**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | Draft text for HRP UWB PHY enhancements |
| Date Submitted | 6 July 2018 |
| Source | Billy Verso (Decawave Ltd),  | billy.verso at decawave.com |
| Re: | Text contribution proposal to TG4z for IEEE 802.15.4z |
| Abstract | HRP UWB PHY enhancements for the TG4z amendment of IEEE Std 802.15.4-2015 |
| Purpose | This document provides draft text intended to be part of the final IEEE Std 802.15.4z (the amendment to IEEE Std 802.15.4) to enhance the UWB PHYs and associated ranging techniques.This draft text relates primarily the enhancement of the HRP UWB PHY as specified by IEEE Std 802.15.4™-2015, essentially presenting the editorial changes necessary to amend the text to apply the enhancements. |
| Notice | This document does not represent the agreed views of the IEEE 802.15 Working Group or IEEE 802.15.8 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:<http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and<http://standards.ieee.org/guides/opman/sect6.html#6.3>.Further information is located at <http://standards.ieee.org/board/pat/pat-material.html> and<http://standards.ieee.org/board/pat>. |

|  |
| --- |
| EXTRA NOTE: The text herein below is based on and keying off the proposals described in submission 15-18-0108-xx, which has developed over time so that some of the content here may be lagging behind. This will be rectified over time by future revisions. |

***The body of this document is draft text for inclusion into IEEE Std 802.15.4z however notes in red (like this one) are not intended to be part of the text of the final 4z standard. Editorial instructions intended to be included in the text of IEEE Std 802.15.4z are bold-italicized-black. The heading text and numbers included here are intended to align with those of IEEE Std 802.15.4-2015 to anchor the position of the text of this amendment with respect to the base standard.***

***NB: New tables and figures in this submission are numbered sequentially and generally cross-referenced in the text, it is expected that the Editor preparing the final text for the amendment may be re-numbering these in line with current practice for amendments. Modifications/additions to existing tables reproduce the table number and the caption text from the IEEE Std 802.15.4-2015 as plain text.***

# Overview

# Normative references

# Definitions, acronyms, and abbreviations

## Definitions

***Add the following new definition(s):***

**ciphered sequence:** a sequence of non-repeating cryptographically generated symbols included in HRP UWB PHY frames when the device is operating as an SRDEV

