IEEE P802.11
Wireless LANs

|  |
| --- |
| CR for Location |
| Date: 2019-08-14 |
| Author(s): |
| Name | Company | Address | Phone | Email |
| Girish Madpuwar | Broadcom | Electronic City, Bangalore India |  | Girish.madpuwar@broadcom.com  |
| Nehru Bhandaru | Broadcom | San JoseCA, USA |  | Nehru.bhandaru@broadcom.com |

**Abstract**

This submission proposes resolutions of comments received from LB240.

* CIDs: 1130, 1325, 1448, 1452, 1453, ~~1454, 1455, 1456,~~ 1459, 1460, 1461

The comments are based on TGaz Draft 1.0 and the proposed changes are relative to TGaz Draft 1.4

Revision 0: initial draft

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 1130 | 9.4.2.280 | 54 | The text "The Range Measurement SAC field is the same value as in the LTF Generation SAC subfield in the STA Info SAC field in the Ranging NDP Announcement frame that solicited the UL NDP and the DL NDP (see 11.22.6.4.6 (Secure Non-TB and -TB Ranging Measurement Exchange Protocol))" is not completely correct. | The STA Info SAC for TB Ranging is in the location trigger subvariant secure sounding frame and not in the NDPA. Edit the paragraph to indicate the TB case correctly. | Accepted: |

*Modify the following paragraphs of Clause 9.4.2.280 Secure LTF Parameters element Draft 1.2 Page 55*

The Measurement result SAC field is used to verify that range measurement results of the Location Measurement Report frame are calculated using the same Secure LTF counter between ISTA and RSTA. The Measurement result SAC field in Location Measurement Report for Secure non-TB Ranging is the same value as in the LTF Generation SAC subfield in the STA Info SAC field in the Ranging NDP Announcement frame that solicited the I2R NDP and the R2I NDP. The Range Measurement SAC field in Location Measurement Report for Secure TB Ranging is the same value as LTF Generation SAC field in Secure LTF Parameter element in a Ranging Secure Sounding Trigger frame. (see 11.22.6.4.6 (Secure Non-TB and -TB Ranging Measurement Exchange Protocol)). This field is reserved in the initial Fine Timing Measurement frame.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 1325 | 6.3.56.1 | 12 | In figure 16-7c, after the Trigger frame from MLME of the RSTA, there is no response to the the trigger frame from ISTA. | as in the comment | accepted  |

*Modify the following figures in Clause 6.3.56.1 General*



Figure 16-7b non-Trigger Based Sounding Exchange for Ranging

*Modify the following figures in Clause 6.3.56.1 General*



Figure 16-7c Trigger Based Sounding Exchange for Ranging

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 1448 | 9.4.2.26 | 36 | it says the secure variant is described in 11.22.6.4 but it actually isn't. | define the secure variant | Rejected: The comment corresponds to D0.6. Usage of SAC field in STA Info SAC Field is described in “11.22.6.4.6 Secure Non-TB and TB ranging Measurement Exchange” |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 1452 | 11.22.6.4.6.3 | 122 | Secure-LTF-bits will be generated differently by the RSTA and ISTA. | if each side generates a different key then name it apppropriately. If they are supposed to generate the same key then reconcile the computation | Rejected:The comment corresponds to D0.6. Secure-LTF-bits in a frame originating from RSTA are named as Secure-LTF-bits-DL and Secure-LTF-bits in a frame originating from ISTA are named as Secure-LTF-bits-R2I and Secure-LTF-bits-I2R |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 1453 |  |  | what is the length? | SAC is a fixed 16 octets, what's the length of Secure-LTF-bits? | Revised:more description added for KDF-Hash-Length function. Number of LTF bits to be generated is documented in Draft 1.2 in section 11.22.6.4.6.3  |

*Modify the following figures in Clause 11.22.6.4.6.3 Secure LTF Generation Information*

**11.22.6.4.6.3 Secure LTF Generation Information**

For a given secure measurement frame (e.g. NDP), the SAC and secret (pseudo-random) bits to protect all of the LTFs in the frame originating from the RSTA are derived as follows

 SAC || Secure-LTF-bits-R2I = KDF-Hash-Length(Secure-LTF-Key-Seed, “Secure LTF Expansion”, Secure-LTF-Counter)

When the derived SAC is equal to 0, the STA shall increment the Secure-LTF-Counter by 1 and derive the SAC until a nonzero SAC value is obtained.

Similarly, for a given secure measurement frame (e.g. NDP), the secret (pseudo-random) bits to protect all of the LTFs in the frame originating from the ISTA for a given SAC are derived as follows

Secure-LTF-bits-I2R = KDF-Hash-Length(Secure-LTF-Key-Seed, “Secure LTF Expansion”, SAC || Secure-LTF-Counter)

where KDF-Hash-Length is the key derivation function defined in 12.7.1.6.2 (Key derivation function

(KDF)) using the hash algorithm identified by the AKM suite selector (see Table 9-151 (AKM suite selectors)). Length indicates the length of the derived key in bits.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 1459 | 12.13.1 | 142.2 | How does PASN tunnel FILS shared key and SAE protocol data? Is there a reason that FILS public key is not similarly tunneled? | explain this tunneling better and if one kind of protocol cannot be tunneled explain why. | Accepted:Motion passed;This comment is with respect to D0.6This comment is already resolved in submission 11-19-0718 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 1460 | 12.13.3 | 109.6 | how does the "comeback cookie" work? | explain what this is for and how it works | Accepted:Motion passed:Section 12.13.9 of draft 1.2 describes comeback cookie.This comment is already resolved in submission 11-19-0718 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 1461 | 12.13.3 | 109.16 | how are ECC private keys generated? | randomness recommendations are needed | Rejected:Spec already has J.5 suggestions for random number generation |