Detect and Block IP Spoofers using Path Backscatter and Trust Based Mechanism

Akshay Kunnul
M. Tech. Student
Department of Computer Science & Engineering
NCERC, Pambady Thiruvilwamala, Thrissur, Kerala

Mr. Girish R
Assistant Professor
Department of Information Technology
NCERC, Pambady Thiruvilwamala, Thrissur, Kerala

Abstract

IP spoofing is one of the major threats in the network security. Hackers use this to hide their identity or to perform an attack. IP spoofing used for many attacks like denial of service, SYN flooding and man in the middle attacks etc. It is necessary to capture or block the spoofers to defend against these attacks. Different IP traceback mechanisms are used for finding the spoofers identity. There is still not a widely supported mechanism to capture or block the spoofers because of the challenges in the deployment and cost. Here I propose a method for finding out spoofers with the help of path backscatter messages. They are ICMP error messages triggered by spoofing traffic helps to find the location of the spoofer based on the available information. By this method we can find the malicious node in the network .A trust based mechanism is proposed to mark this as a malicious node and isolate it from the network. And this node will not be taken for further communications in the network. This can be done with the help of the internet service providers (ISP) of the network. By using the path backscatter and trust value it may be the most useful mechanism to block spoofers and securing the network.

Keywords: Internet Protocol (IP), Internet Service Provider ISP), IP Traceback, Denial of Service (DOS)

I. INTRODUCTION

IP spoofing is used by hackers to hide their identities or perform an attack in the network. Internet protocol is the basic protocol used for communication over the internet network. Every device connected to the network has an IP address for communication. Which is known as the logical address of the device and it is unique. Attackers use someone else's address to sent data over the network to perform an attack or to gain unauthorized access. Flooding ,man in the middle ,DNS amplification , denial of service are the attacks have been made by using this IP spoofing and attackers also use to cover their tracks when they perform other attacks.

A number of IP traceback mechanisms are introduced so far to find ip spoofers. But they are not that effective or face challenges in the deployment. ICMP traceback, packet marking, packet logging are the IP traceback mechanisms are being used widely over the network. But they are not supported by all the internet service providers (ISP) over the internet network. This paper proposes another way to find and block the spoofers using an ICMP error messages known as path backscatter [1]

Ip traceback mechanisms like ICMP traceback used to trace out full path of an attack. But this icmp message has to be generated by a router in the network to find out the attacker [4]. ICMP message contains part of a traversing packet and sends the messages back to the source .every router has to configure for efficient traceback using ICMP messages which is not applicable.

Probabilistic Packet Marking (PPM) is an example for packet marking ip traceback mechanisms. In which Traceback-enabled router has a Marking Agent (MA) to mark the packets going through it [6] .it helps to find the attack graph in order to traceback to the attackers. But every router and internet service providers has to be configured for packet marking [7]. And this traceback mechanism can only be performed after an attack has completed.

In packet logging ip traceback mechanisms every Routers has to log the passage of all IP packets [4]. Packet logging depends on the availability of free space in the marking field of the forwarded packets. If there is free space available in the marking field, routers write their identification information into the packets [5]. But this method also creates storage overhead to routers and each routers has to be configured for trace back purpose

The available traceback mechanisms are not widely supported because of one reason or another. The proposed mechanism needs no deployment and configuration for finding the location of the spoofers. The proposed mechanism only need supported by the internet service providers to block the spoofers for the secure further communication over the network

The traceback mechanism uses the path backscatter messages are known as passive ip traceback mechanism [1]. The path backscatter messages are ICMP error messages which are created when a router may fail to send ip spoofing packets over the network. The path backscatter message will be forwarded to the source address if the address is spoofed it will send to the original source address. Analyzing the path backscatter messages helps to find the location of the spoofers

A trust based mechanism is mainly used in mobile ad-hoc network to isolate malicious node from the network .Each node is assigned with a trust value in the network [2]. If any node exceeds the threshold value due to different activities that node will be marked as malicious node and will not be used for further communications [3]. It secures the further communications in the

network. So this trust mechanism can be effectively used to block the spoofers from the network. In this paper the spoofers found with the help of path backscatter messages are blocked with the help of the trust based mechanism.

