Overview on HRP UWB standard 802.15.4-2024

Gabriele Da Re
School of Computer Engineering
University of Padua
Padua, Veneto, Italy
Email: gabriele.dare00@gmail.com
Mat: 2158818

***Abstract*—The purpose of this survey is to understand and address these topics of the standard IEEE 802.15.4-2024, "IEEE Standard for Low-Rate wireless networks"**

I. Introduction

The standard[1] covers many physical layers and one Medium Access Control layer (MAC) for low rate wireless personal area networks (LR-WPAN). There are some special applications such as Smart Utility Network, Rail Communications and Control, Radio Frequency Identification (RFID), Medical Body Area Networks. Among many others it covers the one we are interested in, the Ultra Wide Band (UWB) technology. UWB is a technology generally defined like others in the standard[1] as a Wireless Personal Area Network (WPAN). So we will give an quick overview of the standard[1] and then focus on the UWB technology.

II. General Description

A. Network Topologies

Topologies for LR-WPAN are two, star and peer-to-peer. In the star topology, the coordinator is the central device and the other devices are the end devices. The coordinator is the only device that can communicate with the end devices, and is usually wall powered, whilst end devices are battery powered. Suited for home automation, personal health care and games. The peer-to-peer topology is a network of devices that can communicate with each other, thus allowing for more complex networks, such as mesh networks, using multiple hops, implemented at higher level, thus not discussed in this standard[1]. Suited for sensor networks, enabling smart agriculture, industrial control and monitoring and asset and inventory traking.

Each indipendent PAN selects a UID (PAN Identifier) thus allowing for multiple PANs to coexist, moreover each device in a PAN can communicate within with a short address, permits to communicate also with another device from another PAN.

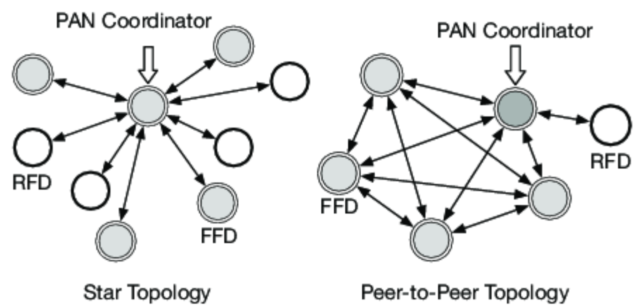

Fig. 1. Star and peer-to-peer topologies

B. Architecture

The architecture is composed of three layers:

- Physical Layer (PHY)
- Medium Access Control (MAC)
- Higher layers

Only PHY and MAC are defined in the standard[1], the higher layers, such as network, that involves its configuration, message routing and manipulation are left to the implementer. as well as the application layer.

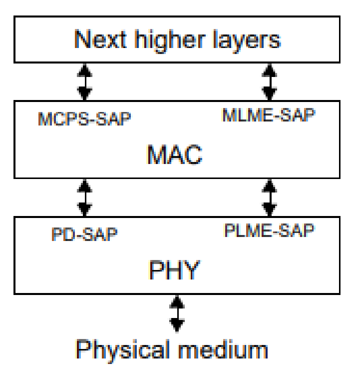

Fig. 2. IEEE 802.15.4-2024 architecture

1) Physical Layer (PHY): The PHY layer has its main focus on the activation and deactivation of the radio transceiver, energy detection, link quality indication, channel freq. selection, clear channel assessment, precision ranging (UWB) and data transmission and reception. In the specific case of High Rate Pulse repetition frequency UWB, it also serves the purpose of precision ranging.

2) Medium Access Control (MAC): The MAC overlay provides 2 services:

- Data service
- Management service

The data service is responsible for the MAC protocol data units transmission and reception, whilst the management service is responsible for the interfacing with the MAC sublayer management entity service access point (MLME-SAP fig.2). In particular the MAC overlay provides the possibility to manage beacons, channel access, association and disassociation, acknowledged frame delivery, guaranteed time slots management and frame validation. In addition can provide security features like managing STS parameters in UWB.

