IEEE P802.11
Wireless LANs

|  |
| --- |
| Frame Anonymization (FA) normative text for 11bi |
| Date: 2023-01-15 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Philip Hawkes | Qualcomm Technologies, Inc. |  |  | 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.

**High level summary of the changes:**

The text addresses CPE features only – leaving open the option of introducing BPE features in the future..

* 10.x “Frame Anonymization”
	+ 10.x.1 “Introduction”.
	+ 10.x.2 “Signalling for frame anonymization”.
	+ 10.x.3 “MAC architecture for Frame Anonymization”.
	+ 10.x.4 “Frame anonymization and transmitting functions”.
	+ 10.x.5 “Frame anonymization and receiving functions”.
	+ 10.x.6 “Frame anonymization and AID”.
	+ 10.x.7 “Frame anonymization, TXOP and retransmissions”.

**Key to highlighting:**

* Yellow highlighting: identifies instructions to the TGbi editor.
* Green highlighting: identifies normative terms like “shall”, “may”, “should”.
* Pink highlighting with black text: identifies cross-references that will need hyperlinks.
* Pink highlighting with yellow text: identifies cross references to unknown clauses (which will also need hyperlinks).
* Blue highlighting: identifies items that may need addressing.

**List of open items:**

* Receiver might need new and old otaMAC and (for S1G) new and old otaAID. Propose excluding PV1.
* Signaling details . (10.x.2)
	+ Non-AP MLD timer after sending FAPU Request frame
	+ Time that a non-AP MLD waits after unsuccessful non-AP-MLD-initiated FAPU.
	+ Determining the active FA parameter set
* Do we need to worry about AID collisions during the FA epoch overlap? (10.x.6/7)
* Scrambler seed.
* SSN

**Proposed spec text:**

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

***TGbi editor: Add new definition to clause 3.2 (Definitions specific to IEEE Std 802.11):***

**active frame anonymization parameter set:** frame anonymization parameter set which are being applied by the transmitter to frames.

**frame anonymization**: MLO mechanisms mitigating against presence monitoring using unencrypted fields in beacon frames and individually addressed frames.

**frame anonymization epoch:** time window in which a set of frame anonymization parameters remain constant.

**frame anonymization parameter set**: set of parameters used in frame anonymization mechanisms.

**frame anonymization parameter update**: mechanism for establishing new parameters for use in frame anonymization mechanisms.

**over-the-air sequence number**: value transmitted in an individually addressed MPDU header in the place of the sequence number as part of frame anonymization.

**over-the-air packet number**: value transmitted in an individually addressed CCMP header or GCMP header in the place of the packet number as part of frame anonymization.

**presence monitoring**: determining the ongoing presence of non-AP MLDs associated to an AP MLD

**retiring frame anonymization parameter set:** frame anonymization parameter set which was active prior to the current active frame anonymization parameter set, where frames processed use that prior frame anonymization parameter set are still being retransmitted.

***TGbi editor: Add new acronyms to clause 3.4 (Acronyms and abbreviations)as follows:***

FA frame anonymization

FAPU frame anonymization parameter update

OSN over-the-airsequence number

OPN over-the-airpacket number

***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. <The paragraph is currently focussed on presence monitoring of clients only. To accommodate BPE, the paragraph can be updated to cover presence monitoring of AP also.>

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. <To accommodate BPE, the paragraph can be generalized to cover BSSID as well>
* 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 using KDK, FA Epoch Start and FA AID:
	+ *FA STA MAC*: New random values for the Affiliated STA MAC address randomization for each set link.
	+ <To accommodate BPE, FA BSSID or similar can be introduced>
	+ *FA SN offsets*: new random values for use in SN / PN anonymization are generated for each supported sequence number space of the AP MLD and each supported sequence number space of the non-AP MLD, see Table 10-5 (Transmitter sequence number spaces).
	+ *FA* *PN offsets*: new random values for use in SN / PN anonymization are generated for the PN assigned by the AP MLD and the PN assigned by the non-AP MLD.
* **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 filtering. <To accommodate BPE, the paragraph can be generalized to cover FA BSSID or similar>
* **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.

