IEEE P802.11Wireless LANs

|  |
| --- |
| Proposed Resolution for CID 7209 of 11az SAB1  |
| Date: 2022-05-08 |
| Author(s): |
| Name | Company | Address | Phone | email |
| Tianyu Wu | Apple Inc.  |  |  | tianyu@apple.com |
| Anuj Batra |  |  |  |
| Qi Wang |  |  |  |

Abstract

This submission proposes the resolution to 11az SAB1 CID-7209.

The page and line numbers refer to those in 11az Draft 4.1 [1].

**Introduction**

This submission proposes the resolutions to 11az SAB1 CID 7209.

The page and line numbers refer to those in 11az Draft 4.1 [1].

**Comments:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page/Line | Clause | Comment | Proposed change | Resolution |
| 7209 | 245/08 | 27.3.18a.4 | Define detection requirements for Secure HE-LTF. The PHY security level is determined by definition of secure LTF as well as detection requirement on secure LTF. To achieve a certain PHY security level, detection requirement need to be specified. | Add a detection requirement for Secure HE-LTF, for example first path SIR > Threshold1 dB, or Attack detection rate > Threshold2. | Revised. Agree in principle. TGaz editor: please incorporate the text changes in this document (22/0712r0) with tag #7209.11-22-0712-00-00az-CR-sab1-CID-7209-Secure-LTF-detection.docx |

**Proposed resolution**

***TGaz Editors: Please modify the text on page 238/line 32 of D4.1 as shown below: (#7209)***

**27.3.18a HE Ranging NDP and HE TB Ranging NDP**

When the TXVECTOR parameter SECURE\_LTF\_FLAG is set to 1, Secure HE-LTFs as defined in 27.3.18d (Construction of Secure HE-LTF), are used and the Packet Extension field will be partially replaced by a zero power GI in its first 1.6 μs, see Figure 27-46c (HE Ranging NDP format with Secure HE-LTFs). For the secure HE-LTF symbol or Packet Extension field with zero power GI, the time domain signal has zero power during the period of the GI. The total number of HE-LTF symbols is the product of the number of HE-LTF repetitions given in 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 transmissions, the number of HE-LTF repetitions given in LTF\_REP shall be greater than 1. (#**7347**)

The intended receiver of the Secure HE-LTFs can detect an attacker by various methods, including checking for the consistency of the channel estimates across HE-LTF repetitions, or by measuring a drop in the signal-to-interference ratio (SIR).

NOTE — The intended receiver can check for consistency of the channel estimates across the HE-LTF repetitions by calculating the mean-squared error between consecutive channel estimates and compare against a threshold relative to the measured noise power. (#**5189**, #**5192**) The intended receiver can also search for a drop in the SIR over a single (or multiple) HE-LTF repetitions. Additional details about the performance analysis for an SIR-based attack detection can be found in Annex AE.

Annex AE

(informative)

**SIR-based Attack Detection**

Assume that an attacker observes the Secure HE-LTF symbol for a duration of Tob, referred to as the observation period. The attacker can use these observations to generate an attack signal over the duration Tc, referred to as the computation period. Finally, the attacker will transmit the attack signal during the attack period, Ta, to create a false first path of arrival that has an earlier arrival time than the true first path of arrival.

Secure LTF OFDM Symbol

Observation Period

Computation Period

Attack Period

A side effect of creating the false first path of arrival is that the attacker will also generate interference at the intended receiver. If we assume that the attack signal has a correlation of with the true Secure HE-LTF signal and creates a false first path of arrival with a relative power level of FFP (dB), then the signal-to-interference (SIR) that is seen by the intended receiver will be:

*SIR*(*dB*) = + 10 log10()

When the attacker is not present, the SIR will be infinity, i.e., no interference. However, when an attacker is present, the SIR will drop and the value will depend on the relative power level of FFP, correlation, and attack period.

For example, if FFP = -10 dB, then the expected SIR levels for different values of and Ta are shown in the following figure:



From this figure, we see that as the correlation of the attack signal decreases or the attack duration decreases, the SIR will drop even further.

Therefore, the presence of an attacker can be detected by looking for drops in the SIR over a single, or multiple, HE-LTF repetitions. The exact details of the algorithm are left to implementor.

**References**

[1] IEEE P802.11az™/D4.1, Draft Standard for information technology – Telecommunications and information exchange between systems Local and metropolitan area networks – Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 4: Enhancements for positioning