Wired LAN and Wireless LAN Attack Detection Using Signature Based and Machine Learning Tools

Jaspreet Kaur

Abstract There are various attack which is possible in the network, it may be from externally or internally. But internal attacks are more dangerous than external. So, my mainly concern upon Wireless LAN and Wired LAN attacks which occurs internally. There are various Signature based tools, IDS/IPS (Intrusion detection or prevention system) available now-a-days for detecting these types of attacks but these are not sufficient due to high false alarm rate. So, I detect these types of attacks with three ways: through Wireshark, with signature based tools (Snort and Kismet) and with machine learning tools (WEKA). In wired LAN attack, my mainly concern on PING scan or PING flood, NMAP scan (portsweep) and ARP spoofing attacks. In wireless LAN attacks, I take care of Deauthentication attack, Disassociation attack and Access point (AP) spoofing attack. Signature based tools detect these types of the attacks based on the stored signature and timing threshold. But machine learning tools take several different feature to detect these types of attacks with more accuracy and low false positive rate.

Keywords Wireless LAN · Wired LAN · Snort · WEKA
Kismet · Wireshark · Spoofing attack

1 Introduction

In the today generation attacks are very dangerous whether its happen due to the internal situations or to the external situations. But internal attacks are very difficult to detect and prevent due to the unawareness of these attacks. These attacks are done either from wired environment or from the wireless environment. In the wireless security (WLAN), my mainly concern on the 3 protections of any packet transmitted in the air: confidentiality, integrity, availability. Confidentiality and

J. Kaur (✉)
Department of Information Technology, Indira Gandhi Delhi Technical University for Women, Delhi 110006, India
e-mail: jaspreetkaur9817@gmail.com

G.M. Perez et al. (eds.), *Networking Communication and Data Knowledge Engineering*, Lecture Notes on Data Engineering and Communications Technologies 3, https://doi.org/10.1007/978-981-10-4585-1_2

integrity are mainly managed by various protocols such as: Wired Equivalent Privacy (WEP), WI-FI Protected Access (WPA) etc. But WLAN is still vulnerable from availability attacks such as DOS attacks. My mainly concern on the MAC layer DOS attacks such as Deauthentication attack, Disassociation attack and AP spoofing attack [1]. In the case of PING scan or PING flood, NMAP scan (portsweep) and ARP spoofing attacks which are to be occurred either through wirily or wirelessly are also very dangerous because PING scan and NMAP scan are the first attack which are done by the attacker for checking the vulnerable systems as PING scan tells the attacker system is up and how distant the system is as TTL, NMAP is used to find out the port and operating system vulnerability. In ARP table changes made the information leakage easily captured by the attacker as man in the middle attack. Firstly I used Wireshark for manually analysis of these attacks, then after used the signature based tools such as Snort (open source) widely used for PING scan, NMAP scan and ARP spoofing attack detection and Kismet as IDS for the Deauthentication attack, Disassociation Attack and Access point spoofing attack detection. Finally I used machine learning tool, WEKA with classification techniques such as Naive Bayes and J48 tree for detecting these types of attacks using appropriate parameters.

This paper is continue with Related Work, Proposed Approach, Setup Environment of Lab, Results and Observations and finally completed with Conclusions and Future Work.

2 Related Work

There are various papers on this topic summarized as follows: In this paper authors discussed MAC layer management frame attacks. Management frames are neither authenticated nor encrypted that's why these can be easily spoofed by the attacker and perform DOS attacks. They gave various solutions as signal print scheme, MAC Spoofing Detection. But solutions are not worked well [2]. In the 2nd paper author mainly consider on the detection of probe request frame DOS attack in 802.11 network. They used back propagation algorithm to find spoofed frames. But what if training data is corrupted [3]. Infrastructure networks based on an AP as a central node through which every communication is started, thus an AP can easily become a weak point for the entire network. They described software platform to detection of the WLAN attacks. But they said that it is not a long term solution [4]. They proved that management frames attacks can be executed by any malicious station, without being neither associated nor authenticated to the access point. APs main vulnerability is unacked frame retransmission. According to them the effective solution should reside at the firmware level [5]. Mainly three algorithm are proposed for detecting and preventing mac layer dos attack as Intrusion detector and manager, Letter envelop protocol with traffic pattern filtering, Medium access protocol spoofed detection and prevention. These 3 algorithms are implemented together at the AP providing the reliable solution and WLAN security. But it has