<Further introductory text on signalling may be required here>

<The text following this point has not been agreed. The text should be stated in a manner that is less normative>

When transitioning from an old FA epoch to a new FA epoch, there is a short overlap in time where the transmitter and receiver allow both retransmissions of old frames (created using FA parameters of the old FA epoch) and transmissions of new frames (created using FA parameters of the new FA epoch). Old frames and new frames are not mixed within a Block Ack or A-MPDU or (on the uplink) TXOP, since this would facilitate relating the old frames to the new frames, resulting in presence monitoring across the FA epoch transition.

10.x.2 Signalling for frame anonymization

<This clause will describe how FA parameter sets are established, define when an FA parameter set is “active” or “retiring”, and provide definitive text for dealing with error cases>

10.x.3 MAC architecture for frame anonymization

Figure 10-a (MAC data plane architecture for frame anonymization) is based on the MAC data plane architecture shown in Figure 5-2a (MAC data plane architecture (MLO) for individually addressed data frames) and Figure 5-2b (MAC data plane architecture for AP MLD and affiliated APs). Figure 10-a illustrates where FA impacts the MAC architecture.

NOTE— Many of the processes shown in Figure 10-a also apply to MLD-level MMPDU flows for the MAC control plane architecture, and the processes shown at the MLD lower MAC sublayer also apply to Control and Extension frames.

NOTE— On the transmitting flow, Figure 10-a shows the functions starting with “Sequence Number Assignment” and subsequent functions up to and including “A-MPDU Aggregation”. The set of functions is identical for AP MLD and non-AP MLD. Note the following differences from Figure 5-2a and Figure 5-2b:

* An FA-specific “SN/PN Anonymization” function has been added.
* The “MPDU Header and CRC Creation” function has decomposed into two functions “MPDU Header Creation” and “FCS Creation”.
* A “Retransmission” function has been added, to clarify where frame retransmission logic occurs. This function was implicit in Figure 5-2a and Figure 5-2b
* The “A-MPDU Aggregation” function is clarified to be applied when transmitting MPDU only.

NOTE— On the receiving flow, Figure 10-a shows the functions starting with “A-MPDU De-aggregation” and subsequent functions up to and including “Replay Protection per PN (optional)”. The set of functions is identical for AP MLD and non-AP MLD, except for the “MPDU distribution by TA (AP only)” function which is applied only in an AP MLD. Note the following differences from Figure 5-2a and Figure 5-2b:

* The “A-MPDU De-aggregation” function is clarified to be applied when transmitting MPDU only.
* The “MPDU Header and CRC Validation” function has decomposed into two functions “FCS Validation” and “MPDU Header Validation”.
* An “Address 1 address filtering” function has been replaced with “Address filtering” to accommodate filtering using both A1 and A2.
* An FA-specific “SN/PN De-anonymization” function has been added.
* The “MPDU Decryption” function has been renamed to “Frame Decryption”.



Figure 10-a MAC data plane architecture for frame anonymization

10.x.4 Frame anonymization and transmitting functions

1. This clause describes the changes to transmitting functions when FA is enabled.

**SN /PN anonymization**: This function is used for frame anonymization only. This function generates an over-the-air SN (OSN) value and an over-the-air PN (OPN) value from the SN value and PN value.

* The OSN value shall be computed from the SN value as OSN = SN + FA\_SN\_offset (mod 212), and the OPN value shall be computed from the PN value as OPN = PN + FA\_PN\_offset (mod 248), where
	+ FA\_SN\_offset and FA\_PN\_offset are generated for the active set of FA parameters for the non-AP MLD (established as per TBD SECTION in 10.x.2 (Signalling)), and
	+ “(mod 2n)” represents reducing the value modulo 2n to produce a value in the range [0, 2n-1].
* The OPN value shall be encoded in fields PN0, PN1, PN2, PN3, PN4, PN5 of the CCMP header or GCMP header of the frame.

