AN ANALYTICAL STUDY OF MAC ADDRESS SPOOFING

[1]Dr. Senthil Kumar M , [2]Ms.Suganya S

[1]Associate professor , [2] PG Scholar
Department of Computer science and Engineering
Valliammai Engineering College

Abstract **- In wireless environment each and every devices connected to particular access point are validated with an unique identifier (Mac Address). There are more vulnerability available in this wireless environment even spoofing attack on MAC address. Spoofing attack is stealing of information in an illegal manner while establishing a connection authentication as well as association takes place by considering MAC address as reference. Simultaneously an adversary can grasp those MAC address from victim and perform de-authentication and de-association and take full control over particular session.**

IndexTerms**: *MAC address, spoofing attack, authentication, association, adversary etc.***

I. INTRODUCTION

In today's world technology plays a vital role and leads to more establishment of new creative and innovative ideas which makes human work faster and easier. Parallel process that has much limitation. MAC address are those which uniquely provided to particular system during its manufacturing itself [1]. It cannot be redundantly used with more than one system. For that too have an threats received by adversaries. Adversary tends to spoof those MAC address while victim is in connection with access point after stealing the unique address it will terminate the connection between client and server.It tend to act as a particular client by using the same MAC address. There will not be any re-authentication in some situation and open access by simply verifying MAC address. For an instance, if we login our gmail account on particular device and connect to particular access point by validating MAC address.

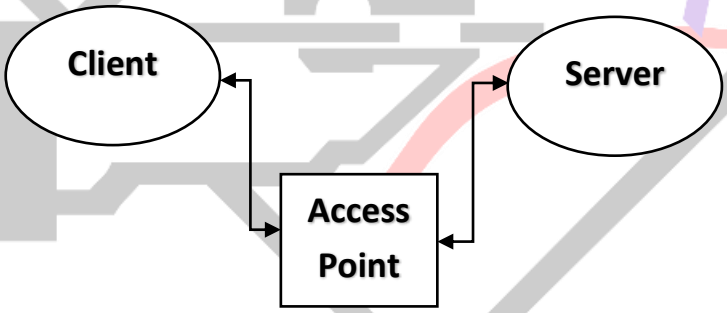

Fig -1 Secure Communication

If an adversary interrupts those connection and reconnect to that particular access point act as a victim in that case our account will not require authentication. Fig-1 shows the secure communication between client and server in absence of adversaries.

II. LITERATURE SURVEY

SHA (Session Hijacking Attack) is a process of overall control taken by an adversary and act as a particular victim to reconnecting those session. It is represented in fig-2 , also shows vulnerability during communication in presence of adversary. The techniques for ensuring and preclusion of spoofing attack are as follows

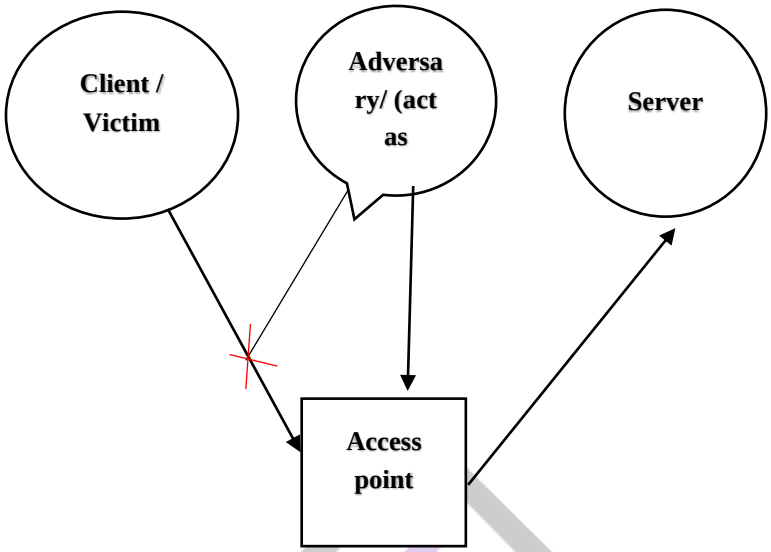

Fig-2 Session Hijacking Attack (SHA)

Detection based on Fingerprinting

Fingerprinting mechanisms based on evaluation of NIC (Network Interface Controller) Mac address and includes RF Fingerprinting[2], Passive Data link layer finger printing and Acknowledgement frame delay . In RF Fingerprinting detection based on the signal frequency by turning on transient. In passive data link layer based on timer. Acknowledgement frame delay is based on network delay occurrence.

