IEEE P802.11
Wireless LANs

|  |
| --- |
| CR for PHY related comments  |
| Date: 2019-09-03 |
| 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: 1922, 1055, 2274, 1339, 2363, 1700, 2501, 2500.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause  | Comment | Proposed Change | Resolution |
| 1922 |  | 27.3.21 | Security for ranging could mean either confidentiality (privacy; not being able to locate other users) or integrity (not being able to spoof the location of legitimate devices). The Secure HE-LTFs don't help with the former since it is possible for an attacker to make the timing measurement using the (non-secure) L-LTF. That leaves spoofing attacks, e.g.1) An attacker transmitting a signal at the same time as the HE-LTF symbols from the legitimate peer in an attempt to introduce a phase shift and hence change the apparent distance.2) A relay attack introducing a phase shift on the relayed HE-LTF symbols to spoof the distance.3) An attacker generating its own HE Ranging NDP instead of relaying from a legitimate peer.If the Secure HE-LTF generation produces a uniform distribution of phases then one would expect all of these attacks to reduce the correlation quality by varying degrees, and for the timing measurement to vary as follows:1) The phase on each subcarrier would be shifted towards that of the attacker's signal, with the average across all subcarriers being zero. Hence, I would not expect this to have a significant effect on the measured range.2) A cyclic shift of a significant proportion of the symbol time could be introduced. Given that even a 1 us shift would be equivalent to a 300 m reduction in the round trip range this would appear to be an effective attack.3) The generated symbols would have a random phase relationship to the expected symbol, so this would result in the measured timing varying by a significant proportion of the symbol duration. This would vary for each symbol measured.Is the receiver expected to do more than just find the earliest correlation peak, such as applying a threshold to the correlation magnitude or performing the correlation independently per sub-carrier and looking at the spread of timings? Something should be added in clause 27.3.21 HE Receive Procedure about this, even if it is just a note saying that implementations may choose to apply additional checks. | As it says in the comment. Need a description of the receiver processing that is expected to be performed (e.g. verifying that the channel estimate is similar for each HE-LTF). | RejectedThe commenter describes some of the attacks and challenges the security support of 11az protects from at both MAC and PHY level.These are fully described in the SFD document where a threat model was specified and the standard was develop according to.However the standard itself is limited to describing normative behavior of the interoperable part and the threat model is not part of which. Also, 11az already defined the IntegrityCheckError for PHY-RXEND.indication primitive and this error indicates “ that during the reception of the HE Ranging NDP PPDU or HE TB Ranging NDP PPDU, an integrity check was performed and failed”, which means in addition to estimate the first path, the receiver also should do intergrity check.   |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause  | Comment | Proposed Change | Resolution |
| 1055 | 156 | 28.3.17d | Clarify the guard interval term "zero-power GI" as compared to "conventional GI". Its not used in 11ax, 11ay or REVmd. It should be defined in clause 3.0. | As commented | Revised TGaz editor makes changes as specified in 11-19/1479r1 for CID 1055. |

*TGaz Editor: please insert the following row at the end of section 3.4 Abbreviations and acronyms on page 6 of 11az draft 1.0.*

**zero-power GI** guard interval with zero signal power

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause  | Comment | Proposed Change | Resolution |
| 2274 | 62 |  | "The TOD time-stamp represents the time, with respect to the ISTA's time base, at which the start of the preamble of the NDP in question appeared at the transmit antenna connector. The TOA time-stamp represents the time, with respect to the ISTA's time base, at which the start of preamble of the NDP in question arrived at the receive antenna connector." The reference point is the beginning of the preamble, however, the reference point is the beginning of the 1st HE-LTF per line 17 to line 21 on page 98. | Modify the spec text so that the reference point for the timestamp reporting is consistent. | RevisedTGaz editor makes changes as specified in 11-19/1479r1 for CID 2274 |

*TGaz Editor: please revise line 14-19 on page 70 of 11az draft 1.0 as below*

The ToA field contains a timestamp that represents the time, with respect to a time base, at which the start of the preamble of the corresponding NDP frame (#2274) arrived at the receive antenna connector. The corresponding NDP frame in an RSTA-2-ISTA LMR frame is an UL NDP, while in an ISTA-2-RSTA LMR frame it is a DL NDP. In both cases the corresponding NDP frame refers to a measurement exchange that included an NPD-A which carried the matching dialog token that is also included in this LMR.

