**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | Ranging procedures and messages | |
| Date Submitted | 10th September 2018 | |
| Source | Billy Verso (DecaWave), | billy.verso @ decawave.com |
| Re: | Draft text covering two way ranging mechanisms, procedures and messages | |
| Abstract | Text for possible inclusion in IEEE 802.15.4z | |
| Purpose | Provision of the text to facilitate its incorporation into the draft text of the IEEE 802.15.4z standard currently under development in the 802.15 TG4z. | |
| 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>. | |

***Goal of this submission:***

*The objective of this submission is to provide text, for inclusion into the 15.4z draft, to standardize the mechanisms, messages and procedures for ranging and location.*

*Essentially, this means employing IE as the mechanism to convey the controls and data necessary to complete the ranging interactions, and providing message sequence charts (MSC) to illustrate the interactions / procedures.*

*Much of the content here has come from an earlier submission to TG8 (*[*15-15-0429-01*](https://mentor.ieee.org/802.15/dcn/15/15-15-0429-01-0008-text-for-relative-positioning-and-location.docx)*), which had a green field to work with.*

*In 15.4, we have preexisting text describing ranging, primitives with ranging related parameters already specified, and even a couple of ranging related IE added for TVWS.*

*Thus this submission has to consider the pre-existing 15.4 text and include any modifications of that pre-existing text of 15.4 that may be necessary to make it consistent with its original intent while encompassing the new mechanisms we want to add.*

*This submission is planned to be close to the format needed for inclusion into the 15.4z draft amendment, by including editing instructions, etc., and by trying to align with the clause numbers in the 802.15.4 – 2015 standard,*

*This is a work in progress, in that it includes highlighted and red text indicating where issues exist that are open / not resolved by the text.*

1. MAC Functional Description

***Change titles of clause 6.9 and its sub-clause 6.9.1 as shown, and modify opening paragraph of 6.9.1 as shown forming the two paragraphs below:***

* 1. Ranging, relative positioning and localization
     1. ~~Ranging requirements~~ Overview

~~Ranging is an optional feature.~~ This standard includes optional features to support relative positioning and location. While received signal strength may allow for a crude measurement of relative proximity for most PHYs, accurate location is generally only achieved where message reception (and transmission) times can be accurately determined, e.g. using one of the UWB PHYs defined in this standard. With accurate message timestamping, techniques such as two-way ranging time of flight (TOF) can give extremely good estimates of relative separation distance between two devices. Similarly an accurate location estimate for a mobile device can be determined, for example, when the distance to a number of fixed devices (of known location) is ascertained.

The fundamental measurements for ranging are achieved using a transmitted frame and a response frame, for instance this could be a Data frame and its Ack response frame ~~sequence~~. The ~~Data frame has~~ the PHR Ranging field set to indicate~~d~~ ranging and the frame is referred to as a ranging frame (RFRAME). Ranging capabilities are enabled in a ranging-capable device (RDEV) with the MCPS-DATA.request primitive. Whenever ranging is enabled in an RDEV, the RDEV delivers timestamp reports to the next higher layer as a result of events at the device antenna. The timestamp that is reported is measured relative to the RMARKER. For all PHYs the RMARKER is defined to be the time when the ~~beginning of the first symbol of the PHR~~ end of the last symbol of the SFD of the RFRAME is at the local antenna.

***Insert in 6.9.1 before 6.9.2 the following paragraphs:***

The relative positioning and locating methods supported by this standard are: single-sided two-way ranging, double-sided two-way ranging and, “one-way” ranging for the time-difference of arrival localization method. These are described further in the clauses below.

In a typical implementation, the timestamps will be captured by digital logic internal to the transmitter and receiver, and then adjusted to account for the time difference between the internally captured time and the time the RMARKER actually launches or arrived at the antenna. These offsets are separately defined for transmitter and receiver as the configurable PIB elements *phyTxRmarkerOffset* and *phyRxRmarkerOffset*.

Where the MCPS-DATA.confirm primitive is reporting an acknowledged transmission, the TxRangingCounter reports the transmit time of the data frame RFRAME, and the RxRangingCounter reports the receive timestamp of the Ack RFRAME. Where non-acknowledged transmission is used, the RxRangingCounter is invalid.

In the receiver, the arrival of a data frame is reported via the MCPS-DATA.indication primitive with the RxRangingCounter parameter reporting the receive timestamp of the RFRAME. If acknowledged transmission is being employed, the TxRangingCounter parameter shall be the transmit timestamp of the Ack, otherwise the TxRangingCounter is invalid.

Devices able to measure distance in a secure and authenticated way are called Secure Ranging DEVices (SRDEV). In SRDEV, the devices are defined as the Verifier (sending the “Challenge”) and the Prover (sending back the “Response” to the Verifier). Secure authenticated ranging is a round-trip-time ranging using a challenge-response protocol in a one-way authentication and/or mutual authentication mechanism.

Secure Ranging capability is enabled in a ranging-capable device (RDEV) with the MCPS-DATA.request primitives Ranging set appropriately and SecurityLevel set to non-zero. In the latter case, Tables defined in Section 6.17 “Secure Authenticated Ranging” apply.

The Standard proposes two types of SRDEV:

• HSRDEV used in HRP UWB PHY: [tbd, STS-related]

• LSRDEV used in LRP UWB PHY: LSRDEV provides additional mechanisms to perform secure authenticated ranging based on distance bounding protocol (distance commitment on payload). Secure authenticated ranging mechanisms are explained in Section 6.17. Proofs and guarantees of the LRP secure authenticated ranging and additional literature references on distance bounding protocols are provided in Annex G.

* + 1. Set-up activities before a ranging exchange

*BV: This is the original clause 6.9.2 paragraph from the 2015 revision. I am thinking we may provide an IE to optionally be used for coordinating DPS, which may still be a useful technique in some circumstances. If we do that, the highlighted text should be modified to refer to the IE as a possible way to perform the coordination:*

The mandatory part of ranging is limited to the generation of timestamp reports during the period that ranging is enabled in an RDEV. It is possible that an RDEV will consume more power when ranging is enabled; therefore, a natural default for an application would be to have ranging disabled. Prior to a two-way ranging exchange, both RDEVs involved in the exchange shall already have ranging enabled. Furthermore, if the optional dynamice preamble selection (DPS) capability is to be used, there shall have been some sort of coordination of preambles prior to the two-way ranging exchange. How this coordination and enabling actually is accomplished is beyond the scope of this standard. It may be perfectly acceptable to accomplish the coordination and enabling with a clock and a look-up table that says what a device should do at a particular time. Because coordination generally involves communication and because the PHYs are designed to achieve communication, it is natural to suggest that the PHY be used for coordination.

