Does disabling Wi-Fi prevent my Android phone from sending Wi-Fi frames?

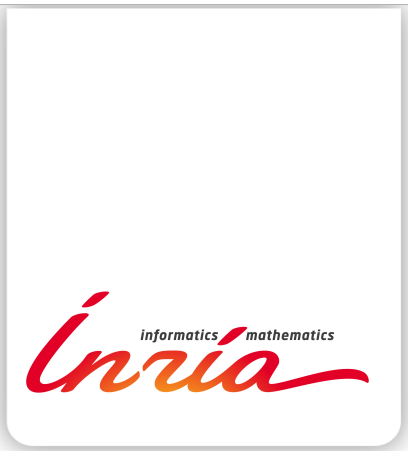
Célestin Matte, Mathieu Cunche, Vincent Toubiana

Does disabling Wi-Fi prevent my Android phone from sending Wi-Fi frames?

Célestin Matte, Mathieu Cunche, Vincent Toubiana

RESEARCH REPORT
N° 9089
AoÃ»t 2017
Project-Teams Privatics

ISSN 0249-6399 ISRN INRIA/RR--9089--FR+ENG



Does disabling Wi-Fi prevent my Android phone from sending Wi-Fi frames?

Célestin Matte, Mathieu Cunche, Vincent Toubiana*

Project-Teams Privatics

Research Report n° 9089 — AoÃ»t 2017 — 11 pages

Abstract: No. We show that another option, called "Always allow scanning", when activated, makes a device send Wi-Fi frames which can be used to track this device, even if the Wi-Fi switch is off. This option is not clearly described in all Android versions, and sometimes even not deactivatable. Besides, the Google Maps application prompts the user to activate this option.

Key-words: Wi-Fi, tracking, Android, privacy

* The views and opinions expressed in this report do not necessarily reflect the views of the CNIL or any individual Commissioner.

RESEARCH CENTRE
GRENOBLE – RHÔNE-ALPES

Inovallée
655 avenue de l'Europe Montbonnot
38334 Saint Ismier Cedex

Est-ce que la désactivation du Wi-Fi empêche mon Android d'emettre des trames Wi-Fi?

Résumé : Non. Nous montrons qu'une autre option, appelée "Always allow scanning", permet à l'appareil d'émettre des trames même si le Wi-Fi est désactivé, exposant ainsi l'utilisateur au traçage Wi-Fi. Cette option n'est pas clairement décrite dans l'ensemble des versions d'Android et est même parfois impossible à désactiver. De plus l'application Google Maps demande à l'utilisateur d'activer cette option.

Mots-clés : Wi-Fi, traçage, Anrdoid, vie privée

1 Introduction

Wi-Fi signals emitted by mobile smartphones can be exploited to passively track users' mobility [7, 5]. Turning off the Wi-Fi interface of the device is often presented as a mean to evade those tracking systems[1]. As a matter of fact this method is sometime suggested by the actors of the Wi-Fi tracking industry as a way to opt-out from those systems[2].

The Android system features an option to enable or disable Wi-Fi on the device. However, disabling Wi-Fi through this option is not sufficient to prevent all Wi-Fi activity of the device. We performed several measurements that confirm this behavior on a range of Android device.

2 Wi-Fi on Android

2.1 Android Wi-Fi scans

The Android system supports Wi-Fi in order to provide network connectivity. As any other Wi-Fi-enabled system, Android relies on Wi-Fi service discovery mechanisms to detect Wi-Fi access points in range. Unlike what is commonly expected [4], as most mobile systems, Android rely on active service discovery, a mechanism in which the device actively searches for nearby access points. To do so, the device perform scans during which it sends wireless inquiries called *probe requests* containing its own – and often unique – MAC address. Access points reply to those requests through *probe responses*, revealing themselves to the device.

Nowadays, Wi-Fi service discovery is also used to get location information. Wi-Fi access points, identified by their unique BSSID (a MAC address), are used as landmarks. Aided by a Wi-Fi-based location engine, a location can be derived from a list of access points detected during a Wi-Fi scans. In Android, Wi-Fi scans are used to enable both network connectivity, and location [3].

