IEEE P802.11
Wireless LANs

|  |
| --- |
| CR for PHY related comments  |
| Date: 2019-09-11 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Feng Jiang | Intel | 3600 Juliette Ln, Santa Clara, CA 95054 |  | feng1.jiang@intel.com |
| Qinghua Li | Intel |  |  | qinghua.li@intel.com |
| Jonathan Segev | Intel |  |  | jonathan.segev@intel.com |

Abstract

This submission addresses the following LB240 CID based on 11az draft 1.4: 1586, 1341, 2483, 1380 and 2312.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause  | Comment | Proposed Change | Resolution |
| 1825 |  | Annex aa | Secured LTF test vectors should be added to cross check implementations, possibly as an annex | Add test vectors  | RejectHaven’t received resolutioin for this CID before the closure of the WG ballot.    |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause  | Comment | Proposed Change | Resolution |
| 1338 | 160 | 28.3.19a | For zero GI, power will not ramp up/down as a brick wall. Has any study done on the impact of power ramp up/down on channel estimation quality? | as in the comment | RejectThe time domain windowing function is implementation dependent as long as the transmit mask requirement is met, and meanwhile the impact to the channel estimation quality should be minimized.  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause  | Comment | Proposed Change | Resolution |
| 2209 | 111 | 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.]Figure 11-xx Normal secure measurement exchange in VHTz mode would be very helpful indeed to try to make sense of the text" | Add the figure, showing where the various security aspects come from and are transmitted/checked | RejectIn the Figure 11-36n Normal secure measurement exchange in Non-TB mode, the illustrarion of the transmitting and receiving of the SAC singaling for secured LTF generation is clesar and how to check the validity of the SAC is clearly defined in the section 11.22.6.4.6.1 Secure Non-TB ranging mode. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause  | Comment | Proposed Change | Resolution |
| 2479 | 150 | 28.3.19a | There doesn't appear to be any PHY signaling that allows the PHY to distinguish HE Ranging NDPs from HE NDPs. This will increase client power consumption. | Add a PHY indication to distinguish HE Ranging NDP from HE NDP. | RejectIn the TB and non-TB ranging sequence or HE sounding sequence, the NDP frame always follows a NDP Announcement frame, and if the HE STA’s AID is not included in the STA info field of the NDP announcement frame, the HE STA should skip the following NDP frame and not process it. Also, a new type of NDP anncement frame is defined for 11az, and if an 11az capable HE STA receives the HE NDP annocuemnt frame, it should skip the HE NDPA and the following HE sounding NDP frames.  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause  | Comment | Proposed Change | Resolution |
| 2244 | 21 | 8.3.4.4 | Does LTF Sequence parameter in Table 8-4 apply to all the PHYs or must be specified by the MAC or PHY? It applies only to HE PHY and possibly future PHYs? | Clarify or may be relocate and have in only PHY specific? | Revised The LTF Sequence parameter is only used by the PHY of secured TB and Non-TB ranging. The table 8-4 was revised by submission IEEE 802.11-19/1504r0 and please refer to this submission for details.  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause  | Comment | Proposed Change | Resolution |
| 2484 | 153 | 28.3.17b | Improve the likelihood that this amendment will actually be adopted in the market. FTM is currently not a very widely adopted technology. Improve the chances that 11az will actually be implemented. Reduce modes. | Eliminiate either non-zero-power-GI or zero-power-GI. Don't retain both options. | RejectPlease refer to the discussion in the submission 11/19-1563r1. |
| 2482 | 151 | 28.3.19a | Do you expect implementations of non-secure ranging? | Eliminate the option of Regular HE-LTFs for the HE Ranging NDP and TB\_PPDU | RejectPlease refer to the discussion in the submission 11/19-1563r1. |
| 2481 | 151 | 28.3.19a | Improve the likelihood that this amendment will actually be adopted in the market. FTM is currently not a very widely adopted technology. Improve the chances that 11az will actually be implemented. Reduce modes. | Eliminate LTF\_OFFSET | RejectPlease refer to the discussion in the submission 11/19-1563r1. |
| 2480 |  | 28.3.19a | Improve the likelihood that this amendment will actually be adopted in the market. FTM is currently not a very widely adopted technology. Improve the chances that 11az will actually be implemented. Reduce modes. | Either eliminate Repetition (no LTF\_REP) or only have LTF\_REP=2. Eliminate the variable from Table 28-2a. | RejectPlease refer to the discussion in the submission 11/19-1563r1. |

**Discussions:**

The non-secured ranging mode in 11az has lower complexity and better efficieny, and can be used in the trusted network, or used in the scenario when security is not a concern. The secured ranging mode has higher complexity and lower efficiency, but this mode provide enhanced security protection for PHY layers, and also sets a high bar for the implementation of the RSTA and ISTA. Both of the secured and non-secured modes are important to the future markets.

In the secured mode, the repetition of the HE-LTF fields in the ranging NDP enbles the RSTA or ISTA to implement integrity check and the higher the number of repetions, the better the security protection can be ahceived and meanwhile the complexity increases. For a tradeoff beween security protection and implementation complexity, the number of HE-LTF repetition is negotiable between ISTA and RSTA. For a better efficieny of the secured raning mode, the LTF\_OFFSET is used in the secured TB ranging to enble different ISTA to share the the same R2I ranging NDP frame.

