**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | Text Proposal for HRP UWB SRDEV PPDU |
| Date Submitted | [7 May, 2018] |
| Source | Frank Leong (NXP Semiconductors)Wolfgang Küchler (NXP Semiconductors)Thomas Baier (NXP Semiconductors)Brima Ibrahim (NXP Semiconductors)Jochen Hammerschmidt (Apple)Ayman Naguib (Apple)Thomas Reisinger (Continental)Daniel Knobloch (BMW) |  |
| 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 | [Proposal for HRP UWB SRDEV PPDU in 802.15.4z] |
| Purpose | [Propose elements of HRP UWB PHY and MAC for 802.15.4z] |
| 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. |

#  Introduction

Present HRP ranging-capable devices (RDEVs) use the content of the SHR to estimate time of flight. Due to the periodicity of the SHR, it may be vulnerable to attack.

This document describes interoperable secure ranging devices (SRDEVs) featuring enhanced immunity to attack. The main enhancement is the inclusion of a Scrambled Timestamp Sequence (STS) in the basic HRP PPDU format.

# Secure Ranging Requirements

## Secure Ranging PPDU Formats

An SRDEV device shall support the basic HRP frame format outlined in [1] §16.2.

In addition, SRDEV shall support the transmission and reception of frames, optimized for Secure Ranging, consisting of:

* “Synchronization Header” with SFD (Start of Frame Delimiter)
* “Scrambled Timestamp Sequence”, changing for every frame (according to a Key and a Seed, to be defined on higher layer)
* Fixed DATA (PHR+PSDU) part

Three Secure Ranging PPDU formats shall be supported, the difference between the formats being the location of the STS section and the existence of a PHR and PHY payload field:



Figure 1: Secure Ranging Frame Format A (mandatory, avoiding STS timing dependency on payload length)



Figure 2: Secure Ranging Frame Format B (optional, backward compatible in case of 62.4 MHz PRF)



Figure 3: Secure Ranging Frame Format C (Optional)

Secure ranging frame format C is intended for certain use cases where the participants in the secure ranging exchange are known to each other such that information about source and/or destination are implicit in the knowledge of what STS is used for transmission and reception between the connected devices, respectively.

## Frame Modulation Parameters

### Mean PRF

A mean PRF of at least 62.4 MHz shall be used for all packets during a ranging session. Mean PRFs lower than 62.4 MHz are not required for SRDEV devices.

### Binary Codes for SFD

To improve the performance of devices with coherent demodulators, the binary sequences listed in the following table can optionally be used as SFD. The selection of the code is either static or signaled via higher layers.

|  |  |  |
| --- | --- | --- |
| ID | Pattern | Nsym |
| 0 | --+- | 4 |
| 1 | ----++-+ | 8 |
| 2 | ---+-+--+--+++-+ | 16 |
| 3 | -----+---+++--+--+-+-+--+--++--- | 32 |
| 4 | -----+---+--+----+-++---+-+-+-------++---++-+-++--+-----++++--+- | 64 |

Table 1: Binary codes for SFD (Optional)

### SYNC Duration

The SYNC duration in number of periodic symbols ($N\_{SYNC}$) shall be configurable and cover the following values: 32, 64, 128, 256, 1024, 2048, and 4096. $N\_{SYNC}$ shall be static or known a priori via signaling at higher protocol layers.

### PHR Data Rate

To allow for reduced PSDU durations, given with very short Payloads, the PHR for ranging messages can optionally have the PHR field coded at the same rate as the payload, i.e., 6.81 and 27.24 Mb/s PHRs are allowed for payloads also coded at the same data rate. Note that 850 kb/s for both payload and PHR is already available per [1].

The signaling of the use of same rate PHRs shall be performed at the MAC layer, i.e., no auto detection of the PHR rate is required.

### Payload Data Rate

It is mandatory for an SRDEV device to also support the 6.8 Mb/s data rate, while 110 kb/s, 850 kb/s and 27.2 Mb/s are optional.

## Scrambled Timestamp Sequence Generation

The NIST, i.e., [2] §10.2.1, based Deterministic Random Bit Generator (DRBG) shall be used to generate the Scrambled Timestamp Sequence (STS). The length of the timestamp sequence shall be configurable.



