ISSN 2278-3091
Volume 9, No.1.3, 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse1391.32020.pdf
https://doi.org/10.30534/ijatcse/2020/1391.32020

DARMA: Defeating and Reconnaissance Manna-karma Attacks in 802.11 with Multiple Detections and Prevention

Norzaidi Baharudin[1], Fakariah HaniMohd Ali[2], Mohd HarizBin Naim@Mohayat[3]
[1]Faculty of Computer and Mathematical Sciences, UniversitiTeknologi Mara, Malaysia, mail@matnet.my
[2]Faculty of Computer and Mathematical Sciences,UniversitiTeknologi Mara, Malaysia, fakariah@tmsk.uitm.edu.my
[3]Faculty of Information and Communication Technology,UniversitiTeknikal Malaysia Melaka, Malaysia, mohdhariz@utem.edu.my

ABSTRACT

The vast growing usage of mobile phones increases Wi-Fi technology. At present, the pattern of human interaction with the internet is not a desktop or laptop anymore. The assimilation of tools for surfing, working, and communication is now shifting to mobile phones. Thus, this is the motivation to expand Wi-Fi technology so that it will be the primary medium for internet connectivity. Hence, increasing the security risk for it attracts attackers despite its popularity among users. The DOS attack in 802.11 management frames is widely known as an initial process before Man-in-the-middle (MiTM) attacks in 802.11 takes part. Karma and Manna's attacks are an unprecedented attack in the 802.11 management frames. This paper proposed a mechanism called Defeating and Reconnaissance Manna-karma Attack (DARMA), which is client-side multiple detection techniques to defeat and prevent karma-manna attack. The proposed mechanism consisted of 4 layers of processes inclusive of monitors, detection, confirmation, and preventions. The effectiveness of the detection is base of the current real-time behaviour of the packets.

Key words: Karma, Manna, Beacon, Probe Response, Probe Request, WLAN, 802.11, Wi-Fi, Management Frames attack.

1. INTRODUCTION

Today, around 5 billion mobile phones are estimated to exist globally [1] and 802.11 signals were cover every single area such as coffee shop, shopping mall, hotels, and many more [2]. The immense, rapid increase of wireless network motivates many attacks that have been leveraging with so many hacking tools available on the internet. The evolutions of 802.11 security have changed in line with various types and they tend to secure the network. The Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA/WPA2) are security mechanisms that protect only the networks but not the authorized client of the wireless network [3]. Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks describe some events where they are harmful and could fail any service [4],[5]. There are five layers of Wi-Fi DOS attacks; physical layer, data link layer, network layer, transport layer and application layer [6][7]. Karma and Manna's are DOS attacks which reside in the data link layer. Data link layer has two types of an adversary namely from the inside and outside of the network. While it may be true, the adversary can launch the attacks from outside of the network because the management frames of 802.11 are used to enable the client to get into the WLAN. The prerequisite to deploying the attacks is that the WLAN adapter should support the monitor mode feature [8].

Wireless Network uses radio frequency to transmit and receive data over the air by exchanging with three types of frames: management frame, control frame and data frame. These frames are sent unencrypted and exposed asplain text on any sniffer applications such as Wireshark. The new Wi-Fi standard/protocol of 802.11w can protect the management frames, but it has several flaws where the deployment is still slow and lots of legacy hardware is yet not supported by this new protocol [3]. Besides, specific existing devices and firmware are unable to be updated with the new protocols, preventing the old devices from getting the protection benefit. Management Frames are the most significant frame, where it enables stations to establish and maintain communication.

Karma-manna attacks use probe request/response that is a subtype of management frames of 802.11. This kind of attack used to be an initial process before the emergence of Evil Twin AP. Devices such as mobile phones and computers maintain the list of connected wireless network called Preferred Network List (PNL) [9]. The wireless interface is periodically sending a probe request to the Service Set Identifier (SSID) listed on the PNL. It is also called a direct probe request. Once an adversary listens to this request, it will reply a send a probe response as depicted in Figure 1. The karma attacks will gain the purpose after the victim is connected to the evil twin or rogue AP.

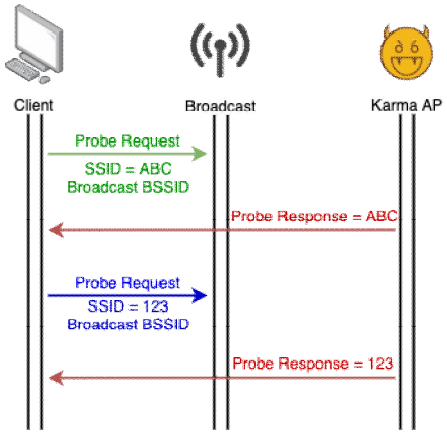

Figure 1: Karma Attacks

Besides, Wi-Fi standard has upgraded the security itself and makes most of the wireless devices now as only send broadcast probe request and not direct probe request to the PNL SSID [9]. Current android or iOS mobile phones are now only sending 802.11 probe request to the broadcast without having any SSID information. Upon receiving the probe request, access point (AP) nearby will send the probe response and deliver the standard information such as SSID name. Wireless clients will compare the SSID name with the current PNL on the list. Thus, this security practice will make Karma obsolete.

A new kind of attacks called Manna [10] has emerged; it is a new version of Karma Attack that leverages a vulnerable mobile phone that is still sending direct probe request and save the list to the database. Manna is assuming that the neighboring mobile should have the same SSID in the PNL. A regular operation of Karma is sending a probe response directly to the requested clients. Alternately, Manna sends probe response to all clients across the network. This method is also known as loud mode where all intersects of two or more devices are considered having the same PNL. Besides a new attack technique called "Known Beacon Attack" [11] has also emerged that elevates the success rates of karma and manna attack. This method is relying on the construction of wordlist files. The words on the file relatively use SSIDs. The attacker will be sending broadcast beacons from the list, and perhaps there will be the same SSID on the target PNL.

