**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **LB207/D01 comment resolution -- Rejects -- CIDs 41, 43, 44, 54, 427, 458, 459, 472, 473, 475, 479, 489, 542, 545, 558, 566, 656, 879, 880, 988, 994, 1003, 1008, 1340, 1360** |
| Date Submitted | Sep 12, 2024 |
| Sources | Alex Krebs (Apple)krebs @ apple.com |
| Re: |   |
| Abstract |  |
| Purpose | To propose resolution for MMS related comments for “P802.15.4ab™/D (pre-ballot) C 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. |

# Rejects

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index #** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Proposed Resolution. Disposition Detail** |
| Tero Kivinen | 427 | 63 | 10.38.3.6.1 | 16 | All the addresses in the compact frames are public, as the privacy properties of the supposed "private addresses" are so weak that they are public too.  | Remove distinction of ranging using private or public addresses, as they both are public, or change to use proper private addresses defined in 802.15.4ac. | Reject. Private addresses provide 24 bits of randomness, which -- other than the current proposals in 802.15.4ac -- is an established standard for privacy in other standards that are used by over 4 billion devices world wide. In DCN 15-24-126r1 claims about the "private address scheme being weak" have been assessed as 1 ranging error every 723 days under worst case conditions (459 initiators sending packets simulataneously every 100ms).  |
| B. Rolfe | 1340 | 66 | 10.38.3.8 | 27 | " may indicate " seems strange here. Is this an option or a statement of fact? If the prior it's fine. If the later it should be "indicates"  | see comment, pick one. | Reject. SMC\_TLV list indication is an optional field. |
| Mickael Maman | 41 | 67 | 10.38.4.1 | 29 | The responder that receives the poll Compact framesuccessfully should transmit a response Compact frame back to the initiator beginning in the ranging slot following the poll period | shall transmit back response if poll correctly received | Reject. There is no obligation or contract that mandates the responder to respond on every Poll message. |
| Mickael Maman | 43 | 68 | 10.38.5 | 27 | duration between RSF and RIF could be defined at least 2ms | The initiator may start transmitting a first RIF fragment at the start of the ranging phase if no RSF fragments are present, or at least two milliseconds (2400 RSTU) after the start of its last RSF fragmenttransmission otherwise. This parameter is RpRifOffsetInitiator. | Reject. Following DCN 452 resolution. |
| Mickael Maman | 44 | 69 | 10.38.5 | 3 | duration between RSF and RIF could be defined at least 2ms | The responder may start transmitting a first RIF fragment at 600 RSTU into the ranging phase if no RSF fragments were transmitted, or at least two milliseconds (2400 RSTU) after the start of its last RSF fragment transmission otherwise.This parameter is RpRifOffsetIResponder. | Reject. Following DCN 452 resolution. |
| Carlos Aldana | 988 | 71 | 10.38.7.3 | 13 | SSBD can be used to specify LBT behavior. Please add the following text: "Channel access using listen before talk shall be used for improved coexistence performance. When used for narrowband assist, SSBD shall use the following control attribute values:phyCcaDuration should be set as required by local regulations;macSsbdMinBf and macSsbdMaxBf shall be set to 0;macSsbdMaxBackoffs shall be set to 0;macSsbdTxOnEnd shall be set to FALSE;macSsbdPersistence shall be set to FALSE;phyCcaMode shall be set to 1 (energy above threshold)phyCcaEdThreshold shall be set to -67 dBm/MHz - Ptx for channels 0 to 49 and to -74 dBm/MHz - Ptx for channels 50 to 249, where Ptx is the equipment’s instantaneous transmit power in dBm." | As in comment | Reject. Mandatory LBT was discussed before, failing to reach acceptance in the group. |
| Tero Kivinen | 458 | 72 | 10.38.7.4.1 | 16 | Using AES-128 as an PRNG here is overkill. It would be better to use for example the algorithm already defined in the base standard section 10.16.1.  | Reuse the existing channel hopping channel shuffling algorithm, as it has the properties of using each channel exactly once before starting to repeat, and as it is repeating patter it does not require synchronized network as devices can find the network by knowing seed and listening channels.  | Reject. The algorithm in 10.16.1 is memory inefficient to use for the greater number of channels introduced for NBA-UWB MMS. AES-128 is required for CCM encryption and STS generation anyways, therefore comes at no additional effort to use. |
| Tero Kivinen | 459 | 72 | 10.38.7.4.3 | 21 | If the receiving device looses synchronization and does not know the ranging block index, how can it recover from that?  | Explain how to regain synchronization after it is lost. | Reject. All operations are deterministic, there is no asynchronicity between initiator and responder that could possibly lead to "loose synchronization" during an established ranging session. |
| Tero Kivinen | 472 | 78 | 10.38.9.1 | 8 | The compact frame id field is not enough to describe the content, as the message control field changes the most of the fields inside the message content field.  | Combine Compact Frame Id and Message Control fields, move that new 8-bit field as 2nd octet, and use the 5-bits in the first octet to include version number, and security support, so every frame can be secured. | Reject. Proposed design works as intented. |
| Tero Kivinen | 473 | 78 | 10.38.9.1 | 10 | Having frames which have either FCS or MIC makes it impossible to easily reject frames with bit errors on the hardware.  | Include FCS on all frames including those frames which have MIC. | Reject. Not all applications may require "easily reject frames", applications that require that can add a CRC or MIC as desired. |
| Tero Kivinen | 475 | 78 | 10.38.9.2.1 | 20 | When the output of the prand is only 24-bits it is complete overkill to use CSPRNG for generating that. The security level of the CSPRNG is 128-bits but the security of the addressing scheme is 24 bits, so any kind of random number generator is acceptable for such low security levels.  | Remove requirement for the CSPRNG as that is not needed when the security level of the addresses are so low. Using CSPRNG will just generate false sense of security. | Reject. AES-128 is required for CCM encryption and STS generation anyways, therefore comes at no additional effort to use. |
