**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **Proposed Resolution for Security – PT Data** |
| Date Submitted | July 2024 |
| Sources | Rojan Chitrakar, Lei Huang (Huawei)rojan.chitrakar@huawei.com |  |
| Re: |   |
| Abstract |  |
| Purpose | To propose resolution for “P802.15.4ab™/D01 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 15-24-0371-00-04ab-consolidated-comments-draft-1-0:***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| Billy Verso | 1038 | 26 | 9.3.4 | 6 | In the secure frames any passthrough data should be encrypted. Securing the MAC payload, i.e. data from the upper layer, is a specified functionality of the 15.4 MAC. Data confidentiality and authenticity should apply to the passthrough data. | Alter text so that the passthrough data is in the encrypted/private part of the frame, for all secured frame types with passthrough data. Also make sure that there is a secured version available of any compact frame with passthrough data. |  |
| Rojan Chitrakar | 105 | 28 | 9.2.12 | 4 | Passthrough field should also be included in the fields to be secured. | Add Passthrough field in the Private Payload field column for all applicable rows and make all necessary changes in the draft to enable the Passthrough field to be secured. |  |
| Tero Kivinen | 319 | 28 | 9.2.12 | 5 | Why are the passthrough fields open payload fields? I would assume that we would like to encrypt communication between upper layers. I can see that Message Control field and Key ID fields must be open payload field, but why do every other field be open?  | Change Open Payload field to be specified as list of fields, i.e. "Message Control field and Key ID field", and move the "all other fields" to private payload fields, i.e., make it encrypted by default, not encrypted as an exception.  |  |
| Tero Kivinen | 638 | 120 | 10.38.9.21 | 2 | I would assume that the passthrough data is exactly something that would need to be encrypted, but currently it is not.  | Either mark passthrough field as being private payload field, or add warning here that its content is not encrypted. |  |
| Billy Verso | 1239 | 120 | 10.38.9.21 | 2 | In the secure frames any passthrough data should be encrypted. Securing the MAC payload, i.e. data from the upper layer, is a specified functionality of the 15.4 MAC. Data confidentiality and authenticity should apply to the passthrough data. | Make it so secure reports encrypt the passthrough data, (but probably not the length though). |  |
| Tero Kivinen | 639 | 120 | 10.38.9.22 | 21 | I would assume that the passthrough data is exactly something that would need to be encrypted, but currently it is not.  | Either mark passthrough field as being private payload field, or add warning here that its content is not encrypted. |  |
| Tero Kivinen | 642 | 121 | 10.38.9.22 | 7 | I would assume that the passthrough data is exactly something that would need to be encrypted, but currently it is not.  | Either mark passthrough field as being private payload field, or add warning here that its content is not encrypted. |  |
| Tero Kivinen | 646 | 122 | 10.38.9.23 | 4 | I would assume that the passthrough data is exactly something that would need to be encrypted, but currently it is not.  | Either mark passthrough field as being private payload field, or add warning here that its content is not encrypted. |  |
| Tero Kivinen | 651 | 123 | 10.38.9.24 | 11 | I would assume that the passthrough data is exactly something that would need to be encrypted, but currently it is not.  | Either mark passthrough field as being private payload field, or add warning here that its content is not encrypted. |  |
| Tero Kivinen | 657 | 124 | 10.38.9.24 | 8 | I would assume that the passthrough data is exactly something that would need to be encrypted, but currently it is not.  | Either mark passthrough field as being private payload field, or add warning here that its content is not encrypted. |  |

**Discussion**：

Currently, secure compact frames only provide security for the Round-trip Time and the Reply Time fields:



It is beneficial to include the Passthrough field in the field to be secured. In addition, the field order can also be swapped so that the secure and unsecure versions of the same frame will have the same order of the fields.





**Disposition: Revised**

**Disposition Detail:**

**Proposed text changes on P802.15.4ab™/D01:**

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

***Change the sub-clause as follows (Track changes ON)***

…

f) **Secure Compact frame**. The Private Payload field and Open Payload field shall be set as indicated in the Table 3. The procedure shall then use the Private Payload field, the Open Payload field, the source address, the frame counter, and the Key to produce the secured Compact frame, according to the transformation process described in 9.3.4.

…

**Table 3—Compact frame exceptions to Private Payload field and Open Payload field definitions**

|  |  |  |
| --- | --- | --- |
| **Compact frame type** | **Private Payload field** | **Open Payload field** |
| One-to-one Initiator Secure Report | The right-concatenation of the Round-trip Time field and the Passthrough field | The Message Control field and all other fields in the Message Content field except the Round-trip Time field and the Passthrough field. |
|
| One-to-one Responder Secure Report | The right-concatenation of the Reply Time field and the Passthrough field | The Message Control field and all other fields in the Message Content field except the Reply Time field and the Passthrough field. |
| One-to-many Initiator Secure Report,with Message Control field = 0x00 | The right-concatenation of the Round-trip Time field and the Passthrough field | The Message Control field and all other fields in the Message Content field except the Round-trip Time field and the Passthrough field. |
| One-to-many Initiator Secure Report,with Message Control field = 0x10 | The right-concatenation of the Round-trip Time Onefield, the Round-trip Time Two field and the Passthrough field | The Message Control field and all other fields in the Message Content field except the Round-trip Time One and Round-trip Time Two fields and the Passthrough field. |
| One-to-many Responder SecureReport | The right-concatenation of the Reply Time field and the Passthrough field | The Message Control field and all other fields in the Message Content field except the Reply Time field and the Passthrough field. |

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

***Change the sub-clause as follows (Track changes ON)***

f) **Unsecure Compact frame**. The Private Payload field and Open Payload field shall be set as indicated in the Table 3. The procedure shall then use the Private Payload field, the Open Payload field, the source address, the frame counter, and the Key to produce the unsecured Compact frame, according to the inverse transformation process described in the security operations, as described in 9.3.5. If the inverse transformation process fails, the procedure shall return with a Status of SECURITY\_ERROR.