little computational overhead [6]. In this they used IDS/IPS approach. IDS program sniff WI-FI data and did analysis. Based on the throughput of the network and Deauthentication frame in the network or at the particular client side its decide DOS attack has to be performed or not [7].

An another author suggest a tool named as the IJAM tool for performing WLAN attack. The author take some assumption such as: The attacker needs high transmit power etc. [8]. In this survey paper author suggest the various vulnerability occur within the WLAN such as Eaves dropping, Message modification, management frame attacks. Then discussed various available solution such as: Pseudo random number based authentication, Letter Envelop Protocol etc. But still DOS attack is possible [9]. In this I studied out various types of layer 2 attacks detection and their countermeasures. They mainly focused on the ARP spoofing and mac attacks and tell that Dynamic ARP inspection prevents current ARP attacks [10]. With the extension of ARP attacks they also consider Deauth attack and rouge Access point attack using some parameters [11]. In this paper they propose a layered architecture called as WISA guard. They uses the OS Fingerprinting, AP Fingerprinting, RSS Fingerprinting technique for attack detection [12]. In next paper, they uses a IDPS method in which Snort uses as IDS and for the prevention technique uses Aireplay-ng tool as sending the deauth packets to the attacker. For attacking purpose they uses the ICMP flood attack [13]. In one paper, they use the machine learning tool called as WEKA which includes the variety of data mining algorithms. But they mainly used the J48 tree and Naive Bayes algorithm for detection of ping sweeps and port sweeps attack [14].

3 Proposed Approach

My mainly concern on the detection of Wired LAN and Wireless LAN attacks using three approaches such as:

1. Manually through Wireshark tool.
2. With the help of signature based tool such as Snort and Kismet.
3. With the help of machine learning based tool such as WEKA using different algorithms. The proposed approach is shown at Fig. 1.

In Fig. 1 myself represent these 3 proposed approaches as (1), (2), (3). In the Wireshark I take the packet dump and manually inspect the various features. In signature based tools like Snort and Kismet, my mainly focus on the signature of the attacks and threshold limit of time such as 5 packets/min for Deauth or Disas packets in the alert rule option. In the machine learning tool WEKA, my mainly concern on the 2 algorithms of classification such as Naive Bayes and J48 tree for attacks detection. Here I take the various parameters for detection of these kinds of attacks as discussed later in this paper.

