POLITECNICO DI MILANO

Wireless Internet Project

MAC Randomization Behavior of Different Devices in Wi-Fi Probe Requests

Hamed Lotfalizadeh – 10946486

Mostafa Hashemiyan – 10946135

Summer 2024

I. Introduction

In this report we analyzed the MAC randomization behavior in Wi-Fi probe requests of the iPhone 15 Pro Max and Xiaomi 11T Pro devices. Using a sniffer in monitor mode and Wireshark, we captured and examined probe request packets in different scenarios. Through a sniffing and filtering procedure, we explored the patterns and variations in MAC randomization for both devices. The findings offer valuable insights into the privacy protection mechanisms employed by these devices during Wi-Fi connections.

In the context of Wi-Fi connections, stations send probe requests to access points (APs) to connect a certain network and get access to it. These probe requests generally include unencrypted information, such as a randomized Media Access Control (MAC) address, to protect user privacy. Understanding the MAC randomization behavior of devices is crucial for evaluating their effectiveness in safeguarding user identities. This report aims to characterize the MAC randomization behavior of iPhone 15 Pro and Xiaomi 11T Pro 5G devices through an analysis of their Wi-Fi probe requests.

II. Examination Process

1- Devices and environment

The sniffing process was conducted using a MacBook Air laptop in monitor mode with Wireshark software, a network protocol analyzer, in a controlled environment, along with two phones (iPhone 15 Pro and Xiaomi 11T Pro). Sniffing was conducted on a single channel, channel number 2, with a bandwidth of 20 MHz. To maintain proximity between the access point and the station, the roles of the phones were switched as needed, with one phone functioning as an access point while the other operated as a station, and vice versa, during the sniffing process. The mobile devices under examination was positioned approximately 20 cm away from the access point.

2- Filtering

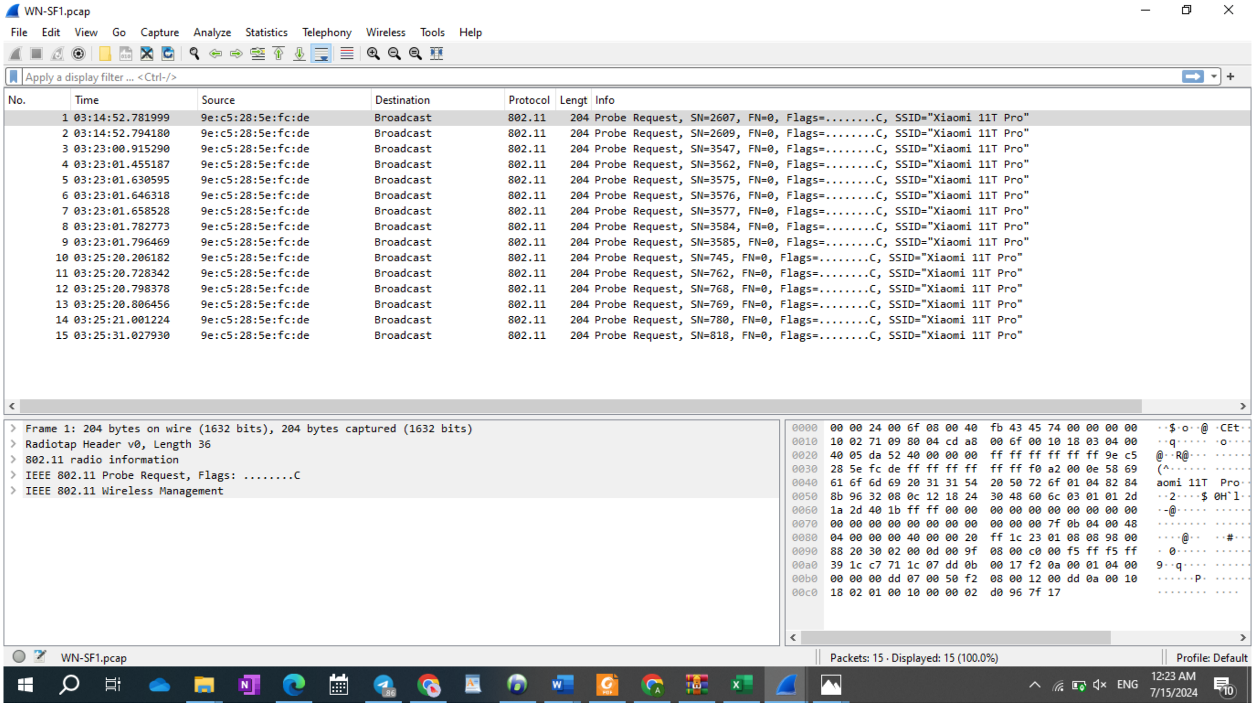
Sniffing was performed for almost 20 minutes in each scenario and 4 hours for 12 scenarios to capture an adequate amount of probe request data. The following states were considered to evaluate the MAC randomization behavior of two devices:

