**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | Sponsor Ballot Comment resolution on Security Part 1 | |
| Date Submitted | November 9, 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: | Recirculation\_Sponsor\_Ballot\_Consolidated\_Comments | |
| Abstract | This document proposes comment resolution on Security CIDs for TG3e Recirculation Sponsor Ballot. | |
| 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 |
| Moon-Sik Lee | ETRI |
| Yeong Jin Kim | ETRI |

CID r02-25

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| r02-25 | 160 | E.7.3.1a | 45 | Add Non-secure multi-protocol data frame and secure multi-protocol data frame for pairnet. | As in the comment | Revised  See the proposed change in 15-16-0804r0. |

**Proposed Text (based on 802.15.3e D06)**

***Add two entries into Table E-3a MAC frames for pairnet as follows:***

**E.7.3.1a MAC frames for pairnet**

**Table E-3a—MAC frames for pairnet**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Item number** | **Item description** | **Reference** | **HRCP Transmitter** | | **HRCP Receiver** | |
| **Status** | **Support**  **N/A Yes No** | **Status** | **Support**  **N/A Yes No** |
|  | (snip) |  |  |  |  |  |
| MF2.10 | Non-secure Multi-protocol Data frame | 6.3.5.1 | X |  | X |  |
| MF2.10a | Non-secure Pairnet Aggregated Multi-protocol Data frame | 6.3.5a.1 | O |  | O |  |
| MF2.11 | Secure Multi-protocol Data frame | 6.3.5.2 | X |  | X |  |
| MF2.11a | Secure Pairnet Aggregated Multi-protocol Data frame | 6.3.5a.2 | O |  | O |  |
|  | (snip) |  |  |  |  |  |

CID r02-23

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| r02-23 | 103 | 9a.4.6 | 41 | Since only the SFC is used for non-Beacon frame, this sentence should be modified. | As in the comment | Revised  See the proposed change in 15-16-0804r0. |

**Proposed Text (based on 802.15.3e D06)**

***Change the last paragraph of 9a.4.6 as follows:***

**9a.4.6 Restrictions**

**….**

The recipient shall use the Time Token and SFC in the received Beacon frame to detect replay attacks on the Beacon frame and ensure beacon freshness. To detect replay attacks on other frames, the recipient shall use the SFC in the received frame. The recipient shall discard the received frame if the replay attack is detected.

CID r02-4

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| r02-4 | 35 | 6.2 | 60 | 15.3e is modifying the definition of pMaxFrameBodySize in the baseline. Since the MAC frame format of 15.3e is different from the baseline (MAC subheader, padding, etc.), it is better to split the sentence into two parts, one for the legacy and the other for 15.3e. | Split the sentence into two parts: (1)pMaxFrameBodySize for the legacy (The sentence in the baseline should be used.) (2) pMaxFrameBodySize for 15.3e (The sentence in the current spec should be used.) | Revised  See the proposed change in 15-16-0804r0. |

**Proposed Text (based on 802.15.3e D06 and 802.15.3-2016)**

***Change the first paragraph of 6.2 in 15.3e D06 as follows:***

**6.2 General frame format**

The MAC frame format, illustrated in Figure 6-3 for piconet DEVs and in Figure 6-3a for PRDEVs, comprises a set of fields that occur in a fixed order in all frames. The figures in this subclause are a representation of the MAC Header field and MAC Frame Body field. The HCS is not shown since this is calculated and verified by the PHY. The MAC frame shall be formatted as illustrated in Figure 6-3 for piconet DEVs and in Figure 6-3a for PRDEVs. For piconet DEVs, the maximum size of the MAC Frame Body field, *pMaxFrameBodySize*, is a PHY-dependent parameter that includes the frame payload and FCS fields, but not the PHY preamble, PHY header, MAC header, MAC subheader, or MAC header validation. For PRDEVs, the maximum size of the MAC Frame Body field, *pMaxFrameBodySize,* is a PHY-dependent parameter that includes the frame payload(s), MAC subheader(s) and padding octets in the aggregated frames, and FCS field(s) but not the PHY preamble, PHY header, MAC header, or MAC header validation. The parameter *pMaxFrameBodySize* is defined in the following subclauses:

CID r02-5 & r02-10

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| r02-5 | 64 | 6.5 | 40 | Description on the secure membership is missed in the sentence. | Add description on secure membership for 15.3e and update the Table 6-22a to include the secure membership.. | Revised  See the proposed change in 15-16-0804r0. |
| r02-10 | 88 | 8.2.2 | 26 | Table 6-22a should be updated to include the secure membership and it should be referenced from this subclause | Update Table 6-22a to include the secure membership and make it referenced in this sub-clause. | Revised  See the proposed change in 15-16-0804r0 |

**Proposed Text (based on 802.15.3e D06)**

***Change Table 6-22a in 15.3e D06 as follows:***

**Table 6-22a—Command types for pairnet**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Command type**  **hex value**  **b15–b0** | **Command name** | **Subclause** | **Associated** | **Secure**  **membership**  **(if required)** |
| 0x0000 | Association Request command | 6.5.1.1 | - |  |
| 0x0001 | Association Response command | 6.5.1.2 | X |  |
| 0x0002 | Disassociation Request command | 6.5.1.3 | X |  |
| 0x0003 | Request Key command | 6.5.2.1 | X | X |
| 0x0004 | Request Key Response command | 6.5.2.2 | X | X |
| 0x0005 | Distribute Key Request command | 6.5.2.3 | X | X |
| 0x0006 | Distribute Key Response  command | 6.5.2.4 | X | X |
| 0x0007-0x000B | Reserved | - | - |  |
| 0x000C | Security Information Request  command | 6.5.4.3 | X | X |
| 0x000D | Security Information command | 6.5.4.4 | X | X |
| 0x000E | Probe Request command | 6.5.4.5 | X |  |
| 0x000F | Probe Response command | 6.5.4.6 | X |  |
| 0x0010–0x0017 | Reserved | - | - |  |
| 0x0018 | Transmit Power Change command | 6.5.7.5 | X |  |
| 0x0019 | Array Training command | 6.5.9.5 | X |  |
| 0x001A | Array Training feedback | 6.5.9.6 | X |  |
| 0x001B–0x001D | Reserved | - | - |  |
| 0x001E | Security Message command | 6.5.9.1 | X |  |
| 0x001F–0x00FF | Reserved | - | - |  |
| 0x0100–0xFFFF | Vendor Defined | 6.5.9.2 | X |  |

***Change the first paragraph of 6.5 in 15.3e D06 as follows:***

**6.5 MAC commands**

The MAC commands are listed in Table 6-22 and Table 6-22a. If the column labeled “Associated” in Table 6-22 or Table 6-22a is marked with an “X,” then that MAC command shall only be sent by a DEV that is associated in the piconet or the pairnet. If the column labeled “Secure membership (if required)” in Table 6-22 or Table 6-22a is marked with an “X” and secure membership is required for the piconet or the pairnet, then that command shall only be sent by a DEV that has established secure membership with the PNC in the piconet or with the PRC in the pairnet. Because a neighbor PNC is not a member of the piconet, it sends only non-secure MAC commands. The PNC or PRC or destination DEV shall ignore any MAC command from a DEV that is not allowed to be sent, as indicated in Table 6-22 and in Table 6-22a. The “Required” column indicates the type of DEVs that are required to support the command.

***Change the second paragraph of 8.2.2 in 15.3e D06 as follows:***

**8.2.2 Security mode 1**

…..

While in mode 1, the cryptographic operations used for secure frames exchanged with the PNC or PRC and with other members of the piconet or pairnet security group shall be performed as specified by the symmetric key security operations. While in this mode, if the MAC receives a frame with the SEC field in the Frame Control field set to a value different than expected, as defined in Table 6-22 for piconet and Table 6-22a for pairnet, the MLME shall generate an MLME-SECURITY-ERROR.indication with the ReasonCode set to INVALID-SEC-VALUE.

