**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **Further HRP Comment Resolutions Vol2** |
| Date Submitted | [16 July, 2019] |
| Source | Frank Leong (NXP Semiconductors)  Brima Ibrahim (NXP Semiconductors)  Benjamin A. Rolfe (Blind Creek Associates / NXP / UWB Alliance) |
| Re: | [If this is a proposed revision, cite the original document.]  [If this is a response to a Call for Contributions, cite the name and date of the Call for Contributions to which this document responds, as well as the relevant item number in the Call for Contributions.]  [Note: Contributions that are not responsive to this section of the template, and contributions which do not address the topic under which they are submitted, may be refused or consigned to the “General Contributions” area.] |
| Abstract | [Further 802.15.4z HRP UWB comment resolutions] |
| Purpose | [Resolve 802.15.4z HRP UWB comments] |
| Notice | This document has been prepared to assist the IEEE P802.15. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. |
| Release | The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15. |

**This document provides resolutions to comments i-0271, i-0527, i-0908, i-1545, i-2243, i-1163, i-1800, i-2863, i-1169, i-1806, and i-2233.**

**The following resolution applies to i-0271.**

***Add the following new rows into Table 7-7:***

**Table AD1 — Element IDs for Header IEs**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Element ID** | **Name** | **Enhanced Beacon** | **Enhanced ACK** | **Data** | **Multipurpose** | **MAC command** | **Format subclause** | **Use description** | **Used by** | **Created by** |
| **<ANA>** | **Ranging STS Key and IV IE** |  |  | **X** |  |  | **7.4.2.19** | **6.9.7.8** | **UL** | **UL** |

***Add 7.4.2.19 as follows:***

**7.4.2.19 Ranging STS Key and IV IE**

The Ranging STS Key and IV IE (RSKI IE) may be used to convey and align the seed, (i.e., key and data IV), used for STS generation. The content field of the RSKI IE shall be formatted as shown in Figure AD2.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Bits: 4 | 1 | 2 | 1 | Octets: 4/8/12/16 | 0/16 | 0/4/8/16 |
| IVC | SKP | CSP | CP | STS IV Counter | STS Key | Checksum |

**Figure AD2 - Ranging STS Key IE Content field format**

The IVC field indicates the content of the STS IV Counter field as follows: if the value of i-th bit in IVC is 1, updated bits [32(i-1):32i-1] of the IV are included, otherwise they are not.

The SKP field indicates the presence of the STS Key field as follows: an SKP field value of 0 means that the STS Key field is not present, (is zero octets), while an SKP field value of 1 means that the 16-octet STS Key field is present.

The CSP field indicates the presence of the Checksum field as per Table AD3.

The CP field is used when the RSKI IE is only conveying the 4-octet Counter portion of the IV, where a CP field value of 1 means the counter value applies to the current packet. A CP field value of 0 means that the RSKI IE applies to a future packet exchange. When unused, the CP field is set to 0.

The STS IV Counter field contains a string intended to set full or portion of the IV. The size of this field equals the number of ones in the IVC field multiplied by four. The string is formed by concatenation of multiple 4-octet strings, each of which is used to update the corresponding portion of IV indicated by IVC. For example, if IVC field value is “1001”, size of STS IV Counter field is 8 octets, where first 4-octet is used to update bits [0:31] of IV, and later 4-octet is used to update bits [96:127] of IV.

The STS Key field if present, as determined by the SKP field, contains a 16-octet string intended to initialize the STS key.

The Checksum field if present, as determined by the CSP field, contains a code intended to allowing the next higher layer to validate the supplied STS Key and STS IV Counter fields. The presence and length of the Checksum field is determined by the CSP field as per Table AD3.

The STS Key, STS IV Counter and Integrity Code fields of the RSKI IE are determined and consumed by the higher layers. The higher layers are responsible for validating these as necessary and programming the *phyHrpUwbStsKey*, *phyHrpUwbStsVUpper96* and *phyHrpUwbStsVCounter* PIB attributes accordingly.

