**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **Proposed Resolution for MMS IRK** |
| Date Submitted | February 2024 |
| Sources | Rojan Chitrakar, Lei Huang (Huawei), Alex Krebs (Apple)rojan.chitrakar@huawei.com |  |
| Re: |   |
| Abstract |  |
| Purpose | To propose resolution for MMS IRK 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. |

Rev 0: Initial version.

Rev 1: Based on Alex’s suggestions, instead of overloading the RPA Hash field, changed the RPA Hash field of relevant Compact frames to either Initiator RPA Hash or Responder RPA Hash.

***Comment Indices in 15-24-0010-00-04ab-consolidated-comments-draft-c:***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| Li-Hsiang Sun | 8 | 64 | 10.38.10.2.1 | 24 | In Fig 25, how do Responder 1 or 2 know they are addressed by SOR? RPA hash is calculated using sender (initiator) IRK so both responders will think SOR is for itslef.Similar situation in Poll msg in Figure 38 | unicast msg should use controlee IRK for calculating RPA hash | Revised |
| Rojan Chitrakar | 643 | 74 | 10.38.10.6 | 20 | When the contention based initialization and setup phase is used for one-to-one ranging (E.g., Figure 25), initiator may receive Advertising Response Compact frames from multiple responders but only choose a single responder for the subsequent ranging phase. However, the Start of Ranging Compact frame is not able to identify a particular responder causing all responders to proceed to the ranging phase. | When the Start of Ranging Compact frame is targetted at a particular responder, the RPA\_hash field shall be set as the RPA of the target responder (instead of the intiator's RPA). Only the targetted responder will go on to participate in the ranging phases at the time indicated by the Start of Ranging Compact frame. | Revised |
| Rojan Chitrakar | 644 | 75 | 10.38.10.7 | 11 | When the contention based initialization and setup phase is used for one-to-one ranging (E.g., Figure 25), initiator may receive Advertising Response Compact frames from multiple responders but only choose a single responder for the subsequent ranging phase. However, the One-to-one Poll Compact frame is not able to identify a particular responder causing all responders to respond to the Poll frame. | When the POLL message is targetted at a particular responder, the RPA\_hash field shall be generated using the IRK of the target responder (instead of the intiator's IRK). If a responder is able to correctly resolve the RPA\_hash using its own IRK, it knows that the POLL is targetted at it. | Revised |

**Discussion**：





Offline discussions led to suggestion to rename the RPA Hash field to a more appropriate name based on its intended use. This is summarized in the table below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Compact frame name**  | Context | IRK used for RPA\_hash | Source of RPA Prand |
| 0  | Advertising Poll  |  | Initiator’s | Adv Poll |
| 1  | Advertising Response  |  | Responder’s | Adv Poll |
| 2  | Start of Ranging  | O2O I&S | Initiator’s | Adv Poll |
| Contention I&S for O2O | Responder’s | Adv Poll |
| Contention I&S for O2M | Initiator’s | Adv Poll |
| 3  | One-to-one Poll  | O2O I&S | Initiator’s | O2O Poll |
| Contention I&S for O2O | Responder’s | O2O Poll |
| 4  | One-to-one Response  |  | Responder’s | O2O Poll |
| 5  | One-to-one Initiator Report  |  | Initiator’s | O2O Poll |
| 6  | One-to-one Responder Report  |  | Responder’s | O2O Poll |
| 7  | Advertising Confirmation  |  | Initiator’s | Adv Poll |
| 8  | One-to-many Poll  |  | Initiator’s | O2M Poll |
| 9  | One-to-many Response  | Contention O2M Non-first Response | Responder’s | First O2M Poll (RIM) or preceding O2M Poll? |
| All other O2M | Responder’s | Preceding O2M Poll |
| 10  | One-to-many Responder Report  |  | Responder’s | Preceding O2M Poll |
| 11  | One-to-many Initiator Report  |  | Initiator’s | Preceding O2M Poll |
| 12  | Public Advertising Poll  |  |  |  |
| 13  | Public Advertising Response  |  |  |  |
| 14  | Public Start of Ranging  |  |  |  |
| 15  | Public Advertising Confirmation  |  |  |  |
| 16  | Acquisition  |  |  |  |
| 17  | One-to-one Initiator Secure Report  |  | Initiator’s | O2O Poll |
| 18  | One-to-one Responder Secure Report  |  | Responder’s | O2O Poll |
| 19  | One-to-many Initiator Secure Report  |  | Initiator’s | O2M Poll |
| 20  | One-to-many Responder Secure Report  |  | Responder’s | Preceding O2M Poll |

**Disposition: Revised**

**Disposition Detail:**

**Proposed text changes on P802.15.4ab™/D (pre-ballot) C:**

**10.38.10.4 Advertising Poll Compact frame**

…

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Octets: 3 | 3 | 1 | variable | 2 |
| Initiator RPA hash | RPA Prand | Message Control | Message Content | FCS |

**Figure 49—Advertising Poll Compact frame format**

The Initiator RPA Hash field shall be calculated as specified in 10.38.10.2.1 using the initiator's IRK.

**10.38.10.5 Advertising Response Compact frame**

…

|  |  |  |  |
| --- | --- | --- | --- |
| Octets: 3 | 1 | variable | 2 |
| Responder RPA hash | Message Control | Message Content | FCS |

**Figure 53—Advertising Response Compact frame format**

The Responder RPA Hash field shall be calculated as specified in 10.38.10.2.1 using the responder's IRK.

