**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | IEEE 802.15.4z PHY LRP - CRG |
| Date Submitted | 21-Oct-2019 |
| Source | Boris Danev (3db Access), Peter Sauer (Microchip) |
| Re: | Letter Ballot comment resolution of draft Standard document P802.15.4z-D1 |
| Abstract | This contribution proposes updated text for the baseline draft P802.15.4z-D1 |
| Purpose | Provision of the text to facilitate its incorporation into the draft text of the IEEE 802.15.4z standard currently under development in TG4z. |
| Notice | This document does not represent the agreed views of the IEEE 802.15 Working Group. It represents only the views of the participants listed in the “Source(s)” field above. 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 |  |
| Patent Policy | The contributor is familiar with the IEEE-SA Patent Policy and Procedures:  <http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and  <http://standards.ieee.org/guides/opman/sect6.html#6.3>.  Further information is located at <http://standards.ieee.org/board/pat/pat-material.html> and  <http://standards.ieee.org/board/pat>. |

***Comments (in complement to Excel file’s “Resolution Detail”)***

**r2-0377: Accept and revise according to the proposed change in the excel:**

***Resolution: Add a new subsection 6.9.8.2.1 to avoid changing the numbering of the remaining sections***

**6.9.8.2.1 Security levels in case of tolerance of bit errors**

Resolution 1: Move text from lines 9-11 and next page 66 lines 1-13 in this new subsection.

Resolution 2: Add the following paragraph at before the paragraph starting with “For larger challenges and responses …”

“The MCPS-RANGING-VERIFIER.request and MCPS-RANGING-PROVER.request primitives contain the parameters *ChallengeLength* and *ResponseLength* to set the length of octets to be generated and transmitted by the MAC sublayer. For this transmission of challenge and response data, the security services according to Clause 9 are not used, i.e., security level is 0.”

**r2-0379: Accept and revise accordingly:**

***Resolution: Add the following text after the sentence on page 66 line 22:***

“The security level given in the MCPS-RANGING-VERIFIER.request or MCPS-RANGING-PROVER.request sets the lower bound for the security level to be performed by the device security services. The use of ACRRC IE can only raise the security level at the receiving device for its next transmission, but not lower it.”

**r2-0384, r2-0383: Reject and revise accordingly:**

***Resolution: Do the following changes***

**Reason:** I prefer keeping VChallenge to show that the Challenge is generated and transmitted by the Verifier. I agree that in 6.9.8.4.1 this is not needed and can be replaced as suggested, but it will make the other sections inconsistent where also the Prover generates a challenge (PChallenge) as part of its Response data.

But this comment made me fix some other issues I spotted related to this as follows:

**In Clause 6.9.8.4.1:**

1. Replace line 18-19 with:

“Upon reception of the Ranging Prover command, the Verifier MAC indicates the transmitted challenge and the received response to the next higher layer and confirms the status.”

**In Clause 6.9.8.4.2:**

Line 6: add a sentence after “a fresh PChallenge” as follows:

“The PChallenge is an unguessable cryptographically generated random sequence of octets corresponding to the length set by the ResponseLength parameter in the MCPS-RANGING-PROVER.request primitive.”

Line 6: Modify text as follows:

“….the prover MAC transmits a Ranging Prover command containing the PChallenge inside the Response field.”

**r2-0386: Accept**

**Resolution: Accept change text in the proposed resolution**

**r2-0380, r2-0381: Accept**

**Resolution: Accept change text in the proposed resolution**

**r2-0382: Accept**

**Resolution: Accept change text provided in r2-0379**

**r2-0389: Accept**

**Resolution: Accept change text provided in r2-0389**

**r2-0390: Accept, but revise as follows:**

**Resolution: Modify as follows:**

“…, the prover MAC transmits a Ranging Prover command containing the PChallenge inside its Response field without using the MAC level security, i.e., security level 0.”

**r2-0387: Accept**

**Resolution provided in r2-0387**

**r2-0391: Accept**

**Resolution provided in r2-0391**

**r2-0393: Revise**

**Resolution 1: Add additional text as follows in 7.5.27 and 7.5.28 to explain in detail:**

In 7.5.27:

Replace text on line 16-18 with new text:

“The Challenge field contains challenge data of length defined by the SecurityLevel parameter of the MCPS-RANGING-VERIFIER.request primitive, as per Table 8.

In the case of ranging modes with tolerance of bit errors as described in 6.9.8.4.2 and 6.9.8.4.5, the Challenge field contains challenge data of length specified in the ChallengeLength parameter in the MCPS-RANGING-PROVER.request primitive. Example of challenge lengths is provided in Table 9.

The challenge data is a fresh unguessable cryptographic random sequence of octets. The generation is typically achieved by a well-established and industry accepted cryptographically secure pseudo-random number generator (CSPRNG).”

In 7.5.28:

Replace all text on line 6-8 with:

“The Response field contains response data. The response data is created by the MAC sublayer according to the authenticated challenge-response ranging modes described in 6.9.8.4. Each of the modes define the content of the Response field according to ranging mode and security level.”

