IEEE P802.11
Wireless LANs

|  |
| --- |
| Rogue Containment use cases |
| Date: 2019-09-15 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Antonio de la Oliva | InterDigital/UC3M |  |  | aoliva@it.uc3m.es |
| Robert Gazda | InterDigital |  |  |  |
| Amelia Andersdotter | Article19 |  |  |  |

Abstract

This submission includes a new use case for RCM consisting of a managed network taking rogue containment measurements to not authorised access points started in a given area.

**Use Case #n – Rogue containment in infrastructure networks**

A managed WLAN network may consider the deployment of rogue containment measurements which prevent un-authorised access points and/or stations from operating in its service area. One such rogue containment mechanism entails de-authenticating users associated to access points which have not been previously allow-listed. Part of the allow-listing information required for this to work, is the MAC addresses of the AP and STAs respectively.

In order to start an AP in the area, the AP and STAs connecting to it will need to be allow-listed by the infrastructure network. For STAs periodically randomizing MAC addresses, the absence of a permanent identifier will preclude white-listing by the rogue containment mechanisms.

**Randomized MAC address impacts**

STAs will not be able to be allow-listed in the infrastructure, and will therefore not be able to connect to the newly deployed APs. Similarly, rogue STAs will be more difficult to discover and track.

**Rapidly changing MAC address impacts**

The faster the speed of change the more difficult to detect, track and/or allow-/block-list STAs.

**Future work on possible mitigations:**

One possible way of mitigating this scenario would be the disclosure of a permanent identifier attached to the STA. On the basis of this identifier, the infrastructure network could determine whether the STA is permitted to connect to an AP.