IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proposed Draft Text for Multi-Link Security for Individual Management Frame | | | | |
| Date: 2022-05-06 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Guogang Huang | Huawei |  |  | huangguogang1@huawei.com |
| Michael Montemurro |  |  |  |
| Stephen McCann |  |  |  |
| Ming Gan |  |  |  |
| Yuchen Guo |  |  |  |
| Yunbo Li |  |  |  |
| Yiqing Li |  |  |  |
| Zhenguo Du |  |  |  |
| Rob Sun |  |  |  |
| Mengyao Ma |  |  |  |

Abstract

This submission contains proposed comment resolutions to comments on P802.11be D1.5.

CID 5181 and 5184 are resolved.

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: include CID 5181

**Introduction**

***Editing instructions formatted like this are intended to be copied into the TGbe Draft 1.5 (i.e., they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

***TGbe Editor: Editing instructions preceded by “TGbe Editor” are instructions to the TGbe editor to modify existing material in the TGbe draft. As a result of adopting the changes, the TGbe editor will execute the instructions rather than copy them to the TGbe Draft.***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CID | Commenter | Page.  Line | Clause Number | Comment | Proposed Change | Resolution |
| 5181 | Guogang Huang | 216.19 | 12.5.3.31 | For the individually addressed protected robust Management frames, how to construct AAD is missing | Please add a subclause to describe how to encrypt the individual MMPDU. The solution is proposed in my presentation DCN21/571 | REVISED  Agreed in principle. Similar to the individually addressed data frame, the MLD MAC address should be used when constructing AAD for the individually addressed Management frame.  Instructions to the editor:  Please make the changes to the spec as shown in 11/21-0704r1 |
| 5184 | Guogang Huang | 215.41 | 12.5.3.31 | Define how to construct AAD for individually addressed management frame | As in comment | REVISED  Agreed in principle. Similar to the individually addressed data frame, the MLD MAC address should be used when constructing AAD for the individually addressed Management frame.  Instructions to the editor:  Please make the changes to the spec as shown in 11/21-0704r1 |

**Discussion:**

Considering that the PTK is derived based on the MLD MAC address, it is reasonable to respectively replace A1, A2 and A3 fields with the corresponding MLD MAC address when constructing AAD for the individually addressed Management frame.

The benefit is the AAD will not change and thus no need to re-encrypt it when retransmitted on another link.

**SP. In R1, do you support that the AAD shall not be changed when an individually addressed MMPDU that is allowed to be transmitted on any enabled link? Specifically,**

1. **Replacing Addresses A1, A2 and A3 with corresponding MLD MAC Addresses for AAD computation,**
2. **Using MLD MAC address in A2 for constructing Nonce.** 
   * + 1. **CCMP cryptographic encapsulation**
          1. **General**

***TGbe editor: Change the first paragraph as follows:***

In case of a secure PV0 MPDU that is an individually addressed frame to be encrypted by an MLD, construct the CCM nonce block as defined in [12.5.3.3.4 (Construct CCM nonce](#bookmark5)) from the PN, transmitting MLD MAC address, and the priority value of the MPDU. Otherwise, construct~~Construct~~ the CCM nonce block as defined in [12.5.3.3.4 (Construct CCM nonce)](#bookmark5) from the PN, A2, and the priority value of the MPDU where A2 is MPDU Address 2. If the Type field of the Frame Control field is 10 (Data frame) and there is a QoS Control field present in the MPDU header, the priority value of the MPDU is equal to the value of the TID subfield of the QoS Control field (bits 0 to 3 of the QoS Control field). If the Type field of the Frame Control field is 00 (Management frame) and the frame is a QMF, the priority value of the MPDU is equal to the value in the ACI subfield of the Sequence Number field. Otherwise, the priority value of the MPDU is equal to the fixed value 0.

* + - * 1. **Construct AAD**

***TGbe editor: Change the first paragraph as follows:***

FC – MPDU Frame Control field, with

Subtype subfield (bits 4 5 6) in a Data frame masked to 0

Retry subfield (bit 11) masked to 0

Power Management subfield (bit 12) masked to 0

More Data subfield (bit 13) masked to 0

Protected Frame subfield (bit 14) always set to 1

vi) +HTC subfield (bit 15) as follows:

Masked to 0 in all Data frames containing a QoS Control field

Unmasked otherwise

vii) Other subfields are not modified

~~A1 – MPDU Address 1 field.~~If dot11MultiLinkActivated is true, for both the transmitter and intended receiver of the MPDU, either of To DS or From DS subfields in the MAC header of the MPDU is set to 1, and the MPDU is an individually addressed frame (#4924)between an AP MLD and a non-AP MLD associated with the AP MLD, then A1 is set to:

* the MLD MAC address of the intended receiver MLD of the MPDU.
* otherwise, Al is set to MPDU Address 1 field.

