An Assessment of Wi-Fi 5 and 6 and its Effects on Location Tracking

Salman Al Musalam, Zeinab Rezaeifar
University of the West of England
UK

Abstract

Location tracking is a privacy attack within the Wi-Fi protocol that recently gained the attention of researchers. Wi-Fi-enabled devices, such as smartphones and watches, constantly broadcast probe requests to connect to an Access Point. These requests contain valuable information, such as MAC addresses, that can be used to identify the individuals. Furthermore, these requests are not encrypted where it can get captured using off-the-shelf hardware and publicly available software. To tackle this problem, MAC address randomization was introduced in 2018. Limited research has been done in this area and most of it has been implemented using Wi-Fi 5, with no research done in the newly released Wi-Fi 6. This project investigates the effect of location tracking in Wi-Fi 6 compared to Wi-Fi 5, outlining the changes within Wi-Fi 6. The investigation is done through a series of experiments in two different environments (Wi-Fi 5 and 6) through two approaches; passive and active using an iOS and Android device. In addition, the effect of MAC address randomization is also investigated in Wi-Fi 5 and 6. Data is collected using a set of tools in the two different approaches, the effectiveness of location tracking in both environments is compared and the strengths and limitations of the two approaches for location tracking are outlined. The main findings show that location tracking in Wi-Fi 6 is still achievable when compared with Wi-Fi 5, but the accuracy and certainty of identifying devices are lower due to new features within Wi-Fi 6.

1. Introduction

Smartphones have a huge impact on our lives, as most of us use them to carry out daily tasks. With that, people tend to carry their smartphones with them most of the time. Such devices support a wide range of wireless communications such as Bluetooth, 4G/5G, and Wi-Fi where they are connected to a pairing device, a cell tower, or an access point. This makes mobile devices vulnerable to a wide range of attacks, especially privacy attacks. One privacy attack that has gained the attention of many researchers recently is location tracking using Wi-Fi through Wi-Fi-enabled devices. This was feasible through probe requests that these devices broadcast to close-range Access Points (APs) for discovery and connection. Those requests contain sensitive information such as the MAC address of the device, the Signal Strength (RSSI), and the data rate [3]. Moreover, these frames are constantly broadcasted in plain text where they can easily get sniffed and captured. With the aid of some publicly available resources, threat actors can use this type of information to locate individuals by maliciously taking advantage of the frames that are used for a different purpose. Limited papers have been published regarding this privacy issue within Wi-Fi and no experimental research was done with Wi-Fi 6. Currently, no solutions have been addressed with regard to sniffing probe requests, apart from MAC address randomization.

The following sections make up the remainder of the paper. Section 2 summarizes recent research done within the area of location tracking; this includes an overview of the research done, the methods that have been used, and how it has been implemented and evaluated. Followed by their strengths and limitations. Section 3 covers the methodology used and the experiment, outlining the two main approaches and the set-up of the artefact is discussed. Section 4 displays the results and observations that have been obtained from the experiments. Section 5 discusses the results that have been obtained in the Methodology and Experiment chapter. Addressing the limitations and strengths of the approaches used, tools, and techniques that have been used. Also, additional behaviors of devices that have been observed during the experiments are outlined and discussed. In the final section, the conclusion of this project is drawn outlining the main findings that have been observed.

2. Literature Review

Research done within this field is limited as only a few papers have been published. Most of these papers cover Wi-Fi 5 and other wireless protocols such as Bluetooth, RIFD, and NFC. One paper published by Ramezanpour, K., Jagannath, J. and Jagannath, A. outlined the privacy vulnerabilities in 5/6G and Wi-Fi 6 [8]. Regarding Wi-Fi 6, they outlined several attacks that are vulnerable to WPA3 such as downgrade attacks, where the protocol is downgraded to WPA2 and exploiting its weakness. This is in addition to rogue APs, DoS attacks, and key reinstallation attacks. The paper failed on how Wi-Fi 6 is vulnerable to other privacy attacks, such as

 | DOI: 10.20533/ijrfidsc.2046.3715.2023.0026

location tracking. However, it talked about how probe requests and AP beacons are not encrypted, but it did not mention how this vulnerability can be used to exploit other attacks.

Dagelic, Perkovic and Cagalj carried out a study where they gathered location-related data over four years, and outlined the approach and techniques that can be used to localize individuals by gathering probe requests and identifying MAC addresses [2]. They have summarized that location tracking depends on three factors: the previous location of the individual, current localization, and dynamic localization. Although they explained how to use Open-Source tools to find APs which leads to discovering the user's PNL (Preferred Network List), taking the advantage of signal strength which reveals an individual's position, and monitoring traffic for probe requests to localize individuals. This paper has explained a general approach to evade privacy location, however it did not mention other methods such as the use of rogue APs (or other hardware such as Wi-Fi pineapple). In addition, their experiment was carried out using only the 2.4 GHz with no regard to the 5 GHz and carried out in Wi-Fi 5.

