**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | Resolution proposals for comments #11-16, 19, 20, 23, 24, 26, 156 | |
| Date Submitted | October 2023 | |
| Sources | Alex Krebs, Jinjing Jiang (Apple) |  |
| Re: |  | |
| Abstract |  | |
| Purpose | To propose resolution to NBA-UWB MMS comments for “P802.15.4ab™/D (pre-ballot) B Draft Standard for Low-Rate Wireless Networks” | |
| Notice | This document does not represent the agreed views of the IEEE 802.15 Working Group or IEEE 802.15.4ab Task Group. It represents only the views of the participants listed in the “Sources” field above.It is offered as a basis for discussion and is not binding on the contributing individuals. The material in this document is subject to change in form and content after further study. The contributors reserve the right to add, amend or withdraw material contained herein. | |

[1 Resolution proposals 3](#_Toc149662230)

[CID #11 Revise 3](#_Toc149662231)

[CID #12 Revise 4](#_Toc149662232)

[CID #13 Accept/Revise 6](#_Toc149662233)

[CID #14 Revise 7](#_Toc149662234)

[CID #15 Revise 8](#_Toc149662235)

[CID #16 Reject 9](#_Toc149662236)

[CID #19 Defer 10](#_Toc149662237)

[CID #20 Revise 11](#_Toc149662238)

[CID #23 Revise 12](#_Toc149662239)

[CID #24 Revise 13](#_Toc149662240)

[CID #26 Reject 14](#_Toc149662241)

[CID #156 Revise 15](#_Toc149662242)

[2 Reassignment proposals 16](#_Toc149662243)

[CID #17 Reassign to Rojan 16](#_Toc149662244)

[CID #237, #238 Reassign to Rojan 17](#_Toc149662245)

# Resolution proposals

CID #11 Revise

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Idx #** | **Cat.** | **Pg.** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** |
| Li-Hsiang Sun | 11 | Technical | 35 | 10.35.3.2.1 | 9 | what is this slot number used for? | specify related procedure |

Reference: A document with text on it

Description automatically generated

Discussion: Initialization slot numbering currently not needed for the NBA-UWB MMS MAC.

Proposed resolution: Revise: Have editor remove paragraph p.35, l.9-10 (as highlighted).

CID #12 Revise

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Idx #** | **Category** | **Pg.** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** |
| Li-Hsiang Sun | 12 | Technical | 35 | 10.35.3.3 | 24 | For 1 to many case using CAP, What is IdentityResolvingKey used in ADV\_POLL and ADV\_RESP? How does initiator selects one of the responders if all their RPA hash the same (corresponding to the RPA hash of ADV\_POLL)? | clarify the addressing in this case |

Reference: A document with text and numbers

Description automatically generated

Discussion: Agree that we need to clearly define the Responder Address calculation and clarify the existing subsection on private address calculation.

Proposed resolution: Revise. Change p.49, l. 13-32, subsection 10.35.9.2.1 as follows:

**10.35.9.2.1 Private addresses**

To impede tracking of HRP-ARDEVs, resolvable private addresses (RPA)s are used by initiator and responder devices. To generate a private address, every device shall use a 128-bit identity resolving key (IRK) and every initiator shall be equipped with a cryptographically secure pseudo random number generator (CSPRNG). The initiator shall generate and communicate a 3-octet output RPA\_prand of the CSPRNG in the first message of every ranging block (in the POLL message).

A 3-octet RPA\_hash is then computed using an IRK and the initiator’s RPA\_prand as follows:

RPA\_hash = AES-128-ECB(key=IdentityResolvingKey, data=RPA\_prand]) % 224

where AES-128-ECB is defined in [2] (using MSB-wise zero-padded inputs) and % is the integer modulo operator. RPA\_hash shall then be used by the device as it’s source RPA for its own packet transmissions.

In order to resolve an RPA of an incoming packet the receiving device shall compute RPA\_hash using the IRK of an assumed sender device and the RPA\_prand communicated by the initiator at the beginning of the ranging round. If the result of the computation matches the received RPA, the incoming packet shall be marked as resolved. Otherwise, the incoming packet shall be marked as unresolved. If marked unresolved, the receiving device may retry the RPA\_hash using other possible IRKs until the incoming packet is marked as resolved, or the receiving device’s list of possible IRKs is exhausted.

The generation and mutual exchange of IRKs among initiator(s) and responder(s) is out of scope of this standard and may be conducted using higher layer methods. Note that devices may carry multiple IRKs to, e.g., assert privacy among multiple responders and/or ranging sessions. Again, methods for association and assignment of IRKs is not defined in this standard, but may be carried out using higher layer methods.