Therefore, the adversary always updates and enhances the attack; then the following questions should be pertinent: (1) What is the comparison between an ordinary packet of beacons and probe? (2) Is it possible to detect and prevent the forged packet through behavior analysis? To answer these questions, regular packets with no adversary were captured, and then the attacks deployed, and the forge packets generated.

Wireless security protection should be practised by everyone by not depending too much on WLAN administrator to secure the network. Thus, the primary significance of DARMA (**D**efeat **A**nd **R**econnaissance **M**anna-karma **A**ttack) is to increase consumer awareness of personal WLAN protection. This paper is classified into five sections; the background and fundamental of 802.11 security, other related works that critically focus on management frames security, preliminary design of experimentation on how the Karma-Manna attacks occur, proposed solution and evaluation procedures followed by conclusion.

2. RELATED WORKS

Management Frames in 802.11 are exposed to several types of attacks because the architecture of the frames is not encrypted and can be read as a plain text. The most famous attack on 802.11 Management Frames is De-authentication attack that can be categorized as a DOS (Denial of Service) [12]. Besides, other attacks include beacons attack and karma-manna attacks. Most of these attacks comprise the preliminary processes to deploy the main attacks called Evil-Twin AP. Some researchers call this attack as Rogues Access Point (RAP) [13].

Most studies have been focusing on how to detect Evil-Twin AP or Rogue AP. Still, this study is focusing on the detection and prevention of forge probe response, leveraging by the Karma and Manna Attacks. All forged packets in 802.11 Management frames are also known as DOS (Denial of Service) [14]. Correspondingly, many studies have been conducted to detect and prevent this attack. Two types of categories are used to detect these attacks; administrator and client-side [15]. While a couple of studies [16], [17] rely on the administrator of the network to detect the attack, some studies [18]–[20] found that wireless clients are capable of detecting DOS attack.

A study also suggests changing the protocol of Management Frames by implementing new rules or policies[21]. This kind of solution is too complicated to be executed because it will require driver and firmware modification.

The current Wi-Fi protocols in Android and iOS operating systems have been upgraded, hence, enhancing the level of security. The Preponderance of Wi-Fi clients now only sends broadcast probe request without any SSID information on the packet [9]. On the contrary, before the probe request is sent directly, the information of the SSID requested will be published. Thus, anybody on the proximity area is able to reply to the probe response upon hearing of the probe request from the prospectus victims. Consequently, a new sophisticated technique is emerging known as Manna attacks which is derived from the Karma. Manna is taking advantage of vulnerable or unsafe mobiles that are still sending direct probe request and storing these SSIDs. Those stored databases will be used to broadcast probe response and perhaps successful hit may be associated with the adversary [9].

3. KARMA AND MANNA ATTACKS

This section discusses first, the current behavior of beacons and probes frames from the legitimate packets. Then, an attack will be produced, generating the forge packets in comparison to the legitimate packets. To realize this phenomenon, the attacks are launched by using Wifi-Pineapple Tetra [22]. It is a hacking tool that can be used for MiTM attacks and all kinds of WLAN attacks such as de-authentication, forge beacons and karma-manna attacks.MiTM is an attack that can intercept communication between victims and collect all required information [23]. In this study, two types of attacks, beacons and probes will be covered as described in the following subsections:

3.1. The legitimate beacons and forge beacons

Beacon is the sub-type of the management frames and used as an announcer to broadcast the existing Access Point (AP) [24]. The packets inclusive of Service Set Identifier (SSID) information, support data rates and capabilities. Most APs send beacons around 100ms time intervals. In terms of captured packets without attack, 5.3% of beacon were captured over 38739 total packets.

The forge beacon packets can also be generated with many free tools such as *mdk3*. It can also be crafted manually with *Scapy* library in *python* where the packets will be crafted first before being transmitted and broadcasted. As depicted in Table 1, the results showed that the beacons frames are generated by Wireless Pineapple tool which has less capability information. For instance, the spoofed packet only has Extended Service Set (ESS) capabilities and zero capabilities for others. Table 1 illustrates a comparison between legit beacons frame and forge beacon frames.

Table 1: Packet with karma-manna attack

Beacons	Total packets	ESS Cap.	Others Cap.
Legit	11657	Yes	Yes
Forge	123997	Yes	No

Around 135654 packets (with karma-manna attack) were captured and 65.02% were identified as beacon frames. From the total of the beacon frames, 8.59% were legit, and 91.4% were forge packets. Beacon and probes packets have a field called capability information which is used to advertise the network capabilities such as ESS/IBS, privacy, Short preamble, PBCC, channel agility, short slot time, DSS-OFDM, contention-free polling bits. As observed, all forge packets only have ESS Capability and does not have any other capabilities. Furthermore, the most significant behaviour of forge beacons is one BSSID of a beacon having too many SSID published as depicted in Figure 2. In addition, the beacon hit rate was higher in the packets (with attacks) which was h = 65.02% and legit packets was just h = 5.3%. For clarification, BSSID refers to MAC address of the particular AP [25].

