IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Reorganization of Secure LTF Measurement Exchange | | | | |
| Date: 2020-08-06 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Christian Berger | NXP | 350 Holger Way, San Jose, CA |  | [Christian.berger@nxp.com](mailto:Christian.berger@nxp.com) |
| Roy Want | Google |  |  | [roywant@google.com](mailto:roywant@google.com) |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This submission proposes to reorganize the clauses addressing measurement exchange using Secure LTF

Revisions:

1. Started drafting the spec text

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGax Draft. This introduction is not part of the adopted material.

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

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

**The text preceded by “Discussion” is not part of the adopted changes.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **P.L** | **Clause** | **Comment** | **Proposed Change** | **Resolution** |
| **3266** | 153.26 | 11.22.6.4.6 | This subclause is very long and hard to read; I would suggest re-organizing it. | The space here is not sufficient to give a detailed description of a comment resolution, but I would make the following points: i) start with a general section describing the differences to the non-secure case. ii) Then have the description of Figure 11-36n to describe the regular case, iii) then explain the NPD-A and NDP transmission parameters, iv) last have the error recovery. Also consider moving both non-TB and TB description of NDP transmission ot a separate (joined) subclause similar to non-secure case. Finally to align with non-secure case, consider re-organizing to put TB mode first. | **Revised** |

TGaz Editor: Swap the order of clause 11.22.6.4.5 and 11.22.6.4.6:

11.22.6.4.5 Transmission of a ranging NDP

TGaz Editor: Rename clause 11.22.6.4.6 as follows:

11.22.6.4.6 Use of Secure LTF in the TB and Non-TB Ranging Measurement Exchange Protocol

TGaz Editor: Add the following subclause at the start of 11.22.6.4.6:

11.22.6.4.6.1 General

Both the TB and the Non-TB Ranging measurement exchanges allow for the use of Secure LTF for PHY security, if the ISTA and RSTA have established a secure LTF measurement setup as defined in 11.22.6.3.4 (Negotiation for secure LTF in the TB and Non-TB measurement exchange). The frame exchange sequences stay nominally the same as described in 11.22.6.4.3 (TB Ranging measurement exchange) and 11.22.6.4.4 (Non-TB Ranging measurement exchange), except that the HE Ranging NDP and HE TB Ranging NDP will use Secure LTF as described in 27.3.18a (HE Ranging NDP) and 27.3.18b (HE TB Ranging NDP) respectively. To use the Secure LTF the ISTA and RSTA need to share and communicate pseudo random bit sequences that are used to generate and demodulate the Secure LTF, the details and management thereof is described in the following.

TGaz Editor: Move Figure 11-36p to the beginning of subclause 11.22.6.4.6.2 and rename:



1. Figure 11-36p—Example of TB Ranging measurement exchange with Secure LTF

TGaz Editor: Switch the order of Non-TB and TB ranging modes:

11.22.6.4.6.2 TB Ranging Measurement Exchange with Secure LTF

One example of the negotiation and two TB Ranging Measurement Exchanges with Secure LTF is shown in Figure 11-36p (Example of TB Ranging measurement exchange with Secure LTF), where the LTF\_GEN\_SAC and LTF\_GEN\_INFO refer to the LTF Generation SAC and Secure LTF Counter. The first LTF Generation SAC and its associated Secure LTF Counter (#2289) parameters are carried in an initial Fine Timing Measurement frame, and a Location Measurement Report frame. The LTF Generation SAC is also included in the Ranging Trigger frame Secure Sounding. (#1129) The description of how these fields are set in the TB Ranging Measurement exchange is given next.

When an RSTA has established a secure LTF measurement setup with an ISTA as specified in 11.22.6.3.4 (Negotiation for secure LTF in the TB and Non-TB measurement exchange), the RSTA that sends a Ranging Secure Sounding Trigger frame to the STA shall set: (#**1260**)

* The SAC subfield in the Trigger Dependent User Info field (#**1129**) corresponding to 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 since 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 the ISTA in the Ranging Secure Sounding Trigger frame to 0 to indicate that a new Secure LTF Counter (#**2289**) is needed.

The RSTA shall set the I2R Rep subfield of the STA Info field corresponding to the ISTA in the Ranging Secure Sounding Trigger frame equal to the *RSTA Assigned I2R Rep* corresponding to the ISTA.