Change in subsection "**10.35.9.11 ADV-CONF**" on p.59, l. 5 as follows:

The RPA\_hash field shall be set as specified in 10.35.9.2.1. Note that if private addresses are used, the IRK used in the RPA\_hash computation shall be the initiator’s IRK for the one-to-many session, and each Responder Address in Message Content shall represent an eligible responder's RPA hash generated using the initiator's RPA\_prand along with that responder's IRK.

Change in subsection "**10.35.9.12 POLL (One-to-many)**" on p.59, l. 15 as follows:

The RPA\_hash and RPA\_prand fields shall be set as specified in 10.35.9.2.1. Note that if private addresses are used, the IRK used in the RPA\_hash computation shall be the initiator’s IRK for the one-to-many session, and each Responder Address in Message Content shall represent an eligible responder's RPA hash generated using the initiator's RPA\_prand along with that responder's IRK.

CID #13 Accept/Revise

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Idx #** | **Cat.** | **Pg.** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** |
| Li-Hsiang Sun | 13 | Technical | 41 | 10.35.5 | 8 | "The responder may start transmitting a first RIF fragment at RpRifOffset into the ranging phase if no RSF fragments were transmitted,"  should be RpRifOffset+600RSTU | as in comment |

Reference:A document with text and numbers

Description automatically generated

Discussion: Agree with commenter.

Proposed resolution: Accept/Revise. Replace "RpRifOffset" by "RpRifOffset + 600 RSTU" (occurs twice in highlighted text)

CID #14 Revise

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Idx #** | **Cat.** | **Pg.** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** |
| Li-Hsiang Sun | 11 | Technical | 38 | 10.35.3.5.1 | 34 | "The responder (controlee) may indicate the supported message control commands for each of SOR, POLL and REPORT messages in ADV-RESP."   Should also add whether responder support ADV-CONF and its message controls | as in comment |

Reference: A document with text and numbers

Description automatically generated

Discussion: Agree with commenter. We had introduced the more generic SMC\_TLV tags to unify the SMCL tag proposals, which now enumerates the allowed message controls as a list to the message ID tag, therefore makes the individual name tagging in the text obsolete.

Proposed resolution: Revise. Replace sentence with: The responder (controlee) may indicate the supported message control list for each compact message by referencing the supported compact message IDs and the supported message control values using the SMC\_TLVs field.

CID #15 Revise

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Idx #** | **Cat.** | **Pg.** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** |
| Li-Hsiang Sun | 15 | Technical | 39 | 10.35.4 | 27 | "The responder that receives the poll message successfully shall transmit a response message back to the initiator beginning in the ranging slot following the poll period. " | change to "The responder that receives the poll message successfully should transmit a response message back to the initiator beginning in the ranging slot following the poll period subject to LBT " |

Reference: A document with text and numbers

Description automatically generated

Discussion: Agree with the commenter, but we can relax this even more, since other reasons but failed LBTs may be present for a responder at certain times that make it inconvenient to respond.

Proposed resolution: Revise. Replace "shall" by "should".

CID #16 Reject

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Idx #** | **Cat.** | **Pg.** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** |
| Li-Hsiang Sun | 16 | Technical | 39 | 10.35.4 | 25 | even if no LBT, there is still a Tx/Rx turnaound time needed for the initiator/responder, so initiator cannot extend its transmission of the poll message up to macMmsRcpPollNSlots | as in comment |

Reference: A document with text on it

Description automatically generated

Discussion: The comment is based on the assumption of a specific implementation, e.g. one with a TX/RX RF switch. However, other implementations are possible, and the "may" statement is not normative.

Proposed resolution: Reject.

CID #19 Defer

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Idx #** | **Cat.** | **Pg.** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** |
| Li-Hsiang Sun | 19 | Technical | 34 | 10.35.3.2 | 5 | "After the initiator has confirmed receipt of the RESP from the responder during control phase, and unless initialization of further devices is required, the initiator shall discontinue ranging initialization and cease transmission of ADV-POLL packets." | If initiator has not received RESP from responder after session initialization, and because there is no ack to RESP, the responder may have sent RIFs OTA. before statring session re-initialization. In the next session re-initialization, the V counter for RIF should be re-initilalized to a different value than the higher layer configured phyHrpUwbStsVCounter |

~~Reference: A document with text and images

Description automatically generated with medium confidence~~

~~Discussion: The commenter is correct in his observation and conclusion that STS keys/variables need to be rotated, but management (e.g., association, rotation) of~~ *~~phyHrpUwbStsKey~~*~~,~~ *~~phyHrpUwbStsVCounter~~*~~, and~~ *~~phyHrpUwbStsVUpper96~~* ~~are out of scope of 802.15.4z.~~

~~Proposed resolution: Reject.~~

CID #20 Revise

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Idx #** | **Cat.** | **Pg.** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** |
| Li-Hsiang Sun | 20 | Technical | 54 | 10.35.6 | 25 | In NBA MMS, the clock drift is corrected using NB msg, whether the value in the REPORT, i.e reply time and turnaround time, are also corrected, or they are reported based on sender's uncorrected clock (let receiver of the report to do correction)? | specify the procedure how to come up with the reported value |

Reference: A paper with text and numbers

Description automatically generated

Discussion: Agree with commenter.

