Detection of ARP Spoofing

Jyoti sangolagi[1], M.S.Kanamadi[2],

[1]Student, ECE dept, BLDEA College, Karnataka, India
[2]Assistant professor, ECE dept, BLDEA College, Karnataka, India

Abstract - *Because of digitization in every field, the number of internet users in the world has been increased in these days. This has also attracted the increase in the cyber attacks. Most of the internet attacks are done using the IP spoofing either to mask the identity of the person or to steal the information from the internet. Some of very commonly used such attacks are denial of service attack, man in the middle attack. In this project work, it has been planned to find the IP spoofing using Modified Hop Count Filtering (M-HCF) method. M-HCF uses all possible hop counts of a host for a given destination. Upon receiving the packet, the hop count in the packet will be compared with the list of hop counts against its IP address in the hop count table maintained at the end point. The method will have added advantage over usual hop count filtering (HCF). It eliminates the rejection of legitimate packets upon change in the route because of router failure or traffic in that path. It has been planned to simulate the idea using NS2 to check the performance of the proposed method.*

Key Words: **M-HCF,HCF**

1. INTRODUCTION

The digitization of the world has laid the usage of internet even to the extent of every common person's life. It's all because of the easy of work and the security that the modern internet is providing. According to the survey made by International *Census Bureau* [1], there are more than 7.3 billion internet users in the world. The usage of internet has been extended to every field of human life such as education, banking, defense, communication, entertainment, social media, agriculture, industry, etc covering all possible fields of human intervention. In modern world, the internet is becoming one of the basic necessities of human beings to lead the life. Life without internet cannot be imagined for the people living in urban cities of the world. Even it does not mean that the villages are void of using internet; but usage may be little less comparatively than the people in urban areas of the world.

With the increase in the usage of internet and its technology, the threat of security has also increased to the maximum extent. The loopholes in the technology of internet have been used to crack the security measures. There are number of internet threats and attacks that are increased as the usage. Developers are trying hard to give the security and the hackers are finding one or other way to crack the security. It is very important to give the unbreakable security to keep the faith and belief of the common person. Some of the threats that are carried out after exploiting the loopholes of the internet are man in the middle attack, denial of service attack, distributed denial of service attack etc. These attacks will use one or other loophole which is a part of TCP/IP protocol suite. These attacks are carried out making use of indirect techniques such as ARP spoofing and IP spoofing.
The whole internet is standing on TCP/IP protocol stack. Some of the features used in the implementation of these protocols have drawbacks and that are used by the hackers successfully to get the unauthorized access to the information. There are three different types of addresses used in the internet to identify the process, host and network by using port address, IP address, and network ID respectively. IP spoofing is a technique of sending the malicious or fake IP packet to the destination to steal the identity of a host in the internet. Once the identity of another host is obtained using this method, it can further be exploited to get the unauthorized access to the secured information. This attack is very much dangerous and can be done at remote locations without loosing the identity of the attacker host.

The IP spoofing, being one of the important attack of the modern era, should be addressed properly to get rid of resulting attacks such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. The DoS attack is a technique of making a process or system to unable to give the service and is carried out from one location or IP address. Whereas DDoS attack is done from different location/IP addresses. When the solution is found for DoS attack then the attacker found a new way to do the same using DDoS attack. In case of DoS attack, IP spoofing is done using single IP address and from single place whereas DDoS attack is done from different places using different IP addresses. This is the difficult task to address as the packets will arrive from different places but targeted to same IP address.

To address the IP spoofing conducted from different places a method called Hop Count Filtering is adopted (HCF) which makes use of TTL (time to live) field of the TCP packet. But it has a disadvantage as it will drop the packets from legitimate host also. In detail discussion on this is done in chapter 2. In this project, my aim is to find the IP spoofing without dropping the packets from legitimate host.

1.1 Problem Statement

IP spoofing is the key attack for conducting the DDoS attack. In IP spoofing, source IP address of an attacker is changed, so it is difficult to find this attack using the simple peek into the IP packet. When HCF approach is adopted to find the IP spoofing, a number of packets from legitimate host is also dropped which will lead to the decrease in overall performance of the network. Because the packet might have routed through the different paths before it reached the destination. This is normal scenario; whenever some routers or paths are busy, other routs will dynamically adopted to send the packets to destination. There are two issue; first one identifying the legitimate packet when it is routed from different routs and the second issue is to find the fake packets that are being injected from different places of the network.

