A Defensive Fingerprinting Approach to 802.11 MAC Layer Attacks

[1]May Aye Chan Aung, [2]Khin Phyo Thant
[1]*Network Security Lab, University of Computer Studies, Mandalay*
[2]*Department of Information Technology and System Maintenance*
University of Computer Studies, Mandalay
mayayechanaung@gmail.com, khinphyothantucsy@gmail.com

***Abstract* – Today, 802.11 networks are becoming more popular among the millions of Laptop users community due to the mobility and ease of use. However, 802.11 networks attracts the lower layers of the open system interconnection (OSI) protocol stack to render the network unusable because of trusted and untrusted traditional boundaries. MAC layer attacks in 802.11 network are known as one of the weakest points of wireless networks because of unprotected management frames. According to these motivation, a defensive approach using MAC layer fingerprinting is proposed based on Probe request, Authentication, Association, Deauthentication, and Disassociation frames. A fingerprint is based on the behavior of a station (STA). Each STA's behavior varies due to implementation of differences 802.11 protocol. The aim is to design and implement a wireless network security system to detect MAC layer attacks using passive fingerprinting. Experiments are implemented with different STAs with a real time set-up using Kali linux environment.**

I. Introduction

Due to the nature of open and volatile border 802.11 network, an attacker has the ability to listen all network traffics which are becoming potential intrusion. An attacker can intrude various attacks based on the vulnerability of management frames, control or data frames. Typically, intrusion detection system (IDS) operates at the network layer or above to detect attacks. Identity attacks, denial of service (DoS) attacks, rouge access points attacks, session hijacking attacks and ARP poisoning attacks are caused after exploiting the vulnerabilities of MAC layer.

A wireless network is a type of computer network connecting devices without any kind of wiring or cables. Two most common types of wireless networks are mobile telecommunication (cellular phones) and wireless local area networks (WLANs). WLANs are based on the 802.11 standard and are referred to as Wireless Fidelity (Wi-Fi) networks or hot-spots. This is a type of network that will be considered in this paper.

There are two operating modes defined in 802.11 networks are ad-hoc mode and infrastructure mode. Most 802.11 networks operate in infrastructure mode and use an access point (AP) opposed to ad-hoc mode to manage all wireless communication. This type of network is set up for proposed fingerprinting approach. Data at the IEEE 802.11 Medium Access Control (MAC) layer is transmitted in the form of frames namely, management, data and control frames. Three different types of frames in 802.11 standard are management, control and data frames. All information and signaling between Stations (STAs) and Access Points (APs) in 802.11 networks are sent by using one or more of these frames types. This paper only considers on the subtypes of management frames.

The main contribution of this paper is the design, implementation and evaluation of a defensive wireless fingerprinting approach to detect MAC layer attacks. This proposed approach is developed to fingerprint the behavior of STAs using MAC layer properties.

The remaining of the paper is organized as follows: A summary of literature review is provided in next section. IEEE 802.11 network is briefly presented in section 3. Section 4 describes the implementation of fingerprinting approach. Implementation and analysis is shown

in section 5. The final conclusion and future work is drawn in section 6.

II. Literature Review

Recently, several vulnerabilities have been discovered in different implementations of fingerprinting 802.11 MAC layer for both offensive and defensive uses. To overcome these vulnerabilities, some researchers have proposed the detection techniques based on MAC sequence numbers and other logical properties of 802.11 MAC layer. However, most of today's WLAN infrastructure systems do not support the protection of management frames protection.

R. Gill et al. [12] addressed two detection techniques based on monitoring received signal strength (RSS) and monitoring round trip time (RTT) to detect MAC spoofing attacks. The accuracy of these techniques was published a year later [13].

Franklin et al. developed a fingerprinting technique based on statistical analysis of the inter-frame timing of transmitted probe request frames [7]. They showed good results with the inter-frame timing method and concluded that the majority of wireless drivers do have a distinct fingerprint.

C. Idland, T. Jelle, and S. F. Mjølsnes proposed the fingerprinting algorithm (FPA) with eight different tests to detect MAC layer spoofing attacks. Comparing with other commercial intrusion detection system (IDSs), proposed FPA is able to detect spoofing attacks where the attacker and victim are not connected simultaneously [4].