C. Functional overview

1) Scheduled access: Access is managed by different implementations of the superframe structure.

Beacon superframe, defined and sent by the coiordinator, dependant on beacons. Can have an active and inactive portion, during the latter the coordinator is able to enter low-power mode (sleep), thus saving energy. Beacon transmission is executed at the beginning of each superframe by the coordinator, in order to synchronize and identify the devices of the PAN. It can be avoided by the coordinator bypassing the beacon transmission. The Superframe Duration $\leq$ Beacon Interval, is divided in two parts:

- Contention Access Period (CAP)
- Contention Free Period (CFP)

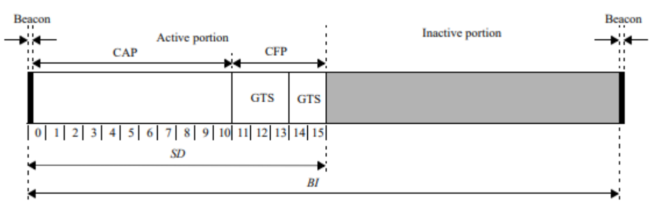

Fig. 3. Beacon superframe with Guaranteed Time Slots (GTS) in the CFP

Deterministic and synchronous multichannel extension (DSME) multi-superframe, as in beacon, starts with the PAN coordinator sending an Enhanced Beacon frame, containing DSME PAN Descriptor Information Element (IE). The multi-superframe is divided in cycles of repeated superframes 4, composed as usual, of enanched beacon frame, CAP and CFP.

Time Slotted Channel Hopping (TSCH) sees the substitution of the superframe with a slotframe, also containing guaranteed or CSMA-CA periods. The difference is the shared notion of time between partecipants, thus allowing for automatic repetition of the slotframe, without involving beacon transmission. It can also communicate the device's assigned timeslot(s) in the slotframe by beacon, but tipically is handled at higher layers. Since all devices are synchronized and share channel information, they can hop over channels decreasing interference and multipath fading, doing so in slotted channels to avoid collisions, thus avoiding retransmissions, usefull in industrial environments.

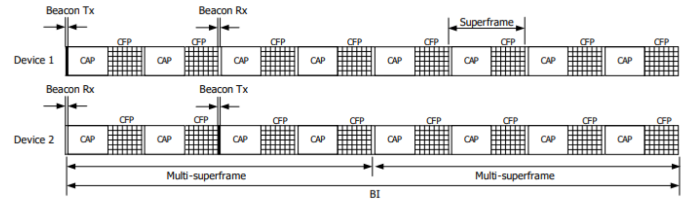

Fig. 4. DSME multi-superframe

TVWS multichannel cluster tree PAN (TMCTP). A cluster tree network is a mesh of clusters, each with a coordinator, that can communicate with other clusters, forming a tree. The easiest is a single cluster, with a coordinator and end devices, but can be extended to multiple clusters by the first PAN coordinator, that instructs a device to become a coordinator of a new cluster. This augment the coverage area, with the downside of augmenting the message latency. The TMCTP is a cluster tree network with a Master PAN coordinator(Super Pan Coordinator), that synchronizes other PAN coordinators over different channels, that in turn synchronize their clusters. Parent PAN coordinator(s) communicate with their PAN-coordinator child(s) in its own channel CAP or CFP, whilst childs send beacons to their parent in a dedicated channel, Dedicated Beacon Slot (DBS) assigned by the coordinator in the Beacon Only Phase (BOP). So the TMCTP has an enhanced superframe structure, with a BOP, a CAP and a CFP.

2) Data Transfer Model: The transfer models of the standard[1] are:

- Transfer to a Coordinator from a device.
- Indirect transfer from a coordinator in which the device recives the data.
- Transfer between two peer devices.

On a correctly recived frame, if requested, the receiver sends an acknowledgment frame that can be of 3 types:

- Immediate acknowledgment
- Enanched acknowledged
- Fragment acknowledgment

Data transfer to a coordinator is managed in two ways depending on beacon enabled or not. If synchronization *beacons are enabled*, the device listens for the beacon, when found it synchronizes to the PAN, and sends the data frame to the coordinator at an appropriate time.
If *not enabled* it transmits directly to the coordinator.

