**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | LB119 Comment resolution on security CIDs | |
| Date Submitted | 18, May, 2016 | |
| Source | Jae Seung Lee ETRI  218 Gajeong-ro, Yuseong-gu, Daejeon, 305-700, Korea | Voice: +82 42 860 1326 Fax: +82 42 860 1326 E-mail: jasonlee@etri.re.kr |
| Re: | LB119\_Consolidated\_Comments | |
| Abstract | This document proposes comment resolution on Security CIDs. | |
| Purpose | To be used by the technical editor to apply the necessary changes to the draft. | |
| Notice | This document has been prepared to assist the IEEE P802.15. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. | |
| Release | The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15. | |

**List of contributors**

|  |  |
| --- | --- |
| **Name** | **Affiliation** |
| Jae Seung Lee | ETRI |
| Jaewoo Park | ETRI |
| Jeeyon Choi | ETRI |
| Moon-Sik Lee | ETRI |
| Yeong Jin Kim | ETRI |

CID 24 and 37

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| 24 | 31 | 6.3.4a.2 | 37 | Now when we have only one SFC per aggregated data, but inside the aggregated data we have multiple FCS and Integrity code fields, it is possible that one of those subframe checks fail. What shall we do with the rest of the subframes. We could try to continue processing them, but we need to keep incrementing SFC for each FAILED subframe too, as otherwise the integrity check always fails. | Add text somewhere explaining what to do for the rest of the subframes, when one of the subframe integrity code or FCS fail. Section 7.9 might be good candidate for the text too, i.e., sender will increment SFC for each frames it sends, and recipient ignores every subframe after the first error. | Revised  Agree in principle.  The SFC increment for each transmitted subframes is already specified in 6.2.7.3 (SFC field).  Receiver’s behavior is added to 8.3.7 (Secure frame reception) instead of 7.9.  See the proposed text in 15-16-0413r0 |
| 37 | 66 | 8.1.7 | 62 | The last SFC received needs to be defined so it is only after the integrity check has passed, the last SFC is stored. I do not remember what is the definition of “received” here, but in some other standards it was just defined so that it passes the FCS check, and no other checks are needed. | Add text explaining that last SFC received is only updated after successfully verifying the integrity code. This could also be in the section 8.3.7 last paragraph. | Revised  Agree in principle.  See the proposed text in 15-16-0413r0 |

**CID 24 and 37: Proposed Text (based on 802.15.3e D02 and 802.15.3RevA-D02)**

***Change the following paragraphs in clause 8.1.7 (Freshness protection) of 802.15.3e D02 as follows:***

To prevent replay of old messages, a strictly-increasing time token is included in the beacon. A DEV shall reject as invalid a received beacon with a time token less than or equal to the current time token. For HRCP, a DEV shall further check the SFC and the SECID included in the beacon and shall reject as invalid the beacon if the SFC in the beacon is not strictly greater than the last SFC received from that DEV corresponding to the key identified by the SECID. The last SFC received shall be only updated after the received integrity code corresponding to the SFC is verified successfully. In addition, for non-HRCP, the time token is included in the nonce, as described in 9.2.4, for each secure frame, as described in 6.2, so the integrity check will fail if a frame is replayed in a different superframe. For HRCP, a DEV shall check the SFC and the SECID included in each secure frame, and shall reject as invalid the received frame if the SFC in the frame is not strictly greater than the last SFC received from that DEV corresponding to the key identified by the SECID to detect wheter the frame is replayed or not. The last SFC received shall be only updated after the received integrity code corresponding to the SFC is verified successfully. A DEV maintains two values for freshness. The CurrentTimeToken is the time token value found in the beacon for the current superframe and is used to protect all messages sent and check all messages received during that superframe. For HRCP, the values are used only to check beacon freshness and the SFC is used to check freshness of other frames. The LastValidTimeToken is used by the DEV to ensure that the security of the beacons have not been compromised.