Scenarios	Wi-Fi	Screen	Power Saving
WN-SN	ON	ON	OFF
WN-SF	ON	OFF	OFF
WF-SN	OFF	ON	OFF
WF-SF	OFF	OFF	OFF
PN- WN-SN	ON	ON	ON
PN- WN-SF	ON	ON	OFF

After capturing the data, we used the 2-step filtering to focus on probe requests and distinguish them from other networks:

1- The filter (wlan.fc.type_subtype == 0x0004) was used to identify packets related to probe requests. This filtering process excluded irrelevant packets, allowing focus only on the probe requests sent by the devices.

2- The RSSI values of the probe requests were used to distinguish devices close to the sniffer from those farther away. The filter (wlan_radio.signal_dbm >= -55) was used to filter out probe requests from devices within a 20 cm range. There were 12 different scenarios for both devices, three of which are shown in Fig.1, Fig.2, and Fig.3. This RSSI-based filtering allowed us to focus on the probe requests from the iPhone 15 Pro and Xiaomi 11T Pro devices under this examination.



```
No.   Time             Source             Destination   Protocol Lengt Info
    1 03:14:52.781999  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=2607, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
    2 03:14:52.794180  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=2609, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
    3 03:23:00.915290  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=3547, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
    4 03:23:01.455187  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=3562, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
    5 03:23:01.630595  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=3575, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
    6 03:23:01.646318  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=3576, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
    7 03:23:01.658528  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=3577, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
    8 03:23:01.782773  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=3584, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
    9 03:23:01.796469  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=3585, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
   10 03:25:20.206182  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=745, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
   11 03:25:20.728342  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=762, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
   12 03:25:20.798378  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=768, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
   13 03:25:20.806456  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=769, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
   14 03:25:21.001224  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=780, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
   15 03:25:31.027930  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=818, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
```

```
> Frame 1: 204 bytes on wire (1632 bits), 204 bytes captured (1632 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Probe Request, Flags: ........C
> IEEE 802.11 Wireless Management
```

