**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | Comment resolution on Annex C | |
| Date Submitted | 17, March, 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: | LB114\_Consolidated\_Comments | |
| Abstract | This document proposes comment resolution on Annex C. | |
| 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 |
| Itaru Maekawa | Japan Radio Co., Ltd |
| Lee Doohwan | NTT Corporation |
| Ken Hiraga | NTT Corporation |
| Hideki Toshinaga | NTT Corporation |
| Keitarou Kondou | Sony Corporation |
| Hiroyuki Matsumura | Sony Corporation |
| Makoto Noda | Sony Corporation |
| Masashi Shinagawa | Sony Corporation |
| Ko Togashi | Toshiba Corporation |
| Kiyoshi Toshimitsu | Toshiba Corporation |
|  |  |

CID

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** | **Resolution Status** |
| 106 | 127 | Annex C | 1 | Annex C (Security consideration) has to be cleaned up for HRCP | Update the Annex C of the baseline | Revised |

**Proposed Text (based on 802.15RevA-D01)**

**Annex C**

(informative)

Security considerations

*Change Clause C.1 as shown:*

**C.1 Background assumptions**

All security solutions rely on assumptions about DEVs and the capabilities of potential attackers to thwart possible threats. The goals of mode 1 security are that only authorized DEVs will be able to join a secure piconet or a secure P2Plink and that communication is restricted to authorized DEVs.

*Change Clause C.1.1 as shown:*

**C.1.1 Physical assumptions**

The assumptions below are made about the physical environment for the piconet or P2Plink. The physical constraints help to determine the security architecture.

* **Open communications medium:** Since the data being transmitted will be able to be received by any other entity that is sufficiently close and has a sufficiently good receiver, it is assumed that transmissions are be heard by entities that are not part of the piconet or P2Plink.
* **Low cost:** Like all other components of a DEV, security is provided with careful attention to cost.
* **Dynamic group membership:** DEVs are expected to be mobile and it is therefore assumed that the DEVs enter or exit the network at any time.
* **No access to external networks:** Security solutions need to be effective without access to external networks
* **Bandwidth:** Since 802.15.3 piconets or P2Plinks provide high data rates, reasonable amounts of bandwidth overhead due to security are acceptable.
* **Computational power:** The DEVs are assumed to have very little computational power with only a small portion of that available for cryptographic computations.
* **Memory:** It is assumed that the low end DEVs implementing 802.15.3 will have little memory available for security.

*Change Clause C.1.2 as shown:*

**C.1.2 Network assumptions**

The assumptions below are made about the network structure of the piconet or P2Plink. The network constraints help to determine the security architecture.

* **Network size:** Although there is a fixed upper bound of fewer than 255 DEVs in a piconet, the security solution might need to scale to arbitrary sets of DEVs, rather than to a fixed set of limited size. DEVs join and leave the network in an ad-hoc fashion and in some cases will not have previously communicated with the other DEV(s).
* **Controller:** One DEV, the PNC or PPC, has the role of managing message control and entry into the piconet or P2Plink.
* **Dynamic controller:** The PNC is assumed to have the ability to leave the network or hand over the PNC role to other DEVs.
* **Device relationships:** The wide array of use cases describe multiple models for the pre-existing relationship of DEVs in the piconet or P2Plink. It is assumed that DEVs could have pre-existing security relationships or that they have never met and that both types of relationship could exist within a single piconet or P2Plink.

*Change Clause C.1.3 as shown:*

**C.1.3 Attack model assumptions**

In order to make statements about the effectiveness of security measures, it is necessary to describe the capabilities of the attackers and the nature of the attackers.

* **Computational capabilities:** It is assumed that the attacker has state of the art technologies to perform rapid computations.
* **Listening capabilities:** It is assumed that the attacker is within listening range of the DEVs in the piconet or P2Plink and understands the communication mechanism.
* **Broadcast capabilities:** It is assumed that the attacker has sophisticated broadcasting equipment that is able to synchronize with the piconet or P2Plink and transmit data for the DEVs in the piconet or P2Plink at the appropriate time.
* **Security setup:** The security setup for the DEVs occurs either before entry into the piconet or P2Plink or after the piconet or P2Plink has been established. No assumptions are made about the presence of attackers during security setup.

**C.1.4 Security key lifecycle issues**

*Change Clause C.1.4.2 as shown:*

**C.1.4.2 Membership lifecycle**

The PNC or another DEV is able to require that each DEV with which it has a secure relationship periodically transmit a secure frame using the management key to be certain that the DEV is still in the piconet. If no secure frames are being transmitted by the target DEV, the PNC or PPC or requesting DEV is able send a secure Probe Request command requesting an IE from the target DEV. If the target DEV does not respond with a secure frame within a period of time determined by the PNC or PPC or requesting DEV, the PNC or PPC or requesting DEV will assume that the target DEV is no longer present and disassociate or terminate the secure relationship with the target DEV.

