2021 IEEE International Symposium on Smart Electronic Systems (iSES) | 978-1-7281-8753-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/iSES52644.2021.00098

Experimental Assessment of Wireless LANs against Rogue Access Points

Narahari Komanduri and Sriram Sankaran
Center for Cybersecurity Systems and Networks
Amrita Vishwa Vidyapeetham
Amritapuri, India
Email: srirams@am.amrita.edu

***Abstract*—Access Points (AP) are traditionally used to provide cost-effective, high speed Wi-Fi connectivity to homes, organizations and communities. Despite Wi-Fi providing numerous benefits such as flexibility, scalability and ease of deployment, it is susceptible to numerous vulnerabilities due to the presence of rogue access points (Rogue AP). In particular, intruders can eavesdrop, exploit, launch remote backdoors and manipulate legitimate clients and APs through Rogue APs thus leading to data breaches or possible network compromise. In this work, we build a real-time Wireless LAN testbed using commodity Wi-Fi devices such as Wi-Fi Pineapple Nano that acts as a rogue AP. Further, we perform different attacks on 802.11 Association process between clients and access points through the rogue AP and analyze their impact on the overall performance. Finally, we leverage a sniffer to capture genuine and malicious traffic and develop a mechanism for signature-based detection for mitigating the attacks caused by rogue APs. Evaluation shows that the proposed signature-based approach effectively detects the attacks caused by rogue APs with a detection rate of 91%.**

***Index Terms*—802.11, Wireless Access Point, Rogue Access Point**

I. Introduction

Wireless LANs are increasingly gaining popularity with the latest standards providing significantly higher bandwidth than the previous ones. For instance, 802.11ad standard provides 7Gbps compared to 802.11ac and is backward-compatible. Access Points are at the heart of Wireless LANs providing low-cost connectivity with ease of deployment. Despite the numerous benefits provided by Wireless LANs, security is a paramount concern due to the networked nature of the LANs coupled with the sensitive data stored in them.

One of the notorious threats in Wireless LANs is connecting to rogue APs which indirectly impacts not only the individual clients but also the entire network. In particular, clients are tricked towards connecting to Rogue APs by making the rogue APs look like legitimate ones. This can be used by intruders to eavesdrop, launch remote backdoors and manipulate legitimate clients and APs thus leading to possible network compromise. Thus, there exists a need for understanding the need for examining the threats caused due to rogue APs.

Signature-based detection helps in detecting malicious threats based on the available signatures stored in databases. Signature generally contains the predefined pattern of the attack metric namely malicious network packets or applications. Attributes of signatures depending on the format. Thus, when malicious traffic enters the network, signature-based detection will match and block them with minimal false alarms.

In this work, we build a real-time Wireless LAN testbed using commodity Wi-fi devices such as Wi-Fi Pineapple Nano that acts as a rogue AP. In addition, we launch numerous attacks on the 802.11 Association process between clients and Access Points through rogue APs and analyze their impact on overall performance. Further, a packet sniffer was implemented to capture genuine and malicious network traffic. Finally, we develop a mechanism for signature-based detection using SNORT to detect attacks caused by rogue APs. Evaluation shows that the proposed approach detects the attacks with a detection rate of 91%.

II. Related Work

J. Shawn *et al.* [1] presented a description of Rogue Access Points and the dangers of connecting to them. In addition, authors analyzed the effectiveness of users getting tricked into connecting to Rogue APs. The limitation of their work was that the authors lacked experimentation of attacks caused by rogue AP and their impact on the overall network. Song *et al.* [2] proposed a mechanism for detecting rogue APs from the client side. The limitation is that there may be false-positives on detection process. Also their mechanism works only for 802.11b and 802.11g networks.

Sriram *et al.* [3] proposed a multi-agent based approach to detect twin and unauthorized rogue APs that leverages master and slave agents. Master agents store the data containing a list of authorized APs and is verified with the AP information recorded by slaves. The limitation is that it depends on the MAC address of the AP which can be easily spoofed. Vanjale S *et al.* [4] developed profiles consisting of SSID, MAC, and RSSI parameters for every AP, to detect Rogue APs. Initially, it looks for SSID and verifies duplicates and replica followed by MAC address. Upon successful match, it classifies as genuine AP. Else, it verifies the MAC address and classifies as genuine AP. The limitation is that it does not detect Evil Twin attacks.

Epidemiological models were developed by [6] to model the impact of flaws in Wi-Fi networks. In addition, numerous mechanisms for detection of rogue APs [8] [5] were developed. Anjum *et al.* [7] developed a signature-based intrusion detection system for ad hoc networks. Prakash *et al.* [9] developed a statistical approach for attack detection based on

978-1-7281-8753-2/21/$31.00 ©2021 IEEE
DOI 10.1109/iSES52644.2021.00098

Fig. 1. Lab Environment Setup

Smartphone utilization patterns. Santhosh *et al.* [10] defended against Sybil attacks in Vehicular Platoons using a verification based approach. Padmashani et al. [11] developed an intrusion detection system using SNORT.