* + 1. Finish-up activities after a ranging exchange

*BV: This is the original clause 6.9.3 paragraph from the 2015 revision. One of the functions of this enhancement submission is to add IE to convey the timestamp, or really the reply time, reports. The highlighted text below, should therefore be modified to refer to this new IE as a possible way to do this:*

At the end of a two-way exchange, each device is in possession of a timestamp report. To accomplish anything useful, both of those timestamp reports shall eventually come to be at the same node where computations are performed. How this movement of timestamp reports is accomplished is beyond the scope of this standard. Timestamp reports are just data. Because movement of data involves communication and because the PHYs are designed to achieve communication, it is natural to suggest that the PHY be used for the final consolidation of timestamp reports.

The application is responsible for enabling the ranging mode in the RDEV before a ranging exchange. After a ranging exchange, the application is again responsible for disabling the ranging mode in the RDEV. If the application fails to disable the ranging mode in the RDEV, there will be no algorithmic harm. Ranging mode is fully compatible with other uses of the RDEV, and the only result of leaving ranging enabled when it is not really being used is that the RDEV will generate useless timestamp reports while potentially consuming more power.

* + 1. Managing DPS

*BV: This is clause 6.9.4 from the 2015 revision. The highlighted text below talks about setting up DPS and ranging. We may have new IE to do both of these activities in which case it would be appropriate to modify the highlighted text to refer to these IE, as one way to do this:*

Figure 6-48 shows a suggested message sequence for two-way ranging. The messages represented in the two top dotted boxes are simply suggestions showing how the communications capability of the RDEV can be used to accomplish the ranging setup activities. The messages in the bottom dotted box are suggestions showing how the communications capability of the RDEV can be used to accomplish the ranging finish-up activities.



The top dotted box in Figure 6-48 illustrates the use of a data exchange to effect the coordination of the preambles to be used for a two-way ranging exchange. The coordination of preambles is needed only when using the optional DPS capability of the PHY. If optional DPS is not used, the communication sequence in the top box can be thought of as arranging for the recipient RDEV to become aware that a ranging exchange is desired and that the recipient next higher layer should enable ranging in the recipient PHY. The second from the top dotted box in Figure 6-48 illustrates the use of the MLME-DPS.request, as described in 8.2.15.1, and the MLME-DPS.confirm, as described in 8.2.15.2. Use of these primitives is unique to the optional DPS mode of ranging.

*BV: The highlighted text below talks about changing to longer preamble symbols, however I believe is probably meaning longer sequences (i.e. with more repetitions), which may actually not be necessary. Really this text should probably just have said “changed to the selected preamble”. I suggest we include a DPS IE to select both the preamble code and the sequence length. For SRDEV it may also be accompanied by an IE to select STS parameters.*

Upon the assertion of the MLME-DPS.confirm primitives, as illustrated in Figure 6-48, both of the PHYs have switched from the normal length preamble symbols to long preamble symbols. This is desirable behavior intended to help hide the PHYs’ transmissions from malicious nodes and protect the PHYs from transmissions by malicious nodes. A side effect of this mode is that neither PHYs can communicate with the rest of the network. To prevent the PHYs from becoming lost as a result of this optional behavior, the MAC sublayers on both sides of the link shall initiate timers after sending the frame (for the originator) or receiving the frame (for the recipient). If the timer duration is exceeded before the MAC sublayer receives the MCPS-DATA.comfirm (for the originator) or the MCPS-DATA.indication primitive (for the recipient), then the MAC sublayer shall initiate a MLME-DPS.indication to the next higher layer as described in 8.2.15.3. Not shown in Figure 6-48, one responsibility of the application, if the optional DPS capability is used, is to initiate the MLME-DPS.request primitive on both sides of the ranging link at the completion of the ranging exchange. Most typically, this MLME-DPS.request primitive would be part of the finish-up activities and would have both TxDPSIndex and RxDPSIndex set to zero to return the PHYs to using phyCurrentCode from the PIB. Also not shown in Figure 6-48, another responsibility of the application is to initiate a MLME-DPS.request primitive in response to an MLME-DPS.indication. Most typically, this MLME-DPS.request primitive would have both TxDPSIndex and RxDPSIndex set to zero and return the PHY to using phyCurrentCode from the PIB.

### Ranging and localization methods

#### Preface

The ranging and localization methods supported by RDEV and SRDEV are based on the time-stamping capability. The three main time based techniques for performing ranging and localization are: simple single-sided two-way ranging, described in 6.9.5.2, double-sided two-way ranging, described in 6.9.5.3, and, time difference of arrival, described in 6.9.5.5. Supplementing this, angle-of-arrival (AOA) and received signal strength indication (RSSI) localization techniques are described in 6.9.5.7 and 6.9.5.8.

#### Single-sided two-way ranging

Single-sided two-way ranging (SS-TWR) involves a simple measurement of the round trip delay of a single message from one device to another and a response sent back to the original device.



Treturn

**Figure 7‑1 – single-sided two-way ranging**

The operation of SS-TWR is as shown in Figure 1, where device A initiates the exchange and device B responds to complete the exchange. Each device precisely timestamps the transmission and reception times of the message frames, and so can calculate times *Tround* and *Treply* by simple subtraction. Hence, the resultant time-of-flight, *Tprop*, may be estimated by the equation:

The times *Tround* and *Treply* are measured independently by device A and B using their respective local clocks, which both have some clock offset error *eA* and *eB* from their nominal frequency. Therefore, the resulting time-of-flight estimate has a considerable error that increases as the reply times get larger, see [B3]. However if the receiver of device A (say) has the capability to measure the relative clock offset between itself and the remote device B transmitter, *Coffs*, then it is possible to adjust the reported *Treply* value to improve the accuracy of the time-of-flight, *Tprop*, estimate result by using the equation:

Where the receiver has the capability to measure the relative clock offset this is reported via the RangingTrackingInterval and RangingOffset parameters of the MCPS-DATA.confirm or MCPS-DATA.indication primitives.

Alternatively, where clock offset cannot be measured, double-sided two-way ranging may be used to achieve good accuracy even in the presence of substantial clock offset.