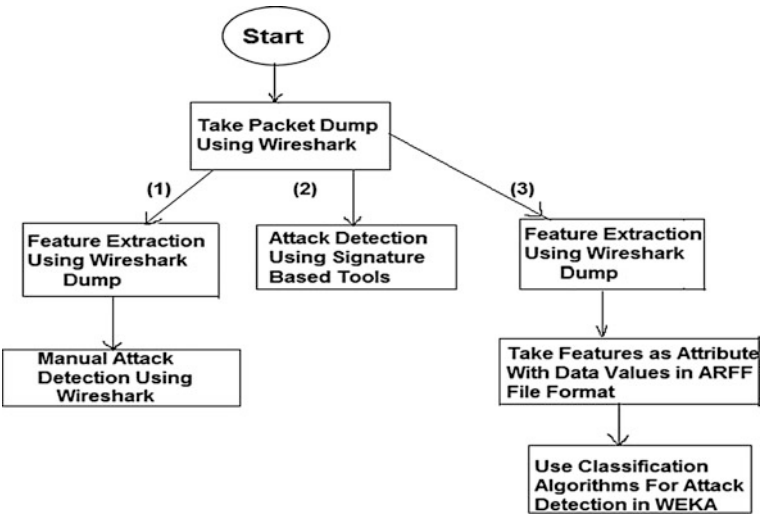

Fig. 1 Proposed approach

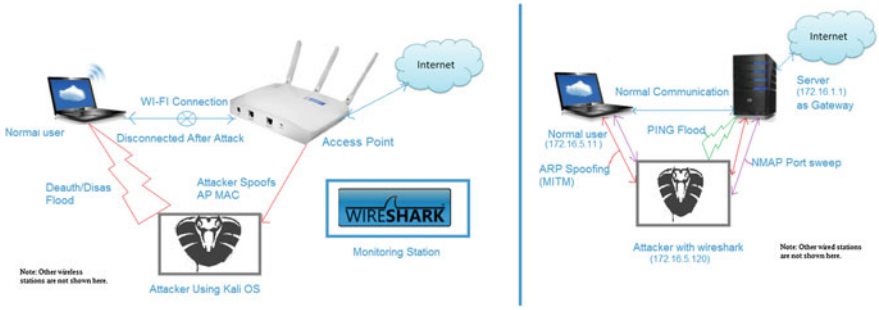

Fig. 2 Wireless LAN and wired LAN setup

4 Setup Environment of Lab

Two setups one for Wired LAN and another for Wireless LAN are mainly used for performing the attacks and analysis of packets. In each setup I capture Wireshark packet dump of 30,000 packets. These packets are firstly manually observed, secondly give in signature based tools and finally apply cross validation approach with various classification algorithms in WEKA tool. The setup is shown Fig. 2.

In the wireless LAN setup there are various clients and APs (access points) communicate to each other through WI-FI. Then attacker comes which spoofs the mac of an particular ap and tried to attempt Deauth or Disassociation flood attack to the particular client or all the clients using Kali OS and I analyze the network traffic

using Wireshark in monitor mode, take the packet capture dump for attack detection with 3 proposed approaches. As per the similar way, in Wired LAN setup various clients and server are communicating normally. Then attacker comes, performs the ping flood attack to the server, NMAP (port sweep attack for TCP port 80) and ARP spoofing attack as man in the middle attack. After that monitor all the traffic using Wireshark and take the packet capture dump for attack detection using 3 proposed approaches.

5 Results and Observations

After the following attacks are taking place, detection of these attacks are to be done with the following three ways such as:

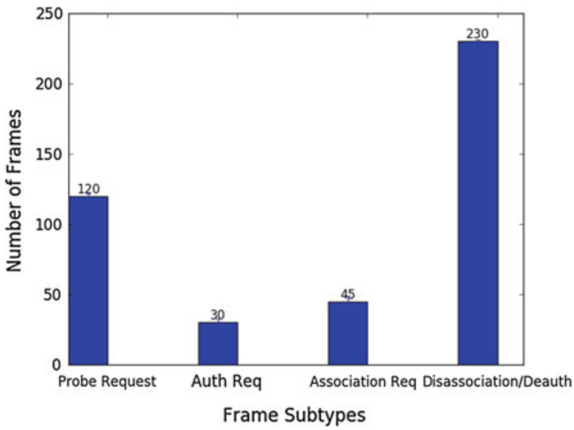

Fig. 3 Packet ratios in the network during wireless LAN attack

Fig. 4 Wireless LAN attack detection using Kismet

5.1 Manually Through Wireshark

When Deauth, Disas attack are taking place along with AP spoofing. Then I observe the packet capture dump using Wireshark. There is various management frames are seen as probe request, authentication, association frame and Deauthentication or disassociation frames. But the Deauth or Disas frames are exponentially increased irrespective of other frames within 2 min in the network. It is due to the attack as shown in Fig. 3.

