

Automated Fake Access Point Attack Detection and Prevention System with IoT Devices

I. F. KILINÇER, F. ERTAM and A. ŞENGÜR


Abstract— Wireless access points (APs), which allow many devices to be easily connected to the Internet, are widely used today because they offer the easiest way to connect to the Internet. With the development of the Internet of Things (IoT), WiFi networks are widely used in our homes, workplaces, social areas, campus areas. With the increase of WiFi networks, attacks on these networks are constantly increasing. In this study, an IoT-based approach to detect and prevent Fake Access point attacks frequently seen in WiFi networks is proposed. A Single Board Computer (SBC) and a wireless antenna in the "Soft AP" feature are used for operation. Fake APs were detected by air scanning. In the first phase of the study, fake Access point broadcasts have been created which can create security weakness. In order to determine the fake Access points created in the second stage, SBC and wifi module were used to scan air. In the final stage, the mac address of the fake AP has been assigned to an unauthorized Virtual Local Area Network (vLAN) on the network to prevent detected fake AP broadcasts. The possible attack methods for the study were implemented and it was revealed that the proposed approach prevented the attack successfully in all scenarios. The study is seen as an effective, developed and economically useful IoT application for network administrators to prevent the attack using fake Access point.

Index Terms— Attack detection; Attack prevention; DoS attack; Network security, Fake access point, IoT


I. INTRODUCTION

CONSIDERING THE increase in the number of devices connected to the Internet and the lack of the possibility of connecting to the Internet via cable on all of these devices, the use of wireless access networks such as WiFi has emerged as a practical solution [1]. In particular, Internet of Things (IoT),


İLHAN FIRAT KILINÇER, is with Department of Informatics of Firat University, Elazig, Turkey, (e-mail: ifkilincer@firat.edu.tr).

 <https://orcid.org/0000-0001-8090-4998>

FATİH ERTAM, is with Department of Digital Forensics of Firat University, Elazig, Turkey, (e-mail: fatih.ertam@firat.edu.tr).

 <https://orcid.org/0000-0002-2306-6008>

ABDÜLKADİR ŞENGÜR, is with Department of Electrical and Electronical Engineering of Firat University, Elazig, Turkey, (e-mail: asengur@firat.edu.tr).

 <https://orcid.org/0000-0002-2306-6008>

Manuscript received October 16, 2019; accepted Nov 13, 2019.

DOI: [10.17694/bajece.634104](https://doi.org/10.17694/bajece.634104)

the way in which the interaction of human and technology changes a little more. Wireless WiFi networks, one of the most important areas of IoT; one or more wireless devices communicating through electromagnetic waves in the same environment. Wireless WiFi technology is the IEEE 802.11 standard and is in the microwave and radar category in the frequency spectrum. Fig. 1 shows the frequency spectrum in which WiFi networks operate [2].

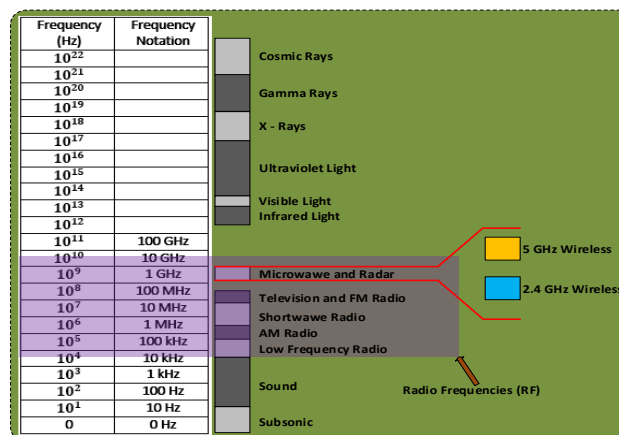


Fig.1. Frequency Spectrum

Fig. 1 shows that the WLAN technology uses the 2.4 GHz and 5 GHz bands. However, the entire band was not used when using these bands. For the 2.4 GHz band; frequencies between 2.400 GHz - 2.4835 GHz 5.7 are used, the frequencies between 5.4 5.150 GHz - 5.250 GHz, 5.250 GHz - 5.350 GHz, 5.470 GHz - 5.725 GHz, 5.725 GHz to 5.825 GHz are used for the 5 GHz band.