Indirect data transfer using the superframe structure, the coordinator that has data for a device, indicates in the beacon that a data message is pending. Since devices are synchronized through the beacon, they can listen for pending

messages, if present, the device sends a Data Request command to the coordinator, that in turn sends the data frame and when succesfuly completed, removes the message from the pending list in the beacon.
If not using the superframe structure, and a Data Frame is pending, the coordinator stores the data and sends it to the device up on request by the latter. Else the coordinator that has no data, either indicates it on the returned ACK if requested by the device that sent the Data Request, or in a Data Frame with zero payload.

Data transfer **between two peer** devices is managed either by a device that constantly recives or synchronizes with the sending device. In the first case the device attempts to send data when channel access is gained, in the second case other measures are taken to achieve sync.

3) Frame Structure: Thought to be reliable in noisy environments while keeping complexity low, the frames are passed from the MAC to the PHY layer as the PHY Service Data Unit (PSDU), that is then converted to the PHY Protocol Data Unit (PPDU) and transmitted. PPDU for HRP-UWB on UWB chapter.

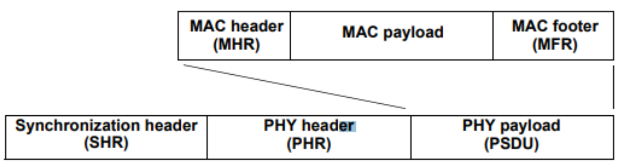

Fig. 5. PHY Protocol Data Unit (PPDU)

4) Information Elements: To transmit information between layers and devices, the standard[1] uses Information Elements (IEs), that consist of an ID and a length field, followed by the information itself. If the IE is not recognized, it is ignored, else it can be accepted or discarded.

5) Access Methods: The standard[1] defines the following access methods:

- Unslotted carrier sense multiple access with collision avoidance (CSMA-CA), used where is not used the superframe structure.
- Slotted CSMA-CA, used in the superframe structure.
- TSCH CCA (TSCH Clear Channel Assessment) in non shared slots where the MAC layer requests a CCA to the PHY layer at a designated time in the timeslot, that in turn returns the result.
- TSCH CSMA-CA, in shared slots (multiple devices can transmit in that assigned timeslot 10.3.2.2-10.3.9.2 section of the standard[1]). Collisions are detected by not reciving an acknowledgment frame. In shared links if there is a collision, retransmission is implemented along with an exp. backoff mechanism to avoid further collisions (backoff exponent increased on every collision).
- CSMA-CA with Priority Channel Access (PCA), used in presence of MAC Service Data Units containing CriticalEventMessage parameter flag set to true
- LECIM (Low Energy Critical Infrastructure Monitoring) ALOHA with PCA.

Frame acknowledgment is optionally sent if requested, to confirm reception and validation of a frame. The reciving device can add content as enhanced acknowledgment frame encapsulated as information elements, then if the originator does not understand the IE content of the Enh-Ack, is ignored but considering the transmission succesful.

Frak is used in a fragment sequence to determine which fragments have been recived and which are missing explicitating the status of one or more fragments.

Octets: 2	variable	2/4
Frak Header	Fragment Status	Frak Validation

Fig. 6. Frak format

Data verification is achieved in MAC service data units through a cyclic redundancy check (CRC). For fragment sequences, is implemented a fragment identity check sequence (FICS) included in each fragment, used also to determine along with the fragment number, which fragments are missing and which are recived.

Octets: 2	variable	2/4
Fragment Header	Fragment Data	FICS

Fig. 7. Fragment packet

6) Power Consumption: Mainly, devices that are battery powered will require duty-cycling, that is the device is active for a short period of time listening on the RF channel for incoming messages and then goes to sleep the majority of the time, thus saving energy. Sleep and listen periods are decided by the application designer, who finds a compromise between message latency and battery consumption. Devices can also continously listen.

In URP UWB, the standard[1] also provides a hybrid modulation that permits noncoherent architectures in order to reduce power consumption and implementation complexity.

