IEEE P802.11
Wireless LANs

|  |
| --- |
| 802.11[802.11az PHY Spec Text for Adaptation of Secure LTF Sequence to Bandwidth/Antenna Change](relative to P802.11az/D1.0\_1) |
| Date: 2019-03-05 |
| Author(s): |
| Name | Company | Address | Phone | Email |
| Qinghua Li  | Intel Corporation | 3600 Juliette Ln, Santa Clara, CA 95054 |  | qinghua.li@intel.com |
| Feng Jiang | Intel Corporation  | 3600 Juliette Ln, Santa Clara, CA 95054 |  | feng1.jiang@intel.com |
| Jonathan Segev | Intel Corporation | 3600 Juliette Ln, Santa Clara, CA 95054 |  | jonathan.segev@intel.com |
| Ido Ouzieli | Intel Corporation |  |  |  |
| Shlomi Vituri | Intel Corporation |  |  |  |
| Elad Oren  | Intel Corporation |  |  |  |
| Gadi Shor | Intel Corporation |  |  |  |
| Robert Stacey | Intel Corporation |  |  |  |
| Yongho Seok | Mediatek |  |  |  |

**Discussion:**

This contribution is for the resolution of comment CID 1821 below.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Clause | Page | Comment Type | Comment | Proposed Change |
| 1821 | 11.22.6.3.4 | 91 | T | There is no definition of how the secured 4P+3 bits are used in the case of only partial BW, e.g. when 80MHz was negotiated but due to channel occupancy only 40MHz is used. | Clarify which part of the generated vector is used especially such that no timing constraint is created, i.e. that the LTF sequence can be generated prior to the TF or NDPA indicating the BW size. |

The suggested edits account for the following issues:

1. The measurement exchange does not include the generation process of the secure bit sequence, which is currently in the negotiation section. The generation process of the secure bit sequence should be in a section other than the negotiation section.
2. Terminology mix-up – there is no separation between DL and UL sequences. The two sequences share the same name Secure-LTF-bits, whereas the UL and DL generated bit sequences need to two different names for two different processes.
3. No clear definition on how the generated bits are used when a measurement instance uses a partial BW (secondary channel occupied) or a smaller number of space-time streams.

Solution:

1. Partition the existing text on Secure LTF to two parts:
	1. Have the current section “11.22.6.3.4 Secure LTF measurement setup” deal with the session setup only (i.e. indication of the negotiation and Secure LTF Key Seed derivation.
	2. Move the text dealing with generation of Secure-LTF-Bits to the “Secure TB and NTB Measurement Exchange Protocol” section where the parameters used (SAC, Secure LTF counter) are described. This text is shared between the TB and NTB.
2. Describe under section 28 what happens if not the maximum allocated BW, UL and DL *N*STS and such are used – which part of the generated bit sequence is used.

Other: DL and UL bit sequences are using the same name – this is a typo so the notations of UL and DL are added to the corresponding sequence names.

**[TGaz Editor: modify section 11.22.6.3.4 as shown below]**

**11.22.6.3.4 Secure LTF measurement setup**

…

When management frame protection is negotiated for TB and non-TB ranging negotiation, a STA shall use the Protected Dual of Public Action frames for an initial Fine Timing Measurement Request, an initial Fine Timing Measurement, and a Location Measurement Report.

An ISTA in which dot11SecureLTFImplemented is false ignores a Secure LTF Parameters if an initial Fine Timing Measurement frame and a Location Measurement Report frame carries the Secure LTF Parameters.

When dot11SecureLTFImplemented is true, prior to generating new LTF Sequence generation information for a given PTKSA, the RSTA initializes a monotonically increasing 48-bit counter Secure-LTF-Counter to 0. The RSTA also derives a Secure-LTF-Key-Seed as follows

 Secure-LTF-Key-Seed = HMAC-Hash(HLTK, “Secure LTF key seed”)

Where HLTK is derived as part of PTKSA establishment, Hash is the hash determined by the AKM and used to derive the PTK.

Similarly, when dot11SecureLTFImplemented is true, an ISTA also derives the same Secure-LTF-Key-Seed prior to initiating a secure FTM negotiation.

For each secure FTM negotiation, prior to transmission of IFTM, and for each measurement within an FTM session, an RSTA shall increment the Secure-LTF-Counter by 1. The Secure-LTF-Counter is included as part of LTF sequence generation information conveyed to the ISTA. An ISTA determines the Secure-LTF-Counter to use for a measurement using the sequence generation information and SAC received from the RSTA in a protected IFTM or LMR frame. The Secure-LTF-Counter shall be reset when a new HLTK is derived as part of a new PTK derivation and it shall continue, and not be reset, for each secure FTM negotiation using a given HLTK.