WiFi technology offers many important advantages over wired connection because of its ability to make roaming and its comfortable use. However, it contains many security weaknesses. Various security mechanisms such as WiredEquivalentPrivacy (WEP), WiFiProtected Access (WPA), WPA2 have been developed to minimize these security vulnerabilities [3-4].

Heartfield et al. [5], classified the security vulnerabilities that occurred in smart homes, which is an IoT application, taxonomically. Not only the attack vectors were emphasized in the study, but also the potential impact of the attack on the system.

WEP is an encryption algorithm developed to provide security in wireless networks. WEP first started with 64-bit encryption and enabled up to 256-bit encryption. However, the

most commonly used type of encryption is the 128-bit encryption method [6]. In spite of many corrections and increased password dimensions in WEP encryption algorithm, it can be easily broken by many open source applications such as aircrack. Therefore, it is not used much today. The WEP encryption method performs the verification in four steps as in Fig. 2. The WEP encryption method performs the verification in four steps as in Fig. 2. Accordingly, the first step goes from the wireless PC to the connection request to the AP. In the second step, the AP creates a random text (64 bit, 128 bit) according to the encryption method and sends the connection to the requesting device. In the third step, the PC encrypts the text from the AP with the WEP password in itself and sends the encrypted text to the AP. In the last step, if the AP acknowledges the accuracy of the encrypted information that is sent to it, authentication takes place and the user connects to the AP [7-8].

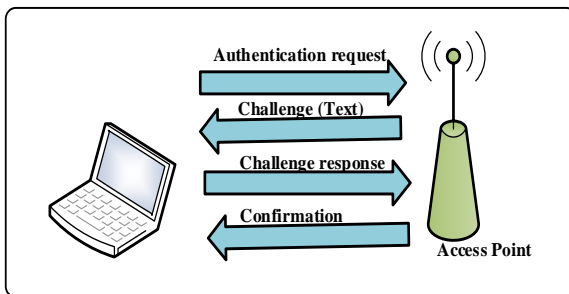


Fig.2. WEP Authentication

The WEP validation method contains many features. Therefore, user data can be easily sniffed by the attacker. The WiFi alliance association then introduced the IEEE802.11i standard to the industry to prevent these vulnerabilities. WPA and WPA2 encryption methods were developed in 2003 with this standard. WPA / WPA2 standards use the Advanced Encryption Standard (AES) based Temporal Key Integrity Protocol (TKIP) and Counter Modewith Cipher Block Chaining Message Authentication Code Protocol (CCMP) encryption methods for secure authentication [6]. In Fig. 3, the classes of the IEEE 802.11i standard are summarized [10].

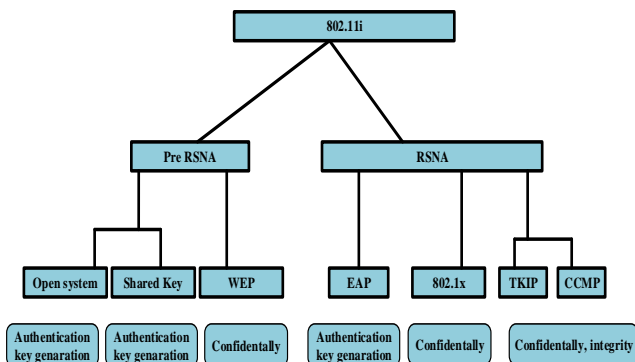


Fig.2. Classes of the 802.11i standard

There are many studies in literature to prevent WEP and WPA cryptography. L YongLei et al. In order to overcome

processor constraints in bruteforce attacks, they proposed distributed multi-core CPU and GPU parallel cracking method (DMCG) method. In this method, WPA has used colored Petri nets to verify the 4-way handshake protocol used in the encryption method. For the DMCG, the generated PSK wordlist is given to each computer running in distributed architecture. GPU processors have also been used to improve performance [11]. V.Kumkar et al. showed how to attack WEP, WPA, WPA2 encrypted networks. WEP and WPA2 networks were attacked and the security vulnerabilities were investigated in real time. The Aircrack-ng framework was used to organize the attack. In the attack, WEP-encrypted networks were seen to be hacked much easier than WPA-encrypted networks [3]. S. Gold, in his study showed that WEP and WPA passwords can be easily broken using tools such as aircrack-ng and aireplay [12].