1.2 Existing System

In current scenario, the IP spoofing attack is detected using the Hop Count Filtering method. As discussed in introduction, in this case a field from TCP called TTL is used to find the IP spoofed packets. The TTL is used as number of hop between source and destination. When a packet is received by any intermediate nodes such as routers, they decrease the hop count by one and forward to next node in the path. This process continues till the packet is reached to its destination. If the hop count of the packet becomes zero before it reaches the destination, then the packet is discarded by that node. This is done to decrease the traffic in the network that is created by the wrong addressed packets; otherwise packets will make round trip in the network and creates huge traffic, decreasing the performance of the network as the time.

In HCF method, after receiving the packet, destination host will check the hop count present in the TTL field and calculates the number of hops between the source and destination based on the TTL value present in the packet. Every host will have the table listing the IP address and the hop count for that IP address. After calculating the hop count value from the packet, it compares the same with the value stored in the hop count table. If both the values matches then the packet is from genuine host or else it is determined as the spoofed one.

This method will work fine when there is DoS attack, which means IP spoofing is done from single host and from single place. But the method fails to give the result when there is a DDoS attack i.e. when IP spoofing is done from different hosts in the network. Because the packet that has arrived from one particular host will have different hop count value than that which has arrived from other host. So the destination host will consider other packets as genuine which have the same hop count values as that stored in the hop count table. This project will address this issue and the new method for this existing one is implemented which will get rid off the problem discussed in section 1.1.

1.3 Objective of the project

The main objective the project work is to address two issue; first one is to identify even such packets which are originated from genuine host but took different paths than the normal scenario. The second objective is to find the spoofed packets which are injected into the network using the concept of DDoS attack.

1.4 Proposed System

There are two issues to be addressed related to IP spoofing as discussed in section 1.1. The solution for the both can be found by making use of a new concept called modified hop count filtering (M-HCF). In this method, destination host will maintain a table containing IP addresses and the all possible hop count for the given IP address. This is the overhead that must be incorporated to get the solution. Against an every source IP address there will be more than one possible hop count value which the packet may take. Because as discussed in section 1.2, packet will be routed through the different path than the normal, whenever there is a link failure or some routers are busy in the path.

Whenever a packet is received at the destination host, it will find the number of hops (hop count) taken by the packet to reach the destination. The obtained hop count value is compared against the all the possible values for the source IP address present in that packet. If the calculated hop count value matches, then it is considered to be the legitimate packet, else the spoofed packet.

1.5 Literature Survey

Stephen M. Specht et.al [2] have made the detail study on DDoS attack and explained the two important attack of DDoS. One is bandwidth depletion attack and the other one is resource depletion attack. Further bandwidth depletion attack is classified into two; one is flood attack and the other one is amplification attack. In case of flood attack, some packets such as ICMP or UDP packets are sent to a vectim host. The victim host will try to process the packets even when they are not intended to it. Even after the packet is sent to same IP but it either may be sent to the open port or closed port. If it is open port, the host try to process the request and if it is sent a closed port, then victim host has to reply with the proper message stating about the closed port in the host. In case of amplification attack, the attacker sends broadcast messages to all the hosts in the network. On receiving the broadcast message sent by attacker on behalf of victim host, now all the hosts in network will send the broadcast reply packet and there decreasing the bandwidth available to the victim host. In case of resource depletion attack, the attacker will make use of loophole in the network protocol and makes the victim host to consume the resources for those fake packets sent. For example, when unnecessarily TCP SYN packets are sent to victim host, it has to reserve some resource and in turn has to send ACK+SYN packet to the other host. This will decrease the bandwidth along with the resource of the victim host. Authors have also explained the potential threats and some measures for finding the DDoS attack but they concluded with the scope to some more robust methods to overcome the DDoS attack.

Wang H. et. al [3] proposed a method to detect the IP spoofing. In this method they discussed the fact that even though the hacker sends the wrong source IP address but he/she cannot change the hop count or the number of hops a packet will take to reach the final destination. According to the authors, in this method they first construct the IP address to hop count table and stores in the destination host. Upon receiving any new packets, the content in the packet are fetched to read the hop count and is compared with the that already stored against the given IP address. In this method, authors have also discussed the methods for rejecting the fake packets. There are three methods and in that first one will reject the packet if the hop count value is not equal to the value stored in the table. Second one will accept the packet even when received hop count is one more than the actual and the last will accept those packet also whose hop count value differs by two. The problem with this method is that, there are more than one routs available between any source and any destination, so there are fair chances of routing the packets through different paths because of link or router failure. This reveals that the hop count value even may differ much compared to the hop count during normal routing.