III. IEEE 802.11 Network

IEEE 802.11 standard defines a set of protocol requirements for lower two layers of the Open System Interconnection (OSI) model that specifies the behavior of link layer communication between stations. OSI model is a network model that consists of seven layers. There are two portions: host and media. The host portion includes Application, Presentation, Session and Transport layers. The media portion includes Network, Data Link and Physical layers. The relationship of 802.11 network and OSI model is shown in figure 1.

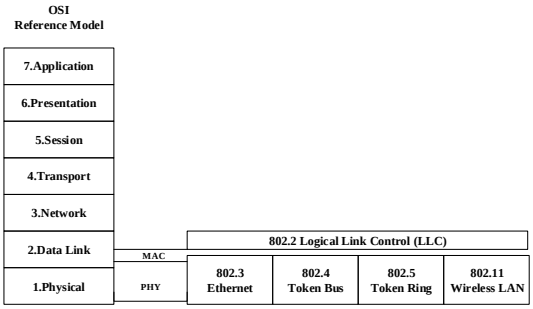

Figure 1. 802.11 Network and OSI Model

In this paper, MAC sub-layer and its frame types are described and focused on research work. MAC sub-layer is the lower link layer (layer 2) in the OSI seven-layer model [14]. It acts as an interface between Logical Link Control (LLC) sub-layer and the network's physical layer. It is responsible for moving data packets to and from one Network Interface Card (NIC) to another across a shared channel. A MAC address is a unique identifier assigned for network interfaces. A 48 bit (12 hexadecimal numbers) creates unique layer 2 address. MAC addresses are used for numerous network technologies and most IEEE 802.11 network technologies including Ethernet. MAC addresses are also referred to as Ethernet Hardware Addresses (EHA), Physical addresses, Layer 2 addresses, or Hardware addresses.

1. Management Frames

Data at the MAC layer is transmitted in the form of frames. WiFi network have a series of MAC frame types described in IEEE 802.11 standard. IEEE 802.11 Medium Access Control (MAC) layer communicates through the three types of messages namely, management, data

and control frames. This paper only focuses on the subtypes of management frames.

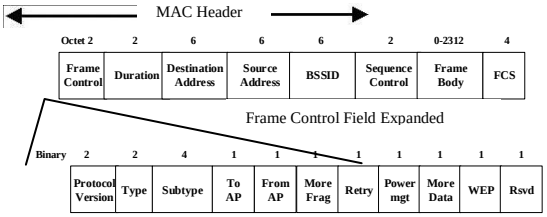

Figure 2. 802.11 Management Frame

IEEE 802.11 management frames are responsible for maintaining communication between Access Point (AP) and wireless clients. The main purpose and use of management frames are to establish and maintain the wireless network to allow wireless clients and AP. 802.11 management frames have a 24 bytes standard header [14]. They contain Frame control, Duration, Destination address (DA). Source address (SA), BSSID, Sequence control and Frame Check Sequence (FCS).

List of all 12 management frame subtypes identified by 802.11 standard are Association Request, Association Response, Reassociation Request, Reassociation Response, Probe request, Probe Response, Beacon, Announcement Traffic Indication Message (ATIM), Disassociation, Authentication, Deauthenication and Action [9, 10]. This paper focuses on the subtypes of management frames: Probe request, Probe response, Association request, Authentication request, Deauthentication and Disassociation. This subtypes allow clients to establish, join, leave and maintain the Wi-Fi networks.

2. MAC Layer DoS Attacks

DoS attacks on wireless networks attempt to halt access to shared network resources. Three types of MAC layer DoS attacks are masquerading, resource flooding and media access DoS attacks as shown in figure 3.

