The Review of Modes of Operation and Randomization in Smartphone Passive Monitoring using WI-FI Probe Context

Vikrom Maikaensarn

Faculty of Logistics and Transportation Management, Panyapiwat Institute of Management,
Nonthaburi, Thailand
E-mail: vikrommai@pim.ac.th

Received: May 6, 2021 / Revised: May 21, 2021 / Accepted: August 3, 2021

***Abstract*—WI-FI probe monitoring is a passive monitoring technique that collects information from the smartphone's probe request information, using a sensor or sniffer, representing the monitored area's users. Nonetheless, as technologies developed, more changes are applied to the smartphone, promoting the user's privacy protection and extending the device's functionality. At the same time, this caused a shift in the smartphone device's probing behavior, which affects the effectiveness of WI-FI probe monitoring. In this study, by reviewing different factors that may affect smartphone WI-FI probe monitoring effectiveness, it was found that developers have adopted the MAC address randomization process in response to the user's privacy protection. Although randomization caused noises in the data and altered the study's outcome while the smartphone device is not connected to the internet, it is possible to monitor the users connected to the internet with the proper SSID and network structure setup.**

***Index Terms*—WI-FI Sniffer, Passive Monitoring, MAC Address Randomization, WI-FI Probe**

I. Introduction

Understanding the behavior of facility users plays a vital role in resource management and facility assessments. Field surveying is used as a tool in collecting information regarding user behaviors. However, field surveys can be time-consuming and could affect the users' normal behaviors within the interested area. Furthermore, the intrusion in daily activities could cause an alteration of people's behaviors to be different from the regular basis.

With the internet of things (IoT), a microcontroller or micro transceiver [1], becoming part of our daily lives, it is possible to passively collect the data without intruding daily personnel activities through users' internet connection via cellular network (4G-LTE, UMTS), and WI-FI. There are many types of wireless technology. The common examples of wireless signals are mobile signal, Bluetooth, WI-FI, Radio Frequency Identification (RFID), and Global System Positioning (GPS). All of these could be found in today's smartphones; used in different activities such as communication, entertainment, data exchange, and connection to smart accessories. Although there are many types of wireless signals, each with a unique range of signal frequencies and properties, this paper focused on the WI-FI signal, which is commonly used in internet connection and is an essential requirement to utilize smartphone functions while lowering the cellular network usage [2].

Even though WI-FI connections are common in this digital era, there are only a few experimental investigations, and the information regarding WI-FI probing limitations is still lacking [3]. Hence, this paper aims to identify smartphone WI-FI probe monitoring limitations to find an alternative WI-FI monitoring approach.

II. Review of Literature

WI-FI sniffer or tracking used WI-FI signal from the access point (AP) and router connection or probe request to collect information such as timestamp and media access control (MAC) address to identify the users within the facility. In general, WI-FI MAC address monitoring is used in counting and localizing the users within the facility's area. In addition to the localization capability [4]-[6], the collected data can also analyze users' behavior while using the facility [4], the study of pedestrians' trajectories [6]-[7], and population distribution [8]. However, as time progressed, new technologies emerged with a new set of regulations. Thus, to determine the future direction of WI-FI tracking, it is important to understand the system's current limitation and the restriction of privacy control.

Note: In some contexts, the WI-FI probe is referred to as the equipment used in monitoring WI-FI requests. Whereas in this paper, the WI-FI probe is referred to internet device WI-FI request. Hence, from the next section onward, sensors and sniffer will be used to refer to the monitoring equipment to prevent any overlaps of the WI-FI probe usage.

A. WI-FI Probe Monitoring

WI-FI (wireless fidelity) or IEEE 802.11 [9] is a wireless signal which enabled the device such as smartphone, laptop and other Internet of things (IoT) to gain access to the internet or enabled any network-based services and activities [10]. The WI-FI probe is a broadcast signal by the WI-FI enabled device requesting for AP connection, with the basic coverage ranging from 150 feet to 300 feet – approximately from 46 meters to around 91 meters depending on the obstruction of the wireless signal [10], [11]. The devices will broadcast the probe request for as long as the user is required to connect to the network and rebroadcast the signal again once the current connection strength dropped [7]. Hence, this process leave behind a unique finger print where it can be used to represent the monitored subject [12]. There are two methods to obtain the WI-FI probe signal information:

- Direct monitoring of the WLAN (wireless local area network) controller, which collects information from APs.
- Smartphone probe requests information monitoring using WI-FI sniffer devices.

