IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Frame Anonymization for 11bi | | | | |
| Date: 2023-10-12 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Philip Hawkes | Qualcomm |  |  | phawkes@qti.qualcomm.com |
| Jouni Malinen |  |  |  |
| Duncan Ho |  |  |  |
| 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 |  |
| 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 |  |
| 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 |  |
| 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 |  |

*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.

**High level summary of the changes:**

Includes Frame Anonymization in figures and text of 5.1.5.1 ((General) introducing the MAC data-plane architecture).

**Proposed spec text:**

The baseline for this text is 802.11be D4.0.

***TGbi editor: Apply the following changes in clause 5.1.5.1 (General):***

***TGbi editor: CHANGE 1. Replace Fig 5-2a (MAC data plane architecture (MLO) for unicast data frames) as with the following (updated blocks have orange fill):***



***TGbi editor: CHANGE 2. Replace Fig 5-2b (MAC data plane architecture for AP MLD and affiliated APs) as with the following (updated blocks have orange fill):***



***TGbi editor: CHANGE 3 Apply the following change:***

The MLD upper MAC sublayer functions include:

* Authentication, association, and reassociation (between an AP MLD and a non-AP MLD)
* Security association (e.g., PMKSA, PTKSA) and distribution of GTK/IGTK/BIGTK
* Frame anonymization parameter update (FAPU) (between an AP MLD and a non-AP MLD).
* SN/PN assignment for frames to be encrypted by PTK for unicast frames

***TGbi editor: CHANGE4 Apply the following change:***

The MLD lower MAC sublayer functions include:

* SN / PN anonymization
* Link specific control information exchange/indication (e.g., RTS/CTS, acknowledgements, NDP, etc.)

***TGbi editor: CHANGE 5 Insert the following after NOTE 4 and before text on the “Block Ack Scoreboarding” block:***

When MLO is being used, Frame Anonymization (FA) maintains anonymity of the non-AP MLD while the non-AP MLD is in State 4. FA consists of the following functions:

* Frame anonymization parameter update (FAPU), which establishes a new AID for the non-AP MLD, a new STA MAC address for each affiliated non-AP STA, and new parameters for SN / PN anonymization.

NOTE 1— PN anonymization applies to the PN corresponding to TK and SN anonymization applies to the (per-TID) SN of the individually addressed data/management frames.

* Applying the parameters established during a FAPU results in frames that appear unrelated to the frames prior the FAPU. A FAPU can be initiated at any time while the non-AP MLD is in State 4.

NOTE 2— AID is not used in MAC data plane architecture and is consequently absent in Figure 5-2a (MAC data plane architecture (MLO) for unicast data frames) (11bi?) and Figure 5-2b (MAC data plane architecture for AP MLD and affiliated APs) (11bi?).

* The latest STA MAC address generated by the FAPU and the previous STA MAC address used by the non-AP MLD for an affiliated non-AP STAs are used directly for MPDU header creation in the MLD lower MAC sublayer of the transmitter and Address 1 address filtering in the MLD lower MAC sublayer of the receiver.
* SN / PN anonymization transforms the predictable “internal” values of SN and PN (assigned in the MLD upper MAC layer) into “over-the-air” values which can be safely transmitted in the clear while maintaining anonymity. SN / PN de-anonymization in the intended receiver transforms the “over-the-air” values back to the “internal” values. Functions which use SN and/or PN in the MLD upper MAC sublayer make use of the “internal” values (e.g., decryption and replay detection), while functions which use SN in the MLD lower MAC sublayer make use of the “over-the-air” values (e.g., MPDU header creation and Block Ack scoreboarding).