IEEE P802.15

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | SC Maintenance |
| Title | **Resolutions to clause 23.3.x technical CIDs** |
| Date Submitted | April 2, 2015 |
| Source | [Jussi Haapola][Centre for Wireless Communications / University of Oulu] | Voice: +358 40 8363 018E-mail: jhaapola@ee.oulu.fi |
| Re: | LB103 Comment resolution |
| Abstract |  |
| Purpose | Comment resolution |
| 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. |

**CID 2147**

Tero Kivinen INSIDE Secure

Page 518 Clause 23.3.1 Line 53

Comment:

The text about macFrameCounter etc is wrong, and is already described in the 9.3.2.3.

Proposed change:

Remove “9.2.1, except that macFrameCounter is replaced with phyFragmentFrameCounter. The phyFragmentFrameCounter shall be comprised of the PSDU counter field, used as the most significant 26 bits, and the fragment number, used as the least significant 6 bits.

Type T

Must be satisfied Yes

Resolution AiP Deferred to Sponsor Ballot

**CID 2148**

Tero Kivinen INSIDE Secure

Page 519 Clause 23.3.2 Line 17

Comment:

Add new step 2b that will fetch the PSDU Counter value from the PIB if secured frame, and increment it afterwards.

Proposed change:

"Add new step:

2b) If Secure Fragment is set to one, set the PSDU Counter value to the phyFragmentFrameCounter. If the PSDU Counter has value of 0x3ff ffff then return error, otherwise increment the phyFragmentFrameCounter."

Type T

Must be satisfied Yes

Resolution AiP Deferred to Sponsor Ballot

**CID 2151**

Tero Kivinen INSIDE Secure

Page 519 Clause 23.3.2 Line 27

Comment:

This paragraph is confusing. I think the abort is sent from the responder as Frak not as Fragment, and also the text on page 521 line 53 says that abort is indicated by setting all bit positions of the Frak Content to zero, not by setting Fragment Number zero. Of course this could also be the case where the sender aborts the transaction and sends Fragment with Fragment Number of zero out to indicate it aborts the transaction, but how does the receiver know this is not first fragment?

Proposed change:

"Replace

Fragments shall be transmitted beginning with fragment 1 and ending with fragment n. The Frak is described in 23.3.5.2. If the Frak retransmission count is exceeded during the transaction, the transaction is terminated and a fragment with the Fragment Number field set to zero is transmitted to signal that receiving device is terminating the transaction.”

With

Fragments shall be transmitted beginning with fragment 1 and ending with fragment n. The Frak is described in 23.3.5.2. If the Frak retransmission count in the receiver is exceeded during the transaction, the transaction is terminated and a fragmentFrak with the Fragment Number field set to zero and Frak Content set to zero, is transmitted to signal that receiving device is terminating the transaction.”

"

Type T

Must be satisfied Yes

Resolution AiP Deferred to Sponsor Ballot

Proposed resolution:

Rationale: The receiver can terminate transaction and with a Frak frame with Frak Content set to zero. This can be only done with Frak Policy field value 0. The transmitter can terminate transaction by setting Fragment Number field to 0, as the first fragment number is 0b000001.

Suggestion: Replace

"Fragments shall be transmitted beginning with fragment 1 and ending with fragment n. The Frak is described in 23.3.5.2. If the Frak retransmission count is exceeded during the transaction, the transaction is terminated and a fragment with the Fragment Number field set to zero is transmitted to signal that receiving device is terminating the transaction.”

With

**“Fragments shall be transmitted beginning with fragment 1 (0b000001) and ending with fragment n. The Frak is described in 23.3.5.2. If the Fragmentation retransmission count is exceeded during the transaction, the transaction is terminated by the transmitter transmitting a fragment with the Fragment Number field set to zero (0b000000). The receiver can terminate the transaction by setting all Frak Content bit positions to zero.”**

**CID 2158**

Tero Kivinen INSIDE Secure

Page 520 Clause 23.3.3 Line 1

Comment:

Does the Fragment Number start from 0 or from 1. There is text saying using Fragment Number 0 abort the transaction, and there is text saying we send fragment 1 first etc.

Proposed change:

Clarify the fragment number range. This same problem is in the Frak.

Type: T

Must be satisfied: Yes

Resolution: AiP Deferred to Sponsor Ballot

Resolution comment: See recommendation to CID 2151.

