IEEE P802.11
Wireless LANs

|  |
| --- |
| LB 240 CR MAC Miscellaneous  |
| Date: 2019-11-09 |
| Author(s): |
| Name | Company | Address | Phone | Email |
| Yongho Seok  | MediaTek |  |  | yongho.seok@mediatek.com  |
| ChaoChun Wang | MediaTek |  |  |  |
| James Yee | MediaTek |  |  |  |

**Abstract**

This submission proposes resolutions of comments received from TGaz LB240.

(The proposed change is based on TGaz Draft 1.5.)

* CIDs: 1015, 2025, 1188, 1454, 2259 (5 CIDs)

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 TGaz 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.***

| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** | **Resolution** |
| --- | --- | --- | --- | --- | --- |
| 1015 | 16.28 | 6.3.56.2.4 | States the MLME returns an error to the SME if there is no active FTM session. Clarify what type of "error" and details on what conditions | Clarify as commented | Revised- Since the SME maintains an FTM session, if there is no active FTM session, the SME does not issue the MLME-FINETIMINGMSMT.request primitive. So, remove the error condition. TGaz editor makes changes as specified in 11-19/1958r0 for CID 1015. |
| **TGaz Editor: Change as the following: (#1015)** **6.3.56.2.4 Effect of receipt** ***Change the following paragraph as follows):*** On receipt of this primitive. (#1766)~~— If there is no active FTM session with the specified peer entity, the MLME returns an error to the SME.~~ ~~— If there is an active FTM session where~~ the corresponding measurement exchange is  |
| 2025 |  |  | [Re-raising this comment from the comment collection, as it is not possible to determine from 18/1544r8 whether/how it was addressed. References are to the CC draft and hence may be wrong against D1.0.]PHY-RXLTFSEQUENCE needs to be added to Table 8-2 | As it says in the comment | Revised- Agree in principle. PHY-RXLTFSEQUENCE is added to Table 8-2.TGaz editor makes changes as specified in 11-19/1958r0 for CID 2025.  |
| **TGaz Editor: Change as the following: (#2025)** **8.3.4.2 PHY-SAP inter-(sub)layer service primitives*****Insert a new last row in Table 8-2 as follows:***

|  |
| --- |
| **Table 8-2 - PHY SAP inter-(sub)layer service primitives** |
| Primitive | Request | Indication | Confirm |
| PHY-RXLTFSEQUENCE | X |   |  |

 |
| 1188 | 21.03 | 8.3.5 | The is no PHY-SAP interface to indicate to the Receiver which sequences should be used in future secure EMDG TRN fields | Add a primitive to send those sequences to the PHY, or modify the PHY\_RTLTFSEQUENCES to enable usage in DMG | Revised- Agree in principle. Add a primitive to send the SECURE\_TRN\_SEQUENCES. TGaz editor makes changes as specified in 11-19/1958r0 for CID 1188. |
| **TGaz Editor: Change as the following: (#1188)** **8.3.4.2 PHY-SAP inter-(sub)layer service primitives*****Insert a new last row in Table 8-2 as follows:***

|  |
| --- |
| **Table 8-2 - PHY SAP inter-(sub)layer service primitives** |
| Primitive | Request | Indication | Confirm |
| PHY-RXTRNSEQUENCE | X |   |  |

8.3.4.4 Vector descriptions*Insert the following rows at the end of Table 8-4:* Table 8-4 —Vector description

|  |  |  |
| --- | --- | --- |
| Parameter | Associated vector | Value |
| TRN\_SEQUENCE | TRNVECTOR | Indicates the Secure TRN bit sequences used in the PEDMG secure ranging PPDU. The Secure TRN bit sequences generation is defiend in 12.2.11 (PEDMG Secure Ranging Sequences).  |

