IEEE P802.11  
Wireless LANs

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | LB253 CR for CID 5189 and 5192 | | | | | | Date: 2021-06-01 | | | | | | Author(s): | | | | | | Name | Affiliation | Address | Phone | email | | Tianyu Wu | Apple Inc. |  |  | Tianyu@apple.com | | Anuj Batra | Apple Inc. |  |  |  | | Qi Wang | Apple Inc. |  |  |  | | Ali Raissinia | Qualcomm |  |  |  | | Steve Shellhammer | Qualcomm |  |  |  | | Bin Tian | Qualcomm |  |  |  | | Nehru Bhandaru | Broadcom |  |  |  | | Manas Deb | Broadcom |  |  |  | | Vinko Erceg | Broadcom |  |  |  | | Gadi Shor | Intel |  |  |  | | Robert Stacey | Intel |  |  |  | |

Abstract

This submission proposes resolutions for the following comments from comment collection on P802.11az D3.0:

5189, 5192

**Revision History:**

R0: Initial version.

# CID 5189, 5192

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page.Line** | **Comment** | **Proposed Change** | **Resolution** |
| 5189 | 11.21.6.3.3 | 128.09 | "The ISTA shall set the Max R2I Rep and Max I2R Rep subfields to a value greater than 0 if the Secure LTF Required subfield of the Ranging Parameters field is equal to 1." - this requirement is receiver implementation specific | Remove this statement, a receiver which requires/finds useful repeated LTF, will request it. | **Revised**  LTF repetition is important for improving the attack detection reliability for secure PHY. Making LTF repetition optional may lead to degredation of security level. The better resolution is to clarify the recommended receiver behavior to utilize the LTF repetition.  **Instruction to TGaz Editor:**  Make the changes as shown in https://mentor.ieee.org/802.11/dcn/21/11-21-0917-00-00az-lb253-CR-CID-5189-5192.docx |
| 5192 | 11.21.6.3.3 | 130.09 | "If the Secure LTF Required subfield of the Ranging Parameters field is equal to 1, the RSTA shall set the Max R2I Rep subfield to a value equal to the corresponding value in the IFTMR frame, and the RSTA shall set the Max I2R Rep subfield to a value greater than 0 and less than or equal to the corresponding value in IFTMR frame." - no reason for >0 repetitions in secure case | Change to : "If the Secure LTF Required subfield of the Ranging Parameters field is equal to 1, the RSTA shall set the Max R2I Rep subfield equal to the corresponding value in the IFTMR frame and the Max I2R Rep subfield to a value less than or equal to the corresponding the value in IFTMR frame." | **Revised**  LTF repetition is important for improving the attack detection reliability for secure PHY. Making LTF repetition optional may lead to degredation of security level. The better resolution is to clarify the recommended receiver behavior to utilize the LTF repetition.  **Instruction to TGaz Editor:**  Make the changes as shown in https://mentor.ieee.org/802.11/dcn/21/11-21-0917-00-00az-lb253-CR-CID-5189-5192.docx |

**Discussion**

LTF repetition >= 2 (Max R2I Rep/ Max I2R Rep >0) is important for secure LTF.

LTF repetition >=2 can improve reliability of detection for attacks. Attack detection based on a single repetition of LTFs can only use SIR degradations to detect for attacks, but with multiple repetitions of LTFs, additional and more reliable attack detection methods can be used, such as consistency check. In addition, each repetition of LTF will have different random sequences and phase rotations, making attacks more difficult and easier to detect at the receiver.

Another benefit of multiple LTF repetitions >=2 is diversity to combat unintentional beamforming. For secure LTF, no CSD are applied, hence there is always a potential of unintentional beamforming. However, with multiple LTF repetitions, each repetition will have its own per stream phase rotation which provides diversity against unintentional beamforming.

In the spec, we propose to add a note to clarify that receiver should use LTF repetitions for consistency check.

**Proposed Text Updates: CIDs 5189, 5192**

*Instruction to TGaz Editor: Insert the following text at D3.0 P225, after L30.*

**27.3.18a HE Ranging NDP**

…….

The total number of HE-LTF symbols is the product of the number of LTF repetitions LTF\_REP and *NHE-LTF*, the number of HE-LTF based on the number of space-time streams N\_STS, as defined in Table 21-13 (Number of VHT-LTFs required for different numbers of space-time streams). (#**2499**, #**4014**) For Secure HE-LTF trasnmissions, the number of LTF repetitions LTF\_REP shall be greater than 1.

Note: The intended receiver can use the LTF repetitions to check for consistency of the channel estimates across the repetitions. One metric that can be used for the consistency check is to take the mean-squared error between consecutive channel estimates and compare against a threshold relative to the measured noise power.

*Instruction to TGaz Editor: Insert the following text at D3.0 P227, after L22.*

27.3.18b HE TB Ranging NDP

…….

The repetitions of the HE-LTF symbols are repetition of the structure for HE-LTF fields. The randomized HE-LTF sequences are different for HE-LTF repetitions. (#**2357**) For Secure HE-LTF trasnmissions, the number of LTF repetitions LTF\_REP shall be greater than 1.

Note: The intended receiver can use the LTF repetitions to check for consistency of the channel estimates across the repetitions. One metric that can be used for the consistency check is to take the mean-squared error between consecutive channel estimates and compare against a threshold relative to the measured noise power.