An Optimized Solution for Detectionof MAC Flooding Attack

Mrs. Ayesha Taranum[1], Juhi Jahan J[2], Likhitha M[3], S Jayalakshmi[4], Shambavi S[5]

Faculty[1], Students[2,3,4,5]

Department Of Information Science and Engineering,

GSSS Institute of Engineering and Technology For Women, Mysuru, India.

---***---

Abstract : Flooding attack is one of the forms of DDos attack whereby certain nodes in the network miss utilizes theallocated channel by flooding packets with very high packet rate to its neighbours, causing a fast energy loss to the neighbors and causing other legitimate nodes a denial of routing and transmission services from the nodes. In this work we propose a novel link layer assessment based flooding attack detection and prevention method.MAC layer of the nodes analyzes the signal properties and incorporated into the routing table by a cross layer MAC/Network interface. Once a node is marked as a flooding node, it is blacklisted in the routing table and it is communicated to MAC through network/MAC cross layer interface. Results show that the proposed technique products more accurate flooding attack detection in comparison to current state of art statistical analysis based flooding attack detection by network layer.

IndexTerms – MANET, Flooding Attack, DDoS, Cross Layer.

1. INTRODUCTION

The MAC Flooding attack is an attacking method which is mainly intended to compromise the security of network switches. It is not a method of attacking any host machine but attacking a network switch, where the attacker continuously sends packets to switch in order to fill the MAC table. The proposed project aims on detection of MAC flooding attack occurring on an networking switch .The main goal of an attacker is to flood the MAC table present in the switch, to downgrade the actual functioning of switch .Once the MAC table is filled the switch enters into an open-fail mode, where the switch acts as a hub by broadcasting the data to all the connected ports, so that it eases the attacker to gain access to the n number of systems connected to it. Hence the filtering of white list genuine users and network traffic control is been carried out by MONOSEK server.

2. EASE OF USE

The distributed denial of service attack(ddos) causes a major threat to the security of target website, Internet infrastructure, by consuming all available bandwidth at the victim side and denying access to legitimate users. A DDoS attack can be launchedin many different ways. One of the approaches is to exploit software and protocol vulnerabilities of the system. The second approach is based on sending huge volume of attack traffic at victim end. Which is called flooding based DDoS attack. This MAC Table consists of individual MAC addresses of the host mainframes on the network which are connected to ports of theswitch. This table allows the switches to direct the data out of the ports where the recipient is located. The hubs broadcast the data to the entire network allowing the data to reach all hosts on the network but switches send the data to the specific machine which the data is intended to be sent. This goal is achieved by the use of MAC tables. 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 the 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 broadcasting. Let's see the benefits of the attacker with the MAC Flooding attack.

As the attacker is a part of the network, the attacker will also get the data packets intended for the victim machine. So the attacker will now 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 honored data even after the attacked switches recover from the MAC Flooding attack.

3. SYSTEM ARCHITECTURE

3.1. Design

System development can generally be thought of having two major components: system analysis and system design. In system design, the system architecture is established. It starts with the requirement document delivered by the requirement phase and maps the requirement into architecture. The architecture defines the components, their interfaces and behaviors. The deliverable design document is the architecture. The design document describes a plan to implement the requirement.

3.2. Architecture
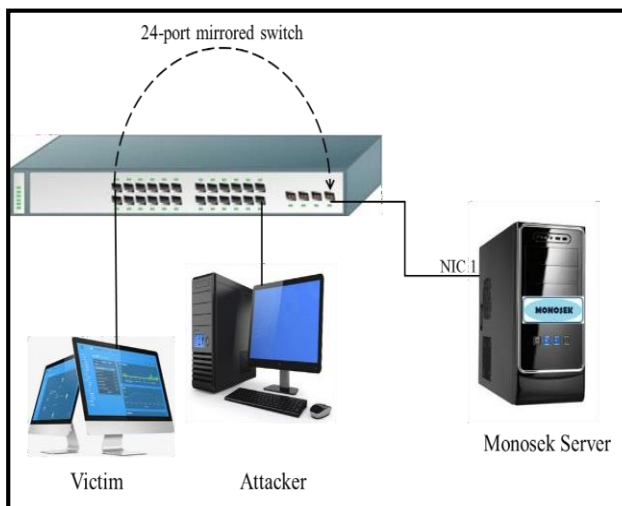
**Figure 1:** System architecture for detection of MAC Flooding Attack.

