ZEBRA

ANALYSIS OF iOS 8 MAC RANDOMIZATION ON LOCATIONING

Introduction

With the ever increasing population of Wi-Fi enabled Smartphone's and other devices, Location Based Services (LBS) and big data analytics are hot topics these days for many businesses. From improved shopper engagement and hotel guest experience, to tracking of assets, knowing where people and assets are located is a key ingredient to providing better services and end user experience. Both Wi-Fi™ and Bluetooth Low Energy (BLE) are common wireless technologies which are found in most consumer devices. The use of these two technologies provide a range of granularity for location accuracy, however their network connectivity and use cases are different.

Until recently, the unique, static MAC address of each Wi-Fi device has been used to uniquely identify a device; however, this has been changed with Apple's introduction iOS 8. Apple announced a new feature in iOS 8 that uses random Media Access Control (MAC) address for Wi-Fi radio in their products. The main motivation for Apple behind introducing this feature is to enable additional safeguard for consumer privacy, while increasing barriers for vendors who track and gather analytics based on the location of unconnected Wi-Fi devices.

This paper provides more details on this new iOS 8 MAC randomization feature and analyzes the impact of this on Wi-Fi locationing and analytics solutions in general. The goal is to help Zebra partners and customers in understanding what it means for location based services using our ADSP Proximity Awareness and Analytics and MPact solutions.

What is MAC Randomization and why did Apple introduce this as part of iOS 8?

A mobile phone, whose Wi-Fi is switched on, will continuously search for a Wi-Fi network to associate to. As part of this process, the phone sends out a packet called 'Probe Request'. The Probe Request is usually a broadcast packet sent to all the devices and includes the MAC address of the mobile phone. This MAC address is unique to that phone. Different phone vendors have different implementation on how frequently should these devices scan for wireless network.

In the last couple of years, business organizations have been using the Wi-Fi MAC address in the Probe Request to uniquely (anonymously though) identify a device and track the behavioral patterns of the user. This provides the business with some insights like number of devices seen, number of repeat users, number of new users. With some additional information like the signal strength, which can again be obtained from the Probe Requests, the access points can also determine how far the clients and gain even more insights as to whether the device was seen inside or outside the building, and this helps in providing analytics like footfalls etc.

iOS 8: Randomized Wi-Fi MAC Address

In the recent WWDC14, Apple reported the following:

"In iOS 8, Wi-Fi scanning behavior has changed to use random, locally administrated MAC addresses

- Probe requests (management frame sub-type 0x4)
- Probe responses (management frame sub-type 0x5)

The MAC address used for Wi-Fi scans may not always be the device's real (universal) address."

This clearly alludes that there are certain conditions under which they may randomize, or not use, the device's static or real MAC address and in other conditions they may use the device real MAC address.

http://devstreaming.apple.com/videos/wwdc/2014/715xx4loqo5can9/715/715_user_privacy_in_ios_and_os_x.pdf

For additional details on iOS 8 MAC randomization refer to:

http://www.networkworld.com/article/2361846/wireless/ios-8-mac-randomizing-just-one-part-of-apple-s-new-privacy-push.html

Since the device MAC address used on Probe Requests are tracked without the knowledge of the user or without opt-in, Apple introduced MAC randomization feature in iOS 8 to protect the privacy of the user.

http://support.apple.com/kb/HT6441

With the introduction of random MAC address, devices running iOS 8 could use pseudo MAC address (locally administered MAC Address) in Probe Request frames while searching for wireless networks. As a result, the MAC address transmitted in Probe Request frames by the iOS 8 device may not be real and it potentially changes every time device scans. To understand the behavior of IOS 8 devices, tests were conducted by Zebra Technologies . From the test results, we interpret and observe that the MAC randomization happens only in certain conditions that are not normal. Read below to understand more about this. Also, while the phone is connected to the Wi-Fi network, the phone always uses the real MAC address in the Probe Requests. So the MAC randomization should have, if at all, very little impact on locationing and analytics.

iOS 8 and Random MAC Address Behavior: Zebra's Observations

Zebra Technologies have performed some tests in the lab on different iPhone models with iOS 8 to better understand the behavior of random MAC used by Wi-Fi radio in these devices.

Based on our testing, we found that, only iPhone 5S and iPhone 6 devices have this feature enabled and for random MAC to occur on these models, the following conditions have to be met:

1. The phone wakes up from a sleep mode
2. The phone is not connected to Wi-Fi

Device Sleep mode — In order to save battery life, an iPhone goes into sleep mode when all the services in the phone are inactive, not just when the screen being switched off by the user. It is important to note that there are many applications that use location service, mail / message notification which could keep the phone awake despite the screen being off. So, in real life, it is very hard to make the phone go to sleep.

Device not connected to the Wi-Fi means the phone's Wi-Fi is turned on, but not associated to the wireless network.

Note that, other legacy Apple devices observed to be using real MAC address all the time.

Test Setup and Details

To understand the randomization of the Wi-Fi MAC address, Zebra Technologies have captured Probe Requests from above iPhone models with iOS 8.0.2 and analyzed the transmitted MAC address in those frames, under various scenarios.