Clearly, when employing SS-TWR, for the time of flight (TOF) to be calculated at device A, it has to know the reply time *Treply* employed by device B. Where *Treply* is determined by device B after its transmission, an additional message is necessary to bring this value to device A. Where *Treply* can be accurately predicted by device B before its transmission, the value can be embedded in the reply message itself. Alternatively if device B has the ability to always reply with sufficiently accurate constant or pre-known reply time, it obviates the need for any transfer of *Treply* as part of the ranging exchange.

The fixed return time constant is added for devices supporting fixed return times as used in two-way round-trip time-of-flight ranging measurements without exchange of timestamps between the two or more (S)RDEV. Two-way round-trip time-of-flight only needs a fixed time constraint for Rx-to-Tx messages on the responding device, this time is determined by Treturn. Treturn is defined as the time between the end of the last received symbol to the beginning of the first transmitted symbol (preamble), usually quantified in an integer number of symbols. Fixing Treturn is equivalent to fixing Treply, their relationship is defined by Treturn+Tframe=Treply, where Tframe is the total duration of the ranging frame. This implies that the Rx-to-Tx turnaround time, which needed to switch the responder device from a receiver into a transmitter, shall be at least smaller than Treturn. Regarding Tx-to-Rx turnaround time, the previous definition in the standard can be used since turnaround time fixes an upper limit to the time that the PHY is ready to receive.

*[BV: Add forward reference to detailed MSC with IE for the various SS-TWR ranging cases.]*

#### Double-sided two-way ranging

Double-sided two-way ranging (DS-TWR), is an extension of the basic single-sided two-way ranging in which two round trip time measurements are used and combined to give the a time of flight result which has a reduced error even for quite long response delays.



**Figure 7‑2 – double-sided two-way ranging**

The operation of DS-TWR is as shown in Figure 2, where device A initiates the first round trip measurement to which device B responds, after which device B initiates the second round trip measurement to which device A responds completing the full DS-TWR exchange. Each device precisely timestamps the transmission and reception times of the messages, and the resultant time-of-flight estimate, *Tprop*, may be calculated using the expression:

Note that this formula does not require symmetric reply times. The typical clock induced error is in the low picosecond range even with 20 ppm crystals, and asymmetric response times. The derivation of this formula and the error calculation are given in IEEE Std 802.15.8™-2017, Annex D clause D2 [XX]

*[BV: XX above should be corrected to reference the bibliography.]*

#### Double-sided two-way ranging with three messages

The four messages of DS-TWR, shown in Figure 2, can be reduced to three messages by using the reply of the first round-trip measurement as the initiator of the second round-trip measurement. This is shown in Figure 3.



**Figure 7‑3 – double-sided two-way ranging with three messages**

#### Time difference of arrival (TDOA)

Time difference of arrival (TDOA) is a technique to locate a mobile device based on the arrival times of a (“blink”) message from the mobile device at a number of fixed (“anchor”) nodes, where the fixed nodes are synchronized in some way so that the arrival times can be compared. For any pair of fixed synchronized nodes the difference in arrival time of a message from a mobile node places that node on a hyperbolic surface. With more fixed nodes receiving the message, locating the mobile sender is a matter of finding the best fit solution that is essentially solving the intersection of the hyperbolic surfaces. By virtue of supporting accurate receive timestamps this standard supports TDOA localization.

Synchronization of fixed nodes can be achieved by a wired distribution of the clock signals. However wireless synchronization schemes are also practical. These may use UWB messages sent between the fixed nodes (and a known / pre-measured TOF) to calculate the relative clock offset and drift between the fixed nodes and use this information to correct the arrival times of the blink messages into a common time base for the TDOA data to be meaningful.

*[BV: I was considering referencing the “multipurpose blink frame” added to the standard by the 802.15.4e amendment, but I notice that the editor preparing the 2015 revision chose not to include this****. For discussion at TG4z session: should we place the text defining the “multipurpose blink frame” into the 802.15.4z amendment and then reference it here?****]*

#### Localization

Two-way ranging gives a distance between two nodes, but does not give the position of either. If a node of fixed known position determines the range R to another mobile node. This essentially places it somewhere on a spherical surface of radius R centered on the fixed position node. To ascertain the 3D position of a mobile node thus requires measuring the range to four fixed nodes and intersecting the resultant spheres. Relative localization is possible with all mobile nodes, depending on their relative geometries, but fixing bearing and true position always requires some fixed nodes, or other information about the system. For TDOA based localization the same is true, fixed known position nodes are needed to solve the TDOA data and locate the mobile device.

Localization thus requires system knowledge and the combination of TWR or TDOA data from multiple nodes in order to resolve the position of a mobile node. This is an upper layer function and beyond the scope of this standard. This standard simply facilitates localization as a result of the capabilities of the PHY to provide accurate timestamps and the capabilities of the MAC to communicate the results to the upper layers.

#### Angle of arrival (AOA)

The angle of arrival (AOA) of a signal can in general only be determined in a device that is equipped with additional antennae and receiver sections able to measure the difference in phase or arrival time of the signals at the antennae and use this with respect to the antenna separation to infer an angle to the sender. An AOA measurement in conjunction with a TOF measurement, essentially gives the location of a remote device as a polar coordinate relative to the local device. Typically, to resolve ambiguities in the solution the results may be combined with compass bearing data, or, successive measurements made during a known movement, captured by an inertial measurement unit (IMU), may be combined to obtain the solution.

Support of AOA is optional for all PHY in this standard, and where supported may be turned on and off using the *macAoaEnable* PIB attribute. Where supported AOA is repotted through the AngleOfArrival parameters of the MCPS-DATA.indication. *[BV: These parameters should also be part of the MCPS-DATA.confirm for the received ACK …. Remember to add this.]*

#### Received signal strength indication (RSSI)

Where accurate two-way ranging has not been performed, or is not supported by the PHY, a measure of RSSI can be used to give a rough indication of the proximity of the sender. The accuracy of RSSI based localization is generally quite poor due to the variation in the RF channel conditions.

Support of RSSI measurement is optional for all PHY in this standard. Where supported RSSI is repotted through the Rssi parameters of the MCPS-DATA.indication

* + 1. The ranging exchange

*BV: This is clause 6.9.5 from the 2015 revision. Will consider what changes are needed given new IE and cipher sequence other changes. Note however that the TVWS also includes ranging and we have to be sure not to break any behaviors needed for TVWS and legacy devices UWB or other.*

The essential core of the ranging exchange is shown in Figure 6-48 starting just below the just after the MLME-DPS exchange. The application is responsible for initiating the MLME-RX-ENABLE.request primitive, as described in 8.2.10.1, with RangingRxControl equal to RANGING\_ON. Once the RDEV has received the MLME-RX-ENABLE.request primitive with RangingRxControl equal to RANGING\_ON, all future RFRAMEs received by the RDEV shall generate timestamp reports until ranging is disabled.