II. IP SPOOFING ATTACKS

There are different types of attacks can successfully performed with ip spoofing attack. The most commonly performed attacks are denial of service, SYN flooding, DNS amplification etc. The types of spoofing attacks are listed here

A. Non-Blind Spoofing

Attackers perform this attack when the attacker is on the same subnet or the same network as the victim. Here the attacker can calculate the sequence and acknowledgement numbers, which eliminates the difficulty of calculating them accurately. This attack is mainly used for gaining unauthorized access. Session Hijacking is an example for this attack. Using ip spoofing the attacker can interfere the connections in the subnet. The attacker can frame someone else for this cause by using their ip address. The attacker can establish a legitimate connation from this network to other networks and perform malicious activities.

B. Blind Spoofing

In this attack the attacker may be not from the same subnet and the sequence and acknowledgement numbers are unavailable for the attackers. Here the Attackers send several packets to the victim's machine in order to sample sequence numbers from the machine. Attackers have no access the reply because he is from different subnet. Which is mainly used for SYN flooding and denial of service attacks.

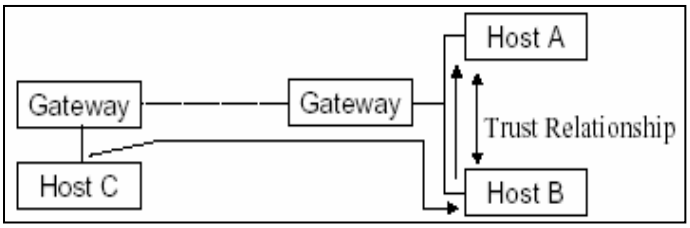

Fig. 1: Blind Spoofing

In figure 1 Host C forwards an IP datagram with the IP address of some other host (Host A) as the source address to Host B. The attacked host (B) replies to the legitimate host (A) as shown in the figure.

C. Man in the Middle Attack

Man in the middle (MITM) attack is a common attack performed using ip spoofing. As the name indicates the attacker lies in between the sender and the receiver. The attacker has the full control of the communication between two legitimate parties and he can manipulate the information as he wishes. The legitimate parties will never know about this attack and the attacker can achieve this by spoofing the sender ip address and send the data to the receiver and vice versa . The attacker can fool the victims and have access to the confidential information they send in between.

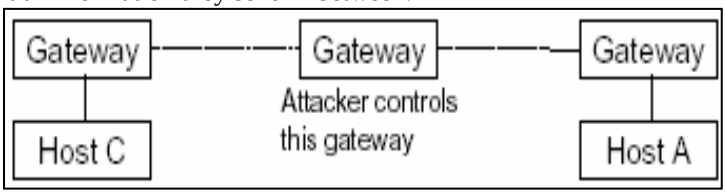

Fig. 2: Man in the Middle Attack

Figure 2 shows the man in the middle attack in between two legitimate users .The attacker can perform this attack easily when the communication is happens in the router which he resides. So that all the data the user send will go through the attacker

III. PATH BACKSCATTER

The IP traceback mechanism that uses path backscatter messages is known as passive ip traceback. Path backscatter messages are ICMP error messages that are created because of many reasons [1]. The traceback mechanism makes use of the ICMP error message to find out the location of the spoofer. These messages are triggered from the attacker's router for the reasons like exceeding time, destination unreachable and source quench etc. The generation of path backscatter messages is shown in the figure 3.

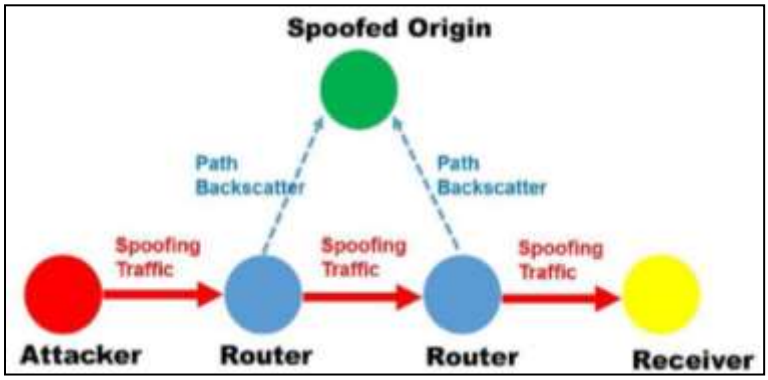

Fig. 3: Generation of path backscatter messages

This path backscatter can be captured by the victim or by using the dark net. By analyzing the path backscatter messages victim can find the ip address of the attacker's router. The path backscatter messages have the spoofed ip address and the destination address of the router etc [1]. The structure of the path backscatter messages is shown in the figure 4.