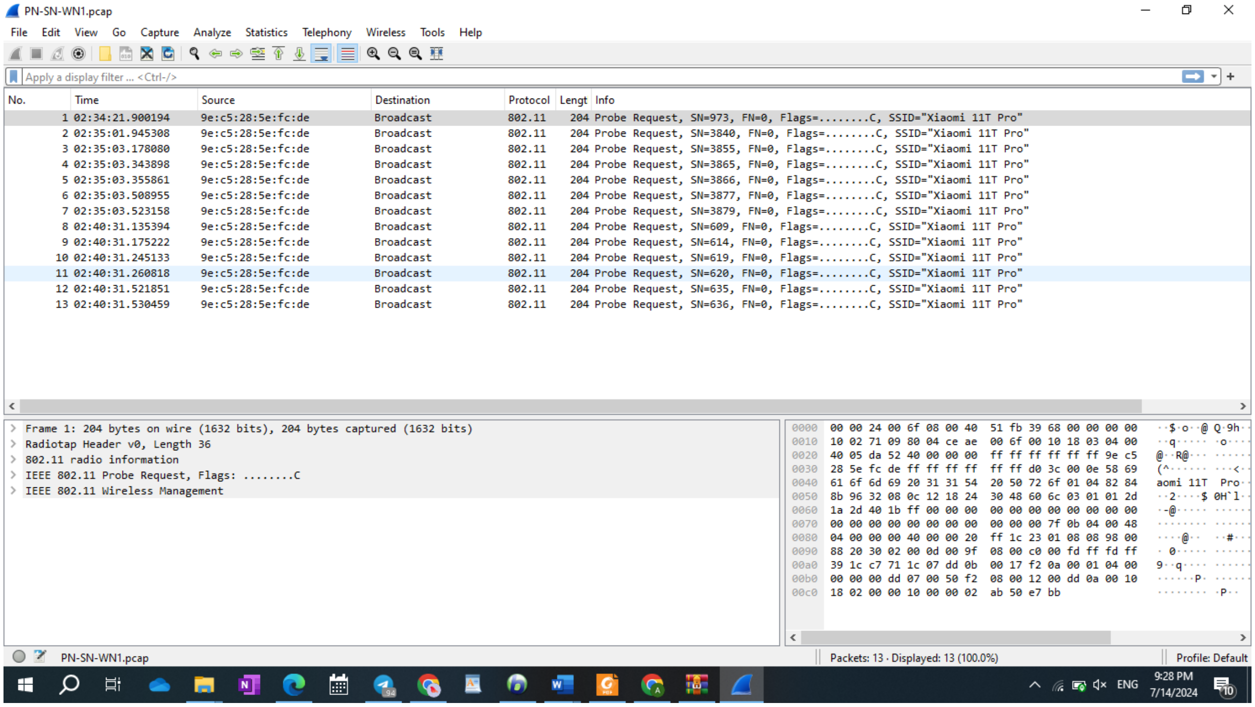
```
0000  00 00 24 00 6f 08 00 40  fb 43 45 74 00 00 00 00   ··$·o··@ ·CEt····
0010  10 02 71 09 80 04 cd a8  00 6f 00 10 18 03 04 00   ··q····· ·o······
0020  40 05 da 52 40 00 00 00  ff ff ff ff ff ff 9e c5   @··R@··· ········
0030  28 5e fc de ff ff ff ff  ff ff f0 a2 00 0e 58 69   (^······ ······Xi
0040  61 6f 6d 69 20 31 31 54  20 50 72 6f 01 04 82 84   aomi 11T  Pro····
0050  8b 96 32 08 0c 12 18 24  30 48 60 6c 03 01 01 2d   ··2····$ 0H`l···-
0060  1a 2d 40 1b ff ff 00 00  00 00 00 00 00 00 00 00   ·-@····· ········
0070  00 00 00 00 00 00 00 00  00 00 00 7f 0b 04 00 48   ········ ·······H
0080  04 00 00 00 40 00 00 20  ff 1c 23 01 08 08 98 00   ····@··  ··#·····
0090  88 20 30 02 00 0d 00 9f  08 00 c0 00 f5 ff f5 ff   · 0····· ········
00a0  39 1c c7 71 1c 07 dd 0b  00 17 f2 0a 00 01 04 00   9··q···· ········
00b0  00 00 00 dd 07 00 50 f2  08 00 12 00 dd 0a 00 10   ······P· ········
00c0  18 02 01 00 10 00 00 02  d0 96 7f 17               ········ ····
```

WN-SF1.pcap

Packets: 15 · Displayed: 15 (100.0%)

Profile: Default

Figure 1: WN-SF Scenario For AP: Xiaomi 11t pro and Station : iPhone 15 pro



```
No.   Time             Source             Destination   Protocol Lengt Info
    1 02:34:21.900194  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=973, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
    2 02:35:01.945308  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=3840, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
    3 02:35:03.178080  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=3855, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
    4 02:35:03.343898  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=3865, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
    5 02:35:03.355861  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=3866, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
    6 02:35:03.508955  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=3877, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
    7 02:35:03.523158  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=3879, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
    8 02:40:31.135394  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=609, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
    9 02:40:31.175222  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=614, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
   10 02:40:31.245133  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=619, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
   11 02:40:31.260818  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=620, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
   12 02:40:31.521851  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=635, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
   13 02:40:31.530459  9e:c5:28:5e:fc:de  Broadcast     802.11    204 Probe Request, SN=636, FN=0, Flags=........C, SSID="Xiaomi 11T Pro"
```

```
> Frame 1: 204 bytes on wire (1632 bits), 204 bytes captured (1632 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Probe Request, Flags: ........C
> IEEE 802.11 Wireless Management
```

