**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 | January 2025 |
| 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.

Rev 1: Included rest of security related comments. Total 39 CIDs

Rev 2: Minor editorial updates

Rev 3: Added related CIDs 647, 1172, 1173. Key changes since r2 highlighted in CYAN.

*Comments related to* ***secure frame format****:*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| Tero Kivinen | 317 | 27 | 9.2.12 | 3 | There must be a way to secure all compact frames, not only certain specific frame types. If those frames are used to transmit any data over the air, there must be a way to secure them.  | Add format for adding security for all compact frames. | ReviseScheme is modified such that all Compact frame used during ranging can be secured. |
| Billy Verso | 1043 | 28 | 9.2.13 | 13 | Arguably to have secure ranging it may be necessary to secure many or all of the other packets involved in controlling the ranging exchange. In this case it would be better to have a generic way to apply security. One way to do this is to sacrifice a bit of the HASH address say to signal a secured frame. This then could signal the inclusion of an appropriate security header in a similar way to the base standard MAC. Then we would not need to have separate security procedures or separate secured versions of each frame. | Make it possible to secure all frames, as described in the comment, and revise the procedures accordingly. | ReviseAgree in principle. Scheme is modified such that all Compact frame used during ranging can be secured. The MSB of the Message Control field is used to indicate whether a Compact frame is secured. |
| Alex Krebs | 1399 | 119 | 10.38.9.21 | 19 | This is an encrypted report, that is not secure e.g. against the attacks previously presented & discussed to/with the group. | Rename this and all following relevant chapters and messages from "secure" to "encrypted" and change the design such that it adds protection against the attacks presented in 22/410r1 and 23/274r0. | RejectThere are options for both authentication and encryption, hence “encrypted” is not appropriate. The usage of the term “secure” is consistent with the usage in the baseline specs. Secure Compact frames offer data authenticity and confidentiality and may be used to compliment other techniques to prevent clock-related attacks. |
| Billy Verso | 1237 | 119 | 10.38.9.21 | 22 | The four Secure Report messages have similar generic format. Each begins with an RPA Hash and a Message Control Octet, the latter of which is a sparse set of values. Seems we have an opportunity to use a common Compact Frame ID field value for all of these saving on Compact Frame ID space over half of which are used up already. | Change to single "Secure Report" ID in Table 1, and use the Message Control field (octet) to identify the meaning and encoding for the different flavours of secure report: One-to-one Initiator, One-to-one Responder, One-to-many Initiator and One-to-many Responder. | ReviseAgree in principle. The MSB of the Message Control field is used to indicate whether a Compact frame is secured. All variants of secure report frames are deleted. |
| Tero Kivinen | 635 | 119 | 10.38.9.21 | 25 | If there is only one possible value for Message control field, it can be also omitted to make message more compact.  | Remove message control field. | RejectThe referenced sub-clause is deleted and so the comment is no longer applicable. |
| Pooria Pakrooh | 1372 | 121 | 10.38.9.22 | 1 | In Figure 130, change "NB Channel Map" field length to 0/2/5/6. | As in the comment | RejectThe referenced sub-clause is deleted and so the comment is no longer applicable. |
| Libra Xiao | 915 | 121 | 10.38.9.22 | #8,#9,#10 | Original text is :""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. It should be clarified how to obtain the value of the Reply Time parameter in the UWB MMS ranging phase with multiple RSFs and/or RIFs (as shown in the example in Figure 36), as the value of the Reply Time parameter can be the cumulative or mean value of multiple RSFs and/or RIFs. | "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. For the multiple RSFs and/or RIFs of the UWB MMS ranging phase,the value of the Reply Time should be the mean value of several Reply Time parameters measured at the responder. " | RejectThe referenced sub-clause is deleted and so the comment is no longer applicable. |
| Pooria Pakrooh | 1373 | 123 | 10.38.9.24 | 18 | In Figure 136, change "NB Channel Map" field length to 0/2/5/6. | As in the comment | RejectThe referenced sub-clause is deleted and so the comment is no longer applicable. |

