IEEE P802.11
Wireless LANs

|  |
| --- |
| Proposed Draft Text for Multi-Link Security for Individual Management Frame |
| Date: 2021-04-01 |
| 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 document contains draft text for Multi-Link Security for individual Management frame.

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Modified some typos

**Introduction**

***Editing instructions formatted like this are intended to be copied into the TGbe Draft 0.4 (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.***

**Discussion:**

***AAD construction for individual Management frame***

Previously, we have agreed that the PTKSA is established between the AP MLD Authenticator and the non-AP MLD Supplicant using MLD MAC address to construct the AAD for the the unicast data frame [1] as part of cryptographic encapsulation. But how cryptographic encapsulation of unicast Management frame is still not decided.

We propose to use the same processes for the unicast Management frame encapsulation as is used for data frames (use the PTK and MLD MAC addresses in the AAD) when considering the following facts:

* The PTK is derived based on the AP MLD MAC address and the non-AP MLD MAC Address;
* The encapsulation/decapsulation functionality using the PTK is located in the MLO MAC sublayer A [2];

Specifically, we propose replacing A1 and A2 with MLD MAC addresses for the AAD construction. A3 is set to the AP MLD MAC address or the affiliated AP BSSID of the target link respectively for the MLD-level MMPDU and the link-level MMPDU. When the MMPDU is transmitted over-the-air (OTA), A1 and A2 will be replaced by the link addresses of the transmitting link. Note that A3 is not modified when transmitted OTA.

In summary, the AAD construction for the unicast MMPDU is shown as the below table.

NOTE – This proposed solution requires that the AP MLD MAC address is different from the MAC address of any affiliated AP.

|  |  |  |
| --- | --- | --- |
| MMPDU | Direction | AAD Construction |
| A1 | A2 | A3 |
| MLD-level MMPDU | To DS=0From DS=1 | Non-AP MLD MAC Address | AP MLD MAC Address | AP MLD MAC Address |
| To DS=1From DS=0 | AP MLD MAC Address | Non-AP MLD MAC Address | AP MLD MAC Address |
| Link-level MMPDU | To DS=0From DS=1 | Non-AP MLD MAC Address | AP MLD MAC Address | Affiliated AP BSSID of target link |
| To DS=1From DS=0 | AP MLD MAC Address | Non-AP MLD MAC Address | Affiliated AP BSSID of target link |

The proposed solution has the following benefits:

* The unicast Management frame is allowed to be transmitted through any link just like the Data frame, irrespective of the link-level Management frame or the MLD-level Management frame;
* When retransmitted through another link, the AAD will not change and thus no need to re-encrypt it;
* Fully decouple the encryption with selecting the transmitting link
* Fully exploit the advantage of multiple links for transmission

***TGbe editor: Modify subclause 9.3.3.1 as follows:***

**9.3.3 (PV0) Management frames(#4614)(#2569)**

**9.3.3.1 Format of (PV0) Management frames(#4614)**

For a STA, the address fields for all Management frames except Multihop Action frames are as follows:

1. The Address 1 field of the Management frame is the RA (=DA) and is (#4678) the destination of the frame.
2. The Address 2 field of the Management frame is the TA (=SA) and is (#4678) the address of the STA transmitting the frame(#2013).
3. If the STA is an AP with dot11MultiBSSDImplemented set to false, then this address is the BSSID.
4. If the STA is an AP with dot11MultiBSSIDImplemented set to true and the Address 1 field is not set to the broadcast address, then this address is the BSSID of the AP’s BSS (which is either the transmitted BSSID or a nontransmitted BSSID).
5. If the STA is an AP with dot11MultiBSSIDImplemented set to true and the Address 1 field is set to the broadcast address, then this address is the transmitted BSSID.
6. The Address 3 field of the Management frame is set and determined as follows:
7. In Probe Request frames, the Address 3 field can be the wildcard BSSID as defined in the procedures specified in 11.1.4 (Acquiring synchronization, scanning). If Address 3 is not the wildcard BSSID, then it is (for a nonmesh STA) the BSSID of the BSS of the intended recipient(s), or (for a mesh STA) the MAC address of the intended recipient.(#4560)

NOTE 2—Per 11.1.4.3.4 (Criteria for sending a response (11ai)), a mesh STA does not examine the Address 3 field in Probe Request frames it receives. Using an individual address, however, might prevent unwanted responses from other STAs.(#4560)