Test Scenario 1

Cellular Voice	On
Cellular Data	On
Location Service	Off
Wi-Fi	On + Not Connected

In this first test, we enabled the phone's cellular voice and data services, but disabled the location service. In this state, even when the phone screen is in the off mode, we were never able to see the phone sending probe requests with a random MAC. The phone always appeared to use its original MAC address.

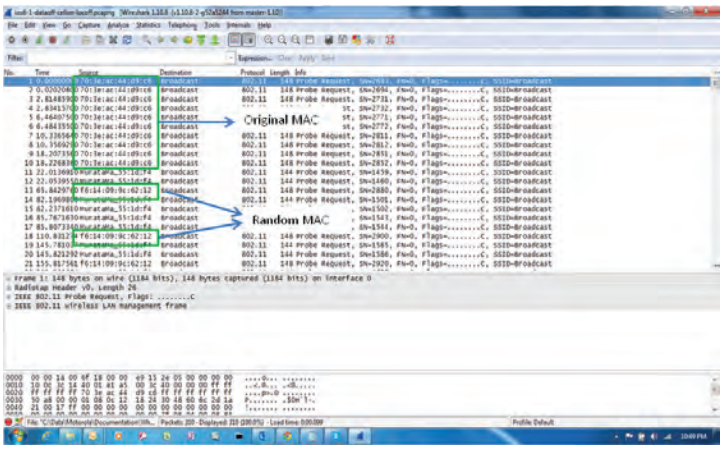
Test Scenario 2

Cellular Voice	On
Cellular Data	Off
Location Service	Off
Wi-Fi	On + Not Connected

In the second test, we turned off the phone's cellular data service and observed the behavior. In this scenario, when the phone's screen is unlocked and while the user is actively using the phone, the device always used its original MAC address for probe requests.

When the phone screen is locked, we observed that the phone sends Probe Request frames using its original MAC address initially for a few times. After a couple of seconds, it then sends out a probe request using a random MAC address. Keeping the phone screen locked, the phone sends probe request using the same random MAC address but at an increasing interval of time.

After about 10 minutes of observing the phone in this state, we noticed a Probe Request using its original MAC address. It is not clear what triggered this.



Interestingly, after the phone sent a couple of probe requests using the original MAC, it then starts using a different random MAC address for the probe request. The phone uses this same random MAC address until something triggers it to send a probe with its original MAC address.

This time, after observing for about 15 minutes, the phone was woken up by an alarm and we could see probe request with its original MAC address.

Test Scenario 3

Cellular Voice	On
Cellular Data	On
Location Service	Off
Wi-Fi	On + Not Connected

In this test, we connected the iPhone to the wireless network and monitored the behavior. In this state, again the phone always seemed to use its original MAC address and never used a random MAC address.

Impact on Wi-Fi Analytics

In an average user's phone, it is fair to assume that the user has some kind of notification applications (like email, gmail, messages, facebook, linkedin, whatsapp, twitter etc). In this most common scenario, according to our internal tests, we found that the phone never used the randomized MAC address. It's only when the device gets a chance to enter into sleep mode, the random MAC is potentially enabled. It is not very clear what conditions would cause the phone to go into sleep mode and also it is not easy to create those conditions in real life as most of the users run multiple applications on their phones which prevent the phone to go into sleep mode. As a result, in practice, the iPhone device rarely enables random MAC address, so overall it will not cause noticeable impact on the Wi-Fi analytics. When the iPhone device generates random MAC addresses, a single iOS 8 device can cause MPact / ADSP to count it multiple times in Wi-Fi analytics. But the impact could be eliminated by using MAC filtering for these locally administered MACs (for example, F6:14:09:9C:62:12 in above scenario) which do not have valid vendor prefix.

Impact on Wi-Fi Location Tracking

As far as Wi-Fi location tracking is concerned, MPact value proposition doesn't change as iOS 8 MAC address randomization is related only for devices scanning for wireless networks and that there is little business value in tracking location for unconnected devices due to the following reasons:

Firstly, when a device is not connected to the network, it doesn't transmit frames at regular interval. Depending on the manufacturer and operating system of the device, this interval could be even up to 5 minutes. So, when the visitor carrying any Wi-Fi device and moves around in the venue without connecting to the network, the estimated location of this device becomes stale very quickly. As a result, location tracking for unconnected device doesn't have much business value.

Secondly, in order to respect consumer privacy, venue-operators ensure that visitors opt-in and agree to their network policies before delivering location based services. Typically, this opt-in phase occurs when the visitor connects to the guest Wi-Fi network. So, the location tracking is important only for devices connected to the network. As iOS 8 devices uses real MAC addresses when they are connected to the network, there is no impact in tracking these devices.

What it Means for BLE Location Tracking and Analytics

Proximity Awareness and Analytics is now part of MPact platform, making it the only unified platform in the market that provides location based services and analytics based both Wi-Fi and BLE technologies. MPact supports Apple's iBeacon mode as well as Zebra Technologies proprietary mode to provide enhanced battery life-time for radio tags used in the solution. The BLE technology uses different architecture and it does not use MAC address of the device. As a result, there is no impact on the BLE based analytics and location based services offered by our MPact solution.

FOR MORE INFORMATION, PLEASE VISIT US ON THE WEB AT: WWW.ZEBRA.COM