	Time	Source	Info
1	05:10.6	OrientPo_	Beacon frame, SN=2672, FN=13, Flags=.....C, BI=100, SSID=Eur otel_16
2	05:10.6	OrientPo_	Beacon frame, SN=3920, FN=7, Flags=.....C, BI=145, SSID=Hote al-KL
3	05:10.6	OrientPo_	Beacon frame, SN=1472, FN=9, Flags=.....C, BI=116, SSID=Iphon
4	05:10.6	OrientPo_	Beacon frame, SN=2608, FN=6, Flags=.....C, BI=117, SSID=John
5	05:10.6	OrientPo_	Beacon frame, SN=1920, FN=8, Flags=.....C, BI=77, SSID=Kama
6	05:10.7	OrientPo_	Beacon frame, SN=2128, FN=6, Flags=.....C, BI=104, SSID=Park
7	05:10.7	OrientPo_	Beacon frame, SN=3136, FN=14, Flags=.....C, BI=53, SSID=STR R@unifi
8	05:10.7	OrientPo_	Beacon frame, SN=1280, FN=12, Flags=.....C, BI=133, SSID=The
9	05:10.7	OrientPo_	Beacon frame, SN=2880, FN=4, Flags=.....C, BI=63, SSID=ViP 2
10	05:10.7	OrientPo_	Beacon frame, SN=2000, FN=10, Flags=.....C, BI=132, SSID=Wi 1
13	05:10.7	OrientPo_	Beacon frame, SN=544, FN=12, Flags=.....C, BI=124, SSID=iphon
15	05:10.7	OrientPo_	Beacon frame, SN=3488, FN=9, Flags=.....C, BI=79, SSID=kamf
18	05:10.7	OrientPo_	Beacon frame, SN=2096, FN=5, Flags=.....C, BI=97, SSID=Bawa ER
19	05:10.7	OrientPo_	Beacon frame, SN=4032, FN=1, Flags=.....C, BI=136, SSID=CITI
20	05:10.7	OrientPo_	Beacon frame, SN=1248, FN=14, Flags=.....C, BI=131, SSID=Eur otel_16
21	05:10.7	OrientPo_	Beacon frame, SN=2800, FN=3, Flags=.....C, BI=134, SSID=Hote al-KL
22	05:10.7	OrientPo_	Beacon frame, SN=1312, FN=2, Flags=.....C, BI=56, SSID=Iphon
24	05:10.7	OrientPo_	Beacon frame, SN=3840, FN=5, Flags=.....C, BI=62, SSID=John
25	05:10.7	OrientPo_	Beacon frame, SN=448, FN=12, Flags=.....C, BI=69, SSID=Kama
26	05:10.7	OrientPo_	Beacon frame, SN=888, FN=0, Flags=.....C, BI=100, SSID=FreeWi
27	05:10.7	OrientPo_	Beacon frame, SN=1568, FN=7, Flags=.....C, BI=73, SSID=Park
32	05:10.7	OrientPo_	Beacon frame, SN=560, FN=15, Flags=.....C, BI=146, SSID=STR R@unifi
33	05:10.7	OrientPo_	Beacon frame, SN=3824, FN=0, Flags=.....C, BI=75, SSID=The E
34	05:10.7	OrientPo_	Beacon frame, SN=1824, FN=10, Flags=.....C, BI=93, SSID=ViP
35	05:10.7	OrientPo_	Beacon frame, SN=2096, FN=13, Flags=.....C, BI=96, SSID=WiF
36	05:10.7	OrientPo_	Beacon frame, SN=1248, FN=2, Flags=.....C, BI=72, SSID=iphon
37	05:10.7	OrientPo_	Beacon frame, SN=288, FN=1, Flags=.....C, BI=128, SSID=kamf
40	05:10.7	OrientPo_	Beacon frame, SN=1280, FN=0, Flags=.....C, BI=120, SSID=Baw SER
41	05:10.7	OrientPo_	Beacon frame, SN=2976, FN=13, Flags=.....C, BI=103, SSID=CITI L
42	05:10.7	OrientPo_	Beacon frame, SN=3856, FN=13, Flags=.....C, BI=74, SSID=Eurc el_16
43	05:10.7	OrientPo_	Beacon frame, SN=1200, FN=7, Flags=.....C, BI=103, SSID=Hote al-KL
44	05:10.7	OrientPo_	Beacon frame, SN=4064, FN=6, Flags=.....C, BI=106, SSID=Iphon
47	05:10.7	OrientPo_	Beacon frame, SN=3616, FN=14, Flags=.....C, BI=138, SSID=Joh
48	05:10.8	OrientPo_	Beacon frame, SN=704, FN=14, Flags=.....C, BI=109, SSID=Kama
49	05:10.8	OrientPo_	Beacon frame, SN=1232, FN=12, Flags=.....C, BI=59, SSID=Park

Figure 2: Forge beacon frames

3.2. The legitimate probes and forge probes

There are two types of probes packet called a probe request and probe response. Probe request is sent by a client to the intended AP and probe response is a reply from the AP back to the client. Probe response can be manipulated with the karma-manna attacks. Karma attack listens to the direct probe request and response to the client with probe response as an impersonation of the real AP. From the result of preliminary experiments, 1917 packets of probe request and 6417 of probe response were captured, representing only 6% of the whole captured packets and 32% of probe request packets were not direct and without any published SSID values as depicted on Table 2. Therefore, 68% of them were vulnerable to karma attacks because it advertised the value of requested SSIDs. Since Karma has been enhanced with Manna, the other 32% should also be exploited.

Table 2: Probe request

Probes	Total packets	Direct Request.	Broadcast Request
Probes-request	1917	1291	626

A legitimate AP would send probe response after receiving the probe request, taking around 10ms [9]. An AP can often send a probe response to many clients with the same SSID. If the AP sends probe response to many clients with two or more different SSIDs, then it might be a forged packet, generated by karma-manna attacks. Figure 3 shows a forge probe response and Figure 4 shows a legitimate probe response.