*Comments related to* ***frame******content*** *to be secured:*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **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. | ReviseAgree in principle. Scheme is modified such that the entire Message Content field of a Compact frame used during ranging can be secured.  |
| 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. | ReviseAgree in principle. Scheme is modified such that the entire Message Content field of a Compact frame used during ranging can 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.  | ReviseAgree in principle. Scheme is modified such that the entire Message Content field of a Compact frame used during ranging can be secured.  |
| 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. | ReviseAgree in principle. Scheme is modified such that the entire Message Content field of a Compact frame used during ranging can be secured.  |
| 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). | ReviseAgree in principle. Scheme is modified such that the entire Message Content field of a Compact frame used during ranging can be secured.  |
| 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. | ReviseAgree in principle. Scheme is modified such that the entire Message Content field of a Compact frame used during ranging can be secured.  |
| Tero Kivinen | 643 | 121 | 10.38.9.22 | 4 | Is there a reason why presence bitmap, NB Channel Map etc are not private payloads, i.e., not encrypted.  | Move those other fields to be private or add warning here that they are not encrypted. | ReviseAgree in principle. Scheme is modified such that the entire Message Content field of a Compact frame used during ranging can be secured.  |
| 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. | ReviseAgree in principle. Scheme is modified such that the entire Message Content field of a Compact frame used during ranging can be secured.  |
| 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. | ReviseAgree in principle. Scheme is modified such that the entire Message Content field of a Compact frame used during ranging can be secured.  |
| Tero Kivinen | 647 | 122 | 10.38.9.23 | 13 | 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. | ReviseAgree in principle. Scheme is modified such that the entire Message Content field of a Compact frame used during ranging can be secured.  |
| 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. | ReviseAgree in principle. Scheme is modified such that the entire Message Content field of a Compact frame used during ranging can be secured.  |
| Tero Kivinen | 658 | 124 | 10.38.9.24 | 1 | Is there a reason why presence bitmap, NB Channel Map etc are not private payloads, i.e., not encrypted.  | Move those other fields to be private or add warning here that they are not encrypted. | ReviseAgree in principle. Scheme is modified such that the entire Message Content field of a Compact frame used during ranging can be secured.  |
| 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. | ReviseAgree in principle. Scheme is modified such that the entire Message Content field of a Compact frame used during ranging can be secured.  |
| Billy Verso | 1189 | 75 | 10.38.8.3 | 22 | This is the first mention of the Secure Report Compact frame! Does it not apply in the other cases of basic one-to-many, or even the one-to-one cases. I think we need a separate section to cover the secure case(s) | Remove security mention from here and have a separate section where the "high integrity" use case are added on top of all the other use cases, by using secured versions of the appropriate frames | ReviseMention of Secure Report Compact frame are removed from the subclause. |
| Billy Verso | 1172 | 70 | 10.38.?.? | 15 | Not sure where it should go, but noting that we have secure format of some messages, maybe we need a clause on the "high integrity" use case. | Add appropriate clause, to cover the "high integrity" use case and consider what compart frames are used for it and make sure all if these frames can be properly protected from attack by rogues. | Revise |
| Billy Verso | 1173 | 70 | 10.38.?.? | 15 | Given secured compact frames only covers one aspect of the ranging (the reply times) which may be insufficient to be sure of secured ranging, lets remove all mention of compact frame security.  | Remove the secured compact frames and all changes to clause 9. And used base line frame format (adding IE if necessary) to have all necessary frames properly covered with security. | RejectBaseline frame format is not compatible with Compact frame formats. Ability to secure the content of Compact frames is useful independent of secure ranging. |

**Discussion**

Several comments suggested to design a more general way of securing Compact frames instead of limiting security to report frames. Many comments also suggested that the entire Message Content field should be secured instead of only securing the report fields (Reply time or Round-trip time).