1. In Public Action frames, the Address 3 field is the BSSID. The BSSID value is set according to 11.17 (Public Action frame addressing).
2. If dot11OCBActivated is true, the Address 3 field is the wildcard BSSID.
3. Otherwise(#2013):
	1. If the STA is an AP or PCP (#4560), the Address 3 field is the same as the Address 2 field.
	2. If the STA is transmitting the Management frame to an AP that is not in a multiple BSSID set or to a PCP, the Address 3 field is the BSSID, irrespective of whether the STA is associated with that AP or PCP.(#4560)
	3. If the STA is transmitting the Management frame to an AP that is in a multiple BSSID set, the Address 3 field is the BSSID of the AP’s BSS (which is either the transmitted BSSID or a nontransmitted BSSID), irrespective of whether the STA is associated with that AP.
	4. If the STA is transmitting the Management frame to one or more IBSS STAs (#2488), the Address 3 field is (#4178)the BSSID.
	5. If the STA is a mesh STA, the Address 3 field is the TA.
	6. If the STA is a TDLS STA transmitting the Management frame to a TDLS peer STA, and the AP to which they are associated is not in a multiple BSSID set, the Address 3 field is the BSSID.(#4560)
	7. If the STA is a TDLS STA transmitting the Management frame to a TDLS peer STA, and the AP to which they are associated is in a multiple BSSID set, the Address 3 field is the BSSID of the AP’s BSS (which is either the transmitted BSSID or a nontransmitted BSSID).(#4560)

For an MLD, the address fields for all Management frames except Multihop Action frames are as follows:

1. The Address 1 field of the Management frame is the RA and is the address of the affiliated STA receiving the frame.
2. The Address 2 field of the Management frame is the TA and is the address of the affiliated STA transmitting the frame.
3. The Address 3 field of the Management frame is set and determined as follows:
4. In Probe Request frames, the Address 3 field can be the wildcard BSSID as defined in the procedures specified in 11.1.4 (Acquiring synchronization, scanning). If Address 3 is not the wildcard BSSID, then it is (for a nonmesh MLD) the MLD MAC address of the AP MLD which the intended recipient of probe request, or (for a mesh MLD) the MLD MAC address of the intended receiving MLD.
5. If dot11OCBActivated is true, the Address 3 field is the wildcard BSSID.
6. Otherwise:
	1. If the transmitting STA is an affiliated STA or an AP and the Management frame is link level, then the Address 3 field is set to the BSSID of the intended link. If the transmitting STA is an affiliated STA or an AP and the Management frame is MLD level, then the Address 3 field is set to the AP MLD MAC address.

***TGbe editor: Modify subclause 12.5.3.3.1 (General) as follows:***

* CCMP cryptographic encapsulation(#2720)
* General(#2720)

The CCMP cryptographic encapsulation process is depicted in Figure 12-18 (CCMP encapsulation block diagram (#4087)).



**Figure 12-18—CCMP encapsulation block diagram**

* (11ah)For secure PV0 MPDUs, CCMP encrypts the Frame Body field of a plaintext MPDU and encapsulates the resulting cipher text using the following steps:
* Increment the PN, to obtain a fresh PN for each MPDU, so that the PN never repeats for the same temporal key.

(#4613)NOTE—Retransmitted MPDUs are not modified on retransmission.

* Use the fields in the MPDU header to construct the additional authentication data (AAD) for CCM. The CCM algorithm provides integrity protection for the fields included in the AAD. MPDU header fields that may change when retransmitted are muted by being masked to 0 or being set to a known value when calculating the AAD as described in 12.5.3.3.3 (Construct AAD).
* In the 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) from the PN, transmitting MLD MAC Address, and the priority value of the MPDU. Otherwise, construct the CCM nonce block (#4613) as defined in 12.5.3.3.4 (Construct CCM nonce (#2720)) 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 (#4385) 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) (#4613) 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.
* (#4613)Construct the CCMP header as defined in 12.5.3.3.5 (Construct CCMP header for PV0 MPDUs (#2720)).
* Use the temporal key, AAD, nonce, and MPDU data to form the cipher text and (#4088)the encrypted MIC. This step is known as CCM originator processing.
* Form the encrypted MPDU by combining the original MPDU header, the CCMP header, the encrypted data and (#4088) the encrypted MIC, as described in 12.5.3.2 (CCMP MPDU format).