**CID 2153**

Tero Kivinen INSIDE Secure

Page 520 Clause 23.3.3 Line 11

Comment:

"Remove “7.2.10, except that the initial remainder value used for CRC calculation shall be as described in

7.4.2.9.” as there is no longer ability to set the remainder values."

Proposed change:

"Remove “7.2.10, except that the initial remainder value used for CRC calculation shall be as described in

7.4.2.9.”"

Type: T

Must be satisfied: Yes

Resolution: AiP Deferred to Sponsor Ballot

Resolution comment to SC maintenance: Why did we remove initial remainder offsetting?

**CID 2154**

Tero Kivinen INSIDE Secure

Page 520 Clause 23.3.3 Line 12

Comment:

Change reference from 23.3.1 to new section 23.3.3b.

Proposed change:

Change reference from 23.3.1 to new section 23.3.3b.

Type: T

Must be satisfied: Yes

Resolution: AiP Deferred to Sponsor Ballot

**CID 2141**

Tero Kivinen INSIDE Secure

Page 520 Clause 23.3.3 Line 14

Comment:

Add section describing how to calculate the FICS when using MIC.

Proposed change:

"Add new section to the 23.3.3b:

23.3.3b Calculating FICS field using MIC

When phyPSDUFragSecure is TRUE, the length of FICS field shall be 4 octets and shall contain the MIC-32 calculated as follows:

The nonce for the CCM transformation is calculated as specified in the 9.3.2.3. The Private Payload field is set to empty, The Open Payload field is set to contain the Fragment Header and Fragment Data. The SecurityLevel is set to 1.

The key is set to be the same key that was used to protect the frame containing the FSCD IE negotiating the exchange. i.e. secure fragments can only be used if security was enabled when setting the transaction up.

The CCM transformation shall then use the Private Payload field, the Open Payload field, the macExtendedAddress, the SecurityLevel, and the key to produce the secured fragment according to the CCM\* transformation process defined in 9.3.4"

Type: T

Must be satisfied: Yes

Resolution: AiP Deferred to Sponsor Ballot

**CID 2155**

Tero Kivinen INSIDE Secure

Page 520 Clause 23.3.5 Line 38

Comment:

The text “Upon completing the transmission of the fragment preceding the expected Frak according to the Frak policy selected, the initiating device shall suspend transmission and wait for the expected Frak.” is confusing. It might be better to write the transmitter operations separately for each frak policy

Proposed change:

"Change “Upon completing the transmission of the fragment preceding the expected Frak according to the Frak policy selected, the initiating device shall suspend transmission and wait for the expected Frak.” with

“When using Frak policy of zero, the transmitter will wait for Frak after each fragment. When using other Frak policies of two the transmitter will wait for Frak only after transmitting the last expected fragment.”"

Type T

Must be satisfied: Yes

Resolution R

Resolution Comment:

There is no confusion.

**CID 2156**

Tero Kivinen INSIDE Secure

Page 520 Clause 23.3.5 Line 41

Comment:

"The text “The number of retransmissions shall be limited by macMaxFrameRetries.” is not clear whether we do macMaxFrameRetries for each fragment separately, or whether we fail the transaction if we get macMaxFrameRetries fragment retraries during the sending of the whole frame."

Proposed change:

Clarify which one is meant.

Type: T

Must be satisfied: Yes

Resolution: AiP Deferred to Sponsor Ballot

Resolution comment:

"As Fragments access the channel as individual frames they should be treated as such and maMaxFrameRetries is per fragment.

Proposed resolution:

Change to: “The number of retransmissions shall be limited by macMaxFrameRetries per fragment.”

**CID 2159**

Tero Kivinen INSIDE Secure

Page 522 Clause 23.3.5 Line 17

Comment:

I assume that if Fragments Received field is omitted, then it is assumed that all bits in there are 0, i.e. the Frak frames get longer all the time we go forward. Other option was to assume that we only indicate those frames which needs to be retransmitted sent, i.e. if we leave out frames 0-15, but include frames 16-31 then it is assumed that everything in 0-15 was already received properly. This needs to be clarified.

Prposed Change:

Type: T

Must be satisfied: Yes

Resolution: AiP Deferred to Sponsor Ballot

Proposed resolution:

Append to line 21: "Once all fragments from a group have been acknowledged, the corresponding group can be omitted from future Frak frames of the same transaction."