**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | **Proposed changes regarding Group ID comments for P802.15.4ab™/Draft (pre-ballot) C** | |
| Date Submitted | Jan 2024 | |
| Sources | Hong Won Lee, Insun Jang, Jinsoo Choi, HanGyu Cho (LG Electronics) |  |
| Re: | Contribution to IEEE 802.15.4ab | |
| Abstract |  | |
| Purpose | To propose comments and proposed changes to “P802.15.4ab™/ Draft (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. | |

***This document aims to propose a resolution proposal regarding Group ID comments for P802.15.4ab™/*** ***Draft (pre-ballot) C Draft Standard***

***Comments in 15-24-0002-00-04ab-tg4ab-preballot-comments-hongwon.xlsx***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Category** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** |
| Technical | 55 | 10.38.7.2 | 13 | Group ID shall be used for one-to-many broadcasting message | Change from "to-many" to "to-many broadcasting message" |
| Technical | 55 | 10.38.7.2 | 16-20 | Group ID shall be used for one-to-many broadcasting message | Change from "A GroupID represents a group of devices in a one-to-many ranging session, as described in 10.38.9. By transmitting a Public Advertising Poll Compact frame with the MessageControl field set to 0x21 on the  initialization channel, a GroupID is shared with responders. The GroupID shall be used to generate the IRK for the RPA\_hash used in One-to-many Poll Compact frame (message id 0x12) in the one-to-many ranging session, as described in 10.38.9, in case GroupID is shared with responders." to "In one-to-many session, POLL (one-to-many) message (message id 0x12, with MessageControl not set to 0x00) in the first sub-round shall be broadcasted as described in 10.35.8. After initialization using public addresses, an IRK for broadcasting message shall be generated. The IRK for broadcasting message is generated using a GroupID which represents a group of devices in a one-to-many ranging session. By transmitting a Public Advertising Poll Compact frame with the MessageControl field set to 0x21 on the  initialization channel, a GroupID is shared with responders." |
| Technical | 55 | 10.38.7.2 | 23 | Group ID shall be used for one-to-many broadcasting message | Change from "One-to-many Poll Compact message (message id 0x12)" to "One-to-many Poll Compact message (message id 0x12, with MessageControl not set to 0x00)" |
| Technical | 55 | 10.38.7.2 | 31 | Group ID shall be used for one-to-many broadcasting message | Change from "IRK2 (for One-to-many Poll Compact frame, message id 0x12)" to "IRK2 (for One-to-many Poll Compact frame, message id 0x12, with Message Control field not set to 0x00)" |
| Technical | 56 | 10.38.7.2 | 3 | Group ID shall be used for one-to-many broadcasting message | Change from "IRK2 (for One-to-many Poll Compact frame, message id 0x12)" to "IRK2 (for One-to-many Poll Compact frame, message id 0x12, with Message Control field not set to 0x00)" |