7) Security: The cost objectives of ad nature of hoc networks impose additional security constraints, but also result difficult to achieve. The problems are low cost devices, mostly with low computational power, available memory and battery power. Also there is the problem of the trusted computer base, or random number generation, that is difficult to achieve. Is futhermore not implied that there is a fixed infrastructure, thus implying that are possible communications between devices that have never communicated before.

Since most of the security features are implementable at higher layers, is out of scope for the standard[1]. (for further info IEEE 802.15.9).

The mechanism used in this standard[1] is based on symmetric key cryptography, and uses keys provided by the higher layer processes, that also provide establishment and maintenance of the latter, thus the MAC layer is not involved in the key management and assumes that the implementation is secure.

The mechanism provides combinations for 3 security services:

- Data confidentiality: assumes informations are not disclosed to unauthorized parties.
- Data integrity: assures the data source, thus not altered during transmission.
- Replay protection: assures that a duplicate is detected. (important for UWB on keyless devices).

The frame protection can be adapted on a per frame basis, varying the security level depending on the requirement of security over security overhead. Keys are either shared between 2 devices (link key) or between a group of devices (group key). This implies lower maintenance and storage costs, but also implies that if adevice in the group is compromised, the whole group is compromised.

III. General PHY requirements

A. Frequency ranges

Band designation	Frequency band MHz
HRP UWB sub-gigahertz	250-750
HRP UWB low band	3244-4742
HRP UWB high band	5944-10 234
LRP UWB	5624.32-10 435.2

TABLE I
FREQUENCY RANGES FOR UWBS (IN MHZ)

B. Channel Assigment

Channel number	Center Frequency	HRP UWB band
0	499.2	Sub-gigahertz
1	3494.4	Low band
2	3993.6	
3	4492.8	
4	3993.6	
5	6489.6	High band
6	6988.8	
7	6489.6	
8	7488.0	
9	7987.2	
10	8486.4	
11	7987.2	
12	8985.6	
13	9484.8	
14	9984.0	
15	9484.8	

TABLE II
CHANNEL ASSIGMENTS FOR HRP UWBS

Channel number	Center Frequency
0	6489.6
1	6988.8
2	7987.2
3	8486.4
4	6681.6
5	7334.4
6	7987.2
7	8640.0
8	9292.8
9	9945.6

TABLE III
CHANNEL ASSIGMENTS FOR LRP UWBS

C. Reciver Energy Detection (ED)

Is intended to be used as a part of a channel selection algorithm. The ED is an estimation of the recived signal power within the channel bandwidth.

D. Clear Channel Assessment (CCA)

UWB should implement one of the following CCA methods (last 2 only for HRP UWB):

- Mode 1: Energy above threshold, it reports the medium busy if the energy is above the ED threshold.
- Mode 2: Carrier sense only, it reports the medium busy if the signal detected is complaint with the standard[1] and same modulation used by the detecting device.
- Mode 3:
  - Mode 3a: Carrier sense with Energy above threshold (either required), it reports busy whether Mode 1 or Mode 2 reports busy.
  - Mode 3b: Carrier sense with Energy above threshold (both required), it reports busy if both Mode 1 and Mode 2 report busy.
- Mode 4: ALOHA, CCA should always report an idle medium.
- Mode 5: Known as preamble sense, it reports busy if after listnening finds the synchronization header of a frame. After it should wait atleast for the frame to be completely sent and acknowledged before reporting idle.
- Mode 6: Preamble sense based on the packet with the

multiplexed preamble.