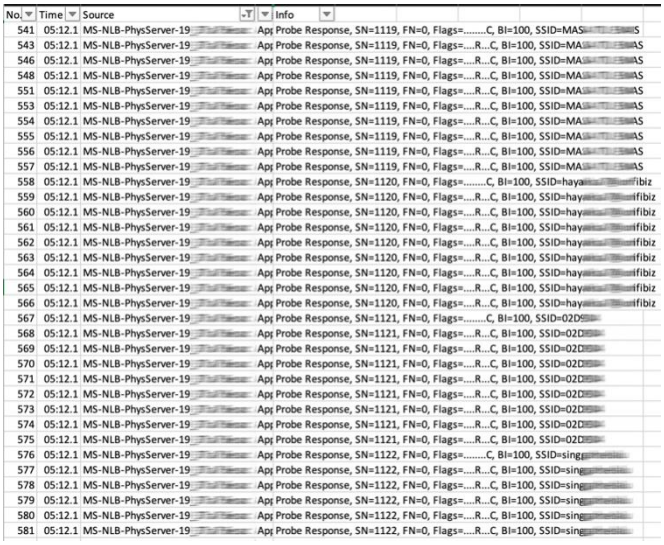

Figure 3: Forge probe response

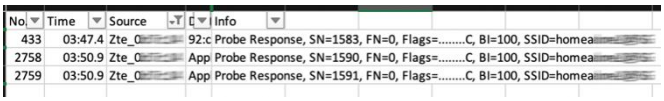

Figure 4: Legitimate probe response

3.3. The impact of karma-manna attacks

From the previous discussion, karma-manna attack is an initial stage before MiTM takes place and it is a crucial stage of APs and clients association. Once a victim is on the adversary network, the MiTM attacks will be launched such as Session hijacking, DNS redirection, javascript injection and cookies sniffing which are the examples of attacks contributed by MiTM. These attacks are known to be able to steal the cookies information and gain the protected area even though the client is in the Wi-Fi Protected Access (WPA) network [19].

4. PROPOSED SOLUTION

We intend to detect and prevent karma-manna attack in WLAN from a client perspective without any administrator intervention support. In this section, the proposed design, requirement, architecture and detection methods are presented.

A. Design Requirements

DARMA is based on client-side detection, and it should fulfil these requirements.

1) The detection can be deployed of any wireless client and do not need any support from the administrator of the WLAN.
2) The solutions do not need any firmware or driver modification neither from the client nor AP.
3) It must be compatible and can be running on most of the 802.11 networks.

B. Architecture Overview

The proposed architecture has four layers of processes which are listening, detection, confirmation and prevention as illustrated in Figure 5. A monitoring phase was in the first layer, where beacons and probes response were monitored. At this point, a preliminary detection was labelled as BSSID Karma List 1 (BKL1). Then, two kinds of detection known as BKL2 and BKL3 were in the second layer. Next, the verification and confirmation, which was known as BKL4, were listed in the third layer. Lastly, the prevention layer launched the countermeasure. The details of the proposed design are as follows.

1) **Listen and monitoring.** The initial setup should set the wireless device to be able to sniff management frames of the 802.11. Thus, the wireless device would be set to the monitor mode. Then we listened on beacons and probe response packets. Afterwards, we listed out all BSSID of the beacons and sorted them out into two categories; BSSID with encryption and BSSID with no encryption. In the meantime, we also listed out all BSSIDs in the probe response. The comparison between the list of BSSID in probe response, and beacons BSSID with no encryption would get the BKL1. The results of BKL1 comprised BSSID in probe response did not exist in BSSID with no encryption in beacons list. Accordingly, in this layer, we had the first suggested detection. The algorithm for BKL1 is illustrated in Figure 6.

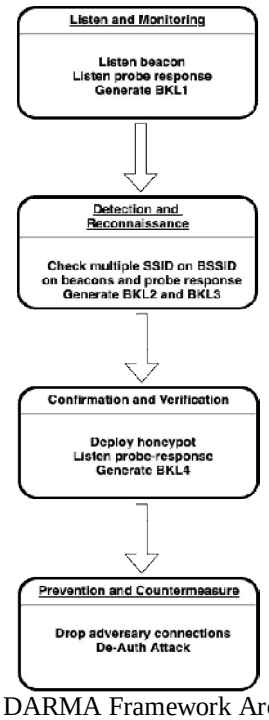

Figure 5: DARMA Framework Architecture

2) **Detection and reconnaissance.**This stage comprised two elements;the first was to examine beacons frame where there were BSSID with multiple SSID or more than two. The list of detection results was known as BKL2. The second was to examine probe response to determine if there is any BSSID that has more than 2 SSIDs. AP should normally have 1 or 2 SSIDs to broadcast. The list of detection was known as BKL3. The algorithms for BKL2 and BKL3 are illustrated in Figure 7.

3) **Confirmation and verification.** In this layer, a honeypot was deployed where forge probe request was generated with uniquemultiple SSIDs.Then, the probe response was actively scanned. If BSSID was responding to our request, then, we listed it out and named it as BSSID Karma List 4 (BKL4). The details of the pseudo-codes are shown in Figure 8.