## Acronyms and abbreviations

***Add the following new acronym(s)/abbreviation(s):***

CSPRNG cryptographically secure pseudorandom number generator

# Format conventions

# General description

# MAC functional description

# MAC frame formats

# MAC services

# Security

# General PHY requirements

# PHY services

## Overview

## PHY constants

## PHY PIB attributes

***Insert the following new PHY PIB attributes into Table 11-2:***

**Table 11-2—PHY PIB attributes**

| **Attribute** | **Type** | **Range** | **Description** |
| --- | --- | --- | --- |
| : | : | : | : |
| *phyHrpUwbCipherKey* | 128-bitUnsigned | 0 to 2128-1 | Where the HRP UWB PHY supports the ciphered sequence, this attribute specifies the key used in the CSPRNG.  |
| *phyHrpUwbCsprngNonceCounter* | 16-bitUnsigned | 1 to 216-1 | Where the HRP UWB PHY supports the cipher sequence, this attribute provides read and write access to the 16-bit counter that supplies the lower 16-bits of the 128-bit *Nonce* input to the CSPRNG. |
| *phyHrpUwbCsprngNonceUpper112* | 112-bitUnsigned | 1 to 2112-1 | Where the HRP UWB PHY supports the ciphered sequence, this attribute provides the upper 112-bits of the 128-bit *Nonce* input to the CSPRNG. |
| *phyHrpUwbCipherMode* | Integer | 0, 1 and 2 | Where the HRP UWB PHY supports the ciphered sequence, this attribute specifies whether or not the ciphered sequence is present in the PHY frame and selects the position of the ciphered sequence as per Table 1.  |
| *phyHrpUwbCipherLength* | Integer | 32 to 2048 | Where the HRP UWB PHY supports the ciphered sequence, this attribute specifies the length of the ciphered sequence in *Ciphered Sequence Units* (CSU), (see 16.2.8.3 for a description of these), to include in the transmitted frame, and to expect in received frames. Note: the value shall be a multiple of 8.  |
| *phyHrpUwbCompressionMode* | Boolean | FALSE, TRUE | Where the HRP UWB PHY supports frame compression modes, when this attribute is TRUE frame compression modes are enabled. |
| *phyHrpUwbDataGuardTimeOff* | Boolean | FALSE, TRUE | Where the HRP UWB PHY supports frame compression modes, and *phyHrpUwbCompressionMode* is TRUE, then for certain sequences this attribute optionally enables additional compression by omitting the data symbol guard times |
| *phyHrpUwbMode2GapExtension* | Integer | TBD | Where the HRP UWB PHY supports the ciphered sequence, this attribute specifies an optional additional delay (gap of zero chips) between the PHY data and the ciphered sequence, when *phyHrpUwbCipherMode* is 2. |
| *phyHrpUwbPhrDataRate* | Enumeration | 0,DR110K DR850K, DR6810K and DR27M | Where the HRP UWB PHY supports frame compression modes, when this attribute is non-zero it overrides the DataRate parameter of the MCPS-DATA.request and causes the PHY to send, (and expect to receive), both PHR and PHY Payload fields at the nominal data rate indicated by the *phyHrpUwbPhrDataRate* value. Where the value refer to the nominal data rates supported by the PHY, and DR27M may be a higher data rate in some compression modes. |
| *phyHrpUwbPsr* | Integer | 0,32 to 2048 | Where the HRP UWB PHY supports frame compression modes, when this attribute is non-zero it overrides the UwbPreambleSymbolRepetitions parameter of the MCPS-DATA.request and specifies the length of the SYNC field. Note: The non-zero value shall be a multiple of 8.  |
| *phyHrpUwbReducedSpreading* | Boolean | FALSE, TRUE | Where the HRP UWB PHY supports frame compression modes, and *phyHrpUwbCompressionMode* is TRUE, then for certain sequences this attribute optionally enables a reduced spreading that gives additional compression of the frame durations. |
| *phyHrpUwbReplyTime* | Integer | xxx | Where the HRP UWB PHY has the ability for precise control of the transmission time, this attribute allows this TX time to be selected. The precision and variability of any resulting RX-to-TX reply time is implementation dependant, but shall be reflected in the RangingCounterStart and RangingCounterStop parameters of the MCPS-DATA.confirm and MCPS-DATA.indication primitive [Need to add a paragraph somewhere that references this feature and refers to and describes this attribute, maybe this is in section on ranging] |
| *phyHrpUwbReplyTimeActive* | Boolean | FALSE, TRUE | Where the HRP UWB PHY has the ability to control the transmission time, this attribute when TRUE specifies that the *phyHrpUwbReplyTime* attribute value its valid and should be used for the next transmission. When this attribute is FALSE the value of the *phyHrpUwbReplyTime* attribute is not used.  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  | : | : | : |

**[Note to self: review PIB to ensure that normative behavior is defined in body and not in this table.]**

# O-QPSK PHY

# Binary phase-shift keying (BPSK) PHY

# Amplitude shift keying (ASK) PHY

# Chirp spread spectrum (CSS) PHY

# HRP UWB PHY

## General

***Add the following paragraph(s) at the end of clause 16.1 just before the start of the succeeding clause:***

The HRP UWB PHY also includes optional frame compression modes to give reduced on-air time for higher density operation, and optional modes where the frame includes a ciphered sequence that increases the integrity and accuracy of ranging measurements. These modes require coherent receiver techniques.

A device with the ability to send and receive frames incorporating the ciphered sequence shall be termed a secure ranging device (SRDEV). The mandatory and optional requirements for an SRDEV are specified within the HRP UWB PHY clause, where the individual features are specified.

An SRDEV shall support interworking non-SRDEV, (i.e. an RDEV), at the nominal 64 MHz PRF by omitting the ciphered sequence.