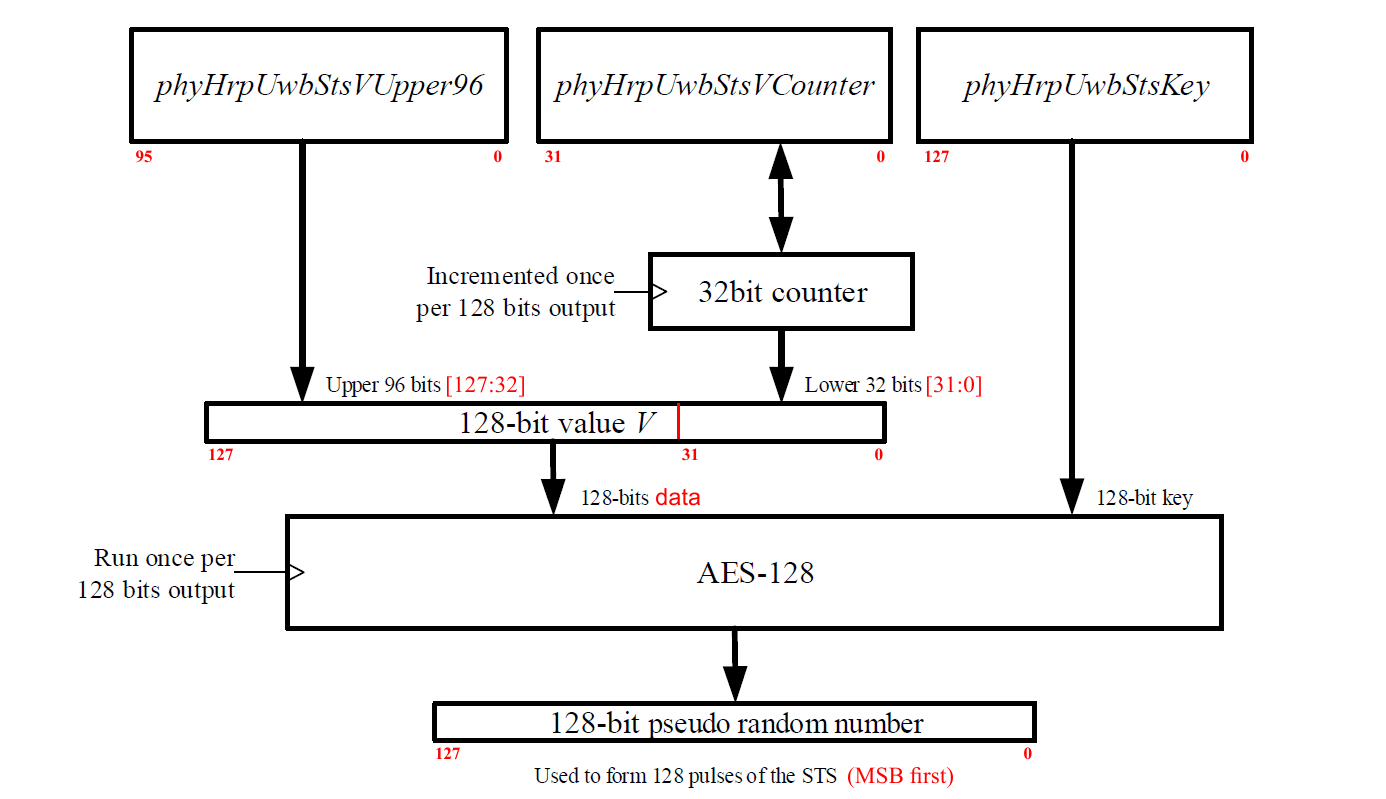
It is assumed that the RSKI IE is sent (broadcast) in plaintext, but the higher layers can include encryption as part of the mapping onto the associated PIBs.

**Table AD3 — Values of the CSP field in the RSKI IE**

|  |  |
| --- | --- |
| **CSP field value** | **Meaning** |
| 0 | The Checksum field is not present in the RSKI IE. |
| 1 | A 4-octet Checksum field is present in the RSKI IE. |
| 2 | An 8-octet Checksum field is present in the RSKI IE. |
| 3 | A 16-octet Checksum field is present in the RSKI IE. |

**The following resolution applies to i-0527.**

***Modify Figure 76 on Page 102 as follows:***



**Figure 76 – DRBG for STS**

***Add Annex as follows:***

### Annex XX

### XX.1 Test vectors for STS generation

This example illustrates the first two blocks generated by the DRBG described in 16.2.8 using following initialization:

key = 14 14 86 74 D1 D3 36 AA F8 60 50 A8 14 EB 22 0F

data = 36 2E EB 34 C4 4F A8 FB D3 7E C3 CA 1F 9A 3D E4

Here, key = *phyHrpUwbStsKey*, and data = *phyHrpUwbStsVUpper96* || *phyHrpUwbStsVCounter*. The associated value of the RSKI IE (without additional Checksum, so IVC set to 3, SKP set to 1, CSP set to 0, and CP set to 0) is F8 36 2E EB 34 C4 4F A8 FB D3 7E C3 CA 1F 9A 3D E4 14 14 86 74 D1 D3 36 AA F8 60 50 A8 14 EB 22 0F and the associated value of *phyHrpUwbStsVCounter* is 1F 9A 3D E4.

