IEEE P802.11
Wireless LANs

|  |
| --- |
| Randomized or Changing MAC address use cases |
| Date: 2019-09-15 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Mark Hamilton | Ruckus/CommScope | 350 W Java DrSunnyvale, CA 94089 | +1.303.818.8472 | mark.hamtilon2152@gmail.com |

Abstract

This submission contains some suggested use cases for the RCM TIG consideration. Each use case tries to identify whether it is randomized MAC addresses at the root of the problem, or rapidly changing the MAC address that causes the problem, and then to propose possible technical steps that could be taken/considered to address the problem raised.

The intent is to provide raw material that could be worked into content for the RCM TIG’s report to the Working Group.

R0 – initial version

**Use Case #1 – Initial infrastructure connection steering**

A dual-band smartphone is configured to prefer 802.11/Wi-Fi over cellular connection, to save the owner costs for their cellular plan. The users bring the phone within range of a multiple-AP infrastructure to which it has attached previously and has a stored configuration, for example at the user’s work or church. Before connecting to the Wi-Fi, the phone scans to discover the available APs.

During this scanning, the infrastructure monitors the signal levels at multiple APs and bands on those APs, determines which AP and band will provide the best service, and steers the client to that AP. This saves the client power by directing its scans and lowering the requirement for the client to thorough scan all APs and bands, and also saves the infrastructure from needing to steer the client after attachment which saves time, connection disruption and bandwidth for management frames.

**Randomized MAC address impacts**

None.

**Rapidly changing MAC address impacts**

If the connecting device changes its MAC address frequently while scanning, in extreme with every Probe Request, for example, the infrastructure does not have a way to correlate the different Probe Requests to make correct steering decisions.

**Future work on possible mitigations:**

Recommendations for, or mechanisms to control, the timing at which the client changes its MAC address while probing can manage the loss of correlation. Alternatively, another method for recognizing that multiple Probe Requests (across channels and bands) are from the same device would also provide the infrastructure the information it needs, without compromising privacy.

**Use Case #2 – Parental controls at home**

A parent has children of ages 10 and 7 years. The parent wants to block access to the home 802.11/Wi-Fi and control access to Internet content based on the user of various devices. For example, the parent has a laptop and a smartphone, and the children each have an age-appropriate laptop and the older child has a smartphone. The parent wants all these devices to be recognized when attaching to the Wi-Fi, without launching an application or using a portal. And, this needs to use a method that the kids can’t hack and circumvent. When one of the childrens’ friends visits, their device(s) should be given only very limited access (if any at all) to the Wi-Fi and Internet; thus unknown devices need to be distinguishable from one of the family’s devices.

**Randomized MAC address impacts**

The home Wi-Fi network has little value in changing its MAC address with any frequency, since there is little privacy loss in knowing that a MAC address associated with the home is detected in the home. However, the phones and laptops changing their MAC addresses frequently enough for privacy/anti-tracking reasons means that the home network cannot recognize or determine when a “authorized” phone is in range and should be allowed on the network, or what permissions should be granted once it is associated.

**Rapidly changing MAC address impacts**

Interactions between the phones and laptops and the home network will be done within the context of an association, so the MAC addresses should not be changing. However, the privacy aspects of whether there is a concern with being to identify when a particular individual is home (or at least their device is) could be explored. This is outside the scope of the random/changing MAC address study, however, and better belongs in a more advanced privacy study.

**Future work on possible mitigations:**

Investigate a method for an infrastructure network (in this case, a home network) to recognize a client device after they have been apart period of time and the device has changed its MAC address. This method must not introduce privacy concerns by exposing personal information about the presence of individuals at home (or decide that this is not a significant privacy concern).

**Use Case #3 – Home automation’s “Welcome home”**

Very similar to Use Case #2, above, two trends in home automation are converging: use of 802.11/Wi-Fi as the ‘backbone’ of the automation system; and a feature of the automation system which allows it to recognize when one of the residents arrives and “welcoming” them home by turning on lights, music, etc., tailed to the individual. This convergence means that using Wi-Fi to detect the individual’s arrival, by detecting their personal Wi-Fi device (smartphone, etc.) is a highly desirable capability.

Such arrival detection has the same concerns as stated above for Use Case #2 – Parental controls at home.

**Randomized MAC address impacts**

See Use Case #2.

**Rapidly changing MAC address impacts**

See Use Case #2.

**Future work on possible mitigations:**

See Use Case #2.

**Use Case #4 – “Pairing” smartphone to a car (with 802.11/Wi-Fi)**

Many modern cars have Wi-Fi capabilities. A common facility also available for some time is the ability to “pair” the smartphone to the car to access messages, calendar, contacts, etc, and make phone calls. This has largely been done with Bluetooth, but since the car has Wi-Fi already, a Wi-Fi based solution could be preferable.

To accomplish this, either the car needs to recognize phone and query it with a security validation, or the phone needs to recognize car and initiate the security validation. However, both devices are likely to change MAC addresses for privacy reasons.