4) **Prevention and countermeasure.**In this layer, the adversary connection was halted, and the clients would get notification of alert about the attacks. Besides, we also generated the de-authentication packet and sent it to the adversary BSSID and disconnected the fake AP to all current connections.

```
BEGIN
IF packet type is "management" AND subtype is "beacons"
THEN
append beacons_with_encryption.list with BSSID & SSID
append beacons_no_encryption.list with BSSID & SSID
ELSE
IF packet type is "management" AND subtype is "probe response"
THEN append probe-response.list with BSSID & SSID
IF BSSID & SSID in probe-response.list NOT IN
beacons_no_encryption.list
append BKL1
END
```

Figure 6: Pseudo code for BKL1

```
BEGIN
IF packet type is "management" AND subtype is "beacons"
AND
IF BSSID have 2 ≥ SSID
THEN append BKL2
else
IF packet type is "management" AND subtype is "probe response"
AND
IF BSSID have 2 ≥ SSID
THEN append BKL3
END
```

Figure 7: Pseudo code for BKL2 and BKL3

```
BEGIN
ssid <-- setRandomSSID()
sendProbeRequest(ssid)
IF receivePacket.type == "beacon" OR "probe response"
THEN
IF receivePacket.ssid == ssid
THEN append BKL4
END
```

Figure 8: Pseudo code for BKL4

C. The weight of Detection

From the architecture, we had four lists of suspected BSSID; one list from the early stage, two from detection and one from the confirmation stage. All these detection results had their respective severity where for BKL1 we gave it the weight of 1, BKL2 and BKL3 with the weight of 2 and BKL4 the highest severity of 3. The calculation of detection is shown in Table3. The value of *N* should be 0 or 1, for those that exist or do not exist. The highest total weight would be the highest number in the karma blacklist.

Table 3: Weight of detection

	BKL1	BKL2	BKL3	BKL4	Total Weight
$BSSID_N$	*N(1)*	*N(2)*	*N(2)*	*N(3)*	*N(1) + N (2) + N (2) + N (3)*

The justification of each severity weight was based on the detection algorithm. The first list of BKL1 assumed that adversary only sent a karma attack without manna. Thus, the fake beacons should not be broadcasted before the probe response was sent. Hence, the value is one that was adequate for the severity. The algorithms of BKL2 and BKL3 were based on current behaviours of both packets of beacons and probe response where it was irregular for an AP to have too many SSIDs. Therefore, the severity of 2 for BKL2 and BKL3 are sufficient. Lastly, BKL4 was the list where the adversary BSSID had been confirmed by the running honeypot. The SSID comprised 32 characters and 7-bits ASCII, and out of 128 characters, 94 were printable. The probability of the random unique SSID was the same with the current one, or PNL SSID was too low. Hence, the severity of 3 was appropriate.

5. EXPERIMENT AND EVALUATION

The DARMA was implemented by using Raspberry Pi 4 and python as the primary programming languages for the development. The raspberry pi acted as an IDS/IPS and also a gateway to connect to any wireless hotspot as illustrated in Fig.9. The operating system used was Raspbian Buster and RaspAP[26] as a gateway. Before running the code, the user should set the wireless device to the monitor mode by using Airmon-ng from Aircrack-suite [27]. Scapy[28] library was also utilized for the python to parse information from dot11.

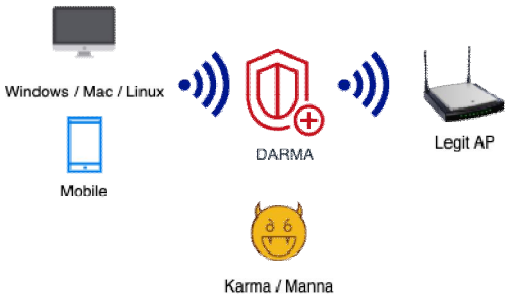

Figure 9: DARMA attack scenario

Two experiments were conducted namely WLAN with no attacks and WLAN with karma-manna attacks. These two experiments were also simulated in different locations and capacities of users.

5.1 Experiment with no attacks

The main objective of this experiment was to get the density of beacons frames and probes response packets from all captured packets. Besides, we also observed if there were packets that had SSID information for more than 2 with particular BSSID. To get more data and good results, these experiments were conducted in three different areas. The first area (location 1) was in a small office that had around 4 APs and ten clients. The second area (location 2) was at a cafeteria with an estimation of 100-200 client per time. Lastly, the experiment was conducted in the public area in a shopping complex (location 3). Tables 4 - 6 show the results of total packets captured by each location and frame.

Table 4: Location 1 no attack – Small Office

Frames	Packets	Density Percentage
Beacons	12090	9%
Probe Response	269	0.2%
Probe Request	1208	0.9%
Others	120765	89.9%
Total	134333	

Table 5: Location 2 no attack – Cafeteria

Frames	Packets	Density Percentage
Beacons	8158	5.6%
Probe Response	584	0.4%
Probe Request	728	0.5%
Others	136221	93.5%
Total	145691	

Table 6: Location 3 no attack – Shopping Complex

Frames	Packets	Density Percentage
Beacons	17189	7.7%
Probe Response	11608	5.2%
Probe Request	4018	1.8%
Others	190422	85.3%
Total	223238	

5.2 Experiment with karma-manna attacks

For this experiment, we launched an attack by using a hardware called wireless pineapple tetra. The main program of this tool was called Hostapd-mana[29]. As per experiment with no attack, we also conducted this experiment in the same area, which is a small office, cafeteria and shopping complex. Tables7 - 9 show the results of the captured packets. For ease of comparison, the total captured packets were similar to experiments with no attacks.