Rutermann, Benabbas and Nicklas proposed a method called Protective Mode Monitoring (PMM) to identify devices connected to an AP, by keeping an eye on frames other than probe requests [9]. It makes use of the so-called protected mode, which guards against problems with data frame transfers in networks operating in both High Throughput (HT) and Very High Throughput (VHT) modes in mixed environments. The device MAC will always be present in either the source or destination of a Request-To-Send (RTS) message in the RTS-CTS (clear-to-send)-ACK handshake since the exchange of information regarding VHT mode support can be started by either the AP or the client. RTS messages appear to be sent often enough to track locations in real-time. Their findings shows that monitoring frames such as CTS, RTS, and ACK apart from probe requests contain MAC addresses that can be used to track mobile devices.

A detection method called Sherlock proposed by Oliveira *et al.* gives an approximate population of the number of people in a certain area by detecting the presence of probe requests using a number of different interfaces [5]. Their solution monitors through the Wi-Fi channels 1-13; where it switches to a different channel every three seconds collecting data in each channel. Their method is evaluated by comparing the actual number of people in a given area with the estimated number of people generated by Sherlock.

The results of Sherlock were quite close to the actual number. Moreover, it has been compared with different algorithms where it outperformed them. However, not all factors were considered; individuals may be carrying more than one device, not all data has been collected or identified, and not all devices have their Wi-Fi enabled.

Li *et al.*conducted an analysis of the effect of channel hopping on Wi-Fi in collecting the number of probe requests that can be used to track devices [4]. Their investigation consists of a series of experiments by which setting different AP configurations, different channel hopping duration as well as the performance of Raspberry Pi and LoPy4 in collecting probes. Their work was evaluated using analysis of variance (ANOVA) to measure each test. Their investigation concluded that factors such as number of APs that are in a certain area, the RSSI, and the number of devices that are in the area. Furthermore, they extended their research to find the effect of MAC address randomization, where they deduced that the number of packets from devices with the real MAC address is much higher than those that are randomized. A limitation addressed in this research is that the experiment was only carried out on the 2.4 GHz, and also the fact that individuals could carry two or more devices with them, and some devices could have more than one Wi-Fi adaptor in them.

Prasad *et al.* investigated the effect of passive scanning in an on-the-move mode (OTM) compared with static (STT) mode, in addition to the use of features in packets that aid in device localization apart from beacons and probe requests [7]. Their experiment is based on collecting packets in each Wi-Fi channel (1-13) using channel hopping with different intervals between hopping. The experiment is conducted twice; one in OTM mode and the other in STT mode. The comparison between the two was based on the number of beacons, probe requests, RSSI values, and packets. The results show that the number of packets, devices, and APs in OTM mode is higher than those in SST, and SST had only a higher number of data packets than OTM. Regarding the RSSI strength, both OTM and SST showed similar results. This research suggests that passive scanning using OTM proved to be a better starting point for further research in this area, however, their results may not be very accurate due to the limitation of the equipment used. Also, the study conducted focused only on 2.4GHz with no consideration for 5GHz.

Abedi and Vasisht developed a low-cost solution that can be implemented on a drone to localize individuals using Wi-Fi called Wi-Peep [1]. The solution consists of a low-power Wi-Fi module to sniff and capture MAC addresses and a voltage regulator. The solution consists of three stages, and the first stage is to identify the mobile devices through MAC address. This was done by exploiting the weakness of the power-saving mechanism in the Wi-Fi protocol. A fake beacon frame is sent from Wi-Peep to the Wi-Fi devices (where these devices assume that it is from their AP), in return, they will respond by revealing their MAC addresses. The second stage consists of measuring the Time-of-Flight (ToF), by calculating the time elapsed between a

 | DOI: 10.20533/ijrfidsc.2046.3715.2023.0026

packet being sent and receiving an ACK request. The final stage is to localize the target using the derived ToF from the previous step. The authors evaluated their solution by repeating the experiment in different locations and mobility of the devices. Results show that the accuracy of their solution mainly depends on the coverage of the drone, which is related to the RSSI strength.

An experiment carried out by Potortì *et al.* investigated the possibility of tracking individuals indoors using Wi-Fi probes [6]. In their experiment, Wi-Fi probes are captured at regular intervals using FogSense that is placed in a certain area. Features from the probes such as MAC address, RSSI, and timestamp are extracted. The experiment was performed in three different environments with different layouts and room sizes. They evaluated their investigation by comparing the number of MAC addresses the Wi-Fi sensor sniffed, with the actual number of devices present in the room through an interpolation-based approach. Results show localizing individuals is plausible, however the effectiveness and accuracy depends on many factors such as the number of sniffers placed (higher numbers will result in higher accuracy and detection), and the positioning of these sniffers. One limitation of this investigation is that MAC address randomization has been ignored, which could affect the number of probe requests that have been captured, which leads to inaccurate results.