Wang et al. by analyzing the deficiencies in WEP and WPA encryption methods, they developed d-WEP and d-WPA-PSK algorithms. According to the developed d-WEP algorithm, the decision is made to determine whether the AP is under attack by looking at the number of ARP requests. On the other hand, in order to prevent d-WPA-PSK attacks, a mechanism has been designed in which the PSK is changed regularly [13].

Apart from the WEP and WPA attacks, one of the methods frequently used by the attackers is creating a fake Access point so that users can view their traffic without making them feel. Attacker fake can do an Access point attack in two ways. In the first method, it can broadcast the name “freeWiFi” which will attract the attention of the users. This allows users to connect to it. In the second method, users can connect to it by making a stronger fake broadcast with the same name as the WiFi network in the location. The attacker can follow two options when making the second method.

Option 1:

Catching a 4-way Handshake: The attacker expects users to be authenticate at first, in a network where users are busy. The attacker then tries to solve the network key by capturing the handshake. 4 way handshake is the IEEE-802.11i standard for secure authentication in wireless networks. Pre-sharedkey (PSK) or 802.1X authentication methods use 4 way handshake encryption. During 4 way handshake, there are 4 messages between client and Access point. In the first step, the AP sends a randomly generated Anonce (Authenticatednumberonce) frame to the client with the message 1. In the second step, after obtaining the Anonceframe, Snonce (Supplicantnumberonce) and PTK are generated and transmitted to the AP together with the MIC as message 2. After receiving the AP Snonceframe in the third step, it generates its own GTK and transmits it to the client as message 3 with its MIC. In the last step, the client sends the AP to acknowledge message 4 and the authentication is complete. The algorithm of 4 way handshake is given in Fig. 4 [14-18].

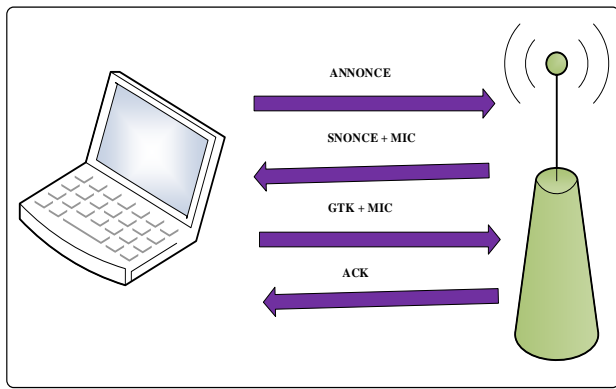


Fig.4. WPA/WPA2 4 way handshake

During the 4-way handshake, GroupTemporalKey (GTK), PairwiseTemporalKey (PTK), Group Master Key (GMK), Pairwise Master Key (PMK), Master SessionKey (MSK), encryption algorithms are used. During authentication, which is the first stage of encryption, the MSK key is generated. In the second stage, the PMK and GMK second level switches produced from the MSK are used to construct the PTK and GTK. The hierarchy of the encryption methods mentioned in Fig. 5 is given.

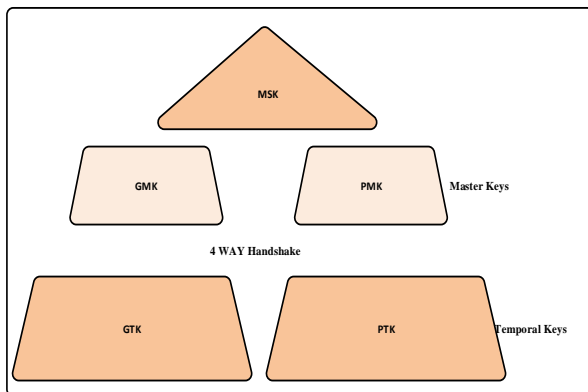


Fig.5. Key Hieararchies

These encryption methods can be briefly summarized as follows [19-20].