## HRP UWB PPDU format

***Add the following paragraph(s), table and figure into clause 16.2 just before the start of sub-clause 16.2.1:***

Where the HRP UWB PHY supports the frame compression mode, the *phyHrpUwbPhrDataRate* attribute shall select the data rate for both PHR and PHY Payload fields. Where the HRP UWB PHY supports the ciphered sequence, the *phyHrpUwbCipherMode* attribute shall select the ciphered sequence position as per Table 1, and as shown in Figure 1. An SRDEV shall support *phyHrpUwbCipherMode* modes 0 and 1, while mode 2 is optional.

Table 1 – ciphered sequence modes

|  |  |
| --- | --- |
| **Value *of the phyHrpUwbCipherMode* attribute** | **Selected ciphered sequence mode** |
| 0 | There is no ciphered sequence field included in the frame. |
| 1 | The ciphered sequence field is placed immediately after the SFD field and before the PHR field. |
| 2 | The ciphered sequence field is placed after the PHY Payload field. |



Figure 1 – PHY frame structure with ciphered sequence

### PPDU encoding process

***In clause 16.2.1, at the end of the list of steps specifying the PPDU encoding process, add a new step (f) as follows:***

f) Where the HRP UWB PHY supports the ciphered sequence, produce the ciphered sequence according to the setting of the *phyHrpUwbCipherMode* attribute as described in 16.2.8

### Symbol structure

### PSDU timing parameters

### Preamble timing parameters

### SHR field

#### SYNC field

 ***Add the following paragraph(s) and tables into clause 16.2.5.1 just before the start of clause 16.2.5.2:***

Where the HRP UWB PHY supports the frame compression mode, and when *phyHrpUwbCompressionMode* attribute is TRUE, the preamble symbol is formed using one of the one of the code sequences from Table 2 identified by a preamble code, as selected by the *phyCurrentCode* attribute.

Each code sequence consists of 25 pulses (positive and negative as denoted in Table 2) and 6 zeros. The code sequences are spread as described above[[1]](#footnote-1) to generate the preamble symbol ***Si*** using the delta function *δL* and length L as given in Table 3. L is 4, when the *phyHrpUwbReducedSpreading* attribute is FALSE, and L = 1 when *phyHrpUwbReducedSpreading* is TRUE.

Where the HRP UWB PHY supports the frame compression mode, the length of the SYNC field (i.e. the *Nsync* number of repetitions of ***Si***) is specified by the *phyHrpUwbPsr* attribute.

Table 2 – Length 31 ternary codes for compressed preamble mode

|  |  |
| --- | --- |
| **Code index** | **Code sequence** |
| 25 | --0+++0+0-+0++-+--00--+-+++-+++ |
| 26 | --+-0--++++-0+-+++-++-00++0+0+- |
| 27 | -0-+++++-+++-0++-0--+-+-0+00++- |
| 28 | -0+00+-++0+-+-+++++--0--+0--+++ |
| 29 | -+0+++0-0-+0--+-++00+---++-++++ |

Table 3 – Preamble parameters for compressed preamble mode

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Ci* CodeLength** | **Peak PRF (MHz)** | **Mean PRF (MHz)** | **Delta Length *δL*** | **#Chips Per Symbol** | **Symbol Duration *Tpsym* (ns)** | **Base Rate****Msymbol/s** |
| 31 | 124.8 | 100.6 | 4 | 124 | 248.40 | 4.03 |
| 31 | 499.2 | 402.6 | 1 | 31 | 62.10 | 16.10 |

#### SFD field

***Add the following paragraph into clause 16.2.5.2 just before the start of clause 16.2.6:***

When the HRP UWB PHY is using frame compression modes or the ciphered sequence, then it shall employ the short SFD given by [-1 -1 -1 -1 +1 -1 0 0] spread by the preamble symbol ***Si***, where the leftmost bit shall be transmitted first in time.

### PHR field

***Add the following paragraph(s) and tables into clause 16.2.6 just before the start of clause 16.2.7:***

Where the *phyHrpUwbPhrDataRate* attribute is non-zero, then the PHR format and encoding shall be as shown in Figure 2. This includes a 2-bit GS field (whose encoding is specified below), along with a 10-bit PHY payload length field, a 1-bit ranging field, and a 6-bit SECDED field which is encoded is as specified above[[2]](#footnote-2). Note that since the PHR is not Reed-Solomon encoded its bit rate is approximately 1.15 times the nominal data rate.