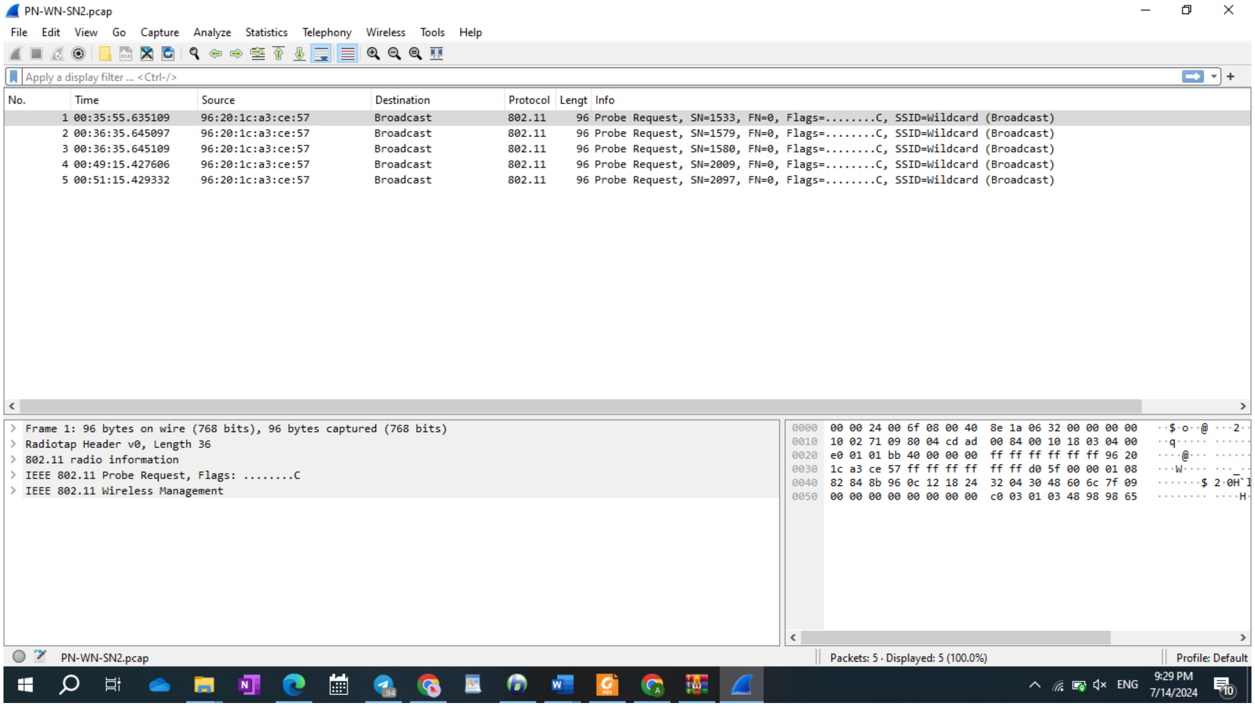
```
0000  00 00 24 00 6f 08 00 40  51 fb 39 68 00 00 00 00   ··$·o··@ Q·9h····
0010  10 02 71 09 80 04 ce ae  00 6f 00 10 18 03 04 00   ··q····· ·o······
0020  40 05 da 52 40 00 00 00  ff ff ff ff ff ff 9e c5   @··R@··· ········
0030  28 5e fc de ff ff ff ff  ff ff d0 3c 00 0e 58 69   (^······ ···<··Xi
0040  61 6f 6d 69 20 31 31 54  20 50 72 6f 01 04 82 84   aomi 11T  Pro····
0050  8b 96 32 08 0c 12 18 24  30 48 60 6c 03 01 01 2d   ··2····$ 0H`l···-
0060  1a 2d 40 1b ff 00 00 00  00 00 00 00 00 00 00 00   ·-@····· ········
0070  00 00 00 00 00 00 00 00  00 00 00 7f 0b 04 00 48   ········ ·······H
0080  04 00 00 00 40 00 00 20  ff 1c 23 01 08 08 98 00   ····@··  ··#·····
0090  88 20 30 02 00 0d 00 9f  08 00 c0 00 fd ff fd ff   · 0····· ········
00a0  39 1c c7 71 1c 07 dd 0b  00 17 f2 0a 00 01 04 00   9··q···· ········
00b0  00 00 00 dd 07 00 50 f2  08 00 12 00 dd 0a 00 10   ······P· ········
00c0  18 02 00 00 10 00 00 02  ab 50 e7 bb               ········ ·P··
```

PN-SN-WN1.pcap

Packets: 13 · Displayed: 13 (100.0%)

Profile: Default

Figure 2: PN- WN-SN Scenario for AP: Xiaomi 11t pro and Station : iPhone 15 pro



PN-WN-SN2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time             Source              Destination  Protocol Lengt Info
    1 00:35:55.635109  96:20:1c:a3:ce:57   Broadcast    802.11      96 Probe Request, SN=1533, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
    2 00:36:35.645097  96:20:1c:a3:ce:57   Broadcast    802.11      96 Probe Request, SN=1579, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
    3 00:36:35.645109  96:20:1c:a3:ce:57   Broadcast    802.11      96 Probe Request, SN=1580, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
    4 00:49:15.427606  96:20:1c:a3:ce:57   Broadcast    802.11      96 Probe Request, SN=2009, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
    5 00:51:15.429332  96:20:1c:a3:ce:57   Broadcast    802.11      96 Probe Request, SN=2097, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
```