In contrast to the existing approaches, we build a real-time Wi-Fi testbed and model attacks on 802.11 association process between client and access point. Further, a sniffer is used to capture traces of normal and attack behavior. Finally, a mechanism for signature-based detection is developed to detect and mitigate attacks using SNORT.

III. Experimental Setup

Figure 1 contains a pictorial description of the experimental set-up for analyzing the impact of the attacks caused by rogue AP. In our proposed approach, we build a real-time Wi-Fi testbed using commodity Wi-Fi devices. Further, numerous attacks caused due to Rogue AP are performed on devices to generate real-time traffic scenarios. Our testbed is composed of the following devices.

- TP Link Access Point
- WiFi-Pineapple Nano external adapter
- TL-WN722N external adapter
- Kali Linux Attacker Machine
- Windows Client Machine
- Ubuntu Client Machine
- Android Client Device

IV. Methodology

Figure 2 refers to the methodology of our proposed work which starts with modeling the attacks on the 802.11 association process. After modeling the appropriate attack strategies and methods to be performed, we launch the attacks on the WLAN. Meanwhile we run the sniffer on the client device to capture the patterns of attacks to construct signatures. Finally, all the signatures will be pushed into the snort database.

Now, when the attacker tries to launch the attacks, we run signature-based detection where network traffic packets are inspected by snort. In particular, the packet will be inspected by comparing the incoming packet with the list of predefined

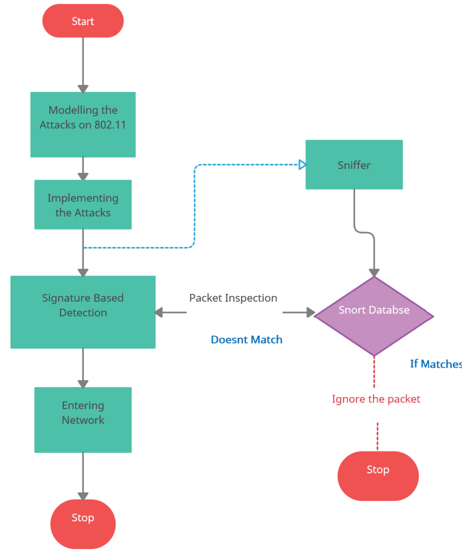

Fig. 2. Flowchart Representation of Methodology

signatures available on snort database. On a successful match, it is considered as malicious and ignored.

A. Modelling the attacks on 802.11

In this section, we have modeled our attacks on 802.11 as shown in Figure 3. From the figure, we have categorized the association process between client and access point into three stages and describe the attacks in each of the stages.

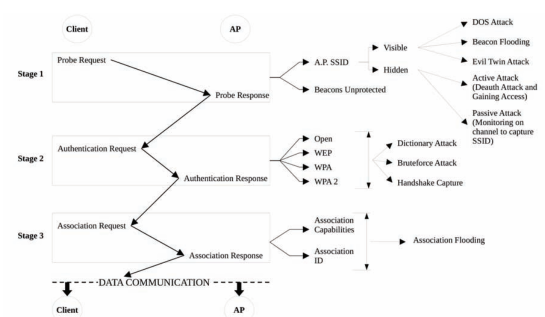

Fig. 3. Modelling Attacks on 802.11 Association

1) Stage-1: This is known as the probing phase before connection establishment between client and AP. In this phase, AP announces its presence in the vicinity by broadcasting the beacons that contains parameters such as SSID, MAC Address, Channel, Timestamp, Capability Information. AP can be configured to be either Visible or Hidden and it depends on broadcasting the SSID. If AP broadcasts, then it becomes visible. In this stage, beacons are unprotected which means that it can be captured and analyzed. Thus, we modeled the possible attacks which can be performed depending on whether AP is visible or hidden. The attacks that are performed in this phase are: beacon flooding, DOS attack, Evil Twin Attack, de-authentication attack when the AP is visible. In case AP is hidden, we will monitor the channel to pawn the hidden SSID in beacon frames.

2) Stage-2: In this phase, 802.11 authentication standard mechanisms can either be open, WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), or WPA2. Thus, we have modeled the attacks based on the available type of authentication chosen by AP. Attacks performed in this phase are dictionary attacks, brute force and handshake capture attacks for WPA2 authentication.

3) Stage-3: In this phase, management frames running in the background are essential for finding AP, manage QoS, associate/ disassociate with AP. Further, these management frames are un-encrypted. Thus we have modeled disassociation attacks, DOS attacks and Spoofing attacks.