Table 7: Location 1 with attack – Small Office

Frames	Packets	Density Percentage
Beacons	89610	66.7%
Probe Response	6583	4.9%
Probe Request	1477	1.1%
Others	36677	27.3%
Total	134349	

Table 8: Location 2 with attack – Cafeteria

Frames	Packets	Density Percentage
Beacons	94997	65.2%
Probe Response	6848	4.7%
Probe Request	1311	0.9%
Others	42399	29.1%
Total	145701	

Table 9: Location 3 with attack – Shopping Complex

Frames	Packets	Density Percentage
Beacons	136854	61.3%
Probe Response	10046	4.5%
Probe Request	2902	1.3%
Others	73450	32.9%
Total	223253	

5.3 Analysis of the experiments

The first analysis was to correlate the packets by each subtype frame; beacons, probe-response and probe-request. The Pearson Correlation was used to calculate the relationship between each frame and a different location. The formula is (1):

$$r = \frac{1}{n-1} \sum \frac{(x_i - \overline{X})(y_i - \overline{Y})}{s_x s_y} \quad (1)$$

Pearson Correlation only had two input variables, hence, we did correlate location 1 with location 2 and location 2 with location 3. For the experiments with no attack, the value or *r* for location 1 and location 2 was 0.9992353 and the value or *r* for location 2 and location 3 was 0.9993671. Likewise, the value of *r* in location 1 and 2 was 0.99911177 and the value or *r* for location 2 and location 3 was 0.99540809. The results showed that the value of *r* was near to the value of 1; thus, it was perfectly linearly related as depicted in Figure 10-12. What can we conclude here is the density of beacons, probe response and probe request from the total of packets are likely linear with a different WLAN and areas.

Furthermore, we observed that beacon frames were too high when the attacks were running as a result of the manna attack that enables Loud Mode. Once it hears any SSID on vulnerable clients, it will impersonate all the SSIDs and send as many beacons; perhaps there are victims to be connected to

the rogue AP. Thus, this is the most significant dissimilarity of the regular packets and attacked packets. Besides, there was also a significant increase of probe response, but it was not as high as the beacons. In the no attack packets, the correlation of the probe response from location 1 and location 2 to location 3 was quite low because location 3 was a crowded area with a high volume of clients and APs.

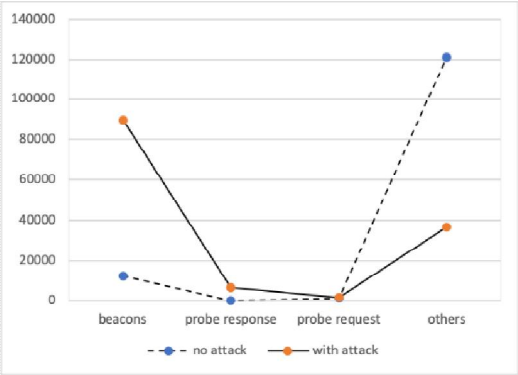

Figure 10: Location 1 – Office

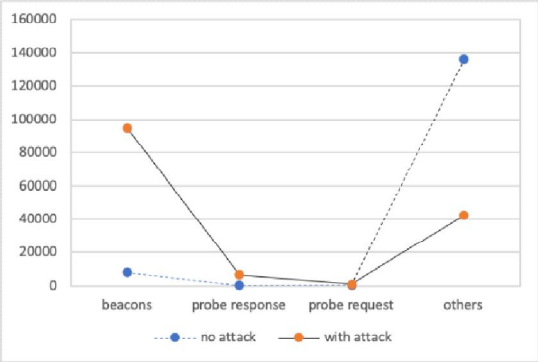

Figure 11: Location 2 – Cafeteria

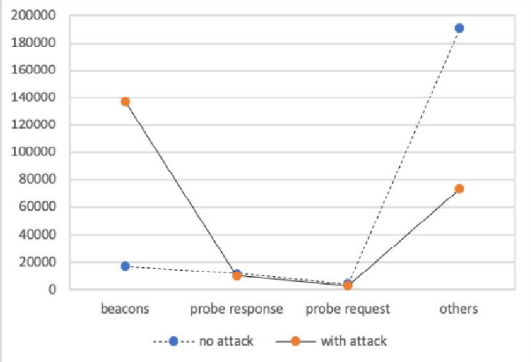

Figure 12: Location 3 – Shopping Complex

5.4. Evaluation of the DARMA

The DARMA evaluation was implemented within two categories. For the first testbed, DARMA was deployed in our dedicated gateway and IPS/IDS hosted in raspberry pi. In the second testbed, DARMA was directly installed and run on the client by using the Ubuntu Linux operating system. Both testbeds need an additional wireless interface for the monitor mode settings. In terms of notification and alert to the clients, DARMA uses Growl Network Transport Protocol (GNTP) [30]. Growl supports multiplatform of clients; hence, all clients can receive any alert from DARMA by using growl client respective of client operating system. Figure 13 shows the flow diagram of the functionality of DARMA in action. To precisely listen and monitor, we used the same method as [18], where DARMA performed as a channel hop to every channel from 1 to 14 to ensure that every packet on the air would be captured for reconnaissance.

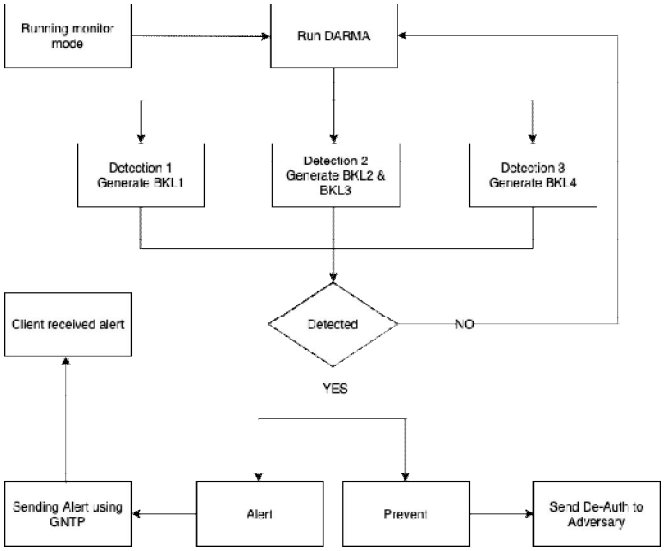

Figure 13: DARMA Framework against Karma Manna Attack

Instead of measuring the real-time behaviour of the packets, the effectiveness of DARMA detection is also recorded. Even though 4 algorithms of detection are executed, the performance of DARMA is still reliable. Besides, DARMA is not relying on any training data; thus, it will have less overhead.