8.3.5.22 PHY-RXTRNSEQUENCE.request8.3.5.22.1 FunctionThis primitive is a request by the MAC sublayer to the local PHY entity to provide the Secure TRN bit sequences for the receipt of the PEDMG secure ranging PPDU. 8.3.5.22.2 Semantics of the service primitiveThis primitive provides the following parameter: PHY-RXTRNSEQUENCE.request(TRNVECTOR)The TRNVECTOR represents the Secure TRN bit sequences used in the PEDMG secure ranging PPDU. 8.3.5.22.3 When generatedThis primitive is issued by the MAC sublayer to the PHY entity before receiving the secure TRN subfield of the PEDMG secure ranging PPDU. 8.3.5.22.4 Effect of receiptThe effect of receipt of this primitive by the PHY entity is to make a secure ranging waveform based on the TRNVECTOR. 8.3.5.23 PHY-RXTRNSEQUENCE.confirm8.3.5.23.1 FunctionThis primitive is issued by the PHY to the local MAC entity to confirm that the PHY has applied the parameters provided by the PHY-RXTRNSEQUENCE.request primitive. 8.3.5.23.2 Semantics of the service primitiveThe semantics of the primitive are as follows:This primitive provides the following parameter: PHY-RXTRNSEQUENCE.confirm ()This primitive has no parameters.8.3.5.23.3 When generatedThis primitive is issued by the PHY to the MAC entity when the PHY has received and successfully applied the parameters in the PHY- RXTRNSEQUENCE.request primitive.8.3.5.23.4 Effect of receiptThe effect of the receipt of this primitive by the MAC is unspecified. |
| 1546 | 71.08 | 9.6.7.48 | The definition of the Time-Stamp Error subfield does not seem very efficient or appropriate. We should consider imprioving on this. | Revisit the definition of the Time-Stamp Error subfield and improve on it. | Rejected- The comment fails to identify a specific issue to be addressed. It fails to identify changes in sufficient detail so that the specific wording of the changes that will satisfy the commenter can be determined. |
| 2259 | 128.27 | 12.2.11 | "The first 32 octets of the Secret Key are used for encryption using AES-Counter Mode...of message exchanges between 28 the I-STA and R-STA" - how does this relate to keys established as part of RSNA negotiations that are used to protected data/management frames. If this applies to FTMR/FTM frames, nonce construction, aad construction may need to be specified (or could be the same as RSNA) | Clarify | Revised- Agree in principle. The first 32 octets of the secret key are removed. But, since the related chanes are applied on <https://mentor.ieee.org/802.11/dcn/19/11-19-1785-04-00az-lb240-secure-edmg-ftm-cids-v2.docx>, TGaz editor needs no changes on TGaz Draft for this CID.  |
|  |  |  |  |  |  |
| **Proposed Text Updates: CID 1828, 1831, 1830, 1832*****TGaz Editor: Change the sub-clause 11.22.6.4.6.1 (Secure Non-TB ranging mode ) as the followings:*** 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:— ~~Secure HE-LTF with pre-determined sequence~~ Either the Secure-LTF-bits-UL 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-UL (see 11.22.6.4.6.3 (Secure LTF Generation Information)) based on (#1830, 1832) 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 is set ~~to the LTF sequence generation information in~~ as follows: — ~~Secure HE-LTF with pre-determined sequence~~ Either the Secure-LTF-bits-DL 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-DL (see 11.22.6.4.6.3 (Secure LTF Generation Information)) based on (#1830, 1832) 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 ~~Secure HE-LTF with pre-determined sequence~~ either the Secure-LTF-bits-UL for generating any secure HE-LTF or null (#1828, 1831); — Send an HE Ranging NDP with the TXVECTOR parameter LTF\_SEQUENCE set to ~~Secure HE-LTF with pre-determined sequence~~ either the Secure-LTF-bits-DL 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 a 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-UL (see 11.22.6.4.6.3 (Secure LTF Generation Information)) based on (#1830, 1832) LTF sequence generation information 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-DL (see 11.22.6.4.6.3 (Secure LTF Generation Information)) based on (#1830, 1832) LTF sequence generation information 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 a STA sending an HE Ranging NDP sets the TXVECTOR parameter LTF\_SEQUENCE to ~~Secure HE-LTF with pre-determined sequence~~ either a bit string (e.g., the Secure-LTF-bits-DL or Secure-LTF-bits-DL) 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 ~~Secure HE-LTF with pre-determined sequence~~ either a bit string (e.g., the Secure-LTF-bits-DL or Secure-LTF-bits-DL) 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.***TGaz Editor: Change the sub-clause 11.22.6.4.6.2 (Secure TB ranging mode ) as the followings:*** 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: — ~~secure HE-LTF with predetermined sequence~~ Either the Secure-LTF-bits-UL 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-UL (see 11.22.6.4.6.3 (Secure LTF Generation Information)) based on (#1830, 1832) LTF sequence generation information 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: (a) Send a Ranging NDP Announcement frame. (b) Send an HE Ranging NDP with the TXVECTOR parameter LTF\_SEQUENCE set to as follows: — ~~secure HE-LTF with predetermined sequence~~ Either the Secure-LTF-bits-DL 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-DL (see 11.22.6.4.6.3 (Secure LTF Generation Information)) based on (#1830, 1832) LTF sequence generation information in the Secure LTF Parameters field in the last transmitted Fine Timing Measurement frame or last transmitted Location Measurement Report frame to the ISTA. (c) Send a Location Measurement Report frame that includes the Secure LTF Parameters field to the ISTA. …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 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: — Send an HE TB Ranging NDP with the TXVECTOR parameter LTF\_SEQUENCE set to ~~either secure HE-LTF with predetermined sequence or~~ the Secure-LTF-bits-UL (see 11.22.6.4.6.3 (Secure LTF Generation Information)) based on (#1830, 1832) 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; — Issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR parameter LTF\_SEQUENCE that is set to ~~either secure HE-LTF with predetermined sequence or~~ the Secure-LTF-bits-DL (see 11.22.6.4.6.3 (Secure LTF Generation Information)) based on (#1830, 1832) 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 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: a) Send an HE TB Ranging NDP with the TXVECTOR parameter LTF\_SEQUENCE set to ~~either secure HE-\_LTF with predetermined sequence 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~~ either the Secure-LTF-bits-UL for generating any secure HE-LTF or null (#1828, 1831); b) Issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR parameter LTF\_SEQUENCE that is set to ~~either Secure HE-\_LTF with predetermined sequence 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~~ either the Secure-LTF-bits-DL for generating any secure HE-LTF or null (#1828, 1831); …When an RSTA sending an HE Ranging NDP sets the TXVECTOR parameter LTF\_SEQUENCE to ~~Secure HE-LTF with predetermined sequence~~ either the bit string (e.g., the Secure-LTF-bits-DL or Secure-LTF-bits-DL) 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 a RSTA receiving an HE TB Ranging NDP sets the LTFVECTOR parameter in the PHY-RXLTFSEQUENCE.request primitive to ~~Secure HE-LTF with predetermined sequence~~ either the bit string (e.g., the Secure-LTF-bits-DL or Secure-LTF-bits-DL) 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 ~~Secure HE-LTF with predetermined sequence~~ either the bit string (e.g., the Secure-LTF-bits-DL or Secure-LTF-bits-DL) 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 ~~Secure HE-\_LTF with predetermined sequence~~ either the bit string (e.g., the Secure-LTF-bits-DL or Secure-LTF-bits-DL) 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.***TGaz Editor: Change Table 28-1 (TXVECTOR and RXVECTOR parameters) as follows:***