**Disposition: Revised**

**Disposition Detail:**

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

**7.3.7.3 Compact Frame ID field**

***Modify Table 1 as follows (Track changes ON):***

**Table 1—Compact frames**

|  |  |  |
| --- | --- | --- |
| **Compact Frame ID value** | **Compact frame name** | **Subclause** |
| … |  |  |
|  |   |  |
|  |  |  |
|  |  |  |
|  |  |  |
| 17 | Secured Compact frame | 10.38.9.2x |
| 18 – 29 | Reserved | - |
| 30 | Reserved for vendor specific use | - |
| 31 | Reserved for extension into 2nd octet | - |

***Delete Sub-clauses 10.38.9.21, 10.38.9.22, 10.38.9.23, 10.38.9.24.***

***Add the following new sub-clause at the end of*** ***10.38.9 Messages for UWB MMS operation:***

**10.38.9.xx Secured Compact frame**

The Secured Compact frame is used when the Message Content field of a corresponding Compact frame is cryptographically protected. The Compact Frame Content field of the Secured Compact frame shall be formatted as shown in Figure xx1.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Octets: 2 | 3 | 0 or 3 | 1 | variable | 4/8/16 |
| Security Control | RPA Hash | RPA Prand | Message Control Version | Message Content | MIC |

**Figure xx1—** **Secured Compact frame Content field format**

The Security Control field shall be formatted as shown in Figure xx2.

|  |  |  |  |
| --- | --- | --- | --- |
| Bits: 0 - 7 | 8 - 10 | 11 - 14 | 15 |
| Secured Compact Frame ID | Security Level | Key ID | Reserved |

**Figure xx2—** **Security Control field format**

The Secured Compact Frame ID field shall be set as the Compact Frame ID of the Compact frame whose Message Content field is to be protected. The Compact frames whose Message Content field may be protected are listed in 10.38.9.2x.

The Security Level field indicates the cryptographic protection level applied to the Compact frame. The security Level field shall have one of the values specified in Table 9-6 except 0 and 4.

The Key ID field identifies the key that is used for cryptographic protection of the Compact frame.

The RPA Hash field shall be set as the RPA Hash carried in the corresponding Compact frame indicated by the Secured Compact Frame ID field.

The RPA Prand field is present if the corresponding Compact frame indicated by the Secured Compact Frame ID field carries a RPA Prand field and is set as the same value. Otherwise, the RPA Prand field is not present.

The Message Control field shall be set as the Message Control field of the corresponding Compact frame indicated by the Secured Compact Frame ID field.

The Message Content field shall be set as the Message Content field of the corresponding Compact frame indicated by the Secured Compact Frame ID field with the same value of the Message Control field.

The MIC field shall be set as specified in 10.38.9.3.18.

**10.38.8.3 Time efficient one-to-many ranging**

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

…

When there are two responders involved in ranging in the same ranging sub-round, the report phase

 consists of one, two, or three periods for transmission of a report packet. The durations of the three

 reporting periods are specified by the *macMms1stReportNSlots*, *macMms2ndReportNSlots*, and

 *macMms3rdReportNSlots* attributes. If the report phase has only a single transmission, the initiator shall

 transmit the One-to-many Initiator Report Compact frame with the Message Control field set to 0x10 or, when security is enabled, the Secured Compact frame carrying the One-to-many Initiator Secure Report Compact frame with the Message Control field set to 0x10 to the two responders in the first reporting period. This message indicates the round-trip time with respect to each of the two responders in the Round-trip Time One and the Round-trip Time Two fields, respectively. If the report phase has two transmissions, the responder with Time Shift Indication field set to zero shall transmit the One-to-many Responder Report Compact frame or when security is enabled, the Secured Compact frame carrying the One-to-many Responder Secure Report Compact frame in the first reporting period, and the responder with Time Shift Indication field set to one shall

 transmit the One-to-many Responder Report Compact frame or the One-to-many Responder Secure Report