Previous research showed different approaches to using Wi-Fi probe requests and additional features in network traffic, such as null data packets to monitor individuals through their mobile devices. As seen previously, most of them have neglected or did not take MAC address randomization into consideration. Furthermore, most of these experiments have been implemented in Wi-Fi 5 and not Wi-Fi 6. In this research, location tracking using Wi-Fi probe requests in Wi-Fi 6 will be investigated and compared to Wi-Fi 5. This will also cover the effect of MAC address randomization in the newly released Wi-Fi 6..

3. Methodology and Experiment

This section discusses the artefact of the project which consists of a series of experiments, covering the tools, hardware, and software used to build an environment to investigate location tracking in two different environments, comparing the results and outlining the differences. The experiment investigates two matters: the effect of location tracking in Wi-Fi 5 and 6, and the effect of MAC address randomization in Wi-Fi 6. Two separate environments will be built for Wi-Fi 5 and Wi-Fi 6 respectively. The experiments consists of two main approaches that are discussed in details in the 'Methodology' section.

3.1. Methodology

The experiments that took place are broken down into two main categories, active and passive. Passive monitoring consists of capturing traffic and analyzing it without interfering with the traffic itself. On the other hand, active monitoring involves interaction with the traffic itself such as sending data to it. Details of the approaches are discussed below.

3.1.1. Passive monitoring. In passive mode, the network traffic is captured and analyzed passively with no interaction with a target device. This works when a wireless sniffer is in monitor mode listening to inbound and outbound traffic in every Wi-Fi channel. Passive monitoring is widely used for network diagnostics, performance, optimization, and usage. The key benefit of this approach is that network traffic can be obtained without raising any suspicions. From an attacker standpoint and referring to the Cyber Kill Chain (CKC) that is created by Lockheed Martin. Reconnaissance is the first stage in obtaining information about a target which is broken down into passive and active reconnaissance. The drawback of this approach would be the limited amount of traffic captured, the high loss of packet data as well as the time to capture it. This is mainly due to interference with other Wi-Fi channels and signals, and environmental obstacles.

Figure 1 shows the flow chart for the passive approach. The station with the enabled monitor mode will sniff traffic transmitted by the Wi-Fi device that is connected to the AP.

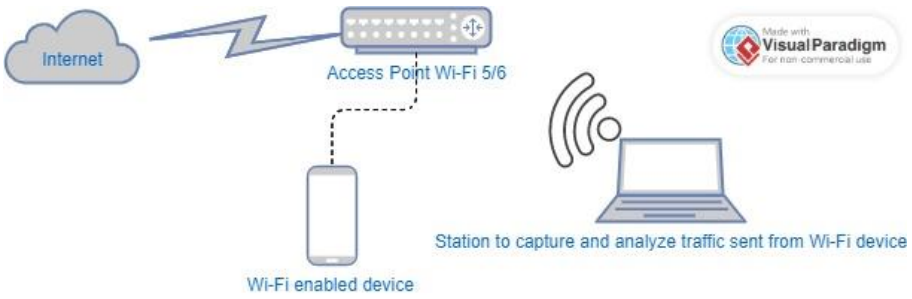

Figure 1. Flow chart for the passive approach

3.1.2. Active monitoring. In active scanning, there is an interaction with the mobile device in which packet requests are sent and awaiting a response. This could be either by sending a request from an AP to a device and waiting for a response, or vice versa. According to studies, this approach is more reliable than passive monitoring as more traffic is captured with a much lower rate of packet data loss, as well as the fact that the time to capture these packets is much faster. Referring to the CKC, active reconnaissance is usually performed after passive once adequate information about the target has been gathered. In this project, the experiments performed to track individuals are carried out from an attacker's point of view, which includes following and implementing the CKC stages. Though the results of active monitoring are better than passive, the main disadvantage of it is that it is more susceptible to detection since there is an interaction with the client.

Figure 2 displays the flow chart for the active approach using Wi-Fi pineapple. The Wi-Fi device is connected the rogue AP (Wi-Fi Pineapple). Traffic is then collected and analyzed through the station.