The first method is information extraction or direct monitoring of the network structure through the APs, as demonstrated by [13], using the structure shown in Fig. 1. Nonetheless, this method requires full access to the WLAN structure, requiring the facility's owner's permission.

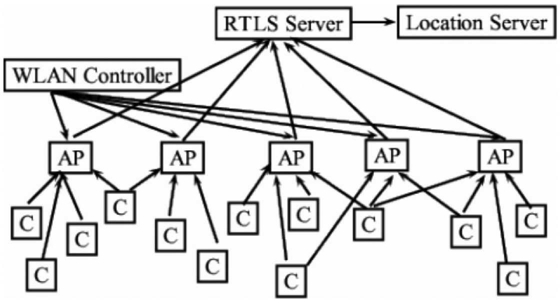


Fig. 1. WLAN controller monitoring setup for indoor localization system, where C – client represent the users' internet device trying to connect to the nearby APs, and RTLS – real-time location system [13].

The second method is to extract the probe signal information through probe request monitoring via sensor or sniffer device, using the model shown in Fig. 2 and the setup as shown in Fig. 3. This method will require either a commercialized technology such as FogSenses [3], or turning an IoT device into monitoring equipment using a WI-FI sniffer and analyzer software such as WireShark, Tshark, and Windump [14].

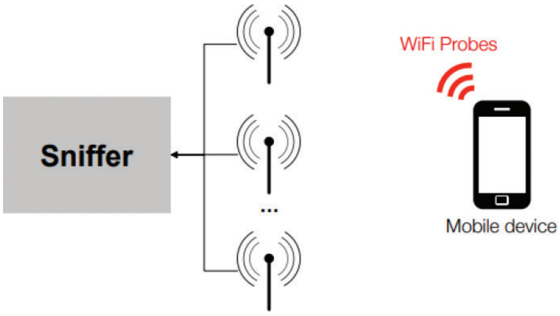


Fig. 2. Probe request monitoring using a sensor or a sniffer with compatible wireless antennas.

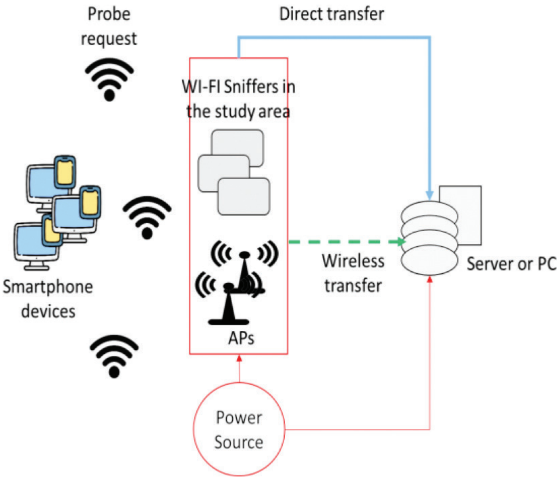
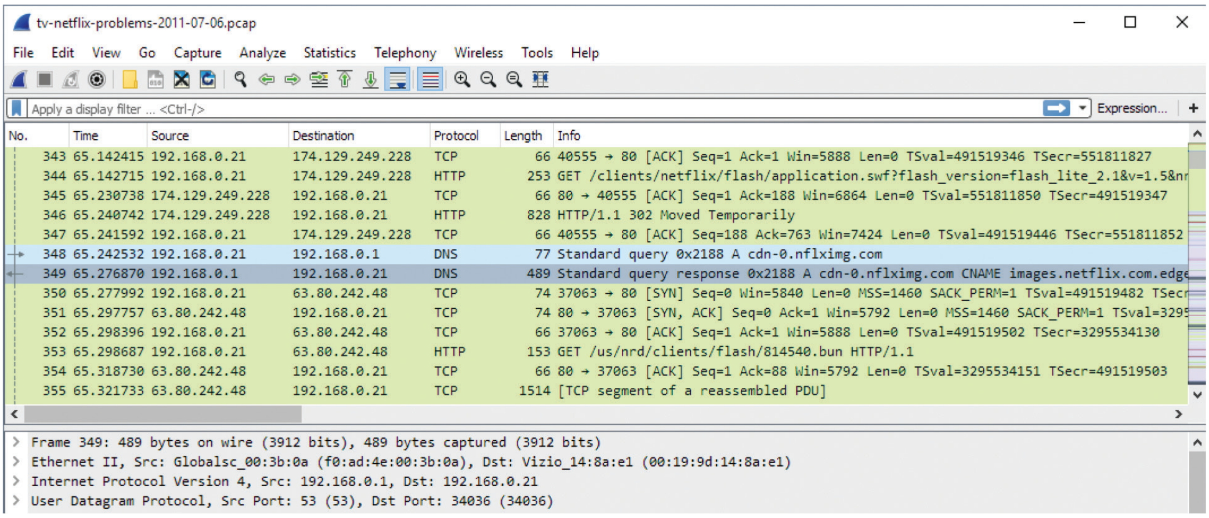