However, Wi-Fi scans are not only used by the device to derive its location, analytics companies now leverage the Wi-Fi *probe requests* to estimate the number of visitors in stores and malls and to record customer mobility. Indeed, by counting the number of unique MAC addresses broadcast in *probe requests*, retailers can derive the number of smartphone carriers in their store. Location tracking of these customers is performed by following these MAC addresses as they are heard by antennas located in different spots.

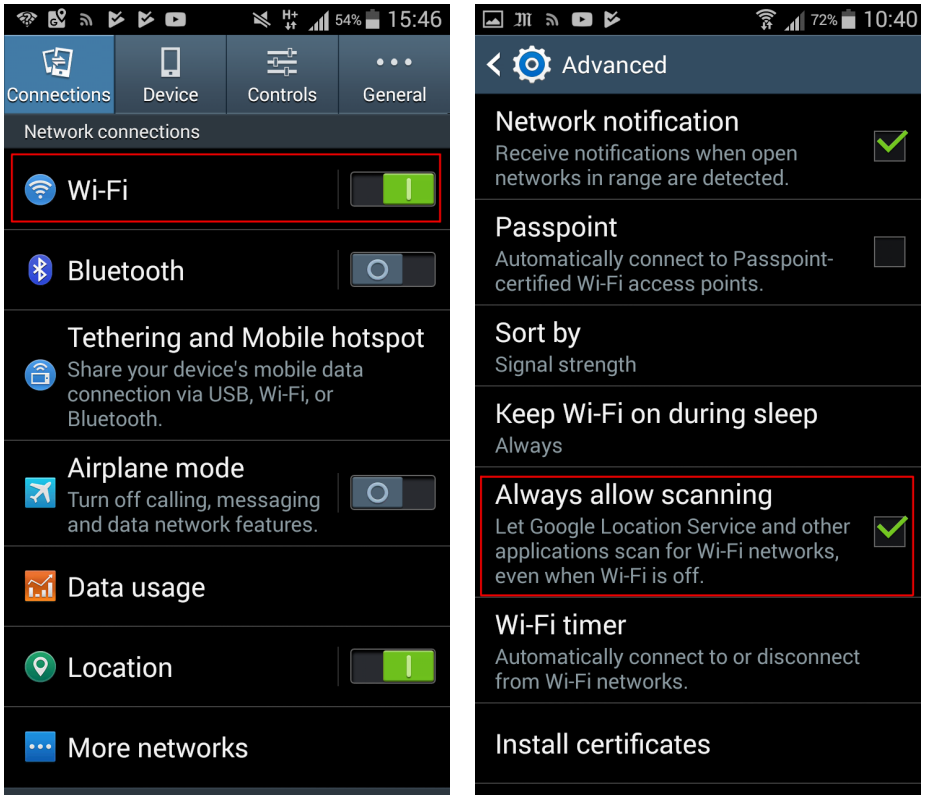
2.2 Wi-Fi-related settings in Android

The Android system includes a number of configuration options that can impact the Wi-Fi activity of the device. The most obvious one is the Wi-Fi switch (see Figure 1a). When this switch is activated, the Wi-Fi interface can be fully used by the operating system and the application (provided that they have sufficient permissions). When the switch is off, network connection through Wi-Fi is unavailable and application cannot access the result of Wi-Fi scans.

A second option called "Always allow scanning" (see Figure 1b), or "scanning always available", allows the device to perform Wi-Fi scans even if the Wi-Fi switch is off. On the Android 4.4.4 of a Samsung Galaxy S3 and the Android 4.3 of a Nexus S, this option is located in `System` → `Wi-Fi` → `Advanced` whereas on the Android 7.0 of a Lenovo Moto G 5, this option is located in `Settings` → `Location` → `Scanning`. On the Android 6.0.1 of a OnePlus One, this option is nowhere to be found. Tests described later in the paper indicate that the option is activated.

[1] `http://lifehacker.com/how-retail-stores-track-you-using-your-smartphone-and-827512308`,`https://nakedsecurity.sophos.com/2014/06/12/apples-ios-8-will-help-keep-out-wi-fi-marketers-and-snoops-but-not-totally/`

[2] `https://twitter.com/adhavet/status/891693199424729092`



(a) Wi-Fi switch option (b) "Always allow scanning" option

Figure 1: Wi-Fi related options in Android 4.4.4.

