

# PREVENTING ROGUE ACCESS IN WIRELESS NETWORKS

Preethi S, Poornima M  
 Sri Sai Ram Engineering College, Chennai  
 Department of Information Technology  
 preethis10@gmail.com,poorni.elan@yahoo.com

**Abstract** - Wireless Communication is one of the biggest assets provided to us through the evolution of wireless networks. Its availability and flexibility has attracted a large number of users in a short span of time, but new technologies bring in new vulnerabilities. Though wireless networking has many advantages and privileges, due to the vulnerabilities of rogue access in the network, it has prevented large enterprises and business people from using the wireless communication for sharing of critical information. Rogue access is the most important threat that brings in a lot of problems like denial of service, rogue clients. This paper addresses a solution to prevent rogue access in wireless network. Rogue access through MAC address spoofing is detected and prevented from acquiring an access in a network and also to prevent setting up of rogue access points within an enterprise network.

**Keywords** - Hybrid detection, Intrusion detection, MAC Spoofing, Rogue Access Point, Stateful Protocol Analysis.

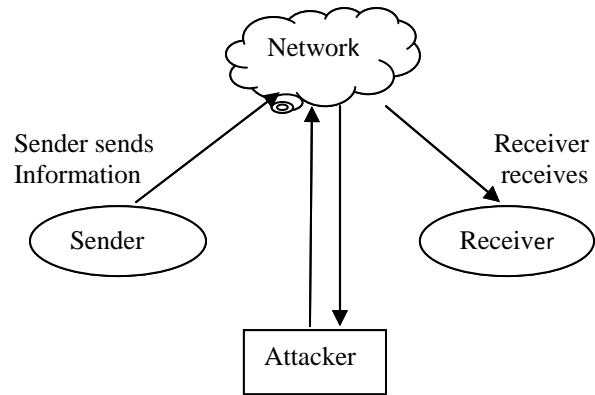
## I. INTRODUCTION

Wireless communication has gained its maximum popularity [1] in the recent years. But still due to the security problems in the wireless networks limits the users from using it. The security issues arising from a wireless communication is entirely different from wired communication. The development in the handheld and mobile devices has increased the necessity to create robust networks. Hence we need to adapt new standards, protocols and technologies which become widespread among the users and also attract the network attacker which brings out the breakability in these standards. The data can be transmitted over a wide area and thus an unauthorized individual within the limits of data transmission can easily acquire the confidential information. Hence these kinds of problems and security issues have to be taken into account in order to have a secured wireless infrastructure.

## II. PROBLEMS IN WRELESS AND SUGGESTED SOLUTIONS

An important attack in the wireless network is man-in-the-middle attack. In this attack, when an attacker comes to know about an unencrypted wireless access

point he inserts himself into the network and starts relaying messages to the users.



Attacker inserts himself in the network and relays message between sender and receiver

Figure 1.1 Man-in-the-middle attack

Due to the development in technology the access points can be easily bought as they are very inexpensive [2]. These access points can be brought inside and connected to an enterprise network. The security policies in these access points are configured to default settings and hence if it violates the enterprise network security policies it becomes unnoticed. These access points become an open network for any outsiders to listen to the enterprise network traffic. If any confidential information that is being relayed between the authorized users it becomes open for an attacker. To prevent these rogue access points with in an enterprise network, sensors has been implemented which detects rogue access points and notify the network administrator.

## III. PREVENTING A ROGUE ACCESS POINT

The network sensor which is used for detecting rogue access point is made to work in both the channels i.e. 2.4 GHz and 5 GHz. If any new access points were set up with in the enterprise network it will detect and notify it to the network administrator. If the network administrator discovers it as a rogue access point, he can deny the service for that access point. If it is not a rogue access point and the user of

that access point wants to connect it to the enterprise network, the user can demand the network administrator to authenticate the connection. Now the administrator can follow the network traffic of the new access point. The administrator can also verify whether the security policy of the newly set up access point matches to the security policy of the enterprise network. If the new access point is open or transmits information to the illegal users, the network administrator should detect it and deny the service. Thus these are the novel solutions for preventing the rogue access within a wireless network.