At the initiator, the application is responsible for initiating a MCPS-DATA.request primitive with Ranging equal to ALL\_RANGING. Upon receipt of a MCPS-DATA.request primitive with Ranging equal to ALL\_RANGING, RDEV shall generate timestamp reports for all RFRAMEs after the transmit frame is transmitted. The timestamp reports will continue until ranging is disabled. The TX-to-RX turnaround enabling the originator to receive the Ack frame is necessary and is not shown in Figure 6-48. This turnaround is the normal turnaround that is done for any exchange expecting an acknowledgment. The turnaround happens without any action required by the originator next higher layer. Timestamp reports are generated to the next higher layer independent of the state of the AR field in the MAC header of received RFRAMEs.

As shown in Figure 6-48, the first timestamp report to the originator next higher layer shall come back as elements of the MCPS-DATA.confirm. The first timestamp report to the recipient next higher layer shall come back as elements of the MCPS-DATA.indication primitive. All subsequent timestamp reports on either side of the link shall come back as elements of MCPS-DATA.indication primitives. The potential additional MCPS-DATA.indication primitives that would be due to unexpected stray RFRAMEs are not shown in Figure 6-48 for simplicity. The timestamp reports due to any strays shall continue until ranging is disabled. The reporting of timestamps for a stream of “strays” is the behavior that enables the RDEV to be used as an infrastructure RDEVs in one-way ranging applications. One-way ranging is described in “Applications of IEEE Std 802.15.4” [B3].

For non-TVWS RDEVs, the timestamp is defined in 16.7. Use of nonzero timestamp reports is limited to RDEVs. Only devices that have *phyRanging* set to TRUE shall return a nonzero timestamp report to a next higher layer.

For TVWS RDEVs, the Timestamp IE, 7.4.4.26, and the Timestamp Difference IE, 7.4.4.27, are provided for exchanging timing information between TVWS RDEVs to support the ranging feature.

***Insert new sub-clauses 6.9.6 and 6.9.7 (given below) to describe Ranging and localization methods and specify new procedures for achieving these in a standardized way:***

### Ranging procedures

#### General ranging procedures

The layers above the MAC are responsible for the decision to participate in a two-way ranging exchange between a pair of devices and for the final calculation of the resulting range. The ranging procedures appropriate to the ranging methods described in 6.9.5 are defined in the clauses below using message sequence charts. The use and support of any of these ranging procedures and associated IE is optional.

Irrespective of whether the timestamps are coming from an RDEV or an SRDEV the same procedures apply.

*[BV: I plan to review and consider whether an SRDEV need any additional text. For example in the HRP UWB PHY where the device is SRDEV, the decision to respond or the response may also depend on some validation of the STS being used to determine the RX timestamp.]*

#### Control of ranging and the transfer of timestamps

Information elements are employed to control two-way ranging and transfer ranging data between the two RDEV participating in a ranging exchange. With reference to the ranging methods defined in 6.9.5.2 and 6.9.5.3, to complete the calculation of the time-of-flight (TOF) between two RDEV, participating in a ranging exchange, it is necessary to combine measurements made by both devices. That is, one device will need to transfer its timestamp measurements to the other. Information elements are specified to provide a mechanism to control two-way ranging and support the transfer of ranging information between the devices participating in the ranging exchange. Table 1 lists these information elements, and references to the clause where the information element usage is specified.

**Table 1 – information elements for ranging**

|  |  |  |
| --- | --- | --- |
| **IE Name** | **Acronym** | **Sub-clause** |
| Ranging Request Reply Time IE | RRRT IE | 7.4.2.1 |
| Ranging Reply Time Instantaneous IE | RRTI IE | 7.4.2.2 |
| Ranging Reply Time Deferred IE | RRTD IE | 7.4.2.3 |
| Ranging Preferred Reply Time IE | RPRT IE | 7.4.2.4 |
| Ranging Control Double-sided TWR IE | RCDT IE | 7.4.2.5 |
| Ranging Round Trip Measurement IE | RRTM IE | 7.4.2.6 |
| Ranging Time-of-Flight IE | RTOF IE | 7.4.2.7 |

#### Ranging procedure for SS-TWR with deferred reply time result

For a single-sided TWR with a deferred reply time result, the ranging exchange is initiated by a ranging frame including the RRRT IE requesting the ranging reply time information. The replying ranging frame completes the round trip measurement and the MCPS-DATA.confirm gives the initiating side timestamps that define the round trip time. At the responding side, the MCPS-DATA.indication supplies the responding side timestamps that define the reply time for the round trip measurement. This reply time is communicated to the initiating side in the RRTD IE carried by the subsequent message. Figure 4 shows the message sequence chart for this exchange. At the point labelled (R) the initiating end has sufficient information to calculate the range between the two devices according to the formula given in 6.9.5.2.

*[BV: This MSC figure and all others denote the PHY as “UWB PHY” but to be more general it probably should just say “RDEV PHY”. The editor/contributor should change this during integration into the standard.]*



**Figure 7‑4 – message sequence chart for single-sided TWR** **with deferred reply time result**

#### Ranging procedure for SS-TWR with embedded reply time result

For a single single-sided TWR with an embedded reply time result, the ranging exchange is initiated by a ranging frame including the RRRT IE requesting the ranging reply time information. The replying ranging frame completes the round trip measurement, and the MCPS-DATA.confirm gives the initiating side timestamps that define the round trip time. At the responding side, the MCPS-DATA.indication supplies the responding side timestamps that define the reply time for the round trip measurement. This reply time is communicated to the initiating side in the RRTI IE carried by the ACK message. Figure 5 shows the message sequence chart for this exchange. At the point labelled (R) the initiating end has sufficient information to calculate the range between the two devices according to the formula given in 6.9.5.2.



**Figure 7‑5 – message sequence chart for single-sided TWR with embedded reply time result**

Even though a device is capable of generating a Ranging Reply Time Instantaneous IE, depending on the timing required for the ACK transmission and the time required to calculate the timestamp of the received ranging message, it may not be possible for the responding device to have the RRTI IE value available in time for the ACK message. The Ranging Preferred Reply Time IE provides a mechanism for an RRTI capable device to indicate how long it needs to prepare the frame with the RRTI. When this time is known, the ranging initiating device then does not request an ACK but rather expects a response message after the RPRT IE specified time. Figure 6 shows the message sequence chart for this exchange. The communication of the RPRT IE may happen at any convenient time before the ranging exchange. Again at the point labelled (R) the initiating end has sufficient information to calculate the range between the two devices according to the formula given in 6.9.5.2.