**Randomized MAC address impacts**

Due to the car changing its MAC address frequently enough to prevent tracking, the phone no longer can detect which car it should pair to. Similarly, the phone changing its MAC address frequently enough, also for the same privacy/anti-tracking reasons, means the car cannot recognize or determine when a “paired” phone is in range and appropriate to initiate the security negotiation.

**Rapidly changing MAC address impacts**

For security reasons, it is likely that the actual paired interaction between the phone and car would be done over an association of some sort (perhaps the car acts an AP, and this is an infrastructure association, or perhaps it is some form of peer-to-peer association). In this situation, both the car and phone should be discouraged from changing their MAC addresses. However, this creates potential privacy concerns, as the car is now easily tracked for the duration of the phone-car pairing/association.

**Future work on possible mitigations:**

A method for either/both devices recognizing the other device after a period of time that they have been apart and either/both have changed their MAC addresses.

An exploration is needed of the privacy concerns of maintaining the same MAC address for the duration of the association, while the car is traveling. Solutions may involve a negotiated method for changing MAC addresses periodically while associated, that allows both devices in the association to follow the transition to new addresses, but is not “followable” by third parties.

**Use Case #5 – Airport security queue measurement**

Airport security (and immigration) line wait times can reach times of an hour or more. It has become a feature of airports to offer information about lines’ wait times to passengers, which requires the ability for an automated system to measure the “average” time individuals are spending in these lines.

A common idea for such measurement is to “track” the 802.11/Wi-Fi devices carried by people in the lines, and detect how long the devices are, effectively, stationary in the area of the queue.

Such tracking generally needs to be effective on devices that are not connected to any network, especially, for example, in an airport where the Wi-Fi is a fee-based service, so few people are attached. Further, the tracking needs to be effective across time spans of an hour or more for worst-case busy hours, when the information is most critically needed and needs to be accurate.

**Randomized MAC address impacts**

None. The airport has no need for identification of the specific device or user.

**Rapidly changing MAC address impacts**

If the device’s change their MAC address frequently while in line, it will be difficult or impossible for the infrastructure to make a determination of time spent in the immediate area.

**Future work on possible mitigations:**

Recommendations for, or mechanisms to control, the timing at which the client changes its MAC address while not connected is needed. Alternatively, another method for recognizing when traffic from a device while not associated (probably probing, across channels and bands) is from the same device would also provide the infrastructure the information it needs. Such a method would need to not compromise privacy - consideration needs to be given to the balance between how frequently an address change is needed, to sufficiently protect the user’s privacy.

**Use Case #6 – Grocery store traffic analysis**

It is now common for a grocery store (or similar retail spaces) to do considerable analysis of the “traffic flow” of their customers. Doing this lets the store recognize the areas that are frequented by most/many customers and also the common pairings or patterns of multiple areas that are frequented in the same visit by many customers. This could be reasons that help the customer (putting frequent items near the front of the store, putting common combinations near each other), or that help the store despite the customer (putting frequent items or frequent combinations far apart, to force the customer to walk through the rest of the store), but either way, someone is benefiting and expects to be able to gather the information to implement their policy.

However, the store does not need to have any information about the actual identity of the people being tracked. Further, the store needs to track people that have no relationship with the store, and are not associating to the store’s network.

To discover useful patterns, the store needs to track individuals for a reasonable period of time – say, roughly a half hour at a minimum.

**Randomized MAC address impacts**

None. The store has no need for identification of the specific device or user.

**Rapidly changing MAC address impacts**

If the device’s change their MAC address frequently while in the store, it will be difficult or impossible for the infrastructure to make a determination of the foot traffic patterns.

**Future work on possible mitigations:**

Just like the airport line estimate Use Case, above, recommendations for, or mechanisms to control, the timing at which the client changes its MAC address while not connected is needed. Alternatively, another method for recognizing when traffic from a device while not associated (probably probing, across channels and bands) is from the same device would also provide the infrastructure the information it needs. Such a method would need to not compromise privacy - consideration needs to be given to the balance between how frequently an address change is needed, to sufficiently protect the user’s privacy.

**Use Case #7 – Grocery store frequent shopper notifications**

A very different use case from the grocery store foot traffic analysis, is a grocery store that wants to recognize and reward frequent shoppers. This should be an “opt-in” service, where the shoppers that are interested in participating with the store indicate that they are willing to have the store know some identity that the store can use (possibly not their true or complete identity, however). For maximum effectiveness, such programs need to recognize when the customer enters (or approaches) the store, and provide information (such as daily specials for frequent shoppers) without any action on the user’s part. Additionally, the store should be able to build a profile of the user, and push content (with a cellular txt, perhaps, since the customer may not be associated to the store’s network) such as items that of likely interest to the customer and are on sale/special, when the customer is near those items in the store.

**Randomized MAC address impacts**

Very different from the foot traffic analysis use case, the frequent shopper use case does need some long-lived identification of the customer (or their commonly carried device), without requiring any user action nor an association with the store’s network.