For the ping flood attack I observe the Echo (ping) request, Echo (ping) reply information with the ICMP packet header identification number. For NMAP port sweep myself see the particular source address with a port number sending various syn packet to range of an IP address for checking port number 80 and get a response for the open ports. For ARP spoofing (mitm) attack I observe the ICMP redirect error, the mac address of the attacker and mac address of the gateway. Both the MAC address of the attacker and gateway is same after ARP spoofing attack. As the result all the information sending to the gateway by the client also captured by the attacker.

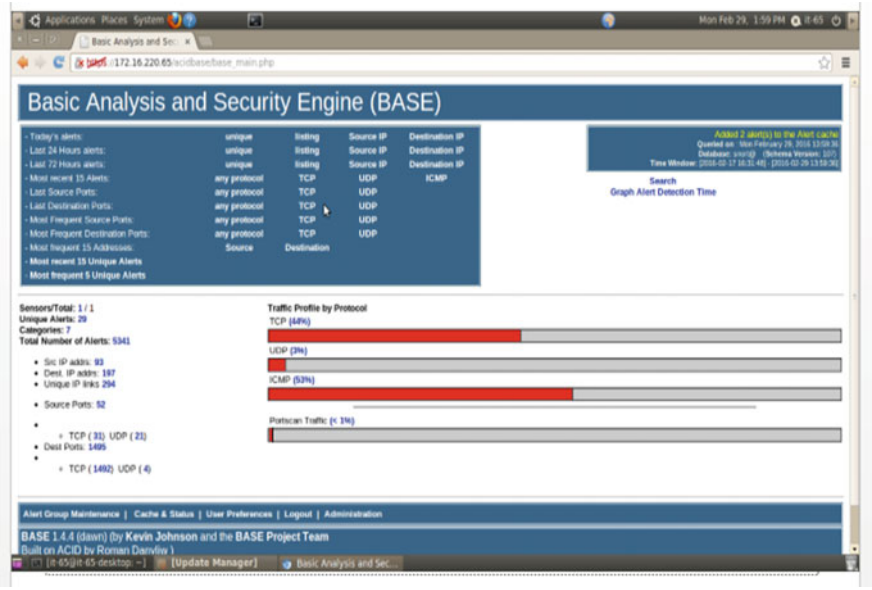

Fig. 5 Wired LAN attack detection using snort

5.2 Using Signature Based Tool

For Wireless LAN attack I used the tool named as Kismet. Kismet has various alert rules for detecting the DOS and AP spoofing attack. This tool detects these types of attacks based on the various signatures of these attacks and the threshold value of time such as 5 packets/min for Disassociation attack. The results are shown in Fig. 4.

For Wired LAN attack I used the tool named as Snort implemented as ACID-BASE. For PING scan this tool gives us alert as ICMP PING *NIX, ICMP PING, ICMP Echo Reply. For NMAP scan this gives alert as PORT SWEEP and finally for ARP spoofing, have the ICMP redirect host alert. In the Fig. 5 we represent the ICMP, UDP, TCP, PortScan alert.

5.3 Using Machine Learning Tool

In machine learning tool WEKA, my mainly focus on the two algorithms of classification as Naive Bayes and J48 tree for these types of attack detection. The parameters based on which myself defined attack is occurred or not is already given in their respective tables. These parameters are taken collectively for detecting the attacks. The Wireshark packet dump is given as a csv file in the input of the WEKA tool.

In the below WEKA table I compare the location of rouge AP and true AP, also see the secure attribute option which is false it means rouge AP does not use WPA2 protocol for packets, channel at which the original AP is worked is different from rouge AP channel and also see the various parameters differ from the original one. So, WEKA predict these packets as a yes, no for attack detection (Table 1).