- PTK is used to encrypt all unicast traffic between user and Access Point.
- GTK is used to encrypt all broadcasts between Access point and multiple users.
- GMK is used to build GTK.
- The PMK is the key generated from the MSK. The PMK is not usually transmitted over the network, this component is not shared and thus increases transaction security.
- The MSK is the first key derived during 802.1X or PSK authentication.

Option 2:

Deauthentication attack: Deauthentication is a Layer 2 DoS attack specific to the 802.11 standard. The attacker will allow the user to disconnect from the network by organizing a deauthentication attack on the user connected to the AP without waiting for the 4-way handshake. This results in 4-

way handshake when the user wants to connect to the network again. At this stage, the attacker catches the 4-way handshake [14-15,21-22].

Fake AP attacks are frequently used to reach user data. In these types of attacks, the attacker makes a broadcast similar to the SSID in the environment and allows the user to connect to this SSID. There are many studies to prevent fake AP attacks in the literature. Take Kuo-FongKao et al. In order to prevent fake AP attacks, they developed an algorithm by looking at the serial numbers, timestamp and range of beacon messages. In their study, they saw that the attackers could change the serial numbers, time stamps and signal intervals of fake APs. However, they suggested that the method they proposed was successful in detecting these attacks [23].

Mohan K Chirumamilla et al. In their study, they developed an agent-based intrusion detection system to find unauthorized APs. Developed agents maintain a list of registered APs. When an AP is added or removed to any agent, the administrator notifies the MAC address of all AP agents. Thus each agent will have a current AP list on it. Another task of agents is to scan for a fake APs. After each scan, he compares the AP mac addresses he sees with the AP mac addresses in his list. If the AP is not in the current list, the administrator will be notified by SMS. The agent developed in the study has each agent, a wireless interface and two network interface cards. The wireless interface card was used to scan and detect fake APs, while two other Ethernet cards were used to connect the agent to the spine [24]. SomayehNikbakhsh et al. in their study, they proposed a method to prevent users from connecting to fake APs. In the proposed method, the route and gateway information of the package were compared to determine whether an AP is fake. With this method, Man in theMiddle (MiTM) attacks are easily detected without the need for a network administrator [25].

In this study, Raspberry PI 3 was chosen as SBC device to prevent and detect fake AP attacks. Kali Linux was installed on the device, and one of the USB ports was installed on the WiFi antenna.

The detailed contributions are as follows.

- It is very easy to integrate into the existing network, especially in large networks that are used in corporate networks. In this way, a direct ready-to-use system is provided for network administrators and system administrators without any configuration problems.
- To capture fake access point attacks on traditional WiFi networks, there is often a need for an access point that needs to work in monitor mode. Therefore, extra budgets are required to prevent such an attack. The proposed method will work effectively on intrusion detection and prevention without incurring major costs.
- The proposed method will automatically notify the system administrator by means of integrated tools such as SMS and mail when the attack is detected.

II. PROPOSED METHOD

Today, hackers are widely using openings in wireless networks to regulate their attacks. In this context, one of the most common types of attacks in wireless networks is Fake Access point attacks. In this study, a new method has been proposed to prevent fake access point attacks. The network diagram of the proposed method is given in Fig. 6.

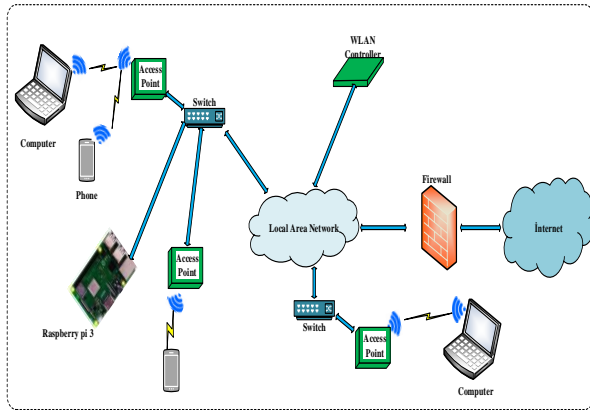


Fig.6. Network diagram of the proposed method

The network diagram given in Fig. 6 is the architecture of a general corporate network. Connected to edge switches in traditional network architectures, the APs transmit incoming traffic to the Wireless controller installed at the center of the network through the LWAPP tunnel.

