IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 802.11az EDMGz Secure ToF Amendment Text | | | | |
| Date: 2018-07-09 | | | | |
| Author(s): | | | | |
| Name | Company | Address | Phone | Email |
| SK Yong | Apple |  |  | skyong [at] apple.com |
| Mingguang Xu |  |  |  |
| John Dogan |  |  |  |
| Anuj Batra |  |  |  |
| Ganesh Venkatensen | Intel |  |  |  |
| Carlos Cordeiro |  |  |  |
| Assaf Kasher | Qualcomm |  |  |  |

**Abstract**

This submission proposes P802.11az draft amendment text for the P802.11az EDMGz secure ranging measurement. This submission addresses SFD (document 17/0462r14) requirements 6 (Security) (17), (18) and (19). The baseline documents that this proposal depends on are (clause numbering relative to .11aj, .11ak, .11aq, .11ax and .11ay)

1. D1.0 of REVmd
2. D8.0 of PIEEE802.11aj
3. D5.0 of PIEEE802.11ak
4. D13.0 of PIEEE802.11aq
5. D1.2 of PIEEE802.11ay and D2.3 of IEEE 802.11ax

***TGaz Editor: Add the following definition to section 3.2 of Rev11md D1.2:***

EDMGz secure ranging physical layer (PHY) protocol data unit (PPDU): EDMG SU PPDUs that contain Secure TRN Sequences in the TRN field to enable secure ranging with PHY-level security

***TGaz Editor: Update the Table 9-272 Format And Bandwidth field as follows:***

|  |  |  |
| --- | --- | --- |
| **Field value** | **Format** | **Bandwidth (MHz)** |
| 0 | No preference | No preference |
| 1-3 | Reserved | Reserved |
| 4 | Non-HT | 5 |
| 5 | Reserved | Reserved |
| 6 | Non-HT | 10 |
| 7 | Reserved | Reserved |
| 8 | Non-HT, excluding Clause 15 (DSSS PHY specification for the 2.4 GHz band designated for ISM -applications) and Clause 16 (High rate direct sequence spread spectrum (HR/DSSS) PHY -specification) | 20 |
| 9 | HT mixed | 20 |
| 10 | VHT | 20 |
| 11 | HT mixed | 40 |
| 12 | VHT | 40 |
| 13 | VHT | 80 |
| 14 | VHT | 80+80 |
| 15 | VHT (two separate RF LOs) | 160 |
| 16 | VHT (single RF LO) | 160 |
| 17-30 | Reserved | Reserved |
| 31 | DMG | 2160 |
| 32 | EDMG (Single Carrier Mode) | 2160 |
| 33 | EDMG (Single Carrier Mode) | 4320 |
| 34 | EDMG (Single Carrier Mode) | 8640 |
| 35 | EDMG (Single Carrier Mode) | 2160+2160 |
| 36 | EDMG (Single Carrier Mode) | 4320+4320 |
| ~~32~~37–63 | Reserved | Reserved |

***TGaz Editor: Modify 9.4.2.246 NGP Parameters as follows (in 11az D0.2)***

*TGaz Editor:* Update Figure 9-610a as follows:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Element ID (255) | Length | Element ID Extension | NGP Parameters | Optional subelement ~~VHTz specific subelement (optional)~~ | ~~HEz specific subelement (optional)~~ | ~~DMGz Specific subelement (optional)~~ | ~~EDMGz Specific subelement (optional)~~ |
| **Octets** | 1 | 1 | 1 | <TBD> | Variable | <TBD> | <TBD> | <TBD> |

Figure 9-610a NGP Parameters element format

*TGaz Editor:* Update Figure 9-610b as follows:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Status Indication | Value | Secure ToF Measurement ~~Secure LTF Required~~ | Secure ToF Supported ~~Secure LTF Support~~ | | Number of Antennas |
| **Bits:** | 2 | 5 | 1 | 1 8 |

**Figure 9-610b NGP Parameters field format**

*TGaz Editor:* Update text in line 30 page 20 till line 5 page 21 as follows:

The Secure ToF Measurement ~~LTF Requied~~ field is set to 1 to enable a secure ToF measurement ~~LTF measurement~~ exchange between an ISTA and an RSTA. Otherwise the Secure ToF Measurement ~~LTF Requied~~ field is set to 0.

