MAC flooding Attack Prevention with Machine Learning

Sreeja Nair M.P[1], Akhila L[2]

[1]Division of CSE, Cochin University College of Engineering Kuttanad, Alappuzha, Kerala, India, sreejanairmp@gmail.com

[2]Division of ECE, Cochin University College of Engineering Kuttanad,Alappuzha, Kerala, India, akhilamailid@gmail.com

Abstract: *Media Access Control (MAC)attack is a type of attack in computer networks to challenge the security of network switches. The network is flooded with fake MAC addresses to steal sensitive information from the network. In this paper we propose three techniques with our traditional methods to prevent MAC Flooding Attack. They are priority scheduling with time stamp, authorization, authentication technique with digital signature and a security measure by using machine learning. Also examine how to limit the number of entries in a MAC table.*

Keywords: MAC, Spoofing, Authentication Filtering

I. INTRODUCTION

MAC Flood Attack is very crucial attack in the cyber world today. To understand the attack in detail we need to understand the following

Media Access Control (MAC)

Media Access Control is a sublayer of the data link layer of OSI reference model. MAC has an important function that is transmitting data packets to and from the network interface Card (NIC)and other channels. It is responsible for flow control and multiplexing for transmission medium. MAC Layer controls the transmission of data packets via remotely shared channels. It is responsible for encapsulating frames so that they are suitable for transmission through the physical medium. Also, MAC resolves the addressing of source station as well as the destination station and performs multiple access resolutions when more than one data frame is to be transmitted. Then determines the channel access method for transmission.

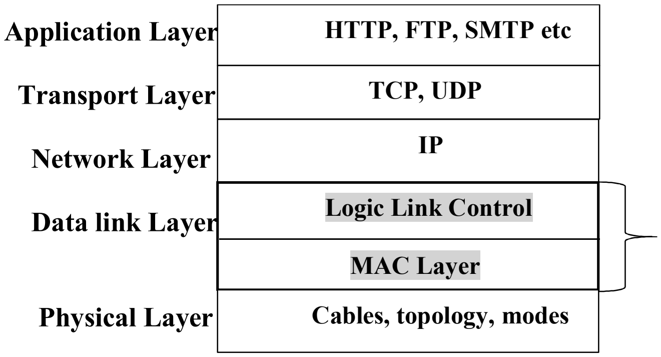


Figure.1. Network Layers

MAC Addresses.

MAC address is a unique identifier allotted to a network Interface Controller (NIC) of a device. It is used as a network address for data transmission with in a network segment like Ethernet, Wi-Fi and Bluetooth. This address is assigned to a network adapter at the time of manufacturing. It is hardwired or hard coded in the Network interface Card(NIC).A MAC address comprises of six groups of two hexadecimal digits, separated by hyphens, colons or no separators: An example of MAC address is 00:0A:89:5B:F0:11.Here the leftmost six digits represents organization unique identifier and last six digits represents network interface card.

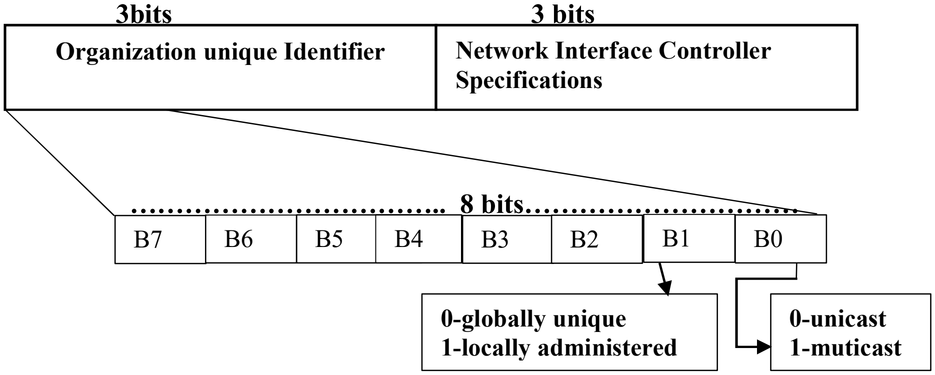

3bits
3 bits
Organization unique Identifier
Network Interface Controller Specifications
.... 8 bits.............................
B7
B6
B5
B4
B3
B2
B1
B0
0-globally unique
1-locally administered
0-unicast
1-muticast