***Change the following paragraphs in clause 8.3.7 (Secure frame reception) of 802.15.3e D02 as follows:***

Before any security operations have been performed on a received frame, the DEV shall check the FCS. For HRCP, if the FCS check for a subframe in the received aggregated frame fails, then the subframe and the other subframes after the subframe in the aggregated frame shall be ignored by the DEV. Table 8-1 provides a listing of the keys that shall be used to protect secure frames and the frames that shall be sent without security for non-HRCP. Table 8-1a provides the listing for HRCP. A DEV may ignore any secure frame if the only key selection in Table 8-1 or Table 8-1a is “none.” A DEV shall ignore any nonsecure frame or a secure frame with an incorrect SECID when security is required.

An associated device that has not yet received the piconet group data key or Pairnet group data key shall accept all secure beacons and ignore the integrity code, SECID, and secure frame counter. When the DEV has received the piconet group data key or Pairnet group data key, it shall set the LastValidTimeToken and CurrentTimeToken to be the time token in that beacon.

When a DEV receives a secure beacon frame, as defined in 6.3.1.2, the DEV shall determine if the received time token is greater than the CurrentTimeToken and less than the LastValidTimeToken + *mMaxTimeTokenChange*.

If not, the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the ReasonCode set to BAD-TIME-TOKEN and shall not perform any additional operations on the received beacon. The DEV shall also determine if the SECID matches the SECID of the piconet group data key or Pairnet group data key stored in the MAC/MLME, or the SECID of a valid old piconet group data key or old Pairnet group data key, as described in 8.3.5. If the SECID matches, an HRCP DEV shall further check the SFC included in the beacon and the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the ReasonCode set to BAD-TIME-TOKEN and shall not perform any additional operations on the received beacon if the SFC in the beacon is not strictly greater than the last SFC received from that DEV corresponding to the key identified by the SECID. The last SFC received shall be only updated after the received integrity code corresponding to the SFC is verified successfully. If the SECID does not match, the DEV may request a new piconet group data key or new Pairnet group data key, as described in 8.3.2. If these checks succeed, the DEV shall check the integrity code on the beacon using the piconet group data key or Pairnet group data key. If this succeeds, the DEV shall accept the beacon and set the LastValidTimeToken and CurrentTimeToken to be the time token in the beacon.

When a DEV receives a secure non-Beacon frame, it shall use the appropriate keying material depending on the type of frame, SECID, and SrcID found in the frame. If the SECID in the frame does not correspond to known keying material in the receiving DEV, the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the ReasonCode set to UNAVAILABLE-KEY and shall not perform any additional operations on the received frame. For non-HRCP, a DEV shall reject all frames that do not have an SFC that is strictly greater than the last SFC received from that DEV in that superframe. For HRCP, a DEV shall reject all frames that do not have an SFC that is strictly greater than the last SFC received from that DEV corresponding to the key identified by the SECID in the received frames. The last SFC received shall be only updated after the received integrity code corresponding to the SFC is verified successfully.

***Change the following paragraphs in clause 8.3.7 (Secure frame reception) of 802.15.3RevA-D02 as follows:***

If there are no previous security errors in the processing of the frame, the DEV shall apply the operations defined by the symmetric key security operations to the frame, as defined in 9.3.2 for non-HRCP and 9a.3.2 for HRCP. If any of the security operations fail, the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the ReasonCode set to FAILED-SECURITY-CHECK and shall not perform any additional operations on the received frame. For HRCP, if the integrity code check for a subframe in the received aggregated frame fails, then the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the ReasonCode set to FAILED-SECURITY-CHECK and shall not perform any additional operations on the subframe and the other subframes after the subframe in the aggregated frame. If the security operations have been successfully performed and the frame has been modified appropriately, the DEV may then continue to process the frame.