#### IV. INTRUSION DETECTION TECHNIQUES

In order to differentiate between the authorized and unauthorized user in a wireless networks, three conventional intrusion detection techniques are under use. (Media Access Control address) a MAC address is a unique identifier ascribed to every network adapters or the Network interface cards(NIC cards).These MAC addresses helps to identify every user uniquely. MAC address spoofing [3] is a case in which an illegal user alters his MAC address to that of the authorized MAC address. These illegal users using the spoofed MAC address can now enter into a network as an authorized user.

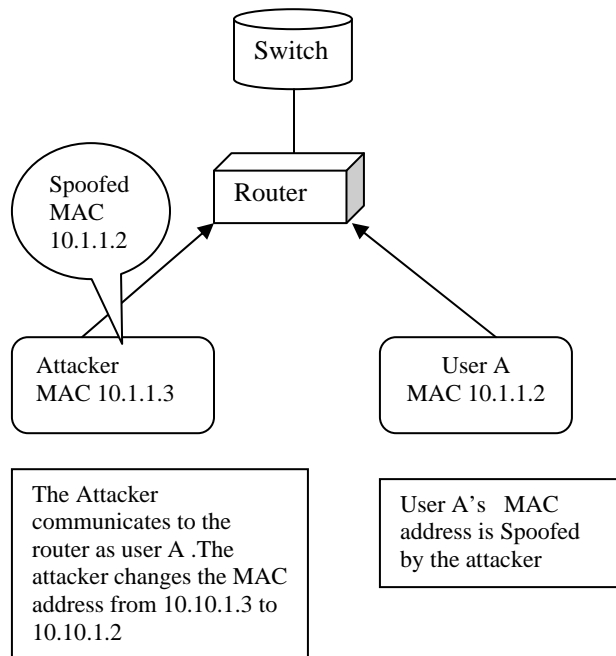


Figure 1.2 MAC Spoofing

Hence to overcome these problems we use intrusion detection techniques. The three types of techniques are as follows

##### A. Anomaly Based Intrusion detection

In this type of detection technique, the system saves the normal behavior as a baseline characteristic. If the current behavior of the user deviates from the baseline it will detect it as an unauthorized user and denies the service.

##### B. Signature Based Intrusion Detection

In this type of detection technique there are predefined attack patterns called signatures. If the system comes across these types of attack patterns within a network it will refuse the services.

##### C. Stateful Protocol Analysis

In this type of detection technique the protocol state of the authorized user is maintained. If the current user's protocol does not match with the maintained record, the system will disclose it as a rogue user. Even though these intrusion detection systems helps to identify MAC spoofed addresses and rogue access in a network, they are not fully reliable since they are vulnerable to produce false positive alarms. To overcome these problems of MAC spoofing and rogue access with in a network we move on to Hybrid Detection technique.

#### V. HYBRID DETECTION TECHNIQUE (PROPOSED)

A combination of all the three detection techniques is called as hybrid detection. The important features in the three detection technique are blended to form hybrid detection. The significant attributes that detects the difference in the users behavior in every detection technique is taken into the Hybrid Detection.

##### A. Detection Mechanism

Here in this technique ,the users behaviors are detected and if any illicit behavior is noticed it is reported to the network administrator .The user's behavior is passed into the hybrid detection system which contains three databases for each type of detection technique .After checking whether the behavior is synchronizing ,the amount of synchronization is calculated for each database .Henceforth three such values are produced from each database .Then the average of all the three calculated values is used in detecting whether the user is an authorized or a unauthorized user. To know whether the user is authorized a minimum percentage of synchronization with the normal behavior is needed, so we define a threshold value. For each type of detection the minimum percentage of synchronization for the normal behavior is calculated.

The calculated values from each database is compared with the threshold value .Thus if it is discovered to be less and if the average is also less than the average of the threshold value, it is considered as a rogue access.

characters or manners in usage. Henceforth it helps to avoid many false positive alarms and irrelevant alerts.

This method of detection has the following advantages

1. It detects for all types of discrepancies in the users behavior.

2. In the existing technology whenever more than one instance of *MAC* address is recognized by the sensors ,access to the network is temporarily blocked ,in our technique both instances of the *MAC* address is tested using our detection technique which checks all the activities of the user .Hence false alarms could be reduced.

3. Rogue Access points set up within a network is also discovered and also helps to set up authenticated access points wherein the network traffic of the network is watched over by the network administrator.