In many ways, this use case is similar to the home automation and parental controls use cases. One important difference is that the user may not want to divulge true identity information to the store. But, even if a method is proposed for a pseudonym identity, such an identity needs to have a very long lifetime (months or years), and needs a method to still protect the user’s privacy from third parties (but not from the store itself).

**Rapidly changing MAC address impacts**

Interactions with the store could often be done without an association, yet the need for the long-lived identification still applies. So, whatever is used for this identification of the customer (MAC address or otherwise) needs to be stable and re-used within the area of the store, for months or years.

**Future work on possible mitigations:**

Similar to the home automation use case, investigate a method for an infrastructure network (in this case, the store network) to recognize a client device after they have been apart for a long time and the device has changed its MAC address. This method must not introduce privacy concerns by exposing trackable information about the individual to third-parties.

**Use Case #8 – Infrastructure (home or enterprise) with different SSIDs per band**

This use case is in reaction to two situations: first is a network where (for whatever reason, perhaps incorrectly) the network (a single LAN, really) has been deployed with different SSIDs on different bands (“XYZ24G” and “XYZ5G”, for example); and second is considering a device that will use a consistent MAC address for a given SSID, but generates a new random address for each new SSID. These scenarios have both been seen, relatively commonly, in the field.

In combination, these two scenarios result in the network infrastructure being unable to correlate the device’s signals, location, and network interaction on the two bands, which makes band steering effectively impossible.

**Randomized MAC address impacts**

It is not the randomization of the MAC address that is a direct impact in this use case, but the scope of that randomization. If the randomization is tied to the SSID, the problem will occur.

**Rapidly changing MAC address impacts**

Not directly applicable. The duration of the two MAC addresses being used by the client is orthogonal to the problem in this use case. It is noted that even devices that keep a given MAC address (for a given SSID) permanently, will still have the issue.

**Future work on possible mitigations:**

Produce recommendations that infrastructure networks that are actually a single LAN be deployed using a single SSID across the entire network, including multiple APs and multiple bands.

Alternatively, investigate a method for an infrastructure network to correlate a client device’s traffic, despite its use of more than one MAC address in that traffic.

**Use Case #9 – Infrastructure (home or enterprise): Probes are randomized, even to/with associated SSID**

A client that is using randomized MAC addresses could easily have an implementation that generates a new random MAC address for every Probe Request. This could even apply to Probe Requests that are directed to the associated SSID, when the client would otherwise use a consistent MAC address for transmissions within an association.

If the client has this extreme (or approaching this extreme) an implementation of MAC address randomization, it will have a strong impact on the infrastructure’s ability to making steering decisions for that client.

When attached to a multiple-AP infrastructure, if the client uses the stable MAC address when probing, the infrastructure can help steer the client across both APs and bands, to give the entire network better experience. This could apply to both directed probes and broadcast probes, too.

**Randomized MAC address impacts**

Similar to Use Case #8, it is not the randomization of the MAC address that is a direct impact in this use case, but the scope of that randomization. If the randomization applies to Probe Requests even when the device is associated, then the problem will occur.

**Rapidly changing MAC address impacts**

Not directly applicable (or entirely the point, depending on how you look at it). The duration of the stable MAC address being used by the client while associated is orthogonal to the problem in this use case. It is a question of whether Probe Requests are treated as special traffic even while associated, and do not use the stable MAC address.

**Future work on possible mitigations:**

Consider recommendations or requirements that devices that are associated to a network, and using a stable MAC address for communicating with that network, also must use that same stable MAC address for probing of the network, or any other SSID or broadcast.

Alternatively, similar to Use Case #8, investigate a method for an infrastructure network to correlate a client device’s probes, despite its use of more than one MAC address for the probes.

**Use Case #10 – Very common SSID (“starbucks”, “xfinitywifi”, etc.)**

An implementation method has been discussed where a client device uses randomized MAC addresses, but it remembers the random address associated with a given SSID, and relatively permanently uses that same address with that SSID, across multiple associations, or even while not associated with that (or any?) network.

Such an implementation addresses some of the Use Cases above, which is promising. However, it introduces a problem when considering an SSID that is very widespread and common, such a common retail chain’s SSID or a common hotspot provider’s SSID. In such a situation, while the device is mobile, it could easily be tracked by eavesdropping for that MAC address near many of the retailer or hotspot installations (potentially world-wide).

The tradeoff in this scenario is that without the same MAC address being used at these locations, the user will lose recognition for frequent across multiple attachments, which can lead to scenarios such as:

* Hotel sign on won’t have duration across the entire stay
* Frequent shoppers aren’t recognized, which leads to frustration and loss of benefits

**Randomized MAC address impacts**

It is not the randomization of the MAC address that is at question in this use case, but the duration of use of the random but stable MAC address that is used for a given association and SSID.

**Rapidly changing MAC address impacts**

It is the lack of rapidly changing MAC address that is the impact of this use case.

**Future work on possible mitigations:**

The concern raised here is one of protection of privacy. There is no technical issue for 802.11/Wi-Fi caused by this use case. The privacy topic should be addressed in a broader, privacy focused forum.