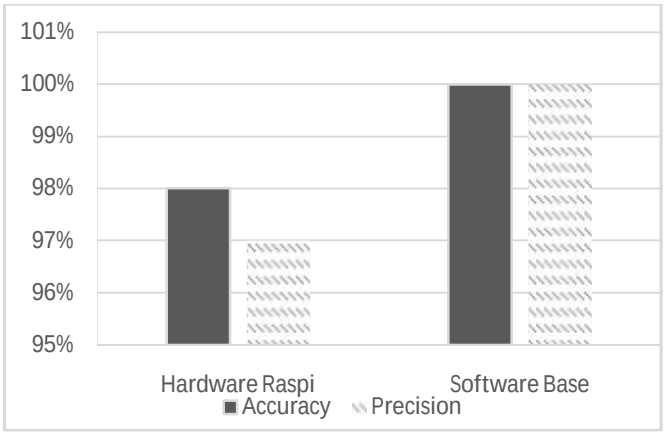

Figure 14: Accuracy and Precision comparison

Figure 14 shows the comparison between DARMA running on Raspberry Pi and running standalone on the client computer. The results show a stunning detection for both testbeds. In terms of dedicated base, the accuracy and precision are slightly less than the software base. It is because of the overhead resources of the hardware used.

Table 10: Detection Hits by algorithms

Time	BKL1 Hit Count	BKL2& BKL3 Hit Count	BKL4 Hit Count
5 s	9	14	0
10 s	17	24	0
20 s	28	39	1
30 s	54	87	3
1 min	78	109	15

Table 10 shows the detection hits categorized by the detection of algorithms. The experiments have been conducted with concurrent and continuous attacks from hardware base karma-manna attack by using Wireless Pineapple and software base hostapd-mana on ubuntu 18.04 workstation. As a result, BKL1 and BKL2 had the higher hit of detection than BKL3 because the algorithm of BKL1 and BKL2 just listens with current packets on the air. Contrarily, BKL3 needs to generate a random SSID first then listens to the packets of the response.

5.5 Limitation of DARMA

Even though the detection shows remarkable results in detecting karma-manna attacks, there are some limitations that arise. There are 14 channels in the Wi-Fi network, and most of the selected Wi-Fi channels are chosen with the best priority by the router. To optimize the DARMA detection, it needs to jump to all channels and listen for the clients. Channel hopping would generate frames lost [31], and it might reduce the performance of the DARMA.

Another limitation is, DARMA needs a dedicated wireless network card to be operational. For the DARMA with software base, it needs to be installed directly to the clients; thus, the clients might not be able to use the current wireless card for other usages because it will not work simultaneously for the monitoring traffic in WLANs. Realistically, the best option of DARMA is to deploy dedicated on specialised hardware such as raspberry pi which has two wireless network cards.

6. CONCLUSION

In conclusion, this study has developed a new framework for detecting and preventing karma-manna attacks. The multi detection methods make this proposed solution accurate and precise. In the same way, our solution is to prevent Rogue AP and also Evil Twin AP because karma-manna is an initial step before those adversaries begin the attacks. On top of that, DARMA solution is easy to implement and can be deployed from the client-side. In future work, we will conduct further research on channel hopping frames lost while detecting karma-manna. Besides, a virtual wireless card can run with monitoring mode.

ACKNOWLEDGEMENT

This research was supported by the Research Management Institute, UniversitiTeknologi MARA and registered under the Research Acculturation Grant Scheme (RAGS) #600-RMI/RAGS 5/3 (017/2017) by the Ministry of Education Malaysia.

REFERENCES

1. L. Silver and S. Cornibert.**Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally,***Pew Research Center*, 2019. https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/.
2. R. Ruslan, A. H. Mohd Nor, R. Saian, M. H. Omar, and M. Manaf.**Performance evaluation of Wi-Fi and White-Fi : Simulation approach,**in *Proceedings - 2016 UKSim-AMSS 18th International Conference on Computer Modelling and Simulation, UKSim 2016*, pp. 343–346, 2016. https://doi.org/10.1109/UKSim.2016.38
3. N. Baharudin, F. H. M. Ali, M. Y. Darus, and N. Awang. **Wireless intruder detection system (WIDS) in detecting de-authentication and disassociation attacks in IEEE 802.11,** in*2015 5th International Conference on IT Convergence and Security, ICITCS 2015 - Proceedings*, pp. 1–5, 2015. https://doi.org/10.1109/ICITCS.2015.7293037
4. M. A. Abdullah, B. M. Alsolami, H. M. Alyahya, and M. H. Alotibi.**Daniel of service attack detection using classification techniques in wsns,***International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 1, pp. 266–272, 2019. https://doi.org/10.30534/ijatcse/2019/4781.12019
5. M. Azahari Mohd Yusof, F. Hani Mohd Ali, and M. Yusof Darus. **Detection and Defense Algorithms of Different Types of DDoS Attacks,***International Journal of Engineering and Technology*, vol. 9, no. 5, pp. 410–444, 2018. https://doi.org/10.7763/IJET.2017.V9.1008
6. H. A. Noman, S. M. Abdullah, and H. I. Mohammed.**An Automated Approach to Detect Deauthentication and Disassociation Dos Attacks on Wireless 802 . 11 Networks,***IJCSI International Journal of Computer Science Issues*, vol. 12, no. 4, pp. 107–112, 2015.
7. M. A. Elsadig, A. Altigani, and M. A. A. Baraka, **Security issues and challenges on wireless sensor networks,***International Journal of Advanced Trends in*