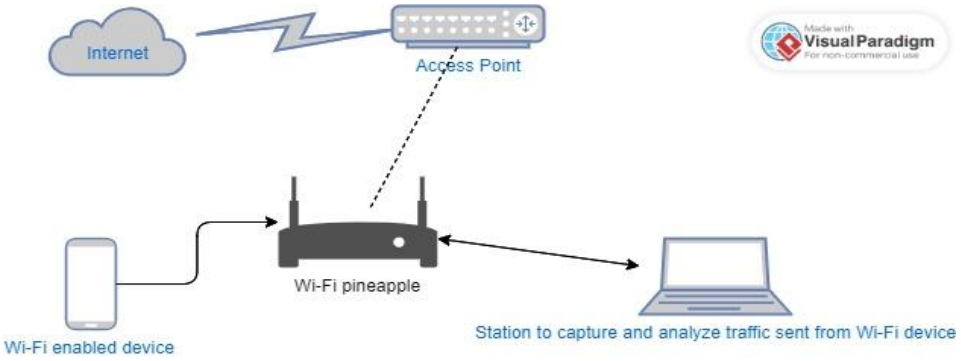

Figure 2. flow chart for the active approach.

3.2. Experiment assumptions

As stated earlier, the experiment is conducted from an attacker's point of view. This includes the use of over-the-shelf hardware and software. In addition, the reconnaissance took place prior to the investigation where the target's whereabouts have been identified (such as workplace and home) and the SSIDs are obtained through WiGLE.

3.3. Experiment set-up

This section will discuss the tools used in this experiment to build a private LAN network. The two main components of this experiment are divided into hardware and software.

3.3.1. Hardware. The hardware tools that have been used as follow:

- Alpha Network – AWUS036ACH USB adaptor
- Alpha Network – AWS036NEH Wi-Fi network Adaptor
- Wi-Fi pineapple Mark VII
- Virgin Media router
- Huawei Wi-Fi AX3
- iPhone XS MAX – iOS 16
- Xiaomi Redmi Note 10S

The second part of the experimental setup is the software, the following are the list of software that have been used.

- Wireshark
- Kismet
- Wifite
- Wi-Fi Pineapple
- Aircrack-ng Suite5

3.4. Experiment metrics

This project is qualitative-based research, metrics used for evaluation and comparison as follow.

- Effectiveness of methods and tools used.
- Effectiveness of the approach taken in identifying the device.
- Ease of use of the tools.
- Ease of use of implementation.
- Number of probe requests collected.
- Probe request rate: calculated by collecting the

 | DOI: 10.20533/ijrfidsc.2046.3715.2023.0026

total amount of requests and dividing by a specific time given.

The limitations and strengths of each method and approach are outlined and discussed in the following chapter.

3.5. Experimental trials

This project consists of eight experiments, six with the passive approach and two with the active.

For the passive, two experiments are done in Wi-Fi 5 with MAC address ON and OFF. Two other similar experiments are carried out with Wi-Fi 6. The next two experiments are carried out with Wi-Fi pineapple with the MAC address ON and OFF respectively.

The active approaches, two experiments are carried out with Wi-Fi pineapple; one with MAC address ON and the other when its OFF. An outline of the experiments is discussed below:

Experiment 1:

- Passive location tracking by monitoring traffic and finding the no. of probe requests, RSSI signal, and MAC address on 2.4 and 5 GHz.
- Carried out on Wi-Fi 5.
- MAC address randomization on target devices is OFF.
- Tools used: Kismet, Wireshark, aircrack-ng.

Experiment 2:

- Passive location tracking by monitoring traffic and finding number of probe requests, RSSI signal, and MAC address on 2.4 and 5 GHz.
- Carried out on Wi-Fi 5.
- MAC address randomization on target devices is ON.
- Tools used: Kismet, Wireshark, aircrack-ng.

Experiment 3:

- Passive location tracking by monitoring traffic and finding number of probe requests, RSSI signal, and MAC address on 2.4 and 5 GHz.
- Carried out on Wi-Fi 6.
- MAC address randomization on target devices is OFF.
- Tools used: Kismet, Wireshark, aircrack-ng.

Experiment 4:

- Passive location tracking by monitoring traffic and finding number of probe requests, RSSI signal, and MAC address on 2.4 and 5 GHz.
- Carried out on Wi-Fi 6.
- MAC address randomization on target devices is ON.
- Tools used: Kismet, Wireshark, aircrack-ng.

Experiment 5:

- Passive location tracking by monitoring traffic and finding number of probe requests, and MAC address on 2.4 and 5 GHz.
- MAC address randomization on target devices is OFF.
- Tools used: Wi-Fi pineapple Mark VII.

Experiment 6:

- Passive location tracking by monitoring traffic and finding number of probe requests, and MAC address on 2.4 and 5 GHz.
- MAC address randomization on target devices is ON.
- Tools used: Wi-Fi pineapple Mark VII.

