**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | **Proposed Comment Resolutions for the comments related to security** | |
| Date Submitted | 16 July 2015 | |
| Source | [Noriyuki Sato, Kiyoshi Fukui]  [OKI Electric Industry Co., Ltd.]  [2-5-7, Hommachi, Chuo-ku, Osaka, 541-0073 Japan] | Voice: [+81-6-6260-0700]  Fax: [+81-6-6260-0700]  E-mail: [sato652@oki.com] |
| Re: | Proposed comment resolutions related to the 802.15.10 Consolidated Comment Entry Form, CID #118, #163, #165, #293, #297, #298, #302, #306, #307, #309, #336, #366, #367, #500, #514, R63, R131, R139, R140, R141 and R165 | |
| Abstract | This document provides a proposed comment resolutions for the comments which are related to the security section of D1 of 802.15.10 | |
| Purpose | To propose | |
| 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. | |

1. **CID#163**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 163 | Tero Kivinen | INSIDE Secure | 22 | 5.2.1 | 8 | The numbers in the description do not match. The range is 0x00-0x02 in HEX, and then there is vlaue 10 (in decimal as no 0x or 0b prefix) for KMP. | Change to refer Table 8 both in range and description. |

**Resolution: Accept**

Replace ‘00: none, 01 : PAN credentials, 10 : KMP, 11 : Reserved.’ with ‘As defined in table 8’

1. **CID #165, #293, #297, #298**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 165 | Don Sturek | SSN | 22 | 5.2.1 | 9 | What does a "security mode" of KMP mean? A KMP is a security establishment protocol that probably starts out with no security. | KMP is not a security mode |
| 293 | Don Sturek | SSN | 46 | 5.5.1.3 | 23 | 802.15.9 defines the MP-IE but it does NOT interface to the L2R Layer. I don't see why MP as it is scoped in 802.15.9 needs to interface to a layer 2 routing layer at all. 802.15.9 defines a one hop delivery of fragmented or unfragmented packets accompanied by a protocol dispatch which could be a KMP. The MP-IE uses the MCSP-DATA primitive. Surely we don't plan to propagate a non-one hop destination through MP-IE or MCPD-DATA. I would expect a standalone L2R-D-IE to carry the multihop delivery information. The MP-IE would then be set with the protocol dispatch of L2R (to be assigned) until the final hop to the actual destination where L2R would put back the original protocol dispatch. Anything other than this begs the question as to how MP-IE handles multihop acknowledgements, etc. | Re-evalute having L2R use MP-IE as a multhop protocol dispatch/fragmentation-reassembly mechanism. |
| 297 | Tero Kivinen | INSIDE Secure | 47 | 5.5.1.3 | 41 | What happens if the L2R Routing IE cannot be appended to the frame, as it gets too big? Is the intermediate device allowed to reassemble the fragments and fragment them again to smaller pieces. Or is it expected that joining device knows that it needs to leave enough space for the L2R Routing IE and KMP IE added by the relaying router? |  |
| 298 | Tero Kivinen | INSIDE Secure | 47 | 5.5.1.3 | 50 | Note, that KMP might be sending back multiple frames. i.e. it completely valid for joining node to send one KMP frame to the PAN coordinator, and PAN coordinator replaying with two KMP frames, and so on. i.e. the KMP protocols do not need to be strict request and reply protocols. | Explain how this is working, i.e. what happens if the PAN coordinator replies with multiple KMP frames (or zero KMP frames, which is also possible). |
| 331 | Brian Weis | Cisco Systems | 54 | 6.2.1.2 | 9 | What are "PAN Credentials"? These are not defined in this document, nor in 802.15.4. | Add a defintion and/or discussion defining what is meant by PAN credentials. |

**Resolution: AiP**

Almost for the CID#165, #331

* Replace ‘Security Mode’ to the ‘Key Exchange Method’ and redefine descriptions in the Table 1 as follows.
  + 0x00: None, 0x01: Pre-shared or Out-of-band, 0x02: With KMP, 0x03: Reserved
* Replace ‘Security Mode’ to the ‘Key Exchange Mode’
* Update the table 8 in section 6.2.1.1 not to use undefined word ‘PAN credential’. Just to use ‘pre-configured and out-of-band’

To address CID#118, following description should be added into the 5.5.1.3.