The Secure ToF Supported ~~LTF Support~~ field is set to 1 in the initial Fine Timing Measurement Request frame to indicate that an ISTA supports a secure ToF measurement ~~LTF measurement~~ exchange. Otherwise the Secure ToF Supported ~~LTF Support~~ field is set to 0. The Secure ToF Supported ~~LTF Support~~ field is reserved in the initial Fine Timing Measurement frame (see 11.22.6.3 (Fine timing measurement procedure negotiation)).

The Optional Subelements field contains zero or more subelements. The subelement format and ordering of

subelements are defined in 9.4.3 (Subelements). The Subelement ID field values for the defined subelements are shown in Table 9-610c (Optional subelement IDs for NGP Parameters).

*Update Figure 9-606 in REVmd D1.0 as shown below:*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | B0 B1 | B2 B6 | B7 | B8 B11 | B12 B15 | B16 B23 | B24 B39 | B40 |
|  | Status Indication | Value | Extension Present  ~~Reserved~~ | Number of Bursts Exponent | Burst Duration | Min Delta FTM | Partial TSF Timer | Partial TSF Timer No Preference |
| **Bits:** | 2 | 5 | 1 | 4 | 4 | 8 | 16 | 1 |
|  | B41 | B42 | B43 B47 | B48 B49 | B50 B55 | B56 B71 | B72 B79 |
|  | ASAP Capable | ASAP | FTMs per Burst | Reserved | Format and Bandwidth | Burst Period | Extension Field |
| **Bits:** | 1 | 1 | 5 | 2 | 6 | 16 | 8 |

Figure 9-606 -- Fine Timing Measurement Parameters field format

***Add the following paragraph in between line 35-37 in 9.4.2.166 Fine Timing Measurement Parameters element (11md in D1.0)***

The Extension Present field is set to 1 to indicate the presence of an Extension field that consists of Secure ToF Measurement field, Secure ToF Supported field and Reserved field as shown in Figure 9-606a. The Extension Present field is set to 0 to indicate there is no Extension field presence.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Secure ToF Measurement | Secure ToF Supported | Reserved |
| **Bits:** | 1 | 1 | 6 |

**Figure 9-606a Extension field format**

***Add the following paragraph to the end of 9.4.2.166 Fine Timing Measurement Parameters element (11md in D1.0)***

The Secure ToF Measurement field is set to 1 to enable a secure ToF measurement exchange between an ISTA and an RSTA. Otherwise the Secure ToF Measurement field is set to 0.

The Secure ToF Supported field is set to 1 in the initial Fine Timing Measurement Request frame to indicate that an ISTA supports a secure ToF measurement exchange. Otherwise the Secure ToF Supported field is set to 0. The Secure ToF Supported field is reserved in the initial Fine Timing Measurement frame (see 11.22.6.3 (Fine timing measurement procedure negotiation)).

***TGaz Editor: Insert Table 9-610c after line 8, page 30***

***Insert to Table 9-4.a Optional subelements for Fine Timing Measurement Parameters and adjust the subelement ID assignment accordingly as shown below:***

**Table 9-4.a—Optional subelement IDs for Fine Timing Measurement Parameters**

|  |  |  |
| --- | --- | --- |
| Subelement ID | Name | Extensible |
| 0 | DMGz Specific Parameter |  |
| 1 | DMG Direction Measurement Parameter |  |
| 2 | EDMGz Specific Parameter |  |
| 3 | EDMG Direction Measurement Parameter |  |
| 4-220 | Reserved |  |
| 221 | Vendor Specific |  |
| 222-255 | Reserved |  |

***Add the following text to the below***

The EDMGz Specific Parameters subelement contains a number of fields that are used to advertise the requested or allocated operation configurations from one EDMG STA to another. The EDMGz Specific Parameters subelement is included in the initial Fine Timing Measurement Request frame, as described in 9.6.7.32 (Fine Timing Measurement frame format), and the initial Fine Timing Measurement frame, as described in 9.6.7.33 (Fine Timing Measurement frame format). The use of the The EDMGz Specific Parameters subelement is described in 11.22.6 (Fine timing measurement procedure).

