IEEE P802.11
Wireless LANs

|  |
| --- |
| TGbi Text Changes for MAC Privacy Enhancements section |
| Date: 2023-09-21 |
| Author(s): |
| Name | Company | Address | Phone | email |
| Carol Ansley | Cox Communications |  |  | carol@ansley.com |
| Po-kai Huang | Intel |  |  | po-kai.huang@intel.com |
|  |  |  |  |  |
|  |  |  |  |  |

**Abstract**

This document contains proposed text for Section 4.5.4.10 MAC privacy enhancements updated from teleconference discussions. Text for other sections was moved to a new submission.

R4 – updated from off-line discussions

The text below is based on REVme D3.0 text and P802.11beD4.0 text.

*Editor: Please make the following changes to this section.*

4.5.4.10 MAC privacy enhancements

When a non-AP STA searches for, and connects to, an infrastructure BSS, IBSS, or PBSS or attempts to discover services on a network preassociation, it defines the addressing of its MAC layer for the particular connection. If the STA uses a fixed MAC address in its over the air (OTA) transmissions it is trivial to track the STA. An MSDU transmitted by a STA is assigned a sequence number that, if never reset, can also be used to track a device irrespective of the MAC address. If OFDM is used, the PHY DATA scrambler used can enable tracking of a device irrespective of the MAC address if it is not reseeded. The dynamic nature of BSS membership combined with this tracking information allows for construction of a network of connections, locations, and behavior.

This network can be used to glean private and sensitive information regarding the individual behind the device. Furthermore, even without establishing a connection, a mobile or portable STA that gratuitously transmits Probe Request frames containing SSIDs of favored infrastructure BSS networks, or announces the existence of IBSS networks, can reveal potentially sensitive information about its location and location history. To mitigate this sort of traffic analysis a STA can support the ability to periodically and randomly change its MAC addresses and reset counters and seeds prior to association. Additional mitigation after association can be provided by EDP MAC Randomization. Other EDP features can be used to restrict OTA transmission of identifying parameters in management frames as well as data frames. While discovering networks, a STA can refrain from gratuitously transmitting Probe Request frames containing SSIDs of favored BSS networks.

*Editor: please add the following section to the end of section 4.5.4*

4.5.4.10a Enhanced Data Privacy (EDP) enhancements

Third parties observing the wireless medium may seek to track device locations and device activity. Using EDP features, a STA or MLD may reduce the amount of information disclosed in several ways. A STA or MLD may reduce the content of pre-association and association messages to reduce the opportunity to fingerprint the STA or MLD through its messages outside of a secured connection. An MLD may change its OTA MAC address(es) during an association either at its own request or at the direction of the AP MLD with which it is associated.

An AP MLD supporting BPE EDP features may reduce the availability of information about itself to a third party observer such as the ESS to which it belongs. An BPE AP MLD may protect the content of its Beacon frames and only be discoverable by BPE non-AP MLDs that are preconfigured to recognize the BPE AP MLD. A BPE EDP AP MLD and its associated non-AP MLDs may change their OTA MAC addresses together with associated values for both unicast and group transmissions.