IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Clause 3 and 4 CIDs | | | | |
| Date: 2018-11-25 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Assaf Kasher | Qualcomm |  |  | akasher@qti.qualcomm.com |
| Alecsander Eitan | Qualcomm |  |  | eitana@qti.qualcomm.com |
| Solomon Trainin | Qualcomm |  |  | strainin@qti.qualcomm.com |

Abstract

This document proposes resolution to CIDs on clause 3 and 4.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 74 | 4.00 | 4.3.19.19 | No architectural discussion of using DOA and AOD for actual positioning | submission will be provided |
| 189 | 4.00 | 4.3.19.19 | Shouldn't have a TBD | Replace the TBD with some text |

Proposed Resolution: **Revised**

#### **4.3.19.19 Fine timing measurement**

Fine timing measurement allows a STA to accurately measure the round trip time (RTT) between it and another STA. With the regular transfer of Fine Timing Measurement frames it is possible for the recipient STA to track changes in its relative location with other STAs in the environment. DMG and EDMG devices can also estimate the direction of the transmission and reception of frames, allowing for a single link positioning. An HE STA may poll other HE STAs using the TB ranging sequence, whether they request range measurement and then schedule times for concurrent range measurements to several HE STAs.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 60 | 3.00 | 3.1 | It doesn't appear common in the 802.11-2016 standard to define a STA with a particular feature with respect to its MIB variable. Cf. "non-40-MHz-capable (non-40MC) high-throughput (HT) station (STA): A STA that is not a 40-MHz- capable (40MC) HT STA." or "geolocation database dependent (GDD) enabling station (STA): A STA that has the authority to control the operation of GDD dependent STAs after obtaining available spectrum for use at its own location." | Just put "Pre-association security negotiation STA: A station that implements pre-association security negotiation (PASN)." |

Proposed Resolution: **Reject**

**Discussion:**

The commenter is right, however, several new definitions in RevMD, especially those associated with security, use MIB variables, Examples are: fast initial link setup station (FILS STA), centralized authentication controlled (CAC) station (STA). In our specific case, the use of the MIB variables makes the definition more accurate, as the PASN may cover many cases.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 183 | 3.00 | 3.1 | "EDMGz" needs to be spelt out, since all abbreviations need to be spelt out in Clause 3 | Rewrite as "blah blah blah (EDMGz)" |
| 186 | 3.00 | 3.1 | It's not clear what a "Secure TRN Sequence" is, with capitals. Is it a field name? | Either append "field" or lowercase |

Proposed Resolution: **Revise**

**Discussion:** The Task Group have agreed to stop using the “z” suffix to define STA and PPDU supporting protocols defined in the draft. We propose to replace EDMGz with PEDMG (standing for Positioning EMDG) and DMGz with PDMG (Positioning DMG). I also think that the text needs to be in 3.2 as it is specific to 802.11.

***TGaz Editor replace all instances of EDMGz with PEDMG.***

***TGaz Editor replace all instances of DMGz with PDMG.***

***TGaz Editor: Add the following abbreviation to clause 3.4 in the right alphabeticl order:***

PDMG positioning directional multi-gigabit

PEDMG positioning enhanced directional multi-gigabit

***TGaz Editor: Modify the definition of secure EDGMz ranging physical layer PPDU (P2L22) as follows:***

**PEDMG secure ranging physical layer (PHY) protocol data unit (PPDU)**: An EDMG SU PPDU that contain Secure TRN subfields in the TRN field to enable secure ranging with PHY-level security.

***TGaz Editor: Modify the begning of Clause 12.2.9 (P77L17) as follows:***

12.2.9 PEDMG Secure Ranging Sequences

Secure PEDMG Ranging uses Secure TRN subfields (see 29.9.3) as part of the TRN fields of EDMG PPDUs. Those TRN subfields are based on bit sequences henceforth denoted as Secure TRN Sequences. These Secure TRN bit Sequences are generated as follows:

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.

***TGaz Editor: Modify 29.9 as follows:***

29.9 EDMG beamforming

29.9.3 PEDMG secure ranging PPDU

29.9.3.1 General

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

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

29.9.3.2 PEDMG secure ranging PPDU structure

An PEDMG 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 subfields only. An PEDMG 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 subfields in the TRN field of PEDMG secure ranging PPDUs shall be transmitted over the entire signal bandwidth of the channel.

29.9.3.3 PEDMG secure ranging PPDU header fields

PEDMG secure ranging PPDU is indicated by setting the Secure TRN field to 1 in EDMG-Header A.

29.9.3.4 PEDMG secure ranging PPDU duration

Duration of an PEDMG 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 Secure TRN subfield is of the same duration as each TRN subfield as described in section 29.9.3.6.

29.9.3.5 TRN field definition with Secure TRN subfields

The Secure TRN subfields enable secure ranging measurements by PEDMG STAs.

29.9.3.5.1 TRN field structure with Secure TRN subfields

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

In an PEDMG 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 Secure TRN subfields that contains based Secure TRN sequences.

* + - * 1. 29.9.3.6 Secure TRN subfield definition for PEDMG secure ranging PPDU

An PEDMG 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 secure PEDMG STA shall support the SU PPDU structure with normal GI as shown in Figure aaa.

The single space-time stream of an PEDMG 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 PEDMG secure ranging PPDU shall be transmitted with the same single transmit chain and AWV chosen by the first path beamforming training procedure.

An PEDMG 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 PEDMG 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.



1. —Figure aaa – PEDMG secure ranging PPDU over 2.16 GHz channel.



1. —Figure aab – PEDMG secure ranging PPDU over 4.32, 6.48, and 8.64 GHz channel.

As shown in Figure aaa and Figure aab, each Secure TRN subfield 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: A Secure ranging waveform composed by 384\* NCB -BPSK modulated channel symbols. The modulated symbols are based on bit sequences of length 384\*NCB which is are taken from the binary sequence SECURE\_TRN\_SEQUENCE in the TXVECTOR parameters as defined in Table 40. Each group of 384\*NCB is taken consecutively without overlap from the sequence. 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 Transmission of an PEDMG secure ranging PPDU**

Transmission of an PEDMG 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.

***TGaz Editor: Modify P74L22025 as follows:***

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

—SECURED\_TRN set to SECURED\_TRN

— SECURE\_TRN\_SEQUENCE contains the Secure TRN bit sequences associated with the Dialog Token Counter.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 185 | 3.00 | 3.1 | 802.11 is only concerned with 802.11 | Delete "802.11" in "802.11 association" (also in 4.5.4.2; also in "802.11 authentication" in 12.13.1) |

Proposed Resolution: **Accept**

***TGaz Editor: Modify P2L15-16 as follows:***

**Pre-association security negotiation (PASN)**: A mechanism to establish security association and allow management frame protection prior to association.

***TGaz Editor: Modify P3L28 as follows:***

authentication allows management frame protection prior to association by establishing a

***TGaz Editor: Modify P82L19 as follows:***

PTKSA using a three message authentication frame exchange. Some salient aspects of this

***TGaz Editor: Modify P82L29 as follows:***

Key establishment and key confirmation is accomplished using authentication frames.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 197 | 3.00 | 3.1 | Definitions for VHTz and HEz are missing | Add missing definitions |

Proposed Resolution: **Reject**

**Discussion:**

VHTz and HEz (as adjectives) have been replaced by non-TB and TB. These are well defined in clause 11 and a definition in clause 3 is not necessary

**SP:** Do you agree to the resolution of CIDs 74, 189, 60, 183, 185, 197 as specified in doc 11-18-2152?

**References:**