The format of the EDMGz Specific Parameters subelement is shown in 9-aaa (EDMGz Specific Parameters subelement format).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Subelement ID | Length | Ranging Operation Parameters | Secure Ranging Parameters |
| Octets | 1 | 1 | 1 | 96 |

**Figure 9-aaa – EDMGz Specific Parameters subelement format**

The format of the Ranging Operation Parameters field is shown in Figure 9-aab (Ranging Operation Parameters field format).

|  |  |  |
| --- | --- | --- |
|  | Number of Random Sequences | Reserved |
| Bit | 4 | 4 |

**Figure 9-aab – Ranging Operation Parameters field format**

The Number of Random Sequences subfield indicates the total number of independent random sequences within a FTM frame that are transmitted for secure time of flight measurmenet exchange during the ranging session.

The format of the Secure Ranging Parameters field is shown in Figure 9-aac (Secure Ranging Parameters field format).

|  |  |  |
| --- | --- | --- |
|  | Secret Key | Salt |
| Octets | 64 | 32 |

**Figure 9-aac – Ranging Operation Parameters field format**

The Secret Key subfield is used to carry the secret key which is used along with Salt value contained in the Salt subfield, to generate the random sequence(s) as described in Section ABC.

***TGaz Editor: Add the following Section ABC:***

The first 32 octets of the Secret Key are used for encryption using AES-Counter Mode CBC-MAC Protocol

(AES-CCMP) [TBD, 802.11i Chapter] to ensure the privacy and integrity of message exchanges between the I-STA and R-STA. The last 32 octets of the Secret Key are used as Input Key Material (IKM) to generate pseudo-random Secure TRN Sequences that are used to construct secure ranging waveforms at the I-STA and R-STA respectively.

Both the Secret Key and Salt shall be discarded after the FTM session is terminated, i.e., each FTM session shall have a different 64-octet Secret Key and 32-octet Salt.

Generation of pseudo-random Secure TRN Sequences is based on the following rules from reference RFC5869 (available at: <https://tools.ietf.org/html/rfc5869>):

* HKDF (Hashed Message Authentication Code (HMAC)-based Key Derivation Function) must be used.
* The hash function to be employed in HKDF is SHA-256.
* The last (i.e., least significant) 32 octets of the Secret Key are to be used as the IKM in HKDF. See RFC5869, Section 2.2 for IKM.
* The Salt is 32 octets and Salt bit string is not all zeros. See RFC5869, Section 2.2 for Salt.
* A pseudo-random key (PRK) is generated using the hash function accepting IKM and salt as inputs as presented at the end of Section 2.2 of RFC5869.
* The Info field is a fixed string unique to this protocol:
* For example: "IEEE 802.11az ranging” in order to guard against accidental key re-use in a different subsystem.
* Key reuse across different subsystems must be avoided through careful system architecture, Secret Key must not be visible outside of the subsystem.
* See RFC5869, Section 2.3 for Info field.
* Pseudo-random Secure TRN Sequences (Output keying material (OKM)) are produced based on PRK, Info and the length of Secure TRN Sequences as inputs as presented in Section 2.3 of RFC5869.
* One-time calculation of all pseudo-random Secure TRN Sequences for multiple timing measurements is recommended for minimizing HKDF set-up costs in case of multiple ranging attempts.
* Furthermore, if memory is not constrained in an implementation, caching multiple Secret Keys and Salt pairs and pre-generating all Secure TRN Sequences for multiple timing measurements and multiple FTM sessions is allowed provided that this information is not revealed to third parties.

***TGaz Editor: Modify the 10.39.9.6 First path beamforming training of 11ay D1.3 as follows:***A first path beamforming training (FPBT) is a procedure used to determine the best AWV corresponding to the first path. The first path is defined to be the propagation path between TX and RX which is estimated to have shortest time of flight. In line of sight (LOS) conditions, the first path corresponds to the LOS path. If several AWVs have the same estimated shortest time of flight, the beamforming training shall select the first path as the one with best quality. The method a STA uses to determine the first path and the first path with best quality is implementation dependent and beyond the scope of this standard.