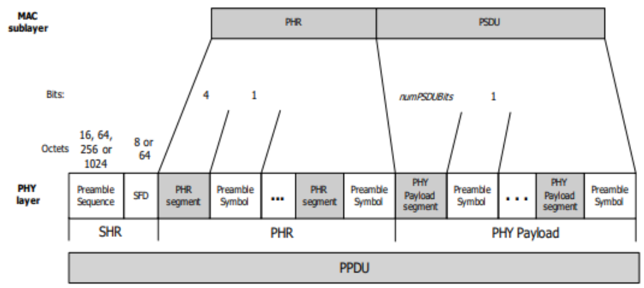

Fig. 8. HRP UWB multiplexed preamble mode

IV. HRP UWB PHY

A. General

To be compliant with the standard[1], the PHY layer must implement support for at least one between the channels 0, 3 and 9. Within each there is support for at least 2 complex channels each with an unique lenght 31 preamble codes. So the device must support the lenght 31 codes for each channel it implements.
More specifically, the standard[1] defines 16 frequency bands, each with 2 complex channels, if a band is choosen, the device must support both channels.

To increment ranging accuracy, reduced on-air time and power consumption, the standard[1] also provides optional modes for example scrambled timestamp sequence (STS), these devices that use this additional modes are called HRP-ERDEV (Enhanced Ranging Devices) and must support:

- Operation at the Base Pulse Repetition Frequency (BPRF) of 64 MHz.
- Operation at higher PRF than BPRF, called HPRF.

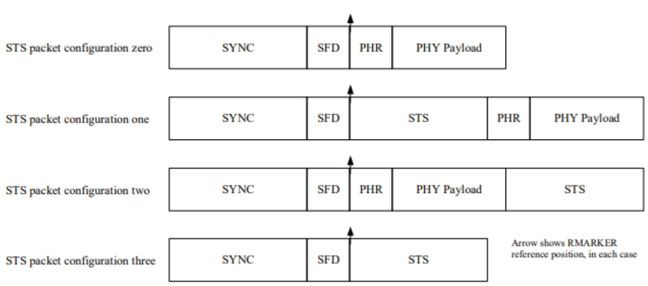

Fig. 9. STS position and Pysical Protocol Data Unit (PPDU) format

B. PPDU encoding

There are different steps in the PPDU encoding, precisely:

1) Reed-Solomon encoding on PSDU.
2) Creation of the PHY header (PHR), including single error correct, double error detect (SEC-DED) code, anteponed to the PSDU.
3) More convolutional encoding is done, so adds parity bits on the datastream, if the stream is 27Mb/s the encoding is bypassed in favor of 2 encoded bits per symbol of BPM-BPSK (Burst Position Modulation-Binary Phase Shifting Keying). The encoder is zeroed by adding 2 ‘0’ bits at the end of the PPDUs (k=3) or 6 to both PHR and PSDU, the latter for a K=7 conv. encoder only in HRP-ERDEV devices.
4) Modulation of PHR and PSDU according to different rates, 110kb/s, 850kb/s, 6.8Mb/s, dependant on the standard[1] (page 642).
5) Production of the synchronization header (SHR) from SYNC field and Start of Frame Delimiter (SFD).
6) For HRP-ERDEV devices, the Scrambled Time Stamp is added to the PPDU.

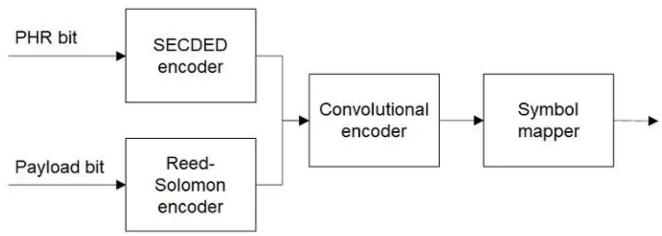

Fig. 10. PPDU encoding

C. Symbol Structure

Using BPM-BPSK, the symbol structure is composed of 2 bits per symbol, with the first bit determining the position (0 or 1) and the second the phase (-1 or +1). In each data symbol interval T_{dsym} is transmitted a single burst, composed of N_{cpb} contiguos chip of duration T_c per burst, each of N_c possible positions. Furthermore, $T_{bpm} = T_{dsym}/2$, so enables binary position modulation and $T_{dsym} = N_c \times T_c$.
To mitigate multipath interference between symbols, the standard[1] limits the burst transmission to the first half of each T_{bpm}, so the first $N_{hop} = N_{burst}/4$ where $N_{burst} = T_{dsym}/T_{burst}$ is the number of brust durations in a symbol and $T_{burst} = N_{cpb} \times T_c$, also $T_{dsym} = T_{burst} \times N_{burst}$.

