**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 | February 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.

***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) will/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).

In the non-hyper block mode, every time the block index is reset to 0, the security key needs to be updated in order to prevent the Nonce from repeating. Since the Round Index field only needs one octet, one additional field (called Block cycle field) can be added to the Nonce, and it is incremented by 1 every time the block index is reset without updating the security key. To help the responders synchronize, the current value of Block Cycle index is carried in the SOR and POLL Compact frames.



**Disposition: Revised**

**Disposition Detail:**

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

**9.3.2.4 AEAD Nonce for Compact frames**

***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. The Block Cycle Index field is set as the value of the Block Cycle Index as described in 10.38.10.3.20.

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

**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 when the Block Cycle Index field reaches its maximum value.

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

**10.38.10.6 Start of Ranging Compact frame**

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

…

The Message Control field value shall be either 0x00, 0x10 or 0x20. This value determines the formatting of the Message Content field.

When the Message Control field value is 0x00 the Message Content field shall be formatted as shown in Figure 60.



**Figure 60—Format of the Message Content field in the** **Start of Ranging Compact frame when the Message Control field value is 0x00**

…

The Ranging MAC Configuration field shall be set as per 10.38.10.3.9

Start of Ranging Compact frame with the Message Control field value equal to 0x20 is used when the ranging phase is expected to use secure Compact frames. When the Message Control field value is 0x10 the Message Content field shall be formatted as shown in Figure 60A.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Octets: 1** | **4** | **1** | **6** | **1** | **7** | **3** | **2** | **0/1** |
| Presence Bitmap | Time Offset | NB Channel Seed | NB Channel Map | Management PHY Configuration | Management MAC Configuration | Ranging PHY Configuration | Ranging MAC Configuration | Block Cycle Index |

**Figure 60A—Format of the Message Content field in the Start of Ranging Compact frame when the Message Control field value is 0x20**

The Presence Bitmap field shall be formatted as shown in Figure 60B.

|  |  |
| --- | --- |
| **Bits: 0** | **1-7** |
| Block Cycle Index Present | Reserved |

**Figure 60B—Presence Bitmap field format**

The Block Cycle Index Present field when one indicates that the Block Cycle Index field is included in the Message Content field or is not included when the Block Cycle Index Present field value is zero.

The encoding/meaning of the subsequent fields in the message content except the Number Of Responders field is identical to that for Message Control field value is 0x00 described above.

The Block Cycle Index field if present shall be set as per 10.38.10.3.20.

**10.38.10.7 One-to-one Poll Compact frame (#51, #730)**

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

…

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Octets: 1** | **1** | **0/6** | **0/1** | **0/7** | **0/1** | **0/1** | **0/2** | **0/1** | **0/1** |
| Request Bitmap | Presence Bitmap | NB Channel Map | Management PHY Configuration | Management MAC Configuration | Ranging PHY Configuration | Ranging MAC Configuration | Block Index | Round Index | Block Cycle Index |

**Figure 63—Format of the Message Content field in the One-to-one Poll Compact frame when the Message Control field value is 0x10**

The Request Bitmap field is formatted as per 10.38.10.3.11.

The Presence Bitmap field shall be formatted as shown in Figure 64.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Bits: 0** | 1 | 2 | 3 | 4 | 5 | 6-7 |
| NB Channel Map Present | Management PHY Configuration Present | Management MAC Configuration Present | Ranging PHY Configuration Present | Ranging MAC Configuration Present | Block Round and Block Cycle Index Present | Reserved |

**Figure 64—Presence Bitmap field format**

…

The Block Round and Block Cycle Index Present field when one indicates that the Block index field, the Round Index field and the Block Cycle Index field are included in the Message Content field or are not included when the Block Round and Block Cycle Index Present field value is zero.

**…**

The Round Index field if present shall be set as per 10.38.10.3.18.

The Block Cycle Index field if present shall be set as per 10.38.10.3.20.

**10.38.10.12 One-to-many Poll Compact frame (#51, #730)**

**…**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Bits: 0** | 1 | 2 | 3 | 4 | 5 | 6-7 |
| NB Channel Map Present | Management PHY Configuration Present | Management MAC Configuration Present | Ranging PHY Configuration Present | Ranging MAC Configuration Present | Block Round and Block Cycle Index Present | Reserved |

**Figure 83—Presence Bitmap field format**

**…**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Octets: 3** | **0/6** | **0/1** | **0/7** | **0/1** | **0/1** | **0/2** | **0/1** | **0/1** |
| Responder Address | NB Channel Map | Management PHY Configuration | Management MAC Configuration | Ranging PHY Configuration | Ranging MAC Configuration | Block Index | Round Index | Block Cycle Index |

**Figure 84—** **Responder Detail element format (Message Control = 0x70)**

**…**

The Round Index field if present shall be set as per 10.38.10.3.18.

The Block Cycle Index field if present shall be set as per 10.38.10.3.20.

**…**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Bits: 0** | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| NB Channel Map Present | Management PHY Configuration Present | Management MAC Configuration Present | Ranging PHY Configuration Present | Ranging MAC Configuration Present | Start and End Slot Indexes Present | Block Round and Block Cycle Index Present | Reserved |

**Figure 86—Presence Bitmap field format**

**…**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Octets: 3** | **0/6** | **0/1** | **0/7** | **0/1** | **0/1** | **0/2** | **0/2** | **0/2** | **0/1** | **0/1** |
| Responder Address | NB Channel Map | Management PHY Configuration | Management MAC Configuration | Ranging PHY Configuration | Ranging MAC Configuration | Start Slot Index | End Slot Index | Block Index | Round Index | Block Cycle Index |

**Figure 87—** **Responder Detail element format (Message Control = 0x80)**

**…**

The Round Index field if present shall be set as per 10.38.10.3.18.

The Block Cycle Index field if present shall be set as per 10.38.10.3.20.

**10.38.10.3.18 The Round Index field**

8-bit index of the current ranging round.

***Add the following new subclause after10.38.10.3.18 The Round Index field.***

**10.38.10.3.20 The Block Cycle Index field**

8-bit index of the current ranging block cycle. The value of the field is initialized to zero when a security key used to secure Compact frames is first negotiated or updated. The value of the field is monotonically incremented every time the block index is reset to zero without updating the corresponding security key.

NOTE—The Block Cycle Index field is used to ensure the uniqueness of the nonce for secured Compact frames (as described in 9.3.2.4) when the same security key is used across multiple block structures.