|  |
| --- |
| Table 28-1—TXVECTOR and RXVECTOR parameters |
| Parameter | Condition | Value | TXVECTOR | RXVECTOR |
| LTF\_SEQUENCE | FORMAT is either HE\_SU or HE\_TB and APEP\_LENGTH is 0 | Indicates the LTF sequence generation information ~~to make the randomized LTF sequence~~ used in the ~~HEz sounding NDP PPDU~~ HE Ranging NDP PPDU or HE TB Ranging NDP PPDU. ~~The LTF sequence generation information is defined in 9.4.2.251 (Secure LTF Parameters).~~Set to the Secure-LTF-bits-DL when the secure HE-LTFs are used and the UPLINK\_FLAG parameter is set to 0 (see 11.22.6.4.6 (Secure Non-TB and -TB Ranging Measurement Exchange Protocol)).Set to the Secure-LTF-bits-UL when the secure HE-LTFs are used and the UPLINK\_FLAG parameter is set to 1 (see 11.22.6.4.6 (Secure Non-TB and -TB Ranging Measurement Exchange Protocol)). Set to null if the regular HE-LTFs are used.  | O | N |
| Otherwise | See corresponding entry in Table 21-1 (TXVECTOR and RXVECTOR parameters). |

***TGaz Editor: Delete 5th entry (LTF\_SEQUENCE parameter) of Table 28-1 (TXVECTOR and RXVECTOR parameters):*** ***TGaz Editor: Change Table 28-2a (LTFVECTOR parameters) as follows:***Table 28-2a—LTFVECTOR parameters

|  |  |
| --- | --- |
| **Parameter** | **Value** |
| LTF\_SEQUENCE | Indicates the LTF sequence generation information ~~to make the randomized LTF sequence~~ used in the ~~HEz sounding NDP PPDU~~ HE Ranging NDP PPDU and HE TB Ranging NDP.~~The LTF sequence generation information is defined in 9.4.2.251 (Secure LTF Parameters).~~Set to the Secure-LTF-bits-DL when receiving the secure HE-LTFs sent by a RSTA. (see 11.22.6.4.6 (Secure Non-TB and -TB Ranging Measurement Exchange Protocol)).Set to the Secure-LTF-bits-UL when receiving the secure HE-LTFs sent by an ISTA. (see 11.22.6.4.6 (Secure Non-TB and -TB Ranging Measurement Exchange Protocol)).Set to null if receiving the regular HE-LTFs.  |

 |
| 1833 | 111.05 | 11.22.6.4.6.1 | "When there is a transmission failure within a secure measurement exchange sequence, therecovery procedure of the LTF Generation SAC and its associated LTF Sequence GenerationInformation parameters is illustrated in Figure 11-o (Error recovery of secure measurementexchange in Non-TB mode)." normative behavior needs to be defined in text not figures. | Reformat figure to normative text. | Rejected- The normative behaviors are already described. Figure shows an example of the error recovery normative behaviour.  |
| 1582 | 116.35 | 11.22.6.4.6.2 | Equation (11-aa) shows in the secure TB ranging mode, the value of Offset in STA info subfield of NDPA is a variable, but when the DL Rep and DL N\_STS is determined, the value of Offset is also determined. Offset\_i = Offset\_{i-1} + DL Rep\_{i-1}\*DL N\_STS\_{i-1} | The equation needs to be revised according to the comment | Rejected- In the Ranging NDPA frame, there is no requirement that the STA Info field shall be listed the ascending order of the Offset subfield value. The changed equation is not correct. |
| 2208 |  | 11.22.6.4.6 | [Re-raising this comment from the comment collection, as it is not possible to determine from 18/1544r8 whether/how it was addressed. References are to the CC draft and hence may be wrong against D1.0.]Most if not all of the "a value of"s are not specifc enough | Change them to "the value of". Similar problem with "keep a current" -> "keep the current" | Rejected- The text changes for the CID 451 that is cited by the commenter had been applied in D1.0. Please refer the below related submission.<https://mentor.ieee.org/802.11/dcn/18/11-18-1781-03-00az-cc28-cr-secure-non-tb-ranging-measurement-exchange-protocol.docx> |
| 2219 |  | 11.22.6.4.6 | [Re-raising this comment from the comment collection, as it is not possible to determine from 18/1544r8 whether/how it was addressed. References are to the CC draft and hence may be wrong against D1.0.]The description of the secure measurement mechanism is extremely opaque | Add a general description outlining the general principles, i.e. what the LTF carries, how this is set at the transmitted and verified at the receiver | Rejected- Based on the comments received in Comment Collection 28, the sub-clause 11.22.6.4.6 (Secure Non-TB and -TB Ranging Measurement Exchange Protocol) has been rewritten for more clarification. Please refer the below submissions.<https://mentor.ieee.org/802.11/dcn/18/11-18-1781-03-00az-cc28-cr-secure-non-tb-ranging-measurement-exchange-protocol.docx><https://mentor.ieee.org/802.11/dcn/18/11-18-1782-02-00az-cc28-cr-secure-tb-ranging-measurement-exchange-protocol.docx> |