**10.38.10.6 Start of Ranging Compact frame (#8, #643)**

***Change the subfield as follows (Track changes ON)***

…

**Figure 59—Start of Ranging Compact frame format**

When the Start of Ranging Compact frame is transmitted to a single responder selected during contention based initialization and setup (as described in 10.38.3.3), the RPA Hash field shall be calculated as specified in 10.38.10.2.1 using the responder's IRK. Otherwise, the RPA Hash field shall be calculated as specified in 10.38.10.2.1 using the initiator's IRK.

**10.38.10.7 One-to-one Poll Compact frame**

…

**Figure 61—One-to-one Poll Compact frame format**

When the One-to-one Poll Compact frame is transmitted to a single responder selected during contention based initialization and setup (as described in 10.38.3.3), the RPA Hash field shall calculated as specified in 10.38.10.2.1 using the responder's IRK. Otherwise, the RPA Hash field shall be calculated as specified in 10.38.10.2.1 using the initiator's IRK. The RPA Prand field shall be set as specified in 10.38.10.2.1. In the scope of a ranging round, the value of RPA\_prand as conveyed in this frame shall be used to compute the RPA\_hash used in all subsequent frames, until the initiator transmits another One-to-one Poll Compact frame or a One-to-many Poll Compact frame.

**10.38.10.8 RESP Compact frame**

**…**

***Change the RPA Hash field in Figure 65 to Responder RPA Hash***

The Responder RPA Hash field shall be calculated as specified in 10.38.10.2.1 using the responder's IRK.

**10.38.10.9 One-to-one Initiator Report Compact frame**

**…**

***Change the RPA Hash field in Figure 68 to Initiator RPA Hash***

The Initiator RPA Hash field shall be calculated as specified in 10.38.10.2.1 using the initiator's IRK.

**10.38.10.10 One-to-one Responder Report Compact frame**

**…**

***Change the RPA Hash field in Figure 70 to Responder RPA Hash***

The Responder RPA Hash field shall be calculated as specified in 10.38.10.2.1 using the responder's IRK.

**10.38.10.11 Advertising Confirmation Compact frame Compact frame**

**…**

***Change the RPA Hash field in Figure 73 to Initiator RPA Hash***

The Initiator RPA Hash field shall be calculated as specified in 10.38.10.2.1 using the initiator's IRK.

**10.38.10.12 One-to-many Poll Compact frame**

**…**

***Change the RPA Hash field in Figure 76 to Initiator RPA Hash***

The Initiator RPA Hash field shall be calculated as specified in 10.38.10.2.1 using the initiator's IRK.

**10.38.10.13 One-to-many Response Compact frame**

**…**

***Change the RPA Hash field in Figure 90 to Responder RPA Hash***

The Responder RPA Hash field shall be calculated as specified in 10.38.10.2.1 using the responder's IRK.

**10.38.10.14 One-to-many Responder Report Compact frame**

**…**

***Change the RPA Hash field in Figure 94 to Responder RPA Hash***

The Responder RPA Hash field shall be calculated as specified in 10.38.10.2.1 using the responder's IRK.

**10.38.10.15 One-to-many Initiator Report Compact frame**

**…**

***Change the RPA Hash field in Figure 97 to Initiator RPA Hash***

The Initiator RPA Hash field shall be calculated as specified in 10.38.10.2.1 using the initiator's IRK.

**10.38.10.21 One-to-one Initiator Secure Report Compact frame**

**…**

***Change the RPA Hash field in Figure 114 to Initiator RPA Hash***

The Initiator RPA Hash field shall be calculated as specified in 10.38.10.2.1 using the initiator's IRK.

**10.38.10.22 One-to-one Responder Secure Report Compact frame**

**…**

***Change the RPA Hash field in Figure 116 to Responder RPA Hash***

The Responder RPA Hash field shall be calculated as specified in 10.38.10.2.1 using the responder's IRK.

**10.38.10.23 One-to-many Initiator Secure Report Compact frame**

**…**

***Change the RPA Hash field in Figure 114 to Initiator RPA Hash***

The Initiator RPA Hash field shall be calculated as specified in 10.38.10.2.1 using the initiator's IRK.

**10.38.10.24 One-to-many Responder Secure Report Compact frame**

**…**

***Change the RPA Hash field in Figure 116 to Responder RPA Hash***

The Responder RPA Hash field shall be calculated as specified in 10.38.10.2.1 using the responder's IRK.

**10.38.10.2.1 Private addresses (#8, #644)**

…

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 modulo division operator. Depending on which compact message is used for transmission, the IRK used for RPA\_hash calculation may be the initiator's IRK, a responder's IRK, or a group IRK that associates with multiple devices. For details see the description of the respective message. An RPA consisting of an RPA\_hash and an RPA\_prand may be used for OTA packet transmissions and can be resolved only at a receiving device that have knowledge of the generating IRK.

In order to resolve an RPA of an incoming packet the receiving device shall compute the RPA\_hash using one or more IRKs that the receiver assumes to have been used by the sender device and the received RPA\_prand communicated over the air by the transmitting device. If the result of the receiver's computation matches the received RPA, the RPA is resolved. Otherwise, the RPA shall be marked as unresolved and the received packet shall be ignored by the receiver.