 Compact frame in the second reporting period. If the report phase has three transmissions, the responder

 with Time Shift Indication field set to zero shall transmit the One-to-many Responder Report Compact

 frame or when security is enabled, the Secured Compact frame carrying the One-to-many Responder Secure Report Compact frame in the first reporting period, the responder with Time Shift Indication field set to one shall transmit the One-to-many Responder Report Compact frame or when security is enabled, the Secured Compact frame carrying the One-to-many Responder Secure Report Compact frame in the second reporting period, and the initiator shall transmit the One-to-many Initiator Report Compact frame with the Message Control field set to 0x10 or when security is enabled, the Secured Compact frame carrying the One-to-many Initiator Secure Report Compact frame with the Message Control field set to 0x10 in the third reporting period. Figure 43 shows the possible report packet positions in the report phase.

***Add the following new sub-clause:***

**10.38.9.2x Security of Compact frames**

A secured Compact frame is a Compact frame whose Message Content field is cryptographically protected. Only Compact frames that are used within a ranging block structure are eligible for security and these frames are:

* One-to-one Poll
* One-to-one Response
* One-to-one Initiator Report
* One-to-one Responder Report
* One-to-many Poll
* One-to-many Response
* One-to-many Responder Report
* One-to-many Initiator Report

Compact frames used outside a ranging block structure are not eligible for security and these frames are:

* Advertising Poll
* Advertising Response
* Start of Ranging
* Advertising Confirmation
* Public Advertising Poll
* Public Advertising Response
* Public Start of Ranging
* Acquisition

A device may cryptographically protect the Message Content field of an eligible Compact frame if all the intended peer devices have indicated support for the secured Message Content field as described in 10.38.9.3.5.

The device shall process a valid Compact frame to be secured using the outgoing frame security procedure described in 9.2.12. If the Status from the outgoing frame security procedure is not SUCCESS, the MLME shall issue the corresponding primitive with the Status parameter set to the status from the outgoing frame security procedure, indicating the error, and shall not transmit the frame. If the Status from the outgoing frame security procedure is SUCCESS, the MAC sublayer shall transmit the frame.

The device shall process a valid secured Compact frame using the incoming frame security procedure described in 9.2.13. If the Status from the incoming frame security procedure is not SUCCESS, the MLME shall issue the corresponding primitive with the Status parameter set to the status from the incoming frame security procedure, indicating the error. If the status from the incoming frame security procedure is SUCCESS, the unsecured Compact frame shall be processed by the MAC sublayer.