Fig. 3. WI-FI probe monitoring setup

The information extracted by sniffer software and sensor, as shown in Fig. 4, generally contains MAC addresses, signal strengths, and timestamps which are later used in the localization and trajectory analyses [3], [13], [15]-[19]. The MAC address is used to represent the internet device, the timestamp is the time log when the WI-FI sniffer detects a probe request, and signal strength is used to calculate the distance between the sensors and the internet device. Using MAC address information, it is possible to localize and detect the presence of facility users within the area and the trajectory of the users; hence, making it the key information in WI-FI passive monitoring. This monitoring technique removes the condition to constantly survey the area for up-to-date information since the WI-FI sniffer can be permanently deployed in the study area. Therefore, simplify the field survey work to only the maintenance of the sniffer devices.



```
No.    Time      Source          Destination     Protocol Length Info
   343 65.142415 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
   344 65.142715 192.168.0.21    174.129.249.228 HTTP      253 GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&nr
   345 65.230738 174.129.249.228 192.168.0.21    TCP        66 80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
   346 65.240742 174.129.249.228 192.168.0.21    HTTP      828 HTTP/1.1 302 Moved Temporarily
   347 65.241592 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
   348 65.242532 192.168.0.21    192.168.0.1     DNS        77 Standard query 0x2188 A cdn-0.nflximg.com
   349 65.276870 192.168.0.1     192.168.0.21    DNS       489 Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
   350 65.277992 192.168.0.21    63.80.242.48    TCP        74 37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
   351 65.297757 63.80.242.48    192.168.0.21    TCP        74 80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
   352 65.298396 192.168.0.21    63.80.242.48    TCP        66 37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
   353 65.298687 192.168.0.21    63.80.242.48    HTTP      153 GET /us/nrd/clients/flash/814540.bun HTTP/1.1
   354 65.318730 63.80.242.48    192.168.0.21    TCP        66 80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
   355 65.321733 63.80.242.48    192.168.0.21    TCP      1514 [TCP segment of a reassembled PDU]

> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
```

Fig. 4 Example of WI-FI sniffer extracted information [20]

B. Smartphone Functions and Probe Request

In the study of localization and trajectory monitoring using WI-FI sniffing, the interested MAC addresses must be non-stationary addresses that of smartphone devices, one of the main equipment carried by the users. Therefore, the smartphone's functions, system setting, and users' privacy protection must be considered to determine WI-FI probe request monitoring effectiveness.

1) Modes of the Smartphone

There are three main modes in the smartphone that could affect the WI-FI probing behavior: Sleep Mode, Power Save Mode, and Airplane Mode. Each mode activation results in behavioral change in the device functions as described in Table I.

TABLE I
DETAILS OF DIFFERENT MODES IN SMARTPHONE

Mode	User interaction	System Default	Effects to the WI-FI probing behavior
Sleep Mode	Automatically occur when the screen is turned off for a short period [21], which vary between different models and system version.		Lesser probe request or no probe request depending on the device setting.
Power Save Mode	Required user to enabled the function	Disable by default	Extends battery life by minimizing the device background activities, including WI-FI activity. Thus, reducing the probe request frequency.
Airplane Mode	Required user to enabled the function	Disable by default	WI-FI disabled upon the mode activation, which stopped the probe request

As shown in Table I, both sleep and airplane modes disabled WI-FI by default, which stops the smartphone's probing request. On the other hand, the power save mode will reduce the probe request frequency. However, both sleep mode and airplane mode contain additional settings, allowing users to re-activate the WI-FI system. Furthermore, in most cases, Airplane Mode is only used on some occasions within designated places. Whereas the Sleep Mode will occur regularly as the user turn-off the device's screen. Nonetheless, in Sleep Mode, users are allowed to keep the WI-FI system enabled, to stay connected to the internet, or sending a probe request at a fixed interval to ready the connection, using the advance setting, with respect to the type of OS and versions [22]-[25].

