IEEE P802.11
Wireless LANs

|  |
| --- |
| TBD resolution for secure non-TB and TB ranging |
| Date: 2019-1-15 |
| Author(s): |
| Name | Company | Address | Phone | Email |
| Girish Madpuwar | Broadcom | Electronic City, Bangalore India |  | Girish.madpuwar@broadcom.com  |
| Nehru Bhandaru | Broadcom |  |  |  |
| Yongho Seok  | MediaTek |  |  |  |

**Abstract**

This submission proposes resolutions of TBD on draft 0.6.

* CIDs: none

**11.22.6.4.6 Secure Non-TB and -TB Ranging Measurement Exchange Protocol**

***TGaz Editor: Change subclause 11.22.6.4.6.1 as the followings:***

**11.22.6.4.6.1 Secure Non-TB ranging mode**

An ISTA that sends a Ranging NDP Announcement frame to a RSTA shall set:

— The SAC subfield in the STA Info SAC field in the Ranging NDP Announcement frame to the same value as in the LTF Generation SAC field in the Secure LTF Parameters field in the last received Fine Timing Measurement frame or last received Location Measurement Report frame from the RSTA, if the ISTA has not sent any Ranging NDP Announcement frame after the last received Fine Timing Measurement frame or last received Location Measurement Report frame from the RSTA;

— Otherwise the SAC subfield in the STA Info SAC field in the Ranging NDP Announcement frame to 0 to indicate that a new LTF Sequence Generation information is needed.

An ISTA that sends a Ranging NDP PPDU a SIFS after transmission of the Ranging NDP Announcement frame to a RSTA shall set the TXVECTOR parameter LTF\_SEQUENCE as follows:

— HE\_LTF, if the SAC subfield in the STA Info SAC field in the Ranging NDP Announcement is set to 0;

— Otherwise the LTF sequence generation information in the Secure LTF Parameters field in the last received Fine Timing Measurement frame or last received Location Measurement Report frame from the RSTA.

After transmission of the Ranging NDP Announcement frame to the RSTA, the ISTA’s MAC sublayer shall issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR parameter that as follows:

— HE\_LTF, if the SAC subfield in the STA Info SAC field in the Ranging NDP Announcement is set to 0;

— Otherwise the LTF sequence generation information in the Secure LTF Parameters field in the last received Fine Timing Measurement frame or last received Location Measurement Report frame from the RSTA.

When a RSTA receives a Ranging NDP Announcement from an ISTA frame in which the SAC subfield in the STA Info SAC field is set to 0, the RSTA shall:

* Issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR parameter that is set to HE\_LTF;
* Send an HE Ranging NDP PPDU with the TXVECTOR parameter LTF\_SEQUENCE set to HE\_LTF to the ISTA, if the RSTA receives an HE Ranging NDP PPDU from the ISTA a SIFS after the ranging NDP Announcement frame;
* Send a Location Measurement Report frame that includes the Secure LTF Parameters field to the ISTA, if the RSTA receives an HE Ranging NDP PPDU from the ISTA a SIFS after the ranging NDP Announcement frame.

…

When a RSTA receives a Ranging NDP Announcement frame from an ISTA in which a value of the SAC subfield in the STA Info SAC field is neither equal to 0 nor the value of the LTF Generation SAC subfield in the Secure LTF Parameters field in the last transmitted Fine Timing Measurement frame or last transmitted Location Measurement Report frame to the ISTA, the RSTA shall:

* Not issue a PHY-RXLTFSEQUENCE.request primitive;
* Not send an HE Ranging NDP PPDU to the ISTA;

Not send a Location Measurement Report frame to the ISTA.

When a Location Measurement Report frame contains range measurement results measured from an UL NDP and a DL NDP, an RSTA shall include the Secure LTF Parameters field in the Location Measurement Report frame and set the Range Measurement SAC subfield in the Secure LTF Parameters field in the Location Measurement Report frame to the same value as in the SAC subfield in the STA Info SAC field in the Ranging NDP Announcement frame that solicited the UL NDP and the DL NDP.

When a STA sending an HE Ranging NDP PPDU sets the TXVECTOR parameter LTF\_SEQUENCE to HE\_LTF, the STA shall not use the ToD value of HE Ranging NDP PPDU for the secure range measurement.