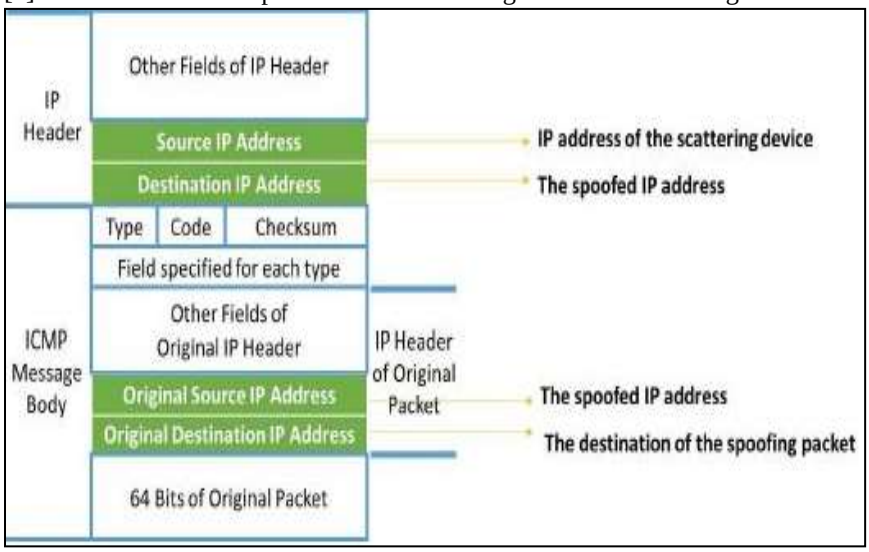

Fig. 4: The format of path backscatter messages.

IV. TRUST BASED MECHANISM

Trust based mechanism is introduced as an alternative option to cryptographic security methods in mobile ad-hoc networks. Initially every node in the network is assigned with a trust value [3]. Trust value is calculated on the basis of nodes action when needed. Trust is introduced to prevent from various attacks like wormhole, black-hole, Dos, selfish attack etc.

In this paper we use trust based mechanism to prevent from ip spoofing attacks over the network [2]. A threshold trust value will be set in the network for analyzing the trust values of nodes in the network

Trust value can be calculated based on different factors like number of packets dropped and any malicious activity on the network and battery level in mobile ad-hoc networks etc. Trust value of each node is calculated and stored in trust index. In MANET node trust calculation process is with the help of data structure neighbour table in each node. This mechanism helps to eliminate the malicious node and also provide a best trusted route for communication. The different types of trust value are listed here.

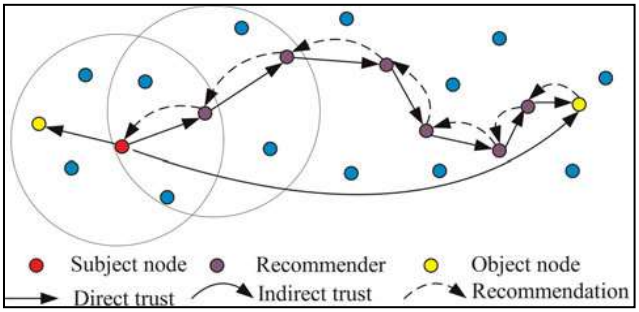

Fig. 5: Trust based Mechanism

A. Direct Trust

In direct trust the trust value is calculated based on the direct communication between the nodes [3]. The calculation of trust of each node based on the packets sent, packets received and packets dropped .if a node A wants to calculate the trust value of node B it calculates based on the factors and find the direct trust value and store it in the neighbour trust table