2) Privacy Protection: MAC Address Randomization

As mentioned, smartphones are one of the main equipment carried by people and are used in many activities. Since many of these activities required an internet connection; therefore, it very common that the smartphone would leave behind a fingerprint which WI-FI sniffer can detect and collects information regarding the smartphone users within different facilities. In response to privacy protection's rising concern, the developers must adopt stronger privacy protection mechanisms [26]-[28].

Both Android and iOS smartphones have adopted MAC address randomization. This protection mechanism generates a random set of variables, replacing the OUI (Organizationally Unique Identifier) or NIC (Network Interface Controller), as shown in

Fig. 5, to be used in place of the device MAC address during probe request.

The randomization process increased the number of MAC addresses detected during the monitoring. Therefore, increase the difficulty to tracks or monitor the facilities' users [29]. As mentioned, MAC address randomization will generate a random variable to create a new MAC address, used in place of the actual unique MAC address during the WI-FI probing process. These randomized MAC addresses are considered short-lived and will not be matched any vendor information, the OUI assigned by IEEE, provided in WI-FI monitoring software [8].

The randomization process behaves differently between different Android and iOS versions. In the early stage of its implementation, the randomization will only occur when the device is not connected to any APs. Meaning that once the user is connected to the internet, the device will revert to the actual MAC address until the connection is discontinued. Thus, allowing WI-FI sniffer to trace a specific MAC address as long as the users are connected to the internet using the APs within the facility. To counter this flaw, the later version of both OS has enabled the users to utilize randomized MAC address every time they are connected to the different APs. The summary of the MAC address randomization from the early release till today is as shown in Table II below.

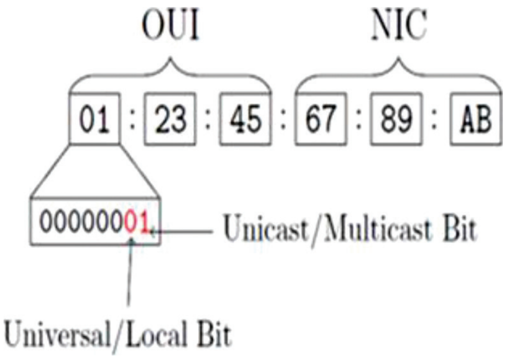


Fig. 5. 48-bit MAC address structure [28]

TABLE II
OS RELEASES AND MAC ADDRESS RANDOMIZATION [30]

Release Year	OS and Version	Randomization Behavior	System Default / Enabled or Disabled by Default	References
2014	iOS 8	MAC address randomized during probe request: Full randomization Revert to globally unique MAC address when connected to the AP	System default	• [30] • [31] • [32] • [7] • [28]
2017	Android 8	MAC address randomized during probe request: Prefix randomization Revert to globally unique MAC address when connected to the AP		
2018	Android 9	MAC address full randomized for both: A. Probe request B. Network connection / SSID (network)	A. System default B. Disable by default; User can enable the function which used the randomized MAC address for the connection session.	• [33] • [34] • [31]
2019	Android 10		A. System default B. Enabled by default	
2020	iOS 14	MAC address full randomized for both: A. Probe request B. Network connection / SSID / 24 hours	A. System default B. Enabled by default	• [30] • [33] • [29] • [32]

Note: SSID or service set identifier is the name of the WI-FI that appears in the WI-FI searching list; **Full randomization** is the process of generating a new set of MAC address during probe request; **Prefix randomization** is the process of generating random Prefix (the OUI) [28] during probe request.

III. Material Methodology and Discussion

Due to digitalization in our daily living, internet connection has become a core requirement in any form of activities that leave behind users' WI-FI fingerprints information. These fingerprints are mainly used in monitoring the people within the interested facility. In most cases, the monitoring allows the facility owner to study the localization, occupancy rate, and pedestrian movement [18], [35]-[38] in the study area. Nonetheless, since most studies involve smartphone monitoring, it is noted that there are chances of the missing data to occur as the devices go into different modes. However, it could be considered a minor issue as compared to the privacy protection problem. In response to the privacy protection, developers adopted the MAC address randomization technique to help prevent the tracking and passive monitoring from the 3rd party by increasing the number of MAC addresses detected by the sniffers.

However, these issues are rarely mentioned because different modes of operation do not have many effects on smartphone monitoring. Furthermore, the randomization of MAC addresses still has a minor impact due to the compatibility to the system during the study period. Nevertheless, as technologies grow, these changes begin to escalate to suit the users and comply with the privacy protection policy. Hence, online articles related to the smartphone's OS and MAC address randomization characteristics were selected, based on the review of the related experiments, to provide insight into the updated system in the smartphone and its potential impact on WI-FI passive monitoring.

