IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Adding a Use Case for Pervasive Monitoring to TIG Group Report | | | | |
| Date: 2019-11-12 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE | 3333 Scott boulevard  Santa Clara, California,  United States of America |  |  |
|  |  |  |  |  |

Abstract

An important use case is missing from the Randomized and Changing MAC Address Topic Interest Group’s (RCM TIG) group report.

**Discussion**:

A major use case that is affected by randomized and changing MAC addresses is that of an organization, such as a despotic government, which relies on fixed MAC addresses in 802 technologies to facilitate surveillance of people and tracking of their movements and behavior to effect societal control.

**Proposal**:

Direct the editor to add the following use case, 3.12, to the group report:

# Use-cases

RCM TIG has explored different use-cases that are impacted by the expected future prevalence of randomized and changing MAC addresses in .11 networks.

## Pervasive Surveillance

Some organizations, both public and private, have a strong desire to monitor people in their behavior and habits. Having a device constantly emitting a unique identifier can help such these organizations surveil people. When people move around, sensors that passively detect these unique identifier emissions can make note of the identifier. Time and location of the sensor can combine with this datum to create a large database of information that can enable tracking of people. Habits can be recorded and observed and deviations from an established baseline can result in an alert regarding the person’s behavior. Artificial intelligence and big data analytics can use this database of information to facilitate this effort. A database of who is where and when can be used for a multitude of purposes, some benign and some nefarious. Records in the database can be used as evidence in a government’s case against a citizen, and personal, and private information about people can be sold without their knowledge or approval.

802.11 is an obvious technology to build such a surveillance apparatus. Fixed MAC addresses will be used in mobile devices even when SIM cards are swapped out or removed. Laptops typically do not have a method of network access that is not bound to a MAC address. The tendency of unconnected devices to find a network results in active probing which can be passively detected, thereby enabling the surveillance apparatus. Indeed, the very nature of 802.11 network discovery and connection establishment compels exposure of MAC addresses and there is no way to disable their use. Using 802.11 to construct a surveillance database is an obvious choice.

* + 1. Randomized MAC address impacts

When a device uses a random MAC address it will be more difficult for organizations to accurately determine who the person using that address is. It will be necessary to obtain personally identifiable information from other sources in order to create records, thereby weakening the integrity of the database or making it more expensive to establish. Some people may slip through the system and may not be capable of being monitored by agents using the database.

* + 1. Rapidly changing MAC address impacts

A rapidly changing MAC (e.g. every minute) will result in the surveillance apparatus inputting increasingly worthless information into the database, eventually making the database unusable. The number of people detected by a sensor cannot be accurate, thereby denying the surveillance organization useful information. Even when other personally identifiable information can be assigned to a gleaned random MAC address, when the address changes the binding is lost. The more rapidly MAC addreesses change the harder it becomes to use 802.11 to build the surveillance database.

# Required .11 features for enabling use-cases

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Possible enabling measures \  Use-case in section | 3.1 | 3.2 | 3.3 | 3.4 | 3.5 | 3.6 | 3.7 | 3.8 | 3.9 | 3.10 | 3.11 |
| A smallest interval between MAC address changes | X |  | X | X |  |  |  |  |  |  |  |
| Recommendations for naming of SSID |  |  |  |  |  | X |  |  |  |  |  |
| Introduction of alternative layer 2  identifiers and method for carrying this identifier without breaking privacy |  | X |  |  | X |  |  | X | X | X | X |
| Correlation of information elements | X |  | X | X |  |  | X |  |  |  | X |

## Alternative identifiers

Access control and arrival detection in a home environment, grocery store frequent shopper notifications, and pervasive surveillance use-cases would be possible if there was a method for an infrastructure network to recognize a client device after they have been apart for a long time and the device has changed its MAC address.

## Correlation of information elements

An alternative way of enabling the Infrastructure connection steering, pervasive surveillance, airport queue measurement, and grocery store flow analysis use-cases is to provide another method of recognizing when traffic from a device while not associated is from the same device (probing across channels and bands). This could be 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.

**References:**