**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **LB207/D01 comment resolution -- Compact frame CRC and RPA Hash -- CIDs 474, 538, 1023, 1024, 1196, 1392** |
| Date Submitted | Feb 4, 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. |

**Table of contents**

[CRC comments (follow up after Kobe) 3](#_Toc187499954)

[RPA Hash comments (follow up after Kobe) 4](#_Toc187499955)

# CRC comments (follow up after Kobe)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index #** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** |
| Billy Verso | 1023 | 15 | 6.6.2 | 15 | This clause in the base standard describes reception steps and tells us to discard frames with bad CRC. Rather than having to amend and maintain this for every compact frame encoding that has MIC instead of CRC, (and complicating the MAC receive processing implementation in the process), suggest to add CRC as part of the compact frame definition in clause 7.3.7 and remove CRC from the Compact Frame Content field definitions of clause 10.38.10. | To simplify the low level MAC processing in everyone's implementation, make the CRC a common mandatory part of all Compact Frames. i.e. Add CRC are the end of the frame in Figure 1, and description text sub-clause in 7.3.7 |
| Billy Verso | 1024 | 17 | 7.3.7.1 | 4 | Other than the extended frame type which is assigned to TIA to define, Compact frames are the first frame type without a MFR specifying a CRC, (and I expect TIA actually specify a CRC are the end of their frames also). Not having a CRC complicates the first level of frame filtering since the individual specific decoding of Compact Frame ID and the Message Control internals of the frame have to be decoded before knowing whether there is a CRC or a MIC. | Add a FCS/CRC as is done for all other frame types, in the standard. Even secured frames with a MIC have CRC as first level of filtering.  |
| Billy Verso | 1196 | 78 | 10.38.91 | 10 | For ease of MAC layering implementation it would make sense for lower layer MAC to always of an FCS check and discard frames with bad FCS, i.e. require a good FCS before parsing the frame to do security processing if the frame needs is.  | Change Compact frame format to always have the CRC field. |

Discussion: Good comments, let's follow up on this during the Kobe meeting and work on a resolution proposal.

Proposed resolution: To be revised.

Disposition detail: after Kobe.

# RPA Hash comments (follow up after Kobe)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index #** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** |
| Alex Krebs | 1392 | 78 | 10.38.9.2.1 | 17 | This scheme does not protect the responder devices against active polling privacy attacks.  | Add an optional extension that assures non-replayable addresses when required by the responders. |
| Tero Kivinen | 474 | 78 | 10.38.9.2.1 | 18 | The current defined address generation method allows easy passive monitoring and tracking of all users, and trivial active tests that will allow attackers to keep track of specific users.  | Remove the currently defined completely broken private addressing scheme, and use the private addressing scheme defined in the 802.15.4ac. |
| Tero Kivinen | 538 | 92 | 10.38.9.4 | 5 | This means that RPA hash changes for every single advertising poll compact frames, thus quite often (for advertising poll compact frames to be useful, they needs to be transmitted at least several times per minute). If an passive attacker listens the advertising poll compact frames for few thousands of frames it can build database of known RPA hash and prand values that will allow it to keep track of sender.  | The current privacy protection provided by the RPA hash and prand method is completely inadequate. Replace the broken privacy methods with the methods defined in 4ac, or more accurately use the existing 802.15.4 frames to which 4ac will provide privacy. |

Discussion: Good comments, let's follow up on this during the Kobe meeting and work on a resolution proposal.

Follow up after Kobe discussion: The initiator can arbitrarily change the value of RPA Prand at the beginning of each ranging block. The specific method to generate RPA Prand is intentionally unrestricted and left to the higher layers. If a use case requires non-replayable packets, the initiator and responder can be specified on higher layers to use a synchronized generating function for RPA Prand. E.g. a non-replayable generating function that assures that initiator and responder are at the same place at the same time is RPA Prand = AES-128(data={UTC time, Lat/Lon coordinates, ...}, key), where key is a shared secret between initiator and responder. While such OOB definitions are possible and suitable for certain use cases with high privacy requirements, the IEEE standard must not restrict application by mandating privacy requirements to the higher layers. It is sufficient that the specification allows for it.

CID 1392 and 474 can be relaxing the requirements on generating the RPA Prand on page 78 as proposed below. CID 538 is confusing the initiator's option to change the RPA Prand in every Advertising Poll Compact Frame with an unspecified mandate for the initiator to do so, and the proposed text change below may aid to a more clear understanding.

Proposed resolution: Revised.

Disposition detail: On page 78, line 17 change the text as follows:

**10.38.9.2.1 Private addresses**

To impede tracking of HRP-ARDEVs resolvable private addresses (RPAs) are used by initiator and

responder devices. To generate a private address, every device shall use a 128-bit identity resolving key

(IRK). The initiator shall communicate a 3-octet RPA Prand in every

Advertising Poll Compact frame during session initialization (10.38.3.2) and in every One-to-one Poll

Compact frame (or One-to-many Poll Compact frame) during the ranging control phase (10.38.4).

A 3-octet RPA\_hash is then computed using an IRK and the initiator’s RPA\_prand. The RPA

hash is then given by bits 0 to 23 of *h*(key=IdentityResolvingKey, data=RPA Prand) where *h( )* is the AES-128 block

cipher described in B.2.2, with an IRK and the initiator's RPA\_prand as inputs. The value of RPA Prand is controlled by the initiator and might change with every Advertising Poll Compact frame or One-to-one Poll compact frame transmission. Higher layer methods may be used to synchronize generation and application of RPA Prand values between the initiator and the responder. The generation and application of RPA Prand is out of scope of this standard.