***TGbe editor: Modify subclause 12.5.3.3.3 (Construct AAD) as follows:***

* Construct AAD(#2720)
* (11ah)For PV0 MPDUs, the format of the AAD is shown in Figure 12-19 (AAD construction for PV0 MPDUs (11ah)). The length of the AAD for PV0 varies depending on the presence or absence of the QC and A4 fields and is shown in Table 12-3 (AAD length for PV0 MPDUs(11ah)).

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | FC | A1 | A2 | A3 | SC | A4 | QC |
| Octets: | 2 | 6 | 6 | 6 | 2 | 6 | 2 |
| * AAD construction for PV0 MPDUs(11ah)
 |

|  |
| --- |
| * AAD length for PV0 MPDUs(11ah)
 |
| QC field | A4 field | AAD length(octets) |
| Absent | Absent | 22 |
| Present | Absent | 24 |
| Absent | Present | 28 |
| Present | Present | 30 |

The AAD is constructed from the MPDU header. (#2352)The AAD includes neither the Duration/ID field nor the HT Control field because the contents of these fields might change during normal operation (e.g., due to a rate change preceding retransmission). The HT Control field might also be inserted or removed during normal operation (e.g., retransmission of an (#4130) A-MPDU where the original (#4130)A-MPDU included an MRQ that has already generated a response). For similar reasons, several subfields in the Frame Control field are masked to 0. (11ah)For PV0 MPDUs, (#4261) AAD construction is performed as follows:

* (11ah)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
* +HTC(#66) subfield (bit 15) as follows:
* Masked to 0 in all Data frames containing a QoS Control field
* Unmasked otherwise
* Other subfields are not modified(#4417)
* (11ah) If dot11MultiLinkActivated is true, for both the transmitter and intended receiver of the MPDU, either of the To DS or the From DS subfields in the MAC header of the MPDU is set to 1, and the MPDU is an individually addressed frame, then A1 is set to:
* the MLD MAC Address of the intended receiver MLD of the MPDU.

– otherwise, A1 is set to the MPDU Address 1 field.

* (11ah) If dot11MultiLinkActivated is true, for both the transmitter and intended receiver of the MPDU, either of the To DS or the From DS subfields in the MAC header of the MPDU is set to 1, and the MPDU is an individually addressed frame, 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.

* (11ah) If dot11MultiLinkActivated is true, the MPDU Address 3 field is set to the BSSID, and the MPDU is an individually addressed Data frame, then:
* if the To DS subfield is set to 0 and the From DS subfield is set to 1 in the MAC header of the MPDU, set A3 to the MLD MAC Address of the transmitting MLD,
* else if the To DS subfield is set to 1 in the MAC header of the MPDU, set A3 to the MLD MAC Address of the receiving MLD, ,
* else set A3 to the MPDU Address 3 field.

If dot11MultiLinkActivated is true, and the MPDU is an individually addressed Management frame, then set A3 to the MPDU Address 3 field.

–

* (11ah)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.
* (11ah)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 Data frame, then A4 is set to the MLD MAC Address of the transmitting MLD.

– otherwise A4, if present is set to the MPDU Address 4 field.

* (11ah)QC – QoS Control field contains (M158) 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).

***TGbe editor: Modify subclause 12.5.3.3.4 (Construct CCM nonce) as follows:***

* Construct CCM nonce(#2720)

The Nonce field occupies 13 octets, and its structure is shown in Figure 12-21 (Nonce field (#1406)(11ah)). The structure of the Nonce Flags subfield of the Nonce field is shown in Figure 12-22 (Nonce Flags subfield (11ah)).

|  |  |  |  |
| --- | --- | --- | --- |
|  | Nonce Flags | STA or MLD MAC Address Identified By A2 | PN |
| Octets: | 1 | 6 | 6 |
| * Nonce field(#1406)(11ah)
 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | B0         B3 | B4 | B5 | B6         B7 |
|  | Priority | Management | PV1 | Zeros |
| Bits: | 4 | 1 | 1 | 2 |
| * Nonce Flags subfield(11ah)
 |

(#4614)The Priority subfield shall be set to the priority value of the MPDU.

(#4614)The Management subfield shall be set to 1 if the MPDU is a Management frame and management frame protection is negotiated; otherwise, it shall be set to 0.

(#4614)The PV1 subfield shall be set to 1 for a PV1 frame; otherwise, it shall be set to 0.

(#4614)The Zeros subfield shall be set to 0.

(#4614) If dot11MultiLinkActivated is true, either the To DS or the 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 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)).