*Change Clause C.1.4.3 as shown:*

**C.1.4.3 Group membership change rekey**

Only DEVs that are currently members of the piconet or P2Plink are allowed to generate, read or modify piconet or P2Plink data. This implies that when a DEV joins or leaves the piconet or P2Plink, the currently active group keys need to be changed. Changes in the group membership key are described in 8.3.2.

**C.2 Claimed security services**

*Change Clause C.2.1 as shown:*

**C.2.1 Beacon protection protocol**

**Table C-1—Beacon protection security services**

|  |  |
| --- | --- |
| **Security service** | **Method provided** |
| Communication of current time token to the DEVs in the piconet or P2Plink. | The PNC or PPC increments the time token for each superframe and protects it using the current group key. The integrity protection on the beacon and the storage of the previous time token allows each DEV to determine that the time token is fresh. |
| Indication of the identity of the PNC or PPC to the DEVs in the piconet or P2Plink. | If PNC handover has not occurred, the DEV address of the current PNC appears in the beacon. If PNC handover has occurred, the DEV address of the new PNC appears in the beacon. The DEV address of the current PPC appears in the beacon. The integrity protection on the beacon and the freshness from the time token allow each DEV to determine the identity of the current PNC or PPC. |

**C.3 Properties of the 802.15.3 security suite**

**C.3.1 Key usage**

*Add the following sentences at the end of C.3.1*

The security operation for HRCP is based on the GCM mode of the AES encryption algorithm with 128 bit key length, 128 bit integrity code, and 96 bit nonce. To avoid a birthday attack, the number of invocation of the authenticated encryption function using a given key should be limitied to 248. In the worst case scenario, secure frames consist of only one AES block per frame may be transmitted at 100 Gbps throughput. In this case, total number of octets that can be encrypted using a single key is 248 \* 24 octets = 252 octets. Then, maximum duration using the single key at 100 Gbps throughput is 252 \* 8 bit / 1011 = 4.17 days. Since a management key is used only for command frames and command frames are not frequently transmitted, the actual lifetime of a management key is much longer than this duration.

*Change Clause C.3.2 as follows:*

**C.3.2 Replay prevention**

This standard uses a Time Token, 6.3.1.1, and Secure Frame Counter (SFC), 6.2.7.3, to provide a method to detect and defeat potential replay attacks. For non-HRCP, t~~T~~he SFC allows up to 65535 frames to be sent in a single superframe or one every microsecond for the largest possible superframe. The Time Token is 6 octets, and so it will repeat only once every 248/235 = 213 years ~ 8192 years if the PNC uses a 1 ms superframe duration.

For HRCP, the 6 octet SFC allows up to 248  frames to be sent in multiple superframes. In the worst case scenario described in C.3.1, the duration for transmitting 248  frames using 6 octet SFC is 4.17 days. 6 octet time token is used in HRCP. In the worst case scenario where a PPC keeps transmitting beacons and no DEV is associated, the time token will roll over every 254 years if we assume 28.5 μs beacon interval.

For non-HRCP, b~~BB~~ecause the nonce includes the Time Token, a replay of one of Distribute Key Request, Distribute Key Response, Request Key or Request Key Response commands would fail for anything other than the current superframe. A replay of one of these commands would not fail integrity code check if either

* The piconet restarts with a lower time token and so eventually the same time token will be used; or

— The time token rolls over in the current piconet (once every 8192 years for a 1 ms superframe duration) and the same SECID is being used by that DEV (which may be true for the management key in shared key operation).

For non-HRCP, i~~I~~n the case where the command is replayed in the same superframe, the duplicate detection algorithm will discard the second occurrence sent by the attacker.

For HRCP, a replay of one of Distribute Key Request, Distribute Key Response, Request Key or Request Key Response commands would fail since the 6 octet SFC is included in the secure frames and it can be used for replay detection. A replay of one of these commands would not fail integrity code check if the SFC rolls over and the same SECID is being used by that DEV.

For non-HRCP, i~~I~~n the case of a piconet starting with a lower time token, the duplicate detection will fail and the integrity code will pass in the case of shared keys if the same management key and SECID are used. If higher layer mutual authentication is used, then the management keys and their SECIDs will change each time the piconet is restarted and the DEVs reauthenticate.