The non-zero-power GI is the mandotary mode used by the non-secure mode and even the legacy 11mc FTM. The zero-power GI is an optional mode for providing security. Eliminating the zero-power GI is essentially eliminating the secure ensurance because the non-zero power GI is vulnerable to CP replay attacks. On the other hand, security is an important feature in the FRD that needs to be supported.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause  | Comment | Proposed Change | Resolution |
| 2478 | 151 | 28.3.19a | Limit the number of modes to improve the likelihood that companies will implement 11az. | Eliminate the 2xLTF+0.8GI. Please don't resolve this comment with some bogus explanation about the need to save overhead for such a short frame | RejectThe HE Ranging NDP is a variant of the HE Sounding NDP and support of the 2x HE-LTF with 0.8us GI and 1.6us GI is mandatory requirement of HE Sounding NDP, so it’s natural to keep both of the 0.8us GI and 1.6us GI for HE Ranging NDP. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause  | Comment | Proposed Change | Resolution |
| 2371 | 156 | 28.3.17c | The subcarrier indices are not consistent. When defining LTF in the same subclause, the index are using indices of the 4x symbol. In this paragraph, the subcarrier index k is the index of the 2x symbol. | Make the definition consistent. | RevisedThe definition of the linear phase shift is corresponding to the random cyclic shift is deinded based on 2XLTF tone spacing and is revised to 4xLTF tone spacing for consistency. TGaz editor makes changes as specified in 11-19/1563r0 for CID 2371. |

*TGaz Editor: please revise the lines 19-22 on page 200 of 11az draft 1.4 as below*

After the subcarrier mapping, a linear phase shift for a time-domain CS is applied to each subcarrier. The phase of the -th subcarrier is rotated by , where is the subcarrier spacing for 4x HE-LTF; is the contiguous subcarrier index for the subcarriers with the spacing ; and is given by Equation (27-rr) **(#2368, #2371)**.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause  | Comment | Proposed Change | Resolution |
| 1586 | 53 | 9.4.2.279 | In the Ranging Parameter field, the R2I AOA Req and I2R AOA Rep have been defined, but there is no definition for the feedback type of R2I AOA and I2R AOA. Similar to the ToA, should we define the immediate and delayed feedback type for the AOA? | Define immediate feedback and delayed feedback for the AOA. | RevisedIn submission submission 11/19-1319r2, the Immediate R2I Feedback and Immediate I2R Feedback subfields are defined in the ranging parameter field. The value of 0 indicates a delayed feedback, in which case the measurement results included in the current Location Measurement Report (LMR) frame are from the previous measurement; the value of 1 indicates an immediate feedback, in which case the measurement results included in the current LMR frame are from the current measurement. Please refer to submission 11/19-1319r2 for details. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause  | Comment | Proposed Change | Resolution |
| 1341 | 162 | 28.3.17c | Why introduces a new modulation 8PSK? | as in the comment | RejectPlease refer to the discussion in the submission 11/19-1563r1.   |
| 2483 | 154 | 28.3.17c | Introducing 8PSK into LTFs will be unique to all the other amendments (11g, 11n, 11ac, FTM, 11ax). | Redesign the Randomized LTF sequences so that 8PSK is not used. Use QPSK. | Reject Please refer to the discussion in the submission 11/19-1563r1. |

**Discussion:**

In the secured ranging mode of 11az, the 8PSK modulation is used to generate the random HE-LTF sequence, such that the sample space of HE-LTF sequence is large enough to reduce the probability of successful random guess attack under 10^-7. Take the 20MHz band as an example, if QPSK modulation is used for the random LTF sequence generation, the sample space of the LTF sequence is around 4^2\*4^6\*1288\*10^6, but when 8PSK modulation is used, the sample space is 8^2\*8^6\*1282\*10^9.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause | Comment | Propsoed Change | Resolution  |
| 1380 | 151 | 28.3.19a | Due to its simplicity compared to TB ranging, non-TB ranging should be mandatory. | Add the following text to the sentence "It is mandatory to support the 2x HE-LTF with 0.8 us GI and 2x HE-LTF with 1.6 us GI. The other combinations of HE-LTF modes and GI duration are disallowed." : "It is also mandatory to support non-TB ranging." | Reject The HE ranging NDP format is already mandatory for TB and NTB ranging sequence.  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause | Comment | Propsoed Change | Resolution  |
| 2312 | 153 | 28.3.17b | A zero power guard interval adds yet another preamble mode and it also may cause undesired behavior in legacy devices |  | RejectFrom the comment, it’s not clear what kind of undesired behavior of legacy device will be caused by zero-power GI.In secured mode of 11az, the zero-power GI is added to the HE-LTF field, and the L-SIG, RL-SIG and HE-SIG-A field still use regular guard interval and legacy device can still decode these fields, and subtract the related information. Also, as explained in the resolution for CID 1700 in submission 11-19/1479r2, the zero-power GI will not cause abnormal defer behavirot for the legacy device.  |