Experiment 7:

- Active location tracking by monitoring traffic and finding number of probe requests, and MAC address on 2.4 and 5 GHz.
- MAC address randomization on target devices is ON.
- Tools used: Wi-Fi pineapple Mark VII.

Experiment 8:

- Active location tracking by monitoring traffic and finding number of probe requests, and MAC address on 2.4 and 5 GHz.
- MAC address randomization on target devices is OFF.
- Tools used: Wi-Fi pineapple Mark VII.

4. Results

The results of the eight experiments that were discussed in the 'experimental trials' earlier are presented in Figures 3 to 9. Results are broken down into two sections: Passive and Active. The duration for passive and active is around 30 and 15 minutes,

 | DOI: 10.20533/ijrfidsc.2046.3715.2023.0026

respectively, for each device used in each experiment. Results are then displayed accordingly.

4.1. Passive Monitoring

Results for the passive approach are displayed below.

4.1.1. Experiment 1: Wi-Fi 5 with MAC address turned OFF. Figure 3 shows the captured probe request of our iOS device that has been sent as a broadcast address (FF:FF:FF:FF:FF:FF) in Wireshark after setting it up in monitor mode. For ethical and privacy reasons, the traffic has been filtered to show only the MAC address of the target.

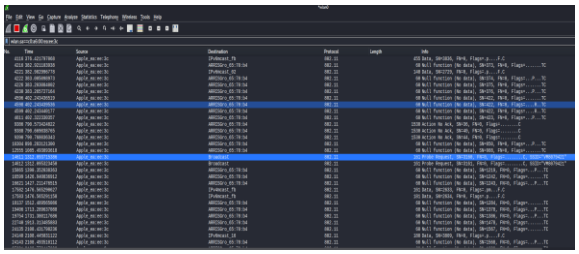

Figure 3. probe request displayed for the Apple device.

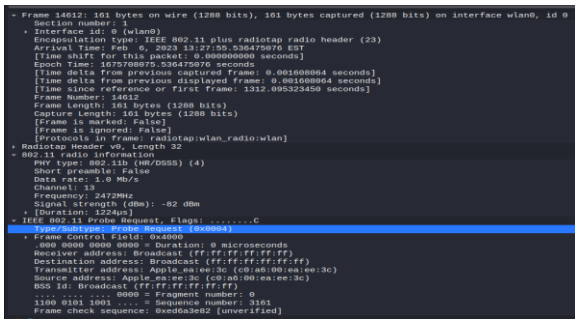

Figure 4. Details of the Probe requests.

Details of the probe request are displayed in Figure 4, displaying the data rate that the device can handle, the RSSI with a value of -82 dBm which indicates that it is within close range, and the MAC address. In addition, the manufacturer of the device is also displayed.

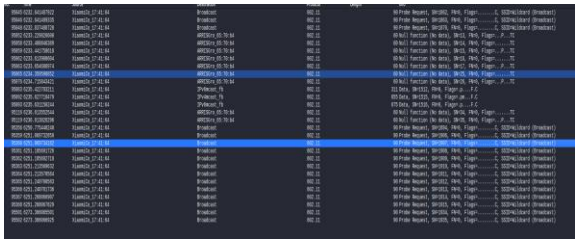

Figure 5. probe requests for the Android device.

The Figure 5 shows the probe requests captured through Wireshark for the Android device running on Xiaomi. Similar to the iOS device, the MAC address has been filtered for privacy.

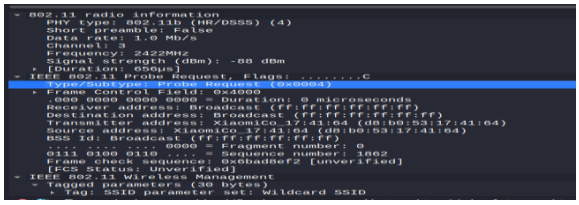

Figure 6. Probe request details of the Android device.

Details of the probe requests are displayed as shown in Figure 6 with an RSSI value of -88 dBm and a data rate of 1Mbs. This is as well as the vendor and MAC address.

Using Kismet on Kali Linux, the devices have been identified as shown in Figure 7. The traffic has been filtered by setting up the SSID of our testing AP, displaying devices within our testing environment.

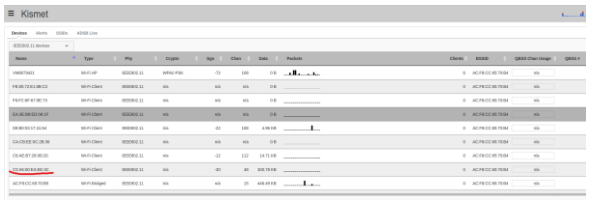

Figure 7. Identifying the iOS device on Kismet.