CID 38 and 51

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| 38 | 74 | 9a.2.2 | 16 | Time Token field is no longer used when using HRCP devices. Only SFC is used. | Remove reference to the Time Token field. | Revised  Time Token is not used for non-beacon frames, but it is still used for beacon frames for checking beacon freshness.  It is better to mention that the Time Token is only used for beacon frames.  See the proposed text in 15-16-0413r0 |
| 51 | 128 | C.3.2 | 58 | Why is there reference to the Time Token in this section. I think only SFC is used anymore. | Remove “6 octet time token is used in HRCP”. | Rejected.  Time Token is not used for non-beacon frames, but it is still used for beacon frames for checking beacon freshness.  For example, When a DEV receives a secure beacon, the DEV determines if the received time token is greater than the CurrentTimeToken and less than the LastValidTimeToken + *mMaxTimeTokenChange*. 15.3e inherits this feature from the baseline. |

**CID 38: Proposed Text (based on 802.15.3e D02)**

***Change the following paragraphs in clause 9a.2.2 of 802.15.3e D02 as follows:***

**9a.2.2 Galois/Counter Mode (GCM) combined encryption and data authentication**

The security operation for HRCP is based on the GCM mode of the AES encryption algorithm. GCM provides confidentiality, authentication, and integrity for secure frames defined in this standard. The Secure Frame Counter (SFC) field provides message freshness as a defense against replay attacks. The SFC field and the Time Token field in the secure beacon frames provide message freshness for the secure beacon frames. GCM is constructed from a symmetric key block cipher with a block size of 128 bits, such as the Advanced Encryption Standard (AES) algorithm. GCM is defined in NIST Special Publication 800-38D.

CID 101

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| 101 | 26 | 6.3.1.2a | 50 | Chane "P2P synchronization parameters" to "Pairnet Synchronization Parameters". Change the field in the other sub-clauses, too. (Clause 9a.3.2, etc.) | Chane "P2P synchronization parameters" to "Pairnet Synchronization Parameters". Change the field in the other sub-clauses, too. (Clause 9a.3.2, etc.) | Revised  See the proposed text in 15-16-0413r0 |

**CID 101: Proposed Text (based on 802.15.3e D02)**

***Change the following figure and the paragraph in clause 6.3.1.2a of 802.15.3e D02 as follows:***

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Octets: 2** | **6** | **6** | **15** | **variable** | **…** | **variable** | **16** | **4** |
| SECID | SFC | Time Token | Pairnet Synchronization Parameters | Informationelement-  1 | … | Information  element-*n* | Integrity  Code | FCS |

**Figure 6-51a—Secure beacon frame format for HRCP**

The Pairnet Synchronization Parameters field is defined in 6.3.1.1a.

***Change the following figure and the paragraph in clause 9a.3.2 of 802.15.3e D02 as follows:***

Figure9a-2 specifies the length information and data input to the GCM operation for secure beacons. The Auth Data Length in octets, *l(a),* shall be set to the length of the Frame Header, SECID, SFC, Time Token, all of the Pairnet Synchronization Parameters field plus the sum of the lengths of the IEs that are included in the beacon. The Enc Data Length in octets, *l(p)*, shall be set to zero. The data input to GCM shall be taken in the order it is received in the frame, omitting the HCS, FCS and Integrity Code.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Octets: 10** | **2** | **6** | **6** | **15** | **L1** | **…** | **L*n*** |  | **2** | **2** |
| Frame Header | SECID | SFC | Time Token | Pairnet Synchronization Parameters | IE-1 | … | IE-*n* |  | Auth Data Length | Enc Data Length |

**Figure 9a-2 GCM input for secure beacons**

CID 100

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| 100 | 65 | 8 | 41 | Check the consistency with the latest baseline. | Modify Clause 8 to reflect the changes in the latest baseline | Revised  See the proposed text in 15-16-0413r0 |

**CID 100: Proposed Text (based on 802.15.3e D02 and 802.15.3RevA-D02)**

***Change the following paragraphs of 802.15.3RevA-D02 as follows:***

**6.5.2 Security commands**

This set of commands is used to establish the security and privacy functions between a DEV and the PNC and between DEVs in the piconet, and between a DEV and the HRCP PNC in the pairnet.