The figure1 describes the system architecture for detection of MAC Flooding attack. The attacker and victim are connected to a 24 port mirrored switch. Port mirroring is used on a network switch to send a copy of network packets seen on one switch port to a network monitoring connection on another switch port. This is used to monitor the network traffic and for detecting the intruder.

The first port of the switch is mirrored with the 24th port. This mirrored port is connected to the NIC 1 port of the MONOSEK server. The MONOSEK server scans the network traffic pattern and analyses the packets. It identifies the packet with receiving time less than threshold.

3.3.Design Diagram
> **Flow chart:**

A flowchart is a type of diagram that represents an algorithm, workflow or process. Flowchart can also be defined as a diagrammatic representation of an algorithm.
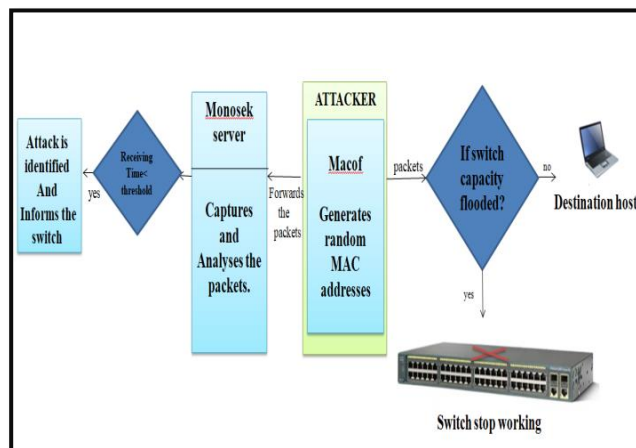
Figure 2: Data Flow Diagram of MAC Flooding Attack

The figure 2 depicts the Data Flow of MAC Flooding Attack. The scanner will collects all the packets and analyze them. If the sender sends genuine packets then the packet is forwarded via switch to its destination host. If the reception time between multiple packets less than attack is detected and an alert message is displayed in the server.
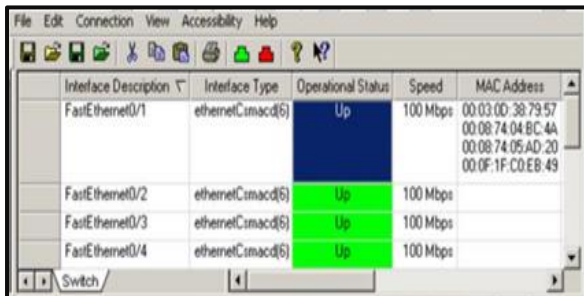
4. ATTACK DESCRIPTION

This attack intends to corrupt the entries in the switch's CAM table, so that the network traffic will be redirected. That is, a malicious host (connected to Port #a in a switch), sends a fake packet, with the source MAC address in the packet's Ethernet header set to the MAC address of a target host (connected to Port #b). The destination MAC address in the packet's Ethernet header can be any address. Once the switch receives the packet, it updates its CAM table. Therefore, the CAM table's entry for that target host's MAC address will be corrupted. Hence, the target host will be considered as a host connected to Port #a. Any packet sent to the target host (destination MAC address in the packet's Ethernet header is equal to the target host's MAC address) will be forwarded to Port #a; that is, to the malicious host. As example of CAM table poisoning attack, Figure 1 shows that in the CAM table of a switch, there are four hosts connected to the switch. Host #1, the malicious host, attacks the switch's CAM table using 3 fake packets. The three packets are almost the same, but they have different source MAC addresses in the Ethernet headers. The information of the packets is as follows:

1. First fake packet: Source MAC address in the Ethernet header= 00:08:74:04:BC:4A (Host #2).

2. Second fake packet: Source MAC address in the Ethernet header = 00:08:74:05:AD:20 (Host #3).

3. Third fake packet: Source MAC address in the Ethernet header = 00:03:0D:38:79:57 (Host #4).

After this attack, the switch's CAM table becomes corrupted, as shown in Figure 1. The CAM table shows that all four hosts are connected to the switch's Port#1 (FastEthernet 0/1). However, physically only Host#1 is connected to Port#1.