Details of the iOS device captured are shown in Figure 8. Results display the RSSI strength value of -23 dBm and identified the device's manufacturer. Furthermore, it shows that the device mostly runs on the 5 GHz band.

In Figure 9, the Android device has been identified in Kismet, and its details are displayed; the RSSI value, the manufacturer as well as the frequency it communicates in.

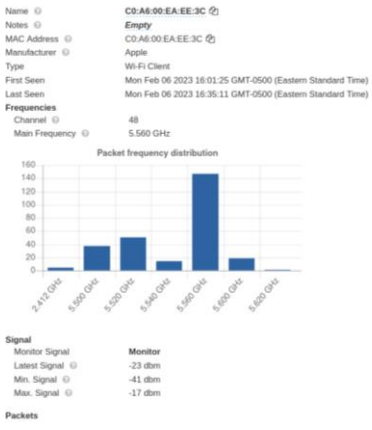

Figure 8. details of the iOS device through Kismet.

 | DOI: 10.20533/ijrfidsc.2046.3715.2023.0026

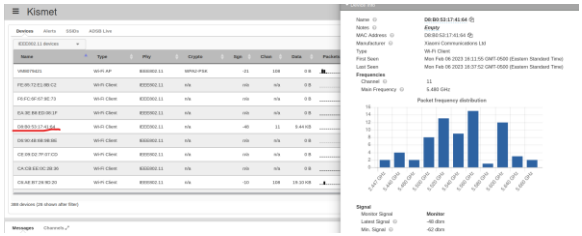

Figure 9. Android device identified, and its details are displayed

4.1.2. Experiment 2: Wi-Fi 5 with MAC address turned ON. *Wireshark* - The MAC address randomization has been enabled in both devices and the traffic has been captured for 30 minutes. The traffic has been analyzed to find probe requests and the device MAC address. However, no data on iOS and Android devices were found.

Kismet - With Kismet, the iOS and Android were located with their randomized MAC address. However, the details of the devices have changed.

4.1.3. Experiment 2: Wi-Fi 6 with MAC address turned OFF. The third experiment was set up in a Wi-Fi 6 environment, with the same monitoring duration of 30. Results are as follows for Wireshark and Kismet.

Wireshark - For the iOS device, no probe request has been detected in Wireshark and the packet transfer data was slower in Wi-Fi 6. For the Android device, probe requests have been detected as shown in figure 31, in addition to other frames such as QoS (Quality of Service).

Kismet - Using Kismet, both devices were detected. However, the duration for the detection varied in both devices. The Android device was detected first and for the iOS, the discovery was not stable like the other device, as the communication keeps on dropping approximately every 3 minutes.

4.1.4. Experiment 4: Wi-Fi 6 with MAC address turned ON. Wireshark - Probe requests have been detected in Wireshark for the iOS device on regular intervals. The number of probe requests captured is higher in Wi-Fi 6, than in Wi-Fi 5. However, the details of the device have changed. For the Android device, no probe requests have been captured. The iOS device has been identified in Kismet after 5 minutes of running the tool, though the device has been detected, its information is changed similar to the previous experiments with MAC address randomization.

Kismet - The Android device has been discovered after the iOS by approximately 3 minutes. An observation that has been made in general with Wi-Fi 6, is that the discovery of the devices is much faster if the user is using his/her phone.

4.1.5. Experiment 5: Passive monitoring with MAC address turned OFF. Using the Wi-Fi pineapple to passively monitor devices through the feature 'Recon'. After 30 minutes of scanning, the Android device was detected around 5 minutes after the scanning has started. The iOS device was detected after around 8 minutes.

4.1.6. Experiment 6: Passive monitoring with MAC address turned ON. With MAC address turned on, the iOS device has been located within the first minutes of scanning. Similar to previous experiments, the device vendor and manufacturer are altered. On the other hand, the Android device appeared later by the end of the scanning duration.

Probe request logging

During the passive scanning experiments on Wi-Fi pineapple with MAC addresses on and off, the device has logged the number of probe requests of our target devices on Wi-Fi 5 and 6. Results of the logging is displayed in the table below after carrying out.

Table 1. no. of probes logged using Wi-Fi pineapple

Device	MAC Address Randomization	No. of probes in Wi-Fi 5	No. of probes in Wi-Fi 6
iOS	OFF	1	4
Android	OFF	57	-
iOS	ON	1	14
Android	ON	108	10

4.2. Active Monitoring

In active monitoring, the test devices have been connected to the Wi-Fi pineapple through the SSID 'test', and probes were monitored for 15 minutes. Both devices have been captured and results are displayed in Table 2 (Experiments 7 and 8: Active monitoring with MAC address turned OFF and ON).