Monitoring RSS and RTT

In wireless network at the physical layer the signal transmission are monitored in many ways. RSS by using antenna the received signal strength is tracked. During the session request as well as response time is totally calculated as round trip time.

Sequence number renovation

In this method ,packet transmission at transport layer contains a three way handshake process. each and every packet recalculates its sequence number[3]. The limitation in this method is easily crack algorithm by collecting frequent packets and identifying its pattern.

Sequence number Gap

Detection of spoofing attack based on gap between sequence number of consecutive frames . If there is a delay then alarm will be raised[4].

Cross layer based IDS

Each node is provided with dynamic profile for establishing session , at physical layer it focuses on RSS value and keep track of it .then at the transport layer , time taken (TT) value during handshake process are focused . Both the RSS value and TT value are added to obtain combined weighted value , which is compared with threshold value . If weighted value is greater than threshold it is an adversary else an normal victim client[5].

Sensor nodes

While session starts between client and server, a client node needs to be in connection with access point(AP). The access point connects many nodes concurrently . If an attacker creates a fake access point to provide communication and collects the information regarding the packets sent and receive. This type of AP in which authentication as well as verification are not done by overall security policy are called as rogue access point[6].

Counter Measures

Mac address can be secured by the following guidelines :

- The user must have a rights to access their own rights by providing right privilege assigned to them
- Mac address need to be lock during TCP session in wireless environment and the router need to be provided with Mac filtering and IP reservation.
- The communication across nodes and access point need to be encrypted[7].

III. CONCLUSION

In this paper, we have studied about MAC address and its challenges across spoofing attack and according to the survey done there are availability of both the passive methods as well as active methods. Passive methods will only monitor the presence of adversary whereas active methods will take certain measures to overcome it. To provide an security to MAC address it is necessary to use both the passive methods (for detection) and active methods (for preventive measures) in an hybrid way.

IV. DISCUSSIONS

There are much more limitations in providing secure wireless environment .The unique identifier can also be spoofed and used in an illegal manner. So there are some above analysis techniques available to ensure and preclude from unauthorized activity. It need to be much focused to establish vulnerable free communications.

REFERENCES

[1] Enos LETSOALO, and Sunday OJO , " Survey of Media Access Control address spoofing attacks detection and prevention techniques in wireless networks", http://www.ist-africa.org/Conference2016
[2] G Lackner, U Payer, and P Teuff, "Combating Wireless LAN MAC-layer Address Spoofing with Fingerprinting Methods", International Journal of Network Security, Vol.9, Sept. 2009.
[3] N Nishanth and S. Suresh Babu, "Sequenced Number Alteration by Logical Transformation (SALT): A Novel Method for Defending Session Hijacking Attack in Mobile Ad hoc Network", International Journal for Computer and Communication Engineering, Vol. 3, No. 5, September 2014.
[4] R Gill, J Smith, M Looi, A Clark, "Passively Detecting Session Hijacking Attacks in IEEE 802.11 Networks", Information Security Institute, Queensland University of Technology, 2005.
[5] J Singh, L Kaur, and S Gupta, "A Cross-Layer Based Intrusion Detection Technique for Wireless Networks", The International Arab Journal of Information Technology, Vol. 9, No. 3, May 2012.
[6] Abishek kumar Bharati and Manoj Chaudhary, Prevention of session hijacking and IP spoofing with sensor nodes and cryptographic approach" , International Journal of Sciences : Basics and Applied Research (IJSBAR) , Vol.6, No.1, 2012.
[7] Payal Pahwa , Gaurav Tiwari , Rashmi Chhabra , "Spoofing Media Access Control (MAC) and its Counter Measures" , International Journal of Advanced Engineering & Application , Jan. 2010.