Figure.2.MAC Address Format)

Managing the MAC Address Table

Switches use MAC address tables to determine how to forward traffic between ports. These MAC tables include dynamic and static addresses. Dynamic addresses are source MAC addresses that the switch learns and then ages when they are not in use. You can change the aging time setting for MAC addresses. The default time is 300 seconds. Setting too short an aging time can cause addresses to be prematurely removed from the table. Then, when the switch receives a packet for an unknown destination, it floods the packet to all ports in the same LAN (or VLAN) as the receiving port. This unnecessary flooding badly affect the performance. Setting too long an aging time can cause the address table to be filled with unused addresses, which prevents new addresses from being entered. This can also cause flooding. The switch provides dynamic addressing by learning the source MAC address of each frame that it receives on each port, and then adding the source MAC address and its associated port number to the MAC address table. As computers are added or removed from the network, the switch updates the MAC address table, adding new entries and aging out those that are currently not in use. A network administrator can specifically assign static MAC addresses to certain ports. Static addresses are not aged out, and the switch always knows which port to send out traffic destined for that specific MAC address. As a result, there is no need to relearn or refresh which port the MAC address is connected to. One reason to implement static MAC addresses is to provide the network administrator complete control over access to the network. Only those devices that are known to the network administrator can connect to the network.

Network Switches

A network switch is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device. It is a multiport network bridge that uses MAC address to forward data at the datalink layer. Switches look the frame's hardware address (MAC address) to determine where the frame needs to be or if it needs to be dropped. Switches offers the following features

- They provide hardware-based bridging (MAC addresses)
- They work at wire speed, therefore have low latency
- They come in three different types: Store & Forward, Cut-Through and Fragment Free (analyzed later)

Every Switch has three stages

- Address Learning
- Forward/Filter decisions
- Loop Avoidance (Optional)

Address learning

When a switch is powered on, the MAC filtering table is empty. When a device transmits and an interface receives a frame, the switch places the source address in the MAC filtering table remembering the interface the device on which it is located. The switch has no choice but to flood the network with this frame because it has no idea where the destination device is located. If a device answers and sends a frame back, then the switch will take the source address from that frame and place the MAC address in the database, associating this address with the interface that received the frame. Since the switch has two MAC addresses in the filtering table, the devices can make a point-to-point connection and the frames will only be forwarded between the two devices. Most desktop switches these days can hold up to 8000 MAC addresses in their table, and once the table is filled, then starting with the very first MAC entry, the switch will start overwriting the entries.

Forward/filter decision

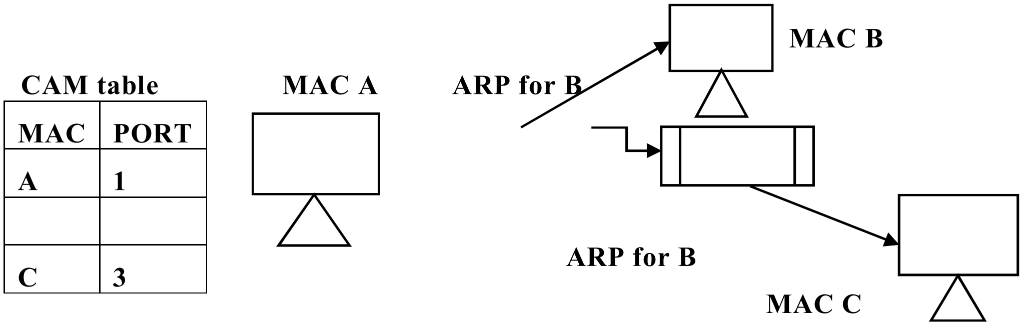
When a frame arrives at the switch, the first step is to check the destination hardware address, which is compared to the forward/filter MAC database. If the destination hardware address is known, then it will transmit it out the correct port, but if the destination hardware address is not known, then it will broadcast the frame out of all ports, except the one which it received it from. If a device (computer) answers to the broadcast, then the MAC address of that device is added to the MAC database of the switch.