(#4614)The PN subfield shall contain the packet number, with PN0 in the last octet of the subfield.

***TGbe editor: Modify subclause 12.5.3.4.1 (General) as follows:***

* CCMP decapsulation(#2720)
* General(#2720)

Figure 12-23 (CCMP decapsulation block diagram (#4087)) depicts the CCMP decapsulation process.



**Figure 12-23—CCMP decapsulation block diagram (#4087)**

* (11ah)For secure PV0 MPDUs, CCMP decrypts the Frame Body field of a cipher text MPDU and decapsulates a plaintext MPDU using the following steps:
* (#4614)(11ah)The encrypted MPDU is parsed to construct the AAD (see 12.5.3.3.3 (Construct AAD (#2720))) and nonce (see 12.5.3.3.4 (Construct CCM nonce (#2720))) values. In addition, if dot11MultiLinkActivated is true, either or both of the To DS or the 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)) and nonce (see 12.5.3.3.4 (Construct CCM nonce)) values.
* (11ah)The (#4088) MIC is extracted for use in (#4386) CCM integrity checking.

***TGbe editor: Modify subclause 12.5.5.3.1 (General) as follows:***

* GCMP cryptographic encapsulation
* General

The GCMP cryptographic encapsulation process is depicted in Figure 12-27 (GCMP encapsulation block diagram (#4087)).



**Figure 12-27—GCMP encapsulation block diagram**

GCMP encrypts the Frame Body field of a plaintext MPDU and encapsulates the resulting cipher text using the following steps:

* Increment the PN, to obtain a fresh PN for each MPDU, so that the PN never repeats for the same temporal key.

NOTE—Retransmitted MPDUs are not modified on retransmission.

* Use the fields in the MPDU header to construct the additional authentication data (AAD) for GCM. The GCM algorithm provides integrity protection for the fields included in the AAD. MPDU header fields that may change when retransmitted are muted by being (#4613) masked to 0 or being set to a known value when calculating the AAD as described in 12.5.5.3.3 (Construct AAD).
* Construct the GCM nonce (#1406) block (#4613)as defined in 12.5.3.3.4 (Construct CCM nonce(#2720)).
* Construct the GCMP header as defined in 12.5.5.3.5 (Construct GCMP header).(#4613)
* Use the temporal key, AAD, nonce, and MPDU data to form the cipher text and (#4088) the MIC. This step is known as GCM originator processing.
* Form the encrypted MPDU by combining the original MPDU header, the GCMP header, the encrypted data and (#4088) the MIC, as described in 12.5.5.2 (GCMP MPDU format).

***TGbe editor: Modify subclause 12.5.5.3.4 (Construct GCM nonce) as follows:***

* Construct GCM nonce

The Nonce field occupies 12 octets, and its structure is shown in Figure 12-28 (Nonce field(#1406)).

|  |  |  |
| --- | --- | --- |
|  | A2 | PN |
| Octets: | 6 | 6 |
| * Nonce field(#1406)
 |

(#4614) If dot11MultiLinkActivated is true, either the To DS or the From DS subfields in the MAC header of the MPDU is 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 A2 subfield shall contain the Address 2 field from the MAC header.

(#4614)The PN subfield shall contain the packet number, with PN0 in the last octet of the subfield.

***TGbe editor: Modify subclause 12.5.5.4.1 (General) as follows:***

* GCMP decapsulation
* General

Figure 12-29 (GCMP decapsulation block diagram(#4087)) shows the GCMP decapsulation process.



**Figure 12-29—GCMP decapsulation block diagram (#4087)**

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

* (#4614)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)) values. In addition, if dot11MultiLinkActivated is true, either or both of the To DS or the 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)) values.
* The MIC is extracted for use in (#4386)GCM integrity checking.

***TGbe editor: Modify subclause 35.3.3 as follows:***

**35.3.3 Multi-link device addressing**

An MLD has an MLD MAC address that singly identifies the MLD.

(#1156)The MAC address of each AP affiliated with an AP MLD shall be different from each other. The AP MLD MAC address is different from the MAC address of any affiliated AP.

**Straw Poll: Do you support to incorporate the proposed draft text in this document 11-21/0571r1, to the latest TGbe Draft?**

**Result: Yes/No/Abstain**

**References**

[1]11-21-0233-03-00be-pdt-mld-security-considerations.docx

[2]11-21-0316-00-0arc-mlo-architecture-reference-model.pptx