**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **DraftC comment resolution - Miscellaneous - CIDs 10, 41, 563, 564, 605, 630, 323** |
| Date Submitted | May 08, 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. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **CID** | **p.** | **Sub-clause** | **l.** | **Comment** | **Proposed Change** | **Proposed Resolution** |
| Youngwan So | 563 | 49 | 10.38.3.6 | 41 | The channel specified by "default value of" the macMmsNbInitChannel attribute   and   the channel specified by "default value of" the macMmsUwbChannel attribute   shall be used for coordination | Change  "The initiator transmits the NB Acquisition Compact frame in the initialization channel specified by the macMmsNbInitChannel attribute and transmits the UWB Acquisition Compact frame in the channel specified by the macMmsUwbChannel attribute."  to   "The initiator transmits the NB Acquisition Compact frame in the initialization channel specified by the default value of macMmsNbInitChannel attribute and transmits the UWB Acquisition Compact frame in the channel specified by the default value of the macMmsUwbChannel attribute." | Revise. (Accept, but replace "and" by "and/or") |
| Youngwan So | 564 | 50 | 10.38.3.6 | 3 | The channel specified by "default value of" the macMmsNbInitChannel attribute   and   the channel specified by "default value of" the macMmsUwbChannel attribute   shall be used for coordination | Change  "If coordination is active, before starting a new session, the initiator scans for Acquisition Compact frame on the initialization channel specified by the macMmsNbInitChannel attribute and/or the channel specified by the macMmsUwbChannel attribute."  to   "If coordination is active, before starting a new session, the initiator scans for Acquisition Compact frame on the initialization channel specified by the default value of macMmsNbInitChannel attribute and/or the channel specified by the default value of macMmsUwbChannel attribute." | Accept. |
| Li-Hsiang Sun | 10 | 49 | 10.38.3.5.1 | 28 | "The Start of Ranging Compact frame may contain all these fields." | change to shall | Revise. Replace the sentence with "Unless values for all fields are carried in the Start of Ranging Compact frame, if applicable, the receiver shall assume the omitted values unchanged from previous OOB communication, and shall assume default values otherwise." |
| Li-Hsiang Sun | 41 | 51 | 10.38.4.2 | 10 | There are many different scenarios that initiator and responder's phyHrpUwbStsVCounter may become out of sync,   for example, an attacker may send a poll (currently unprotected) to trigger RIF transmissions from responder  for another example, RESP message is lost and responder advances its counter after sending RIFS while initiator does not increments its counter  In 4z RSSD IE can be used may be used to synchronize the values of V and the STS seed between HRP-ERDEVs  In MMS ranging, we currently do not have such mechanism. | suggest if secure ranging is required, phyHrpUwbStsVCounter is constructed from an increasing counter (such as block/slot index) mainatined by the initiator and signaled to the responder.   The counter signaling is carried in a protected message such as SOR or POLL to synchronize between initiator and one or more responders   The RIFs from responder triggered by replaying of the protected message can be discarded by initiator due to outdated counter value  The protection of the counter prevents attacker to trigger RIFs to be generated based on future counter values | Reject. The currently proposed ranging mode is not assumed to be secure against any form of attacks, and the use of STS fragments does not imply secure ranging.  Discussion: Offline discussion: aside from "attacks" specifically provoking out of sync states which are out of scope, the defined protocol cannot run out of sync accidentally, since the Initiator is the Controller of the time grid and the time grid is communicated only one-way from the Initiator to the Responder in the SOR packet cannot be changed later on. Regarding "secure ranging", we can discuss in the group if there is a common interest to extend the 4ab specification in that regard in the next draft iteration. |
| Rojan Chitrakar | 605 | 46 | 10.38.3.2.1 | 11 | To allow the slot duration to be updated via the Advertising Poll Compact frame or Public Advertising Poll Compact frame, the InitializationSlotDuration parameter should be included in more Advertising Poll Compact frame or Public Advertising Poll Compact frame versions, not just the ones with CapDuration. | as in comment | Revise. Append trailing column [1; Initialization Slot Duration] to Figure 50 on p.71 l.17, and add text from p.72 l.7 to p.71 after l.19 (according to 15-24-0024-00-04ab-proposed-comments-resolution-on-compact-frame.docx) |
| Rojan Chitrakar | 630 | 64 | 10.38.10.2.1 | 27 | The outcome of the RPA resolution should also be explained, i.e., what's the next step if the RPA of a received frame cannot be resolved even after all possible IRKs are exhausted? | as in comment | Revise. Extend the paragraph on p.64 l.29 by "Incoming packets for which the RPA is not resolved shall be discarded by the receiver." |
| Bin Qian | 323 | 52 | 10.38.5 | 2 | After the first RSF fragment, the responder should continue to send up to phyUwbMmsRsfNumberFrags RSF fragments at regular intervals of 1200 RSTU | As in the comment | Revise. Replace sentence by "The responder may send phyUwbMmsRsfNumberFrags RSF fragments at regular intervals of 1200 RSTU." Similarly, change the last sentence on p.51 by removing "up to". |
| Carl Murray | 743 | 72 | 10.38.10.5 | 15 | Would it be better to get rid of message control 0x00 as 0x01 provides the same functionality but is more flexible at the cost of 1 octet | Should discuss | Reject. 0x00 has lower complexity.  Discussion: It's not about the 1 byte, but I prefer to have a simple baseline method without variable length/presence bitmap control complications. |