**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | Resolution proposals for comments #12 and #27 |
| Date Submitted | November 2023 |
| Sources | Alex Krebs, Jinjing Jiang (Apple) |  |
| Re: |  |
| Abstract |  |
| Purpose | To propose resolution to NBA-UWB MMS comments for “P802.15.4ab™/D (pre-ballot) B 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. |

CID #12 Revise

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Idx #** | **Category** | **Pg.** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** |
| Li-Hsiang Sun | 12 | Technical | 35 | 10.35.3.3 | 24 | For 1 to many case using CAP, What is IdentityResolvingKey used in ADV\_POLL and ADV\_RESP?How does initiator selects one of the responders if all their RPA hash the same (corresponding to the RPA hash of ADV\_POLL)?  | clarify the addressing in this case |
| Li-Hsiang Sun | 27 | Technical | 59 | 10.35.9.11 | 7 | Not sure what are the Responder Address when RPA is used | as in comment |

Reference:
 

Discussion: Agree that we need to clearly define the Responder Address calculation and clarify the existing subsection on private address calculation. Rojan: 1) ADV-CONF is ambiguously used for P2P and O2M => needs distinction in text. 2) ADV-RESP's RPA\_hash == ADV\_CONF's Responder Address (same RPA\_prand taken from preceding ADV-POLL).

Proposed resolution: Revise. Change p.49, l. 13-32, subsection 10.35.9.2.1 as follows:

**10.35.9.2.1 Private addresses**

To impede tracking of HRP-ARDEVs, resolvable private addresses (RPA)s are used by initiator and responder devices. To generate a private address, every device shall use a 128-bit identity resolving key (IRK) and every initiator shall be equipped with a cryptographically secure pseudo random number generator (CSPRNG). The initiator shall generate and communicate a 3-octet output RPA\_prand of the CSPRNG in the ADV-POLL message during session initialization (10.35.3.2) and in the POLL (or POLL one-to-many) message during the ranging control phase (10.35.4).

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 integer modulo operator. RPA\_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 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.

The generation and mutual exchange of IRKs among initiator(s) and responder(s) is out of scope of this standard and may be conducted using higher layer methods. Note that devices may carry multiple IRKs to, e.g., assert privacy among multiple responders and/or ranging sessions. Again, methods for association and assignment of IRKs is not defined in this standard, but may be carried out using higher layer methods.

Change in subsection "**10.35.9.4 ADV-POLL**" on p.54, l. 7 as follows:

The RPAprand field shall be set as specified in 10.35.9.2.1. During initialisation phase, the value of RPA\_prand as conveyed in this message shall be used to compute RPA\_hash in all following messages, until the initiator transmits another ADV-POLL message.

Change in subsection "**10.35.9.7 POLL**" on p.56, l. 16 as follows:

The RPA Hash and RPA Prand fields shall be set as specified in 10.35.9.2.1. In the scope of a ranging round, the value of RPA\_prand as conveyed in this message shall be used to compute RPA\_hash in all following messages, until the initiator transmits another POLL or POLL (One-to-many) message.

Change in subsection "**10.35.9.11 ADV-CONF**" on p.59, l. 5 as follows:

The RPA\_hash field shall be set as specified in 10.35.9.2.1. Note that if Message Content contains one or more Responder Address fields, each Responder Address in Message Content shall represent an eligible responder's RPA hash generated using the initiator's RPA\_prand from the preceding ADV-POLL message along with that responder's IRK.

Change in subsection "**10.35.9.12 POLL (One-to-many)**" on p.59, l. 14-15 as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| **Octets: 3** | **3** | **1** | **variable** |
| RPA\_hash | RPA\_prand | Message Control | Message Content |

**Figure 55—One-to-many POLL Compact Message**

The RPA\_hash and RPA\_prand fields shall be set as specified in 10.35.9.2.1. Note that if Message Content contains one or more Responder Address fields, each Responder Address in Message Content shall represent an eligible responder's RPA hash generated using the RPA\_prand as conveyed in this message along with that responder's IRK.