**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)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. Addresses the following comments:

***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 | RPA Hash field | IRK | Source of RPA Prand |
| 0  | Advertising Poll  |  | Initiator RPA Hash | Initiator’s | Adv Poll |
| 1  | Advertising Response  |  | Responder RPA Hash | Responder’s | Adv Poll |
| 2  | Start of Ranging  | O2O I&S | Initiator RPA Hash | Initiator’s | Adv Poll |
| Contention I&S for O2O | Responder RPA Hash | Responder’s | Adv Poll |
| Contention I&S for O2M | Initiator RPA Hash | Initiator’s | Adv Poll |
| 3  | One-to-one Poll  | O2O I&S | Initiator RPA Hash | Initiator’s | O2O Poll |
| Contention I&S for O2O | Responder RPA Hash | Responder’s | O2O Poll |
| 4  | One-to-one Response  |  | Responder RPA Hash | Responder’s | O2O Poll |
| 5  | One-to-one Initiator Report  |  | Initiator RPA Hash | Initiator’s | O2O Poll |
| 6  | One-to-one Responder Report  |  | Responder RPA Hash | Responder’s | O2O Poll |
| 7  | Advertising Confirmation  |  | Initiator RPA Hash | Initiator’s | Adv Poll |
| 8  | One-to-many Poll  |  | Initiator RPA Hash | Initiator’s | O2M Poll |
| 9  | One-to-many Response  | Contention O2M Non-first Response | Responder RPA Hash | Responder’s | First O2M Poll (RIM) or preceding O2M Poll? |
| All other O2M | Responder RPA Hash | Responder’s | Preceding O2M Poll |
| 10  | One-to-many Responder Report  |  | Responder RPA Hash | Responder’s | Preceding O2M Poll |
| 11  | One-to-many Initiator Report  |  | Initiator RPA Hash | 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 RPA Hash | Initiator’s | O2O Poll |
| 18  | One-to-one Responder Secure Report  |  | Responder RPA Hash | Responder’s | O2O Poll |
| 19  | One-to-many Initiator Secure Report  |  | Initiator RPA Hash | Initiator’s | O2M Poll |
| 20  | One-to-many Responder Secure Report  |  | Responder RPA Hash | 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**

…

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

The RPA Hash field shall be set to InitiatorRPA\_Hash as specified in 10.38.10.2.1.

**10.38.10.5 Advertising Response Compact frame**

…

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

The RPA Hash field shall be set to ResponderRPA\_Hash as specified in 10.38.10.2.1.

**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 set to ResponderRPA\_Hash as specified in 10.38.10.2.1. Otherwise, the RPA Hash field shall be set to InitiatorRPA\_Hash as specified in 10.38.10.2.1.

**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 be set to ResponderRPA\_Hash as specified in 10.38.10.2.1. Otherwise, the RPA Hash field shall be set to InitiatorRPA\_Hash as specified in 10.38.10.2.1. 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.

… Other Compact frames to be added….

**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. If the RPA\_hash is generated using the initiator’s IRK, the RPA\_hash is known as InitiatorRPA\_hash. If the RPA\_hash is generated using a responder’s IRK, the RPA\_hash is known as ResponderRPA\_hash. Either the InitiatorRPA\_hash or the ResponderRPA\_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 or an assumed recipient and the RPA\_prand communicated by the initiator. 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.