```
> Frame 1: 96 bytes on wire (768 bits), 96 bytes captured (768 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Probe Request, Flags: ........C
> IEEE 802.11 Wireless Management
```

```
0000  00 00 24 00 6f 08 00 40  8e 1a 06 32 00 00 00 00
0010  10 02 71 09 80 04 cd ad  00 84 00 10 18 03 04 00
0020  e0 01 01 bb 40 00 00 00  ff ff ff ff ff ff 96 20
0030  1c a3 ce 57 ff ff ff ff  ff ff d0 5f 00 00 01 08
0040  82 84 8b 96 0c 12 18 24  32 04 30 48 60 6c 7f 09
0050  00 00 00 00 00 00 00 00  c0 03 01 03 48 98 98 65
```

Figure 3: PN- WN-SN Scenario for AP: iPhone 15 pro and station : Xiaomi 11t pro

III. Results

The analysis of MAC randomization behavior in Wi-Fi probe requests illustrated the following MAC addresses for iPhone 15 pro and Xiaomi 11t pro devices. The results, captured by Mac Air and filtered in Wireshark application, are shown in Fig.4 to represent a better insight for comparison of the two devices mechanism and performance in allocating MAC addresses, when they request to get access to networks. And finally, the following table shows the original and the randomized MAC addresses after the filtering.

Phone Devices Model and Brand	*Device 1: iPhone 15 pro*	*Device 2: Xiaomi 11t Pro*
Main MAC addresses	a0:52:72:1d:e2:bf	8c:7a:3d:b5:70:22
Randomized MAC addresses	9e:c5:28:5e:fc:de	be:3c:53:70:c3:6d 96:20:1c:a3:ce:57

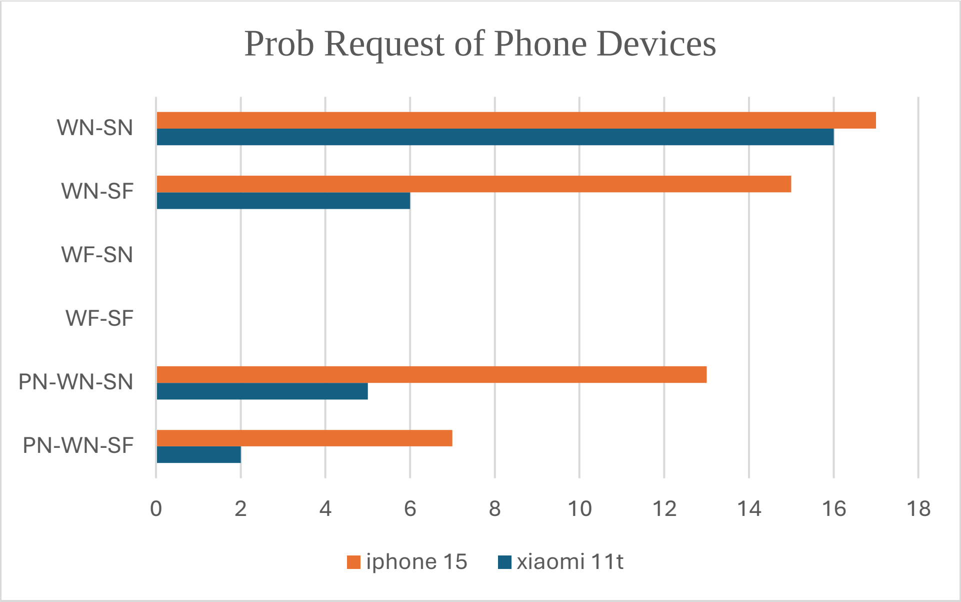


Figure 4: Comparison of different scenarios in two examined devices

IV. Conclusion

To sum up, this report represents the MAC randomization behavior in Wi-Fi probe requests for the iPhone 15 Pro and Xiaomi 11T Pro devices in different scenarios in an isolated place. The analysis illustrated variations in MAC randomization activity based on different device states and their companies' policies. When both the Wi-Fi interface and screen are on, the number of probe requests is at its highest. With the screen off, the number of probe requests decreases. When the Wi-Fi interface is off, no probe requests are observed. The power-saving feature reduces network activity and the number of probe requests. Therefore, in power-saving mode with the screen off, the number of probe requests is at its lowest.

These findings enhance our understanding of how device states and power-saving features affect probe request behavior. Additionally, they provide insights into the privacy protection measures used by these devices during Wi-Fi connections, particularly highlighting the effectiveness of MAC randomization in enhancing user privacy.