When a STA receiving an HE Ranging NDP PPDU sets the LTFVECTOR parameter in the PHY-RXLTFSEQUENCE.request primitive to HE\_LTF, the STA shall not use the ToA value of the HE Ranging NDP PPDU and set the Invalid Measurement Indication subfield to 1 in the ToA Error field in the Location Measurement Report carrying the ToA value of the HE Ranging NDP PPDU.

***TGaz Editor: Repalce Figure 11-yy (Error recovery of secure measurement exchange in Non-TB mode) with the following:***



**Figure 11-yy—Error recovery of secure measurement exchange in non-TB mode**

***TGaz Editor: Change subclause 11.22.6.4.6.2 as the followings:***

11.22.6.4.6.2 Secure TB ranging mode

A RSTA that sends a Ranging Secure Sounding Trigger frame to an ISTA shall set:

— The SAC subfield in the Trigger Dependent User Info field in the STA Info field corresponding to AID/RID of the ISTA in the Ranging Secure Sounding Trigger frame to the same value as in the LTF Generation SAC field in the Secure LTF Parameters field in the last transmitted Fine Timing Measurement frame or last transmitted Location Measurement Report frame to the ISTA, if the RSTA has not sent any Ranging Secure Sounding Trigger frame to the ISTA after the last transmitted Fine Timing Measurement frame or last transmitted Location Measurement Report frame to the ISTA;

— Otherwise the SAC subfield in the Trigger Dependent User Info field in the STA Info field corresponding to AID/RID of the ISTA in the Ranging Secure Sounding Trigger frame to 0 to indicate that a new LTF Sequence Generation information is needed.

…

After transmission of the Ranging Secure Sounding Trigger frame to the ISTA, the RSTA’s MAC sublayer shall issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR parameter LTF\_SEQUENCE that is set to as follows:

— HE\_LTF, if the SAC subfield in the Trigger Dependent User Info field in the Ranging Secure Sounding Trigger frame to 0.

— Otherwise the LTF sequence generation information in the Secure LTF Parameters field in the the last transmitted Fine Timing Measurement frame or last transmitted Location Measurement Report frame to the ISTA.

When the RSTA receives the HE TB Ranging NDP PPDU from the ISTA, the RSTA shall:

1. Send a Ranging NDP Announcement frame.
2. Send an HE Ranging NDP PPDU with the TXVECTOR parameter LTF\_SEQUENCE set to as follows:

— HE\_LTF, if the SAC subfield in the Trigger Dependent User Info field in the Ranging Secure Sounding Trigger frame to 0.

— Otherwise the LTF sequence generation information in the Secure LTF Parameters field in the the last transmitted Fine Timing Measurement frame or last transmitted Location Measurement Report frame to the ISTA.

1. Send a Location Measurement Report frame that includes the Secure LTF Parameters field to the ISTA.

Otherwise, the RSTA shall follow the rules in 10.22.2.2 (EDCA backoff procedure) as the frame exchange is not successful.

…

When an ISTA receives a Ranging Secure Sounding Trigger frame from a RSTA in which the value of the SAC subfield in the Trigger Dependent User Info field is not equal to the value of the LTF Generation SAC subfield in the Secure LTF Parameters field in the last received Fine Timing Measurement frame or last received Location Measurement Report frame from the RSTA, the ISTA shall:

1. Send an HE TB Ranging NDP PPDU with the TXVECTOR parameter LTF\_SEQUENCE set to either HE\_LTF or the LTF sequence generation information in the Secure LTF Parameters field in the last received Fine Timing Measurement frame or last received Location Measurement Report frame from the RSTA;
2. Issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR parameter LTF\_SEQUENCE that is set to either HE\_LTF or the LTF sequence generation information in the Secure LTF Parameters field in the the last received Fine Timing Measurement frame or last received Location Measurement Report frame from the RSTA;

…

When an RSTA sending an HE Ranging NDP PPDU sets the TXVECTOR parameter LTF\_SEQUENCE to HE\_LTF, the RSTA shall not use the ToD value of HE Ranging NDP PPDU for the range measurement.

