Wireless Internet Project: Characterizing MAC Randomization

Bahram Hedayati **Person Code: 10870276**

Mahsa Delaram **Person Code: 10847175**

1. Introduction

Probe requests are a fundamental part of the discovery process in wireless communications. This kind of frame contains the MAC address of the device (for instance, a smartphone) and requests information from the Access Points which are in its range. However, using the same MAC address in the probe requests can cause privacy concerns because someone can track the device via sniffing. To overcome this issue, device manufacturers implement some MAC randomization mechanisms in their products. MAC randomization is a technique to enhance privacy and make it more difficult for third parties to track the movements of devices and their owners. This project has a look at this subject though doing some experiments.

2. Experiment Setup

According to the project description, I use the devices below:

- my smartphone as the device which sends probe requests periodically. The specification of the smart phone is Xiaomi POCO X3 Pro (Non-randomized MAC address: 8c:d9:d6:32:3a:22).
- Access Point (FastGate GPON Model: FGA2130FWB)
- My laptop (HP Model: Pavilion 15-eg1) as the sniffer. I use Kali linux as the operating system to capture the probe requests in monitor mode via WireShark successfully.
  (Non-randomized MAC address: 34:6f:24:2c:0b:f3)

I tried to design and set the topology of the experiment as similar as the one in the paper mentioned in the project description. The smart phone was placed near the sniffer (within 20 cm). At distances greater than 2 m, no power peak of signal equal to or over −60 dBm was detected. After these arrangements, I changed the mode of my wireless adapter interface (wlan0) from managed mode into monitor mode, set its channel to 6 and run the WireShark with the super user privileges (sudo wireshark).

Figure 1: Topology of experiment

3. Experiment Execution

The experiment considers the combination of three main device's status including 6 different activity modes which are displayed briefly in the table 1.

Mode	Active Screen	WiFi	Power Saving
A	*	*	
S		*	
PA	*	*	*
PS		*	*
WA	*		
WS			

Table 1: Device Modes (* means that the related mode is ON)

Before beginning of capturing each mode, I turned off all wireless devices except the Access Point and the sniffer to make sure that there is not any signal greater than -40 dBm in the environment. I captured each mode for 20 minutes (as it has mentioned in the reference paper) and save the results in separated pcap files. Then, I filtered the results with two main merged conditions to extract only the smartphone's probe requests among all the captured frames:

1. Display only Probe Requests
   Filter Expression: **`wlan.fc.type_subtype == 0x0004`**
2. Display only the signals with high strength (RSSI) to make sure that I analyse the frames which published in the close proximity.
   Filter Expression: **`wlan_radio.signal_dbm >= -40`**

4. Results

The results show various number of probe requests in different activity modes of the smartphone. In addition, the randomization of MAC addresses can be seen clearly. Since the number of probe requests is more than the number of distinct MAC addresses in each capturing mode (due to the retransmission mechanism) The A mode[1] has the most number of probe requests and randomized MAC addresses compared to other modes. In contrast, I did not get any probe request during the sniffing while the WiFi of the smartphone was OFF (there was no difference between being ON or OFF status of the smartphone's screen). While the screen was ON in Power Saving mode, the second highest number of probe requests and their related randomized MAC addresses was received, while with an OFF screen, only 14 and 6 probe requests and distinct MAC addresses were captured respectively. The number of probe requests and the randomized MAC addresses which were received in each mode is reported in table 2. Also, more comprehensive details of the randomized MAC addresses which are received in each mode are illustrated in table 3.

Mode	Number of Probe Requests	Number of Distinct MAC Addresses
A	204	60
S	7	3
PA	102	45
PS	14	6
WA	0	0
WS	0	0

Table 2: Number of probe requests and the number of distinct randomized MAC addresses captured in each mode

[1] WiFi is ON while a movie was playing on the smartphone so the screen was on during the 20-minutes capturing.

