IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| LB253 Resolution to some CID set2 | | | | |
| Date: 2021-02-24 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Assaf Kasher | Qualcomm |  |  | assaf.kasher@gmail.com |
|  |  |  |  |  |

Abstract

Editor instruction based on D3.0

CIDs resolved: 5219, 5029, 5400, 5139, 5152, 5097, 5098, 5429, 5260

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 5219 | 133.00 | 36 | 11.21.6.3.7 | AoA Results could be used for non-DMG devices | Add text that enables AoA for non-DMG devices | **Revise**,  TGaz Editor: perform the instructions in [https://mentor.ieee.org/802.11/dcn/21/11-21-0564-02-00az-lb253-resolution-to-cid-set2.docx](https://mentor.ieee.org/802.11/dcn/21/11-21-0564-00-00az-lb253-resolution-to-cid-set2.docx) |
| 5029 | 101.00 |  | 9.6.7.49 | The spec states for TB/Non-TB to use 'Directional Measurement Result Element' to report 'AoA Feedback' as some of the fields in that element do not apply such as 'Best AWV ID' etc. | Add a new element for reporting AoA feedback for TB and Non-TB | **Revise**,  TGaz Editor: perform the instructions in [https://mentor.ieee.org/802.11/dcn/21/11-21-0564-02-00az-lb253-resolution-to-cid-set2.docx](https://mentor.ieee.org/802.11/dcn/21/11-21-0564-00-00az-lb253-resolution-to-cid-set2.docx) |

***TGaz Editor: Modify the text in P81L33 as follows:***

element).

***TGaz Editor: Modify the text in P82L23-27 as follows:***

If the STA sending the frame containing the element is a DMG STA, and the frame containing the Direction Measurement Result element follows an ISTA PPDU that enabled AOD by containing TRN-T subfields, the Best AWV ID subfield contains the index of the TRN-T subfield that was received with the highest SNR. If the ISTA PPDU than enabled AOD contained EDMG TRN-T subfields, the AWV ID field contains the AWV ID (see 28.9.2.2.5 (TRN field definition)) of the TRN subfields that were received with the highest SNR.

If the STA sending the frame containing the element is a non-DMG STA, the Best AWV ID subfield is reserved.

***TGaz editor: add the text below in page 154 after line 12 starting a new paragraph within section 11.21.6.4.3.4 Reporting phase of TB Ranging measurement***

In TB ranging measurement reporting phase, if R2I AOA feedback was negotiated the RSTA shall include the optional AOA feedback subfield in the R2I LMR frame and if I2R LMR reporting was negotiated in addition to I2R AOA Feedback reporting then the ISTA shall include the optional AOA feedback subfield in the I2R LMR frame. The AOA field contains the Direction Measurement Results element described in 9.4.2.300.

***TGaz editor add the text below in page 160 after line 23 starting a new paragraph within section 11.21.6.4.4.3 Non-TB Ranging Measurement Reporting phase***

In Non-TB ranging measurement reporting phase, if R2I AOA feedback was negotiated the RSTA shall include the optional AOA feedback subfield in the R2I LMR frame and if R2I LMR reporting was negotiated in addition to I2R AOA Feedback reporting then the ISTA shall include the optional AOA feedback subfield (see 9.4.2.300, Direction Measurement Results element) in the I2R LMR frame. The AOA field contains the Direction Measurement Results element described in 9.4.2.300.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 5400 | 142.00 | 27 | 11.21.6.4.2.1.6 | Meaningless sentence "When an ISTA transmits an EDMG secure ranging PPDU, it shall include the Ack frame in a control response of the received Protected FTM" frame. | Remove the sentence | **Revise**,  TGaz Editor: perform the instructions in [https://mentor.ieee.org/802.11/dcn/21/11-21-0564-02-00az-lb253-resolution-to-cid-set2.docx](https://mentor.ieee.org/802.11/dcn/21/11-21-0364-00-00az-lb253-resolution-to-cid-set2.docx) |

