**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 | 17-Oct-2019 |
| Source | Boris Danev (3db Access) |
| 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>. |

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

**r2-0270:**

***Resolution: It is used only in line 19. Change as below:***

Page 63 line 19: Replace “nodes” with “devices”

**r2-0171:**

***Resolution 1: Indeed this is to be handled by the higher level. Apply following changes:***

**Page 66, line 7-10**

“For larger challenges and responses, the formula ~~shall~~ should be used by the higher layer to compute the number of maximum allowed bit errors in order to verify the desired security level of the received challenge and/or response. ~~The MCPS-RANGING-VERIFIER.request and MCPS-RANGING-PROVER.request primitives ea include a NumMaxAllowedBitErrors parameter for the next higher layer to set this number.~~

Page 128, line 13: Remove NumMaxAllowedBitErrors and replace see Resolution 2

Page 129, Table 34: Remove line NumMaxAllowedBitErrors and replace see Resolution 2

Page 133, line 11: Remove line NumMaxAllowedBitErrors and replace see Resolution 2

Page 134, Table 37: Remove line NumMaxAllowedBitErrors and replace see Resolution 2

***Resolution 2: The MCPS-RANGING-VERIFIER.request and MCPS-RANGING-PROVER.request need to include the Challenge and Response length in bytes to be used by the MAC layer to generate the appropriate challenge/response length***

**In 8.3.6 MCPS-RANGING-VERIFIER.request** replace with ChallengeLength

MCPS-RANGING-VERIFIER.request (

TimeOut,

AuthenticatedChallengeResponseRangingMode,

RawMode,

ChallengeLength,

…

SeqNumSupressed

)

|  |  |  |  |
| --- | --- | --- | --- |
| ChallengeLength | Set of octets | As defined in clause 7.5.27 | Specifies the length in octets of the challenge to be used by the MAC sublayer when RawMode is set to TRUE |

Page 130, lines 2-6:

Upon receipt of the MCPS-RANGING-VERIFIER.request primitive, the MAC sublayer is enabled with a set of selected parameters including a timeout, the authenticated challenge-response ranging mode, enabling or disabling the FCS checking (RawMode), setting the challenge length (for RawMode), ~~the number of maximum allowed bit errors~~, distance commitment level and the other parameters as defined in Table 34. Setting these parameters depends on the authenticated challenge-response ranging scheme and it is described in 6.9.8 for each scheme.

**In 8.3.9 MCPS-RANGING-Prover.request** replace NumMaxAllowedBitErrors with ResponseLength

MCPS-RANGING-PROVER.request (

TimeOut,

AuthenticatedChallengeResponseRangingMode,

RawMode,

ResponseLength,

…

SeqNumSupressed

)

|  |  |  |  |
| --- | --- | --- | --- |
| ResponseLength | Set of octets | As defined in clause 7.5.28 | Specifies the length in octets of the response to be used by the MAC sublayer when RawMode is set to TRUE. |

Page 135, line 2-7:

Upon receipt of the MCPS-RANGING-PROVER.request primitive, the MAC sublayer enables the receiver to receive the challenge and process it according to the set parameters including a timeout, the authenticated challenge-response ranging mode, enabling or disabling the FCS checking (RawMode), setting the response length (for RawMode) ~~the number of maximum allowed bit errors~~, distance commitment level and the other MCPS parameters as defined in Table 37. The choice of parameter values depends on the authenticated challenge-response ranging mode and it is described in 6.9.8 for each mode .

**r2-0280:**

***Resolution: Delete “mode”***

***r2-0281, r2-0286, r2-0288, r2-0289:***

***Resolution: Introduce a parameter in the VERIFIER-REQUEST and PROVER-REQUEST to inform the MAC sublayer to create and send an ACRRC IE in the RangingVerifier and RangingProver command in addition to the Challenge/Response.***

**In 8.3.6 MCPS-RANGING-VERIFIER.request** introduce a parameter:  **AcrrcIEIncluded**

MCPS-RANGING-VERIFIER.request (

TimeOut,

AuthenticatedChallengeResponseRangingMode,

RawMode,

ChallengeLength,

AcrrcIEIncluded

…

SeqNumSupressed

)

|  |  |  |  |
| --- | --- | --- | --- |
| AcrrcIEIncluded | Boolean | TRUE, FALSE | If set to TRUE, the MAC sublayer generates an ACCRC IE and transmits it within the command frame. The content of the fields of the ACCRC IE shall correspond to the values indicated in the parameters AuthenticatedChallengeResponseRangingMode and Security Level. |