Figure 2 – PHY header frame structure in frame compression modes

#### GS sub-field of the PHR

These are General Signaling bits, except when the *phyHrpUwbCipherMode* value is 2 in which case this GS field becomes the Gap Specification bits. In the Gap specification mode they tell the receiver which element of the GsRxTab[4] to use to align with the ciphered sequence arrival.

<Need to add more detail here>

### PHY Payload field

***Change the final sentence of 6.2.7 as shown:***

— When the PHY supports the frame compression mode, and the *phyHrpUwbCompressionMode* attribute is TRUE, then spread and modulate the encoded block as described in 16.3.4, otherwise spread ~~Spread~~ and modulate the encoded block using BPM-BPSK modulation as described in 16.3.

***Insert new clause 16.2.8 “Ciphered Sequence” as follows:***

### Ciphered sequence

This ciphered sequence consists of non-repeating symbols each consisting of a pseudo randomized set of pulses generated using a CSPRNG (cryptographically secure pseudo-random number generator) block based on AES‑128 in counter mode.

#### The ciphered sequence CSPRNG

The CSPRNG is run once for each pair of ciphered sequence symbols generated, producing a 128-bit pseudo-random number from which the lower-64 bits are used to form the 1st symbol of the ciphered sequence (and every alternate symbol thereafter) and the upper-64 bits are used to form the 2nd symbol of the ciphered sequence (and every alternate symbol thereafter). Each symbol is formed as described in 16.2.8.3.

The general structure of the CSPRNG is shown in Figure 3.



Figure 3 – ciphered sequence CSPRNG

The 128-bit key is specified via the *phyHrpUwbCipherKey* attribute, while the 128-bit *Nonce* is a combination the state of a 16-bit counter providing the low 16 bits and the value of the *phyHrpUwbCsprngNonceUpper112* attribute which provides the upper 112 bits. The 16-bit counter is advanced (clocked) once each time the CSPRNG is run, i.e. once for each pair of ciphered sequence symbols generated.

The value of the 16-bit counter may be set by the upper layer writing the *phyHrpUwbCsprngNonceCounter* attribute, and the state of the 16-bit counter may be ascertained by the upper layer by reading the *phyHrpUwbCsprngNonceCounter* attribute.

#### Ciphered sequence symbol formation

Using the 64-bit numbers generated by the CSPRNG (as described in 16.2.8.1), each ciphered symbol is formed as follows:

The input 64-bit number is taken and each bit with a value of 1 produces is treated as a positive polarity pulse (i.e. is a +1 pulse), while each bit of value 0 is treated as a negative polarity pulse (i.e. is a -1 pulse). The result is a list indexed 0 to 63 of pulse polarity values that are either +1 or -1, where index 0 is the first in time coming from the least significant bit of the input number, and index 63 is the last in time coming from most significant bit of the input number.

These 64 pulse polarity values are all used to generate the ciphered symbol when the mean PRF is 62.4 MHz or higher.

For the mean PRF of 15.6 MHz, only 16 of the pulse positions are maintained. These are those at the following indices: [0 3 7 12 19 21 27 30 34 38 44 48 53 58 60 63]. All other positions are removed (i.e. zeroed).

Then the 64 pulse polarity values (0, +1, -1) are spread by the delta function *δL* of length L = 4, as is done for the SYNC field as described in 16.2.5.1, to create 256 chips (at the chipping rate of 499.2 MHz) comprising the *Ciphered Sequence Unit* (CSU).

When *phyHrpUwbCompressionMode* attribute is FALSE, theseCSUare each sent followed by a *Ciphered Sequence Interval* (CSI) consisting of 256 zero level chips. Thus the ciphered sequence “symbol” period, *TCSYMB* sequence symbol is 512 chips, which is approximately 1.0256 µs, and the mean PRF is 62.4 MHz. A gap of 512 zero chips is inserted before the first CSU (i.e after SFD in Mode 1 or after the data in Mode 2)

When *phyHrpUwbCompressionMode* attribute is TRUE, the CSI are removed, and the ciphered sequence consists of continuous CSU, with the only gaps being 256 zero chips inserted both before and after the full sequence.