Proposed resolution: Revise. Replace p.42, line 6 with the following paragraph:

A report message primarily serves to provide ranging results obtained during the ranging phase. The values TurnAroundTime and RoundTripTime shall be reported as measured by its sender's local clock without CFO compensation to the receiver's side.

CID #23 Revise

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Idx #** | **Cat.** | **Pg.** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** |
| Li-Hsiang Sun | 23 | Technical | 44 | 10.35.7.4.3 | 31 | macMmsPrngSeed is only 8 bits not 128 bits, use the description as in 10.35.9.2.1 that MSBs are padded 0 | as in comment |

Reference: A screenshot of a document

Description automatically generated

Discussion: Agree with comment.

Proposed resolution: Revise. Replace p.44, l.30 with:

The least significant 32 bits of the output of the PRNG are then calculated from the input variables with MSBs zero-padded as

CID #24 Revise

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Idx #** | **Cat.** | **Pg.** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** |
| Li-Hsiang Sun | 24 | Editorial | 45 | 10.35.7.4.3 | 1 | RangingBlockIndex should be macMmsNbChannelAllowList | as in comment |

Reference: A document with text and numbers

Description automatically generated

Proposed resolution: Revise. On p.45, l.1 replace "RangingBlockIndex" by "macNbMmsChannelAllowList"

CID #26 Reject

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Idx #** | **Cat.** | **Pg.** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** |
| Li-Hsiang Sun | 26 | Technical | 57 | 10.35.9.8 | 15 | what is the reason that message content must have at least 5 bytes? | as in comment |

Reference: A screenshot of a computer

Description automatically generated

Discussion: Even if no data payload information needs to be transferred, the NBA POLL and RESP packets of sufficient airtime are needed to estimate the CFO of the following UWB RSF and RIF fragments.

Proposed resolution: Reject.

CID #156 Revise

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **CID** | **Category** | **page** | **section** | **line** | **Comment** | **Proposed change** |
| Pooria Pakrooh | 156 | General | 33 | 10.35.2 | 6 | "UWB packets with data" configurations are not defined in this draft. | Intended data configurations need to be defined. |

Reference: *A document with text and numbers

Description automatically generated*

Discussion: Agree with the comment. I assume this has been addressed by Riku in DCN 509r4 in the past September meeting in Atlanta. DCN 509r4 is currently in the process of being integrated to the next draft by the technical editor. Therefore we should mark it as "revised" and Pooria can check/comment again when Draft0(c) is out.

Proposed resolution: Revise (no further action required).

# Reassignment proposals

CID #17 Reassign to Rojan

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Idx #** | **Cat.** | **Pg.** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** |
| Li-Hsiang Sun | 17 | Technical | 39 | 10.35.4 | 40 | " The poll message is transmitted at long-term NB PHY configuration." however, it is not clear if NB Channel select is included in the previous REPORT message from responder, is it counted as short term config?   It is not clear what is the protocol to change Allowed channel list in the middle of the session | NB channel select is not counted as short term operating parameters because it cannot be applied to the next round just for messages other than POLL  There should be a protocol that based on suggested NB channel select to update allowed channel list. However, initiator may need to stay on the channels for additional rounds based on the current alowed list if it does not receive a responding message to resend the new list. |

Reference: A document with text and numbers

Description automatically generated

Discussion: Assign to Rojan.

Proposed Resolution: tbd.

CID #237, #238 Reassign to Rojan

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **CID** | **Category** | **page** | **section** | **line** | **Comment** | **Proposed change** |
| Carlos Aldana | 237 | Technical | 44 | 10.35.7.4.2 | 1 | What happens if all the channels are deemed unavailable or unusable? | Please specify expected behavior |
| Carlos Aldana | 238 | Technical | 44 | 10.35.7.4.2 | 20 | When does the responder employ the list of available channels? Is it immediate, or after X ms? If X ms, what is X? | Please specify expected behavior |

Reference: *A paper with text and numbers

Description automatically generatedA screenshot of a document

Description automatically generated*

Discussion: I assume the comment is less about the channel allow list in general, but rather on what happens during a short-term parameter change in a live session. If that's the case, Rojan would be the expert.

Proposed resolution: tbd.