**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 | 15 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:**

In IEEE 802.15.4z the STS generation covers the whole packet, i.e., runs through all segments in the STS with each new 128 bits generated by running a DRBG iteration and incrementing the counter value so that all segments are unique. It makes sense to also do this in the RIF fragments of the 4ab packet. 4z is also specified in such a way the AES block is shared by TX and RX, i.e., at different times it is generating the sequence for the pattern of pulses in the transmitted STS, and the expected pattern for cross-­correlation/validation in the receiver with the received sequence. This should also be done in 4ab, but current RIF clause doesn’t clearly specify it.



The comment seeks to make it clear that a single AES DRBG can be used to generate the sequence for RIF TX and RX, without any per fragment reprogramming during the interleaved packet transmission and reception; and, allow the same configuration of the seed (key and IV) in both initiator and responder(s) be set before the MMS ranging packet exchange is initiated.

For the interleaved UWB MMS packet TX/RX, this means arranging for the AES output to advance sequentially as it is alternately (a) consumed by the transmitter to form the “symbols” of a TX RIF fragment, and (b) consumed by the receiver to form the “symbols” used to cross correlate with the received samples of an expected RX RIF fragment. The initiator side transmitting first does (a) then (b) in each millisecond, while the responder receiving first does (b) then (a) in the same millisecond. The AES counter then stays synchronised at both sides across the whole packet.



***To support this we should….***

***Modify clause 16.2.11.3, inserting the new paragraph 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 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.

In the case of interleaved RIF fragment transmissions and receptions, the non-repeating DRBG output shall be consumed alternately by the transmitter and receiver in turn as required, i.e., for each fragment reception the DRBG is called iteratively with its output applied to generating the reference sequence for cross correlation with the received fragment, and for each fragment transmission the DRBG is called iteratively and its output applied to generating the transmitted RIF fragment.

The non-interleaved case is trivially the same as 4z, either the AES DRBG is being used by the transmitter iterating through all TX fragments, or by the receiver generating the pattern for cross correlation and iterating through all RX fragments.

There is a more complicated case to consider, which is the optional “time efficient” one-to-many case, where two responders are transmitting interleaved fragments. Here the initiator transmits its fragments and receives/processes the fragments from all responders, while each responder only wants to receive the initiator’s fragment and transmit its own response fragments but not receive/process the fragments from the other responder.

To have the same AES DRBG configuration (seed, counter) running for the interleaved responses, each of the responders needs to “know” that it is one of a pair, so that it can adjust its AES count appropriately. In each millisecond then, the initiator sends its fragment and receives fragments from both responders; while, each responder receives the initiator’s fragment and sends its own fragment, Responder-1 sending at 400 RSTU and Responder-2 sending at 800 RSTU.

To keep the RIF (STS) AES DRBG counter (*phyHrpUwbStsVCounter*) values in each node synchronised, each responder must advance its counter to take account of the other responder’s transmissions. The approach proposed here is to specify two additional parameters: *StsCountAdvanceAfterTx*, and *StsCountAdvanceAfterRx*, to specify the number of AES iteration counts to advance after a fragment is transmitted or received. Each device (next higher layer) sets these appropriately depending on whether they are the initiator or 1st or 2nd responder. This is quite flexible.

To visualise how this works, the graphic below shows a couple of milliseconds RIF TX and RX (coloured boxes) for three nodes participating in a “time efficient” MMS exchange. As each TX fragment is generated in the *StsVCounter* advances by *N*, a value that depends on the fragment length, (e.g., for fragment length 32, the RIF is 32 x 512 chips, or 4096 pulses, which requires 32 iterations of the DRBG to generate, so *N* is 32). Similarly, for each fragment RX the *StsVCounter* advances by *N* as the device generates the reference sequence for its cross‑correlation/validation.



Considering Responder‑1, it firstly generates the sequence for reception of the initiator’s RIF fragment advancing *StsVCounter* by N, and does no extra update because *StsCntAdvAfterRx*= 0; then its RIF transmission advances *StsVCounter* by N and then because *StsCntAdvAfterTx*= N, it further increments the *StsVCounter* by N adjusting for the counter advance resulting from Responder-2’s fragment transmission that is received by the initiator. Similarly, the values of *StsCntAdvAfterRx*= N and *StsCntAdvAfterTx = 0* in Responder-2 cause its *StsVCounter* to be correctly adjusted to account Responder‑1’s RIF fragment TX.

A further issue not addressed here is whether “*Time efficient*” receiving of two interleaved responses (ref 10.38.8.3)needs two receivers. One could argue that treating it so is a neat way of handling all the parameters than need to be doubled-up. This would certainly be the best way to incorporate the multiple receiver instances required to handle those cases with multiple overlapping transmissions per slot (ref 10.38.8.3). This is an architectural question we can leave to another day, but either way, the mechanism proposed above will work, i.e., we can easily treat the initiator as two devices, one doing an interleaved TX+RX and one doing just RX with an appropriate *StsCntAdvAfterRx* adjusting its *StsVCounter* appropriately for the next reception.

The changes to the draft are on the following pages:

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

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

| **Attribute** | **Type** | **Range** | **Description** |
| --- | --- | --- | --- |
| *phyHrpUwbStsCntAdvAfterRx* | Unsigned Integer | 0x00000000–0xffffffff | For UWB MMS packets, this attribute specifies a number by which to advance (i.e. add to) the running *phyHrpUwbStsVCounter* after each RIF fragment reception. This attribute shall not be modified during packet transmission or reception. |
| *phyHrpUwbStsCntAdvAfterTx* | Unsigned Integer | 0x00000000–0xffffffff | For UWB MMS packets, this attribute specifies a number by which to advance (i.e. add to) the running *phyHrpUwbStsVCounter* after each RIF fragment transmission. This attribute shall not be modified during packet transmission or reception. |

***Modify clause 16.2.11.3, inserting the two new paragraphs 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 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.

In the case of interleaved RIF fragment transmissions and receptions, the non-repeating DRBG output shall be consumed alternately by the transmitter and receiver in turn as required, i.e., for each fragment reception the DRBG is called iteratively with its output applied to generating the reference sequence for cross correlation with the received fragment, and for each fragment transmission the DRBG is called iteratively and its output applied to generating the transmitted RIF fragment.

To allow for various interleaving scenarios, with shared STS seed information among participants, the *phyHrpUwbStsVCounter* is incremented by *phyHrpUwbStsCntAdvAfterTx* after each RIF fragment transmission and by *phyHrpUwbStsCntAdvAfterRx* after each RIF fragment reception.

***<END >***