3 Analysis of generated Wi-Fi activity

A total of 5 devices covering a Android versions ranging from 2.2.1 to 6.0.1 . The devices considered in this study are the following:

- **Galaxy S3**: Samsung Galaxy S3 (GT-I9...), Android 4.4.4
- **HTC wildfire**, Android 2.3.7, CyanogenMod 7.2.0
- **Samsung Galaxy Spica**, Android 2.2.1, CyanogenMod 6.1.1
- **Nexus S**, Android 4.3, CyanogenMod 10.2.1.1
- **OnePlus One**, Android 6.0.1, CyanogenMod 13.1.2

3.1 Experimental protocol

We monitored the Wi-Fi traffic generated by each smartphone in different configuration and under different types of activities. Devices were never associated to an access point. Monitoring was performed using a Wi-Fi interface set in monitoring mode and capturing the traffic on a

fixed channel. The source MAC address of the collected Wi-Fi frame was used to detect traffic generated by a device. Indeed, all Wi-Fi frames emitted by those devices include their MAC address in the frame header[3].

Several configuration options have been considered:

- **Wi-Fi switch**: the option controlling the activation of Wi-Fi.
- **Always allow scanning**: the option allowing Wi-Fi scans when the Wi-Fi is off.
- **Location**: the option controlling the location feature. In some devices, the option is divided into 2 options: GPS geolocation and cellular/Wi-Fi geolocation. We only considered the latter.

Several activities, reflecting a typical usage were considered:

- **Screen on**: the screen is on and the device is kept in this state by switching between panels for a few minutes.
- **Idle**: the device is left untouched for at least 5 minutes after the screen has automatically turned off.
- **Leaving idle**: the device is put out of idle mode by touching the power key.
- **Google Maps**: the Google Maps application is running on the device.
- **Starting Google Maps**: the Google Maps application is started by the user.
- **Uncorrelated**: when the event happens without any obvious correlation with the user activity.

For each device and for each combination of the previous options, the Wi-Fi traffic was captured while the device was put through the different type of activity.

All devices except the OnePlus One and the Galaxy S3 had no other source of Internet connection.

3.2 Measurement results

Results of the measurements are presented in Table **??**. During those measurements, only frames of probe request type were generated by the device.

3.2.1 Galaxy S3

The measurements show that the Wi-Fi activity depends on all three parameters: "Wi-Fi switch", "Always allow scanning" and "Location". Obviously, when Wi-Fi is activated, the device sends Wi-Fi frames at any time and in particular when leaving the idle mode.

Starting Google Maps also triggers the emission of probe requests, but only if Location is activated. Probing is observed both when Google Maps is running or not.

An important observation is that disabling Wi-Fi does not necessarily prevent Wi-Fi activity. For instance, if "Always allow scanning" and Location are both activated, Wi-Fi traffic will be generated when Google Maps is used. This is likely due to the use of Google Wi-Fi-based location engine.

[3]These devices do not support MAC address randomization.

Wi-Fi switch	off	off	off	off	on	on	on	on
Always allow scanning	off	off	on	on	off	off	on	on
Location	off	on	off	on	off	on	off	on
Summary	×	×	✓	✓	✓	✓	✓	✓
Screen on	×	×	×	✓	✓	✓	✓	✓
Idle	×	×	×	×	✓	✓	✓	✓
Leaving Idle	×	×	×	×	✓	✓	✓	✓
Google Maps	×	×	×	✓	✓	✓	✓	✓
Starting Google Maps	×	×	×	✓	×	✓	×	✓
Uncorrelated			✓					

Table 1: Wi-Fi activity generated in various settings for the Galaxy S3.