Prior to performing the FPBT, the two EDMG STAs are assumed to know its best transmit AWV and receive AWV for data communication. A FPBT shall be completed within the CBAP or SP in which it was initiated.

An EDMG STA that has the First Path Training Supported subfield in the STA’s EDMG Capabilities element equal to 1 is first path beamforming capable.

An EDMG STA shall not initiate ~~first path beamforming training~~ FPBT with a peer EDMG STA that is not capable of ~~performing first path beamforming capable~~ FPBT procedure.

~~An EDMG STA requests first path beamforming training transmitting a BRP frame as part of a BRP setup or BRP training request that has the First Path Training subfield set to 1. An EDMG STA that is first path beamforming capable and that receives a BRP frame with the First Path Training subfield equal to 1 shall set the First Path Training subfield to 1 in the frame that it sends in response to the reception of the BRP frame.~~

~~In a BRP transaction that is part of a first path beamforming training, all transmitted BRP frames shall have the First Path Training subfield set to 1 and shall have the FIRST\_PATH\_TRAINING parameter in the TXVECTOR set to 1. In such a transaction, all TX and RX beamforming training are used to find the AWV of the first path and not the best path~~

The FPBT procedure is the same as BRP-TXSS procedure (see 10.39.9.5) except with the following differences

1. FPBT shall be performed in SISO configuration (corresponding to 10.39.9.5.2 SISO BRP\_TXSS) over a single channel, bonded channel bonding or channel aggregation. FPBT shall not be performed in MIMO configuration.
2. All the phases of the BRP-TXSS procedure shall be supported in FPBT. The use of these phases is dependent on the antenna recipcory and antenna pattern reciprocity properties of the involved EDMG STAs.
3. In the setup phase, the EDMG STA shall transmit BRP frame with First Path Training subfield set to 1 to requests FPBT. An EDMG STA that is FPBT capable, and receives a BRP frame with the First Path Training subfield equal to 1, shall set the First Path Training subfield to 1 in the BRP frame that it sends in response to the reception of the BRP frame.
4. In a BRP transaction (Initiator BRP-TXSS, receive training phase of the responder, Responder BRP-TXSS, and receive training phase of the initiator) that is part of a first path beamforming training, all transmitted BRP frames shall have the First Path Training subfield set to 1 and shall have the FIRST\_PATH\_TRAINING parameter in the TXVECTOR set to 1. In such a transaction, all TX and RX beamforming training using the TRN-field are used to find the AWV of the first path and not the best path.
5. The TRN field of the EDMG BRP-RX packet used for receive training of the responder

* Shall be transmitted with the best first path AWV identified in the preceding Initiator BRP TXSS
* Shall be received with the DMG antenna corresponding to the best first path AWV configuration identified in the preceding Initiator BRP TXSS

1. The TRN field of the EDMG BRP-RX packet used for receive training of the initiator

* Shall be transmitted with the best first path AWV identified in the preceding Responder BRP TXSS or in the receive training of the responder, as defined in 10.39.9.5.2.2.2. 6
* Shall be received with the DMG antenna corresponding to the best first path AWV configuration identified in the Responder BRP TXSS or in the Initiator BRP TXSS, or with multiple DMG antennas, as defined in 10.39.9.5.2.2.2 9

NOTE—First path beamforming training can be employed for positioning applications where it is desired that range and direction measurements are performed with beamforming in favor of the LOS path.

***TGaz Editor: Insert the following paragraphs to 9.4.2.250.2 Beamforming Capability field in 11ay D1.2***

***Update Figure 32 as follows:***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | B0 B4 | B5 | B6 | B7 | B8 |
|  | Requested BRP SC Blocks | MU-MIMO Supported | Reciprocal MU-MIMO Supported | SU-MIMO Supported | Grant Required |
| bits | 5 | 1 | 1 | 1 | 1 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | B9 | B10 | B11 | B12 | B13 | ~~B13~~ B14-B15 |
|  | DMG TRN RX Only Capable | First Path Training Supported | Hybrid Beamforming and MU-MIMO Supported | Hybrid Beamforming and SU-MIMO Supported | EDMG Ranging Supported | Reserved |
| bits | 1 | 1 | 1 | 1 | 1 | 2 ~~3~~ |