**[Instructions for the TGaz Editor: move following text from “Section 11.22.6.3.4 Secure LTF measurement setup” to a new “Section 11.22.6.4.6.3 LTF Sequence 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-DL = 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-UL = KDF-Hash-Length(Secure-LTF-Key-Seed, “Secure LTF Expansion”, SAC || Secure-LTF-Counter)

Where KDF and Hash are the key derivation function and hash function determined by the AKM used to derive the PTKSA, and Length is the length in bits required for the SAC concatenated with the LTF sequence generation input.

Integer to octet string conversion (MSB first) specified in 12.4.7.2.2 shall be used to encode the Secure-LTF-Counter input to the KDF as well as in the transmitted LTF sequence information. It shall be padded with leading (MSB) 0s to be exactly 6 octets. The SAC transmitted and used in deriving Secure-LTF-bits shall also be of exactly 2 octets in length.

NOTE—A 6 octet sequence counter is sufficient because a unicast protected management frame that uses a 6 octet packet number is used to convey the LTF sequence information that carries the counter.

With the preceding construction, an attacker not knowing Secure-LTF-Key-Seed, would not be able to predict the SAC that would be used for given measurement.

For each measurement, the maximal numbers of bits in Secure-LTF-bits-DL and Secure-LTF-bits-UL shall be derived by Equations (11-yy) and (11-zz), respectively.

 Maximum Length of Secure-LTF-bits-DL , (11-yy)

 Maximum Length of Secure-LTF-bits-UL , (11-zz)

where

* is a bandwidth dependent parameter based on the assigned, maximum bandwidth for this session (refer to 28.3.17c). shall be 7, 8, 9, and 10 for assigned, maximum bandwidths 20, 40, 80, and 160/80+80 MHz, respectively (refer to Table 9-281 Format and Bandwidth field);
* is the assigned, maximum of number of secure LTF symbols per repetition within the DL Ranging NDP (refer to Table 21-13 Number of VHT-LTFs required for different numbers of space-time streams);
* is the assigned, maximum number of secure LTF symbols per repetition within the UL Ranging NDP (refer to Table 21-13 Number of VHT-LTFs required for different numbers of space-time streams);
* is the assigned number of DL repetitions equal to the value set in LTF\_REP within the TXVECTOR and the RXVECTOR for the downlink;
* is the assigned number of UL repetitions equal to the value set in LTF\_REP within the TXVECTOR and the RXVECTOR for the uplink.

Secure LTF measurement may require variable subsets of Secure-LTF-bits-DL and Secure-LTF-bits-UL based on the parameters for each ranging measurement instance (i.e. allocated bandwidth, negotiated repetition, allocated UL and allocated DL ), refer to Section 28.3.17d.

Note that in a DL NDP frame used for range measurement, LTFs assigned to each of the recipient STAs would use key material derived from their corresponding Secure-LTF-bits.

Secure-LTF-Counter shall be maintained for the lifetime of a PTKSA used for Secure LTF measurements. It shall not be reset between measurements and shall not be reset for multiple FTM negotiations using the same PTKSA. The Secure-LTF-Counter value used for each measurement using the HLTK derived for a given PTKSA shall be unique.

**[Instructions for the TGaz Editor: modify Section 28.3.17c Generation of Randomized LTF Sequence as follows:]**

**28.3.17c Generation of Randomized LTF Sequence**

When Secure HE-LTFs are used the regular HE-LTF sequence shall be replaced by a randomized LTF sequence. Using the TXVECTOR and RXVECTOR, MAC shall provide the PHY with the Secure-LTF-bits-UL, the Secure-LTF-bits-DL, and their respective parameters for the assigned and per-instance bandwidths, the numbers of space-time streams, and the number of repetitions. Based on these parameters, the PHY shall extract bits for each secure LTF symbol from the Secure-LTF-bits-UL or the Secure- LTF-bits-DL for UL or DL as shown in Procedure (28-oo) and Procedure (28-pp), respectively and as illustrated in Figure 28-52ga.

Procedure (28-oo)

1. Divide bit stream Secure-LTF-bits-DL into parameter segments each of bits long.
2. Further divide each segment from a) into sub-segments each of bits long.
3. Subdivide each sub-segment resulting from b) into bits used for CSD generation and bits used for 8PSK sequence generation.

