**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 2 | |
| 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 r02-6

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| r02-6 | 69 | 6.5.2.3 | 28 | No-ACK policy can be used for Distributed Key Request command in the baseline, but it may not be useful for 15.3e since the Key is distributed to only one DEV in the pairnet. | Consider to make the 15.3e always use Stk-ACK as the ack policy for Distributed Key Request command | Revised  See the proposed change in 15-16-0809r0. |

Discussion

For the key distribution by the PNC, 15.3 uses Distribute Key Request and Distribute Key Response commands. The PNC should transmit the key to each DEV in the piconet using Distribute Key Request command. Since there may be many DEVs associated with the PNC, it may take some time to distribute the key to all DEVs in the piconet. In that case, using No-ACK policy for Distribute Key Request command may be useful for efficiency, but there is only one DEV in the pairnet and using No-ACK policy is not so beneficial.

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

***Change the first paragraph of 6.5.2.3 as follows:***

**6.5.2.3 Distribute Key Request command**

The Distribute Key Request command is used to transmit a key to another DEV. The SEC field in the Frame Control field shall be set to one. For piconet, this command may have the ACK Policy field set to no-ACK only if the source ID is the PNCID. For pairnet, this command shall have the ACK Policy field set to Stk-ACK. This command shall be protected using the management key that is shared between the requesting DEV and the key originator. The Distribute Key Request command Payload filed shall be formatted as illustrated in Figure 6-131.

CID r02-11 and r02-12

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| r02-11 | 88 | 8.3.2 | 57 | This paragraph specifies that a PRC changes the SECID in the beacon after Key Distribution and the DEV can use the new key after receiving the beacon, but it cannot be applied to pairnet since the beacon is not transmitted during the associated phase and the key change is not possible for pairnet during associated phase. | Modify the key distribution method for pairnet to allow the key change during the associated phase. | Revised  See the proposed change in 15-16-0809r0. |
| r02-12 | 88 | 8.3.2 | 64 | Since the key originator only needs to distribute the key to one DEV in the pairnet, mMaxKeyChangeDuration can be very short. | Change the behavior on mMaxKeyChangeDuration. | Revised  See the proposed change in 15-16-0809r0. |

Discussion

Since there may be many DEVs associated with a PNC, it may take some time to distribute the new key to all DEVs in the piconet. Before the key is distributed to all DEVs, some DEVs may have the new key and some DEVs may not have the new key. Legacy DEVs cannot use the new key distributed by PNC using the Distribute Key Request command immediately and it can start to use the new key after it receives the beacon with the new SECID. That is, new key can be used at the next superframe. Baseline spec allows to use both new and old piconet group data key during mMaxKeyChangeDuration.

Since PRC needs to distribute the key to only one DEV, we can make the new key to be used immediately after the Distribute Key Request/Distribute Key Response command. In that case, we can remove mMaxKeyChangeDuration from pairnet. Since the beacon is not transmitted during associated phase, we have to use non-beacon frames to trigger the use of the new key.

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

***Change the first paragraph of 8.3.2 as follows:***

**8.3.2 Changes in the piconet group data key or pairnet group data key**

When the PNC or PRC changes the piconet group data key or pairnet group data key, the PNC or PRC shall transmit the new key to all of the members of the piconet or pairnet that are in ACTIVE mode using the Distribute Key Request command, as described in 6.5.2.3.

For piconet, ~~O~~once the Distribute Key Request command has been issued for all of the members of the piconet that are in ACTIVE mode, the PNC may change the SECID in the beacon. When a DEV receives a valid Distribute Key Request command, as described in 6.5.2.3, from the PNC, the DEV shall use the new key for all outgoing secure frames that require the use of the piconet group data key once it sees the corresponding SECID in the beacon. The DEV may continue to accept frames protected by the old piconet group data key for up to *mMaxKeyChangeDuration* since the DEV last received a valid beacon protected by the old piconet-wide group data key.

For pairnet, once the Distribute Key Request command has been issued for the member of the pairnet that are in ACTIVE mode, the PRC shall change the SECID in the outgoing secure frames. When a DEV receives a valid Distribute Key Request command, as described in 6.5.2.3, from the PRC, the DEV shall use the new key for all outgoing secure frames that require the use of the pairnet group data key once it sees the corresponding SECID in the received frame.

CID r02-17

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| r02-17 | 91 | 8.3.6 | 11 | mMaxTimeTokenChange is not defined in 15.3e. | Define mMaxTimeTokenChange in clause 7.16 | Revised  See the proposed change in 15-16-0809r0. |

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

***Add the following entry at the end of Table 7-10a:***

**Table 7-10b—MAC sublayer parameters—HRCP SC PHY dependent**

|  |  |
| --- | --- |
| **Parameter** | **Values** |
| ….. | …. |
| *mMaxTimeTokenChange* | 65535 |