Table 1 Wireless LAN attack detection using tool WEKA

Parameters considered	Predicted attack as yes	Predicted attack as no
Source MAC address	Netgear_61:ad:da	Netgear_61:ad:da
Destination MAC address	Xiaomi_7f:04:4f	Xiaomi_7f:04:4f
Range of sequence no.	0–0	712–718
Latitude of AP	28.663615	28.663405
Longitude of AP	77.233468	77.233700
Frame length	34	56
Secure	False	True
Signal strength	90	80
Channel no.	11	6
Reason code	Unspecified reason	MICFLeaving
Frame control flags	0x00	0x08
Other information	DeauthDiasas	DeauthDiasas

Table 2 PING scan attack detection using tool WEKA

Parameters considered	Predicted attack as yes	Predicted attack as no
Source IP address	172.16.5.120	172.16.1.1
Destination IP address	172.16.1.1	172.16.5.11
Frame length	74	74
Identification number for ICMP	0x0100	0x0100
Time to live	64 (for Linux)	128 (for Windows)
Packet count	10	2
Other information	PING reqreply	PING reqreply

Table 3 NMAP scan (portsweep) attack detection using tool WEKA

Parameters considered	Predicted attack as yes	Predicted attack as no
Source IP address	172.16.5.120	172.16.1.1
Destination IP address	172.16.1.1-15	172.16.5.11-25
Frame length	58	66
Source port	3128	33422
Destination port	80	80
Window size	1024	8192
Other information	SYN	SYN

In the PING scan or PING flood and NMAP portsweep attack, if administrator (172.16.1.1) scans the network for testing the IP addresses or testing the specific services is working or not, then its not an attack otherwise for rest of the users which want to perform such an action these parameters detected them as an attack. Admin (Linux sever) always send 2 PING request but attacker send any no. of ping request for performing ping flood. My server is on Linux. So, I mainly look TTL for Linux to more security purpose. For Portsweep admin always use fixed size of window and particular source port no. to scanning the services. As shown in Tables 2 and 3.

In the Table 4 I show the ARP spoofing as source address is attacker address and destination address is gateway, both having the same mac address and ICMP redirect error. So, the parameters predicted these as an attack. On the other hand both source and destination having different mac address, protocol uses as TCP rather than ICMP or UDP and working as normal user, gateway. So, its not an attack.

As everyone see that from the below graph accuracy I have met is quite sufficient with taking the parameters of mine in the machine learning tool WEKA using any of the classification algorithms Naive Bayes or J48 tree (Fig. 6).

Table 4 ARP spoofing attack detection using tool WEKA

Parameters considered	Predicted attack as yes	PREDICTED ATTACK AS NO
Source IP address	172.16.5.120	172.16.5.120
Destination IP address	172.16.1.1	172.16.1.1
MAC address of source	00:26:b9:22:4b:8a	00:26:b9:22:4b:8a
MAC address of destination	00:26:b9:22:4b:8a	a0:48:1c:a5:b1:9e
Protocol	ICMP, UDP	TCP
Other information	Redirect (ICMP error)	Normal data