**Figure 7‑6 – message sequence chart for single-sided TWR after RPRT IE**

#### Ranging procedure for DS-TWR with deferred timestamp information

Double-sided two-way ranging essentially involves completing single sided ranging exchanges initiated at either end and combining the results. The DS-TWR exchange is initiated by a ranging data frame carrying a Ranging Control Double-sided TWR IE (RCDT IE) with control field set according to Table 2. This frame and its acknowledgement define the first round trip measurement, while the RCDT IE delivery in the MCPS-DATA.indication tells the next higher layer to initiate the second round trip measurement of the exchange by the sending of a data frame in the other direction. This data frame includes Ranging Request Reply Time IE and an RCDT IE with control field set according to Table 2 to indicate this is the continuation of the exchange and requesting the result of the first round trip measurement. The acknowledgement to this message completes the second round trip measurement. A subsequent message from the initiator conveys the first round trip time measurement in an RRTM IE and the reply time for the second first round trip time measurement an RRTD IE. Figure 7 shows the message sequence chart for this exchange. At the point labelled (R) the responding end has sufficient information to calculate the range between the two devices according to the formula given in 6.9.5.3. The subsequent reporting of the ranging result the initiating end, in the RTOF IE, shall depend on the value of the control field in the initiating RCDT IE.



**Figure 7‑7 – message sequence chart for DS-TWR with deferred reply time result**

#### Ranging procedure for DS-TWR with embedded timestamp information

To achieve the three message DS-TWR exchange described in Figure 3 requires that the initiating end is able to embed the reply time as part of completing the second round trip measurement and additionally that the parties have previously exchanged Ranging Preferred Reply Time IE to communicate the reply times that each will use. These reply times do not have to be the same. When the reply times are known it allows the receiver to be turned at the appropriate time that the response is expected, saving power compared to turning the receiver on immediately after the transmission. With reference to the message sequence chart of Figure 8, the DS-TWR is initiated by a ranging data frame carrying a Ranging Control Double-sided TWR IE (RCDT IE) with control field set according to Table 2 to indicate, in this instance, that the initiating end does not require a report of the ranging result. The responding side completes the first round trip measurement and initiates the second with ranging data frame carrying a Ranging Control Double-sided TWR IE (RCDT IE) with control field set according to Table 2 to indicate this is the continuation of the exchange and requesting the result of the first round trip measurement and also carrying a Ranging Request Reply Time IE to request the reply time for the second round trip measurement. The original initiator completes the exchange by sending a final ranging data frame carrying the first round trip time measurement in an RRTM IE and the reply time of this second first round trip measurement in an RRTI IE.



**Figure 7‑8 – message sequence chart for DS-TWR with three messages**

At the point labelled (R) the responding end has sufficient information to calculate the range between the two devices according to the formula given in 6.9.5.3. Where the initiator of the ranging exchange wants the result this shall be requested in the control field of the initial frame’s RCDT IE, and the responding end shall convey the Ranging Time-of-Flight IE in a subsequent message as is done at the end of the exchange shown in Figure 7.

*[BV: I plan to also cover those conditions where there is a fixed response time and no need for over-the-air data communications.]*

#### Ranging procedure with fixed response (return) time



Figure 7‑9message sequence chart for ranging with fixed response (return) time

#### Other procedures for coordinating RDEV and SRDEV

For successful interworking of HSRDEV, where an STS is being employed, the transmitter and receiver need to be aligned with respect to the key and nonce counter values used in the transmitter to generate the STS and in the receiver to correlate with the received sequence.

The secure private data communication capability of this standard may be used to transfer the key and nonce counter values. To support this, the xxxx IE is defined, see x.x.x. *[Need to define an appropriate IE(s) for communicating the key and synchronizing the nonce for secure ranging.]*

As described in 6.9.4, when using DPS the RDEV need to coordinate the preamble codes they are going to employ. Here again secure private data communication capability of this standard may be used for this. To support this, the xxxx IE is defined, see x.x.x. *[Need to define an appropriate IE to coordinate the use of DPS.]*

### Secure authenticated ranging

Secure authenticated ranging is a round-trip-time ranging using a challenge-response one-way authentication and/or mutual authentication mechanism.

Secure authenticated ranging uses the MAC sublayer providing the security services defined in Clause 9. Secure ranging is provably secure in LRP UWB Base and Dual-Frequency Modes as defined in Clause 19. Secure authenticated ranging provides the highest security guarantees as defined by the Security Levels of the MAC sublayer in Table 9-6.

Secure authenticated ranging uses data frames as defined in 7.3.2. When specified in this clause as secured, data frames used for secure authenticated ranging are secured at security level 1, 2 or 3.

A device performing secure authenticated ranging with one-way authentication or mutual authentication shall have the macSecurityEnabled set to TRUE and shall be disabled otherwise. The secure ranging devices shall provide cryptographic transformations on incoming and outgoing frames using information in the PIB attributes associated with security services defined in Clause 9.

**[Comment<1>:** Is there need DefineIEto indicate one-way vs. mutual authentication**]**

**6.17.1 Secure ranging with one-way authentication**

This subclause describes the two-way message exchange based on AES CCM\* security services in 9.1 used to achieve secure ranging with one-way authentication.



Figure 1- Secure ranging with one-way authentication

**6.17.1.1 VChallenge**

VChallenge is a fresh random number of 32, 64 or 128 bits corresponding to the chosen Security Level. The generation mechanism is outside the scope of this standard.

|  |  |
| --- | --- |
| **VChallenge** | **Length (bits)** |
| VChallenge32 | 32 |
| VChallenge64 | 64 |
| VChallenge128 | 128 |

The Security Level shall be set to 0 in the Security Control field of the Auxiliary Security Header. This indicates that VChallenge is neither authenticated, nor encrypted data, i.e., no CCM\* transformation is performed on the VChallenge.

**6.17.1.2 PResponse**

PResponse is a secured frame which contains the received VChallenge and its MIC (Message Integrity Code) computed using the security service of data authenticity as defined in Table 9-4. Table X defines the *a*data to be used for the CCM\* authentication transformation to compute the *c* data. VChallenge shall be the Unsecured Private Payload field defined in Table 9.3.

|  |  |  |  |
| --- | --- | --- | --- |
| Security level | *a* data | *m* data | *c* data |
| 0 | Not applicable | Not applicable | Not applicable |
| 1 | MHR || VChallenge32 | None | MIC-32 |
| 2 | MHR || VChallenge64 | None | MIC-64 |
| 3 | MHR || VChallenge128 | None | MIC-128 |

NOTE—The MHR contains the Auxiliary Security Header field, as defined in 7.2

**6.17.2 Secure ranging with mutual authentication**

This subclause describes the three-way message exchange based on AES CCM\* security services in 9.1 in order to achieve secure ranging with mutual authentication.



