IEEE P802.11
Wireless LANs

|  |
| --- |
| Frame Anonymization (FA) normative text for 11bi |
| Date: 2024-01-18 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Philip Hawkes | Qualcomm |  |  | phawkes@qti.qualcomm.com |
| Duncan Ho |  |  |  |
| Jouni Malinen |  |  |  |
| George Cherian |  |  |  |

Abstract

We propose the draft specification for the following requirements in contribution “11-23-0892-03-00bi-requirements-and-issues-tracking” for TGbi draft D0.1.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Requirement** | **Issue**  | **Status** | **Information** |
| 7 | 11bi shall define a mechanism for a CPE Client to initiate changing its own OTA MAC Address used with a CPE AP in Associate STA State 4 without any loss of connection. | MAC address change while associated | Discussions underway | See FAPU Request & FAPU Response 10.x.2.2 |
| 9 | Edited to: 11bi shall define a mechanism for a CPE Client and CPE AP to change the transmitted SN and the scrambler seed on downlink and uplink to uncorrelated new values in Associate STA State 4, without any loss of connection when the OTA MAC address of the CPE Client is changed. | MAC address change while associated | Discussions underway |  For SN, See 10.x.2.4.2 and 10.x.4. Scrambler seed not addressed in r00 and r01. |
| 10 | Edited to: 11bi shall define a mechanism for a CPE Client and CPE AP to change the transmitted PN on downlink and uplink to uncorrelated new values in Associate STA State 4, without any loss of connection when the OTA MAC address of the CPE Client is changed. | MAC address change while associated | Discussions underway | See 10.x.2.4.2 and 10.x.4 |
| 11 | 11bi shall define a mechanism for a CPE Client and CPE AP to change the CPE Client’s AID to an uncorrelated new value in Associate STA State 4, without any loss of connection when the OTA MAC address of the CPE Client is changed | MAC address change while associated | Discussions underway | See 10.x.2.4.1 |

*Notes:*

* *Requirement 13 (11bi shall define or reuse a mechanism for CPE Clients and CPE APs to protect the SA/DA values from exposure OTA to 3rd parties) is expected to use a different mechanism which will be introduced separately.*

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: editorial updates
* Rev 2: Changes proposed during Hawaii F2F Plenary Thursday 2023-11-16 PM1 Session.
* Rev 3: Changes proposed during TGbi call Thursday 2023-12-15.
* Rev 4: Changes proposed during TGbi call Thursday 2024-01-04. Text is significantly simplified. Removed text might be reintroduced in an informative annex in a future contribution.
* Rev 5: Approved text from Rev 3 for use in motion.

**Proposed spec text:**

The baseline for this text is 802.11 REVme D4.1.

***TGbi editor: Add new subclause of 10.x (Frame Anonymization) under clause 10 (MAC sublayer functional description) as follows:***

# 10.x Frame anonymization

10.x.1 Introduction

Some unencrypted fields in beacon frames and individually addressed frames contain values which facilitate *presence monitoring*, determining the continued presence of a client even if the long-term identity of the client cannot be determined. Presence monitoring can be a threat to privacy of the client user. User privacy can be improved by shortening the presence-monitoring time-windows. It is possible to limit presence-monitoring time-windows by doing (re-)association as defined in 11.3. However, (re-)association results in leaving State 4 and introduces a loss in connectivity which could create a negative user experience.

Frame anonymization (FA) is a EDP feature available when MLO is supported.

The unencrypted fields which facilitate presence monitoring of a non-AP MLD are:

* Traffic indication map (TIM), which allows determining the AIDs of associated non-AP MLDs.
* AID of associated non-AP MLDs.
* Address 1 (on the downlink) and Address 2 (on the uplink) which contains the MAC address of the Affiliated STA of the non-AP MLD on the link on which the frame is transmitted.
* Sequence Number (SN).
* Packet Number (PN).

FA enables restricting presence-monitoring time-windows to portions of a single association (that is, without leaving State 4). These time-windows are called *FA epochs*. For a given non-AP MLD, an FA epoch ends when the next FA Epoch starts. FA provides of the following functions:

* **FAPU:** A *frame anonymization parameter update (FAPU)* operation provides *FA parameters* for a set of one or more new FA epoch:
	+ *FA Epoch Start TSF*: the TSF time at which the FA Epoch starts.
	+ *FA AID*: new random value to be used as the non-AP MLD AID. The FA AID is selected by the AP MLD using implementation-specific means.

An FAPU can be performed at any time while a non-AP MLD is in State 4. When the TSF time reaches FA Epoch Start, then the non-AP MLD and AP MLD apply the other FA parameters to both transmitted and received frames. This results in the frames exchanged in an FA epoch appearing unrelated to the frames exchanged in other FA epoch.

* Additional FA parameters are generated at both the non-AP MLD and AP MLD:
	+ *FA STA MAC*: New random values for the Affiliated STA MAC address randomization for each set link are generated from KDK, FA Epoch Start, FA AID and the Link ID.
	+ *FA SN offset* and *FA* *PN offset*: new random values for use in SN / PN anonymization are generated from KDK, FA Epoch Start, FA AID and (in the case of SN) TID.
* **AID randomization:** The FA AID is used directly wherever AID is currently used.
* **Affiliated STA MAC address randomization**. For each link, the FA STA MAC address, is used directly in MAC header creation of the transmitter. These addresses are also used in the MAC header processing of the receiver: e.g., in Address 1 address filtering.
* **SN / PN anonymization**: The transmitter applies the FA SN Offset and FA PN Offset to the SN and PN values to produce over-the-air values which can be safely transmitted in the clear while maintaining anonymity. The transmitted values appear to do a random “jump” to a new starting value, and then continue incrementing from the new starting value. The intended receiver transforms the over-the-air values back to the original values of SN and PN.

NOTE—The following list clarifies the scope of attacks which FA mitigates:

* FA mitigates against presence monitoring across multiple FA epochs.
* FA does not mitigate against presence monitoring within a single FA epoch.
* FA does not mitigate identifying frames belonging to a single MLD within a single FA epoch.
* FA does not mitigate using traffic analysis using known transmission behavior of upper layer protocols for presence monitoring across multiple FA epochs.