~~A2 – MPDU Address 2 field.~~If dot11MultiLinkActivated is true, for both the transmitter and intended receiver of the MPDU, either of To DS or From DS subfields in the MAC header of the MPDU is set to 1, and the MPDU is an individually addressed frame (#4924)between an AP MLD and a non-AP MLD associated with the AP MLD, then A2 is set to:

* the MLD MAC address of the transmitting MLD of the MPDU.
* otherwise, A2 is set to MPDU Address 2 field.

~~A3 – MPDU Address 3 field.~~If dot11MultiLinkActivated is true, MPDU Address 3 field is BSSID and the MPDU is an individually addressed frame (#4924)between an AP MLD and a non-AP MLD associated with the AP MLD, then:

* (#4924)A3 is set to the MLD MAC address of the AP MLD, where the corresponding AP with the BSSID is affiliated with the AP MLD.
* (#4924)Otherwise, A3 is set to the MPDU Address 3 field.

SC – MPDU Sequence Control field, with the Sequence Number subfield (bits 4–15 of the Sequence Control field) masked to 0. The Fragment Number subfield is not modified.

~~A4 – MPDU Address field, if present.~~A4, if present, is set as follows:

* if dot11MultiLinkActivated is true, MPDU Address 4 field is a BSSID, and the MPDU is an individually addressed frame (#4924)between an AP MLD and a non-AP MLD associated with the AP MLD, then A4 is set to the MLD MAC address of the AP MLD, where the corresponding AP with the BSSID is affiliated with the AP MLD.
* otherwise A4, if present, is set to the MPDU Address 4 field.

QC – QoS Control field contains the MSDU priority, if present. The QC TID is used in the construction of the AAD. When in a non-DMG BSS and both the STA and its peer have their SPP A-MSDU Capable fields equal to 1, bit 7 (the A-MSDU Present field) is used in the construction of the AAD. The remaining QC fields are masked to 0 for the AAD calculation (bits 4 to 6, bits 8 to 15, and bit 7 when either the STA or its peer has the SPP A-MSDU Capable field equal to 0). When in a DMG BSS, the A-MSDU Present bit 7 and A-MSDU Type bit 8 are used in the construction of the AAD, and the remaining QC fields are masked to 0 for the AAD calculation (bits 4 to 6, bits 9 to 15).

* + - * 1. **Construct CCM nonce**

***TGbe editor: Change the sixth paragraph as follows:***

If dot11MultiLinkActivated is true, either To DS or From DS subfields in the MAC header of the MPDU are set to 1, and the MPDU is an individually addressed frame, then the STA Or MLD MAC Address Identified By A2 subfield shall contain the MLD MAC address of the transmitting MLD. Otherwise, the~~The~~ STA Or MLD MAC Address Identified By A2 subfield shall contain the Address 2 field from the MAC header for PV0 MPDUs and the MAC address identified by the A2 field in the MAC header for PV1 MPDUs (see 9.8.3.2 (Address fields)).

* + - 1. **CCMP decapsulation**
         1. **General**

***TGbe editor: Change item a) 1) in the first paragraph as follows:***

For secure PV0 MPDUs, CCMP decrypts the Frame Body field of a cipher text MPDU and decapsulates a plaintext MPDU using the following steps:

The encrypted MPDU is parsed to construct the AAD (see [12.5.3.3.3 (Construct AAD)](#bookmark4)) and nonce (see [12.5.3.3.4 (Construct CCM nonce)](#bookmark5)) values. In addition, if dot11MultiLinkActivated is true, either or both of To DS or From DS subfields in the MAC header of the MPDU is set to 1, and the MPDU is an individually addressed frame transmitted by a STA affiliated with an MLD, then the transmitter and receiver MLD MAC addresses are passed to construct the AAD (see [12.5.3.3.3 (Construct AAD)](#bookmark4)) and nonce (see [12.5.3.3.4 (Construct CCM nonce)](#bookmark5)) values.

**12.5.5.3.4 Construct GCM nonce**

***TGbe editor: Change the second paragraph as follows:***

If dot11MultiLinkActivated is true, either To DS or From DS subfields in the MAC header of the MPDU are set to 1, and the MPDU is an individually addressed frame, then the A2 subfield shall contain the MLD MAC address of the transmitting MLD. Otherwise, the~~The~~ A2 subfield shall contain the Address 2 field from the MAC header.

* + - 1. **GCMP decapsulation**
         1. **General**

***TGbe editor: Change item a) of the second paragraph as follows:***

GCMP decrypts the Frame Body field of a cipher text MPDU and decapsulates a plaintext MPDU using the following steps:

1. The encrypted MPDU is parsed to construct the AAD (see 12.5.5.3.3 (Construct AAD)) and nonce (see [12.5.5.3.4 (Construct GCM nonce)](#bookmark10)) values. In addition, if dot11MultiLinkActivated is true, either or both To DS or From DS subfields in the MAC header of the MPDU is set to 1, and the MPDU is an individually addressed frame transmitted by a STA affiliated with an MLD, then the transmitter and receiver MLD MAC addresses are passed to construct the AAD (see 12.5.5.3.3 (Construct AAD)) and nonce (see [12.5.5.3.4 (Construct GCM nonce)](#bookmark10)) values.