Loop avoidance (optional)

The design and operation of ethernet requires that only a single packet transmission path may exist between any two stations. An ethernet grows by extending branches in a network topology called a tree structure, which consist of multiple switches branching off a central switch. In a complex network it is very dangerous because multiple inter switch connection can create a loop path in the network. Packets will circulate endlessly around the loop causes high traffic and overload. The IEEE 802.1D bridging standard provides a spanning tree protocol to avoid this problem by automatically suppressing forwarding loops.

II. MAC Flooding Attack

The MAC Flooding is an attacking method intended to not compromise the security of the network switches. Usually, the switches maintain a table structure called MAC Table. This MAC Table consists of individual MAC addresses of the host computers on the network which are connected to ports of the switch. This table allows the switches to direct the data out of the ports where the recipient is located. The aim of the MAC Flooding is to takedown this MAC Table. In a typical MAC Flooding attack, the attacker sends Ethernet Frames in a huge number. When sending many Ethernet Frames to the switch, these frames will have various sender addresses. The intention of the attacker is consuming the memory of the switch that is used to store the MAC address table. The MAC addresses of legitimate users will be pushed out of the MAC Table. Now the switch cannot deliver the incoming data to the destination system. So considerable number of incoming frames will be flooded at all ports.MAC Address Table is full and it is unable to save new MAC addresses. It will lead the switch to enter into a fail-open mode and the switch will now behave same as a network hub. It will forward the incoming data to all ports like a broadcasting. As the attacker is a part of the network, the attacker will also get the data packets intended for the victim machine. So that the attacker will be able to steal sensitive data from the communication of the victim and other computers. Usually a packet analyzer is used to capture these sensitive data. After launching a MAC Flood attack successfully, the attacker can also follow up with an ARP spoofing attack. This will help the attacker retaining access to the privileged data even after the attacked switches recover from the MAC Flooding attack.



CAM table

MAC	PORT
A	1
C	3

Figure.3.MAC Flooding

III. Prevention against MAC flooding

MAC flooding attack is a dangerous attack in the cyberworld today. This type flooding leads a denial of service in the internet. Some traditional methods are existing to prevent this attack. We propose some kind of new algorithms in the existing technique to improve the performance and result. The existing traditional methods are as follows
1.port security
2.Authentication with AAA server
3.Security Measures to prevent ARP spoofing or IP spoofing
4.Implement IEEE 802.1X suite

We introduce a new port security technique with priority scheduling and a time stamp.Thus, ports are free from flooding or congestion. To track authentication, we suggest to use packet filter firewall that implement with direct digital signature. Then apply some security measures like exact match checking for MAC address with a machine learning approach like decision tree method. This technique would help to avoid ARP spoofing or IP spoof attack generated by MAC Flooding attack.

Port Security with priority scheduling and a time stamp

Switch ports are vulnerable to flooding. So, we need to limit number of MAC addresses that are to connected to the port of end stations. To limit the number of MAC address, we propose a method that is priority scheduling with timestamps. Priority scheduling is a method based on priority in which the MAC addresses are selected as per the priority. The address with high priority should be done first whereas the addresses with equal priority are carried out as first in first out method or time scheduling method. Priority depends on memory requirements, time requirements etc. Ports accepts the addressees only if the address contains a time stamp that in ports knowledge of current time. This approach requires that clocks among various ports of the connection to be synchronized.

Authentication with AAA server and packet filtering firewalls with machine learning

An ***AAA*** server is a server program that handles user requests for access to computer resources and for an enterprise provides ***authentication, authorization and accounting services***. ***Authentication*** is the process of identifying a MAC address usually based on the availability in the MAC address table. ***Authorization*** is the process of granting or denying a user access to network resources one authentication is completed. ***Accounting*** is the process of keeping track of the activity while accessing the network resources including the amount of time spent in the network etc.

As per our concern, Authentication and Authorization can be provided with ***direct digital signature***. The direct digital signature involves only source and destination. Destination knows the public key of the source. Digital signature may be formed encrypting the entire message with the sender's private key by encrypting a hash code of the message with sender's private key.

