ISSN:0975-9646

A Novel and Light Weight Defence Mechanism for Securing Wireless Networks

Prajnya Priyadarsini Satapathy[#1], Debi Prasad Mishra[*2] Deepesh Kumar Singh[#3]
[#]*Department of Information Technology, College of Engineering and Technology,*
Bhubaneswar, Odisha, India

***Abstract*— Wireless network is the network which is easy to deploy and very easy to access that network and that network is user friendly. The main reason behind wireless lan is gaining popularity because it provide benefits, like easy installation, flexibility, mobility, scalability and reduced cost of ownership. But drawback in these wireless networks is that it doesn't provide security as much as required, due to that user faces attacks of various types which are damageable to user information. Spoofing with falsified IP-MAC pair is the first step in most LAN based attacks. Address Resolution Protocol (ARP) is stateless, which is the main cause that makes spoofing possible.**

Several network level and host level mechanisms have been proposed to detect and mitigate ARP spoofing but each of them has their own drawback. In this proposed work a new technique is developed for detecting identity attacks or spoofed MAC attack exploited in 802.11 wireless network. Current methods of device identification includes only probe request packets which results in large amount of false positive. In our proposed work the algorithms are developed upon three frames which are required in three section of connectivity phase and that frames are probe request frame, authentication frame and association frame. The proposed scheme is successfully verified under all possible attack scenarios. The scheme is successfully validated in a test bed with various attack scenarios and the result shows the effectiveness of the proposed technique.

Keywords:- IP-MAC pair, Probe frame, Association frame, Authentication frame , IEEE 802.11 wlan, spoofing attacks

I. INTRODUCTION

Wireless Local Networks are hard and difficult and hard to provide stronger security as compared to wired local area network , main reason behind these weakness and possibility of attacks is the fact that these network can be accessed by Wireless networks communicate to each other and the Internet via an Access Point (AP) or a wireless router. The AP needs to be connected to a backbone [1] wired network in order to connect its wireless clients to the Internet. In order to achieve this setup the AP is connected to a switch, which serves wired clients as shown in Figure 1. This enables the wireless clients to access the Internet just like the wired clients connected to this switch. Based on the security and performance considerations, it is not practical to design a pure wireless network system for the enterprise. As different technologies developed and several companies started manufacturing the communication devices, a strong need was felt to standardize their identification mechanism and to have a common addressing scheme which could be used to identify these different communication devices their types, manufactures and other related details on the networks. One such mechanism that has now been standardized by IEEE is the Media Access Control Address (MAC) addressing scheme.

A Media Access Control address (MAC address) is a unique identifier assigned to network interfacing devices for communications on the network segment. MAC addresses are used for numerous network technologies and most IEEE 802 network technologies including Ethernet. Logically, MAC addresses are used in the Media Access Control protocol sub-layer. The MAC addressing scheme acts as a permanent worldwide identification mechanism assigned to Network interface card (NIC) & other networking equipment by their Manufacturers. The MAC address is usually burnt in the hardware by the manufacturer of the device.

II. BACKGROUND

As per the 802.11 specification [1] client authentication process consists of the following transactions as mentioned below

1. The Access points continuously send out Beacon Frames which are picked up by the nearby wlan clients.
2. The client can also broadcast on its own probe request frame on every channel
3. Access points within range respond with a probe response frame
4. The client decides which access point (AP) is the best for access and sends an authentication request
5. The access point will send an authentication reply
6. Upon successful authentication, the client will send an association request frame to the access point
7. The access point will reply with an association response
8. The client is now able to pass traffic to the access point

There are 3 types [2, 3] of frames used in the 802.11 MAC layer 2 communications happening over the air which manages and controls the wireless link.

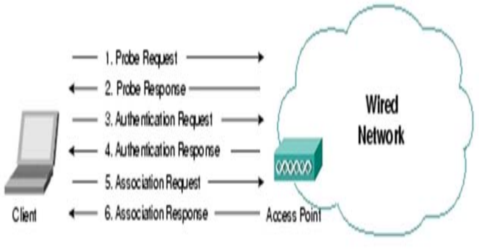

Figure 1: IEEE 802.11 Client Architecture

They are Management Frames, Control Frames and Data frames. Let's take a peek at what those frames consist of in little details to help us in analyze the wlan problems better while working with wlan sniffer traces. 802.11 management frames enable stations to establish and maintain communications.[4]