**Discussion:**

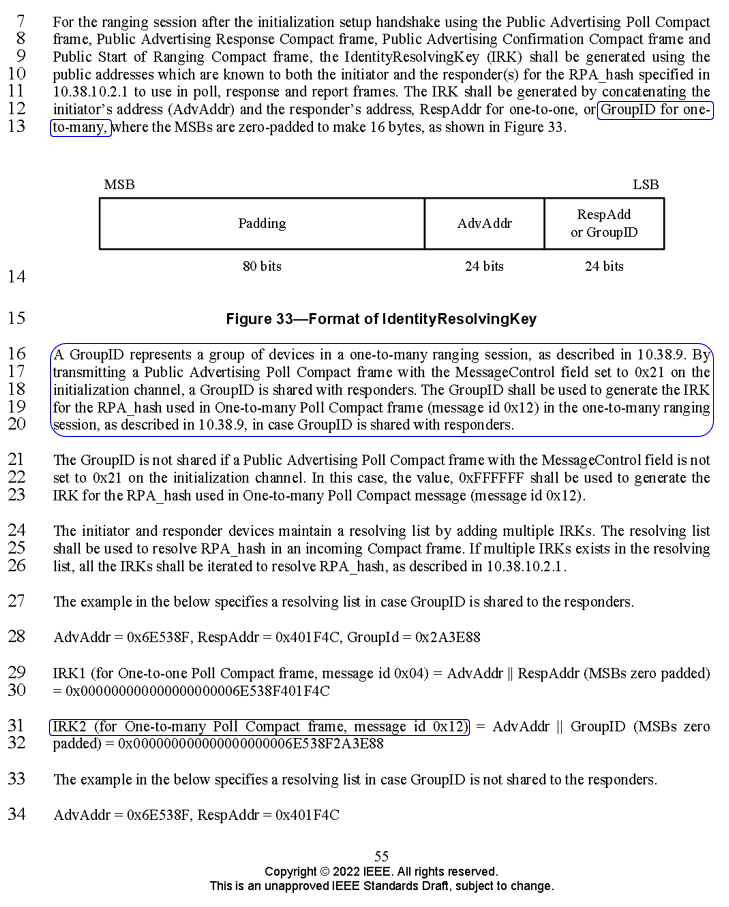
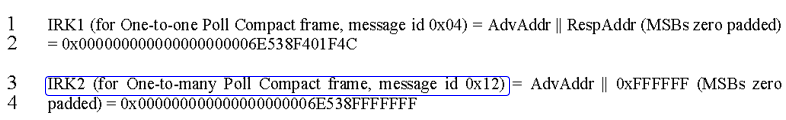
The IRK for RPA\_hash of One-to-many Poll broadcasting Compact frame (Message Control not set to 0x00) after initialization using public addresses shall be generated using the Group ID. The IRK for RPA\_hash of one-to-many Poll Compact frame (Message Control set to 0x00) after initialization using public addresses shall be generated using AdvAddr and RespAddr. This changes to clarify which IRK shall be used for RPA\_hash generation according to Message Control id of One-to-many Poll Compact frame.

**Resolution: Revised**

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

**10.38.7.2 RPA\_hash generation and resolution after initialization using public addresses**

**- Original Text**

**- Proposed change**

***Revise the sub-clause 10.38.7.2 RPA\_hash generation and resolution after initialization using public addresses in IEEE P802.15.4ab/Draft (pre-ballot) C as follows:***

**(*pp. 55 line #13, #16-20, #23, #31 / pp. 56 line #3*)**

***--------------------------------------------------------------------------------------------------------------------------------***

**10.38.7.2 RPA\_hash generation and resolution after initialization using public addresses**

……….

The IRK shall be generated by concatenating the initiator’s address (AdvAddr) and the responder’s address (RespAddr for one-to-one, or GroupID for one-to-many broadcasting message) (MSBs zero-padded to make 16 bytes).

……….

In one-to-many session, POLL (one-to-many) message (message id 0x12, with MessageControl not set to 0x00) in the first sub-round shall be broadcasted as described in 10.35.8. After initialization using public addresses, an IRK for broadcasting message shall be generated. The IRK for broadcasting message is generated using a GroupID which represents a group of devices in a one-to-many ranging session. By transmitting a Public Advertising Poll Compact frame with the MessageControl field set to 0x21 on the initialization channel, a GroupID is shared with responders.

The GroupID is not shared if a Public Advertising Poll Compact frame with the MessageControl field is not set to 0x21 on the initialization channel. In this case, the value, 0xFFFFFF shall be used to generate the IRK for the RPA\_hash used in POLL (one-to-many) (message id 0x12, with MessageControl not set to 0x00).

……….

IRK2 (for One-to-many Poll Compact frame (message id 0x12, with MessageControl not set to 0x00)) = AdvAddr || GroupID (MSBs zero padded) = 0x000000000000000000006E538F2A3E88

……….

IRK2 (for One-to-many Poll Compact frame (message id 0x12, with MessageControl not set to 0x00)) = AdvAddr || 0xFFFFFF (MSBs zero padded) = 0x000000000000000000006E538FFFFFFF

……….

***--------------------------------------------------------------------------------------------------------------------------------***