**Frame header creation**: The following description assumes that the transmitting MLD and receiving MLD comprise a non-AP MLD with FA enabled and associated to an AP, and the Affiliated AP is on the same link as the Affiliated STA.

When the AP MLD transmits a protected individually addressed frame to the non-AP MLD, then the Affiliated AP shall create the frame header as per SECTION\_REF with the following changes:

* The Affiliated AP shall set A1 to the FA STA MAC address of the Affiliated STA in the active FA parameter set for the non-AP MLD (established as per TBD SECTION in 10.x.2 (Signalling)), and
* The Affiliated AP shall set the SN field to the OSN value computed for the by SN / PN anonymization function using the applicable FA SN offset in the active FA parameter set.

When the non-AP MLD transmits a protected individually addressed frame to the AP MLD, then the Affiliated STA shall create the frame header as per SECTION\_REF with the following changes:

* The Affiliated STA shall set A2 to the FA STA MAC address of the Affiliated STA in the active FA parameter set for the non-AP MLD (established as per TBD SECTION in 10.x.2 (Signalling)), and
* The Affiliated AP shall set the SN field to the OSN value computed for the by SN / PN anonymization function using the applicable FA SN offset in the active FA parameter set for the non-AP MLD.

<To accommodate BPE, the above text can be updated by adding similar text referring to setting A1 or A2 (as appropriate) to FA BSSID when BPE is enabled>

1. NOTE—As specified in 9.7.3 (A-MPDU contents), all MPDUs within an A-MPDU have the identical RA and the identical TA. When FA is applied, then at least one of the RA and TA changes when the FA parameters change. Consequently, if FA is enabled then all MPDUs within an A-MPDU have FA applied using a single set of FA parameters. Furthermore, FA is either applied for all MPDUs within an A-MPDU or FA is not applied for all MPDUs within an A-MPDU.
2. Frame anonymization considerations for TXOP and retransmissions are discussed in 10.x.7 (Frame anonymization, TXOP and retransmissions).
3. All other transmitting functions are unchanged (although some per-link functions are applied to fields and elements with values impacted by frame anonymization).

10.x.5 Frame anonymization and receiving functions

1. This clause describes the changes to receiving functions when frame anonymization is enabled.

**Address filtering**: Address filtering is the mechanism by which an Affiliated STA/AP determines (a) that it is as an intended receiver of a received frame, (b) the transmitting MLD, and (c) the context which the transmitting MLD used to generate the frame. When FA is enabled, then the Affiliated STA/AP additionally determines the FA parameter set used to generate the frame.

In the context of the address filtering function, a *valid FA STA MAC address* for an Affiliated STA (of a non-AP MLD with FA enabled) is an FA STA MAC assigned to the Affiliated STA in an active FA parameter set or a retiring FA parameter set.

< To accommodate BPE, a valid FA BSSID can be defined here and the text below updated by referring to a valid FA BSSID when BPE is enabled >

When FA is enabled for a non-AP MLD, then an Affiliated STA of the non-AP MLD shall identify a received protected individually addressed frame for which the Affiliated STA is the intended receiver as per SECTION\_REF using A1 and A2, with the following change:

* The Affiliated STA shall match A1 to a valid FA STA MAC address for the Affiliated STA (established as per TBD SECTION in 10.x.2 (Signalling)).

When FA is enabled for one or more non-AP MLD associated to an AP MLD, then an Affiliated AP of the AP MLD shall identify an individually addressed frame for which the Affiliated AP is the intended receiver as per SECTION\_REF using A1 and A2, with the following change:

* The Affiliated AP shall match A2 to the set of valid FA STA MAC addresses assigned to Affiliated STA on the link of the associated non-AP MLDs with FA enabled (established as per TBD SECTION in 10.x.2 (Signalling)) and the (non-FA) MAC addresses assigned to Affiliated STA on the link of the associated non-AP MLDs with FA disabled.