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 as follows:

— Either the Secure-LTF-bits-I2R for generating any secure HE-LTF or null (#**1828**, #**1831**), if the SAC subfield in the Trigger Dependent User Info field in the Ranging Secure Sounding Trigger frame 0.

— Otherwise the Secure-LTF-bits-I2R (see 11.22.6.4.6.3 (Secure LTF Generation Information)) based on (#**1830**, #**1832**)Secure LTF Counter (#2289) in the Secure LTF Parameters field in 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 from the ISTA, the RSTA shall:

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

— Either the Secure-LTF-bits-R2I for generating any secure HE-LTF or null (#**1828**, #**1831**), if the SAC subfield in the Trigger Dependent User Info field in the Ranging Secure Sounding Trigger frame 0.

— Otherwise the Secure-LTF-bits-R2I (see 11.22.6.4.6.3 (Secure LTF Generation Information)) based on (#**1830**, #**1832**) Secure LTF Counter (#**2289**) in the Secure LTF Parameters field in 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.

The RSTA that sends the Ranging NDP Announcement frame shall set the Offset subfield in the STA Info field corresponding to the ISTA in the Ranging NDP Announcement frame to values meeting the Equation (11-aa):

(11-aa)



where

*Offsetn* represents the Offset subfield value of *nth* STA Info field in the Ranging NDP Announcement frame.

*N\_LTFn* represents the number of HE-LTF symbols required for the R2I N\_STS subfield value plus 1 space-time streams of *nth* STA Info field in the Ranging NDP Announcement frame.

*Repn* represents the R2I Rep subfield value plus 1 of *nth* STA Info field in the Ranging NDP Announcement frame.

*MinOffset* represents the set of indexes of the STA Info fields of which the Offset subfield values are less than the Offset subfield value of *ith* STA Info field in the Ranging NDP Announcement frame.

*MaxOffset* represents the set of indexes of all STA Info fields excluding *ith* STA Info field.

The RSTA shall set the R2I Rep subfield of the STA Info field corresponding to the ISTA in the Ranging NDP Announcement frame equal to the *RSTA Assigned R2I Rep*corresponding to the ISTA.

When an ISTA receives a Ranging Secure Sounding Trigger frame from an RSTA in which the value of the SAC subfield in the Trigger Dependent User Info field is equal to the value of the LTF Generation SAC subfield in the Secure LTF Parameters field in the last Fine Timing Measurement frame received or last Location Measurement Report frame received from the RSTA, the ISTA shall:

* Send an HE TB Ranging NDP with the TXVECTOR parameter LTF\_SEQUENCE set to the Secure-LTF-bits-I2R; see 11.22.6.4.6.3 (Secure LTF Generation Information)) based on (#**1830**, #**1832**) the Secure LTF Counter (#**2289**) in the Secure LTF Parameters field in the last Fine Timing Measurement frame received, or last Location Measurement Report frame received from the RSTA;
* Issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR parameter LTF\_SEQUENCE that is set to the Secure-LTF-bits-R2I; see 11.22.6.4.6.3 (Secure LTF Generation Information)) based on (#**1830**, #**1832)** the Secure LTF Counter (#**2289**)in the Secure LTF Parameters field in the last Fine Timing Measurement frame received, or last Location Measurement Report frame received from the RSTA;

When an ISTA receives a Ranging Secure Sounding Trigger frame from an 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 Fine Timing Measurement frame received or last Location Measurement Report frame received from the RSTA, the ISTA shall:

1. Send an HE TB Ranging NDP with the TXVECTOR parameter LTF\_SEQUENCE set to (#**2289**) either the Secure-LTF-bits-I2R for generating any secure HE-LTF or null (#**1828**, #**1831**);
2. Issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR parameter LTF\_SEQUENCE that is set to (#**2289**) either the Secure-LTF-bits-R2I for generating any secure HE-LTF or null (#**1828**, #**1831**);

When an ISTA receives a Ranging NDP Announcement frame from an RSTA in which the AID11/RSID11 subfield in one of the STA Info fields contains the 11 least significant bits of the AID or RSID of the ISTA, the ISTA shall:

1. Issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR parameter LTF\_OFFSET that is set to the Offset subfield value in the STA Info field;
2. Issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR parameter LTF\_N\_STS that is set to the R2I N\_STS subfield value in the STA Info field;
3. Issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR parameter LTF\_REP that is set to the R2I Rep subfield value in the STA Info field;