L2R Bootstrapping is divided into 3 phases of step. First is the scanning to scan appropriate network to join in. Second is the association to let a node join to the network. The last is sharing routing information. If the KMP bootstrapping is used, key exchanging is considered to be done in second phase. Securing L2R-D IE used in the scanning process may be applied when ‘Pre-shared or out-of-band’ mode or ‘With KMP’ mode is used. However, how to exchange key for securing L2R-D IE prior to second phase is out-of-scope of this document.

Not having multi-hop delivery of the credential in the IEEE802.15.10 to address CID #293, #297 and #298 – update 5.5.1.3 to make it out of the scope

* Remove extended IEEE802.15.9 architecture with L2R
* Remove ‘and extended within this docoument…’on l.7, p.57.
* Remove all description regarding key exchange and put a description to explain when KMP is used in L2R starting process and provide a guidance to show examples – how the joiner’s parent verify the credential from the joiner, how the joiner’s parent pass the credential to the PAN Coordinator to make it verify the credential or how the joiner forward KMP frames to the PAN Coordinator

1. **CID #302, #307, #309**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 302 | Noriyuki Sato | OKI | 49 | 5.5.1.3 | 1 | Section should be updated by describing how the device manage secured frame during forwarding per keyID mode. | Describe how to process per keyID mode. |
| 307 | Tero Kivinen | INSIDE Secure | 49 | 5.5.1.3 | 50 | The enhanced beacons can also be unencrypted, but authenticated. i.e. joiner can see the IEs and join based on them, members of the network can also authenticate the information in IEs (for example the NLM information etc). | Add text describing that. |
| 309 | Noriyuki Sato | OKI | 50 | 5.5.1.3 | 1 | Section should be updated by describing how the device manage secured frame during forwarding per keyID mode. | Describe how to process per keyID mode. |

**Resolution: AiP**

Having a section to describe how the L2R layer manages key parameters – KeyIDMode, KeySourceID, KeyIndex, Security Level,

Having subsection which describes sending frame including:

* Data frame sent by L2R-Data.request
* Periodically broadcast - TC IE and NLM IE
* Periodically unicast – RA IE
* Address assignment related – AA-RQ IE, AA-RP IE,
* E2E ACK IE

Having a subsection to describe for forwarding frame:

* Frame with L2R Routing IE

Add new PIB related to the security parameter used in primitives which is invoked by L2R layer to send secured frame:

* Security Level
* KeyIDMode
* KeySource
* KeyIndex

Those PIBs shall be prepared for each IE – TC IE, RA IE, NLM IE, AA-RQ/RP IE (e.g. l2rTCSecurityLevel, l2rTCKeyIDMode..)

Common setting is useful to avoid complex setting. Having PIBs as follows:

* l2rSecurityCommonSettingIsUsed Boolean If true, Individual setting for each IE is not used
* l2rSecurityCommonSettingSecurityLevel Integer
* l2rSecurityCommonSettingKeyIDMode Integer
* l2rSecurityCommonSettingKeySource Set of octets
* l2rSecurityCommonSettingKeyIndex Integer

Note: Common setting is not used for securing L2R-D IE.

Key Parameters PIBs per neighbor is required for forwarding process:

* l2rListOfKeyPerNeighbor (List of KeyPerNeighbor)
  + KeyPerNeighbor
    - Neighbor address
    - KeyIDMode
    - KeySource not used when the KeyIDMode is 0x00 or 0x01
    - KeyIndex not used when the KeyIDMode is 0x00 or 0x01. CommonKeyIndex is used instead.
* CommonKeyIndex only used when the KeyIDMode is 0x01

When a device is going to send a frame due to L2R-Data.reuqest invoked by higher layer, necessary parameters for securing frame are given by the primitive. When a device is going to send a frame to forward a received frame which final destination is not the device, same KeyIDMode and KeySource as received frame are used to send a frame to the next hop. When a device is going to send a frame due to a process in L2R layer (e.g. periodical TC IE broadcasting, sending frames related address assignment), related PIBs are used to set security parameters in MCPS-Data.request primitive.