**In 8.3.9 MCPS-RANGING-Prover.request** introduce a parameter:  **AcrrcIEIncluded**

MCPS-RANGING-PROVER.request (

TimeOut,

AuthenticatedChallengeResponseRangingMode,

RawMode,

ResponseLength,

AcrrcIEIncluded

…

SeqNumSupressed

)

|  |  |  |  |
| --- | --- | --- | --- |
| AcrrcIEIncluded | Boolean | TRUE, FALSE | If set to TRUE, the MAC sublayer generates an ACCRC IE and transmits it within the command frame. The content of the fields of the ACCRC IE shall correspond to the values indicated in the parameters AuthenticatedChallengeResponseRangingMode and Security Level. |

Replace the following lines 19-22 in section 6.9.8.3 with the following text:

“The MCPS-RANGING-VERIFIER.request and MCPS-RANGING-PROVER.request primitives contain the parameter AccrcIEIncluded to enable the transmission of the ACRRC IE in the RangingVerifier or RangingProver command frame for the next transmission to request the authenticated challenge response ranging mode and/or security level to be used by the receiving MAC sublayer. In such case, the receiving MAC sublayer shall use the values received in the ACRRC IE instead of any previously set ones for its next transmission (response).”

***r2-0172:***

***Resolution: Solved by resolutions on r2-0281, r2-0286, r2-0288, r2-0289.***

**r2-0173:**

***Resolution: Accept the proposed changed in the Excel sheet***

***r2-0174: Reject***

**Reason:** We discussed this in Hanoi during the meeting with Ben and Tero, that there is no need to specify a method for cryptographic random number generation. The base standard does not specify a random number procedure. Many methods exists and it is up to the implementation to choose and implement the random number generator.

**r2-0282:**

***Resolution: Change in the following way***

Change “Message Type” to “Message”

In the column keep only the number 1, 2, etc

To be done on all Tables 10, 11, 12, 13, 14 and 15

Also remove Command 1, Command 2, Data frame 3, 4, etc from all figures.

**r2-0285:**

***Resolution: Replace the following text:***

***Page 67, line 9-10 Replace sentence with:***

Optionally ACRRC IE can be used by enabling it in the MCPS-RANGING-VERIFIER.request to communicate the security level which the Prover MAC sublayer shall use for its next response command message.

***Page 70, line 9-10: Replace sentence with:***

Optionally ACRRC IE can be used by enabling it in the MCPS-RANGING-VERIFIER.request to communicate the security level which the Prover MAC sublayer shall use for its next response command message.

***Page 72, line 3-4: Replace sentence with:***

Optionally ACRRC IE can be used by enabling it in the MCPS-RANGING-VERIFIER.request to communicate the security level the Prover MAC sublayer shall use for its response command message in the next exchange. In a similar way, the ACRRC IE can be used by enabling it in the MCPS-RANGING-PROVER.request to communicate the security level the Verifier MAC sublayer shall use for its response command message in the next exchange.

**r2-0290:**

***Resolution: Reject the comment.***

The content of Table 13 was verified again and is correct.

**r2-0292: Accept**

We propose the following changes in the text on Page 74, line 12-14:

“With the fourth and fifth message of the sequence the verifier and the prover verify the integrity of the measurement and provide mutual authentication. The fourth message is a data frame containing VChallenge1 and PChallenge which the prover device sends to the verifier device with security level 1-7. The fifth message is a data frame containing VChallenge2 and PChallenge with security level 1-7 transmitted by the verifier device”. The data frame are preferably …

**r2-0176: Revise**

Change to “with security level 1-7.”

***r2-0320: Accepted with resolution***

Add UL, UL in Table 7-16 for the ACCRC IE.

***r2-0357: Revise with resolution***

The modes are already described and numbered in Table 27. The best is to modify the column in Table 34 and Table 37 as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| AuthenticatedChallengeResponseRangingMode | Integer | 0,1,2,3 | Specifies the authenticated challenge response ranging mode as described in Table 27. |

**r2-0295: Revise the text on line 9-10 on page 76 and 1-2 on page 77:**

“The next higher layer in each prover device should pre-configure the device’s fixed reply time referred to as *FixedReplyDelayTime*(1…N) on Figure 46 according to some pre-agreed sequence of replying before initiating the MCPS-RANGING-PROVER.request.

For example, using an LRP-ERDEV, the prover device fixed reply delay time can be configured by setting a multiplication factor using the PIB attribute *phyLrpUwbFixedDelayFactor.* The value in *phyLrpUwbFixedDelayFactor* is multiplied to the value in the in the PIB attribute *phyLrpUwbFixedReplyTime* to obtain the desired fixed reply delay time.”

**r2-0372: Accept and revise according to the proposed change in the excel:**

Replace “scheme”, “ACCR scheme” with "ranging mode" as proposed by Tero. This is much simpler.