**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **Proposed Resolution for Hyperblock Security** |
| Date Submitted | May 2024 |
| Sources | Rojan Chitrakar, Lei Huang (Huawei)rojan.chitrakar@huawei.com |  |
| Re: |   |
| Abstract |  |
| Purpose | To propose resolution for comments related to Hyperblock security 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: Simplified the resolution based on the new block index numbering for hyper blocks.

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

***Part 1:***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| Benjamin Rolfe | 139 | 25 | 9.2.12 | 13 | It is possible (e.g. when hyper-block mode is used) for ranging slot, round and block to repeat, and so thus the frame counter value can repeat. This is used (static?) source EUI to form the nonce (9.3.2.4), which should not repeat for a given key.  | Clarify how repeating the same value of a nonce is prevented in this processing | Revised |
| Benjamin Rolfe | 144 | 26 | 9.2.13 | 13 | It is possible (e.g. when hyper-block mode is used) for ranging slot, round and block to repeat, and so thus the frame counter value can repeat. This is used (static?) source EUI to form the nonce (9.3.2.4), which should not repeat for a given key.  | Clarify how repeating the same value of a nonce is prevented in this processing | Revised |
| Benjamin Rolfe | 145 | 27 | 9.3.2.4 | 5 | Note. In hyper-block mode the block index can repeat. The slot index and round index repeat in every block. This can result in repeating the nonce.  | Add to note: When using hyper-block mode will result in repeating a nonce and so key values need to be updated for Hyper Block boundary or the fabric of the universe will unravel due to nonce repetition.  | Revised |
| Alex Krebs | 50 | 27 | 9.3.2.4 | 1 | Uniqueness of Nonce not guaranteed for Hyperblock Mode 10.13.3.5 | Clarify how/if encryption applies/does not apply to Hyperblock mode. Alternatively, change 10.13.3.5 to clarify that Hyperblock mode must not use Compact frames. | Revised |

**Discussion**：







**Resolution for CID#595 (Youngwan**’s **24/249r) has changed the Ranging Block Index field to 1 octet.**



If the Ranging Block Index field is reduced to 1 octet, the Hyper Block Index can also be included in the Nonce and hence preventing the repeating of the Nonce across hyper blocks.

***Part 2:***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| Alex Krebs | 51 | 27 | 9.3.2.4 | 4 | 16-bit Round Index field is maybe unnecessarily long, since 10.38.10.3.10 defines 255 as max value. | Reduce Round Index field length to 8 bits | Revised |
| Carl Murray | 730 | 70 | 10.38.10.3.18 | 28 | According to pg68, line 6 the ranging block can have a max range of 255 ranging rounds. Does this field need to be restricted? | resolve | Revised |

**Discussions:**





We agree that the Round Index field in the Nonce can be reduced to 1 octet (8 bits).

**Disposition: Revised**

**Disposition Detail:**

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

**9.3.2.4 AEAD Nonce for Compact frames (#51, #730)**

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

…

The Frame Counter field is formatted as illustrated in Figure 4 and the Slot Index field, the Round Index field and the Block Index field are set as the indices of the ranging slot, ranging round and ranging block in which the Compact frame is transmitted or received respectively.

|  |  |  |  |
| --- | --- | --- | --- |
| **Bits: 0-7** | **8-15** | **16-31** | **32-39** |
| Slot Index | Round Index | Block Index | 0x00 |

**Figure 4—Frame Counter field for Compact frame nonce**

NOTE—To ensure the uniqueness of the nonce, the key used to secure Compact frames needs to be updated every time the block structure is setup or re-setup, and not reused used across multiple block structures.

**9.2.12 Outgoing frame security procedure for Compact frames**

…

e) Set frame counter. The frame counter is set as the indices of the ranging slot, ranging round and ranging block in which the Compact frame is to be transmitted, as shown in Figure 4. If the Compact frame is transmitted in the Hyper block mode, the Block Index is set as the ranging block index that is calculated as explained in xxxxx.

**9.2.13 Incoming frame security procedure for the Compact frames**

…

e) Set frame counter. The frame counter is set as the indices of the ranging slot, ranging round and ranging block in which the Compact frame is received, as shown in Figure 4. If the Compact frame is received in the Hyper block mode, the Block Index is set as the ranging block index that is calculated as explained in xxxxx.

**10.38.10.3.18 The Round Index field (#51, #730)**

8-bit index of the current ranging round.