Once a packet is sent to one of these three hosts (Host#2, Host#3 and Host#4), the switch will forward it to Port#1; that is, to Host#1. This situation may create a DoS situation, since the switch is not forwarding the packets, issued from these three hosts, to their destinations.
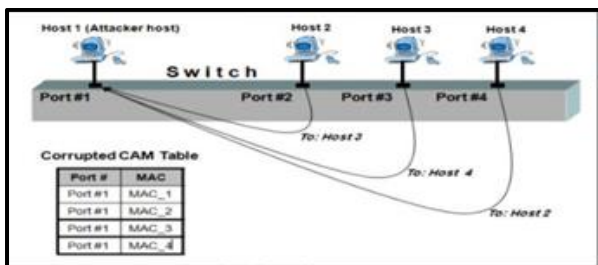
We assume that Host A wants to poison the switch's CAM table, by inserting the invalid entry: MAC address of Host B i.e Switch's Port 0/2 (Fa0/2). This invalid entry will tell the switch that Host B is now located at Port 0/2 (Fa0/2). However, physically, Host B is still located at Port 0/4 (Fa0/4). Hence to perform this attack, Host A should send to any destination host in the LAN network a fake packet (IP or ARP packet) whose Ethernet source MAC address is equal to the MAC address of Host B.

CONCLUSION

The proposed system will reduce the probability of an system getting Mac flooding attack by bringing the actions taken by attacker to security provider concern. The detection of attackers is done and flooding of switches is controlled.

REFERENCES

[1] Annamalai, Arunmozhi "Secured System against DDoS Attack in Mobile Adhoc Network"

[2] Priyadharshini, V., and K. Kuppusamy. "Prevention of DDOS Attacks using New Cracking Algorithm." International Journal of Engineering Research and Applications 2.3 (2012):2263-2267.

[3] Ming, Yu. "Mitigating Flooding-Based DDoS Attacks by Stochastic Fairness Queueing." Advances in Information Sciences & Service Sciences 4.6 (2012).

[4] Sharma, Prajeet, Niresh Sharma, and Rajdeep Singh. "A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network."International Journal of Computer Applications 41.21 (2012): 16- 21.

[5] Kumar, Mukesh, and Naresh Kumar. "Detection and Prevention of DDOS Attack in MANET'S Using Disable IP Broadcast Technique." International Journal of Application or Innovation in Engineering & Management (2013).

[6] J. Soryal and T. Saadawi, "Ieee 802.11 denial of service attack detection in manet," in Wireless Telecommunications Symposium (WTS), 2012. IEEE, 2012, pp. 1–8.

[7] "Byzantine attack isolation in ieee 802.11 wireless ad-hoc networks," in Mobile Adhoc and Sensor Systems (MASS), 2012 IEEE 9th International Conference on. IEEE, 2012, pp. 1–5.

[8] S. Radosavac, A. A. Cardenas, J. S. Baras, and G. V. Moustakides, ´ "Detecting ieee 802.11 mac layer misbehavior in ad hoc networks: Robust strategies against individual and colluding attackers," Journal of Computer Security, vol. 15, no. 1, pp. 103–128, 2007.

[9] C. Alocious, H. Xiao, and B. Christianson, "Analysis of dos attacks at mac layer in mobile adhoc networks," in Wireless Communications and Mobile Computing Conference (IWCMC), 2015 International. IEEE, 2015, pp. 811–816.

[10] Y. Zhou, D. Wu, and S. M. Nettles, "Analyzing and preventing maclayer denial of service attacks for stock 802.11 systems," in Workshop on Broadband Wireless Services and Applications (BROADNETS), 2004.