| Tero Kivinen | 479 | 79 | 10.38.9.2.2 | 21 | This public address scheme is much more private than the private address scheme described earlier. This method of addressing provides quite good privacy properties, provided that devices change their public addresses often enough. Only downside is that even the devices participating with the ranging cannot keep track of the devices they are doing ranging with.  | Rename this to private address method, and remove currently defined broken private addresses method. Define method here to do what 802.15.4ac plans to do i.e. to add method of initiator and responder to send secure token that will tell other end who has the key who the other end is. Or simply shorten the 3-octet addresses to 2-octets, use them as short addresses, and reuse what 802.15.4ac defines. | Reject. The public address scheme does not provide more privacy than the private address scheme. |
| Tero Kivinen | 489 | 81 | 10.38.9.3.7 | 20 | The intersection operator is not defined anywhere in this standard of base standard.  | Add text describing what the intersection operation does. | Reject. Not different from other basic math operators like plus, minus, integral, and other operators "undefined" in the base standard.  |
| Pooria Pakrooh | 1360 | 85 | 10.38.9.3.11 | 3 | Why number of RSF/RIF MAC param? it is part of the MMS PHY packet. Clarify whether these are Phy or MAC parameters. | As in the comment | Reject. Number of RSF fragements is number of RSF fragments. No point in arguing if a field's value is referring to a MAC or PHY entity. |
| Carl Murray | 879 | 85 | 10.38.9.3.11 | 7 | Make it more clear that the reserved entries of Table 14 might be used in the future.   | Change "Reserved" to "Reserved for future use". | Reject. Unnecessary long and meaningless, as there is no defined transmitter/receiver behaviour for "Reserved for ...") |
| Carl Murray | 880 | 85 | 10.38.9.3.11 | 11 | Make it more clear that the reserved entries of Table 15 might be used in the future.   | Change "Reserved" to "Reserved for future use". | Reject. Unnecessary long and meaningless, as there is no defined transmitter/receiver behaviour for "Reserved for ...") |
| Mickael Maman | 54 | 86 | 10.38.9.3.12 | 3 | what are the range of ranging slot duration? | from 300/600 RSTU to 2400 RSTU? | Reject. Answer is yes. |
| Tero Kivinen | 542 | 93 | 10.38.9.5 | 14 | The Responder RPA Hash field description should be clear that the responder IRK that is used, is the IRK of the transmitter of this frame.  | Add "(i.e. the IRK of device transmitting this frame)" to the end. | Reject. The sentence unambiguously says: "The Responder RPA Hash field shall be set as specified in 10.38.9.2.1 using the responder's IRK." |
| Tero Kivinen | 545 | 94 | 10.38.9.6 | 23 | How does the responder know which IRK is used to calculate, or is it assumed to check both?  | Specify how the responder of the start of ranging compact frame will know which IRK to use, or specify that initiator needs to calculate both RPA Hash with both IRKs and by comparing them to the RPA hash of the frame they know whether it was for single responder or for multiple.  | Reject. As the text says, the one happens when contention based initialization is used, the other one happens when one-to-one intialization is used. Since the SOR frame is sent at the end of either procedure, the responder knows in what procedure it has participated before. |
| Carlos Aldana | 1003 | 97 | 10.38.9.7 | 7 | This frame keeps getting longer after every draft. Let's limit the duration to 1ms. Add text that says so. | As in comment | Reject. The PHR allows up to 127 octets of PSDU, resulting in >4ms frames. |
| Tero Kivinen | 558 | 97 | 10.38.9.7 | 22 | What is the point of including two extra octets of zero when the frames are supposed to be compact.  | Remove extra unneeded data. | Reject. This particular frame is does not provide sufficient airtime for CFO estimation. |
| Tero Kivinen | 566 | 99 | 10.38.9.9 | 23 | If there is no different message control fields, the whole field can be omitted. This is supposed to be compact frames, make them compact.  | Remove Message Control field. | Reject. Removing the MsgCtrl field would break the SMC\_TLVs negotiation and also make it impossible to define variants of this frame in the future. |
| Tero Kivinen | 656 | 124 | 10.38.10.1 | 16 | There is no point of using Prng with Seed if the seed is going to be only one octet long. The problem with Prng is that it can generate non-optimal distribution of channels, and as there is no security reasons for using Prng using some kind of permutation function that picks channel numbers intelligently would be better.  | What is the point of using Prgn here? Wouldn't some kind of permutation function be better.  | Reject. One octet seed enables up to 256 time synchronized devices to operate at exactly the same time at randomly different channels.Since there is only 250 O-QPSK channels, it doesn't make sense to allow for more than 250 randomized sequences, as those would map to the colliding channels with increasing collision probability. |
| Carlos Aldana | 994 | 125 | 10.38.10.1 | 1 | macMmsNbInitChannel should be carefully selected and not have a wide range from 0-249 to prevent it from being interfered with. Change it so that it covers the union of the following 2 sets : 1) from 5725 to 5732.5 (0 to 2) MHz 2) from 5835 to 5850 MHz (44 to 49) | As in comment | Reject. Discussed before in DCN 15-23-591r1, more channels is better. |
| Carlos Aldana | 1008 | 125 | 10.38.10.1 | 1 | The range of both macMmsRcpPollNSlots and macMmsRcpRespNSlots is quite large (up to 7.5ms when slot duration is set to 0.5ms and 15 ms when slot duration is set to 1ms). Consider limiting duration to 1ms. | As in comment | Reject. Particular values mentioned don't justify reducing bits, as reducing the bits for slots would require more bits for rounds and blocks. |