*TGaz Editor: please revise line 17-21 on page 98 of 11az draft 1.0 as below*

The TOA field’s value contains a time stamp that represents the time, with respect to a time base, at which the start of the preamble of the corresponding NDP frame (#2274)arrived at the receive antenna connector. The TOD field’s value contains a timestamp that represents the time, with respect to the same time base, at which the start of the first HE-LTF of the associated NDP frame appeared at the transmit antenna connector.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause  | Comment | Proposed Change | Resolution |
| 1339 | 160 | 28.3.19a | Why zero GI is needed for PE. Also, how to generate a 4us PE with 1.6us GI? | as in the comment | RejectedIn the secured mode of ranging, circular convolution between the channel and LTF symbols becomes linear convolution, and the Packet Extension field with zero-power GI is necessary for the STA to calculate the linear convolution without intersymbol interference from PE.The generation of the PE with zero power GI is implementation specific, and one possible way is to first generate the 4us regular GI and then set the samples within 1.6us GI to 0.  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause  | Comment | Proposed Change | Resolution |
| 2363 | 151 | 28.3.19a | NUM\_STS[1] is not defined. This parameter should be defined as NUM\_STS for the first user. Also NUM\_STS parameter in TXVECTOR is defined as SU when FORMAT is HE\_SU. This is not accurate since for HE Ranging NDP which is HE\_SU format, it can carry HE-LTFs for multiple users. | Clarify the spec as suggested in the comment. | RejectedIn lines 29-33 on page 105 of 11az draft 1.0, we have the following definition “In the secure variant of the TB ranging measurement exchange, The NUM\_STS[*p*] is set to the same value as the DL N\_STS field in the STA Info field addressed to the corresponding STA *p* in the preceding Ranging NDP Announcement frame when the HE Ranging NPD PPDU is transmitted to more than one ISTAs.” And this has addressed the first part of the comment.In the last row of the table for TXVECTOR and RXVECTOR on page 148 of 11az draft1.0, we have the following definition “If NUM\_USERS is larger 1, NUM\_STS, LTF\_REP, and LTF\_SEQUENCE will be MU”, and this has addressed the second part of the comment.   |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause  | Comment | Proposed Change | Resolution |
| 1700 | 160 | 28.3.19a | Zero-power Guard intervals spaced by 7.2 or 8 us will lead to a flaky CCA signal in HT, VHT or HE receivers, which sample the channel every slot time, at an unspecified instant within that slot time. This will lead to unpredictable defer behavior. This isn't necesssarily a problem in the primary channel where the LSIG protects the packet, but does affect CCA in the secondary channel, as specified in section 11.16.9 of the 802.11 standard. | Delete "zero power GI" mode from Clause 28. To address concern of GI replay attack invent an alternate measures. | Rejected In section 11.16.9 of 802.11Revmd draft0.5, there are following description: “the STA may transmit a pending 40 MHz mask PPDUonly if the secondary channel has also been idle during the times the primary channel CCA is performed(defined in 10.24.2.4 (Obtaining an EDCA TXOP)) during an interval of a PIFS for the 5 GHz band andDIFS for the 2.4 GHz band immediately preceding the expiration of the backoff counter.”According to the above description, only when the legacy device detects idle medium for PIFS or DIFS time, the device can initiate a transmission, and since the zero GI in 11az secured NDP is only 0.8us or 1.6us, the legacy device shall be able to detect the secured NDP frame and defer accordingly.  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause  | Comment | Proposed Change | Resolution |
| 2501 | 152 | 28.3.19a | When the PHY detects the integrity check error, it shall report the error condition to the MAC. | Please add the following sentence at the end of 28.3.17a (HE Ranging NDP)."The PHY shall issue the error condition PHY-RXEND.indication(Integrity Check Error) primitive if the PHY detects the integrity check error." | Revised The “IntegrityCheckError” is used to indicate that during the reception of the HE Ranging NDP PPDU or HE TB Ranging NDP PPDU, an integrity check was performance and failed, and the invalid measurement field shall be set. In current 11az draft 1.0, when to issue this IntegrityCheckError is missing, and spec text is revised accordingly. TGaz editor makes changes as specified in 11-19/1479r1 for CID 2501. |
| 2500 | 153 | 28.3.17b | When the PHY detects the integrity check error, it shall report the error condition to the MAC. | "Please add the following sentence at the end of 28.3.17b (HE TB Ranging NDP).""The PHY shall issue the error condition PHY-RXEND.indication(Integrity Check Error) primitive if the PHY detects the integrity check error.""" | Revised The “IntegrityCheckError” is used to indicate that during the reception of the HE Ranging NDP PPDU or HE TB Ranging NDP PPDU, an integrity check was performance and failed, and the invalid measurement field shall be set. In current 11az draft 1.0, when to issue this IntegrityCheckError is missing, and spec text is revised accordingly. TGaz editor makes changes as specified in 11-19/1479r1 for CID 2500. |

*TGaz Editor: please change the last paragraph of section 11.22.6.4.3.4 TB Ranging Measurement Reporting Part on page 100 of 11az D1.0 as below:*

In the TB ranging, the PHY shall issue the PHY-RXEND.indication primitive with error condition IntegrityCheckError, if the PHY detects the integrity check error in the reception of the corresponding HE Ranging NDP or HE TB Ranging NDP. If the PHY of an RSTA issues a PHY-RXEND.indication primitive with error condition IntegrityCheckError, the RSTA shall set the Invalid Measurement field in the RSTA-to-ISTA LMR frame carrying the TOA measured from the UL NDP to 1. Similarly, if ISTA-to-RSTA LMR was negotiated between the ISTA and RSTA and the PHY of an ISTA issues a PHY-RXEND.indication
 primitive with error condition IntegrityCheckError, the ISTA shall set the Invalid Measurement field in the ISTA-to-
RSTA LMR carrying the TOA measured from the DL NDP to 1.(#2501, #2500)

*TGaz Editor: please change the last paragraph of section 11.22.6.4.4.3 Non-TB Ranging Measurement Reporting Part on page 104 of 11az D1.0 as below:*

In the Non-TB ranging, the PHY shall issue the PHY-RXEND.indication primitive with error condition IntegrityCheckError, if the PHY detects the integrity check error in the reception of the corresponding HE Ranging NDP or HE TB Ranging NDP. If the PHY of an RSTA issues a PHY-RXEND.indication primitive with error condition IntegrityCheckError, the RSTA shall set the Invalid Measurement field in the RSTA-to-ISTA LMR frame carrying the TOA measured from the UL NDP to 1. Correspondingly, if ISTA-to-RSTA LMR was negotiated between the ISTA and RSTA and the PHY of the ISTA issues a PHY-RXEND.indication primitive with error condition IntegrityCheckError, the ISTA shall set the Invalid Measurement field in the ISTA-to-RSTA LMR carrying the TOA measured from the DL NDP to 1.(#2501, #2500)