**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | IEEE 802.15.4z MAC - CRG |
| Date Submitted |  |
| Source | Boris Danev (3db Access) |
| Re: | Letter Ballot Comments assigned to Boris Danev – 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>. |

**Technical Comments Resolution**

* i-1183, i-1820, i-2836, i-1184, i-1821, i-2837

In current LRP UWB the LEIP sequence is delayed by a constant *aLeipDelayTime* from start of SFD. Therefore we need to provide a way to change this behavior for LRP ERDEV. Therefore the PIBs *phyLrpUwbLeipEnabled* and *phyLrpUwbLeipLength* were proposed to override the base LRP UWB.

* i-0520

“A LRP device shall support default value of 128“ replace with “LRP UWB PHY supports up to 128. LRP UWB ERDEV supports up to 256.

* i-0002, i-0539, i-0579, i-0538, i-1862, i-2443, i-0535, i-0578, i-0536, i-0532, i-0420,

Line 18-21 replace with new following modified definition:

“The LRP-ERDEV supports challenge-response authenticated ranging with distance commitment on secret data payload.

A set of authenticated ranging schemes is described in 6.9.9 using the security services (Clause 9). Annex G provides the requirements to support distance bounding by distance commitment on the data payload.”

* i-0593, i-0592, i-0591, i-0472, i-0590, i-0913, i-1550, i-2751, i-0912, i-1549, i-2750, i-0474,i-0473,i-0911,i-1548,i-2473,i-0910,i-1547,i-2450,i-0916,i-1553,i-2613, i-0595, i-0476, i-0477, i-0603

Replace with revised 6.9.9. Doc 15-19-0259-00-004z-lb-comment-resolution-6.9.9.docx.

* i-0915,i-1552,i-2595,i-0914,i-1551,i-2571

Proposal of introducing MLME-RAW-ENABLE request primitive available in Doc. 15-19-0251-01-004z-letter-ballot-comments-MAC-LRP.

* i-0918, i-1555,i-2845,i-0917,i-1554,i-2844

Table 2 was simplified and corrected to follow Clause 9. Replace with revised 6.9.9 in Doc. 15-19-0259-00-004z-lb-comment-resolution-6.9.9.docx.

* i-0920,i-1557,i-2124,i-0919,i-1556,i-2068

Introduced two Payload IEs (Challenge and Response IE) following recommendation from Tero. SR c-data concept was removed.

Doc. 15-19-0251-01-004z-letter-ballot-comments-MAC-LRP.docx

Doc. 15-19-0259-00-004z-lb-comment-resolution-6.9.9.docx.

* i-1561

Section 6.9.9.4 was revised.

Doc. 15-19-0259-00-004z-lb-comment-resolution-6.9.9.docx.

* i-2123,i-0603,i-0481,i-0480,i-0479,i-2311,i-0240,i-0927,i-0928,i-0929,i-0931,i-1564,i-1565,i-1566,i-1568,i-2752,i-2753,i-2754,i-2755,i-0926,i-1563,i-2861,i-0482,i-0483,i-2153,i-0242,i-0484,i-0932,i-0933,i-0934,i-0935,i-0936,i-1569,i-1570,i-1571,i-1572,i-1573,i-2756,i-2757,i-2758,i-2759,i-2760,i-0243,i-0485,i-0486,i-0937,i-1574,i-2761,i-0938,i-0939,i-0940,i-0941,i-0942,i-0943,i-0944,i-1575,i-1576,i-1577,i-1578,i-1579,i-1580,i-1581,i-2762,i-2763,i-2764,i-2765,i-2766,i-2767,i-2768,i-0244,i-0945,i-0946,i-0947,i-0948,i-0949,i-0950,i-0951,i-1582,i-1583,i-1584,i-1585,i-1586,i-1587,i-1588,i-2769,i-2770,i-2771,i-2772,i-2773,i-2774,i-2775,i-0246,i-0245,i-0952,i-0953,i-1589,i-1590,i-2776,i-2777, i-0930, i-1567, i-1562, i-0925

All comments on Figures 36-40 are addressed in modified figures and corresponding text in the revised section 6.9.9.

Doc. 15-19-0259-00-004z-lb-comment-resolution-6.9.9.docx.

* i-0003, i-0004, i-1863, i-2465, i-2888,i-2884,i-2885,i-2565,i-2442,i-0577,i-2029,i-1194,i-1831,i-2030,i-0607,i-0325

Replace with revised Annex G provided in 15-19-0260-00-004z-lb-comment-resolution-Annex-G.docx. I followed the guidelines for information in annexes and the base standard structure of the annex content (e.g., Annex B, Annex F).

* i-2029, i-2030

Include the following references into Annex A.

[B24] Catherine Meadows, Paul Syverson, Range Authentication Protocols for Localization, 2007

[B25] David A. Basin, Srdjan Capkun, Patrick Schaller, Benedikt Schmidt, Formal Reasoning about Physical Properties of Security Protocols. ACM Trans. Inf. Syst. Secur. 14(2): 16:1-16:28 (2011)

[B26] Jolyon Clulow, Gerhard P. Hancke, Markus G.Kuhn, and Tyler Moore. So near and yet so far: Distance-bounding attacks in wireless networks. In Proceedings of the European Workshop on Security and Privacy in Ad-hoc and Sensor Networks (ESAS), 2006.

[B27] Nils Ole Tippenhauer, Heinrich Luecken, Marc Kuhn and Srdjan Capkun, UWB Rapid-Bit-Exchange System for Distance Bounding, In Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2015

[B28] Marcin Poturalski, Secure Neighbor Discovery and Ranging in Wireless Networks, Ph.D. dissertation, EPFL\_TH5131 (2011), https://infoscience.epfl.ch/record/166938/files/EPFL\_TH5131.pdf