B. Recommendation Trust

In recommendation trust each node will collect the trust values of the target node from the neighbour nodes [3]. But the neighbour collecting trust value cannot be fully trusted so when collecting trust value of other nodes from the neighbour nodes the trust value of that node should also be considered. This information is generally known as the recommendation trust. The recommendation trust is not so reliable as direct trust. The network nodes passing the trust values is shown in the figure 5

V. PROPOSED SYSTEM

The proposed system makes use of both path backscatter messages and trust based mechanism for detecting and blocking IP spoofers from the network. The path backscatter messages helps to trace out the location of the spoofer node which is actually a router from the network. The ip address of this router is the source address of the path backscatter messages which is forwarded to the original ip address. This can be found out by analyzing the path backscatter message received. The path back scatter messages are basically ICMP messages which are triggered due to various reasons such destination unreachable and source quench etc. As the IP address of the victim is spoofed this icmp error message will be passed on to the original IP address. The victim can capture this messages passed on to his IP address and he will know that his IP address is being spoofed.

Now that victim knows the attacker's router ip address and further actions should be taken care for blocking the spoofer and pass this attackers information on all over the network. A trust based mechanism is proposed for blocking the spoofer's access to the communications. Trust based mechanism is mainly used in mobile ad-hoc networks as an alternative to security algorithms. In this mechanism each routers is assigned with a trust value. A threshold trust valve will be assigned in the network with the help of internet service providers or the private network administrator. Here the victim knows the ip address of the attacker's router and the trust value of this router will be decreased based on the number of packets received and sent by the router. And the victim's router will update the trust value of that router and it will not be used for further communications and an alternative route will be taken for the current communication taking place. The victim's router will pass the updated trust value of the attacker's router to all other routers in the network and the attacker's router will be blacklisted and will not be used for communications.

The attacker can perform the IP spoofing attacks in mainly two ways in the network. They are blind spoofing and man in the middle attack. Blind spoofing attacks are mainly used for attacks like denial of service and DNS amplification etc. Here the attacker knows the ip address of the victim and establish a connection using that IP address. The attacker comes in between the source and destination and manipulates the communicating data. These attacks are simulated in ns2 simulator. Detecting and blocking of the spoofers using path backscatter and trust mechanism is performed.

VI. ANALYSIS FOR PROPOSED SYSTEM

The simulation of the proposed system is carried out using a simulator NS2. A mobile ad-hoc network is created with few nodes as shown in the figure 6. Numbers of routers are taken as nodes to form the network

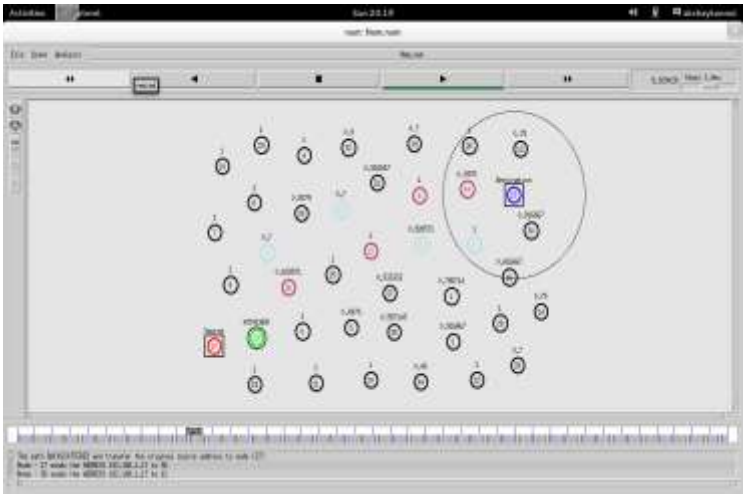

Fig. 5: Man in the middle attack

The analysis of the proposed mechanism is done by simulating both man in the middle attack and blind spoofing. The simulation of man in the middle attack is shown in the figure 6. In which the attacker comes in the middle and have full access to the communicated data. Here the victim gets notified with the path backscatter message because the ip is spoofed. And victim uses trust based mechanism to block the spoofer node from the communication path. And reduces the trust value of the attacker node and passes the information to other nodes.

The simulation of blind spoofing attack is shown in figure 7. Here the attacker node spoofs the ip address of destination to perform attack or steal information as shown in the figure. These attacks are mainly used for denial of service attacks and flooding etc.