***Add to the following text to the end of the paragraph***

The EDMG Ranging Suported subfield is set to 1 to inficate that the EDMG STA is capable of performing range measurement based on FTM. This subfield is set to 0 otherwise

***TGaz Editor: Insert the following paragraphs to the end of the 11.22.6.1 Overview:***

For DMG and EDMG, an FTM session shall be preceded by a First Path Beamforming Training as described in 10.39.9.6 First Path Beamgorming Training [802.11ay D1.2].

11.22.6 Fine timing measurement (FTM) procedure

***Change the last two paragraphs in subclause 11.22.6.1 as follows:***

The measurement exchange is one of the following:

1. FTM Measurement Exchange: Exchange of Fine Timing Measurement frames in bursts.
2. VHTz Ranging: a sequence of uplink Null Data Packet Announcement, uplink Null Data Packet, downlink Null Data Packet and downlink Location Measurement Report.
3. HEz Ranging: Multiuser exchange of downlink poll, multiuser uplink poll response, downlink trigger, multiuser uplink NDPA, multiuser uplink NDP, downlink NDP and downlink Location Measurement Report to multiple STAs.
4. DMGz Ranging: FTM Measurement Exchange (see (a)) between DMG STAs ~~Ranging over a link in the 60 GHz band~~.
5. eDMGZ Ranging: FTM Measurement Exchange (see (a)) between EDMG STAs ~~<tbd> sequence over a 802.11ay link~~.

~~Sequences (b), (c), (d) and (e) above are referred to as 802.11az ranging protocols in this specification.~~

***TGaz Editor: Change the last two paragraphs in subclause 11.22.6.1.1 as follows:***

The ISTA in Figure 11-35 (Concurrent FTM sessions) establishes sessions with RSTA 1 and RSTA 2 on different channels. The sessions’ availability window instance periodicity might be different as well as the RSTAs’ clock offsets and thus, over time, some temporal conflicts may occur. To overcome this, during each availability window the ISTA indicates its availability. The method to indicate availability depends on the channel access method used for FTM. There are two basic channel access methods for RSTA centric scheduling: Trigger Based channel access used by HEz and EDCA based channel access used by legacy FTM, VHTz, DMGz and EDMGz. In HEz at the beginning of each availability window the RSTA polls the ISTAs to indicate their need for measurement resources and allocates medium for channel sounding based on the ISTAs’ responses. In EDCA based measurement the ISTA transmits an FTM Request to indicate its on channel availability.

In EDCA based channel access the ISTA transmits a Fine Timing Measurement Request frame (see 11.22.6.4 (Measurement exchange)). During each burst instance, the RSTA transmits one or more Fine Timing Measurement frames as negotiated.

***TGaz Editor: Change the following paragraph after the 4th paragraph in 11.22.6.2***

1. DMGz Ranging, it shall set the DMG Range Measurement field of the Extended Capabilities element to 1. Otherwise it shall set the Multi User Range Measurement field of the Extended Capabilities element to 0.
2. EDMGz Ranging, it shall set the DMG Ranging Supported subfield of the Beamfoming Capability field in the Extended Capabilities field of the EDMG Capabilities element to 1. Otherwise it shall set to 0.

***TGaz Editor: Change the 3rd and 4th paragraphs in Clause 11.22.6.3 as shown below:***

The initial Fine Timing Measurement Request frame shall have:

— the Trigger field set to 1,

— a set of scheduling parameters in a Fine Timing Measurement Parameters element or a set range measurement parameters in a NGP Parameters element that describe the ISTA’s availability for measurement exchange.