Procedure (28-pp)

1. Divide bit stream Secure-LTF-bits-UL into parameter segments each of bits long.
2. Further divide each of segments from a) into sub-segments each of bits long.
3. Subdivide each sub-segment resulting from b) into bits used for CSD generation and bits used for 8PSK sequence generation.

 Figure 28-52-ga - Partitioning of randomized UL and DL bit streams into segments for secure LTF symbol generation, where and for the downlink and uplink, respectively;and for the downlink and uplink, respectively.

Each measurement instance may use a bandwidth and an HE-LTF field size, , smaller than or equal to the assigned bandwidth and the assigned HE-LTF field size, or . For the adaptation to a different bandwidth or a different HE-LTF field size, subsets of the bits shall be extracted from the partitions resulting from Procedure (28-oo) and Procedure (28-pp). The bit extraction procedures are given by Procedure (28-qq) and Procedure (28-rr) for the downlink and uplink, respectively, and are illustrated by Figure 28-52gb. The bits shall have the same order as in the KDF-Hash function output, which is described in Section 11.22.6.4.6.3 Secure LTF Generation Information.

Procedure (28-qq)

1. For the -th secure HE-LTF field, take bits from the -th bit long segment in Secure-LTF-bits-DL resulting from Procedure (28-oo) for , where is the number of repetitions for the per-instance measurement.
2. For the -th secure LTF symbol within the -th repetition, take the -th bit long sub-segment within the -th bit long segment resulting from Procedure (28-oo) for and , and discard the remaining sub-segments, where is the number of secure LTF symbols per secure HE-LTF field for the per-instance measurement.
3. For the -th secure LTF symbol within the -th repetition, take the first and the first bits from the CSD bits and 8PSK bits in the corresponding sub-segment resulting from b), respectively as illustrated by Figure 28-52-gb, where shall be 7, 8, 9, and 10 for the per-instance bandwidths 20, 40, 80, and 160/80+80 MHz, respectively.

Procedure (28-rr)

1. For the -th secure HE-LTF field, take bits from the -th bit long segment in Secure-LTF-bits-DL resulting from Procedure (28-pp) for , where is the number of repetitions for the per-instance measurement.
2. For the -th secure LTF symbol within the -th repetition, take the -th bit long sub-segment within the -th bit long segment resulting from Procedure (28-pp) for and , and discard the remaining sub-segments, where is the number of secure LTF symbols per secure HE-LTF field for the per-instance measurement.
3. For the -th secure LTF symbol within the -th repetition, take the first and the first bits from the CSD bits and 8PSK bits in the corresponding sub-segment resulting from b), respectively as illustrated by Figure 28-52-gb, where shall be 7, 8, 9, and 10 for the per-instance bandwidths 20, 40, 80, and 160/80+80 MHz, respectively.



Figure 28-52-gb - Extraction of randomized bits from DL- and UL-Secure-LTF-bits, where and for the downlink and uplink, respectively;and for the downlink and uplink, respectively.

For each Secure LTF symbol denote the corresponding 4*P*+3 bits resulting from Procedure (28-qq) and Procedure (28-rr) by for .

The LTF symbol generation process is shown in Figure 28-52g (Generation of Randomized LTF Sequence).

 

**Figure 28-52g - Generation of Randomized LTF Sequence**

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

 (28-rr)

where is 50, 25, 12.5, and 6.25 ns for 20, 40, 80, and 160/80+80 MHz transmissions, respectively; the bits for are the first bits of the input bits. A sequence of 8PSK symbols are generated by iterations. In the -th iteration, two sequences and are generated by concatenating two sequences and that were generated in the (-th iteration as

 and (28-ss)

, for (28-tt)

where denotes the concatenation of two sequences and ; denotes the multiplications of a scalar with each element of sequence ; the initial sequences and are two 8PSK symbols and are given by

 (28-uu)

 (28-vv)

where is the -th bit of the input bits. The phase rotation scalar in Equation (28-tt) is given by 3 consecutive input bits as

, for (28-ww)

where is the -th bit of the input bits.

The 8PSK sequences generated by Equations (28-ss) – (28-ww) for the assigned bandwidth shall include the 8PSK sequence for the per-instance bandwidths as its respective first portions as illustrated in Figure 28-52-gc. For example, the 8PSK sequence for an assigned 80 MHz measurement shall include the 8PSK sequence for the per-instance 40 MHz measurement as the first half and the 8PSK sequence for the per-instance 20 MHz measurement as the first quarter.



**Figure 28-52-gc – Illustration of the nested structure of the 8PSK sequences used by the assigned bandwidth and various per-instance bandwidths, respectively.**