When a RSTA receiving an HE TB Ranging NDP PPDU sets the LTFVECTOR parameter in the PHY-RXLTFSEQUENCE.request primitive to HE\_LTF, the RSTA shall not use the ToA value of the HE Ranging NDP PPDU and set the Invaild Measurement Indication subfield to 1 in the ToA Error field in the Location Measurement Report carrying the ToA value of the HE TB Ranging NDP PPDU.

When an ISTA sending an HE TB Ranging NDP PPDU sets the TXVECTOR parameter LTF\_SEQUENCE to HE\_LTF, the ISTA shall not use the ToD value of HE TB Ranging NDP PPDU for the range measurement. ***TGaz Editor: Repalce Figure 11-yy (Error recovery of secure measurement exchange in TB mode) with the following:***



Figure 11-yy— Error recovery of secure measurement exchange in TB mode

***TGaz Editor: Change subclause 9.4.2.280 (Secure LTF Parameters) as the followings:***

The specific LTF Sequence Generation Information field format is 9-610d (LTF Sequence Generation Information field format) (The keys or cipher sequence (if needed) for LTF Sequence Generation are the result of the FTM negotiation). This field is present in the Location Measurement Report frame transmitted from an RSTA to an ISTA and is reserved otherwise.

The LTF Generation SAC field is used to authenticate that the randomized LTF sequence is generated from a reliable LTF Sequence Generation Information. The LTF Generation SAC field is a nonzero value associated with LTF Sequence Generation Information carried in the same Secure LTF Parameters element (see 11.22.6.3.2 (Secure LTF measurement setup)). This field is present in the Location Measurement Report frame transmitted from an RSTA to an ISTA and is reserved otherwise.

The Range Measurement SAC field is used to verify that range measurement results of the Location Measurement Report frame are calculated using the same LTF sequence between ISTA and RSTA. The Range Measurement SAC field is the same value as in the LTF Generation SAC subfield in the STA Info SAC field in the Ranging NDP Announcement frame that solicited the UL NDP and the DL NDP (see 11.22.6.4.6 (Secure Non-TB and -TB Ranging Measurement Exchange Protocol)).This field is reserved in the initial Fine Timing Measurement frame

***TGaz Editor: Change <TBD> to 13 in Figure 9-xxx (Fine Timing Measurement Report Action field format), Page 56 line 21.***

***TGaz Editor: Change subclause 11.3.3 as the followings:***

b) Class 2 frames

1) Management frames

i) Association Request/Response

ii) Reassociation Request/Response

iii) Disassociation

iv) Unicast Protected Dual of Public Action frames (9.6.10) when PTKSA from PASN authentication exists

***TGaz Editor: Change subclause 11.22.6.3.2 as the followings:***

**11.22.6.3.2 Secure LTF measurement setup**

For a given secure measurement frame (e.g. NDP), the SAC and secret (pseudo-random) bits to protect all of the LTFs in the frame originating from the RSTA are derived as follows

SAC || Secure-LTF-RSTA-bits = KDF-Hash-Length(Secure-LTF-Key-Seed, “Secure LTF Expansion”, Secure-LTF-Counter)When the derived SAC is equal to 0, the STA shall increment the Secure-LTF-Counter by 1 and derive the SAC until a nonzero SAC value is obtained.

Similarly, for a given secure measurement frame (e.g. NDP), the secret (pseudo-random) bits to protect all of the LTFs in the frame originating from the ISTA for a given SAC are derived as follows

Secure-LTF-ISTA-bits = KDF-Hash-Length(Secure-LTF-Key-Seed, “Secure LTF Expansion”, SAC || Secure-LTF-Counter)

***TGaz Editor: modify following in section 9.3.1.19 as the followings in D0.6 page 20 line 25 :***

9.3.1.19 VHT/HE/Ranging NDP Announcement frame format

The STA Info SAC field is used in the secure variant of the non-TB Ranging measurement exchange protocol to carry the seqeunce authentication code (SAC), see Figure 9-51f. It is included in the Ranging NDP Announcement frame after the other STA Info field(s), see Figure 9-51d.

***TGaz Editor: modify following in section 12.13 as the followings in D0.6 page 109 line 16:***

12.13 Pre Association Security Negotiation

12.13.1 General

A cryptographic RNG is available to generate ECC private keys