A. *Effects of Different Modes in Smartphone*

In the context of WI-FI probing and an internet connection, modes in smartphones have different behavior depending on the OS and version. Nonetheless, the basic characteristics of each mode still stand:

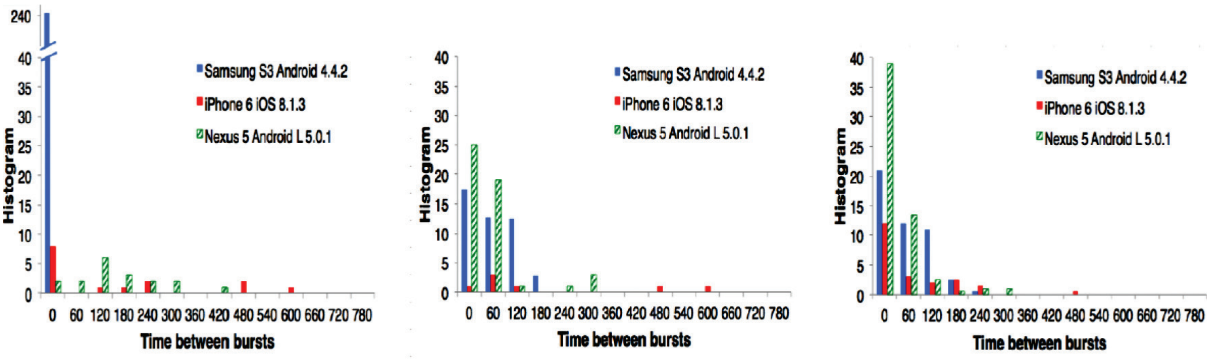
- *Sleep Mode* – reduce smartphone background operation to extend the battery's operation time which includes WI-FI operation.
- *Power Save Mode* – extending battery's operation time by reducing background activities depending on users' activities.
- *Airplane Mode*–disable wireless signal operations, which disable the transmitter and receiver of the device as per regulation during the flight

In general, the easiest mode to occur is sleep mode, which happens when users turn off the screen for a few seconds, whereby all these mobile modes of operations will disable the WI-FI activities by default. But in the latest OS version, the users can reactivate the feature or provide the users with connecting to the internet network setup to enhance user experiences when using a smartphone. In any case, the impact level of these modes' activation depends on the users, which required close monitoring to analyze the users' smartphone activity level in the study area and how often these modes are triggered. Although, in passive monitoring, the goal is to extract the information without disturbing the users. Thus, missing data from modes of operation in a smartphone could be considered a general case in passive mobile monitoring. However, the important part is how these modes can affect the randomization process, which required close monitoring of the devices with different OS and versions.

B. *Effects of Randomization to WI-FI Monitoring*

MAC address randomization generates new MAC addresses to be used while searching for the internet connection, hence increase the MAC addresses based on the amount of probe burst. A probe burst is a group of probe requests continuously sent over a period that varies between OS and environment [2], [26], as shown in Fig. 6.

As shown in Table I, both sleep and airplane modes disabled WI-FI by default, which stops the smartphone's probing request. On the other hand, the power save mode will reduce the probe request frequency. However, both sleep mode and airplane mode does allow additional setting which allows user to re-activate WI-FI system. Furthermore, in most cases, Airplane Mode is only used on some occasions within designated places. Whereas the Sleep Mode will occur regularly as the user turn-off the device's screen. Nonetheless, in Sleep Mode, users are allowed to keep the WI-FI system enabled, to stay connected to the internet, or sending a probe request at a fixed interval to ready the connection, using the advance setting, with respect to the type of OS and versions [22]-[25].



(a) 0 Known SSIDs (b) 4 Known SSIDs (c) 20 Known SSIDs

Fig. 6. Frequency of probe requests given the different known number of SSIDs [26]

These probe bursts coupled with the randomization generate noisy data, which resulted in missing information and altered the outcomes of different analyses, as shown in Table III.

TABLE III
EFFECTS OF MAC ADDRESS RANDOMIZATION

Cases	Randomization effects	Results
Occupancy study	• The increasing number of MAC addresses detected (noisy data). • Missing information as the smartphone disconnect from the network, causing the randomization to kick in during WI-FI searching.	• The spike number of MAC addresses detected as the monitoring period increase may result in an overfitting model. • The increasing number does not represent the true. • population in the study area
Localization study		• The results do not represent the true number of facility users. • The viable sampling collected by the sniffer may be too small to represent the population.
Pedestrian trips/behavior monitoring		• Missing trip information resulted in the alteration of trip mapping and trip patterns in behavior study.