Figure 2 Secure ranging with mutual authentication

**6.17.2.1 VChallenge**

VChallenge is a fresh random number of 32, 64 or 128 bits corresponding to the chosen Security Level. The generation mechanism is outside the scope of this standard.

**6.17.2.2 PResponseChallenge**

PResponseChallenge is a secured frame which contains the received VChallenge from the Verifier device and a freshly generated random number PChallenge by the Prover device and their MIC computed using the security service of data authenticity as defined in Table 9-4.

PChallenge is a fresh random number of 32, 64 or 128 bits generated by the Prover device according to the chosen Security Level.

Table X defines the *a*data to be used for the CCM\* authentication transformation to compute the *c* data of the PResponseChallenge message. The VChallenge and PChallenge shall be the Unsecured Private Payload field defined in Table 9.3.

|  |  |  |  |
| --- | --- | --- | --- |
| Security level | *a* data | *m* data | *c* data |
| 0 | Not applicable | Not applicable | Not applicable |
| 1 | MHR || PChallenge32 || VChallenge32 | None | MIC-32 |
| 2 | MHR || PChallenge64 || VChallenge64 | None | MIC-64 |
| 3 | MHR || PChallenge128 || VChallenge128 | None | MIC-128 |

NOTE—The MHR contains the Auxiliary Security Header field, as defined in 7.2

**6.17.2.4 VResponse**

VResponse is a secured frame which contains the received VChallenge and PChallenge from the Prover device and their MIC computed using the security service of data authenticity as defined in Table 9-4.

Table X defines the *a*data to be used for the CCM\* transformation to compute the *c* data of the VResponse. The VChallenge and PChallenge shall be the Unsecured Private Payload field defined in Table 9.3.

|  |  |  |  |
| --- | --- | --- | --- |
| Security level | *a* data | *m* data | *c* data |
| 0 | Not applicable | Not applicable | Not applicable |
| 1 | MHR || VChallenge32 || PChallenge32 | None | MIC-32 |
| 2 | MHR || VChallenge64 || PChallenge64 | None | MIC-64 |
| 3 | MHR || VChallenge128 || PChallenge128 | None | MIC-128 |

NOTE—The MHR contains the Auxiliary Security Header field, as defined in 7.2

**6.17.3 Secure ranging with tolerance of bit errors**

This subclause describes the two-way message exchange for secure ranging which allows tolerance of bit errors during the ranging.

This type of secure ranging assumes that VChallenge and PChallenge are exchanged between the Verifier device and Prover device before the secure ranging takes place or after the secure ranging has taken place.



Knowledge of VChallenge and PChallenge by the Verifier device and Prover device prior to the two-way ranging or after the two-way ranging allows the upper application layer to verify the validity of the VChallenge and PChallenge even if bit errors have occurred during the transmission. Annex G provides informative information on the sizes of VChallenge and PChallenge in order to achieve the desired Security Level.

VChallenge and PChallenge can be securely exchanged between the Verifier device and Prover device by using the security services in Clause 9, out-of-band (OOB) communication or other means by the upper application layers.

**6.17.3.1 VChallenge**

VChallenge is a fresh random number of a given amount of bits. Annex G provides examples on how to compute the amount of bits to be used based on the required Security Level. The generation mechanism is outside the scope of this standard.

**6.17.3.2 PChallenge**

PChallenge is a fresh random number of a given amount of bits. Annex G provides examples on how to compute the amount of bits to be used based on the required Security Level. The generation mechanism is outside the scope of this standard.

**6.17.4 Distance commitment**

Distance commitment ensures that the data of the PSDU carrying the nonce and MIC of the MAC payload is decoded at the measured distance by the earliest path(s). This is essential to secure authenticated ranging and provable security as defined in Annex G.

Figure 3 illustrate the distance commitment. Channel state information (channel impulse response) is available after the SHR. The earliest path(s) are detected from the channel state information. During reception of PSDU only the “earliest path(s)” portion of the received signal shall be used for data decoding.

**[Comment<2>:** Provide more precise definition of “earliest path(s)” in order to ensure strict security guarantees between different chip vendors. This would need to be formulated in Annex G as normative.**]**



Figure 3 Distance commitment

**6.17.5 Protocol verification**

Verification for success or failure is performed by the Verifier in the one-way authentication and by both the Verifier and the Prover in the mutual authentication.

The verification procedure of secure authenticated ranging consists of bit-wise matching the received nonces and computed MIC.

**[Comment<3>:** Include a section on the type of shared keys to be used. Especially, mandate the use of only link keys (i.e., pair-wise shared keys) between devices and not group keys. Keys shared by a group of devices can be subject to insider attacks, i.e., the attacker can impersonate as an innocent device, associate with the group, thereby obtain the group key for launching the forgery attacks. Can be stated as requirement when using Secure authenticated ranging, or as a strong recommendation TBD]

# MAC frame formats

## Device extended address

## General MAC frame format

## Format of individual frame types

## IEs

### xxxxx

#### Ranging Request Reply Time IE

The Ranging Request Reply Time IE (RRRT IE) is used as part of a ranging exchange to request a ranging reply time from the remote device participating in the ranging exchange. The Ranging Request Reply Time IE has a zero length Content field. The procedures for using the RRRT IE are defined in 6.9.7.

