**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](mailto: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.

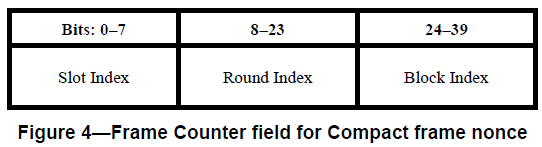
Rev 4: Resolves hyperblock security related CID on top of the changes made by 24/112r3.

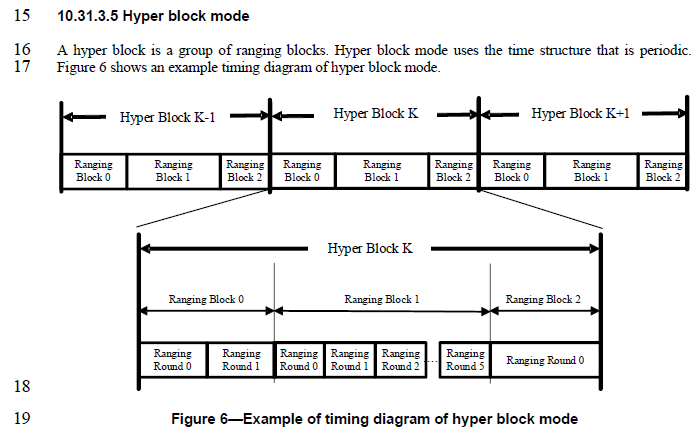
***Comment Indices in 15-24-0010-00-04ab-consolidated-comments-draft-c related to Hyperblock:***

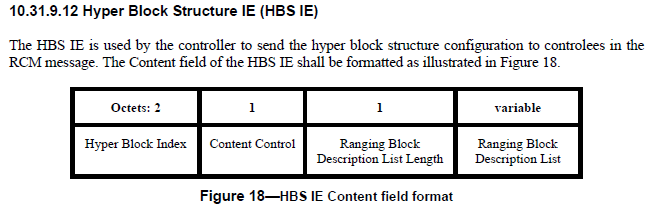
***Part 1:***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **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 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

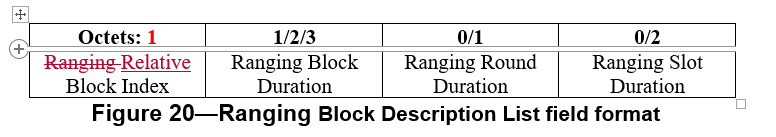
**Discussion**：







**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.

**Disposition: Revised**

**Disposition Detail:**

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

**9.3.2.4 AEAD Nonce for Compact frames (#139)**

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

…

The Frame Counter field for non-hyper block mode is formatted as illustrated in Figure 4. 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 in non-hyper block mode**

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.

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Bits: 0-7** | **8-15** | **16-23** | **24-39** |
| Slot Index | Round Index | Relative Block Index | Hyper Block Index |

**Figure 4B—Frame Counter field for Compact frame nonce in hyper block mode**

NOTE—To ensure the uniqueness of the nonce, the key used to secure Compact frames needs to be updated when the Hyper Block Index field reaches its maximum value.

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

…

e) Set frame counter. In hyper block mode the frame counter is set as the indices of the ranging slot, ranging round, relative ranging block and the hyper block in which the Compact frame is to be transmitted, as shown in Figure 4B. In non-hyper block mode, 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.

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

…

e) Set frame counter. In hyper block mode the frame counter is set as the indices of the ranging slot, ranging round, ranging block and the hyper block in which the Compact frame is received, as shown in Figure 4B. In non-hyper block mode 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.