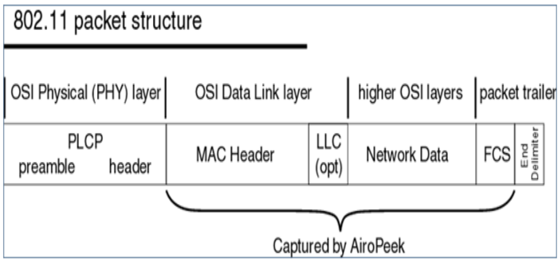

Figure 2: IEEE Packet Structure

The following are common 802.11 management frame subtypes:

- **Authentication frame**: 802.11 authentication is a process whereby the access point either accepts or rejects the identity of a radio NIC. The NIC begins the process by sending an authentication frame containing its identity to the access point. With open system authentication (the default), the radio NIC sends only one authentication frame, and the access point responds with an authentication frame as a response indicating acceptance (or rejection). With the optional shared key authentication, the radio NIC sends an initial authentication frame, and the access point responds [3] with an authentication frame containing challenge text. The radio NIC must send an encrypted version of the challenge text (using its WEP key) in an authentication frame back to the access point. The access point ensures that the radio NIC has the correct WEP key (which is the basis for authentication) by seeing whether the challenge text recovered after decryption is the same that was sent previously. Based on the results of this comparison, the access point replies to the radio NIC with an authentication frame signifying the result of authentication.
- **De-authentication frame**: A station sends a de-authentication frame to another station if it wishes to terminate secure communications.
- **Association request frame:** 802.11 associations enable the access point to allocate resources for and synchronize with a radio NIC. A NIC begins the association process by sending an association request to an access point.[4] This frame carries information about the NIC (e.g., supported data rates) and the SSID of the network it wishes to associate with. After receiving the association request, the access point considers associating with the NIC, and (if accepted) reserves memory space and establishes an association ID for the NIC.
- **Association response frame**: An access point sends an association response frame containing an acceptance or rejection notice to the radio NIC requesting association. If the access point accepts the radio NIC, the frame includes information regarding the association, such as association ID and supported data rates. If the outcome of the association is positive, the radio NIC can utilize the access point to communicate with other NICs on the network and systems on the distribution (i.e., Ethernet) side of the access point.
- **Re-association request frame**: If a radio NIC roams away from the currently associated access point and finds another access point having a stronger beacon signal, the radio NIC will send a re-association frame to the new access point. The new access point then coordinates the forwarding of data frames that may still be in the buffer of the previous access point waiting for transmission to the radio NIC.
- **Re-association response frame**: An access point sends a re-association response frame containing an acceptance or rejection notice to the radio NIC requesting re-association. Similar to the association process, the frame includes information regarding the association, such as association ID and supported data rates.
- **Disassociation frame**: A station sends a disassociation frame to another station if it wishes to terminate the association. For example, a radio NIC that is shut down gracefully can send a disassociation frame to alert the access point that the NIC is powering off. The access point can then relinquish memory allocations and remove the radio NIC from the association table.
- **Beacon frame**: The access point periodically sends a beacon frame to announce its presence and relay information, such as timestamp, SSID, and other parameters regarding the access point to radio NICs that are within range. Radio NICs continually scan all 802.11 radio channels and listen to beacons as the basis for choosing which access [4] point is best to associate with.
- **Probe request frame**: A station sends a probe request frame when it needs to obtain information from another station. For example, a radio NIC would send a probe request to determine which access points are within range.
- P**robe response frame**: A station will respond with a probe response frame, containing capability information, supported data rates, etc., when after it receives a probe request frame.

1) Control Frames

802.11 control frames assist in the delivery of data frames between stations. The following are common 802.11 control frame subtypes:

- **Request to Send (RTS) frame**: The RTS/CTS function is optional and reduces frame collisions present when hidden stations have associations with the same access point. A station sends a RTS frame to another station as the first phase of a twoway handshake necessary before sending a data frame.

- **Clear to Send (CTS) frame**: A station responds to a RTS with a CTS frame, providing clearance for the requesting station to send a data frame. The CTS includes a time value that causes all other stations (including hidden stations) to hold off transmission of frames for a time period necessary for the requesting station to send its frame. This minimizes collisions among hidden stations, which can result in higher throughput if you implement it properly.
- **Acknowledgement (ACK) frame**: After receiving a data frame, the receiving station will utilize an error checking processes to detect the presence of errors. The receiving station will send an ACK frame to the sending station if no errors are found. If the sending station doesn't receive an ACK after a period of time, the sending station will retransmit the frame. [6, 7]

2) Data Frames

Of course the main purpose of having a wireless LAN is to transport data. 802.11 defines a data frame type that carries packets from higher layers, such as web pages, printer control data, etc., within the body of the frame. When viewing 802.11 data frames with a packet analyzer, you can generally observe the contents of the frame body to see what packets that the 802.11 data frames are transporting. [4]

III. Proposed scheme

In this section we discuss the proposed spoofing detection works.