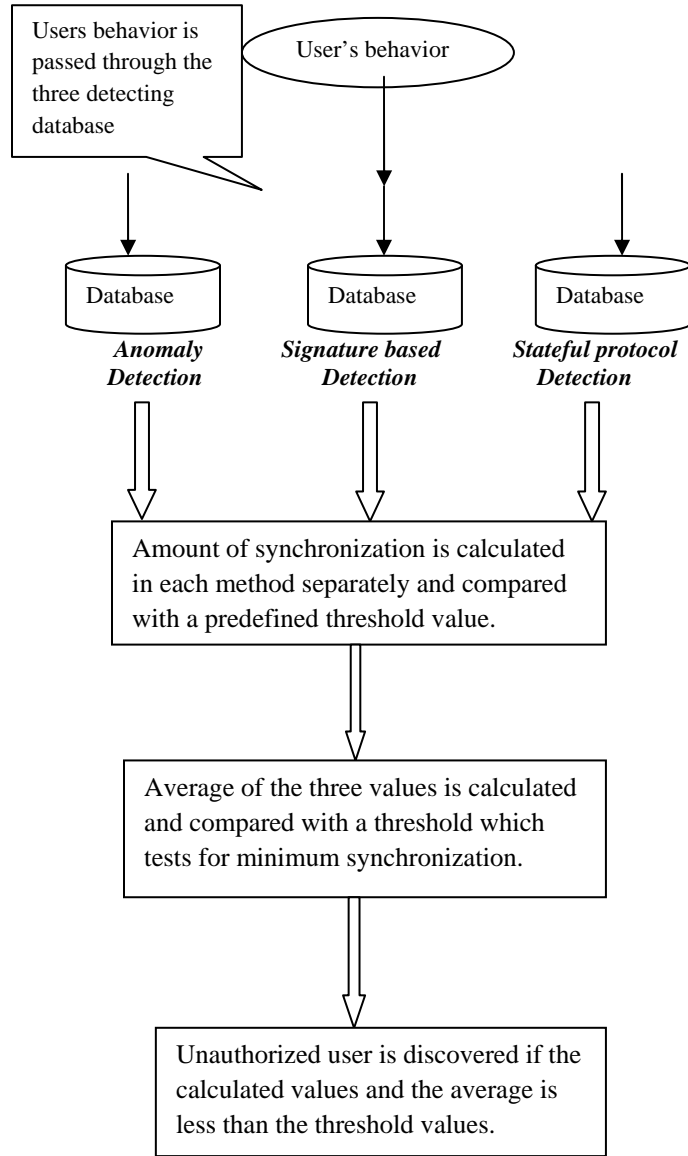


Figure 1.3 Hybrid detection technique

### B.Solution for MAC Spoofing

If more than one instance of *MAC* address is spotted in an enterprise network, both the *MAC* address user's behavior is tested using the hybrid intrusion detection .Both the user's behavior is passed through the detection technique as shown in the above figure1.3. The spoofed *MAC* address can be easily found using this technique .Since the behavior of the normal authorized user is assumed to have similar

## VI. CONCLUSION

Thus the security issues and vulnerabilities in a wireless enterprise network are discussed and the possible solution for constructing a secured infrastructure to relay critical information among the authorized users in established connection. Thus confidentiality of the data in an enterprise network is maintained.

## REFERENCES

[1] Din0 A. Dai Zovi, Shane A. Macaulay "Attacking Automatic Wireless Network Selection" Proceedings of the 2005 IEEE Workshop on Information Assurance and Security. United States Military Academy, West Point, NY.  
 [2] Neel Diksha and Agarwal Shubham "Backdoor Intrusion in Wireless Networks- problems and solutions". Indian Institute of Information Technology-Allahabad, India  
 [3] Mudhakar Srivatsa," Who is Listening, Security in Wireless Networks" .IEEE-International Conference on Signal processing, Communications and Networking. Madras Institute of Technology, Anna University Chennai India, Jan 4-6, 2008. Pp1 67-172  
 [4] Taghi M. Khoshgoftaar, Shyam V. Nath, and Shi Zhong, Naeem Seliya "Intrusion Detection in Wireless Networks using Clustering Techniques with Expert Analysis" Proceedings of the Fourth International Conference on Machine Learning and Applications (ICMLA'05) 2005 IEEE.