CID r02-18, r02-19, r02-20, and r02-21

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| r02-18 | 91 | 8.3.7 | 36 | A reference to the pairnet secure Beacon frame should be added. | Add reference to the pairnet secure Beacon frame. | Revised  See the proposed change in 15-16-0804r0. |
| r02-19 | 91 | 8.3.7 | 46 | To distinguish SFC related security error and the time token related error, it is better to use different name other than BAD-TIME-TOKEN | Add a reason code for SFC related error. | Revised  See the proposed change in 15-16-0804r0 |
| r02-20 | 91 | 8.3.7 | 65 | It is better to return an error indication on SFC verification error. | Specify that the SFC error indication is returned. | Revised  See the proposed change in 15-16-0804r0 |
| r02-21 | 92 | 8.3.7 | 18 | The last paragraph in 8.3.7 in the baseline should be amended for 15.3e. | Amend the last paragraph in the baseline | Revised  See the proposed change in 15-16-0804r0 |

**Proposed Text (based on 802.15.3e D06 and 802.15.3-2016)**

***CID r02-18 & r02-19:***

***Change the third paragraph of 8.3.7 in 15.3e D06 as follows:***

When a DEV receives a secure Beacon frame, as defined in 6.3.1.2 for piconet and 6.3.1.2a for pairnet, 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, a PRDEV shall further check the SFC included in the Beacon frame and the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the ReasonCode set to BAD-SFC and shall not perform any additional operations on the received Beacon frame if the SFC value in the Beacon frame is not strictly greater than the last SFC value received from that DEV corresponding to the key identified by the SECID. The last SFC value received shall be only updated after the received integrity code corresponding to the SFC value of the received frame or subframe is successfully verified. 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 ~~both of~~ 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.

***Modify the last row of Table 5-12 as follows:***

**Table 5-12—MLME-MEMBERSHIP-UPDATE and MLME-SECURITY-ERROR primitive parameters**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
| SECID | 2 octets | As defined in 6.2.7.2 | The identifier for the key. |
| OrigId | Integer | Any valid DEVID, as defined in 6.2.3 for piconet and as defined in 6.2.3a for pairnet, except for the BcstID, the McstID or the UnassocID | Either the PNCID or PRCID, if this key is for the DEV’s PNC or PRC personality, or the DEV’s DEVID. |
| TrgtId | Integer | Any valid DEVID, as defined in 6.2.3 for piconet and as defined in 6.2.3a for pairnet, except for the BcstID, the McstID or the UnassocID | The DEVID of the target DEV for this relationship. |
| MembershipStatus | Enumeration | MEMBER,  NON-MEMBER | Indicates the membership status for the provided SECID. If NON-MEMBER, KeyInfo is zero length. |
| KeyOriginator | Boolean | TRUE, FALSE | Indicates if the DEV is the key originator for this relationship. This is always true when the OrigId is the PNCID or PRCID. |
| KeyInfo | Octet string | Any valid symmetric key for the symmetric key security operations, as defined in 9.3 for piconet and as defined in 9a.3 for pairnet | The key used for protecting frames between this DEV and the TrgtId DEV. |
| SrcID | Integer | Any valid DEVID, as defined in 6.2.3 for piconet and as defined in 6.2.3a for pairnet, except for the BcstID, the McstID or the UnassocID | The DEVID of the DEV that is the source of a security error. |
| Timeout | Integer | 0–65535 | The time in milliseconds allowed for the primitive to complete. |
| ResultCode | Enumeration | SUCCESS, FAILURE | Indicates the result of the MLME request. |
| ReasonCode | Enumeration | NOT\_ASSOCIATED,  TARGET\_UNAVAILABLE,  UNAVAILABLE\_KEY,  FAILED\_SECURITY\_CHECK,  BAD\_TIME\_TOKEN,  INVALID\_SEC\_VALUE,  BAD\_SFC,  OTHER | The reason for a security error. |

***CID r02-20:***

***Change the fourth paragraph of 8.3.7 in 15.3e D06 as follows:***

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. ~~A~~For piconets, 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 pairnets, a DEV shall reject all frames or subframes that do not have a corresponding SFC value that is strictly greater than the last SFC value received from that DEV corresponding to the key identified by the SECID in the received frames, and the MLME shall return an MLME-SECURITY-ERROR.indication to the DME with the ReasonCode set to BAD-SFC and shall not perform any additional operations on the rejected frames or subframes. The last SFC value received shall be only updated after the received integrity code corresponding to the SFC value of the received frame or subframe is successfully verified.

***CID r02-21:***

***Amend the last paragraph of 8.3.7 in 802.15.3-2016 as follows:***

While operating in mode 1, if the MAC receives a command frame with the SEC field in the Frame Control field set to a value different than expected, as defined in Table 6-22 for piconet and Table 6-22a for pairnet, the MLME shall generate an MLME-SECURITY-ERROR.indication with the ReasonCode set to INVALID-SEC-VALUE.