Wi-Fi switch	off	off	on	on
Location	off	on	off	on
Summary	✓	✓	✓	✓
Screen on	×	×	✓	✓
Idle	×	✓	✓	✓
Leaving Idle	✓	✓	✓	✓
Google Maps	×	✓	✓	✓
Starting Google Maps	×	×	×	×

Table 2: Wi-Fi activity generated in various settings for the OnePlus One. On this device, the "Always allow scanning" is not displayed in the parameters. *Device immediately prompts for the user to activate location. Clicking "OK" does so.

Total lack of Wi-Fi activity was observed in only two configurations when both Wi-Fi and "Always allow scanning" were disabled, regardless of the Location option.

When both Location and Wi-Fi are disabled but not Always allow scanning, we observed Wi-Fi scan events for which we were unable to associate any specific activity on the device. In other words, those scan events seems to happen regardless of the activity on the phone. It is not clear what the purpose of those scans is.

3.2.2 OnePlus One

Results for the OnePlus One, presented in Table 2 are similar to the ones of the previous device, with the difference that the "always allow scanning" is not deactivatable. One difference subsists: when both the Wi-Fi switch and the location option are off, the device still sends a burst of probe requests each time it leaves idle mode. Reasons for this behavior aren't clear, but are troublesome: it means there is no way to prevent the device from send probe requests except using airplane mode or turning it off completely.

3.2.3 Nexus S

Results for the Nexus S, presented in Table 3, only reveal minor differences with the Galaxy S3. One notable behavior is that, even with Wi-Fi switch and location option turned off, the device sends a burst of probe requests every time the "always allow scanning" option is toggled.

Wi-Fi switch	off	off	off	off	on	on	on	on
Always allow scanning	off	off	on	on	off	off	on	on
Location	off	on	off	on	off	on	off	on
Summary	×**	×	×**	✓	✓	✓	✓	✓
Screen on	×	×	×	×	✓	✓	✓	✓
Idle	×	×	×	×	✓	✓	✓	✓
Leaving Idle	×	×	×	✓	✓	✓	✓	✓
Google Maps	×	×	×	✓	✓	✓	✓	✓
Starting Google Maps	×*	×	×*	×	×	×	×	×

Table 3: Wi-Fi activity generated in various settings for the Nexus S. *Device immediately prompts for the user to activate location. Clicking "OK" does so. **The device, however, sends a burst of probe requests upon activating or deactivating the "always allow scanning" option.

Wi-Fi switch	off	off	on	on
Location	off	on	off	on
Summary	×	×	✓	✓
Screen on	×	×	✓	✓
Idle	×	×	✓	✓
Leaving Idle	×	×	✓	✓
Google Maps	×	×	✓	✓
Starting Google Maps	×	×	×	×

Table 4: Wi-Fi activity generated in various settings for the HTC WildFire. The "Always allow scanning" option does not exist in the early version of Android running on this device.

3.2.4 HTC WildFire and Galaxy Spica

Results for the HTC WildFire, presented in Table 4, are not surprising. In this early version of Android where the "always allow scanning" option did not exist, probe requests are sent if and only if the Wi-Fi switch is on. Results for the Samsung Galaxy Spica are not included because very similar, with the only difference that the device was not seen sending probe requests in idle mode or when leaving it.

3.2.5 Moto G5 Plus

Results for the Lenovo Moto G5 Plus are presented in Table 5. It uses a slightly customized version of Android 7.0 and randomization behavior is surprising: the device seems to randomize the MAC address only when probing in idle mode. The "Always allow scanning" is accessible through the Wi-Fi settings but only when Wi-Fi is off and permanently through the "Location settings".

3.2.6 Summary of the measurements

All devices send Wi-Fi frames when Wi-Fi is activated, which is expected. When the Wi-Fi is deactivated, we observed two different behaviors depending on the version of Android. On older versions (2.2.1 and 2.3.7), no frames were observed when the Wi-Fi is turned off. On most recent versions (4.3 and above), Wi-Fi activity depends on whether the "Always allow scanning" option

Wi-Fi switch	off	off	off	off	on	on	on	on
Always allow scanning	off	off	on	on	off	off	on	on
Location	off	on	off	on	off	on	off	on
Summary	×	×	×	✓	✓	✓	✓	✓
Screen on	×	×	×	×	✓	✓	✓	✓
Idle	×	×	×	×	✓*	✓*	✓*	✓*
Leaving Idle	×	×	×	✓	✓	✓	✓	✓
Google Maps	×	×	×	✓	✓	✓	✓	✓
Starting Google Maps	×	×	×	×	×	×	×	×