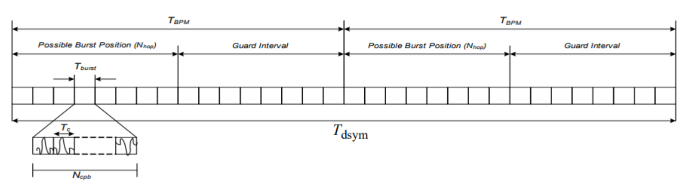

Fig. 11. Symbol structure

D. PSDU timing parameters

Within each HRP UWB channel 0:15 the peak Pulse Repetition Frequency (PRF) is 499.2MHz, where the mean PRF is the number of pulses per symbol period divided by the lenght of the symbol period $MeanPRF = N_{cpb}/T_{dsym}$. As previously stated, the device must support the lenght 31

codes for each channel it implements, and both 15.6 MHz and 3.90 MHz mean PRFs for PSDU, optionally if using the lenght 127 codes, it must support also 62.4 MHz mean PRF frequency.
There are larger bandwith channels 4, 7, 11, 15 that have bandwidths $> 500MHz$, thus premitting higher power transmissions (limited to power spectral density). Achieving higher range, ranging accuracy and enhanced multipath resistance.
Different datarates are achieved by changing the number of chips within a burst ($T_c \approx 2ns$), whith the total number of burst positions constant.
Symbol rate is the inverse of the symbol period, so $1/T_{dsym}$, and the bit rate is also considering the Forward Error Correction (FEC) overhead, so $1/T_{dsym} \times (2 \times OverallFECrate)$.

E. Preamble timing parameters

Different parameters are used fort the SHR, composed of the SYNC field and the SFD, and the PSDU. Indeed the mean PRF for the preamble is slightly higher since in the SHR are not used power of 2 lenght codes, nor number of chips.
The SHR has 4 possible durations, denoted by different lenghts of the SYNC field, that repeats the preamble symbol 16, 64, 1024 or 4096 times. This repetition yields different PPDU time durations.

F. SHR field

There are 4 preamble lenghts as previously stated, called, in order, short, default, medium, long, the one to used is specified in a parameter in MCPS-DATA.request primitive.

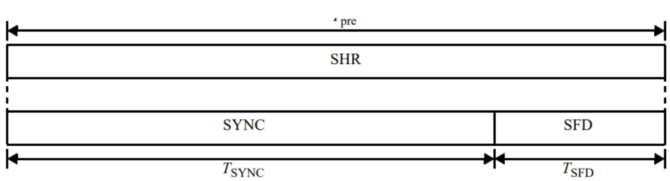

Fig. 12. SHR field

1) SYNC field: Each PAN in a HRP UWB channel is identified by a preamble code, the SYNC field is composed by symbols defined by a preamble code. Each *preamble code* is a *sequence of code symbols* from a ternary alphabet (-1,0,1), and can be of lenght 31 or 127 (91 for ERDEV). Each channel has a fixed amount of possible preamble codes. As previously stated data is sent in bursts, each of N_{cpb} contiguos chips, each of N_c possible values of duration T_c. The SYNC field is composed by N_{sync} repetitions of the symbol $\mathbf{S}_i$, denoted by the code itself getting spread by a δ_L function, becoming then the symbol $\mathbf{S}_i$. So the code with index i ($\mathbf{C}_i$ table 16-7 16-8 16-9 of the std) spread over function δ_L (L = spreading factor, table 16-5 16-10). SYNC field scales with the number of Preamble Symbol Repetitions (PSR), that is the N_{sync} repetitions of the symbol $\mathbf{S}_i$ in the SYNC field.

$$\mathbf{S}_i = \mathbf{C}_i \otimes \delta_L(n)$$

$$\delta_L(n) = \begin{cases} 1 & n = 0 \\ 0 & n = 1, 2, \ldots, L-1 \end{cases}$$

