	null
8	Node8	null	null
9	Node9	null	null

```
normal
normal
normal
```

Figure6:Normal case—Node finder

ii) SPOOFING CASE



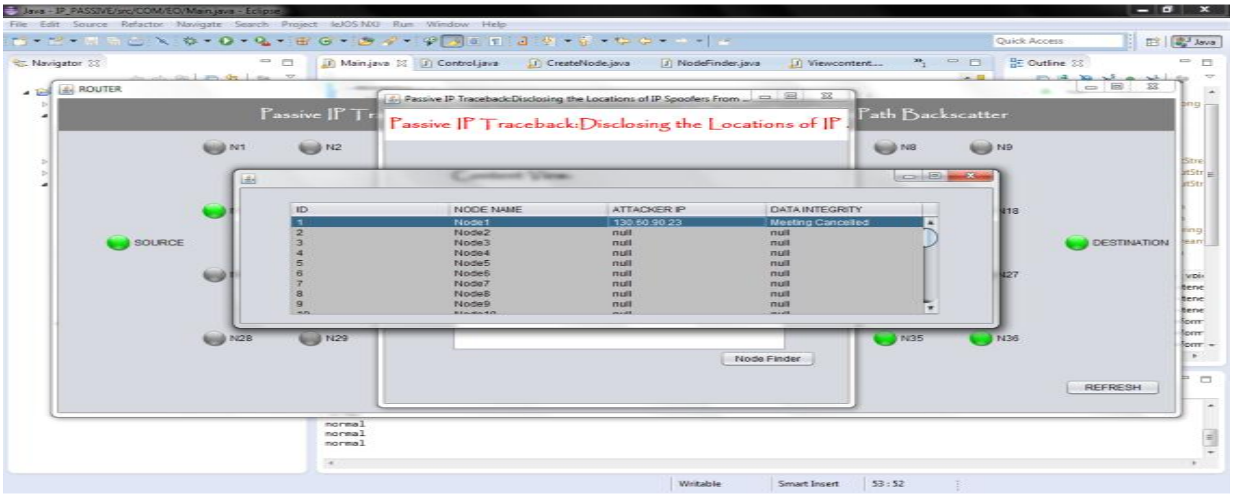
Select Node Name: Node1

Enter the Fake Data: Meeting cancelled

Spoofed IPAddress: 130.60.90.23

Data Integrated!

Figure7: IP Spoofing Case – Selecting the file with modified data


Java - IP_PASSIVE/src/COM/EO/Main.java - Eclipse
File Edit Source Refactor Navigate Search Project leJOS NXJ Run Window Help
Navigator
Main.java
Control.java
CreateNode.java
NodeFinder.java
Viewcontent....
Outline
ROUTER
Passive IP Tr
Path Backscatter
Passive IP Traceback:Disclosing the Locations of IP Spoofers From ...
Passive IP Traceback:Disclosing the Locations of IP
N1
N2
N8
N9
SOURCE
DESTINATION
N18
N27
N28
N29
N35
N36
Node Finder
REFRESH
Writable
Smart Insert
53 : 52

ID	NODE NAME	ATTACKER IP	DATA INTEGRITY
1	Node1	130.60.90.23	Meeting Cancelled
2	Node2	null	null
3	Node3	null	null
4	Node4	null	null
5	Node5	null	null
6	Node6	null	null
7	Node7	null	null
8	Node8	null	null
9	Node9	null	null

```
normal
normal
normal
```

Figure8: IP Spoofing Case—Node finder with Attacked IP

IX. Conclusion

Usually its common that we try to dissipate the mist on the locations of spoofers based on investigating the path backscatter messages. In this paper, we proposed Passive IP traceback which tracks spoofers based on path backscatter messages and public available information. We illustrate causes, collection, and statistical results on path backscatter. When the topology and routing are both known, or the routing is unknown, or neither of them are known, we have specified how to apply Passive IP traceback system to trace out the IP locations of spoofers. We presented two effective algorithms to apply the proposed mechanism in large scale networks and proved their correctness. We have explained the efficiency of the system based on simulation. The results are produced by developing the system in eclipse as a simulation model by using java platform. The system produces the results for both normal case as well as spoofed case by identifying the locations of spoofers on the path backscatter dataset.

References

[1].Passive IP Traceback: Disclosing the Locations of IP Spoofers From Path Backscatter Guang Yao, Jun Bi, Senior Member, IEEE, and Athanasios V. Vasilakos, Senior Member.

[2] 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.

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

[4] C. Labovitz, "Bots, DDoS and ground truth," presented at the 50thNANOG, Oct. 2010.

[5] The UCSD Network Telescope. [Online]. Available: http://www.caida.org/projects/network_telescope/

[6] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for IP traceback," in Proc. Conf. Appl., Technol., Archit., Protocols Comput. Commun. (SIGCOMM), 2000, pp. 295–306.

[7] S. Bellovin. ICMP Traceback Messages.[Online]. Available: http://tools.ietf.org/html/draft-ietf-itrace-04, accessed Feb. 2003.

[8] A. C. Snoeren et al., "Hash-based IP traceback," SIGCOMM Comput. Commun. Rev., vol. 31, no. 4, pp. 3–14, Aug. 2001. [8] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage,"Inferring internet denial-of-service activity," ACM Trans. Comput. Syst., vol. 24, no. 2, pp. 115–139, May 2006. [Online]. Available: http://doi.acm.org/10.1145/1132026.1132027

[9] M. T. Goodrich, "Efficient packet marking for large-scale IP traceback,"in Proc. 9th ACM Conf. Comput. Commun.Secur. (CCS), 2002,pp. 117–126.

[10] D. X. Song and A. Perrig, "Advanced and authenticated marking schemes for IP traceback," in Proc. IEEE 20th Annu. Joint Conf. IEEE Comput.Commun.Soc. (INFOCOM), vol. 2. Apr. 2001, pp. 878–886.

[11] A. 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] 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.

[13] K. Park and H. Lee, "On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack," in Proc. IEEE 20th Annu. Joint Conf. IEEE Comput.Commun.Soc. (INFOCOM), vol. 1. Apr. 2001, pp. 338–347