Security Measures to prevent ARP spoofing or IP spoofing

Different security measures can be added. In this paper we suggest packet filtering firewall with decision tree machine learning algorithm and security protocols. So the exact matching MAC addresses are entered and processed. Others are filtered out. It can avoid ARP spoofing and IP spoofing attacks.

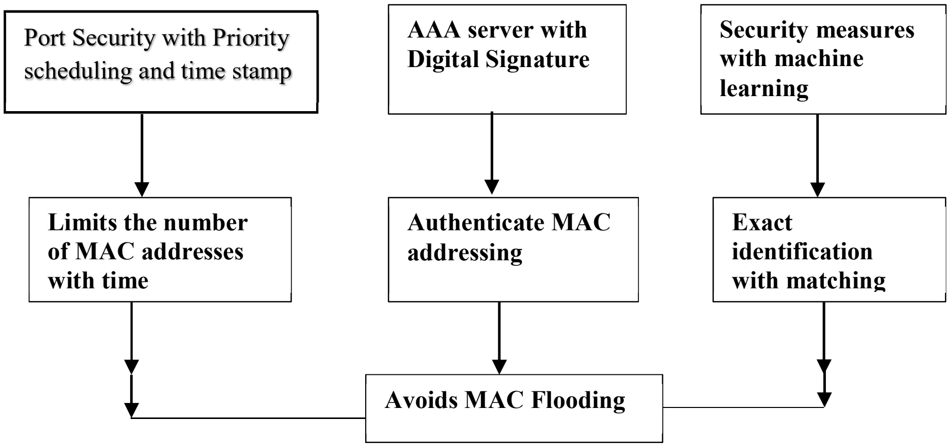

Port Security with Priority scheduling and time stamp
AAA server with Digital Signature
Security measures with machine learning
Limits the number of MAC addresses with time
Authenticate MAC addressing
Exact identification with matching
Avoids MAC Flooding

Figure.5. Proposed System

IV. Results and Discussion

MAC flooding attack happening in the second layer that misleads the switch ports, Memory of the victim computer, System configuration etc. Moreover, it leads the system in congestion, flooding etc. Network switches are always in open mode. But due to this issue it will fall in to fail-open mode. Thus, a denial of service attack may be happened, the clients cannot reach the destination. Our proposed System provide better result in security, authentication, congestion control, limited flood etc. Performance increasing as 90%. The following table shows which parameters give a better result with our proposed system.

Table.1.Performance of proposed system

Parameters	Existing System	Proposed System
Congestion	**May be**	**Not formulate**
Hijacking	**Less effective**	**More Effective**
Authenticity	**minimum**	**Maximum**
Flooding	**more**	**Less**
Injection of malicious data	**more**	**less**
Accounting	**Not much safe**	**safe**
Matching	**Not much clear**	**Clear very well**
Time	Not limited	Limited

V. Conclusion

MAC flooding attack is very intensive attack today in the lowest network level. We examined the scope of the attack in detail and suggest some new methods to prevent the effect of MAC flooding attack. Exact differentiation of processing is available. So clear cut output should be obtained.

Acknowledgments

Sincere Thanks to all who gave support and guidance for this work

REFERENCES

[1] L.Senecal, "*Understanding and preventing attacks at layer 2 of the OSI reference Model*", 4th annual communication Networks and Services conference (2006)

[2] William Stallings, "*Cryptography and network Security*", Fourth edition, Pearson Education.

[3] Sumit Dhar, *"Switch Sniff, Linux Journal*" (2002)

[4] Tapan P Gondaliya, Maninder Singh, "*Intrusion Detection System on MAC layer for attack prevention in MANET*", Fourth International conference on computing, Communications and Networking technologies",2013

[5] Larsen, R. Trip and C. R. Johnson, "*Methods for procedures related to the electrophysiology of the heart"*, U.S. Patent 5,529,067, **(1995)** June 25.

[6] Mallesham Dasani, Stony Brook, "*Real Time Detection of MAC Layer DOS attack in IEEE 802.11 wireless networks*",14th IEEE Annual Consumer Communications And Networking conference (2017)