Computer Science and Engineering, vol. 8, no. 4, pp. 1551–1559, 2019. https://doi.org/10.30534/ijatcse/2019/78842019

8. S. M. Günther, M. Leclaire, J. Michaelis, and G. Carle. **Analysis of injection capabilities and media access of IEEE 802.11 hardware in monitor mode,***IEEE/IFIP NOMS 2014 - IEEE/IFIP Network Operations and Management Symposium: Management in a Software Defined World*, 2014.
9. X. Liu, J. Wen, S. Tang, J. Cao, and J. Shen. **City-Hunter: Hunting Smartphones in Urban Areas,**in *Proceedings - International Conference on Distributed Computing Systems*, pp. 162–171, 2017. https://doi.org/10.1109/ICDCS.2017.148
10. D. White, **Karma Manna Attacks.** https://github.com/sensepost/hostapd-mana/wiki/KARMA---MANA-Attack-Theory.
11. **Known Beacons Attack,** [Online]. Available: https://census-labs.com/news/2018/02/01/known-beacons-attack-34c3/.
12. S. S. Kumar and K. Kulothungan. **An Anomaly Behavior based Detection and Prevention of DoS Attack in IoT Environment,** in*2017 9th International Conference on Advanced Computing, ICoAC 2017*, pp. 287–292, 2018. https://doi.org/10.1109/ICoAC.2017.8441322
13. R. Gonçalves, M. E. Correia, and P. Brandão. **A flexible framework for rogue access point detection,** in *ICETE 2018 - Proceedings of the 15th International Joint Conference on e-Business and Telecommunications*, vol. 2, pp. 466–471, 2018.
14. 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*, vol. 25, no. 2, pp. 130–145, 2018. https://doi.org/10.1007/s10776-018-0396-1
15. Q. Lu, H. Qu, Y. Zhuang, X. J. Lin, and Y. Ouyang. **Client-side evil twin attacks detection using statistical characteristics of 802.11 data frames,***IEICE Transactions on Information and Systems*, vol. E101D, no. 10, pp. 2465–2473, 2018.
16. L. Ma, A. Y. Teymorian, and X. Cheng. **A hybrid rogue access point protection framework for commodity Wi-Fi networks,** in*Proceedings - IEEE INFOCOM*, pp. 1894–1902, 2008.
17. 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, no. 3, pp. 449–462, 2010. https://doi.org/10.1109/TMC.2009.145
18. O. Nakhila and C. Zou. **User-side Wi-Fi evil twin attack detection using random wireless channel monitoring,** in*Proceedings - IEEE Military Communications Conference MILCOM*, pp. 1243–1248, 2016.
19. H. Mustafa and W. Xu. **CETAD: Detecting evil twin access point attacks in wireless hotspots,** in*2014 IEEE Conference on Communications and Network Security, CNS 2014*, pp. 238–246, 2014. https://doi.org/10.1109/CNS.2014.6997491
20. F. H. Hsu, C. S. Wang, Y. L. Hsu, Y. P. Cheng, and Y. H. Hsneh. **A client-side detection mechanism for evil twins,***Computers and Electrical Engineering*, vol. 59, pp. 76–85, 2017.
21. M. Korcak, J. Lamer, and F. Jakab. **Intrusion Prevention/Intrusion Detection System (IPS/IDS) for Wifi Networks,***International journal of Computer Networks & Communications*, vol. 6, no. 4, pp. 77–89, 2014. https://doi.org/10.5121/ijcnc.2014.6407
22. Hak5,**WiFi Pineapple auditing platform,** 2017. https://wifipineapple.com.
23. M. I. Mohd Saad, K. Abd Jalil, and M. Manaf. **Anonymous authentication against man-in-the-middle attack,***Journal of Telecommunication, Electronic and Computer Engineering*, vol. 9, no. 2–4, pp. 149–153, 2017.
24. J. Freudiger. **Short: How talkative is your mobile device? An experimental study of Wi-Fi probe requests,** in *Proceedings of the 8th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec 2015*, 2015. https://doi.org/10.1145/2766498.2766517
25. K. A. Jalil, N. S. K. Bashah, and M. H. Naim. **A new technique for protecting server against MAC spoofing via software attestation,***Advanced Science Letters*, vol. 21, no. 10, pp. 3019–3023,2015.
26. B. Zimmerman.**RaspAP - WebGui.**https://raspap.com/.
27. Aircrack-ng.**Aircrack-ng is a complete suite of tools to assess WiFi network security,***09-Dic-2018*, 2018. https://www.aircrack-ng.org/.
28. P. Biondi. **Scapy - Packet crafting for Python2 and Python3,***Scapy*, 2018, [Online]. Available: https://scapy.net/.
29. Sensepost. **hostapd-mana,** https://w1f1.net/.
30. Growl. **Growl Network Transport Protocol,** http://growl.info/.
31. H. Alipour, Y. B. Al-Nashif, P. Satam, and S. Hariri.**Wireless Anomaly Detection Based on IEEE 802.11 Behavior Analysis,***IEEE Transactions on Information Forensics and Security*, vol. 10, no. 10, pp. 2158–2170, 2015. https://doi.org/10.1109/TIFS.2015.2433898