Figure 4: DRBG for STS generation

The ith output bit of the DRBG is notated with symbol C(i). Internally the DRBG uses a block size of 128 bit. The jth generated block is notated with symbol B(j). Whereas j = floor(i / 128). The mapping from blocks to DRBG output bits is as following B(j) = {C(j\*128), C(j\*128 + 1), … C(j\*128 + 127)}.

An example of the first 256 generated bits of the DRBG can be found in Section 6.1.

The STS format shall be such that the standard correlator used for SHR processing can also be reused for STS processing, so in all modes, the spreading and SFD procedures described in [1], section 16.2.5 shall be used, with a given δL and a sequence of values for Ci derived from the DRBG sequence.

### 62.4 MHz PRF, Hopped Mode (Mandatory)

This mode allows use of non-coherent receivers, specifically to identify the STS according to the transmitted hopping bits.

Two consecutive values of the DRBG sequence A(i , i+1) is mapped directly to the STS code C(i, i+1) using the following table, i.e. bit Ai sets hopping position and bit Ai+1 sets binary value.

|  |  |
| --- | --- |
| $$A\_{(i,i+1)}$$ | $$C\_{(i,i+1)}$$ |
| $$0,0$$ | $$1,0$$ |
| $$0,1$$ | $$-1,0$$ |
| $$1,0$$ | $$0,1$$ |
| $$1,1$$ | $$0,-1$$ |

(i = 0,2,4,…)

The resulting sequence Ci is then spread using δL = 4.

### 62.4 MHz PRF, Data Symbol Structure Based Mode (Optional)

In this mode, the conventional payload mapper is used to map DRBG bits to UWB pulses. Specifically, following the Data Symbol Structure nomenclature of Table 16.3 in HRP UWB PHY of [1], the number of hop bursts is chosen to be 2 ($ N\_{hop}=2$), and the number of chips per burst is 1 ($N\_{cpb}=1$), for a total number of chips per symbol of 8. DRBG bits are directly passed to the symbol mapper with no encoding, where the DRBG and the PN sequence together determine the pulse position and pulse polarity (see BPM as described in [1], Sections 16.2.2 and 16.3).

### STS Length and Gaps

In 62.4 MHz PRF mode, the STS Building Block of the STS field in the frame is shown below:



Figure 5: STS Building Block

A segment of active (non-zero) pulsing at the PRF of 62.4 MHz is encapsulated by guard intervals, or gaps, of length Lgap in counts of chips. Lgap shall be 512, a guard duration of, roughly, 1 µs. All chips during each gap shall carry no signal energies at each respective transmitter.

The STS active segment length is specified in number of chips as follows:

$$N\_{STS,segment}= 16384\*2^{l}, with l\in \left\{0,1,2,3\right\}.$$

All devices shall support $l=1$, while other values of $l$ are optional.

Several STS Active intervals and Gaps can be combined to form the overall STS. The following diagram shows an example of two concatenated Building Blocks:



Figure 6: STS consisting of two STS Building Blocks

A single Gap of length 512 chips shall be inserted between successive STS Active intervals A and B, and Gaps shall also be inserted before and after the first and last STS Active segment. During the gap between successive STS Active intervals, the STS code shall be paused, and be resumed again after the gap.

Any number of STS Building Blocks can be concatenated, always with a single Gap of length 512 chips between consecutive STS Active intervals, up to 8 STS Building Blocks. The number of STS Building Blocks to be concatenated shall be static or made available a priori via upper layer signaling. All devices shall support use of 1, 2, 3, and 4 STS Building Blocks, while support of 5, 6, 7, 8 is optional.

The segmented approach allows consistency checks to improve the security and/or to exploit a stronger overall processing gain for the correlation.

# 124.8 MHz PRF PHY

## Introduction

A variety of optional techniques are suggested here to further improve Secure Ranging performance.

## Proposed Techniques

Modest increases in the average PRF can reduce overall power consumption, which is desirable for devices powered by coin-cell batteries. Specifically, doubling the average PRF from the default 62.4 MHz formats from chapter 2 to 124.8 MHz can result in a power efficient optional mode. In what follows, for the sake of simplicity, formats with a PRF of 62.4 MHz will be referred to as “PRF 64”, and formats with a PRF of 124.8 MHz will be referred to as “PRF 128”.