“In the case of ranging modes with tolerance of bit errors as described in 6.9.8.4.2 and 6.9.8.4.5, the response data in the Response field is a fresh unguessable cryptographic random sequence of octets with number of octets set by the ResponseLength parameter in the MCPS-RANGING-PROVER.request primitive. Examples of response length (same as challenge length) is provided in Table 9. The generation is typically achieved by a well-established and industry accepted cryptographically secure pseudo-random number generator (CSPRNG).”

**Resolution 2: Modify accordingly section 6.9.8.4.2 and 6.9.8.4.5**

In 6.9.8.4.2 change on page 68, line 11 by:

“desired security level” with “desired response length”.

In 6.9.8.4.2 replace text on page 69, line 1-4 by :

“The Verifier next higher layer initiates the ranging exchange by invoking the MCPS-RANGING-VERIFIER.request with the desired challenge length, distance commitment level, and the RawMode set to TRUE. The Verifier MAC generates a fresh VChallenge and transmits a Ranging Prover command containing this VChallenge inside its Challenge field.”

In 6.9.8.4.5 change on page 73, line 5:

“desired security level” with “desired response length”

In 6.9.8.4.5 change on page 74, line 2:

“desired security level” with “desired challenge length”

**r2-0401, r2-0406: Revise**

**Resolution: Remove parameter DistanceCommitmentLevel from VERIFIER.indication and PROVER.indication**

**Reason:** There is no need to indicate this as it is set by the request primitives.

**r2-0402: Accept and revise**

**Resolution: Add description in 8.3.7**

p.132 line 1 – add:

The MCPS- RANGING-VERIFIER.indication primitive is generated by the MAC sublayer at the verifier device and issued to the next higher layer upon receipt of a Ranging Prover command. The primitive provides the received Response from the prover device and the transmitted Challenge from the verifier device to the next higher layer together with the RX RangingCounter value and the RangingStatus as listed in Table 35.

**r2-0404: Accept and revise**

**Resolution: Add description in 8.3.8**

p.133 line 2 – add:

The MCPS-RANGING-VERIFIER.confirm primitive is generated by the MAC sublayer at the verifier device and issued to the next higher layer after the ranging operation has finished either by receiving a Ranging Prover command and issuing a MCPS- RANGING-VERIFIER.indication primitive or when a timeout has occurred as shown in Figure 38 and Figure 39.

**r2-0408: Accept and revise**

**Resolution: 8.3.10 and 8.3.7 add new RangingSecurityLevel which might be different than Security Level, in case the ACRRC IE is used.**

|  |  |  |  |
| --- | --- | --- | --- |
| RangingSecurityLevel | Integer | As defined in Table 8-77 | Provides the security level used by the MAC security services during the ranging exchange when ACRRC IE is used. |

**r2-0409: Accept and revise**

**Resolution: Add description in 8.3.10**

p.137 line 1 – add:

The MCPS- RANGING-PROVER.indication primitive is generated by the MAC sublayer at the prover device and issued to the next higher layer upon receipt of a Ranging Verifier command. The primitive will provide the received Challenge from the verifier device and the generated Response from the prover device to the next higher layer as listed in Table 38.

**r2-0410: Accept and revise**

**Resolution: Add description in 8.3.11**

p.137 line 11 – add:

The MCPS-RANGING-PROVER.confirm primitive is generated by the MAC sublayer at the prover device and issued to the next higher layer after the ranging operation has finished either by issuing a MCPS- RANGING-VERIFIER.indication primitive and expiration of the fixed reply time timer or when a timeout has occurred as shown in Figure 38.

**r2-0388: Accept and revise**

**Resolution: Add a new ChallengeResponseTransfer IE as 7.4.4.52**

**7.4.4.52 ChallengeResponseTransfer IE**

The ChallengeResponseTransfer IE Content field shall be formatted as shown in Figure 7-7X. The IE allows to transfer the challenge and response data between devices for the ranging modes defined in 6.9.8.4.2 and 6.9.8.4.5.

|  |  |  |
| --- | --- | --- |
| Octets: 1 | 0/4/8/16/32/64/128 | 0/4/8/16/32/64/128 |
| Length | Challenge | Response |

Figure 7-7X

The Length field contains the number of octets of the data in the Challenge and Response fields

The Challenge field contains the challenge data

The Response field contains the response data

**Resolution step 2:**

Include in the table of the IEs and mark the columns UL, UL

**Resolution step 3:**

Page 68, Figure 41 last message sequence:

1. Update Figure 41 MCPS-DATA.request and MCPS-DATA.indication to use the ChallengeResponseTransfer IE
2. Replace “Challenge, Response (with Security Level)” by “ChallengeResponseTransfer IE (with Security Level)”
3. Replace “Challenge, Response” with “ChallengeResponseTransfer IE”

Page 73, Figure 44: last two messages. Do the same as for Figure 44.