When a Location Measurement Report frame contains range measurement results measured from an I2R NDP and a R2I NDP, an RSTA or ISTA that transmits the RSTA2ISTA or ISTA2RSTA Location Measurement Report frame shall include the Secure LTF Parameters field in the Location Measurement Report frame and 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 Trigger Dependent User Info field in the Ranging Secure Sounding Trigger frame that solicited the I2R NDP and the R2I NDP. The Measurement Result LTF Offset field in the Secure LTF Parameter element in the Location Measurement Report frame shall set to the same value as in the Offset subfield of User Info field in the Ranging NDP Announcement frame that precedes the R2I NDP. When an ISTA or RSTA receives RSTA2ISTA or ISTA2RSTA Location Measurement Report frame, the ISTA or RSTA shall compare the value of Measurement Result LTF Offset field with the value of the Offset subfield in the corresponding User Info field of Ranging NDP Announcement frame, and if these two values don’t match, the ISTA or RSTA shall discard the measurement results carried in the Location Measurement Report frame. (**#1580, #2283, #1163**)

When an RSTA sending an HE Ranging NDP sets the TXVECTOR parameter LTF\_SEQUENCE to either the bit string (e.g., the Secure-LTF-bits-R2I or Secure-LTF-bits-I2R) for generating any secure HE-LTF or null (#**1828**, #**1831**), the RSTA shall not use the TOD value of HE Ranging NDP for the range measurement.

When an RSTA receiving an HE TB Ranging NDP sets the LTFVECTOR parameter in the PHY-RXLTFSEQUENCE.request primitive to either the bit string (e.g., the Secure-LTF-bits-R2I or Secure-LTF-bits-I2R) for generating any secure HE-LTF or null (#**1828**, #**1831**), the RSTA shall not use the TOA value of the HE Ranging NDP 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 TB Ranging NDP.

When an ISTA sending an HE TB Ranging NDP sets the TXVECTOR parameter LTF\_SEQUENCE to either the bit string (e.g., the Secure-LTF-bits-R2I or Secure-LTF-bits-I2R) for generating any secure HE-LTF or null (#**1828**, #**1831**), the ISTA shall not use the TOD value of HE TB Ranging NDP for the range measurement.

When an ISTA receiving an HE Ranging NDP sets the LTFVECTOR parameter in the PHY-RXLTFSEQUENCE.request primitive to either the bit string (e.g., the Secure-LTF-bits-R2I or Secure-LTF-bits-I2R) for generating any secure HE-LTF or null (#**1828**, #**1831**), the ISTA shall not use the TOA value of the HE Ranging NDP, 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 if the Location Measurement Report transmission from the ISTA was negotiated.

When there is a transmission failure within a secure measurement exchange sequence, the recovery procedure of the LTF Generation SAC and its associated Secure LTF Counter (#**2289**) parameters is illustrated in Figure 11-36q (Error recovery of TB Ranging measurement exchange using Secure LTF).



1. Figure 11-36q—Error recovery of TB Ranging measurement exchange using Secure LTF

TGaz Editor: Switch the order of Non-TB and TB ranging modes and rename:

TGaz Editor: Move Figure 11-36n to the beginning of the subclause and rename:



1. Figure 11-36n—Example of Non-TB Ranging measurement exchange with Secure LTF

11.22.6.4.6.3 Non-TB Ranging Measurement Exchange with Secure LTF

An example of the negotiation and two Non-TB Ranging measuerment exchanges are illustrated in Figure 11-36n (Example of Non-TB Ranging measurement exchange with Secure LTF). The LTF Generation SAC and its associated Secure LTF Counter (#2289) parameters (referred to as LTF\_GEN\_SAC and LTF\_GEN\_INFO) are carried in an initial Fine Timing Measurement frame and a Location Measurement Report frame. The LTF Generation SAC is also included in the Ranging NDP Announcement frame. (#1129) The detailed description of how the fields in these frames are set follows.

