IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CR for PHY related comments | | | | |
| Date: 2019-05-14 | | | | |
| 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 CIDs related with sections 28.3.17: 1341, 2483, 1342, 2312, 2368, 2370, and 2484.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause | Comment | Proposed Change | Resolution |
| 1341 | 162 | 28.3.17c | Why introduces a new modulation 8PSK? | as in the comment | Reject  Please refer to the discussion part for more details. |
| 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 part for more details. |

**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 8\*10^6, but when 8PSK modulation is used, the sample space is 2\*10^9.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause | Comment | Proposed Change | Resolution |
| 1342 | 164 | 28.3.17d | Where P HE LTF matrix is defined? Is the P matrix applied across frequency or time? Why abondon the single stream pilot? How to do the phase tracking during HE LTFs | as in the comment | Revised  The “P HE LTF matrix” is not an accuracte descriptopn, and it should be matrix, and this matrix is defined in equation (27-56) of 802.11ax draft 4.1. and this matrix is applied across the time domin HE-LTF symbols. The text is revised. For other comments, pleaes review dicussions for details. |

**Discussion:**

The reason for removing single stream pilot is to mitigate the pilot tone attacker. If there exist pilot tone in HE-LTF symbol, the attacker can generate the pilot tone with some fake phase and transmit the pilot tone during the transmission of secure HE-LTF field of NDP frame, and when the receiver of NDP use pilot tone to estimate phase offset, the receiver will get a fake phase offset, and this will produce a wrong residual CFO value, hurt the channel estimation and the ToA estimation accuracy.

The secured NDP frame includes at least one repetition of HE-LTF field, and the HE-LTF symbols in two HE-LTF fields can be used for phase offset estimation. For example, after receiving the first HE-LTF symbol, transform the time domain signal to frequence domain, and unmask the random LTF sequence in frequency domain, then a combined channel response is obtained and after receiving the first HE-LTF symbol in second HE-LTF field, also transform the time domain singal to frequency domain and unmask the random LTF sequenc, then a second combined channel response is obtained. When there is no phase offset, these two channel response should have the same phase, and through comparing the phase of these two combined channel response, the pahse offset can be estimated.

**Proposed Text Updates for CID 1342**

*TGaz Editor: Please change the lines 24 and 25 on page 156 of section 28.3.17d as below*

* There are no single stream pilot subcarriers in the secure HE-LTFs, all subcarriers are mapped using the matrix

*TGaz Editor: Please change the lines 31 and 32 on page 156 of section 28.3.17d as below*

1. matrix mapping: Apply the matrix to all tones of the secure HE-LTF sequence.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause | Comment | Proposed 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 |  | Reject  In secured mode of 11az, the zero power guard interval 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. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause | Comment | Proposed Change | Resolution |
| 2368 | 154 | 28.3.17c | "CSD" is a confusion term here and may misleading to the per antenna or per stream CSD in 11ax. In 11az, "CSD" is a cyclic shift of the time domain signal with a random time shift applied to all antenna. The CSD value here could be much larger than CSD in 11ac/ax. | Choose a better term and add some clarification for the concept. | Revised  After the frequency domain random LTF sequence is generated, a random cyclic shift is applied to the time domain LTF symbol to increase sample space of random LTF symbol. Instead of using CSD (cyclic shift diversity), it’s better to use CS (cyclic shift). The related spec text has been revised. |

**Proposed Text Updates for CID 2368**

*TGaz Editor: please replace Figure 28-52g - Generation of Randomized LTF Sequence in section 28.3.17c Generation of Randomized LTF Sequence with the following figure.*



*TGaz Editor: Please change the lines 6 and 7 on page 154 of section 28.3.17c as below*

The number is 7, 8, 9, and 10 for 20, 40, 80, and 160/80+80 MHz transmissions, respectively. A Cyclic Shift (CS) value is given by

*TGaz Editor: Please change the lines 6 and 7 on page 154 of section 28.3.17c 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 2x HE-LTF; is the contiguous subcarrier index for the subcarriers with the spacing ; and is given by Equation (28-rr).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause | Comment | Proposed Change | Resolution |
| 2370 | 155 | 28.3.17c | The definition of secure LTF for 160MHz and 80+80MHz is not correct. Length of LTF80MHz\_lower and LTF80MHz\_upper should be 501 but is only defined for 498. Also it seems not necessary to hole out part of s1 and s2 sequences. For example, just use s1^(p-1)(5:1:505) to define LTF80MHz\_lower. | Correct the LTF sequence definition. | Reject  As stated in line 6 on page 155 of section 28.3.17c, the LTF sequence are mapped to the non-zero subcarriers of 2x HE-LTF symbol. For *LTF*80MHz\_lower or *LTF*80MHz\_upper, there are 498 non-zero subcarriers plus 3 zero DC tones, and in total there are 501 subcarrers. So the current mapping is correct.  The LTF mapping with puncturing part of s1 or s2 sequence tries to maximumly exploit the benefit of the Golay sequence structure, such that the PAPR can be minimized. The current mapping structure shall be kept. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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. | Reject  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.  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. |