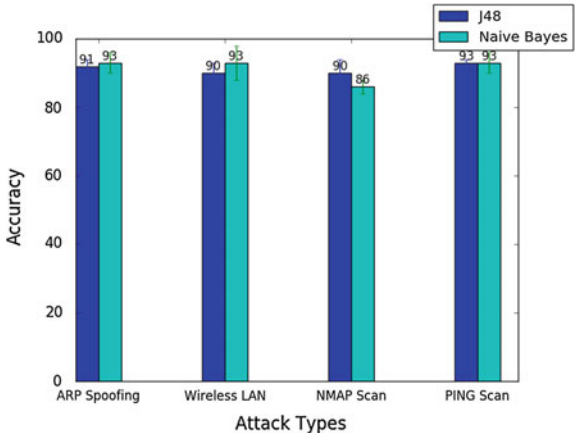

Fig. 6 Accuracy comparison of attacks using Naive Bayes and J48 tree

6 Conclusion and Future Work

As I see that there are various wireless LAN attack and wired LAN attack which are very dangerous for any network environment. So, myself need to detect these types of attacks. My mainly concern on the 3 ways for detecting these kinds of attacks. First one is the manually inspection of packets for these kinds of attacks, then use the signature based and machine learning tool for detection of these. As I see the signature based tools detect these kinds of attacks with less accuracy. So, I need some more parameters as mention in machine learning tool for high accuracy rate. As you see machine learning tool WEKA give me very high satisfactory results using my parameters. For the future work, I combine the signature based parameters and machine learning parameters for very high accuracy results along with more parameters. My mainly next step is concentrate on the prevention strategy of these kinds of attacks.

References

1. Mitchell, Changhua He John C.: Security Analysis and Improvements for IEEE 802.11 i, In: 12th annual network and distributed system security symposium, NDSS05 (2005).
2. Farooq, Taimur, David Llewellyn-Jones, and Madjid M.: MAC Layer DoS Attacks in IEEE 802.11 Networks, In: The 11th Annual Conference on the Convergence of Telecommunications, Networking and Broadcasting, PGNet, Liverpool, UK, (2010).
3. Ratnayake, Deepthi N., et al.: An intelligent approach to detect probe request attacks in IEEE 802.11 networks, In: Engineering Applications of Neural Networks, Springer Berlin Heidelberg, pp. 372–381, (2011).
4. Bellardo, John, and Stefan S.: 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions, USENIX security, (2003).
5. Bernaschi, Massimo, Francesco Ferreri, and Leonardo V.: Access points vulnerabilities to DoS attacks in 802.11 networks, Wireless Networks14.2, pp. 159–169, (2008).
6. B. Vani, L.: Framework to Detect and Prevent Medium Access Control Layer Denial of Service Attacks in WLAN, International Journal of Computer Networks and Wireless Communications, ISSN: 2250-3501 Vol .3, No 2, April (2013).
7. Agarwal, Mohini, Santosh Biswas, and Sukumar N.: Detection of Deauthentication Denial of Service attack in 802.11 networks, India Conference, INDICON, IEEE, (2013).
8. Noman, Haitham Ameen, Shahidan M. Abdullah, and Haydar Imad M.: An Automated Approach to Detect Deauthentication and Disassociation Dos Attacks on Wireless 802.11 Networks, In: International Journal of Computer Science Issues, IJCSI 12.4 pp. 107 (2015).
9. Arockiam, L., and B. Vani: A Survey of Denial of Service Attacks and its Counter measures on Wireless Network, International Journal on Computer Science and Engineering Vol. 02, No. 05, pp. 1563–1571 (2011).
10. Yusuf B.: LAYER 2 ATTACKS & MITIGATION TECHNIQUES. http://www.sanog.org/resources/sanog7/yusuf-L2-attack-mitigation.pdf (2005).
11. OConnor, T. J.: Detecting and responding to data link layer attacks, SANS Institute InfoSec Reading Room, Oct 13 (2010).
12. Tao, Kai, Jing Li, and Srinivas S.: Wise guard-MAC address spoofing detection system for wireless LANs, Second International Conference on Security and Cryptography, Barcelona, Spain, pp. 140–147 (2007).
13. Korck, Michal, Jaroslav Lmer, and Frantisek J.: Intrusion Prevention/Intrusion Detection System (IPS/IDS) For Wifi Networks, International Journal of Computer Networks and Communications 6.4, pp. 77, (2014).
14. Nevlud, Pavel, et al.: Anomaly-based Network Intrusion Detection Methods, Advances in Electrical and Electronic Engineering 11.6, pp. 468, (2013).

http://www.springer.com/978-981-10-4584-4

Networking Communication and Data Knowledge Engineering
Volume 1
Perez, G.M.; Mishra, K.K.; Tiwari, S.; Trivedi, M.C. (Eds.)
2018, XX, 312 p. 145 illus., Softcover
ISBN: 978-981-10-4584-4