DRBG Blocks:

B(0) = 7A A6 F6 3E F9 17 AE 47 11 5E B6 FE 3B 5A 57 91

B(1) = 41 DA 0C 75 03 56 63 57 EB F3 8B 2C 12 BB 3E 92

C(0:255) = 0111101010100110111101100011111011111001000101111010111001000111  
0001000101011110101101101111111000111011010110100101011110010001  
0100000111011010000011000111010100000011010101100110001101010111  
1110101111110011100010110010110000010010101110110011111010010010

After transmission of 4096 STS pulses (a ~64 µs long BPRF STS or a ~32 µs long HPRF STS), the counter will have updated 16 times, resulting in a *phyHrpUwbStsVCounter* value of 1F 9A 3D F4. The associated value of data = *phyHrpUwbStsVUpper96* || *phyHrpUwbStsVCounter* is 36 2E EB 34 C4 4F A8 FB D3 7E C3 CA 1F 9A 3D F4.

### XX.2 Resulting STS modulation

This example illustrates how bits C(0:255) in XX.1 are mapped to BPSK modulation polarities of the first 256 pulses of the STS, as described in 16.2.8. Symbols A(i) are then spread by δL = 8 chips (BPRF) or δL = 4 chips (HPRF).

A(0:255) =  
+----+-+-+-++--+----+--+++-----+-----++-+++-+----+-+---++-+++---  
+++-+++-+-+----+-+--+--+-------+++---+--+-+--+-++-+-+----++-+++-  
+-+++++---+--+-+++++--+++---+-+-++++++--+-+-+--++--+++--+-+-+---  
---+-+------++---+++-+--++-+--+++++-++-+-+---+--++-----+-++-++-+

**The following resolution applies to i-0908, i-1545, i-2243.**

**Resolution detail:**

The procedure for DS-TWR with SP3 packets is very similar to SS-TWR with SP3 packets. In both cases, the participants in the ranging exchange can prepare for SP3 packet transmission/reception by means of the MLME-STS.request primitive. As, according to the schemes shown in Figure 30 and Figure 31 respectively, SS-TWR requires *i+1* SP3 packets for *i* responders, and DS-TWR requires *i+2* SP3 packets for *i* responders, SS-TWR requires one less (SP3) packet to be transmitted/received.

***In 6.9.8.8.1 on Page 38, add the following text after “After the RCM, the SP3 ranging starts.” (Line 11) as follows:***

The next higher layer is responsible for properly configuring the operation at both ends, which involves use of the MLME-STS.request primitive parameters TxStsPacketStructure and RxStsPacketStructure to set *phyHrpUwbStsPacketConfiguration* = 3 (i.e., SP3 packet format), as well as setting the PIB attributes *phyHrpUwbStsKey*, *phyHrpUwbStsVCounter* and *phyHrpUwbStsVUpper96* to the correct values.

***In 6.9.8.8.2 on Page 39, change text on Line 10 as follows:***

Change “The main difference is that there is a final SP3 packet in the ranging phase from the initiator.” to “The main difference is that there is a final SP3 packet in the ranging phase from the initiator. Configuration of all SP3 transmission/reception (including the additional SP3 packet) is performed by the same method as for SS-TWR with SP3 packets.”.

**The following resolution applies to i-1163, i-1800, i-2863.**

**Resolution detail:**

The higher layers are responsible for resetting the ranging counter. It is reasonable to assume that the ranging counter is reset before or at the start of each ranging exchange, and that, in case of a previous ranging exchange, the ranging counter is reset after the previous ranging exchange has been completed. However, as IEEE 802.15.4 does not specify higher layer behavior, this is outside the scope of the standard. Note that the MAC is not aware of the start and end of a ranging exchange (only the higher layers are aware), so the MAC should not be responsible for resetting the ranging counter. It is up to the implementer to ensure that the time at which the ranging counter is reset is in agreement with other timings within the ranging exchange(s). The ranging counter predates 4z and its behavior should not be modified by the amendment.

**The following resolution applies to i-1169, i-1806, i-2233.**

**Resolution detail:**

The implementer needs to ensure that the higher layer timings are in accordance with setting/unsetting of SP3 packet use by the MAC. The setting/unsetting of SP3 operation in the receiver is conceptually no different than switching between preamble codes, data rates, or RF channels.