***TGaz Editor: Modify the text in P142L27 as follows:***

An ISTA shall transmits an Ack frame to the received Protected FTM frame as an EDMG secure ranging PPDU.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 5139 | 138.00 | 39 | 11.21.6.4.2.1.2 | "The RSTA may use implementation dependent AWV (such as sectors) in the TRN field." - this is a bit confusing because of the for purpose of the I2R AOD is the RSTA is receiving | replace with "The RSTA may use implementation dependent AWV (such as sectors) in the reception of the TRN field." |  |

***TGaz Editor: Modify the text in P138L10-42, P139-1-5, as follows:***

In a Direction Measurement FTM pair that agreed on R2I AOA, the RSTA shall add a TRN field to the FTM frames in the exchanges specified by the Direction Measurement Density field by setting the TRN\_LEN/EDMG\_TRN\_LEN to the value of the L\_RX field sent by the ISTA and PPDU\_TYPE/EDMG\_PPDU\_TYPE to 0. In a first path AWV FTM exchange the RSTA shall also set the FIRST\_PATH\_AWV\_TRN TXVECTOR parameter to FIRST\_PATH\_AWV\_ON\_TRN in the Fine Timing Measurement frames it sends to the ISTA. The ISTA may receive the TRN field using implementation dependent AWV settings.(#**2347**,#**1444**)

In a Direction Measurement FTM pair that agreed on I2R AOA, the ISTA shall add a TRN field to the Ack frames in the exchanges specified by the Direction Measurement Density field by setting the TRN\_LEN/EDMG\_TRN\_LEN to the value of the L\_RX field of the DMG Direction Measurement Parameters received from the RSTA and PPDU\_TYPE/EDMG\_PPDU\_TYPE to 0. In a first path AWV FTM exchange the ISTA shall also set the FIRST\_PATH\_AWV\_TRN TXVECTOR parameter to FIRST\_PATH\_AWV\_ON\_TRN in the Ack frames it sends to the RSTA. The RSTA may receive the TRN field using implementation dependent AWV setting. The RSTA shall provide the AOA measurement results in the Direction Measurement Result element included in the next FTM frame sent to the ISTA.

In a Direction Measurement FTM pair that agreed on R2I AOD, the RSTA shall add a TRN field to the FTM frames in the exchanges specified by the Direction Measurement Density field by setting the TRN\_LEN/EDMG\_TRN\_LEN to a non-zero value and PPDU\_TYPE/EDMG\_PPDU\_TYPE to 1. In a first path AWV FTM exchange the RSTA shall also set the FIRST\_PATH\_AWV\_TRN TXVECTOR parameter to FIRST\_PATH\_AWV\_ON\_TRN in the Fine Timing Measurement frames it sends to the ISTA. The ISTA shall receive the TRN field using the first path AWV setting. The RSTA may use implementation dependent AWV (such as sectors) in the TRN field.