In this study, a cheaper and effective method has been proposed to prevent fake Access points. Accordingly, instead of an additional Access point, the Raspberry pi device is positioned in the desired area to be monitored and the Wi-Fi broadcasts in the environment are monitored by operating in Raspberry pi monitor mode. Raspberry PI 3 device was used in this study. Kali Linux operating system was installed on 16 GB Class 10 Micro SD card on Raspberry PI 3 device. In this study, ODROID module is installed on the Raspberry PI 3 device for aircan. Raspberry PI and its connections are given Fig.7.



Fig.7. Raspberry PI 3 SBC and connection modules

After the installation of the necessary tools, the algorithm in Fig. 8 was used to find the attacker broadcasting the fake Access point.

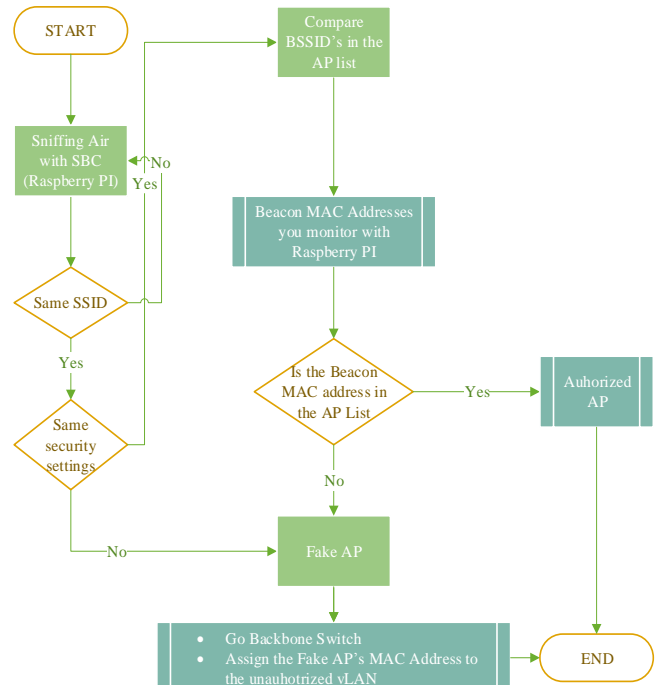


Fig.8. Algorithm of the proposed method

The steps of the flowchart given in Fig. 8 and the tools used for aircan on the Raspberry PI 3 during these steps are described below.

Step-1: In the first stage, the ODROID module installed on Raspberry PI 3 was taken in the monitor mode. The "airmon-ng start wlan0" command was used for this. Then the, "iwconfig" command is used to see that the module is in monitor mode. Fig. 9 shows the output of this process.

```

root@root:~# airmon-ng start wlan0

PHY      Interface  Driver      Chipset
phy3     wlan0     rt2800usb   Ralink Technology, Corp. RT5572

(mac80211 monitor mode vif enabled for [phy3]wlan0 on [phy3]wlan0mon)
(mac80211 station mode vif disabled for [phy3]wlan0)

root@root:~# iwconfig
wlan0mon IEEE 802.11 Mode:Monitor Frequency:2.457 GHz Tx-Power=20 dBm
Retry short long limit:2 RTS thr:off Fragment thr:off
Power Management:off

eth0     no wireless extensions.
lo       no wireless extensions.
    
```

Fig.9. Odroid module in monitor mode

Step-2: In the second stage, aircan was launched with the command "airodump-ng wlan0mon". For the first test case, the 00:11:22:33:44:00 BSSID mac address and the fake SSID called FU_TEST are published. In this scenario, only the SSID name was made similar to the current FU_TEST SSID name used on the network. There is no security setting in the SSID that the attacker issued when there was WPA2 encryption in the current FU_TEST broadcast. In this kind of attacks, users prefer the easy way because there is no authentication process

and connects to open SSID. The attacker then starts to sniff the traffic of the connected users. For this scenario, the attacker is set to have bssid value 00:11:22:33:44:00 over the FU_TEST for SSID broadcast in the “hostapd-mana.conf” file

```
root@root:~# airodump-ng wlan0mon

CH 9 ][ Elapsed: 2 mins ][ 2019-03-27 02:23

BSSID            PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
00:11:22:33:44:00 -35    23         0  0  6  11  OPN             FU_TEST
4C:FA:CA:4A:E6:C0 -69    19         2  0  1  720 WPA2 CCMP MGT  FU_TEST
```