Table 5: Wi-Fi activity generated in various settings for the Moto G5 Plus. * When the device is idle, it keeps probing but with randomized MAC addresses, otherwise the real MAC address is used

is activated. Wi-Fi frames are emitted if the "Always allow scanning" is activated no matter what is the status of the Wi-Fi switch. To fully prevent emission of Wi-Fi frames it is necessary to disable both the Wi-Fi and the "Always allow scanning" options. We note that on OnePlus One, the "Always allow scanning" is not available and it is thus impossible to prevent the phone from sending Wi-Fi frame without turning it off or using the plane mode.

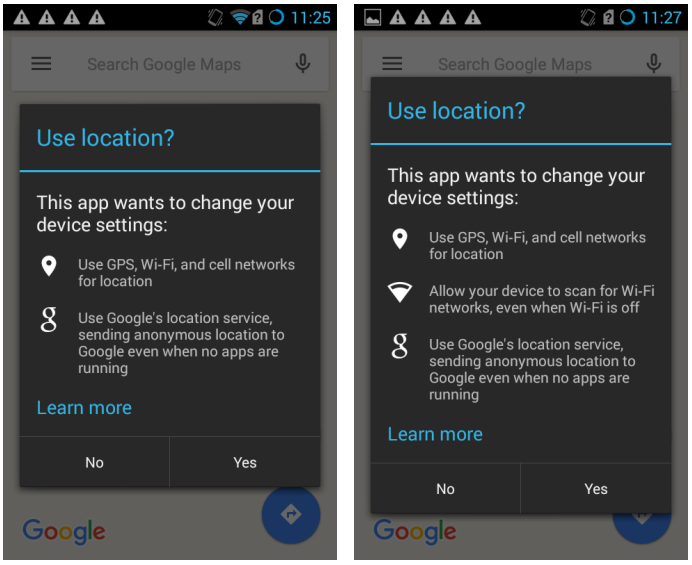
3.3 Probing frequency

Probing frequency varies across devices, configurations and situation. While this work does not aim to review these behavioral differences, it can still be noted that devices in some situation can be lead to send signals at a high frequency. In such case, the possibility of tracking these devices is raised to a fined-grained level. For instance, the OnePlus One sends probe requests every 5 seconds when the Google Maps application is open if either the Wi-Fi switch or the location option is on.

4 Prompting for location activation

On some versions of Android, devices in which location is not activated will immediately prompt the user to activate it upon launching Google Maps. On the HTC Wildfire, the user is redirected towards the related parameters section. On the OnePlus One, simply replying "OK" to the prompted message immediately activates the option. If the user ignores the message, it is not prompted again in later Google Maps startups. It is, however, prompted again if the user clicks on the location button (top button in the bottom right corner in Figure 2). On the Nexus S, we notice two possible outcomes (see Figure 2):

- If the Wi-Fi switch is deactivated and both location and the "always allow scanning" option are deactivated as well, the device will prompt the user to activate both and do so if the user replies "Yes".
- If the Wi-Fi switch is activated and both location and the "always allow scanning" option are deactivated, the device will only prompt the user to activate location, and remain the "always allow scanning" option untouched.



(a) "Always allow scanning" activated

(b) "Always allow scanning" deactivated

Figure 2: Google Maps prompting for Wi-Fi activation on the Nexus S

5 Conclusions

On Android, disabling Wi-Fi is not necessarily sufficient to prevent the device from sending Wi-Fi frames as some devices still generate Wi-Fi frames after Wi-Fi has been disabled. Therefore, **disabling Wi-Fi is not enough to escape data collection by Wi-Fi tracking systems**. To prevent the device from sending Wi-Fi frame, it is necessary to disable two features on the device: both Wi-Fi and the "Always allow scanning" option must be disabled in order to have a silent device. On some devices this option is not even available, meaning that the user cannot prevent its phone from sending Wi-Fi frames.