The first Fine Timing Measurement frame in the FTM session is called the *initial* Fine Timing Measurement frame. The RSTA should transmit an initial Fine Timing Measurement frame within 10 ms in response to the initial Fine Timing Measurement Request frame. This initial Fine Timing Measurement frame shall include the Fine Timing Measurement Parameters element or a NGP Parameters element. If an NGP Parameters element is included in the initial Fine Timing Measuremetn frame, it shall contain one of the VHTz Specific subelement or the HEz Specific subelement ~~or the DMGz Specific sublement or the EDMGz Specific subelement~~. If a Fine Timing Measurement Parameters is included in the initial Fine Timing Measuremetn frame, the Fine Timing Measurement Parameters element shall contain one of the DMGz Specific Parameter subelement or the EDMGz Specific Parameters subelement. The value of the Status Indication field indicates the outcome of the request.

***TGaz Editor: Add the following between the 7th and 8th paragraphs in Clause 11.22.6.3 (RevMD D1.0) as shown below:***

The ISTA that supports secure ToF measurement shall set the Secure ToF Supported field to 1, and shall set the Secure ToF Measurement field

—to 1 if it intended to setup a secure ToF measurement exchange protocol.

—to 0 if it intended to setup a non-secure ToF measurement exchange protocol

The ISTA that does not support secure ToF measurement shall set the Secure ToF Supported field to 0, and shall always set the Secure ToF Measurement field to 0.

Depending on the setting of the Secure ToF Supported field and Secure ToF Measurement field of the ISTA, the RSTA may set the Secure ToF Measurement field according to Table abc. Other combinations not listed in the Table abc, shall not be set by both the ISTA and RSTA.

**Table abc: 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.**

|  |  |  |  |
| --- | --- | --- | --- |
| ISTA (valid combination) | | RSTA (valid combination) | |
| Secure ToF Supported field | Secure ToF Measurement field | Secure ToF Supported field | Secure ToF Measurement  field |
| 0 | 0 | 0 | 0 |
| 1 | 0 |
| 1 | 0 | 0 | 0 |
| 1 | 0 |
| 1 | 1 | 0 | 0 |
| 1 | 1 |

***TGaz Editor: Insert the following text in 11.22.6.3 in between the 8th and 9th paragrapgh (11az D0.2)***

An EDMG ISTA and an EDMG RSTA may use secure ToF Measurement exchange mode of the EDMGz ranging protocol as described in the subclause 11.22.6.5a (Secure EDMG Measurement Exchange Protocol).

An RSTA in which dot11SecureLTFImplemented is true shall set the Secure LTF Support field in the Extended Capabilities element to 1. An ISTA in which dot11SecureLTFImplemented is true shall set the Secure LTF Support field to 1 in the NGP Parameters field in an initial Fine Timing Measurement Request frame.

When an RSTA has set the Secure LTF Support field to 1 in the Extended Capabilities element it transmits, an ISTA with dot11SecureLTFImplemented equal to true may set the Secure LTF Required subfield in the NGP Parameters field in an initial Fine Timing Measurement Request frame to 1 to activate a secure LTF measurement exchange mode between the ISTA and the RSTA

When an ISTA has set the Secure LTF Support field to 1 in the NGP Parameters field in an initial Fine Timing Measurement Request frame it transmits, an RSTA with dot11SecureLTFImplemented equal to true may set the Secure LTF Required subfield in the NGP Parameters field in an initial Fine Timing Measurement frame to 1 to activate a secure LTF measurement exchange mode between the ISTA and the RSTA,

An initial Fine Timing Measurement frame shall contain a Secure LTF Parameters field with a new LTF Generation SAC and a new LTF Sequence Generation Information associated with the LTF Generation SAC when one of the following conditions is met:

— An RSTA received an initial Fine Timing Measurement Request frame where the Secure LTF Required subfield in the NGP Parameters field in the received initial Fine Timing Measurement Request frame is equal to 1.

— An RSTA sets the Secure LTF Required subfield in the NGP Parameters field in a transmitted initial Fine Timing Measurement frame to 1.

When management frame protection is negotiated, a STA shall use the Protected Dual of Public Action frames for an initial Fine Timing Measurement Request, an initial Fine Timing Measurement, and a Location Measurement Report.

An ISTA in which dot11SecureLTFImplemented is false ignores a Secure LTF Parameters if an initial Fine Timing Measurement frame and a Location Measurement Report frame carries the Secure LTF Parameters.