Wang, Xia et. al [4] have given a variant of the method by [3]. According to the authors, they conduct the hop count comparison at every intermediate node than the destination. This method will surely not only given the protection to the destination system but also to the whole network. This method will improve the performance of the network as the fake packet from the attacker will not be forwarded unnecessarily and will be caught at the intermediate nodes and discarded there.

2.IP SPOOFING

T The backbone of inter networking or the internet is the TCP/IP protocol stack. Whole computer communication now a days is based on the different protocols of this stack. Transport Control Protocol (TCP) and Internet Protocol (IP) are two major protocols of the TCP/IP family. TCP is a transport layer protocol where as IP is a network layer protocol. IP is responsible for end-to-end delivery of the packet. It gives the unreliable and connectionless service, which means that the packets that are sent may or may not be successfully received at the destination and every packet may take different path.

Network layer uses a type of address to logically group the computers in the internet. The protocol used for the purpose is IP. Every computer on the network should have a unique address to be able to communicate with other computers in the network. Two different computers cannot have same IP address on a same network. All the computer in a network communicate with one another using the layered approach shown in figure 2.1. A layer in TCP/IP protocol gives the service to the layer above it and get the service from the layer below it.

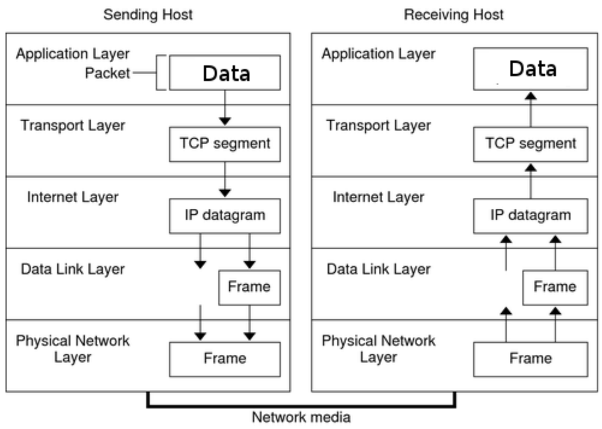

Figure 2.1: Layered architecture of TCP/IP protocol stack

The data that needs to be sent to a destination is encapsulated by different types of protocols at different layers. To send any packet in the network a frame is constructed containing header from protocols of different layers and the data for the intended destination. As shown in figure 2.2, at the sender side every layer takes the data from the layer above it and adds its own header and sends it to the layer below it. This procedure continues till the physical layer. Whereas at the receiver side, every layer gets the data from the layer below it, removes the header which is added by the peer layer at the source and processes the header information before it sends the remaining data to the layer above it. This procedure is continued till the data is received at the application layer. To send any reply to the packet which is received as the request of some service, the receiver will make use of the source IP address present in the packet. It constructs a frame by making the source IP address of the received packet as the destination IP address and send the data to the computer which has requested some service.

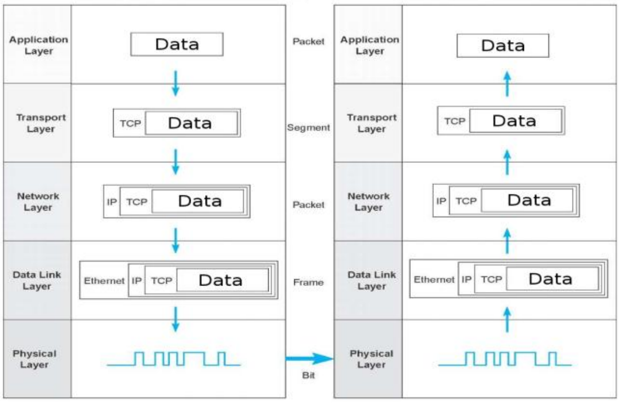

Fig-2.2: Data encapsulation in network communication

After we study all the mechanism incurred in the process of computer communication, one thing is clearly noticed that, there is no authentication about the sender or receiver identity on the network. This lack of authentication is the main drawback of the any network attack. And the giving authentication to every host in the network is much complected technique. The attackers of the network will use the lack of authentication in network and send forged or fake packet by inserting some others IP address as the source address. This will lead to two wrong interpretation, one is the destination host will think that the packet has been sent actually from the source IP address present in the packet and second one is, by this technique, the actual sender will hide its own identity. So, basically IP spoofing is sending a fake or forged IP packet to some other host/hosts in the network.