A	PS	WS	WA	S mode	PA mode
Fa:29:8a:35:40:af	1a:74:de:cc:98:89	-	-	B2:ed:af:6f:e2:55	Da:73:68:07:91:0d
4e:55:5b:6e:24:01	De:b8:e1:84:88:52			9e:c6:4d:34:00:bc	Ea:be:5d:a4:a5:de
2a:bd:40:ea:18:74	Fe:b6:a9:2b:0e:77			0a:c3:8a:ae:08:bc	52:a5:f7:04:e2:24
5e:88:23:a5:0a:39	62:86:95:58:90:14				C2:55:92:fe:70:9d
92:b5:26:fa:31:47	1a:b8:a8:18:04:c6				56:67:01:8f:b2:cc
9e:53:1a:f2:21:66	6e:d0:5b:6b:71:fd				B2:23:2f:7b:57:a7
Ca:e4:6c:bb:75:c6					46:1f:41:25:19:5f
66:97:0a:43:17:e1					Ae:ab:c5:7c:77:9c
B2:b4:f4:f6:0b:c9					Fe:53:f2:a3:8c:a0
2a:43:39:3b:14:6b					56:2e:c1:0a:d6:cb
F2:bd:06:48:56:88					42:e3:75:8e:2a:f8
46:ab:c2:f6:2c:b8					E2:57:b1:ad:fc:bf
9a:f9:a5:58:28:a3					De:ec:6d:fc:92:3a
86:3e:0e:dc:1c:a1					Ee:50:dc:8f:ee:74
A2:53:05:a0:3c:07					3a:43:8c:20:1c:d5
26:02:70:7a:51:e1					3e:30:80:df:fb:15
4e:a3:81:6b:f7:f9					16:45:d7:b6:fb:fe
72:1f:24:fd:e7:24					A6:90:09:97:16:4c
7a:f8:38:85:67:22					32:6f:7d:87:50:15
66:18:8c:25:7e:30					C6:98:9c:ba:a9:1e
9a:2d:36:b9:8d:65					92:e9:4e:35:42:97
Fe:f3:49:5c:ac:f5					7e:0d:91:a9:7e:44
76:89:a1:0d:58:e9					Fa:f4:5f:b0:22:4d
D6:ea:58:3c:25:2b					A2:44:29:f3:89:23
Ee:61:41:38:e0:a1					Da:f1:6f:c6:fc:b9
F2:16:c0:a0:b3:9a					Fe:af:f6:49:e9:7e
Be:39:7d:38:af:24					Da:dc:7f:b4:6e:7a
Ea:f9:43:f9:d5:7b					Ca:ad:64:1f:3f:69
76:01:f0:3e:11:06					B6:62:76:e5:44:12
02:f4:89:d9:ab:8a					2e:84:23:ce:01:1d
2a:73:23:f0:6e:1a					Be:06:6f:3e:02:cd
9e:41:af:c9:3b:48					C6:1a:e4:35:d8:68
56:5a:0a:46:f9:cc					Fa:66:82:27:e9:88
56:b5:07:cc:42:7d					8e:5d:72:69:f2:41
5e:99:2c:39:54:e1					Aa:5d:4a:64:60:40
C2:ca:d2:a5:d7:1b					Ba:29:fa:ac:ec:88
7a:8e:f0:d6:c4:21					92:21:7b:39:c8:6a
9a:da:4b:f8:8f:d3					0e:46:a5:97:69:69
1e:8f:31:b2:ec:53					36:de:88:c1:51:8c
Be:67:53:63:5d:7b					52:7e:f1:c5:6f:41
0e:32:1c:cf:80:57					Ba:eb:56:29:b5:63
8a:61:24:1c:4a:03					26:0b:8a:5b:0d:f2
56:de:f8:43:f1:8e					3a:bd:5c:37:39:c0
0a:ad:99:fd:a0:f7					B2:ef:87:d4:19:f4
F2:86:44:0e:9a:67					Ce:6e:f7:4c:a5:8e
C6:9c:ed:17:70:71					
8a:97:7e:c9:e8:e9					
6e:a6:32:d0:ab:9a					
36:75:91:90:0d:12					
B2:f4:c8:2a:be:65					
16:d7:89:a2:61:60					
82:f0:2a:62:cb:d4					
F6:ae:5e:9b:61:db					
72:f4:21:94:a5:c7					
3a:29:9f:9e:8a:2d					
6e:9d:b5:c3:8d:f5					
76:97:d6:81:72:a0					
A2:38:5c:e9:95:79					
6e:97:ce:f3:a6:be					
E6:a8:f0:59:c1:04					

Table 3: details of the randomized MAC addresses which are received during 20 minutes in each mode

5. Conclusion

The WiFi, Screen status and Power Saving modes of the smartphone significantly impact on the number of probe requests which are published by the device. We can see that the smartphone continuously sends out probe requests at regular intervals to gather information about nearby access points when it is in A mode. If the smartphone's screen is OFF, the number of generated probe requests will radically reduce (modes S and PS), regardless of Power Saving mode. Furthermore, when the device is in Power Saving mode, the frequency of publishing its probe requests will decrease (PS and PA modes) due to reduce energy consumption. Obviously, no probe requests are generated by the mobile phone when the WiFi is OFF. Finally, I should say it is interesting that I witnessed a large number of generations of MAC addresses in a randomized manner which are proportional to the number of published probe requests.