When the *phyHrpUwbCompressionMode* attribute and the *phyHrpUwbReducedSpreading* attribute is are TRUE, te spreading factor is reduced to L = 1.

#### Ciphered sequence additional mode 2 gap

Where *phyHrpUwbCipherMode* is 2 an additional gap programmed in the *phyHrpUwbMode2GapExtension* attribute shall be inserted between the end of the PHY Payload and start of the ciphered sequence.

#### Ciphered sequence length

The length of the ciphered sequence to send (and to expect when receiving it) is specified by the *phyHrpUwbCipherLength* attribute. This shall be configurable, in steps of 8, with valid values being 32 symbols up to 2048 symbols.

## Modulation

### Modulation mathematical framework

### Spreading

### FEC

#### Reed-Solomon encoding

#### Systematic convolutional encoding

***Insert new clause 16.3.4 “Compressed modulation mode” as follows:***

### Compressed modulation mode

When compressed frame mode is active, i.e. the *phyHrpUwbCompressionMode* attribute is TRUE, then the modulation is performed as follows:

With reference to the convolutional encoder specified in 16.3.3.2 and Figure 16-11, the $g\_{0}^{(n)}$ output determines which of two possible pulse sequences $s^{\left(n\right)} $will be used:

|  |  |  |
| --- | --- | --- |
|  | $$s^{\left(n\right)}=\left\{\begin{array}{c}s\_{0}=\left[-,-,-,-, -, -, -, -\right] , when g\_{0}^{\left(n\right)}=0, \\s\_{1}=\left[+, +, -, -, -, +, +,+\right], when g\_{0}^{\left(n\right)}=1,\end{array}\right.$$ |  |

while the $g\_{1}^{(n)}$ output determines the sign or polarity of sequence$ s^{(n)}$ by multiplying it by the bipolar version of $g\_{1}^{(n)}$ to get $v^{(n)}$

|  |  |  |
| --- | --- | --- |
|  | $$v^{(n)}=s^{(n)}.\left(-1\right)^{g\_{1}^{(n)}}$$ |  |

The pulse sequence $v^{(n)}$ is then scrambled by applying successive outputs Sn of the LFSR (described in 16.3.2) to each pulse, inverting the pulse polarity when Sn is 1, and leaving the pulse polarity unchanged when Sn is 0.

The number of chips per burst, *Ncpb*, is 8. A single burst position is defined, i.e. *Nhop* = 1, and there is no position modulation in that the scrambled burst occupies the first half of symbol, while the second half of symbol is a guard interval. Figure 6 shows the symbol structure.



Figure 6 – symbol structure in compressed mode

The symbol is 16 chips in duration. The timing parameters are given in Table 4.

Table 4 – compressed (27 Mb/s) mode timing parameters

|  |  |  |  |
| --- | --- | --- | --- |
| **Peak PRF (MHz)** | **Modulation & Coding** | **Symbol Structure** | **Data** |
| **Viterbi Rate** | **RS Rate** | **Overall FEC rate** | **#Chips Per Burst *Ncpb*** | **#Chips Per Symbol** | **Burst Duration *Tburst* (ns)** | **Symbol Duration *Tdsym* (ns)** | **Symbol Rate (MHz)** | **Bit Rate Mb/s** | **Mean PRF (MHz)** |
| 499.2 | 0.5 | 0.87 | 0.44 | 8 | 16 | 16.026 | 32.05 | 31.2 | 27.24 | 249.6 |

## RF requirements

## HRP UWB PHY optional pulse shapes

## Extended preamble for optional CCA mode 6

## Ranging

# GFSK PHY

# MSK PHY

# LRP UWB PHY

# SUN FSK PHY

# SUN OFDM PHY

# SUN O-QPSK PHY

# LECIM DSSS PHYs

# LECIM FSK PHY specification

# TVWS-FSK PHY

# TVWS-OFDM PHY

# TVWS-NB-OFDM

# RCC LMR PHY

# RCC DSSS BPSK PHY

1. This is referring to text pre-existing in IEEE Std 802.15.4-2015. [↑](#footnote-ref-1)
2. This is referring to the text pre-existing in clause 16.2.6 of IEEE Std 802.15.4-2015. [↑](#footnote-ref-2)