Fig.10. Result of the first test case

According to the algorithm proposed in this type of attack, Raspberry PI 3 accepts this unsecured broadcast, fake SSID. Then the Raspberry PI connects backbone to ssh and assigns the BSSID mac address of this fake broadcast to an unauthorized VLAN previously set in the backbone. Users will not be able to access the Internet even if they connect to the SSID of this fake AP.

Step-3: In the third stage, the fake SSID with the 00:11:22:33:44:00 BSSID mac address and the same security settings as the original SSID of FU_TEST is issued. The airodump-ng was then started with the “airodump-ng wlan0mon” command as shown in Fig. 11. This kind of attacks are used to sniff traffic without making users feel. For this scenario, the attacker has made the following settings in the “hostapd-mana.conf” file in the “mana-toolkit” tool.

```
interface=wlan0
bssid=00:11:22:33:44:00
driver=nl80211
ssid=FU_TEST
channel=6
wpa=2
wpa_key_mgmt=WPA-EAP
wpa_pairwise=TKIP CCMP
wpa_passphrase=AsecurePassword
```

```
root@root:~# airodump-ng wlan0mon

CH 10 ][ Elapsed: 12 s ][ 2019-03-27 03:18

BSSID            PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
00:11:22:33:44:00 -46     3         0  0  7  11  WPA2 CCMP MGT  FU_TEST
4C:FA:CA:4A:E6:C0 -66     2         0  0  1  720 WPA2 CCMP MGT  FU_TEST
```

Fig.11. Fake AP broadcast with the same security settings as the original SSID

In order to prevent such attacks, the network administrator needs a table with bssid mac addresses of the original broadcast access points. Raspberry PI compares the bssid mac address, which it sees when it sees the SSID broadcast with

located in the “mana-toolkit” tool. FU_TEST broadcast is made from channel 6. The screen output for this scenario is shown in Fig. 10.

the same name and the same security settings, with the previously prepared list. If the bssid mac address of the fake broadcast access point is not in the pre-prepared list, then this SSID is published from the fake AP. Then the Raspberry PI is connected to the backbone switch with ssh. Then the fake access point bssid mac address is assigned to an unauthorized VLAN which previously created on the backbone switch. After this stage, users will not be able to access the Internet even if they connect to the SSID of this fake AP.

Step-4: In the last scenario, the attacker can do the same with the original AP as the bssid mac address of the access point where the attacker does the fake broadcast as well as the SSID and security settings. Fig. 12 presents the output of this scenario. Also for this scenario, the change made to the file “hostapd-mana.conf.” In the “mana-toolkit” tool is given below.

```
interface=wlan0
bssid=00:11:22:33:44:00
driver=nl80211
ssid=FU_TEST
channel=7
wpa=2
wpa_key_mgmt=WPA-EAP
wpa_pairwise=TKIP CCMP
wpa_passphrase=AsecurePassword
```

```
root@root:~# airodump-ng wlan0mon

CH 9 ][ Elapsed: 4 mins ][ 2019-03-27 03:25

BSSID            PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
4C:FA:CA:4A:E6:C0 -54    71         10  0  7  720 WPA2 CCMP MGT  FU_TEST
```

Fig.12. Fake AP attack with same bssid, SSID and security settings

In such attacks, access points on the campus WiFi network saw this attack and did not allow such an attack against it. The output from the WiFi Controller used in AP management in the campus WiFi network is shown in Fig. 13. Many of the WiFi controllers of this kind of attacks are black-listed bssidmac address fake broadcast. Therefore, in the algorithm given in Fig. 8, a method for this type of attack has not been proposed.