***TGaz Editor: Add the following text to the subclause 11.22.6.4 as follows:***

**11.22.6.4 FTM Measurement exchange overview**

FTM measurement has three basic scheduling mechanisms:

— RSTA centric EDCA based legacy scheduling mode (including DMGz and EDMGz) described in section 11.22.6.4.1

— HEz scheduling mode described in section 11.22.6.4.2

— VHTZ scheduling mode described in section 11.22.6.4.3

***TGaz Editor: Insert the following subclauses after the 11.22.4a.3:***

**11.22.6.4a.3 Secure EDMG Measurement Exchange Protocol**

The Secure EDMG Measurement exchange protocol shall be used based on Table abc as described in 11.22.6.3. (**Fine timing measurement procedure negotiation)**. 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 time stamps its captured, and shall capture a new set of timestamps.

**PHY PART in Section 29.**

***TGaz Editor: Insert the following item to the end of the 29.1.1 Introduction to the EDMG PHY:***

**29.1.1 Introduction to the EDMG PHY**

An EMDG STA may support the following features:

…

* 2.16 GHz, 4.32 GHz, 6.48 GHz, and 8.64 GHz EDMGz secure ranging PPDU using EDMG SC mode (transmit and receive)

***TGaz Editor: In section 29.2.2, replace the two rows of “SECURED\_TRN” and “SECURED\_TRN\_WAVEFORM” with the following ones in Table 40:***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Table 40— TXVECTOR and RXVECTOR parameters** | | | | |
| **Parameter** | **Condition** | **Value** | **TXVECTOR** | **RXVECTOR** |
| SECURED\_TRN | FORMAT is EDMG, EDMG\_MODULATION is EDMG\_SC\_MODE, NUM\_USERS is 1, NUM\_STS is 1 | Indicates whether TRN field, if present in the PPDU, contains Secure TRN sequences.  Enumerated type:  SECURED\_TRN  NON\_SECURED\_TRN | Y | Y |
| Otherwise | Not present | N | N |
| SECURE\_TRN\_  SEQUENCES | FORMAT is EDMG, EDMG\_MODULATION is EDMG\_SC\_MODE, NUM\_USERS is 1, NUM\_STS is 1 | Indicates the Secure TRN Sequences used in the EDMGz secure ranging PPDU. | Y | N |
| Otherwise | Not present | N | N |

***TGay or TGaz Editor: Insert the following item to the end of section 30.2.2 Introduction to the EDMG PHY:***

***TGaz Editor: Insert the following note to the end of section 29.3.2.1***

NOTE—For EDMGz secure ranging PPDU, the TRN field contains Secure TRN Sequences.

***TGaz Editor: Modify the following row in Table 51:***

|  |  |  |  |
| --- | --- | --- | --- |
| Secured TRN | 1 | 5 | When set to 1, indicates that the TRN field, if present, in the PPDU contains Secure TRN Sequences specified in 29.9.3.5. Otherwise, the TRN field, if present, uses the format specified in 29.9.2.2.5. |

***TGaz Editor: Insert the following item to the end of the first paragraph of 29.4.2.3***

The cyclic shift shall not be applied to TRN units that contain Secure TRN Sequences and each transmit chain transmits its own Secure TRN Sequences as defined in section 29.9.3.5 in the case of an EDMGz secure ranging PPDU.

***TGaz Editor: Insert the following item to the end of 29.5.9.2.2.2***

A Secure TRN field (see 29.9.3.5) shall be appended to an SU PPDU for EDMGz secure ranging PPDU.

***TGaz Editor: Add a new section after 29.9.2 PPDU transmission***

**29.9.3 EDMGz secure ranging PPDU**

**29.9.3.1 General**

EDMGz secure ranging PPDUs are used for secure ToF measurements and may be used for secure AoA/AoD measurements.

EDMGz secure ranging PPDU is defined for single space-time stream (*iSTS*=1) PPDUs only.

**29.9.3.2 EDMGz secure ranging PPDU structure**

An EDMGz secure ranging PPDU shall be composed of a non-EDMG portion containing an L-STF, an L-CEF, and L-Header, and of an EDMG portion containing an EDMG-Header-A, a Data field, and a TRN field that contains Secure TRN Sequences only. An EDMGz secure ranging PPDU may include an EDMG-STF and an EDMG-CEF.