In the HRP PHY described in [1], PRF 64 utilizes a ternary signaling alphabet for the SHR Preamble, where on average about 50% of utilized pulse positions have zero-amplitude (see below Figure 7, top).



Figure 7: PRF 64 and PRF 128 (example)

Moving towards a binary signaling scheme or a ternary signaling scheme with a larger percentage of non-zero pulses can increase the average pulse density for PRF 128 without substantially increasing the levels of short-term measured peak power spikes that are already present in PRF 64 (Figure 7, bottom). For the binary signaling scheme, m-sequences of length 127 are candidates for use in the SHR.

Similar arguments can be made for the SFD and/or the new Scrambled Timestamp Sequence field.

The increased average pulse density can be exploited to reduce the “on-the-air” time for the packet, thereby decreasing power consumption and reducing collisions.

The achievable transmit power level in the current PRF 64 formats is often limited by the PHR and PSDU segments of the packet, owing to regulatory constraints on the short-term measured peak powers. The dense bursts used for Burst Position Modulation (BPM) in the current PRF 64 formats are particularly visible in creating substantial peak power spikes, which opens up a potential for revised header and payload structures to overcome these limitations.

Additional enhancements may be achieved by further raising the average PRF to 249.6 MHz (PRF 256).

## STS Format for 124.8 MHz PRF Mode

This mode provides the highest entropy/time density that can be realized without changing the Peak PRF of the SHR as defined for PRF 64.2 MHz in [1].

The DRBG sequence Ai is mapped directly to the STS code Ci using the equation:

$C\_{i}=-2\*A\_{i}+1, A\_{i}\in \left\{1,0\right\}, i=0,1,2,3,…$,

The resulting sequence Ci is then spread using δL = 4.

# MAC

This is a partial list of capability fields that need to be included in the MAC to support the changes described above:

* Specifying the STS frame format: 0 = No STS (mandatory), 1 = STS before PHR (mandatory), 2 = STS after PSDU (optional), 3 = STS-Only (optional)
* Specifying the STS building block configuration parameters
* Specifying the NIST DRBG Key and Seed initial value
* Specifying the capability and configuration of PHR being at specified data rate 6.81Mb/s or 27Mb/s (optional)

# References

1. IEEE Standard for Low-Rate Wireless Networks (IEEE Std 802.15.4™-2015).
2. NIST SP 800-90A Rev. 1 (2015)

# Appendix

## Example Data for STS Construction

### DRBG Data

This example illustrates the first two blocks generated by the DRBG described in Section 2.3 using following initialization:

key = 0x14148674D1D336AAF86050A814EB220F

data = 0x362EEB34C44FA8FBD37EC3CA1F9A3DE4

b = 0x00000000

DRBG Blocks:

B(0) = 0x7AA6F63EF917AE47115EB6FE3B5A5791

B(1) = 0x41DA0C7503566357EBF38B2C12BB3E92

C(0:255) = 0111101010100110111101100011111011111001000101111010111001000111000100010101111010110110111111100011101101011010010101111001000101000001110110100000110001110101000000110101011001100011010101111110101111110011100010110010110000010010101110110011111010010010

### Example for the 62.4 MHz hopped STS for the first 1024 chips before zero insertion (δL = 4) using the same DRBG initialization as in 6.1.1

A(0:255) = -00-0+0+0+0+-00+0-0--00++00-0-0+0-0-0+-0+0-0-00-0+0+0-0+-0+0-00-+0-0+0-0-0-00-0+0+0--00+0-0-0-0++00-0+0--0-00+0+-0-0-00-0+-0+0-0-0+0+0-00--00+0++0+00-+0-00--0-0+0+0+00--0-0-00+-00++00--0-0-00-0-0+0+0-0-0-+00-0++00+0-+00+0-+0+0-0+00+0+0-0+0-+00-0-0+0+-0+00+'

### Example for the 124.8 MHz STS for the first 1024 chips before zero insertion (δL = 4) using the same DRBG initialization as in 6.1.1

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