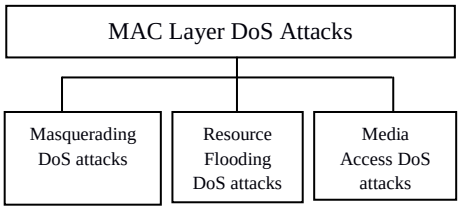

Figure 3. Classification of MAC Layer DoS Attacks

The Masquerading attack refers to an attack in which an adversary targets a specific client by spoofing its MAC address or the address of its current access point [2]. The Resource Depletion attack refers to an attack in which an adversary generates high rates of requests with random MAC addresses in order to consume shared resources. Finally Media Access attacks refer to attacks against the Distributed Coordinated Function (DCF) of 802.11 networks. These attacks are also called Jamming attacks.

The MAC layer DoS attacks are possible due to the unencrypted transmission of management frames that carries MAC address of the source. With the help of available tools, the attackers simply make MAC layer DoS attacks either on the client or AP. MAC layer DoS attacks are perpetrated by spoofing messages exchanged between a client and Access Point (AP). The attackers spoof the MAC address of AP or the client. The recipient of these spoofed frames processes them unknowingly whether they are legitimate or illegitimate requests.

IV. Fingerprinting Approach

Fingerprinting is the process of collecting information from the specific workstation to ensure the authenticity of corresponding station and is used to obtain detailed information on a specific target [4]. It makes profiles to identify this workstation by comparing its profile to current nature of workstation. Fingerprinting can be done actively or passively.

A sniffer use passive fingerprinting to capture traffic sent from a system. It traces the captured traffics coming from a connecting host going to local network. This cannot be done by the intruder away. Passive OS Fingerprinting (p0f) is a tool that uses a variety of complex, purely passive traffic fingerprinting mechanisms.

Active fingerprinting scans for live hosts, operating system (OS), packets filtering and

open ports on remote hosts. Network mapper (nmap) sends network packets to the target machine and determines the OS of target machine. It is an effective application for both admins and attackers. In this proposed framework, both active and passive fingerprinting methods will be used.

In this proposed work, a profile is passively created based on monitoring the workstation's behaviors of different 802.11 management frames. The whole proposed approach has four different phases in figure 4. Phase 1 and 2 are performed in this paper.

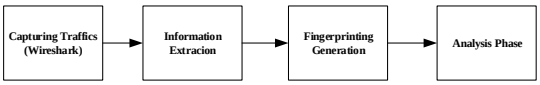

Figure 4. Overview of Fingerprinting Approach

There are many different sources for fingerprinting. Some popular and relevant sources of fingerprinting in 802.11 networks are users, web browser, TCP/IP stack, MAC layer. In this paper, MAC layer properties is chosen for the source of fingerprinting.

1. Phase 1: Capturing Traffics

In capturing traffics phase, management frames emitted from wireless clients are passively collected. Probe requests frames, authentication request frames, and association request frames and other management frames are captured.

Firstly, network interface card (NIC) card is put into monitor mode by using airmon-ng tool. Commands which are used on kali linux terminal for changing managed mode to monitor mode is given below:

- ifconfig - used to find out the interface used by wireless card
- iwconfig - find out the card working mode
- airmon-ng start wlan0 - create an interface whose working is in monitor mode

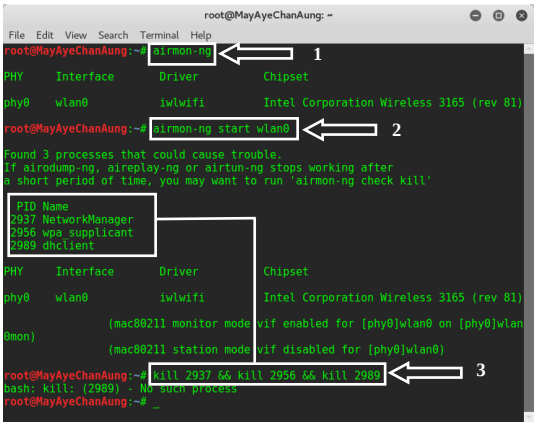

Figure 5. Setting Monitoring Mode

After setting up monitor mode, the task of collecting frames are performed by using wireshark tool. That pcap file is converted into comma separated value (csv) file using tshark in terminal mode of wireshark.

2. Phase 2: Information Extraction

A management frame on 802.11 network consists of several fields. The following properties extracted details information of management frames from figure 7 for this proposed work are given in table 1.