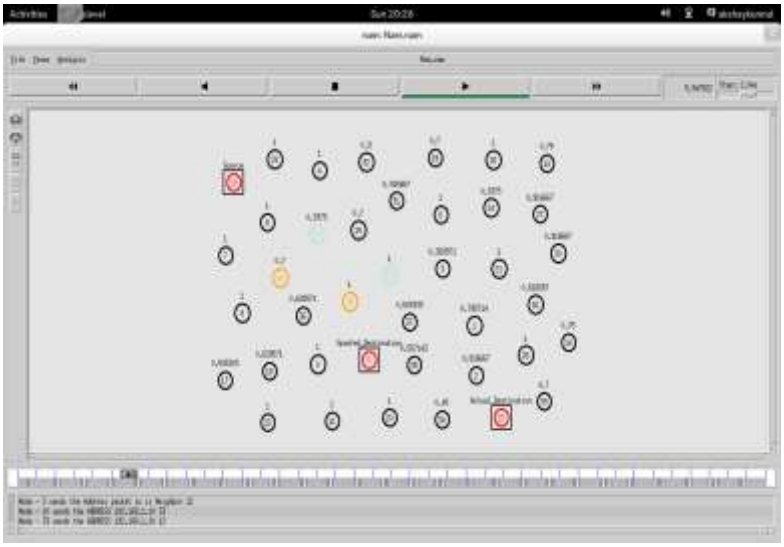

Fig. 7: Blind Spoofing Attack

Here also path backscatter message is created and forwarded to the actual destination as shown in figure 6. In both attacks the spoofer node will not be used for further communications. An alternative route will be chosen for next communication as shown in figure 7. Every node will pass the trust value of attacker node to each other and that secures the communications through the network. This mechanism can be effectively used in mobile ad hoc network for securing the network and it will work as alternative to cryptographic algorithms.

Fig. 7: Alternative path choosing

VII. CONCLUSION

Every attacker spoofs their IP address to cover their tracks when they perform an attack. This makes IP spoofing an important threat to the networking world. The proposed mechanism can effectively detect and block the spoofers from the network. The path backscatter messages are forwarded without any deployment and trust based mechanism is currently widely popular in mobile ad-hoc networks. This makes the introduced mechanism so efficient and it may be the best way to find and blacklist the spoofers from the network. It may put an end to different kind of attacks in the network and secures the network from spoofers

REFERENCES

[1] Passive IP Trace back: Disclosing the Locations of IP Spoofers From Path Backscatter -Guang yao ,jun bi , senior member , IEEE, and Athanasios v, Vasilakos, senior member IEEE 2015
[2] Energy-Efficient and Trust-Aware Routing Techniques for WSN,Ms. Dipali Dikondwar Prof. R. K. Krishna, International Journal of Engineering Research & Technology (IJERT)Vol. 2 Issue 2, February- 2013
[3] X. Li, Z. Jia, P. Zhang, R. Zhang, and H. Wang, "Trust based on-demand multipath routing in mobile ad hoc networks," Information Security, IET, vol. 4, issue 4, pp. 212-232, Dec 2010.
[4] Univ. Putra, Serdang and Othman M , "Accurate ICMP Traceback Model under DoS/DDoS Attack" IEEE 2008.
[5] S.Bellovin. ICMP Traceback Messages. [Online]. Available:http://tools.ietf.org/html/draft-ietf-itrace-04, accessed Feb. 2003.
[6] A. Yaar, A. Perrig, and D. Song, "Fit: fast internet traceback," in INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies Proceedings IEEE, vol. 2, March 2005, pp. 1395–1406 vol. 2.
[7] J. Liu, Z.-J. Lee, and Y.-C. Chung, "Dynamic probabilistic packet marking for efficient ip traceback," Computer Networks, vol. 51, no. 3, pp. 866 – 882, 2007.
[8] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring internet denial-of-service activity," on Computational. Systems. vol. 24, no. 2, pp. 115–139, May 2006.
[9] M.-H. Yang and M.-C. Yang, "Riht: A novel hybrid ip traceback scheme," Information Forensics and Security, IEEE Transactions, vol. 7, no. 2, pp. 789–797, April 2012