Table 2. Probe requests for active monitoring of both devices

Device	MAC address randomization	No. of probes
iOS	ON	9
Android	ON	1
iOS	OFF	26
Android	OFF	2

5. Discussion

This section discusses the results that have been obtained earlier outlining the differences observed between Wi-Fi 5 and 6, the strengths and limitations

 | DOI: 10.20533/ijrfidsc.2046.3715.2023.0026

of the approaches and tools that have been used. Moreover, the shortcomings and limitations of the experiments are stated.

Passive approach Wi-Fi 5

Main points that have been observed between the behavior of the devices in Wi-Fi 5 with MAC address ON and OFF:

- The Android device sends more probe requests than the iOS device.
- Detection of Android device is faster than iOS in both modes.
- Out of all the off-shelf tools used, Kismet had the best performance in terms of device detection, duration, and ease-of-use.
- With MAC address randomization ON, detection of the devices is slower than when its OFF.
- Device specification changes with randomized MAC address which can make the device difficult to track. However, some features have not been changed such as the frequency and signal strength.

Details of the observations are expressed as follows.

Passive approach in Wi-Fi 5 MAC with address OFF

In general, for passive probe requests and MAC addresses for the iOS and Android devices have been obtained as seen earlier. However, there are slight differences in the duration of detecting between devices in addition to transmission of other packets than probe requests. Through Wireshark, the Android device has sent more probe requests than the iOS device over the experiment duration. The RSSI value was quite similar due to the geographical area of the experiment that took place. An interesting observation that has been noted is that a number of null data frame packets have been captured along with the probe requests. As explained earlier, null data frames sent by mobile devices for power and management purposes to the AP. This observation agrees with research conducted by (Hong, Luo and Chan, 2016), by which different frames can be used to monitor devices. The number of null data frames captured is higher in iOS than the Android device.

Using Kismet, devices were identified much faster than with Wireshark. In addition, manufacturer and vendors of the device have been captured which aids in device localization.

Passive approach in Wi-Fi 5 MAC with address ON

Wireshark failed to detect the iOS and Android devices as a number of probe requests have been captured. This could be due to the limitation within the tool used such as infrequent channel hopping scanning, in addition to scanning in a specific band such as 2.4 or 5 GHz and not both.

On the other hand, Kismet has been able to detect the iOS and Android device. However, it took more time to detect both devices with MAC randomization on, than it was off by around 10 minutes. In terms of device, the Android device have been detected before the iOS with a slight difference of around 3 minutes.

Detection of the devices cannot be very accurate with MAC address randomization on, due to the uncertainty of device in terms of changed device details and the frequent detection. Although, some details have not been changed such as the frequency that the device communicates on and the RSSI value.

Passive approach Wi-Fi 6

The main points observed in Wi-Fi 6 between the devices with MAC address ON and OFF:

- Detection of both devices are slower in Wi-Fi 6 than in Wi-Fi 5.
- For Wi-Fi 6, Kismet has outperformed the rest of the tools in terms of device discovery, duration, and ease-of-use.
- Communication of the devices are not constant as in Wi-Fi 5, as devices disappears and reappear in the logs at regular intervals.
- Device discovery for the Android and iOS is much faster when the user is actively using the phone.

Details of the observations are described below:

Passive approach in Wi-Fi 6 MAC with address OFF

Wireshark has not performed well in general for both devices in terms of device identification and capturing probe requests with MAC address ON. With no detection of device or probe request with the iOS, results are opposite with the Android. One observation made is that the number of null data frames is much higher with the Android device than the probe requests compared with Wi-Fi 5. The low performance could be due to limitations within the tool used.

With Kismet, both devices have been detected. The Android device was detected first which was then briefly followed by the iOS. An interesting observation noted is that during the first 15 minutes of the experiment no detection was found of both devices. The state of the devices was idle, meaning it was not being used. After the 15-minute mark, both devices were used in which both apps and browser were accessed. With that, the detection of the iOS and

 | DOI: 10.20533/ijrfidsc.2046.3715.2023.0026

Android were captured. Furthermore, discovery of the devices was not very stable as it kept appearing and disappearing in the log. One hypothesis for this is that the new Wi-Fi 6 supports TWT, in which the connection with the AP is minimized to increase the power efficiency of the device, in which the communicate at regular intervals.

Passive approach in Wi-Fi 6 MAC with address ON

Unexpected results were found in Wireshark with the iOS device with MAC address ON. Compared with Wi-Fi 5, the number of probe requests detected were much higher in Wi-Fi 6, around 71 probe requests were captured. On the other hand, the Android device has not been identified as no probe requests were captured. Regarding the MAC address randomization, similar results obtained compared with Wi-Fi. However as stated earlier, detection is much faster while the user is active.