#### Ranging Reply Time Instantaneous IE

The Ranging Reply Time Instantaneous IE (RRTI IE) content shall be time difference between the receive time of most recently received RFRAME and the transmit time of the RFRAME containing the IE. The reference for these time values is the RMARKER. The Ranging Reply Time Instantaneous IE is appropriate for use where the device is able to accurately pre-determine the transmission time of the frame containing the IE and complete the calculations to timestamp the last received RFRAME in time to calculate and insert this RRTI IE into the transmitted frame. The content field of the Ranging Reply Time Instantaneous IE shall be formatted as shown in Figure 9. The units of time are defined in 10.4.1. The procedures for using the RRTI IE are defined in 6.9.7.

|  |
| --- |
| **Octets : 4** |
| RX to TX Reply Time |

**Figure 7‑1 – Ranging Reply Time Instantaneous IE Content field format**

#### Ranging Reply Time Deferred IE

The Ranging Reply Time Deferred IE (RRTD IE) content shall be time difference between the receive time of most recently received RFRAME and the transmit time of the responding RFRAME transmitted, sent most recently before the frame containing this IE. The reference for these time values is the RMARKER. The Ranging Reply Time Deferred IE is employed as part of completing two-way ranging exchanges, and used in the case where the device cannot determine the reply time until after the reply has been sent, and in this case the RRTD IE carries the reply time in a subsequent frame. The content field of the Ranging Reply Time Deferred IE shall be formatted as shown in Figure 10. The units of time are defined in 10.4.1. The procedures for using the RRTD IE are defined in 6.9.7.

|  |
| --- |
| **Octets : 4** |
| RX to TX Reply Time |

**Figure 7‑2 – Ranging Reply Time Deferred IE Content field format**

#### Ranging Preferred Reply Time IE

The Ranging Preferred Reply Time IE is sent by a device to communicate its ability to send a ranging response that can employ the RRTI IE and it communicates its preferred reply time for this. When this is known it can be used to modify the ranging exchange to minimize the number of messages needed for a ranging measurement and thus save power, see Figure 6 and its associated description in 6.9.7.4 for details. The content field of the Ranging Preferred Reply Time IE shall be formatted as shown in Figure 11. The units of time are defined in 10.4.1. While these units are very precise an actual implementation may have some quantization in the reply times that it can support. The value reported in the RRTI IE or RRTD IE shall be the actual resultant reply time of the appropriate individual ranging reply.

|  |
| --- |
| **Octets : 4** |
| Preferred Reply Time |

**Figure 7‑3 – Ranging Preferred Reply Time IE Content field format**

The Ranging Preferred Reply Time IE is applicable in both single-sided and double-sided two-way ranging exchanges. When the reply time is known, it can be used to delay turning on the receiver until the expected reply time which gives a power saving.

#### Ranging Control Double-sided TWR IE

The Ranging Control Double-sided TWR IE (RCDT IE) is used to control the double-sided two-way ranging exchange with the remote device. The content field of the Ranging Control Double-sided Ranging IE shall be the formatted as shown in Figure 12. The Control Info shall have one of the values defined in Table 1. The procedures for using the RCDT IE are defined in 6.9.7.

|  |
| --- |
| **Octets : 1** |
| Control Info |

**Figure 7‑4 – Ranging Control Double-sided TWR IE Content field format**

**Table 2 – values of the Control Info field in the Ranging Control Double-sided TWR IE**

|  |  |
| --- | --- |
| **Control Info value** | **Meaning** |
| 0 | This frame is initiating DS-TWR and indicates that the initiating end does not require the ranging result. |
| 1 | This frame is initiating DS-TWR and requesting that the ranging result is sent back at end of exchange |
| 2 | This frame is continuing the DS-TWR, forming the request for the 2nd TX-to-RX round trip measurement |

#### Ranging Round Trip Measurement IE

The Ranging Round Trip Measurement IE (RRTM IE) content shall be time difference between the transmit time of the RFRAME initiating a round trip measurement and the receive time of the response RFRAME that completes a round trip measurement. The reference for these time values is the RMARKER. This IE is employed as part of completing a double-sided two-way ranging exchange. The content field of the Ranging Round Trip Measurement IE shall be formatted as shown in Figure 13. The units of time are defined in 10.4.1. The procedures for using the RRTM IE are defined in 6.9.7.

|  |
| --- |
| **Octets : 4** |
| TX to RX round trip time |

**Figure 7‑5 – Ranging Round Trip Measurement IE Content field format**

#### Ranging Time-of-Flight IE

The Ranging Time-of-Flight IE (RTOF IE) is used after a double-sided two-way ranging exchange to communicate the resultant time-of-flight estimate to the far end if this is requested. The content field of the Ranging Time-of-Flight IE shall be formatted as shown in Figure 13. The units of time are defined in 10.4.1. The procedures for using the RTOF IE are defined in 6.9.7.

|  |
| --- |
| **Octets : 4** |
| TX to RX round trip time |

**Figure 7‑6 – Ranging Round Trip Measurement IE Content field format**

## MAC commands

**BEYOND HERE I HAVE NOT REVIEWED/REVISED YET SO PLEASE IGNORE**

# MAC services

## MAC data service

### MCPS-DATA.confirm

The MCPS-DATA.confirm primitive reports the results of a request to transfer data to another device.

The semantics of the MCPS-DATA.confirm primitive are as follows:

MCPS-DATA.confirm (

MsduHandle,

Timestamp,

RangingReceived,

~~RangingCounterStart~~ TxRangingCounter,

~~RangingCounterStop~~ RxRangingCounter,

RangingTrackingInterval,

RangingOffset,

RangingFom,

NumBackoffs,

AckPayload,

Status

)

The primitive parameters are defined in Table 8-76.

**Table 8-76—MCPS-DATA.confirm parameters**

*[The following are out of order with respect to the clauses in the standard, but are new items captured for inclusion into the 4z amendment text]*

# Definitions, acronyms, and abbreviations

## Definitions

## Acronyms and abbreviations

*Add the following new acronyms.*

AOA angle of arrival

STS scrambled timestamp sequence

TOF time of flight

*Place the text below in a new section, [and remove any similar place holding clauses on positioning or ranging, e.g. MAC work items doc 802.15-15-0074-00-0008 nominates a section “5.1.8 Ranging” and the P802.15.8\_D0.8 draft has an empty clause “13 – Relative positioning”].*

# Relative positioning and localization

## Overview

## Service access points for message time stamps

# MAC services

*The items below are just place holders of note for the editor and authors of the MAC clauses. They are part of the API to/from the ranging procedures captured above and so need to be part of the MAC service layer API definition. This is not complete, as we need to fully define the passing IE from MAC to upper layers and vice-versa, and we may will need other PIB values.*

## MAC data service

### MCPS-DATA.request

*The following items are referred to in the text above and so need to be included in the parameters of the MCPS-DATA.request primitive. A larger set of parameters will be present in the complete table. The editor should integrate these.*