If beam refinement is performed on a 4.32 GHz, 6.48 GHz, or 8.64 GHz channel, the Secure TRN Sequences in the TRN field of EDMGz secure ranging PPDUs shall be transmitted over the entire signal bandwidth of the channel.

**29.9.3.3 EDMGz secure ranging PPDU header fields**

EDMGz secure ranging PPDU is indicated by setting the Secure TRN subfield in Table 51 shall be set to 1 in EDMG-Header A.

**29.9.3.4 EDMGz secure ranging PPDU duration**

Duration of an EDMGz secure ranging PPDU follows the same procedure as an EDMG SU PPDU with TRN field appended as described in section 29.9.2.2.4. Each TRN subfield that contains the Secure TRN sequence is of the same duration as each TRN subfield as described in section 29.9.3.6.

**29.9.3.5 TRN field definition for Secure TRN Sequences**

The Secure TRN Sequences enable secure ranging measurements by EDMGz STAs.

**29.9.3.5.1 TRN field structure for Secure TRN Sequences**

The TRN field structure containing the Secure TRN Sequences in EDMGz secure ranging PPDU is shown in Figure 175 with P=0, M=[TBD], and N=0.

In an EDMGz secure ranging PPDU, all TRN subfields of all TRN-Units shall be transmitted using the same AWV as the preamble and data field of the PPDU. Each TRN-Unit shall have TBD TRN subfield that contains Secure TRN Sequences.

**29.9.3.6 TRN subfield definition for EDMGz secure ranging PPDU**

An EDMGz secure ranging PPDU transmitted over a 2.16 GHz channel shall be defined at the SC chip rate equal to 1.76 GHz. The symbol blocking structure for the normal GI shall be as shown in Figure aaa. An EDMGz STA shall support the SU PPDU structure with normal GI as shown in Figure aaa.

The single space-time stream of an EDMGz secure ranging PPDU with *iSTS*=1 shall be mapped to a single transmit chain with *iTX* =1 as defined in 30.5.10.4.1, and the single transmit chain is chosen by the first path beamforming training procedure in 10.39.9.6. All fields of EDMGz secure ranging PPDU shall be transmitted with the same single transmit chain and AWV chosen by the first path beamforming training procedure.

An EDMGz secure ranging PPDU transmission over a 4.32 GHz, 6.48 GHz, and 8.64 GHz channel shall be defined at the *NCB*×1.76 GHz chip rate. The symbol blocking structure for the normal GI is as shown in Figure aab. An EDMGz STA shall support the SU PPDU structure with normal GI as shown in Figure aaa and Figure aab, for 2.16GHz and 4.32, 6.48, and 8.64 GHz, respectively.



Figure aaa – EDMGz secure ranging PPDU over 2.16 GHz channel.



Figure aab – EDMGz secure ranging PPDU over 4.32, 6.48, and 8.64 GHz channel.

As shown in Figure aaa and Figure aab, each TRN subfield that contains Secure TRN Sequences shall consist of five consecutive segments:

* GI: the GIe164\*NCB as defined in section 29.10;
* Zero prefix: A prefix of 128\*NCB zero channel symbols;
* Secure ranging field: Secure ranging waveform composed by 384\* NCB -BPSK modulated channel symbols, which is generated based on the binary pseudo-random SECURE\_TRN\_SEQUENCE in the TXVECTOR parameters as defined in Table 40. Constellation mapper maps the sequence of bits to constellation points; see section 29.4.5.2.4;
* Zero postfix: A postfix of 128\*NCB zero channel symbols;
* GI: the GIe164\*NCB as defined in section 29.10.

The overall length of each Secure TRN subfield is the same as each TRN subfield defined as in section 29.9.2.2.7.

**29.9.3.7 Tranmission of an EDMGz secure ranging PPDU.**

Tranmission of an EDMGz secure ranging PPDU follows the same procedure as EDMG SU PPDU transmission as in section 29.5.10.4 with TRN field containing Secure TRN Sequences.