*Comments related to* ***Security Level****:*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| Billy Verso | 1041 | 27 | 9.2.12 | 18 | If security level is zero here, there will be no MIC and the defined secured frame will not even have a CRC. | Add a CRC to these frame types. | ReviseSecurity level zero is disallowed for Compact frames. |
| Tero Kivinen | 320 | 28 | 9.2.13 | 17 | This system assumes there is exactly one security level possible for the device at one time, this makes it impossible to implement devices who want to talk to multiple devices if those devices happen to use different security levels.  | Perhaps the security level should be tied to the key, i.e., when we know the sender and the key used, we could use security level tied to that specific key instead of global security level. Either add support for multiple security levels, or add description of that limitation. | ReviseSecurity Level field is added to a secured Compact frame allowing different security levels for different peers. |
| Tero Kivinen | 331 | 32 | 9.5.1 | 1 | How is the secCompactFrameSecurityLevel negotiated? It is global to device, so it can't be negotiated per device or per network.  | Add reference where the security level for compact frames are negotiated. | ReviseSecurity Level field is added to a secured Compact frame. |
| Billy Verso | 1048 | 32 | 9.5.1 | 1.5 | The secCompactFrameSecurityLevel range references table 9-6 which includes bits to be sent in the security header so that receiver knows the security level to be used for decoding the frame. Is such a field needed for secured Compact frames? The Key ID octet could be reduced to 5 bits to carry this in the other 3 bits. | If it is not needed then the description should say "to be used both in securing outgoing compact frames and processing incoming secured compact frames," Or perhaps we need separate TX and RX values if this can be asymmetric with different capability in TX and RX devices. | ReviseSecurity Level field is added to a secured Compact frame. |
| Billy Verso | 1049 | 32 | 9.5.1 | 1.6 | Are all 8 levels here applicable? Do we need this flexibility, if not perhaps a single level could be specified, which would reduce the testing needed for validation of products and for interworking tests. | Consider whether all 8 levels are applicable/needed and if not specify only those that are. | ReviseSecurity level zero and four are disallowed for Compact frames. Rest 6 levels may be used. |
| Billy Verso | 1050 | 32 | 9.5.1 | 1.7 | The secCompactFrameSecurityLevel description says the value is "negotiated for Compact frames".  | If a negotiation mechanism is part of the standard, add a reference to the clause where it is described. Otherwise say that this is decided via out of band means.  | ReviseThe *secCompactFrameSecurityLevel* attribute is deleted. |
| Billy Verso | 1238 | 119 | 10.38.9.21 | 23 | How does the MAC receiving this frame know what size the MIC is, i.e. can it tell the difference between a longer MIC or a Shorter mic with passthrough data which it says "presence can be inferred from the frame length". | Consider if we need something in MHR to indicate MIC length | RejectThe Security Level indicates the MIC length. |

*Comments related to* ***KeySource, KeyIndex, Secuirty PIBs****:*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| Billy Verso | 1040 | 27 | 9.2.12 | 13 | The "extended address" here (as described in 10.38.9.2.3) may be the address of the destination, what information in the MCPS-DATA.request does the MAC use to know which extended address to use. | Clarify how this is determined, either here or in 10.38.9.2.3, with reference to the appropriate MCPS-DATA.request parameter. | ReviseCompactSecurityParams element carrying the KeySource (an extended address) is added to the MCPS-DATA.request  |
| Tero Kivinen | 322 | 29 | 9.2.13 | 15 | The output fields of KeySource and KeyIndex are not yet initialized here, so they can't be used when searching for the key. The step c could in theory fill in the KeySource provided it has a way of mapping the RPA hashes extracted from the frame to extended address, but KeyID has not yet been parsed.  | Add step between b and c that will parse the frame and fill in the KeyID and KeySource fields that can be used in c and d steps. | ReviseA parsing step is added as suggested to obtain the security level and Key ID. |
| Tero Kivinen | 321 | 29 | 9.2.13 | 11 | How does the recipient of the frame know the originator of the compact frame? The compact frames in question only have either initiator or the responder RPA hash, so it needs to somehow map that to the extended address of the originator.  | Describe how the initiator RPA hash and responder RPA hash are mapped to the extended address of the originator. | ReviseReference is added to 10.38.9.2.3 in which the procedure is described |
| Billy Verso | 1044 | 29 | 9.2.13 | 11 | It is not immediately apparent to me where to get the "extended address of the originator". Also, does this work for group addressing? | Add to the line some additional text to indicate where/how this is address is retrieved . | ReviseReference is added to 10.38.9.2.3 in which the procedure is described |
| `Billy Verso | 1047 | 32 | 9.5.1 | 1.2 | secCompactFrameSecurityEnabled seems superfluous since there are specific "secure" compact frames. On RX side when these form of frames are received they should be validated and discarded. Or maybe we need to add text to make the non-secure ones be discarded if security is enabled? On TX side, I assume that the next higher layer is involved in the decision to send the report so again it can choose whether to send secure/unsecure ones? | In it is not needed delete it or describe some the uses cases where it has a role. Suggest to do this in a new high-integrity (not called secure) MMS section of 10.39. | ReviseThe purpose is similar to that of the macSecurityEnabled PIB for non Compact frames. |
| Tero Kivinen | 333 | 32 | 9.5.11 | 6 | The key should also be associated with the Aead Algorithm as specified in the Table 9-9 to provide crypto agility.  | Add Aead Algorithm to be associated with the key. | RevisesecAeadAlgorithm is added to the secCompactFrameKeyDescriptor |
| Billy Verso | 1051 | 32 | 9.5.11 | 7 | secCompactFrameKeyID says range is as described in10.38.9.3.21, but that clause does not give any range or size. I think it is a single Octet so the range here is 0 to 255. Good to clarify if same key ID might be used for a different link and decided based on RPA resolution also, or is unique. | Change to say range is 0 to 255, and add text to indicate if appropriate that it shall be a unique number in the list, or if this is not the case that it needs to be qualified by some address resolution also. | Revise10.38.9.3.21 is deleted. Clarified the range as 0x00 – 0x07 based on a 3 bits field. |