When an ISTA has established a secure LTF measurement setup with an RSTA as specified in 11.22.6.3.4 (Negotiation for Secure LTF in the TB and Non-TB Ranging measurement exchange), this ISTA shall set the following subfields in any Ranging NDP Announcement frame addressed to that RSTA as follows(#**1260**):

— 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 Fine Timing Measurement frame received or last Location Measurement Report frame received from the RSTA, if the ISTA has not sent any Ranging NDP Announcement frame after the last Fine Timing Measurement frame received or last Location Measurement Report frame received 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 Secure LTF Counter (#**2289**) is needed.

The ISTA shall set the I2R Rep subfield and R2I Rep subfield of the STA Info field in the Ranging NDP Announcement frame to the Max I2R Rep subfield value and the Max R2I Rep subfield value in the Ranging Parameters field in the last Fine Timing Measurement frame received from the RSTA.

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

—Either the Secure-LTF-bits-I2R for generating any secure HE-LTF , or null (#**1828**, #**1831**) if the SAC subfield in the STA Info SAC field in the Ranging NDP Announcement is set to a value of 0;

— Otherwise the Secure-LTF-bits-I2R; see 11.22.6.4.6.3 (Secure LTF Generation Information) based on (#**1830**, #**1832**) the Secure LTF Counter (#**2289**) in the Secure LTF Parameters field in the last Fine Timing Measurement frame received or last Location Measurement Report frame received 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 is set (#**2289**)as follows:

— Either the Secure-LTF-bits-R2I for generating any secure HE-LTF, or null (#**1828**, #**1831**) if the SAC subfield in the STA Info SAC field in the Ranging NDP Announcement is set to 0

—Otherwise the Secure-LTF-bits-R2I (see 11.22.6.4.6.3 (Secure LTF Generation Information)) based on (#**1830**, #**1832**) the Secure LTF Parameters field in the last Fine Timing Measurement frame received or last Location Measurement Report frame received from the RSTA.

When an 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 either the Secure-LTF-bits-R2I for generating any secure HE-LTF or null (**#1828, #1831**)**;**
* Send an HE Ranging NDP with the TXVECTOR parameter LTF\_SEQUENCE set to either the Secure-LTF-bits-R2I for generating any secure HE-LTF or null (#**1828**, #**1831**) to the ISTA, if the RSTA receives an HE Ranging NDP 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 from the ISTA a SIFS after the ranging NDP Announcement frame.

When an RSTA receives a Ranging NDP Announcement frame from an ISTA in which the value of the SAC subfield in the STA Info SAC field is equal to 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:

* Issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR parameter that is set to the Secure-LTF-bits-I2R; see 11.22.6.4.6.3 (Secure LTF Generation Information)) based on (#**1830**, #**1832**) the Secure LTF Counter (#**2289**) in the Secure LTF Parameters field in the last transmitted Fine Timing Measurement frame, or last transmitted Location Measurement Report frame to the ISTA;
* Send an HE Ranging NDP with the TXVECTOR parameter LTF\_SEQUENCE set to the Secure-LTF-bits-R2I; see 11.22.6.4.6.3 (Secure LTF Generation Information)) based on (#**1830,** #**1832**) the Secure LTF Counter (#**2289**) 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 receives an HE Ranging NDP 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 from the ISTA a SIFS after the ranging NDP Announcement frame.

When an 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 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 I2R NDP and a R2I 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 I2R NDP and the R2I NDP.

When a STA sending an HE Ranging NDP sets the TXVECTOR parameter LTF\_SEQUENCE to either a bit string (e.g., the Secure-LTF-bits-R2I or Secure-LTF-bits-I2R) for generating any secure HE-LTF or null (#**1828**, #**1831**)**,** the STA shall not use the TOD value of HE Ranging NDP for the secure range measurement.

When a STA receiving an HE Ranging NDP sets the LTFVECTOR parameter in the PHY-RXLTFSEQUENCE.request primitive to either a bit string (e.g., the Secure-LTF-bits-R2I or Secure-LTF-bits-I2R) for generating any secure HE-LTF or null (#**1828**, #**1831)**, the STA shall not use the TOA value of the HE Ranging NDP 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.

When there is a transmission failure within a secure measurement exchange sequence, the recovery procedure of the LTF Generation SAC (#**2289)** is illustrated in Figure 11-36o (Error recovery of Non-TB Ranging measurement exchange using Secure LTF ). (#**1129**)



1. Figure 11-36o—Error recovery of Non-TB Ranging measurement exchange using Secure LTF