$\otimes$ is Kronker product, note that the $L-1$ zeroes are interponed between each ternary element of $\mathbf{C}_i$ ($\mathbf{C}_i(x); x = 0:30$ *or* $0:126$)

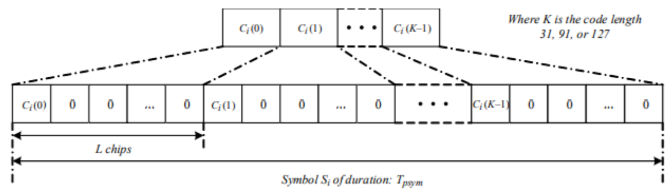

Fig. 13. Preamble Symbol Period, part of the SYNC field

2) SFD field: Start of frame delimiter can be of 2 types, the short for default and medium datarates, and the long for low datarates.

G. PHR field

Formatted like in the figure below.

Bits	Field
0-1	Data Rate
2-8	Frame Length
9	Ranging
10	Reserved
11-12	Preamble Duration
13-18	SECDED

Datarate indicates the datarate of the PHY payload field, specified in a particular attribute, depending on mean Pulse Repetition Frequency, 850kb/s is the only non optional to be supported. Bit setup seen in table (16-12 of the std), with regard to datarates with different mean PRFs.
Frame lenght is an unsigned integer indicating the number of octets in the PSDU.
Ranging is set to 1 if the frame is a ranging frame, 0 otherwise.
Preamble duration represents the lenght (as N_{sync} number of symbol repetitions) of the SYNC field in the SHR.

Field value, b11 b12	SYNC length (symbols)
00	16
01	64
10	1024
11	4096

TABLE IV
SYNC LENGTH VALUES BASED ON PREAMBLE DURATION FIELD VALUE

The duration is used for ranging operations, in order to determine when the PHY layer got and started tracking the

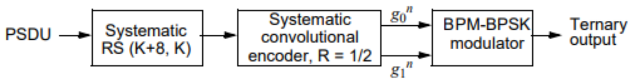

Fig. 14. PHY payload encoding

preamble. Also used by reciver to set its own preamble duration upon the value reviced when is sending a ranging Acknowledgment frame.
SECDED is a field that enables the detection of 2 errors and the correction of one. It depends on the previous PHR bits (0-12) and computed xoring different bits of the header.

1) PHR for HRP-ERDEV BPRF and HPRF: For HRP-ERDEV devices, the PHR differentiates between BPRF and HPRF, with the addition to BPRF that the PHR might be sent at the same rate of the PSDU (data), and the HPRF has a different PHR.

Bits	Field
0	A1
1	A0
2-11	PHY payload length
12	Ranging
13-18	SECDED

TABLE V
PHR FOR HRP-ERDEV HPRF

H. PHY Payload Field

Encoded as follows:

The first step is the Reed-Solomon encoding of the PSDU with 48 parity bits. The second part is encoded through a convolutional encoder, where parity bits are calculated using a sliding window on the datastream (in some cases is bypassed). Then the data is modulated according to HPRF or BPRF, if the latter, BPM-BPSK is used.

I. Scrambled Time Stamp (STS)

Is a sequence of pseudo random pulses generated by a Deterministic Random Bit Generator (DRBG) based on AES-128. Arranged in 1 to 4 active blocks separated by silent blocks (Gaps).

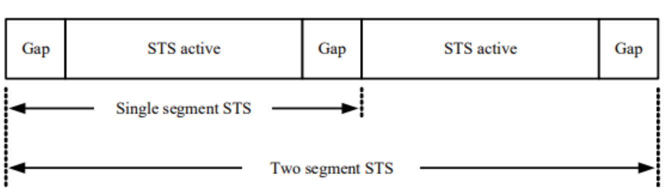

Fig. 15. STS structure with 2 active blocks

The optimal PPDU position for the STS is at the end of the Payload, (packet configuration 2 Fig. 9)