**8.3.4 MCPS-DATA.request**

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

**Table 2—Elements of the CompactFrameDescriptor**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid Range** | **Description** |
| … |  |  |  |
| CompactMessageControl | Unsigned Integer | 0x00–0xff | This provides Message Control field value,which identifies the contents of the MessageContent field |
| CompactMessageContent | Set of octets | - | The data to be contained in the MessageContent field. |
| CompactSecurityEnabled | Boolean | FALSE, TRUE | When TRUE indicates that the Message Content field of the Compact frame is secured. |
| CompactSecurityParams | Structure | As defined in Table 8-XX | Carries the security parameters for Compact frame. Only present if CompactSecurityEnabled is TRUE. |
|  |  |  |  |

***Add a new table as follows (Track changes ON)***

**Table 8-XX—Elements of the CompactSecurityParam**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid Range** | **Description** |
| SecurityLevel | Integer | 0x01-0x03, 0x05-0x07 | The security level purportedly used by theReceived Compact frame or to be used when transmitting aCompact frame, as defined in Table 9-6. |
| KeyIndex | Integer | 0x00 – 0x07 | The index of the key purportedly used by the originator of the received Compact frame or to be used when transmitting a Compact frame. |
| KeySource | IEEE address | An extendedIEEE address | The Extended address associated with the key purportedly used by the originator of the received frame or to be used when transmitting a frame as described in 10.38.9.2.3.  |

**9.2.1 General**

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

A device may optionally implement security. A device that implements security shall provide a mechanism for the MAC sublayer to perform cryptographic transformations on incoming and outgoing frames using information in the PIB attributes associated with security only if the macSecurityEnabled attribute is set to TRUE for frames other than Compact frames and only if secCompactFrameSecurityEnabled is set to TRUE for Compact frames. A device that does not implement security is not required to provide a mechanism for the MAC sublayer to perform any cryptographic transformation on incoming and outgoing frames nor require any PIB attributes associated with security.

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

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

This procedure shall be used to secure the Compact frames that are eligible for security as described in 10.38.9.2x:

 This procedure does not apply to Compact frames that are eligible for security.

To secure other frame types, the procedure in 9.2.2 shall be used.

 The inputs to this procedure are the Compact frame to be secured, the SecurityLevel, KeySource, and KeyIndex parameters. The inputs are as follows:

 ⎯ SecurityLevel shall be set to the Security Level element inside the CompactSecurityParams element in the MCPS-DATA.request primitive.

 ⎯ KeySource shall be set to the KeySource element inside the CompactSecurityParams element in the MCPS-DATA.request primitive.

 ⎯ KeyIndex shall be set to the KeyIndex element inside the CompactSecurityParams element in the MCPS-DATA.request primitive.

The outputs from this procedure are the Status of the procedure and, if this Status is SUCCESS, the secured Compact frame.