B. Implementation of Attacks

In this paper, we perform attacks on 802.11 HOME/SOHO Networks in 2.4GHz channels. To demonstrate attacker behavior, we use KaliLinux as an attacker machine with TPLink and TL-WN722N external hardware adapters which are used to mount WiFi-Pineapple that acts a Rogue AP.

The attacks that are implemented are beacon flooding, DoS attacks, Evil Twin attack using Rogue AP, handshake capture, bruteforce and dictionary attacks, spoofing attacks using SSID and MAC Address, association flooding, password cracking attack on WPA2, jamming attacks through DOS.

In case of a DOS attack, using the Wifi-Pineapple hardware to perform attacks on each client connected to the access point separately targeting individual clients. Also in the meanwhile, we have also performed DOS attack on the whole access point ie.. attacking all the clients connected to the access point thus making all the clients get disconnected through the DOS attack at a time.

V. Results and Analysis

Figure 4 contains a pictorial representation of beacon flooding attack. In particular, we have performed a beacon flooding attack using the SSID name “narahari”. This attack was successful due to the flaw in beacon packet format structure. In particular, the beacon parameters are unencrypted as a result of which beacon flooding attacks were performed.

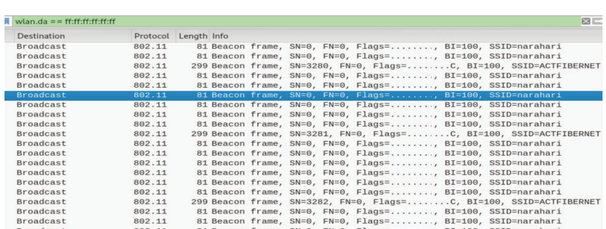

Fig. 4. Beacon Flooding Attack

From figure 5, we consider a target SSID access point, and out of all the connected clients, we have targeted a specific client and send de-authentication packets to disconnect from the access point. Our graph shows that the black plot is overall traffic and red plot describes the de-authentication packets. It is evident from the red plot that we have performed the de-authentication attack three times on the client. Also, we have performed the de-authentication attack on whole access points thus all the clients who were connected to that access point their connectivity will be lost until this attack is either stopped or completed.

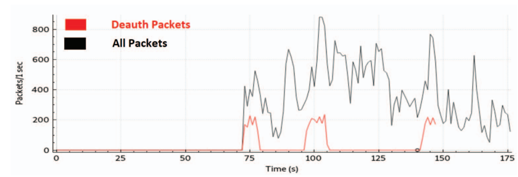

Fig. 5. De-Authentication Attack

Figure 6 shows a pictorial description of the Rogue AP attack. The goal of rogue access point attack is to flood the Access Point thus causing extensive resource usage. From the figure, black plot represents the normal traffic while red dots denote the presence of rogue access point. From the graph, we can observe that Rogue AP has triggered the flooding in between 125-150 time steps.

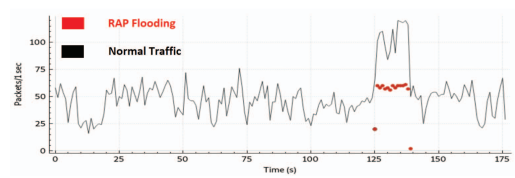

Fig. 6. RAP Attack

VI. Detection Mechanism

A. Detection Mechanism using Signature Based Detection

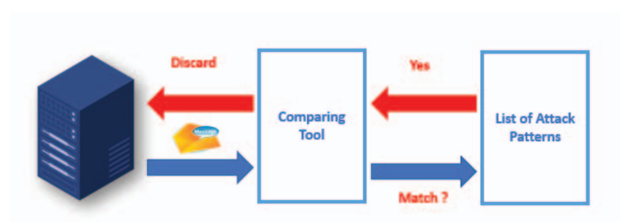

Fig. 7. Snort Signature Database

In this section, we propose to develop a signature-based detection mechanism using SNORT. Initially, at the time of attack implementation, we have run the sniffer in the background to record the network traffic of every attack performed on this experiment and recorded the data traffic as PCAP files individually. Further, we will develop the rule for each type of attack based on the individual attack parameters so as to generate a signature for every attack.

Signatures/rules are created for the attacks and pushed and stored into the SNORT database for detection. From figure 8, SNORT detects the attacks by comparing the incoming packet with its list of signatures from the database. In case of match, SNORT detects and issues an alert. These rules are generic in that it can be customized to suit the kinds of attacks in diverse kinds of networks. So the advantage here is if once the rule is written and pushed then whenever the malicious packet enters it will detect as many times as the attacker attempts.