Attack Detection Information (Spoofing attack)				
MAC Address	Channel	RSSI (dBm)	Monitor AP	Last Discovered At
4cfa-ca4e-6c0	7	-79	ap-1	2019-03-27 10:25:56

Fig.13. WiFi controller attack log

The pseudo-code generated for the algorithm used in the proposed method is given below.

Start

Input: Sniff air for 802.11 beacons

Output: Predicted Fake AP

If there is more than one ssid with the same name

if SSIDs have the same security settings

Compare BSSIDs in the AP list and the beacon mac addresses you monitor with Raspberry PI

If the beacon mac address is in the AP list

Then it is Authorized AP

Else

Then it is Fake AP, send warning message and take Fake AP to the unauthorized VLAN

Else

Then it is Fake AP, send warning message and take Fake AP to the unauthorized VLAN

else

Then Sniff air again

End

III. CONCLUSION AND FUTURE WORKS

The use of wireless WiFi devices is increasing day by day with the widespread use of internet. As a result, the possibility of capturing the information flow via wireless signals is also increasing due to the existing security vulnerabilities and intriguing by the attackers. The ability of attackers to view, receive and modify user data using these vulnerabilities has become inevitable in internet areas where security measures are not taken sufficiently. In this study, a method is proposed against fake AP attacks which is one of the attack types in wireless WiFi networks. The scenarios of the proposed method and the types of attacks that can be made are determined and the success of the proposed method against these scenarios is emphasized. These attacks were attempted to be identified with the given algorithm and the pseudo-code snippet, and then the studies to prevent these attacks were presented. Kali Linux operating system has been installed on Raspberry PI 3 which is one of the most widely used SBC devices. It was also used with the Odroid module SBC to monitor wireless broadcasts. As a result of the study, it was seen that fake AP attacks were successfully detected and prevented by the proposed method.

In future studies, an application will be developed to find fake APs that have the same security settings as the same beaconmac address in the same SSID. This application will be run on raspberry PI or similar SBC device and when it sees more than the same SSID, these SSIDs will be connected to the engine and traceroute will determine the number of hop and the software will be prepared with an interface where the accesspoint is fake and reported.

ACKNOWLEDGMENT

This work was supported by the FUBAP (Firat University Scientific Research Projects Unit) under Grant No: TEKF.18.13.

REFERENCES

- [1] C. Xu, W. Jin, X. Wang, G. Zhao, and S. Yu, "MC-VAP: A multi-connection virtual access point for high performance software-defined wireless networks," *J. Netw. Comput. Appl.*, vol. 122, pp. 88–98, 2018.
- [2] D. Liu, B. Barber, and L. DiGrande, Cisco CCNA/CCENT exam 640-802, 640-822, 640-816 preparation kit. 2009.
- [3] V. Kumkar, A. Tiwari, P. Tiwari, A. Gupta, and S. Shrawne, "Vulnerabilities of Wireless Security protocols (WEP and WPA2)," *Int. J. Adv. Res. Comput. Eng. Technol.*, vol. 1, no. 2, pp. 2278–1323, 2012.
- [4] H. R. Hassan and Y. Challal, "Enhanced WEP: an efficient solution to WEP threats," 2005, pp. 594–599.
- [5] R. Heartfield et al., "A taxonomy of cyber-physical threats and impact in the smart home," *Computers and Security*. 2018.
- [6] S. Wong, "The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards," sans.org/rr/whitepapers/wireless/1109. php Retrieved, pp. 1–10, 2003.
- [7] S. Vibhuti, "IEEE 802.11 WEP Wired Equivalent Privacy Concepts and Vulnerability," *San Jose State Univ.*, no. Iv, 2008.
- [8] A. H. Lashkari, R. S. Hosseini, and F. Towhidi, "Wired equivalent privacy (WEP)," in *Proceedings - 2009 International Conference on Future Computer and Communication, ICFCC 2009*, 2009, pp. 492–495.
- [9] Y. Liu, Z. Jin, and Y. Wang, "Survey on security scheme and attacking methods of WPA/WPA2," 2010 6th Int. Conf. Wirel. Commun. Netw. Mob. Comput. WiCOM 2010, pp. 1–4, 2010.
- [10] A. H. Adnan et al., "A comparative study of WLAN security protocols: WPA, WPA2," in *Proceedings of 2015 3rd International Conference on Advances in Electrical Engineering, ICAEE 2015*, 2016, pp. 165–169.
- [11] J. Z. Liu Yong-lei, "Distributed method for cracking WPA/WPA2-PSK on multi-coreCPU and GPU architecture," no. November 2013, pp. 723–742, 2009.
- [12] S. Gold, "Cracking wireless networks," *Netw. Secur.*, vol. 2011, no. 11, pp. 14–18, 2011.
- [13] Y. Wang, Z. Jin, and X. Zhao, "Practical defense against WEP and WPA-PSK attack for WLAN," in 2010 6th International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM 2010, 2010.
- [14] K. Bicakci and B. Tavli, "Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks," *Computer Standards and Interfaces*, vol. 31, no. 5. pp. 931–941, 2009.
- [15] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," in *USENIX security*, 2003, pp. 15–28.
- [16] X. Zha and M. Ma, "Security improvements of IEEE 802.11i 4-way handshake scheme," in 12th IEEE International Conference on Communication Systems 2010, ICCS 2010, 2010, pp. 667–671.
- [17] Z. Bai and Y. Bai, "4-Way handshake solutions to avoid denial of service attack in ultra wideband networks," in 3rd International Symposium on Intelligent Information Technology Application, IITA 2009, 2009, vol. 3, pp. 232–235.
- [18] S. H. Eum, Y. H. Kim, and H. K. Choi, "A Secure 4- Way Handshake in 802.11i Using Cookies.pdf," vol. 2, no. 1, 2008.
- [19] A. Alabdulatif, X. Ma, and L. Nolle, "Analysing and attacking the 4-way handshake of IEEE 802.11i standard," in 2013 8th International