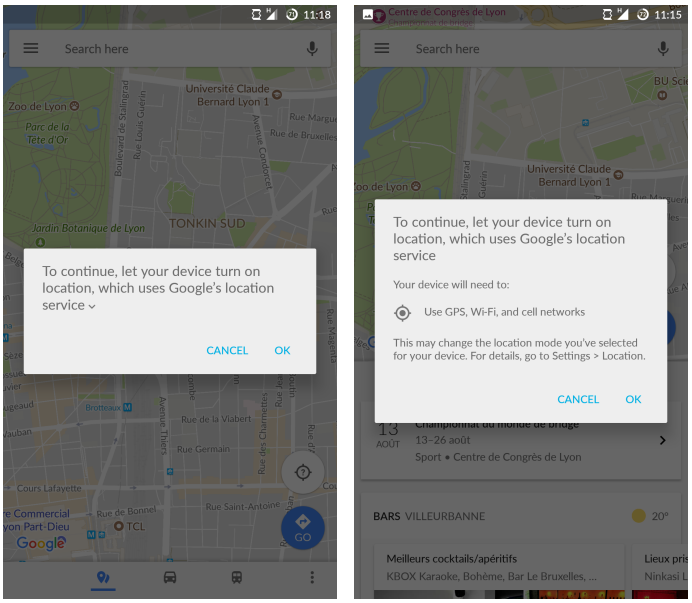
Although most recent versions of Android include MAC address randomization [1], there are still a number of devices that are not supporting this feature. The MAC address randomization feature has been introduced in version 6.0 of Android, and as of today 54.2% of Android devices are using an older version [2]. Furthermore, MAC randomization is activated provided that the hardware supports it, which is rarely the case as of 2017 [6].

References

[1] Android 6.0 changes. Retrieved from `https://developer.android.com/about/versions/marshmallow/android-6.0-changes.html`, 2015.

[2] Android dashboards: Platform versions. Retrieved from `https://developer.android.com/about/dashboards/index.html#Platform`, 2015. accessed 11-08-2017.

[3] Android location strategies. Retrieved from `https://developer.android.com/guide/topics/location/strategies.html`, 2015. accessed 11-08-2017.



(a) (b) same message after clicking on the arrow

Figure 3: Google Maps prompting for Wi-Fi activation on the OnePlus One

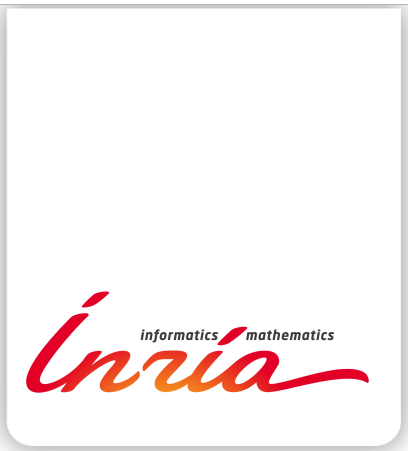
[4] Android scan forum. Retrieved from `https://android.stackexchange.com/questions/131414/do-android-devices-make-active-or-passive-scan-when-looking-for-wifi-ap`, 2015. accessed 14-08-2017.

[5] The Washington Post Brian Fung. How stores use your phone's WiFi to track your shopping habits, October 2013.

[6] Jeremy Martin, Travis Mayberry, Collin Donahue, Lucas Foppe, Lamont Brown, Chad wick Riggins, Erik C Rye, and Dane Brown. A study of mac address randomization in mobile devices and when it fails. *arXiv preprint arXiv:1703.02874*, 2017.

[7] A. B. M. Musa and Jakob Eriksson. Tracking Unmodified Smartphones Using Wi-fi Monitors. In *Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems*, SenSys '12, pages 281–294, New York, NY, USA, 2012. ACM.

Contents



RESEARCH CENTRE
GRENOBLE – RHÔNE-ALPES

Inovallée
655 avenue de l'Europe Montbonnot
38334 Saint Ismier Cedex

Publisher
Inria
Domaine de Voluceau - Rocquencourt
BP 105 - 78153 Le Chesnay Cedex
inria.fr

ISSN 0249-6399