**10.38.9.21 One-to-one Initiator Secure Report Compact frame**

***Change the sub-clause as follows (Track changes ON)***

**…**

The MIC field shall be set as specified in 10.38.9.3.18.

|  |  |  |  |
| --- | --- | --- | --- |
| Octets: 1 |  | 5 | 0/variable |
| Key ID |  | Round-trip Time | Passthrough |

**Figure 126—Format of the Message Content field in the One-to-one Initiator Secure Report Compact frame**

The Round-trip Time field value is an unsigned integer that reports the time difference, measured at the

initiator, between the RMARKERs of the initiator’s MMS fragments and the responder’s MMS fragments.

The units of time are specified in 10.29.1.4 *(Ranging counter time unit)*.

**10.38.9.22 One-to-one Responder Secure Report Compact frame**

***Change the sub-clause as follows (Track changes ON)***

**…**

The MIC field shall be set as specified in 10.38.9.3.18.

…

|  |  |  |  |
| --- | --- | --- | --- |
| Octets: 1 |  | 5 | 0/variable |
| Key ID |  | Round-trip Time | Passthrough |

**Figure 129—Format of the Message Content field in the One-to-one Responder Secure Report Compact frame when the Message Control field value is 0x00**

The Reply Time field value is an unsigned integer reporting the time difference, measured at the responder,

between the RMARKERs of the MMS fragments received from the initiator and the MMS fragments

transmitted by the responder. The units of time are specified in 10.29.1.4 *(Ranging counter time unit)*.

…

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Octets: 1 | 1 | 0/6 | 0/1 | 0/7 | 0/3 | 0/2 |  | 5 | **0/variable** |
| Key ID | Presence Bitmap | NB Channel Map | Management PHY Configuration | Management MAC Configuration | Ranging PHY Configuration | Ranging MAC Configuration |  | Reply Time | Passthrough |

**Figure 130—** **Format of the Message Content field in the One-to-one Responder Secure Report Compact frame when the Message Control field value is 0x10**

**…**

The Reply Time field value is an unsigned integer reporting the time difference, measured at the responder,

between the RMARKERs of the MMS fragments received from the initiator and the MMS fragments

transmitted by the responder. The units of time are specified in 10.29.1.4 *(Ranging counter time unit)*.

**10.38.9.23 One-to-many Initiator Secure Report Compact frame**

***Change the sub-clause as follows (Track changes ON)***

**…**

The MIC field shall be set as specified in 10.38.9.3.18.

|  |  |  |  |
| --- | --- | --- | --- |
| Octets: 1 |  | 5 | 0/variable |
| Key ID |  | Round-trip Time | Passthrough |

**Figure 132—Format of the Message Content field in the One-to-many Initiator Secure Report Compact frame when the Message Control field value is 0x00**

The Round-trip Time field value is an unsigned integer that reports the time difference, measured at the

initiator, between the RMARKERs of the initiator’s MMS fragments and the responder’s MMS fragments.

The units of time are specified in 10.29.1.4 *(Ranging counter time unit)*.

…

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Octets: 1 |  | 5 | 5 | 0/variable |
| Key ID |  | Round-trip Time One | Round-trip Time Two | Passthrough |

**Figure 133—Format of the Message Content field in the One-to-many Initiator Secure Report Compact frame when the Message Control field value is 0x10**

The Round-trip Time One field is an unsigned integer that conveys the time difference between the transmit

time of the poll MMS fragments initiating a round-trip time measurement and the receive time of the

response MMS fragments from the responder with Time Shift Indication field (defined in 10.38.9.12) set to

zero that completes the round-trip time measurement. The units of time are as specified in 10.29.1.4

(*Ranging counter time unit*).

**10.38.9.24 One-to-many Responder Secure Report Compact frame**

***Change the sub-clause as follows (Track changes ON)***

**…**

The MIC field shall be set as specified in 10.38.9.3.18.

|  |  |  |  |
| --- | --- | --- | --- |
| Octets: 1 |  | 5 | 0/variable |
| Key ID |  | Round-trip Time | Passthrough |

**Figure 135—Format of the Message Content field in the One-to-many Responder Secure Report Compact frame when the Message Control field value is 0x00**

The Reply Time field value is an unsigned integer reporting the time difference, measured at the responder,

between the RMARKERs of the MMS fragments received from the initiator and the MMS fragments

transmitted by the responder. The units of time are specified in 10.29.1.4 *(Ranging counter time unit)*.

**…**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Octets: 1 | 1 | 0/6 | 0/1 | 0/7 | 0/3 | 0/2 |  | 5 | **0/variable** |
| Key ID | Presence Bitmap | NB Channel Map | Management PHY Configuration | Management MAC Configuration | Ranging PHY Configuration | Ranging MAC Configuration |  | Reply Time | Passthrough |

**Figure 136—Format of the Message Content field in the One-to-many Responder Secure Report Compact frame when the Message Control field value is 0x10**

**…**

The Reply Time field value is an unsigned integer reporting the time difference, measured at the responder,

between the RMARKERs of the MMS fragments received from the initiator and the MMS fragments

transmitted by the responder. The units of time are specified in 10.29.1.4 *(Ranging counter time unit)*.