In a Direction Measurement FTM pair that agreed on I2R AOD, the ISTA shall add a TRN field to the Ack frames in the exchanges specified by the Direction Measurement Density by setting the TRN\_LEN/EDMG\_TRN\_LEN to a non-zero value and PPDU\_TYPE/EDMG\_PPDU\_TYPE to 1. In a first path AWV FTM exchange the ISTA shall also set the FIRST\_PATH\_AWV\_TRN TXVECTOR parameter to FIRST\_PATH\_AWV\_ON\_TRN in the Ack frames it sends to the RSTA. The RSTA shall receive the TRN field using the first path AWV setting. The ISTA may use implementation dependent AWV (such as sectors) in the TRN field. The RSTA shall set the Best AWV Id field in the Fine Timing Measurement frames sent to the ISTA following these Ack frames to the AWV Id or the Best Sector Index of the TRN field (if the Ack was an EDMG/DMG PPDU respectively). If the RSTA has set the AOD Channel Measurement Feedback subfield to 1 in the DMG Direction Measurement Capabilities field, it shall also include a Channel Measurement Feedback Type field and a Channel Measurement Feedback field in the Fine Timing Measurement frames sent to the ISTA following the reception of the Ack frames that its RXVECTOR PPDU\_TYPE parameter equal to TRN-T or EDMG\_PPDU\_TYPE equal to EDMG-TRN-T, and TRN-LEN greater than 0 or EDMG-TRN-LEN greater than 0.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 5152 | 20.00 | 17 | 3.2 | It is hard to reconcile the adjective "secure" in "secure ranging physical layer" (and in other terms used elsewhere in this draft) in conjunction with the enhanced ranging protocol. Given the attacks described in documents on the TGaz server, I suspect that a) it is fair to say that Wi-Fi chipsets intended for typical consumer devices will not be able to attack a ranging exchange, but b) FPGA-based device(s) at a few (tens of) thousand dollars will be able to attack a ranging exchange. Given the history of 802.11 security, we should be very careful of overclaiming the practical security reality. | a) add strong security into this exchange, and/or b) find an adjective a good deal weaker than "secure" to describe this exchange, expressing some notion around "non-effortlessly-attackable". | **Reject:**  The group believes the algorithm referenced by the definition in P20L14-17, based on completely “random” sequences, deserves to be called secure. There were no presentation to the group on weaknesses in this method. |
| 5097 | 21.00 | 33 | 3.2 | "DMG" is defined in the baseline 802.11-2020, there is no need to redefine it here as an accronym | remove the accronym definition of DMG | **Accept** |
| 5098 | 21.00 | 34 | 3.2 | "EDMG" is defined in the baseline (P802.11ayD7.0 P22L41). There is no need to redefine it here | remove the accronym definition of EDMG | **Accept** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 5429 | 20.00 | 22 | 3.2 | The definition for "FTM frame", "FTMR frame", "I2R LMR frame", "LMR frame", and "R2I LMR frame" are simply abbreviations. However, "FTM "is already included in the abbreviation section of 802.11MD\_D4.0, "I2R", "R2I" and "LMR" are already included in the "abbreviation" section of 11az\_D3.0. These definitions do not provide any additional information. | Delete definitions for "FTM frame", "FTMR frame", "I2R LMR frame", "R2I LMR frame" and LMR frame" in clause 3.2. Add "FTMR" to the abbreviation section of the 11az spec. | **Revise:**  Accept in principle.  TGaz Editor: perform the instructions in [https://mentor.ieee.org/802.11/dcn/21/11-21-0564-02-00az-lb253-resolution-to-cid-set2.docx](https://mentor.ieee.org/802.11/dcn/21/11-21-0364-00-00az-lb253-resolution-to-cid-set2.docx) |

***TGaz editor:***

***Delete definitions for "FTM frame", "FTMR frame", "I2R LMR frame", "R2I LMR frame" and LMR frame" in clause 3.2.***

***Insert the following definitions in clause 3.4 (P21L25)***

FTMR Fine Timing Measurement Request

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 5260 | 22.00 | 27 | 4.3.19.19 | What is a "FTM session frame" in "The Pre-association Security Negotiation protocol enables establishment of a security context for the exchange of protected frames to establish an FTM session between two unassociated (#3314) peers and the FTM session frames that enable the measurement exchange." | Define "FTM Session frame" or replace "the FTM Session frame that enable the measurement exchange" with "to execute the measurement exchanges with the corresponding FTM session established." | **Revise:**  (accept one option)  TGaz Editor: perform the instructions in [https://mentor.ieee.org/802.11/dcn/21/11-21-0564-02-00az-lb253-resolution-to-cid-set2.docx](https://mentor.ieee.org/802.11/dcn/21/11-21-0364-00-00az-lb253-resolution-to-cid-set2.docx) |

***TGaz Editor: change the text in P22L27 as follows:***

The Pre-association Security Negotiation protocol enables establishment of a security context for the exchange of protected frames without association, for example, for establishing a secure FTM session between two unassociated (#**3314**) peers and for securing the negotioation and measurement exchanges.

**References: DraftP802.11az\_D3.0**