IEEE P802.11
Wireless LANs

|  |
| --- |
| CC28 CR of Secure EDMG Measurement Exchange Protocol |
| Date: 2018-09-10 |
| Author(s): |
| Name | Company | Address | Phone | Email |
| SK Yong | Apple |  |  | skyong@apple.com  |
| Mingguang Xu |  |  |  |
| John Dogan |  |  |  |
| Anuj Batra |  |  |  |
| Yongho Seok  | MediaTek |  |  | yongho.seok@mediatek.com  |

**Abstract**

This submission proposes resolutions of comments received from TGaz CC28.

(The proposed change is based on TGaz Draft 0.4.)

* CIDs: 527, 533 (2 CIDs)

| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** | **Resolution** |
| --- | --- | --- | --- | --- | --- |
| 527 | 69.16 | 11.22.6.4.8 | More rules are needed to describe the FTM retransmissio | A contribution will be submitted | Revised- Agree in principle. TGaz editor makes changes as shown in the as specified in 11-18/1616r0.  |
| 533 | 68.43 | 11.22.6.4.8 | "The FTM frames transmitted shall be based on the format as described in Section 29.9.3."When the FTM frames are transmitted in the EDMGz secure ranging PPDU format, the TXVECTOR SECURE\_TRN\_SEQUENCES parameter is provided by the MAC layer.The draft shall specify how the MAC layer determines the TXVECTOR SECURE\_TRN\_SEQUENCES parameter. | Define the procedure that the MAC determines the TXVECTOR SECURE\_TRN\_SEQUENCES parameter. | Revised- Agree in principle. TGaz editor makes changes as shown in the as specified in 11-18/1616r0. |

***TGaz Editor: change the table title of 11.22.6.3.3 as follows:***

***Table ~~abc~~ 11-11a: ~~Possible setting of Secure ToF Measurement field based on the setting of the Secure ToF Supported field and Secure ToF Measurement field of the intiating STA~~Secure ToF Supported and Secure ToF Measurement field combinations.***

***TGaz Editor: Change the subclause 11.22.6.4.8 as follows:***

**11.22.6.4.8 Secure EDMG Measurement Exchange Protocol**

The Secure EDMG Measurement exchange protocol shall be used based on Table ~~abc~~ 11-11a (Secure ToF Supported and Secure ToF Measurement field combinations) as described in ~~11.22.6.3. (Fine timing measurement procedure negotiation)~~11.22.6.3.3 (EDMG Secure ToF Measurement Setup). The Secure EDMG Measurement exchange protocol follows the procedure as described in 11.22.6.4.1 with the following changes:

—The FTM frames transmitted shall be based on the format as described in Section 29.9.3.

—The Secure TRN subfield in Table 51 shall be set to 1

—The FTM frame transmitted by the responder to initiator shall use the first path AWVs obtained during First Path Beamforming Training as described in 10.39.9.6 First Path Beamgorming Training ~~[802.11ay D1.2]~~.

—The Ack frame transmitted by the initiator to the responder shall use the first path AWVs obtained during First Path Beamforming Training as described in 10.39.9.6 First Path Beamforming Training ~~[802.11ay D1.2]~~.

—If the Ack frame for a transmitted FTM frame is not received, the RSTA may retransmit the FTM frame. In this case, the RSTA shall send a FTM frame with the same Action frame body as the Fine Timing Measurement frame for which the Ack was not received, except for updating the Dialog Token if it was nonzero, and a new Secure TRN Sequence shall be used. The Sequence Number in the MAC header is also updated.

~~The ISTA shall check if the the TOA & TOD in the new FTM contents is the same as previous FTM frame it received. If the content is the same, then the initiator shall discard the previous timestamps its captured, and shall capture a new set of timestamps.~~

The following rules apply to the FTM retransmission of the secure EDMG measurement exchange:

1. If FTM retransmission is successful, the ISTA may derive the RTT using the received TOA (t4) and TOD (t1) values included in the retransmitted Fine Timing Measurement frame, and t2 and t3 values estimated locally in the prior (or preceding) fine timing measurement.
2. During the FTM retransmission, the t2 value estimated by the ISTA shall not be used for RTT calculation in the subsequent fine timing measurement. This is because the t2 was estimated by correlating two unmatched secure TRN as a result of FTM retransmission
3. During the FTM retransmission, the t4 value estimated by the RSTA shall not be included in the subsequent Fine Timing Measurement frame. This is because the t4 was estimated by correlating two unmatched secure TRN as a result of FTM retransmission.
4. Due to rule a) and/or rule b, the fine timing measurement immediately after the FTM retransmission shall not be used by ISTA for RTT calculation
5. A successful FTM retransmission shall only be counted towards to the total number of FTMs Per Burst value

If an RSTA does not perform FTM retransmission, the maximum number of Fine Timing Measurement frame retransmissions the RSTA might attempt to zero, the RTSA shall send a new Fine Timing Measurement frame (with TOA=0, TOD=0, updated Dialog Token) with new Secure TRN (associated with the updated dialog token) appended.

An STA shall maintain the Dialog Token Counter, and update the Dialog Token Counter to (Dialog Token field value – 1) mode 254 + 1, where the Dialog Token field value corresponds to the value of the Dialog Token field either in the lastly transmitted FTM frame if the STA is an RSTA frame or in the lastly received FTM frame if the STA is an ISTA.

A STA transmitting an EDMGz secure ranging PPDU to a peer STA shall set the TXVECTOR parameter as follows:

— Secure TRN set to 1

— Secure TRN Sequence contains the TRN sequences associated with the Dialog Token Counter.

After transmitting an EDMGz secure ranging PPDU, a STAs MAC sublayer issues a PHY-RXTRNSEQUENCE.request with a TRNVECTOR parameter that provides the TRN sequence associated with the Dialog Token Counter.

When an RSTA transmits an EDMGz secure ranging PPDU, it shall include the Protected FTM frame in which where the Dialog Token field is set to the Dialog Token Counter.

When an ISTA transmits an EDMGz secure ranging PPDU, it shall include the ACK frame in a control response of the received Protected FTM frame.

An ISTA shall discard the time stamps measured from an EDMGz secure ranging PPDU if the Dialog Token field in the Protected FTM frame in the EDMGz secure ranging PPDU is not matched with its Dialog Token Counter.