After packets have been captured in pcap files, filtering process is performed using wireshark filtering commands. The filter used to apply and find only probe request packets is "wlan.fc.type_subtype == 0x04" shown in figure 6.

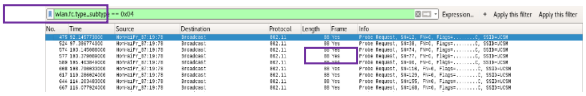

Figure 6. Probe Request Frame

Table1. Selected Property of Management Frames

Property	Description
Arrival time	Arrival time of value

Epoch time	Time relative to epoch
Time delta from previous frame	Time difference between two consecutive frame
Time from first frame	Relative time from first frame
Timestamp	Time synchronization
Type/Subtype	Different type and subtype of management frames
DA	Destination address of the packet
SA	Sender address of the packet
BSSID	Ethernet address of the access point
Fragment Number	From the sequence control field
Sequence number	Sequence number filed mod 4096 in each frame

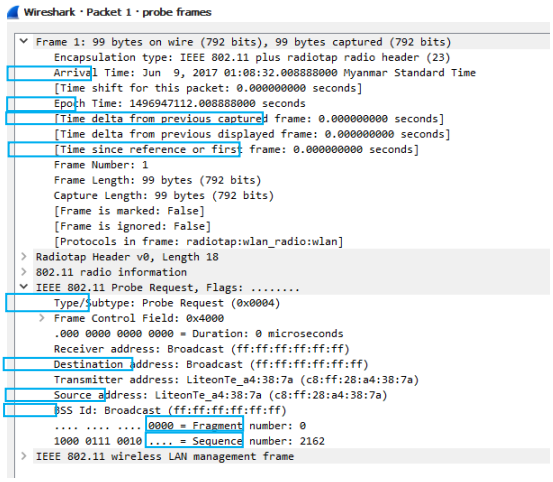

Figure 7. Details Information of a probe request Frame

IV. Implementation and Analysis

This section describes the testbed setup for a wireless network security system and the analysis of management frames.

1. Testbed Setup

The testbed consists of one AP, one victim STA, one attacker STA and one monitor mode. The monitor mode is co-located with the AP to receive all frames that are sending and receiving from AP. The monitor mode runs on Debian based kali linux using wireshark for monitoring the wireless traffics of AP.

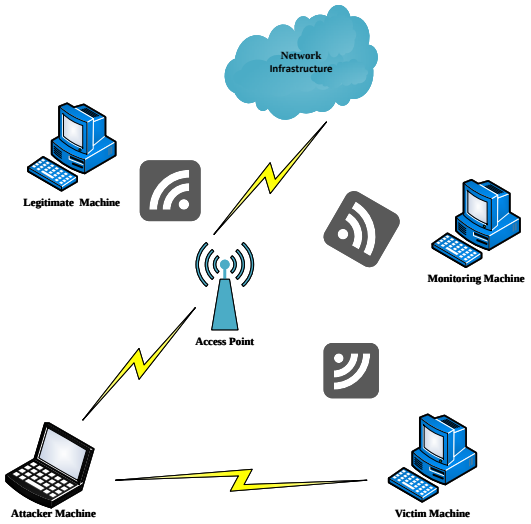

Figure 8. Testbed Setup

2. Frame Analysis

Figure 9 and 10 are plots of time delta between arriving probe request frames transmitted by two wireless drivers.

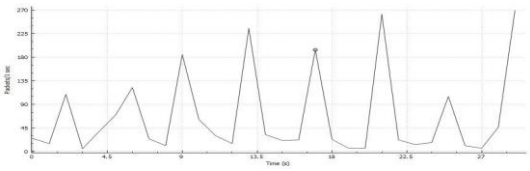

Figure 9. Probe Request Frames Transmitted RTL8111/8168/8411 PCI Wireless Driver

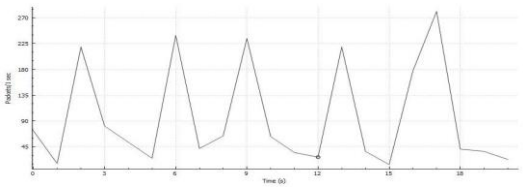

Figure 10 . Probe Request Frames Transmitted Intel Corporation Wireless 3165 Driver