To understand how attackers have exploited the loophole of the network protocol, namely the IP, it is necessary for us to study the header structure of IP. Figure 2.3 shows the header structure of internet protocol [5]. The header length varies anywhere between 20Bytes (without any options) to 40Bytes (with maximum of 20Bytes of options).

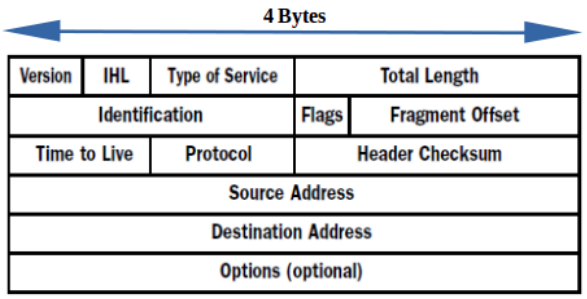

Fig- 2.3: Header format of Internet Protocol

The Internet Protocol has different fields as discussed below:

Version: This is the version number of the internet protocol; there are two versions used, one is IPv4 and the other IPv6.

IHL: This filed gives the length of header.

Type of Service: A field to get distinguished type of service.

Total Length: This field gives the entire length of the IP packet including the header length.

Identification: A packet from layer above the network layer may be required to fragment. This field gives the unique identification number which all the fragments of the packet will have.

Flags: These are 3 flags related to the fragmentation of the IP packet.

Fragment Offset: When the packet is fragmented, this field gives the position of the fragment in the packet.

Time to Live: This is the one of the important field for this project. Actually this field itself is used to count the number of hops between source and destination. The number of count stored in this field restricts the packet to be forwarded to next node, because of this the field is called as time to live.

Protocol: This field gives the protocol for which the packet has been sent.

Header Checksum: Field for error checking and correction.

Source Address: 32 bit IP address of the source.

Destination Address: 32 bit IP address of the destination host.

Options: Optional fields giving different options for routing, time stamp, etc.

Using the information of IP header structure, anybody can construct an IP packet by filling the required data and substitute the anybody's IP address. The packet constructed so can be sent through the network. There is no means to identify whether the packet is from genuine host or not. The packet will be routed as any other and will reach the destination without any interruption.

Normally an attacker who wishes to attack the host or a part of the network will flood the IP spoofed packet to that host so that other hosts in the network don't get the service of the victim host. IP spoofing can be used to get the fake identity of any other host just by sending the IP address of that host as the source address in the packet sent by it. And to hide his/her identity, attacker will use some random IP address as the source address and does the attack on the host. Using the IP spoofing, many other attacks can be conducted such as man-in-the-middle attack (MiTM), denial of service attack and many other.

4. CONCLUSIONS

Thus, IP Spoofing is less of the threat today due to the patches to the Unix operating system and the wide spread use of random sequence numbering. many security experts are predicting a shift from IP spoofing attacks to application-related spoofing in which hackers can exploit a weakness in a particular service send and receive information under false identities. As security professional we must remain current with the operating systems that we use in our day to day activities. A study stream of changes and new challenges is assured as the hacker community continues to seek out vulnerabilities and weaknesses in our systems and our networks.

REFERENCES

[1] "Total Midyear Population for the World: 1950-2050"". International Programs Center for Demographic and Economic Studies, U.S. Census Bureau. Retrieved 2014-05-24.

[2] Stephen M. Specht, Ruby B. Lee "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures"

[3] Wang H., Jin C. and Shang K., "Defense Against Spoofed IP Traffic Using Hop-Count Filtering", IEEE/ACM Trans. Networking, vol. 15, no. 1, pp. 40-53, 2007.

[4] Wang, Xia, Li, Ming, Li, Muhai, "A scheme of distributed hop-count filtering of traffic," IET International Communication Conference on Wireless Mobile and Computing (CCWMC), pp.516-521, 7-9, 2009.

[5] Information Sciences Institute, Internet Protocol, Information Processing Techniques Office, University of Southern California, September 1981