Passive scanning with Wi-Fi Pineapple with MAC address ON and OFF

With the 'Recon' feature used, Android device was initially detected with MAC address randomization OFF, where with the MAC address ON, iOS was discovered first. Though the Wi-Fi pineapple supports more features than the other tools used, Kismet still outperforms it in terms of device detection, and duration of the detection.

Based on the results of probe requests in figure 49, a higher number of probes were captured in Wi-Fi 5 than Wi-Fi 6 in general, regardless of whether MAC address randomization is ON or OFF for the Android device, however, for the iOS it was quite the opposite. The probes were logged and viewed through the 'logging' feature in the Wi-Fi Pineapple.

Active scanning with Wi-Fi Pineapple with MAC address ON and OFF

Results obtained from active scanning were quite interesting. The detection is much faster using the active approach as the device connects to the network using the PineAP feature in the Wi-Fi pineapple, the duration was shortened to 15 minutes to observe the behavior of the devices. As both devices were identified, the number of probes have been captured as well. For the iOS device, 9 probe requests have been captured in the first 4 minutes and stayed constant to the end of the experiment, with randomization ON and 26 probes while it was OFF. For the Android device, the number of probes was similar with randomization ON and OFF.

One interesting observation made is when the devices were disconnected from the PineAP, the number of probes logged increased for both devices, but was much higher with the Android. During the first 5 minutes after disconnection, the number of probes jumped from 2 to 72 with MAC address randomization turned OFF, while the increase in iOS was just slightly even with randomization ON. With randomization ON in Android, probe requests increased from 1 to 13 in the first two minutes.

6. Conclusion

This project investigated the effect of a tracking device in Wi-Fi 5 and 6, with the use of use of off-the-shelf tools and hardware, as well as resources that are available online. An Android and an iOS device were used in a series of experiments to monitor and analyze the behavior of the device, and how they differ in the two different environments. Furthermore, the implementation of the MAC address randomization feature in recent mobile OSes has been investigated as well as how effective is it against location tracking.

Two main contributions in this project are the effectiveness of location tracking between Wi-Fi 5 and the newly released Wi-Fi 6. Secondly, the effect of MAC address randomization in location tracking between to the environments. The main findings of this project concluded that mobile tracking in Wi-Fi 6 is still effective, but less feasible due to the new features that the Wi-Fi 6 supports such as TWT. Furthermore, MAC address randomization also makes location tracking a bit ineffective in terms of device identification, however, other features can still be used that have not changed (in regard to Wi-Fi 5 and 6) such as the RSSI signal strength. Moreover, Android devices are more susceptible to being tracked as they have been detected before the iOS, and sent more probe requests than the other device in the majority of the experiments that have taken place. Another unexpected finding found is that both mobile devices sent a large number of probe requests when they are not associated or connected to an AP.

7. References

[1] Abedi, A. and Vasisht, D. (2022). Non-cooperative wi-fi localization & its privacy implications. Proceedings of the 28th Annual International Conference on Mobile Computing And Networking.

[2] Dagelic, A., Perkovic, T. and Cagalj, M. (2019). Location Privacy and Changes in Wi-Fi Probe Request Based Connection Protocols Usage Through Years. 2019 4th International Conference on Smart and Sustainable Technologies (SpliTech).

[3] Hong, H., Luo, C. and Chan, C. (2016). SocialProbe: Understanding Social Interaction Through Passive WiFi Monitoring. Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, pp.94–103.

 | DOI: 10.20533/ijrfidsc.2046.3715.2023.0026

[4] Li, Y., Barthelemy, J., Sun, S., Perez, P. and Moran, B. (2020). A Case Study of Wi-Fi Sniffing Performance Evaluation. IEEE, pp.129224–129235.

[5] Oliveira, L., Schneider, D., De Souza, J. and Shen, W. (2019). Mobile Device Detection Through WiFi Probe Request Analysis. IEEE, pp.98579–98588.

[6] Potortì, F., Crivello, A., Girolami, M., Barsocchi, P. and Traficante, E. (2018). Localising crowds through Wi-Fi probes. Ad Hoc Networks, 75–76, pp.87–97.

[7] Prasad, A., Verma, S.S., Dahiya, P. and Kumar, A. (2021). A Case Study on the Monitor Mode Passive Capturing of WLAN Packets in an On-the-Move Setup. IEEE pp.152408–152420.

[8] Ramezanpour, K., Jagannath, J. and Jagannath, A. (2022). Security and Privacy vulnerabilities of 5G/6G and WiFi 6: Survey and Research Directions from a Coexistence Perspective.

[9] Rutermann, T., Benabbas, A. and Nicklas, D. (2019). Know Thy Quality: Assessment of Device Detection by Wi-Fi Signals. 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops).

 | DOI: 10.20533/ijrfidsc.2046.3715.2023.0026