IEEE P802.11
Wireless LANs

|  |
| --- |
| MAC header anonymization functions text for 11bi |
| Date: 2024-05-14 |
| 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. |

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Updated to address comments in Denver F2F Monday (2024-03-11) AM1 session.
	+ Deleting unnecessary text (e.g., summary text)
	+ Adding some missing text

Responses to some comments:

* + **Okan Mutgan** (Nokia): Comment on 10.71.4.2 (Sequence number anonymization).
	See 10.3.2.14.2 (Transmitter requirements)

“If dot11MACPrivacyActivated is true, the counter in each sequence number space shall be set to a random number modulo 4096 when the STA’s MAC address is changed.”

Do we need to add 11bi text to 10.3.2.14.2 too?

* + - Author’s response: Firstly, see clause 12.2.10 (Requirements for support of MAC privacy enhancements) which defines dot11MACPrivacyActivated:

“MAC privacy enhancements are enabled on a non-AP STA when dot11MACPrivacyActivated is set to true. The STA shall periodically change its MAC address to a random value while not associated to a BSS.”

Frame anonymization changes MAC address to a random value while associated to a BSS, so the identified text in 10.3.2.14.2 does not apply to frame anonymization.

Secondly, the proposed mechanism does not impact 10.3.2.14 (Duplicate detection and recovery) – it only impacts the values transmitted over the air. Consequently, no text is needed in 10.3.2.14.2.

* + **Okan Mutgan** (Nokia): Comment on 10.71.4.3 (Packet number anonymization).
	Does IPN for broadcast frames need protection?
		- Author’s response: Privacy for broadcast frames is a BPE feature, not a CPE feature. This this clause can be updated when BPE features are added.
* Rev 2: Updated to address comments in Denver F2F Tuesday (2024-03-12) PM2 session.
* Rev 3: Updated to address comments in Denver F2F Wednesday (2024-03-13) PM2 session.
* Rev 4: Proposal for Warsaw F2F.
	+ Renamed “frame anonymization” to MAC header anonymization” where appropriate, to clarify that the text does not apply to AID anonymization/obfuscation.
* Rev 5: Updated to address comments in Warsaw F2F Monday (2024-05-13) AM2 session.
	+ Removed section 10.71.7 which covered TXOP and retransmissions, as requested.
	+ Clarified the “mod 2N” notation, as requested.

**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\_D0.3.

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

### MAC Header anonymization and transmitting functions

* *< Add text to clarify when these functions are applied>.*

#### MAC header anonymization parameter set selection

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

* *< Retransmissions are TBD.>*

The transmitting MLD shall apply the changes shown in the subsequent subclauses of this subclause using this MAC header anonymization 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 + EDP\_SN\_offset) mod 212,

where EDP\_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 MAC header anonymization parameter set selected for the frame, and “mod 212” denotes reducing the result modulo 212 to a value in the range 0 to (212-1).

The transmitter shall transmit frames over the air using the OSN value in the Sequence Number subfield of the Sequence Control field (see 9.2.4.4 (Sequence Control field)).

#### Packet number anonymization

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

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

where EDP\_PN\_offset is the PN offset value generated for the transmitting MLD (non-AP MLD or AP MLD) in the MAC header anonymization parameter set selected for the frame, and “mod 248” denotes reducing the result modulo 248 to a value in the range 0 to (248-1).

The transmitter shall transmit frames over the air using 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).

#### Addressing

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 EDP\_STA\_MAC value assigned to that link in the selected MAC header anonymization parameter set.
* *< Add text to definition of EDP\_STA\_MAC to clarify that (a) Local/Global bit is set to value 0, local address and (b) Individual/Group bit is set to value 0, individual address>.*

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

### MAC header anonymization and receiving functions

* *< Add text to clarify when these functions are applied>.*

#### Address filtering

Address filtering shall be applied per 10.2.8 (MAC data service) with the addressing clarifications in 10.71.4.4 (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 MAC header parameter set containing the EDP\_STA\_MAC value matching the Address 1 field in the MAC header.

A receiving AP affiliated with a AP MLD shall perform packet number de-anonymization (10.71.5.3) and sequence number de-anonymization (10.71.5.4) using the MAC header anonymization parameter set containing the EDP\_STA\_MAC value matching the Address 2 field in the MAC header.

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

#### 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 - EDP\_PN\_offset) mod 248,

where EDP\_PN\_offset is the PN offset value generated for the transmitting MLD (non-AP MLD or AP MLD) in the MAC header anonymization parameter set selected for the frame, and “mod 248” denotes reducing the result modulo 248 to a value in the range 0 to (248-1).

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 - EDP\_SN\_offset) mod 212,

where EDP\_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 MAC header anonymization parameter set selected for the frame, and “mod 212” denotes reducing the result modulo 212 to a value in the range 0 to (212-1).

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