Table 3 –MCPS-DATA.request parameters

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
| AckTX | Boolean | FALSE, TRUE | TRUE if acknowledged transmission is used,  FALSE otherwise. |
| Ranging | Boolean | FALSE, TRUE | TRUE if ranging bit in PHR is to be set,  FALSE otherwise. |
| IeList | Set if IEs as described in Table 1 |  | Determines/supplies the IEs to be sent, including:  RRRT IE, RRTD IE, RPRT IE, RRTM IE, RCDT IE and RTOF IE |
| RequestRrtiTx | Boolean |  | This parameter requests that the device inserts an RRTI IE in the sent data frame. If the MCPS-DATA.request is early enough the data frame shall be sent at the configured *macRngRrtiTime* otherwise shall be sent as soon as possible thereafter. |

### MCPS-DATA.confirm

*The following items are referred to in the text above and so need to be included in the parameters of the MCPS-DATA.confirm primitive. A larger set of parameters will be present in the complete table. The editor should integrate these.*

Table 4 –MCPS-DATA.confirm parameters

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
| TxRangingCounter | Unsigned Integer |  | The timestamp of the transmitted data frame |
| RxRangingCounter | Unsigned Integer |  | For an acknowledged transmission this is the timestamp of the received acknowledgement frame. For a non-acknowledged transmission this parameter is invalid. |
| IeList | IEs received in the ACK |  | For an acknowledged transmission this reports the IEs received in the ACK including: RRTI IE |
| TxRrtiValue | Unsigned Integer |  | This reports the value sent in the RRTI IE where this was requested by the RequestRrtiTx parameter of the MCPS-DATA.request. |
| AoaAzimuth | Float | -π to +π | For an acknowledged transmission this is the AOA of the received signal in azimuth measured in radians, relative to some device specific axis defined by its antenna arrangement or orientation. This parameter is valid only when the AoaPresent parameter is either AZIMUTH or BOTH. |
| AoaElevation | Float | -π to +π | For an acknowledged transmission this is the AOA of the received signal AOA of the received signal in elevation measured in radians. This parameter is valid only when the AoaPresent parameter is either ELEVATION or BOTH. |
| AoaPresent | Enumeration | NONE,  BOTH,  AZIMUTH,  ELEVATION | Indicates validity of AoaAzimuth and AoaElevation parameter. For a non-acknowledged transmission or where AOA is not supported this parameter value shall be NONE. |
| Rssi | Integer | 0x00–0xff | For an acknowledged transmission this reports the received signal strength for the ACK frame. This is a measure of the RF power level at the antenna based on the gain setting in the RX chain and the measured signal level in the channel. For the UWB PHY the RSSI value is measured during the frame Preamble and locked when a valid SFD is detected. A value of zero indicates that RSSI measurement is not supported or was not measured for this frame. |

### MCPS-DATA.indication

*The following items are referred to in the text above and so need to be included in the parameters of the MCPS-DATA.indication primitive. A larger set of parameters will be present in the complete table. The editor should integrate these.*

Table 5 –MCPS-DATA.indication parameters

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
| RxRangingCounter | Unsigned Integer |  | The timestamp of the received data frame |
| TxRangingCounter | Unsigned Integer |  | If the received frame had the AR bit set, then this is the timestamp of the transmitted acknowledgement frame, otherwise this parameter is invalid. |
| IeList | Set if IEs as described in Table 1 |  | Reports the IEs received including:  RRRT IE, RRTD IE, RRTI IE, RPRT IE, RRTM IE, RCDT IE and RTOF IE |
| AoaAzimuth | Float | -π to +π | AOA of the received signal in azimuth measured in radians, relative to some device specific axis defined by its antenna arrangement or orientation. This parameter is valid only when the AoaPresent parameter is either AZIMUTH or BOTH. |
| AoaElevation | Float | -π to +π | AOA of the received signal in elevation measured in radians. This parameter is valid only when the AoaPresent parameter is either ELEVATION or BOTH. |
| AoaPresent | Enumeration | NONE,  BOTH,  AZIMUTH,  ELEVATION | Indicates validity of AoaAzimuth and AoaElevation parameter. Where AOA is not supported this parameter value shall be NONE. |
| Rssi | Integer | 0x00–0xff | The received signal strength for received frame. This is a measure of the RF power level at the antenna based on the gain setting in the RX chain and the measured signal level in the channel. For the UWB PHY the RSSI value is measured during the frame Preamble and locked when a valid SFD is detected. A value of zero indicates that RSSI measurement is not supported or was not measured for this frame. |

## PIB

*The following items are referred to in the text above and so need to be included in the PIB. A larger set of parameters will be present in the complete table. The editor should integrate these.*

**Table 6 – PIB attributes**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Attribute** | **Type** | **Range** | **Description** | **Default** |
| *phyTxRmarkerOffset* | Unsigned Integer |  | The propagation time from the internal transmit timestamp to the transmit antenna. The units of this are defined in 10.4.1. The device adds this offset to its internal transmit timestamp to get the reported TxRangingCounter value. |  |
| *phyRxRmarkerOffset* | Unsigned Integer |  | The propagation time from the receive antenna to the internal receiver timestamp. The units of this are defined in 10.4.1. The device subtracts this offset from its internal receive timestamp to get the reported RxRangingCounter value. |  |
| *macRngAckRrtiSupport* | Boolean | READ ONLY | Read only value indicating whether the device is able to generate an RRTI IE within the *ACK response time* and insert it into a ranging ACK frame.  *[I am not sure of the response time for the enhanced ACK that may be used to carry the IE, or whether there is a MAC constant or PIB value to quote here to cover this?]* |  |
| *macRngAckRrtiEnable* | Boolean |  | When set the MAC shall automatically generate and insert an RRTI IE in a ranging ACK frame, where the RFRAME being acknowledged carried an RRRT IE and where *macRngAckRrtiSupport* indicates that the device is capable of doing this. |  |
| *macRngMinRrtiTime* | Unsigned Integer | READ ONLY | This is a read only value reporting the minimum RX to TX response time that the device supports for inserting an RRTI IE into a MAC data frame. The units of this are defined in 10.4.1. A value of zero shall indicate that the device cannot support RRTI insertion, i.e. so the upper layers know to employ an RRTD IE in the ranging exchanges. |  |
| *macRngRrtiTime* | Unsigned Integer |  | This sets the desired RX-to-TX response time for the device to use when inserting an RRTI IE into a MAC data frame. The units of this are defined in 10.4.1. The value set should take account of the *macRngMinRrtiTime* and any upper layer delays in initiating transmission, be reflected in the preferred response time indicated via RPRT IE exchanges. |  |
| *macAoaEnable* | Boolean |  | Where AOA is supported by the PHY receiver this will enable/disable the measurement of AOA for received frames. Where AOA measurement is not needed for every frame some power saving may be made by disabling the AOA measurement via this attribute. |  |