 This procedure involves the following steps:

 a) Is security needed? If the SecurityLevel parameter is zero or four, the procedure shall return with a Status of UNSUPPORTED\_SECURITY.

 b) Is security enabled? If secCompactFrameSecurityEnabled is set to FALSE, the procedure shall return with a Status of UNSUPPORTED\_SECURITY.

…

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 4. 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 3.

f) I**nsert Security Control field**. The Security Control field is added to the frame as follows:

1. The Secured Compact Frame ID field shall be set as the Compact Frame ID of the Compact frame to be secured.
2. The Security Level field of the Security Control field shall be set to the SecurityLevel parameter.
3. The Key ID field of the Security Control field shall be set to the KeyIndex parameter.

g) **Secure Compact frame**. The Private Payload field shall be set to the Message Content field, and Open Payload field shall be empty. 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.

…

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

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

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

This procedure shall be used for the incoming Compact frames that are eligible for security as described in 10.38.9.2x.

This procedure does not apply to Compact frames that are not eligible for security.

 For other frame types, the procedures in 9.2.4 or 9.2.5 shall be used.

 The inputs to this procedure are the Compact frame to be unsecured.

The outputs from this procedure are the status of the procedure and, if the status is SUCCESS the

unsecured Compact frame, and the *CompactSecurityParams* containing the Security Level, KeySource, and Key ID.

All outputs of this procedure are assumed to be invalid unless and until explicitly set in this procedure.

This procedure involves the following steps:

 a) **Check for secCompactFrameSecurityEnabled**. If *secCompactFrameSecurityEnabled* is set to FALSE, the procedure shall return with a Status of UNSUPPORTED\_SECURITY.

 b) **Parse Security Control field**. The procedure shall set SecurityLevel and

KeyIdex to the Security Level field and Key ID field, respectively, of the frame to be unsecured. If the SecurityLevel is zero or four, the procedure shall return with a Status of UNSUPPORTED\_SECURITY. If the Secured Compact Frame ID field is not set as the ID of a Compact frame eligible for security, the procedure shall return with a Status of UNSUPPORTED\_SECURITY.

c) **Obtain source address**. Source address and KeySource shall be set to the extended address of the originator of the Compact frame as described in 10.38.9.2.3.

…

f) **Unsecure Compact frame**. The Private Payload field shall be set to the Message Content field, and Open Payload field shall be empty. 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.

g) **Return unsecured Compact frame**. The procedure shall return with the unsecured Compact

frame, the *CompactSecurityParams* containing the Security Level, KeySource, KeyIndex and a Status of SUCCESS.

**9.3.4 AEAD transformation data representation**

 **9.3.4.3 a data and m data**

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

***Change the main and NOTE paragraphs of 9.3.4.3 (a data and m data) as shown:***

 In the AEAD transformation process, the data fields shall be applied as in Table 9-3. For frames other than

 Compact frames, the MHR is as defined in 7.2. For secure Compact frames, the MHR as used in Table 9-3, is defined as the right-concatenation of the Frame Type field, the Compact Frame ID field, the Security Control field, the RPA Hash field, if present, the RPA Prand field, and the Message Control field.

 NOTE—For frames other than Compact frames, the MHR contains the Auxiliary Security Header field, as defined in

 7.2.

 **9.3.5 AEAD inverse transformation data representation**

 **9.3.5.3 c data and a data**

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

***Change the main and NOTE paragraphs of 9.3.5.3 (c data and m data) as shown:***

 In the AEAD inverse transformation process, the data fields shall be applied as in Table 9-5. For frames

 other than Compact frames, the MHR is as defined in 7.2. For secure Compact frames, the MHR as used in Table 9-5, is defined as the right-concatenation of the Frame Type field, the Compact Frame ID field, the Security Control field, the RPA Hash field and, if present, the RPA Prand field, and the Message Control field.

 NOTE—For frames other than Compact frames, the MHR contains the Auxiliary Security Header field, as defined in

 7.2.