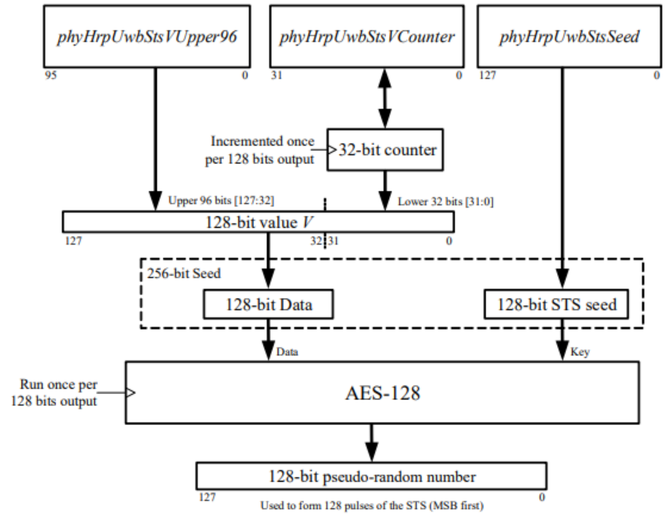

Fig. 16. STS encoding

As in figure 16, the STS seed is decided by the above layer through an attribute, as the counter, incremented each iteration of the DRBG, in order to always give a new V value.
Synchronization of V and seed values is responsibility of the higher layers, though an RSSD IE can be used to align seed and counter to the reciver. This information element is composed of the first bits specifying the presence or not of certain fields, then there are the optional fields, among which the seed and counter fields. 4 octects for the 32bit counter and 16 octects for the 128bit seed.

Bits	Field
0	V3P
1	V2P
2	V1P
3	VCP
4	SSP
5–6	ACP
7	CP
Octets	**Field**
0/4	V3
0/4	V2
0/4	V1
0/4	V Counter
0/16	STS Seed
0/4/8/16	Application Code

V1, V2, V3 coitain in order 32-63, 64-95, 96-127 bits of STS generation data, V Counter is the counter value(0-31 bits of STS), STS Seed is the seed value, Application Code is used to transfer additional data from the higher layer, which is also responsible for the validation and programming of these fields. The P means that the field is present, so if bit 0 is 1, V3 is present, if bit 1 is 1, V2 is present, and so on.

1) Forming the STS: As described in IV-F1, the STS after the 128bit random number is generated, in which each **0** bit is a **positive** polarity pulse and each **1** bit is a **negative** polarity pulse, is spread by the δ_L function with L=8 in BPRF and L=4 in HPRF.
As in Fig. 15, the STS is composed of 1 to 4 active blocks, each of the *same length*.

J. Modulation

1) FEC: The Forward Error Correction (FEC) in the HRP UWB PHY is concatenated code consisting of an outer shell of Reed-Solomon encoding and an inner half-rate convolutional encoding (first bit encoded and second not). As previously stated the inner convolutional encoding is not enabled at all datarates (table 16-4 of the std where viterbi rate is 1 conv. is disabled for the PSDU of the physical frame).

2) Reed-Solomon generator:

$$\begin{aligned} g(x) &= \prod_{k=1}^{\circ}(x+\alpha^k) \\ &= x^8 + 55x^7 + 61x^6 + 37x^5 + 48x^4 \\ &\quad + 47x^3 + 20x^2 + 6x + 22 \end{aligned}$$

3) Convolutional encoding: As stated previously, the encoder can have k of both 3 and 7 depending if HPRF is in use, if in use k=7 can be optionally employed over k=3. If k=7 is used, Reed-Solomon encoding is disabled on the PSDU, moreover the conv. encoder is run over the whole PHR (in halved rate) and PSDU. Datarate is higher using conv. encoder over Reed-Solomon encoding in HPRF devices, in both 124.8 MHz PRF and 249.6 MHz PRF.
Convolutional encoding is not supported in noncoherent reciver so the only performance improvement possible is through Reed-Solomon decoding.

REFERENCES

[1] “Ieee standard for low-rate wireless networks,” *IEEE Std 802.15.4-2024 (Revision of IEEE Std 802.15.4-2020)*, pp. 1–967, 2024.