**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.

Rev 2: Added the reference to 10.31.3.5 Hyper block mode based on 24/271.

Rev 3: removed hyperblock related CIDs and changes.

***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** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**Discussion**：



***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.

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

8-bit index of the current ranging round.

***Change the length of the Round Index field in the following locations from “0/2” to “0/1”: Figure 63, Figure 84, Figure 87***