In short, the randomization process reduces the effectiveness of WI-FI probe monitoring by generating random MAC addresses, which cannot be used to trace the users in the study area. Thus, researchers must devise an alternative approach to monitor the randomization sequence pattern for further identification unless a direct attack on the user's smart device, such as the Karma attack [27]. Nonetheless, according to the finding, the smart devices must use a static MAC address to maintain the connection in one SSID network, which can be classified as shown in Fig.7 below.

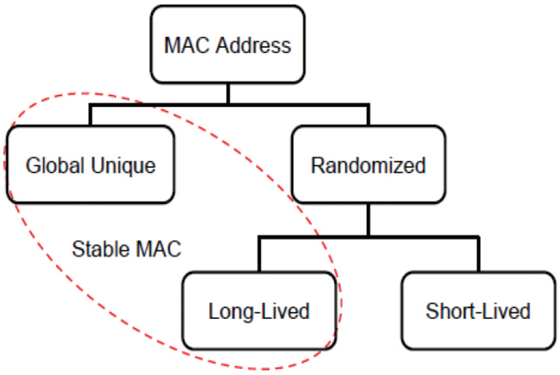


Fig. 7. MAC address classification [7]

IV. CONCLUSION

It is important during observation to monitor the population without interfering with their activities. WI-FI probe monitoring technique collects smartphone probe request information, representing the users within the facility without affecting the users' routine. The literature reviews show that there are two main factors that directly affect the smartphone's probing behavior: modes of the smartphone and MAC address randomization. In different modes, smartphone WI-FI probing behavior will change according to the system. Whereby, in most cases, it resulted in the cease function of the WI-FI feature.

Another factor, which occurs in response to smartphone users' privacy protection, is MAC address randomization. This algorithm generates random variables used in place of the actual MAC address for APs scanning. This algorithm has evolved throughout the years as technology changes to strengthen security. As mentioned in section 3.1, the randomization process altered the behavior of the monitored users due to the missing data used in the analyses. To further analyze the randomization, the actual WI-FI sniffer's detection range should be considered to prevent the overlapping of the monitoring zones, which further increases the detected MAC addresses and causes an error in the localization during the monitoring process.

Nevertheless, this does not mean that WI-FI probe monitoring technique will be obsolete. Although altering the MAC address helps protect the users' privacy, the device requires a static MAC address while connecting to one network SSID; hence, it allows one to continue monitoring the facility's users as long as they are connected to the internet.

V. SUGGESTION

The implementation of MAC address randomization creates a challenge in WI-FI probe passive monitoring technique. Nonetheless, it is possible to continue observing the facility users by limiting the sampling group to those with long-lived MAC addresses, assuming the sampling group used the latest OS, as mentioned in Table II. Hence, it is essential to ensure that the facility used the appropriate network setup, using a single SSID network throughout the study area to make WI-FI probe monitoring viable.

Another solution, other than a direct attack method, is to analyze the embedded information elements in each probe bursts generated by the smartphone to create signatures specific to the device to monitor them, as demonstrated in [39].

Lastly, the PDPA (Personal Data Protection Act) should be considered before conducting the WI-FI probe monitoring. Therefore, security and data management control should be strengthened and ensure the users' consent before initiating the monitoring process to comply with the PDPA and its based regulation, GDPR (General Data Protection Regulation) [40].

REFERENCES

[1] A. Zanella, N. Bui, A. Castellani et al., "Internet of Things for Smart Cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22-32, Feb. 2014.

[2] X. Hu, L. Song, D. Van Bruggen et al., "Is There WiFi Yet? How Aggressive WiFi Probe Requests Deteriorate Energy and Throughput," in *Proc. The 2015 Internet Measurement Conference*, 2015, pp. 317-323.

[3] F. Potortì, A. Crivello, M. Girolami et al., "Localising Crowds Through Wi-Fi probes," *Ad Hoc Networks*, vol. 75-76, pp. 87-97, Jun. 2018.

[4] Y. Wang, J. Liu, Y. Chen, M. Gruteser et al., "E-eyes: Device-Free Location-Oriented Activity Identification Using Fine-Grained WiFi Signatures," in *Proc. Annual International Conference on Mobile Computing and Networking MOBICOM*, 2014, pp. 617-628.

