IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Adding a Use Case for Despotic Governments 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 a despotic government which relies on fixed MAC addresses in 802 technologies to facilitate surveillance of citizens and tracking of their movements and behaviour 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.

## Despotic Government

Some governments have a strong desire to control their citizens, monitor their behavior and habits, and force them to comply with government edicts. Having a device constantly emitting a unique identifier can help such governments surveil their citizens. When citizens 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 citizens. Citizens habits can be recorded and observed and deviations from an established baseline can alert the authorities to the citizen’s behavior. Artificial intelligence and big data analytics can use this databaser of information to facilitate societal control. In addition, despotic governments tend to control who can go where and when and such a surveillance apparatus will allow them to identify citizens and determine whether they are forbidden from being where they are and, if so, go arrest them. Records in the database can also be used as evidence in a government’s case against a citizen.

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 not be possible for the despotic government to accurately determine who the user 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 citizens may slip through the system and may not be capable of being controlled by government 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 despotic government useful information and thwarting its efforts to control its citizens. 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.

**References:**