***Change sub-clause 9.3.3 as follows (Track changes ON)***

**9.3.3 AEAD prerequisites**

 ***Change the second paragraphs of 9.3.3 (AEAD prerequisites) as shown:***

 The length M of the Authentication field for the AEAD forward transformation and the AEAD inverse

 transformation is determined from Table 9-6, using the Security Level field of the Security Control field for Compact frames

 and using the Security Level field of the Security Control field of the auxiliary security header of the frame

 for frames other than Compact frames.

***Change Table 9-8 as follows (Track changes ON)***

**Table 9-8—Security-related MAC PIB attributes**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Attribute** | **Type** | **Range** | **Description** | **Default** |
| … |  |  |  |  |
| *secCompactFrameSecurityEnabled* | Boolean | TRUE, FALSE | Indication of whetherthe security ofCompact frames isenabled. A value ofTRUE indicates thatsecurity is enabled,while a value ofFALSE indicates thatsecurity is disabled. | FALSE |
|  |  |  |  |  |

**9.5.11 secCompactFrameKeyDescriptor**

***Add a new row at the end of Table 4 as follows (Track changes ON)***

**Table 4—Elements of the secCompactFrameKeyDescriptor**

|  |  |  |  |
| --- | --- | --- | --- |
| **Attribute** | **Type** | **Range** | **Description** |
| … |  |  |  |
| *secCompactFrameKeyID* | Integer | 0x00 – 0x15 | The Key ID associated with the*secCompactFrameKey*, |
| *secCompactFrameKey* | Set of octets | - | The value of the key used for Compact frames |
| *secAeadAlgorithm* | Integer | As defined inTable 9-9 | The AEAD algorithm selected by thesecAeadAlgorithm attribute as definedin Table 9-9. |

*Comments related to* ***Nonce****:*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| Li-Hsiang Sun | 234 | 30 | 9.3.2.4 | 6 | A compact frame could occupy multiple slots and multiple slot indices.  | Add a clarification that the slot index in Fig 3,4 refers to the slot at the start of a compact frame  | ReviseClarification is added as suggested. |
| Tero Kivinen | 327 | 30 | 9.3.2.4 | 7 | This requirement is needed for the security of the system, so it can't be in the informal note.  | Add text saying that different key shall be used for each block structure setups. | ReviseNote is deleted and rewritten as normative requirement. |
| Billy Verso | 1045 | 30 | 9.2.13 | 7 | Given this note and the one on line 14, it is worth also mentioning what frames/formats are necessary to use to ensure block, round and slot indices are aligned. | Specify the Compact Frame formats used to signal these indices. Maybe also mandate their use? | ReviseNote is added regarding relevant frames. |
| Billy Verso | 1046 | 30 | 9.2.13 | 7 | If security / reply attack protection is relying on block, round and slot indices, the frames used to signal these also need to be secured. | Include security for those frames also. | ReviseScheme is modified such that all Compact frame used during ranging can be secured. However, SOR cannot be secured. |

**9.3.2.4 AEAD Nonce for Compact frames**

***Change Table 9-8 as follows (Track changes ON)***

…

The Frame Counter field for non-hyper block mode is formatted as illustrated in Figure 3 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. If the Compact frame occupy more than one slot, the Slot Index field is set as the index of the ranging slot in which the transmission or the reception of the Compact frame starts.

NOTE – In the block-based mode, an SOR Compact frame carrying a Starting Block Index field provides synchronization to the index of the first ranging block, and an One-to-one Poll Compact frame or an One-to-many Poll compact frame carrying a Block Index field and a Round Index field provide synchronization to the indices of the current round and block.



When the index of the ranging block used in the frame counter reaches its maximum value, the associated keying

material shall no longer be used, thus requiring this key to be updated by changing to use a new key. This

provides a mechanism for ensuring that the keying material for every frame is unique and, thereby, provides

for sequential freshness.

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



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.