***Delete the paragraph under 8.Security as follows:***

**8. Security**

***Delete the sub-clause title and the paragraph under 8.1.3 Data encryption as follows:***

***Change the last paragraph in sub-clause 8.3.2 of 802.15.3RevA-D02 as follows:***

If a DEV receives a beacon with a time token greater than the last known time token, but with a SECID that does not match the SECID of the known key, the DEV shall send a Key Request command to the PNC or HRCP PNC to obtain the new key.

***Change sub-clause 8.4.3 of 802.15.3RevA-D02 as follows:***

**8.4.3 Key request protocol**

In a secure piconet or pairnet, if a DEV receives a frame or beacon with an unknown SECID, it may initiate the request key protocol in order to obtain the unknown key from the key originator of the relationship. The DEV initiates the protocol by sending the Request Key command to the key originator. When the key originator receives a Request Key command that has a valid Integrity Code, it checks to see whether it has a secure relationship with the requesting DEV. If there is a secure relationship, the key originator sends the Request Key Response command to the requesting DEV using the management key for that secure relationship.

***Modify Table 8-1a as follows:***

Table 8-1a—Key selection for secure HRCP frames

| Frame type or command | None | HRCP PNC-DEV mgmt key | Pairnet group data key | Comment |
| --- | --- | --- | --- | --- |
| Beacon frame |  |  | X | All secure beacon frames shall be protected by the Pairnet group data key. |
| Stk-ACK frame | X |  |  | Stk-ACK frames shall not be secured with any key. |
| Data frame |  |  | X | Only secure data frames shall be exchanged between DEVs that have a secure relationship. The Pairnet group data key shall be used for secure data frames between DEVs in Pairnet. |
| Association request | X |  |  | Association Request commands shall not be secured with any key. |
| Association response | X |  |  | Association Response commands shall not be secured with any key. |
| Disassociation request | X | X |  | Disassociation Request commands shall not be secured with any key before the DEV establishes secure membership in the Pairnet and shall be protected by the HRCP PNC-DEV management key otherwise. |
| Request key |  | X |  | The management key for the relationship shall be used for this command. |
| Request key response |  | X |  | The management key for the relationship shall be used for this command. |
| Distribute key request |  | X |  | The management key for the relationship shall be used for this command. |
| Distribute key response |  | X |  | The management key for the relationship shall be used for this command. |
| Security Information Request |  | X |  |  |
| Security Information |  | X |  |  |
| Probe request | X | X | X | If the Probe Request command is sent to or from the HRCP PNC before the DEV becomes a secure member of the Pairnet, the command shall not be secured by any key. If the DEVs do not share an individual relationship, the Pairnet group data key shall be used. Otherwise, the HRCP PNC-DEV management key for the relationship shall be used. |
| Probe Response | X | X | X | If the Probe Request command is sent to or from the HRCP PNC before the DEV becomes a secure member of the Pairnet, the command shall not be secured by any key. If the DEVs do not share an individual relationship, the Pairnet group data key shall be used. Otherwise, the HRCP PNC-DEV management key for the relationship shall be used. |
| Transmit power change |  | X | X | If the DEVs do not share an individual relationship, the Pairnet group data key shall be used. Otherwise, the HRCP PNC-DEV management key for the relationship shall be used. |
| Array training |  | X | X | If the DEVs do not share an individual relationship, the Pairnet group data key shall be used. Otherwise, the HRCP PNC-DEV management key for the relationship shall be used. |
| Security Message | X |  |  |  |
| PM Mode Change Response |  | X |  |  |
| PM Mode Change |  | X |  |  |
| Vendor Defined |  | X | X | If the DEVs do not share an individual relationship, the Pairnet group data key shall be used. Otherwise, the HRCP PNC-DEV management key for the relationship shall be used. |