1. **CID #306**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 306 | Don Sturek | SSN | 49 | 5.5.1.4 | 50 | Why is a draft addressing Layer 2 Routing defining pairwise security? This seems wildly out of scope. | Remove the section on pair-wise security and point to a draft where key management protocols are in scope (eg, why not use IEEE 802.15.9? And if that does not have the key management protocol you want to use, add it in a new Annex) |

**Resolution: Accept**

Remove the section 5.5.1.4. Intention was not to provide new key exchanging mechanism here. How to manage KMP is out of scope of this document

1. **CID #336, #366, #367, #500**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 336 | Tero Kivinen | INSIDE Secure | 54 | 6.2.1.5 | 36 | What is the meaning of the security level here? What does it tell to the recipient of the IE? Is this the expected security level of the frames or what? | Clarify why security level is here. |
| 366 | Tero Kivinen | INSIDE Secure | 57 | 6.2.2.9 | 47 | Security level is 3-bit field, and here it is stored in the one octet field. Either you need to define a format for this, or even better move this to be part of the Descriptor field and put it in bits 5-7 or 10-12 in it (depending whether it is needed for short format too or not)? |  |
| 367 | Tero Kivinen | INSIDE Secure | 57 | 6.2.2.9 | 47 | What is the meaning of the security level here? What does it tell to the recipient of the IE? Is this the expected security level of the frames or what? | Clarify why security level is here. |
| 500 | Tero Kivinen | INSIDE Secure | 77 | 7.1.1.2 | 13 | SecurityMode is described here to be boolean? What does that mean. It is not matching Security Levels in 802.15.4, nor does it match the security modes in table 8. | I assume this is supposed to mean security modes as in table 8. |

**Resolution: AiP**

Remove security level field from the L2R-D IE and TC IE.

1. **CID #514**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 514 | Tero Kivinen | INSIDE Secure | 78 | 7.1.1.2 | 20 | Security level on its own is not useful. You also need to have other security parameters, i.e. the KeyIdMode, KeyIndex and KeySource. | Add other security related parameters. |

**Resolution: Reject**

PANIDDescriptor in ScanResultList includes security parameters indicated by this comment.

1. **CID R63**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| R63 | Charlie Perkins | Futurewei | 17 | 5.1.2.2 | 33 | "unless the encryption key ... known to all the devices" | How can the devices tell? Is a bit needed in the beacon? |

**Resolution: Reject**

Auxiliary Security header defined in 15.4 provides what key ID is used. No need to provide by L2R.

1. **CID R131**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| R131 | Charlie Perkins | Futurewei | 45 | 5.5.1.3 | 24 | Last section said key exchange was out of scope | Reword to indicate whether KMP is normative |

**Resolution: AiP**

If the bootstrap mode with KMP is used, KMP is normative. Intention was make how to use KMP out of scope since it is up to higher layer implementation. The indicated sentence is going to be removed to address other comments. However, need to clearly

1. **CID R139**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| R139 | Charlie Perkins | Futurewei | 47 | 5.5.1.3 | 48 | "out of the scope of this document" | Either a citation is required, or it SHOULD be in scope |

**Resolution: Reject**

Basically if the PAN ID connectivity flag is 1 in the TC IE, the tree root is considered to be connected PAN ID since they are implemented in the same device or since they are communicated by out-of-scope method.

1. **CID R140, R141**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| R140 | Charlie Perkins | Futurewei | 48 | 5.5.1.3 |  | The figure is way too big. Should be decomposed. | Idea: one figure at functional module granularity, and other figures showing signaling with each functional module |
| R141 | Charlie Perkins | Futurewei | 48 | 5.5.1.3 | 39 | Text in procedure block is too long | Break down into multiple procedure blocks |

**Resolution: AiP**

Comments are accepted but the figure indicated by them will be removed to address other comments.

1. **CID R165**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| R165 | Charlie Perkins | Futurewei | 53 | 6.2.1.1 | 47 | "Security Level field is present in the TC IE." | Why not put the field here? |

**Resolution: AiP**

Security Level in TC IE is not used any more to address other comments.