[5] M. Seifeldin, A. Saeed, A. E. Kosba et. al., "Nuzzer: A Large-Scale Device-Free Passive Localization System for Wireless Environments," *IEEE Transactions on Mobile Computing*, vol. 12, no. 7, pp. 1321-1334, Jul. 2013.

[6] X. Hu, P. Shen, Y. Shi et al., "Using Wi-Fi Probe and Location Data to Analyze the Human Distribution Characteristics of Green Spaces: A Case Study of the Yanfu Greenland Park, China," *Urban Forestry & Urban Greening*, vol. 54, p. 126733, Oct. 2020.

[7] H. Hong, G. Silva, and M. Chan, "CrowdProbe: Non-Invasive Crowd Monitoring with Wi-Fi Probe," *ACM on Interactive, Mobile, Wearable, and Ubiquitous Technologies*, vol. 2, no. 3, pp. 1-23, Sep. 2018.

[8] M. Uras, R. Cossu, and L. Atzori, "PmA: A Solution for People Mobility Monitoring and Analysis Based on WiFi Probes," in *Proc. 2019 4th International Conference on Smart and Sustainable Technologies (SpliTech),* 2019, pp. 1-6.

[9] ElectronicsNotes. (2021, Mar, 12). *What is WiFi: IEEE 802.11.* [Online]. Available: https://www.electronics-note.com/articles/connectivity/wifi-ieee-802-11/what-is-wifi.php

[10] DataPro. (2021, Mar, 12). *802.11 Wireless Info & FAQ*. [Online]. Available: https://www.datapro.net/techinfo/wifi_ _info.html

[11] B. Mitchell. (2020, Mar. 12). *How Far Will Your Wi-Fi Reach?* . [Online]. Available: https://www.lifewire.com/range-of-typical-wifi-network-816564

[12] J. Franklin, D. McCoy, P. Tabriz et al., "Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting," in *Proc. The 15th Conference on USENIX Security Symposium*, 2006, pp. 1-12.

[13] D. Jaisinghani, V. Naik, R. Balan et al., "Experiences & Challenges with Server-Side WiFi Indoor Localization Using Existing Infrastructure," in *Proc. The 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, 2018, pp. 226-235.

[14] J. Watson. (2019, Mar. 12). *11 Best Packet Sniffers Reviewed in 2021 (Free + Paid)*. [Online]. Available: https://www.comparitech.com/net-admin/packet-sniffer-network-analyzers/

[15] S.-S. Jan, S.-J. Yeh, and Y. W. Liu, "Received Signal Strength Database Interpolation by Kriging for a Wi-Fi Indoor Positioning System," *Sensors*, vol. 15, no.9, pp. 21377-21393, Sep. 2015.

[16] A. B. M. Musa and J. Eriksson, "Tracking Unmodified Smartphones Using Wi-Fi Monitors," in *Proc. The 10th ACM Conference on Embedded Network Sensor Systems*, 2012, pp. 281-294.

[17] W. Wang, Z. Lin, and J. Chen, "Promoting Energy Efficiency of HVAC Operation in Large Office Spaces with a Wi-Fi Probe Enabled Markov Time Window Occupancy Detection Approach," *Energy Procedia*, vol. 143, pp. 204-209, Jan. 2017.

[18] C. Wu, Z. Yang, Y. Liu, and W. Xi, "WILL: Wireless Indoor Localization without Site Survey," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 4, pp. 64-72, Apr. 2013.

[19] A. Rai, K. K. Chintalapudi, V. N. Padmanabhan et al., "Zee: Zero-Effort Crowdsourcing for Indoor Localization," in *Proc. The Proceedings of the 18th Annual International Conference on Mobile computing and networking*, 2012. pp. 293-304.

[20] WireShark. (2021, Mar. 12). *Chapter 1. Introduction*. [Online]. Available: https://www.wiresshark.org/docs/wsug_html/ChapterIntroduction.html

[21] Motorola. (2021, Mar. 15). *Use Sleep Mode to Save Power*. [Online]. Available: https://help.motorola.com/hc/3309/444/444/verizon/en-us/T1401264327.html

[22] Huawei. (2021, Mar. 15). *Can't Find the Keep Wi-Fi on During Sleep Setting | HUAWEI Support Global*. [Online]. Available: https://consumer.huawei.com/en/support/content/en-us00677572/

[23] A. McCambridge. (2020, Mar. 15). *How to Turn Off Wi-Fi During Sleep Mode on an Android Device*. [Online]. Available: https://ccm.net/faq/35580-how-to-set-the-wi-fi-sleep-policy-of-your-android-device

