**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | CID 1287 DRBG for RIFs | |
| Date Submitted | 30 January 2025 | |
| Source | Billy Verso (Qorvo), | billy.verso at qorvo.com |
| Re: | IEEE P802.15.4ab | |
| Abstract | Comment Resolutions for selected comments on the LB207 / P802.15.4ab D01. | |
| Purpose | This document provides text changes intended to be part of the final IEEE Std 802.15.4ab (amendment to IEEE Std 802.15.4), as part of resolving selected comments from the consolidated spreadsheet (doc 15-24-0371) that have been assigned to the author to resolve. | |
| Notice | This document does not represent the agreed views of the IEEE 802.15 Working Group or IEEE 802.15.4ab Task Group. It represents only the views of the participants listed in the “Source(s)” field above. 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. | |
| Patent Policy | The contributor is familiar with the IEEE-SA Patent Policy and Procedures.  <https://standards.ieee.org/about/sasb/patcom/materials/> | |

|  |
| --- |
| **CIDs addressed here:** |

[1 Comment Index # 1287 2](#_Toc178262607)

# Comment Index # 1287

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Index** | **page** | **clause** | **line** | **Comment** | **Proposed Change** |
| 1287 (Billy) | 194 | 16.2.11.3 | 7 | It would make most sense to have a single AES PRNG for STS and have the same SEED (Key and IV) set up at both ends of the link. Then, since RIF transmissions from initiator and responder are interleaved, the PRNG output should be consumed sequentially at both ends of the link, alternatively generating the sequence for transmission, and the sequence for cross-correlation in the receiver. | I will prepare a submission to cover this. |

**Discussion/Introduction:**

The initial versions of this submission (r0 and r1) proposed a scheme where the DRBG output was consumed alternatively for transmit and receive RIF in the case of the interleaved MMS UWB packet exchange. Feedback from TG4ab was that an independent DRBG configuration for TX and RX is the preferred approach.

The changes proposed below capture what is necessary to specify this in the 4ab text.

The proposed resolution to the comment is then: **Revised**

With the changes to the draft being as specified below:

***Changes with respect to P802.15.4ab D01:***

***Modify clause 16.2.11.3, as shown below:***

**16.2.11.3 Ranging integrity fragments (RIF)**

Each RIF shall consist of a sequence of active STS pulses generated as described in 16.2.9, where the DRBG is called iteratively to generate a non-repeating sequence across all the RIF fragments of the packet, ~~and the~~ with *phyHrpUwbRifTxKey*, *phyHrpUwbRifTxVCounter* and *phyHrpUwbRifTxVUpper96* configuring the DRBG generating the transmitted RIF fragments, and *phyHrpUwbRifRxKey*, *phyHrpUwbRifRxVCounter* and *phyHrpUwbRifRxVUpper96* configuring the DRBG generating the sequence to validate received RIF fragments. The pulses are spread by the spreading factor L=4. Each RIF in the packet shall have the same length from one of the following permitted lengths: 32, 64, 128 or 256, in units of 512 chips.

***And insert these new PIB attributes into Table 12-8 as follows:***

***Note these new attributes are modeled upon the phyHrpUwbStsSeed, phyHrpUwbStsVCounter and phyHrpUwbStsVUpper96 attributes specified in IEEE Std 802.15.4-2024 for STS generation.***

***Insert the following new rows into Table 12-8 “HRP UWB related PIB attributes:***

| **Attribute** | **Type** | **Range** | **Description** |
| --- | --- | --- | --- |
| *phyHrpUwbRifTxKey* | 16 octets | — | This attribute specifies the seed used in the DRBG for generating the transmitted RIF fragments, as specified in 16.2.11.3. When the DRBG is running, write access to this attribute shall be delayed until after packet transmission/reception. |
| *phyHrpUwbRifTxVCounter* | 4 octets | — | This attribute provides read and write access to the 32-bit counter that supplies the least significant 32 bits of the 128-bit value V used in the DRBG for generating the transmitted RIF fragments, as specified in 16.2.11.3. During packet transmission or reception, this attribute shall not be writable, and a read shall provide the initial state of the attribute at the beginning of packet transmission/reception. |
| *phyHrpUwbRifTxVUpper96* | 12 octets | — | This attribute supplies the most significant 96 bits of the 128-bit value V used in the DRBG for generating the transmitted RIF fragments, as specified in 16.2.11.3. This attribute shall not be modified during packet transmission or reception. |
| *phyHrpUwbRifRxKey* | 16 octets | — | This attribute specifies the seed used in the DRBG for generating the sequence to validate received RIF fragments, as specified in 16.2.11.3. When the DRBG is running, write access to this attribute shall be delayed until after packet transmission/reception. |
| *phyHrpUwbRifRxVCounter* | 4 octets | — | This attribute provides read and write access to the 32-bit counter that supplies the least significant 32 bits of the 128-bit value V used in the DRBG for generating the sequence to validate received RIF fragments, as specified in 16.2.11.3. During packet transmission or reception, this attribute shall not be writable, and a read shall provide the initial state of the attribute at the beginning of packet transmission/reception. |
| *phyHrpUwbRifRxVUpper96* | 12 octets | — | This attribute supplies the most significant 96 bits of the 128-bit value V used in the DRBG for generating the sequence to validate received RIF fragments, as specified in 16.2.11.3. This attribute shall not be modified during packet transmission or reception. |

***<END >***