Conference for Internet Technology and Secured Transactions, ICITST 2013, 2013, pp. 382–387.

[20] Internet, “4 Way Handshake.” .

[21] T. D. Nguyen, D. H. M. Nguyen, B. N. Tran, H. Vu, and N. Mittal, “A lightweight solution for defending against deauthentication/ disassociation attacks on 802.11 networks,” Proc. - Int. Conf. Comput. Commun. Networks, ICCCN, pp. 185–190, 2008.

[22] K. El-Khatib, “Impact of feature reduction on the efficiency of wireless intrusion detection systems,” IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 8, pp. 1143–1149, 2010.

[23] K. F. Kao, W. C. Chen, J. C. Chang, and H. Te Chu, “An accurate fake access point detection method based on deviation of beacon time interval,” in Proceedings - 8th International Conference on Software Security and Reliability - Companion, SERE-C 2014, 2014, pp. 1–2.

[24] M. K. Chirumamilla and B. Ramamurthy, “Agent based intrusion detection and response system for wireless LANs,” 2004, pp. 492–496.

[25] S. Nikbakhsh, A. B. A. Manaf, M. Zamani, and M. Janbeglou, “A novel approach for rogue access point detection on the client-side,” in Proceedings - 26th IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2012, 2012, pp. 684–687.

BIOGRAPHIES



İlhan Firat Kilincer was born in Elazig, Turkey in 1986. He received B. S. degree in Electric Electronic engineering from Kocaeli University, Kocaeli, Turkey, in 2012. He is currently pursuing the Ph.D. degree in electrical engineering. He works as network security expert in the Computer

Center, Firat University, Elazig



Fatih Ertam was born in Elazig, Turkey in 1978. He received the B.S. and M.S. degrees in computer science from Firat University, in 2000 and 2005, respectively, and the Ph.D. degree in software engineering from Firat University, in 2016. He is currently an

assistant professor with the Digital Forensics Engineering, Firat University. His current research interests include network security, machine learning, deep learning, and network forensics.



Abdulkadir Sengur graduated from the department of Electronics and Computer Education at Firat University in 1999. He obtained his M.S. degree from the same department and the same university in 2003. His Ph.D. degree was from the department of Electronic Engineering at

Firat University in 2006. He is a professor at Firat University. His interest areas include pattern recognition, machine learning and image processing.