IV. Conclusion and Future Work

Wireless communication networks have become an inevitable medium for communication. MAC layer DoS attacks are

caused due to the open nature of unprotected management frames. These management frames carry the source MAC address and are susceptible to wireless MAC layer attacks. According to this issues, an approach that can detect and mitigate According to this issues, a defensive approach using MAC layer fingerprinting has been proposed based on Probe request, Authentication, Association, Deauthentication, and Disassociation frames. In the whole process with four phases, two phases have been performed in this paper. In future, the remaining phases will be processed and analyzed. Proposed approach will be tested with different wireless stations in their default configurations.

References

[1] Arockiam. L and Vani.B , "A Survey of Denial of Service Attacks and it's Countermeasures on Wireless Network", International Journal on Computer Science and Engineering (IJCSE), Vol. 02, No. 05, 1563-1571, 2010.

[2] B. Kemal and T. Bulent, "Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks," *Comput. Stand. Interfaces*, vol. 31(5), pp. 931-941.

[3] Baber Aslam, M Hasan Islam and Shoab A. Khan, "Pseudo Randomized Sequence Number Based Solution to 802.11 Disassociation Denial of Service Attack", *IEEE Xplore*, 2008.

[4] C. Idland, T. Jelle, and S. F. Mjølsnes, "Detection of Masqueraded Wireless Access Using 802.11 MAC Layer Fingerprints," Digital Forensis and Cyber Crime, pp.283-301, Springer, 2013.

[5] Chibiao Liu and James Yu, "A Solution to WLAN Authentication and Association DoS Attacks", *IAENG International Journal of Computer Science*, August 2007.

[6] Chibiao Liu and James Yu, "Rogue Access Point Based DoS Attacks against 802.11 WLANs", The Fourth Advanced International Conference on Telecommunications, IEEE Xplore, 2008, pp-271-276.

[7] Jason Franklin, Damon McCoy, Parisa Tabriz, Vicentiu Neagoe, Jamie Van Randwyk, and Douglas Sicker, "Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting," Proceedings of the 15th Conference on USENIX Security Symposium-Volume 15, 2006.

[8] L. Arockiam and B. Vani, "Security algorithms to prevent Denial of Service (DoS) attacks in WLAN" *International Journal of Wireless Communications and Networking Technologies*, Volume 2, No.1, January 2013.

[9] M.A.C. Aung, "*Proposed Framework for Link Layer Attack Detection System in Wireless Network*", 15th International Conference on Computer Applications (ICCA), Yangon, Myanmar, 16th -17th February, pp. 169-175, 2017.

[10] M.A.C. Aung, "*Detection and Mitigation of Wireless Link Layer Attacks*", 15th IEEE/ACIS International Conference on Software Engineering Research, Management and Application (SERA), June 7 – 9, The University of Greenwich, London, UK, pp. 173-178, 2017.

[11] M. Bernaschi, F. Ferreri, and L. Valcamonici, "Access points vulnerabilities to DoS attacks in 802.11 networks," *Wirel. Netw.*, vol. 14(2), pp. 159-169, 2008.

[12] Rupinder Gill, Jason Smith, Mark Looi, and Andrew Clark, "Passive Techniues for Detecting Session Hijacking Attacks in IEEE 802.11 Wireless Networks," Asia Pacific Information Technology Security Conference Refereed R&D Stream (AusCERT), pp.26-38, 2005.

[13] Rupinder Gill, Jason Smith, Mark Looi, and Andrew Clark, "Experiences in Passively Deteting Session Hijacking Attacks in IEEE 802.11 Networks," Procedding of 4th

Australasian Information Security Workshop (Network Security), 2006.

[14] TJ O Connor, "Detecting and Responding to Data Link Layer Attacks", *SANS Institute*, October 13, 2010.

[15] Thuc D Nguyen and Duc H M Nguyen., "A light weight solution for defending against deauthentication /disassociation attacks on 802.11 networks", *17th International Conference on Computer Communications and Networks*, at St Thomas, US Virgin Islands, USA. August 3 -7, 2008.