IEEE P802.11
Wireless LANs

|  |
| --- |
| Frame anonymization (FA) functions text for 11bi |
| Date: 2024-03-11 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Philip Hawkes | Qualcomm |  |  | phawkes@qti.qualcomm.com |
| Duncan Ho |  |  |  |
| Jouni Malinen |  |  |  |
| George Cherian |  |  |  |

Abstract

We propose draft specification text for the following requirements in contribution “11-23-0892-03-00bi-requirements-and-issues-tracking” for TGbi draft D0.3.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **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 | Use of OTA MAC addressed in 10.71.4.4 and 10.71.5.1 |
| 8 | 11bi shall define a mechanism for a CPE AP to initiate **changing the OTA MAC Addresses of a set of associated CPE Client’s** in the BSS (those CPE Clients in Associate STA State 4) without any loss of connection. | MAC address change while associated | Discussions underway | See requirement 7 |
| 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 10.71.4.2 and 10.71.5.4. Scrambler seed not addressed. |
| 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 10.71.4.3 and 10.71.5.3. |
| 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 10.71.6. |

Revisions:

* Rev 0: Initial version of the document.

**High level summary of the changes:**

The text describes the provides additional details when frame anonymization is enabled.

**Proposed spec text:**

The baseline for this text is Draft P802.11bi\_D0.2

***TGbi editor: Apply the following changes to 10.71.4 (Frame anonymization and transmitting functions)***

### Frame anonymization and transmitting functions

1. This subclause describes the additional requirements for transmitting functions when frame anonymization is enabled.

#### Frame anonymization parameter set selection

The transmitting MLD shall select the FA parameter set generated for the current EDP epoch of the non-AP MLD at the time when the frame is to be transmitted for the first time (i.e., with the Retry subfield in the Frame Control field set to 0).

The transmitting MLD shall apply the changes to the transmitting functions shown in the subsequent subclauses of this subclause using this FA parameter set.

#### Sequence number anonymization

If the MAC header of the frame includes a Sequence Control field, then the transmitter shall compute an over-the-air SN (OSN) value from the value in the Sequence Number subfield as follows:

OSN = (SN + FA\_SN\_offset) mod 212,

where FA\_SN\_offset is the offset value generated for the sequence number space of the transmitting MLD (non-AP MLD or AP MLD) used in the frame (see Table 10-5 (Transmitter sequence number spaces)) in the FA parameter set selected for the frame.

The transmitter shall then place the OSN value in the Sequnce Number subfield of the Sequence Control field (see 9.2.4.4 (Sequence Control field)) thus overwriting the original SN value before anonymization.

#### Packet number anonymization

For encrypted frames, the transmitter shall compute an over-the-air PN (OPN) value from the PN value in the CCMP or GCMP header of the frame as follows:

OPN = (PN + FA\_PN\_offset) mod 248,

where FA\_PN\_offset is the PN offset value generated for the transmitting MLD (non-AP MLD or AP MLD) in the FA parameter set selected for the frame.

The transmitter shall then place the OPN value encoded in fields PN0, PN1, PN2, PN3, PN4, PN5 of the CCMP header (see 12.5.2.2 (CCMP MPDU format)) or GCMP header (see 12.5.4.2. (GCMP MPDU format) of the frame thus overwriting the original PN value before anonymization.

#### Frame anonymization and MAC header creation

MLD addressing shall be applied per 35.3.2 (MLD addressing) with the following addressing clarification:

* The MAC address of a STA affiliated with a non-AP MLD corresponding to a link is the FA MAC value assigned to that link in the selected FA parameter set.

***TGbi editor: Apply the following changes to 10.71.5 (Frame anonymization and receiving functions)***

### Frame anonymization and receiving functions

1. This subclause describes the additional requirements for receiving functions when frame anonymization is enabled.

#### Frame anonymization and address filtering

Address filtering shall be applied per 10.2.8 (MAC data service) with the addressing clarifications in 10.71.4.4 (Frame anonymization and MAC header creation).

A receiving STA affiliated with a non-AP MLD shall perform packet number de-anonymization (10.71.5.3) and sequence number de-anonymization (10.71.5.4) using the FA parameter set containing the FA MAC value matching the Address 1 field in the MAC header.

* *< The first sentence can be updated to include previous EDP epoch if allowing a transition period>.*

#### Frame anonymization and block ack scoreboarding

Block ack scoreboarding shall be applied per 35.3.8 (Block ack procedures in MLO), with the following clarifications:

* The values in the A1 field and A2 field of the (per-link) Block Ack shall be the values in the A2 field and A1 field (respectively) of the corresponding A-MPDU.
* The (per-link) Block Ack shall report the OSN values received in the SN field of the MPDU header within the A-MPDU (rather than reporting the SN values recovered after SN de-anonymization).

#### Packet number de-anonymization

For encrypted frames, the receiver shall recover the original PN value (assigned by the transmitter) from the OPN value encoded in the PN0, PN1, PN2, PN3, PN4, PN5 of the CCMP header or GCMP header as follows:

PN = (OPN - FA\_PN\_offset) mod 248,

where FA\_PN\_offset is the PN offset value generated for the transmitting MLD (non-AP MLD or AP MLD) in the FA parameter set selected for the frame.

1. The recovered original PN value shall replace the OPN value in subsequent processing of the frame in the receiving MLD.

#### Sequence number de-anonymization

For frames including an SN field in the MAC header, the receiver shall compute the original SN value from the OSN value in the SN field as follows:

SN = (OSN - FA\_SN\_offset) mod 212,

where FA\_SN\_offset is the offset value generated for the sequence number space of the transmitting MLD (non-AP MLD or AP MLD) used in the frame (see Table 10-5 (Transmitter sequence number spaces)) in the FA parameter set selected for the frame.

1. The recovered original SN value shall replace the OSN value in subsequent processing of the frame in the receiving MLD.
2. ***TGbi editor: Apply the following changes to 10.71.7 (Frame anonymization, TXOP and retransmission)***

### Frame anonymization, TXOP and retransmissions

This subclause describes the additional requirements for TXOP and retransmissions when frame anonymization is enabled.

All frames transmitted by a non-AP MLD within a TXOP shall use FA parameters from a single FA parameter set.

All frames transmitted by an AP MLD to a given non-AP MLD within a TXOP shall use FA parameters from a single FA parameter set corresponding to the non-AP MLD.

That is, no two frames transmitted by or to a non-AP MLD within a TXOP, use FA parameters from distinct FA parameter sets.

The transmitter shall anonymize retransmitted frames using the FA parameters from the same FA parameter set as the first transmission (i.e., the transmission with the Retry subfield in the Frame Control field set to 0).

* *< Further text describing the transition period (if any) is TBD>.*