[24] Resilio. (2021, Mar. 15). *Configuring Auto Sleep & Battery Saver (Android)*. [Online]. Available: https://help.resilio.com/hc/en-us/articles/204762699-Configuring-Auto-Sleep-Battery-Saver-Android-

[25] J. Taylor. (2021, Mar. 15). *How to Fix Wi-Fi Disconnects When iPhone Is Locked - iMobie Inc*. [Online]. Available: https://www.imobie.com/support/wifi-disconnects-when-iphone-is-locked.htm

[26] J. Freudiger, "How Talkative is Your Mobile Device? An Experimental Study of Wi-Fi Probe Requests," in *Proc. The 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 2015, pp. 1-6.

[27] M. Vanhoef, C. Matte, M. Cunche et al., "Why MAC Address Randomization is Not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms," in *Proc. The 11th ACM on Asia Conference on Computer and Communications Security*, 2016. pp. 413-424.

[28] J. Martin, T. Mayberry, C. Donahue et al., "A Study of MAC Address Randomization in Mobile Devices and When it Fails," *Proceedings on Privacy Enhancing Technologies*, vol. 2017. no. 4, Mar. 2017. pp. 1-23.

[29] M. Burton. (2021, Mar. 15). *Wi-Fi MAC Randomization – Privacy and Collateral Damage*. [Online]. Available: https://www.extremenetworks.com/extreme-networks-blog/wi-fi-mac-randomization-privacy-and-collateral-damage/

[30] Eleven. (2020, Mar. 17). *How MAC Address Randomization Can Affect the Wi-Fi Experience*. [Online]. Available: https://blog.elevensoftware.com/how-mac-address-randomization-can-affect-the-wifi-experience

[31] Android. (2021, Mar. 17). *Privacy Changes in Android 10*. [Online]. Available: https://developer.android.com/about/versions//10/privacy/changes

[32] Apple. (2021, Mar. 17). *Wi-Fi privacy*. [Online]. Available: https://support.apple.com/guide/security/wi-fi-privacy-secb9cb3140c/web

[33] TechRepublic. (2020, Mar. 17). *How to Manage or Disable MAC Randomization in iOS and iPadOS 14*. [Online]. Available: https://www.techrepublic.com/article/how-to-manage-or-disable-mac-randomization-in-ios-and-ipados-14/

[34] Android. (2020, Mar. 17). *Privacy: MAC Randomization*. [Online]. Available: https://source.android.com/devices/tech/connect/wifi-mac-randomization

[35] W. Wang, A. Liu, M. Shahzad, et al., "Understanding and Modeling of WiFi Signal Based Human Activity Recognition," in *Proc. The 21st Annual International Conference on Mobile Computing and Networking*, 2015. pp. 65-76.

[36] Y. Chen, N. Crespi, L. Lv et al., "Locating Using Prior Information: Wireless Indoor Localization Algorithm," *ACM SIGCOMM Computer Communication Review*, vol. 43. no. 4, pp. 463-464, Oct. 2013.

[37] A. Goswami, L. E. Ortiz, and S. R. Das, "WiGEM: A learning-based Approach for Indoor Localization," In *Proc. The Seventh Conference on emerging Networking Experiments and Technologies*, 2011. pp. 1-12.

[38] H. Liu, H. Darabi, P. Banerjee, and J. Liu, "Survey of Wireless Indoor Positioning Techniques and Systems," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 37, no. 6, pp. 1067-1080, Nov. 2007.

[39] M. Uras, R. Cossu, E. Ferrara et al., "WiFi Probes Sniffing: an Artificial Intelligence Based Approach for MAC Addresses de-randomization," in *Proc. 2020 IEEE 25th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2020, pp. 1-6.

[40] M. Uras, R. Cossu, E. Ferrara et al., "PmA: A Real-World System for People Mobility Monitoring and Analysis Based on Wi-Fi probes," *Journal of Cleaner Production*, vol. 270, p. 122084, Oct. 2020.

Vikrom Maikaensarn is a Lecturer at the Faculty of Logistics and Transportation Management, Panyapiwat Institute of Management, Thailand where he teaches logistics and supply chain management. He received the B.Eng. in Civil Engineering and Technology and M.Sc. in Civil Engineering and Technology in transportation from Sirindhorn International Institute of Technology (SIIT), Thammasat University, Thailand. His research interests are pedestrian passive monitoring using the internet of things