From the probe request frame the first 3 bytes of MAC header is taken out for consideration which is Organisationally Unique Identifier (OUI) then it is compared with the table registered with IEEE ARP table present at the IEEE website. If the vendor ID of NIC and vendor name is found dissimilar then MAC Address is spoofed and client is not given permission for the access, otherwise the probe response frame is sent to the client and in the data field of the probe response is sent to the client then the client side the authentication request and the authentication request frame is compared with the value present at registry or configuration file depending on the operating system with the same network address. If any duplicate address is found then client is disconnected and authentication frame is not sent. Otherwise client is genuine and given access through the access point.[6, 7]

IV. Performance analysis

Scenario1:

The text bed had created for our experiments consist of different operating system: Ubuntu 14.04, windows 7 on Lenovo-pc, kali linux on SONY-pc. We name the machine as A, B, C where the machine C with kali linux is acting as the attacker machine.

When machine B sends probe request to access point A and NIC number is checked against ARP table present in the access point machine and is found to be correct and probe response is send. Then association request is send by the machine B to the access point A though no duplicate entry is found access point A gives permission for access to machine B.

When machine C sends probe request to access point A and NIC number is checked against ARP table present in the access point machine and is found to be incorrect and probe response can't send to machine C access point A doesn't gives permission for access to machine C.

Scenario 2:

The text bed had created for our experiments consist of different operating system: Ubuntu 14.04, windows 7 on SONY-pc, kali linux on SONY-pc. We name the machine as A,B,C where the machine C with kali linux is acting as the attacker machine.

When machine B sends probe request to access point A and NIC number is checked against ARP table present in the access point machine and is found to be correct and probe response is send. Then association request is send by the machine B to the access point A though no duplicate entry is found access point A gives permission for access to machine B.

When machine C sends probe request to access point A and NIC number is checked against ARP table present in the access point machine and is found to be correct and probe response send to machine C by the access point A then machine C sends association request to access point A and founds the duplicate entry then it doesn't give permission for access to machine C.

V. Conclusion

This technique is able to identify and find out which device is without spoofed MAC address and actual device and which one is spoofed one in the condition where the both victim(exploited)device and attacker device need not to be simultaneously connected

Here this experiment is performed with various machines and it is resulted that our proposed technique is mostly identify the device correctly. Our technique provide stronger and correctly identification of device because it uses three phase identification, first is on basis of probe request, second is on basis of authentication phase and third is on basis of association phase.

VI. Future scope

After more than one decade of research on spoof detection and prevention by all the researchers throughout the world, none of the proposed technique is able to stop MAC spoofing attacks (Identity based attacks) when NIC card of both the attacker and victim have same developer. Both NIC card at mostly times produce same properties, so to differentiate between them is a typical task. Also today there is a concept called Hardware Abstraction Layer is used in some NIC card which allows program developers to write software independently for any device, which provide high performance. This proposed work is also not able to correctly identify the device when developer of that NIC card is same. So in the future work main work to develop technique which is used to identify devices of same developer means devices which have same properties and also identify device which have HAL (Hardware abstraction layer) concept used in development of that device.

REFERENCES

[1] Brik, Vladimir, et al. "Wireless device identification with radiometric signatures." *Proceedings of the 14th ACM international conference on Mobile computing and networking*. ACM, 2008.

[2] Pandey, Alok, and Jatinderkumar R. Saini. "Counter Measures to Combat Misuses of MAC Address Spoofing Techniques." *International Journal of Advanced Networking & Applications* 3.5 (2012).

[3] Srinivasan, T., Vivek Vijaykumar, and R. Chandrasekar. "A Self-organized Agent-based architecture for Power-aware Intrusion Detection in wireless ad-hoc networks." *Computing & Informatics, 2006. ICOCI'06. International Conference on*. IEEE, 2006.

[4] http://www.wifiplanet.com/tutorials/article.php/1447501/Understanding-80211-Frame-Types.htm

[5] Abad, Cristina L., and Rafael I. Bonilla. "An analysis on the schemes for detecting and preventing ARP cache poisoning attacks." *Distributed Computing Systems Workshops, 2007. ICDCSW'07. 27th International Conference on*. IEEE, 2007.

[6] Sheng, Yong, et al. "Detecting 802.11 MAC layer spoofing using received signal strength." *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. IEEE, 2008.