Signature based Rule: *alert icmp any any* → *$HOME_NET any* (*msg* : *"De − Authentication Attack on Client"*; *itype* : 12; *GID* : 1; *sid* : 10000001; *rev* : 001; *classtype* : *attempted − dos*;)

Fig. 8. Snort Signature Database

Signature Description: Snort follows a syntax to write the rules from the above rule, "alert" is an action and it will be alerted whenever the rule condition is met, "any" for the source IP address, "any" for destination IP address, "right arrow" describes the direction from source to destination,"HOMENET" is the value which is taken from configuration file which is generally the network address, "msg" denotes when the rule is triggered this message will be displayed on alert, "itype" refers to the content from wireless packet and this is used to pick the sub type inside an wireless packet and rule "12" refers to the de-authentication from the wlan packet header structure, "GID" is the group id, "sid" is the snort rule id and we have given 10000001 because rule ids from 1 to 1000000 are reserved and user defined starts thereafter, "rev" is used for revision. If changes occur, this value needs to be increased for maintenance purposes, "classtype" is used for categorization. SNORT has predefined classtypes which can be utilized.

Signature Based Detection using Snort Analysis: In the Snort database, we create individual signatures for each type of attack. Further, we have tested SNORT with implemented signatures for 10 runs for each of the attacks. Alert logs generated by snort shows that after 10 runs we have calculated an average detection rate of all attacks in each run. Finally overall average rate of 91% was obtained as the detection rate for all the attacks.

TABLE I: Detection Analysis

Snort Detection Analysis	
	Number of Packets
Total Attack Packets	7200
Total Detected Packets	6552
Detection Rate = 91%	

Figure 9 presents an analysis of packet drop as a result of attacks performed on the access point. From the figure,

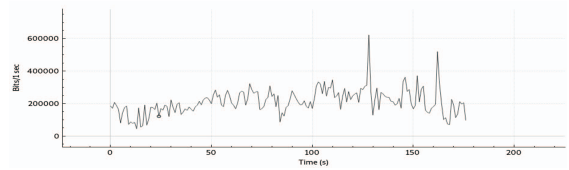

Fig. 9. Packet Drop Analysis

it is evident that there exists varying packet flows due to the packet drop. Packet drop happens due to the attacks performed on access point as well as on clients.

VII. Conclusion

In this work, we have modeled the impact of rogue APs on Wireless LANs. Towards this goal, we build a real-time Wireless testbed using commodity Wi-Fi devices such as Rogue APs that acts a Rogue AP. Further, attacks exploiting the 802.11 Association process between Clients and Access Points are performed through the Rogue AP. In addition, a sniffer is used to capture genuine and malicious traffic. Finally, a signature-based detection mechanism is developed to detect and mitigate the attacks caused by the rogue AP. Evaluation shows that our proposed detection mechanism effectively detects the attacks with a detection rate of 91%.

References

[1] J.Shawn, Tamirat T,Bryson R. Payne and Ash Mady, "Hijacking Wireless Communications using WiFi Pineapple NANO as a Rogue Access Point," 2018 ksu conference on cybersecurity education, research and practice

[2] Yimin Song, Chao Yang, Guofei Gu, who is peeping your passwords at Starbucks? – To catch an Evil-Twin Attack , 2010 IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)

[3] Shankar Sriram, G. Sahoo, Krishna Kant Agarwal "Detecting and eliminating Rogue Access Points in IEEE-802.11 WLAN-a multi-agentsourcing Methodology", Advance Computing Conference (IACC), 2010IEEE 2nd International (pp. 256-260)

[4] Vanjale, S., Mane, P. B. (2014, December) " A novel approach for elimination of rogue access point in wireless network", India Conference(INDICON), 2014 Annual IEEE (pp. 1-4)

[5] Anil Kumar,Partha Paul, Security analysis and implementation of a simple method for prevention and detection against Evil Twin attack in IEEE 802.11 wireless LAN , 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)

[6] Amirali Sanatinia, Sashank Narain, Wireless Spreading of WiFi APs Infections using WPS Flaws: an Epidemiological and Experimental Study,2013 IEEE Conference on Communications and Network Security (CNS)

[7] F.Anjum, D.Subhadrabandhu, S.Sarkar "Signature based intrusion detection for wireless ad-hoc networks: a comparative study of various routing protocols", IEEE 58th Vehicular Technology Conference, 2003

[8] Ganesh B. Bandal, Vidya S. Dhamdhere, Siddharth A. Pardeshi , Rogue Access Point Detection System in Wireless LAN, International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 2, Issue 5, October 2012

[9] J. Prakash, S. Sankaran and J. Jithish, "Attack Detection based on Statistical Analysis of Smartphone Resource Utilization," 2019 IEEE 16th India Council International Conference (INDICON), 2019

[10] J. Santhosh and S. Sankaran, "Defending against Sybil Attacks in Vehicular Platoons," 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2019

[11] Ra Padmashani, Shiju Sathyadevan, and Dath, Da, "BSnort IPS: Better snort intrusion detection/prevention system", in International Conference on Intelligent Systems Design and Applications, ISDA, Kochi,