IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Establishing frame anonymization parameter sets text for 11bi | | | | |
| Date: 2024-09-11 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Philip Hawkes | Qualcomm |  |  | phawkes@qti.qualcomm.com |
| Duncan Ho |  |  |  |
| Jouni Malinen |  |  |  |
| George Cherian |  |  |  |

Abstract

Abstract

This submission proposes resolution of comments received against the following sections of TGbi Draft 0.4:

* 10.71.1 (Introduction).

We propose draft specification text for TGbi draft D0.6.

Accepted/Revised CID with changes in this document: 1068, 1312, 1313, 1314, 1316, 1503

Accepted CID with changes addressed by other CID in this document:

Rejected CID:

Open CID:

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Addresses feedback during 2024-09-09 F2F Hawaii PM2 session
* Rev 2: Addresses feedback during 2024-09-10 F2F Hawaii AM2 session, and some subsequent minor editorial updates.
* Rev 3: Addresses feedback during 2024-09-11 F2F Hawaii AM2 session, and some subsequent minor editorial updates.

| **CID** | **Commenter** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| --- | --- | --- | --- | --- | --- | --- |
| 1312 | Mark RISON | 10.71 | 53.26 | Why is frame anonmyisation restricted to MLDs? Why don't non-MLDs want to be anonymous? | As it says in the comment | **Revised**.  TGbi has consensus that frame anonymization is used only with MLDs. The reason was that non-MLDs do not allow for link/OTA MAC address independent of MAC addresses used for authentication.  It would be helpful to identify (at the start of the section) that frame anonymization is MLO only.  Document 1606r2 accounts for resolution of this CID.  Instruction to the editor: apply changes referenced with tag: #1312 |
| 1068 | Antonio DeLaOlivaDelgado | 10.71.1 | 53.29 | The phrase "The unencrypted fields that facilitate presence monitoring of a non-AP MLD are:" applies to non MLO STAs too, it is the mechanism to solve it the one applied only to MLO STAs. Change non-AP MLD to non-AP STAs. | As in comment | **Revised.**  Document 1606r1 accounts for resolution of this CID.  Instruction to the editor: apply changes referenced with tag: #1068 |
| 1313 | Mark RISON | 10.71.1 | 53.13 | "Some unencrypted fields in Beacon frames and individually addressed frames contain values that facilitate presence monitoring," -- which fields in Beacon frames? At line 30 the AID is referred to, but how does this facilitate presence monitoring per se, in the context of Beacon frames? | As it says in the comment | **Revised**.  The TIM in Beacon frames (and TIM frames), contain the AID of non-AP MLD for which the AP MLD has buffered data frames. An attacker can monitor TIMs in Beacon/TIM frames and note which AIDs are used to form the TIM. This can be used to deduce “the continued presence of a non-AP MLD even if the long-term identity of the non-AP MLD cannot be determined.”, which is the definition of presence monitoring (as noted in CID 1314). This is covered by including text “and fields and elements derived from the AID” at P.L=53.30 which also addresses CID 1503.  Document 1606r1 accounts for resolution of this CID.  Instruction to the editor: apply changes referenced with tag: #1313 |
| 1314 | Mark RISON | 10.71.1 | 53.13 | "Some unencrypted fields in Beacon frames and individually addressed frames contain values that facilitate presence monitoring, determining the continued presence of a non-AP MLD even if the long-term identity of the non-AP MLD cannot be determined." is unclear | Was "Some unencrypted fields in Beacon frames and individually addressed frames contain values that facilitate presence monitoring, i.e. determining the continued presence of a non-AP MLD, even if the long-term identity of the non-AP MLD cannot be determined." intended? | **Accepted.**  Document 1606r0 accounts for resolution of this CID.  Instruction to the editor: apply changes referenced with tag: #1314 |
| 1316 | Mark RISON | 10.71.1 | 54.01 | It is not clear how this list differs from the lists on page 53 | Clarify | **Accepted.**  The text from P.L=31.41 to 54.15 adds un-necessary details. Alternative text is provided for those lines.  Document 1606r0 accounts for resolution of this CID.  Instruction to the editor: apply changes referenced with tag: #1316 |
| 1503 | Mark RISON | 10.71.1 | 54.01 | If the AID is changed, does the partial AID change? If not, then you can be tracked with that, but if so there will be issues with receivers needing to be able to receive on two partial AIDs (the "old" one and the "new " one) | As it says in the comment | **Revised**  Agreed in principle.  However, the text referenced here has been removed by the changes for CID 1316. This is covered by including text “and fields and elements derived from the AID” at P.L=53.30, which also addresses CID 1313.  Document 1606r0 accounts for resolution of this CID.  Instruction to the editor: apply changes referenced with tag: #1503 |

**Proposed spec text:**

***TGbi editor: Apply the following changes to 10.71.1 (Introduction). The baseline for this text is Draft P802.11bi\_D0.5.***

* **Introduction**

Frame anonymization (FA) is an EDP CPE feature available when MLO is supported.(#1312)

Frame anonymization addresses unencrypted fields and elements in Beacon frames and individually addressed frames contain values that facilitate presence monitoring of a non-AP MLD (#1068), i.e., (#1314)determining the continued presence of a non-AP MLD even if the long-term identity of the non-AP MLD cannot be determined. Presence monitoring can be a threat to privacy of the user of the non-AP MLD. User privacy can be improved by shortening the presence monitoring time windows(#Ed). It is possible to limit presence monitoring time windows by doing (re)association as defined in 11.3 (Authentication and association). However, (re)association results in leaving State 4 and introduces a loss in connectivity that could create a negative user experience.

(#1312)

The unencrypted fields and elements that facilitate presence monitoring of a non-AP MLD are:

* AID and fields and elements derived from the AID(#1313,#1503)(#1068).
* Address 1 (on the downlink) and Address 2 (on the uplink)(#1068).
* Sequence Number (SN).
* Packet Number (PN).

FA enables restricting presence monitoring time windows(#Ed) to portions of a single association (that is, without leaving State 4). These time windows are the EDP epochs described in 10.71.2 (EDP epoch operation). A new frame anonymization parameter set (FA parameter set) is established between the AP MLD and non-AP MLD for each new EDP epoch of the non-AP MLD as described in 10.71.3 (Establishing frame anonymization parameter sets).

The transmitting MLD applies the processing in 10.71.4 (MAC header anonymization and transmitting functions) to the identified MAC header fields.

* The sequence number and packet number (assigned by the transmitting MLD) are transformed into over the air values that can be safely transmitted in the clear while maintaining anonymity.
* The Address 1 field (on the downlink), or the Address 2 field (on the uplink), is set to a temporary random MAC address for the affiliated STA of the non-AP MLD on the link on which the frame is transmitted.

The intended receiving MLD applies the processing described in 10.71.5 (MAC header anonymization and receiving functions) to the over the air MAC header field values.

* During address filtering, the over the air value in Address 1 (on the downlink) or Address 2 (on the uplink) is matched to the temporary random MAC address for the affiliated STA of the non-AP MLD on the link on which the frame is transmitted.
* The over the air values for the sequence number and packet number are transformed back to the original sequence number and packet number assigned by the transmitting MLD.(#1316)

NOTE—The following list clarifies the scope of attacks that 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 transmitted from 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.