**(Per-link) Block Ack Scoreboarding**: The receiver applies per-link Block Ack Scoreboarding as per SECTION\_REF with the following changes:

* 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 / PN de-anonymization).
1. NOTE— The SN values in each SN space are assigned sequentially. If FA is enabled, then the MPDUs in an A-MPDU are processed using the same set of FA parameters (see Note 1), including the SN offset values. The resulting over-the-air (OSN) values for the MPDUs in an A-MPDU will differ by the same amounts as the SN values assigned to the MPDUs. Consequently, the (per-link) Block Ack Scoreboarding function using OSN when if FA is enabled is identical to (per-link) Block Ack Scoreboarding function using SN when if FA is disabled.
2. **SN /PN de-anonymization**: This function is used for frame anonymization only. This function recovers the SN value (assigned by the sequence number assignment function in the transmitting flow) from the OSN received in the frame, and recovers the PN value (assigned by the packet number assignment function in the transmitting flow) from the OPN value received in the frame.
* The OSN value shall be the value in the SN field of the frame Header.
* The OPN value shall be the value formed from the fields PN0, PN1, PN2, PN3, PN4, PN5 of the CCMP header or GCMP header of the received frame.
* The SN value shall be computed from the OSN value as SN = OSN - FA\_SN\_offset (mod 212), and the PN value shall be computed from the OPN value as PN = OPN - FA\_PN\_offset (mod 248), where
	+ The FA\_SN\_offset and FA\_PN\_offset are from the FA parameter set for the non-AP MLD which the address filtering function determined was used to generate the frame (established as per TBD SECTION in 10.x.2 (Signaling)), and
	+ “(mod 2n)” represents reducing the value modulo 2n to produce a value in the range [0, 2n-1].
* The OSN value shall be replaced by the computed SN value.
* The OPN value shall be encoded in fields PN0, PN1, PN2, PN3, PN4, PN5 of the CCMP header or GCMP header of the frame.
1. Frame anonymization considerations for TXOP and retransmissions are discussed in 10.x.5 (Frame anonymization, TXOP and retransmissions).
2. All other receiving functions are unchanged (although some per-link functions are applied to fields and elements with values impacted by frame anonymization).

10.x.6 Frame anonymization and AID

Wherever AID of the non-AP MLD would be used (if FA was not enabled), the FA AID of the active FA parameter set for the non-AP MLD (established as per TBD SECTION in 10.x.2 (Signaling)),, shall be used by when FA is enabled.

NOTE— Some frames include either AID directly (e.g., AID12 subfield of a User Info field in a trigger frame) or a field generated using AID values (e.g., TIM element in a beacon frame). If FA is enabled, then the TIM element of a beacon frame is computed using the FA AID, and the AID12 subfield of a User Info field in a trigger frame is set to the FA AID.

10.x.7 Frame anonymization, TXOP and retransmissions

This clause describes the considerations for TXOP and retransmissions when using frame anonymization.

All frames in a TXOP shall have identical values in the A2 field.

NOTE— (Motivation for the preceding requirement) When FA is not enabled, then the value in the A2 field of frames transmitted by a given MLD on a given link do not change within an association, and (in this case) all frames in a TXOP implicitly have identical values in the A2 field. When FA is enabled, the value in the A2 field of frames transmitted by a given device on a given link can change within an association, and (unless prohibited) a TXOP can include frames with distinct values in the A2 field. If a TXOP includes frames with distinct values in the A2 field, then an eavesdropper learns that those values of A2 correspond to a single MLD. This might facilitate presence monitoring over multiple FA epochs. An explicit requirement is added to prevent this situation.

<This clause will also explain what happens during the transition to a new FA parameter set, while the previous FA FA parameter set is “retiring” (i.e., only retransmissions of frames using the previous FA parameter set), addressing aggregation/de-aggregation and TXOP considerations. Work in progress. >