**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **Proposed Resolution for MMS – Public part 2** |
| Date Submitted | November 2024 |
| Sources | Hong Won Lee (LG Electronics)hongwon.lee@lge.com |  |
| Re: |   |
| Abstract |  |
| Purpose | To propose resolution for “P802.15.4ab™/D01 Draft Standard for Low-Rate Wireless Networks” .  |
| Notice | This document does not represent the agreed views of the IEEE 802.15 Working Group or IEEE 802.15.4ab Task Group. It represents only the views of the participants listed in the “Sources” field above.It is offered as a basis for discussion and is not binding on the contributing individuals. The material in this document is subject to change in form and content after further study. The contributors reserve the right to add, amend or withdraw material contained herein. |

This submission contains the proposed comment resolutions for the CIDs 430, 431, 432, 433, 437, 438, 1152, 1154, 1156 and 1412

Rev 0: Initial version.

***Comment index#1152 in 15-24-0371-01-04ab-consolidated-comments-draft-1-0.xlsx***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| Billy Verso | 1152 | 63 | 10.38.3.6.1 | 29 | "Once a responder has received Public Advertising Poll Compact frame", missing "a", but also perhaps there is some qualification needed here, i.e., some validation by the application that it wants to start talking to this particular initiator. | "If a responder receives a Public Advertising Poll Compact frame from an initiator that it wants to perform ranging with, …." | Revised |

**Discussion**：Agree with the commenter. Intended responder should transmit the Public Advertising Response Compact frame as the commenter proposed

**Disposition: Revised**

**Disposition Detail:**

**- Original Text**



**- Proposed change**

***Change the sub-clause as follows (Track changes ON)***

**(*pp. 63 line #29*)**

After transmitting Public Advertising Poll Compact frame on the initialization channel, the initiator shall listen for an incoming Public Advertising Response Compact frame in the subsequent initialization slot. If a responder receives a Public Advertising Poll Compact frame from an initiator with which it intends to perform ranging, it should transmit the Public Advertising Response Compact frame with the public responder address specified in 10.38.9.2.2 in the subsequent initialization slot.

***Comment indices #430, 431 and 1154 in 15-24-0371-01-04ab-consolidated-comments-draft-1-0.xlsx***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| Tero Kivinen | 430 | 64 | 10.38.3.6.1 | 7 | The figure 32 should be expanded to proper message sequence chart, and include the MLME calls made by each side to send those messages. | Expand Figure 32 to proper MSC. | Revised |
| Tero Kivinen | 431 | 64 | 10.38.3.6.1 | 9 | The figure 32 is missing the POLL and RESP and ranging phases and REPORT frames shown on figure 33. | Add second half to the figure 32 to show what frames are sent / received and what MLME calls are done during the actual ranging phase on the ranging channel (you could use different arrow to indicate which messages are sent in initialization channel and which are sent on ranging channel). | Revised |
| Billy Verso | 1154 | 64 | 10.38.3.6.1 | 9 | Figure is wrong, the frame names should match compact frame names, and not be in upper case hyphenated typically only used for primitives. Also RespAddr should be "Responder Address". | Change "RespAddr" to "Responder Address", and change "PUBLIC-ADV-POLL", to "Public Advertising Response Compact frame" etc. | Revised |

**Discussion**：

Figure 32 should be changed to a proper message sequence chart to align with the baseline text. The purpose of this chart is to show how public addresses are used during the initialization setup phase, so the ranging phase does not need to be included. To ensure alignment with the baseline text, MLME and MCPS primitives have been included in the revised message sequence chart

**Disposition: Revised**

**Disposition Detail:**

**- Original Text**







**- Proposed change**

***Change the sub-clause as follows (Track changes ON)***

**(*pp. 63 line #27-33*)**

Figure 32 presents a message sequence chart that illustrates how public addresses are used in the initialization setup phase. After transmitting Public Advertising Poll Compact frame on the initialization channel, the initiator shall listen for an incoming Public Advertising Response Compact frame in the subsequent initialization slot. Once a responder has received Public Advertising Poll Compact frame, it should transmit the Public Advertising Response Compact frame in the subsequent initialization slot. The responder shall use its Responder Address as the source address and the Initiator Address obtained from Public Advertising Poll Compact frame as the destination address when transmitting the Public Advertising Response Compact frame.

**(*pp. 64 line #1-9*)**

After transmitting Public Advertising Response Compact frame, the responder shall listen for a Public Start of Ranging Compact frame in the initialization slot following the Public Advertising Response Compact frame. Once the initiator receives a Public Advertising Response Compact frame, the initiator shall use its Initiator Address as the source address and the Responder Address obtained from the Public Advertising Response Compact frame as the destination address for the Public Start of Ranging Compact frame. Subsequently, the initiator should transmit a Public Start of Ranging Compact frame in the initialization slot following the Public Advertising Response Compact frame. This procedure is shown in the Figure 32.



**Figure 32 – A message sequence chart for Initialization setup handshake using public addresses**

***Comment index #432 in 15-24-0371-01-04ab-consolidated-comments-draft-1-0.xlsx***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| Tero Kivinen | 432 | 64 | 10.38.3.6.1 | 15 | The figure 27 does not show the use of public start of ranging compact frames. | Change text to say "transmission of the Public Start of Ranging Compact frame similarly as is done in Figure 27", as we are just doing things similarly than in figure 27, but using different frames. | Revise |

**Discussion**：

The Figure 27 can be generalized to add representative expression in Table 1. As a result, Figure 27 can be referred to describe initialization setup procedure using public addresses. Additionally, O2MI RPRT and O2MR RPRT in Figure 31 should be changed to O2M RPRT based on changes in Table 1 and REPORT in Figure 26~30 should be changed to “RPRT” for consistency

**Disposition: Revised**

**Disposition Detail:**

**Proposed text changes on P802.15.4ab™/D01:**

**10.38.3.6 UWB MMS ranging session initialization using public addresses**

**- Original Text**









**- Proposed change**

***Change the sub-clause as follows (Track changes ON)***

**(*pp. 18 line #1*)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Compact Frame ID value** | **Compact frame name** | **Subclause** | **Representative Expression** |
| 0 | Advertising Poll | 10.38.9.4 | ADV POLL |
| 1 | Advertising Response | 10.38.9.5 | ADV RESP |
| 2 | Start of Ranging | 10.38.9.6 | SOR |
| 3 | One-to-one Poll | 10.38.9.7 | POLL |
| 4 | One-to-one Response | 10.38.9.8 | RESP |
| 5 | One-to-one Initiator Report | 10.38.9.9 | RPRT |
| 6 | One-to-one Responder Report | 10.38.9.10 | RPRT |
| 7 | Advertising Confirmation | 10.38.9.11 | ADV CONF |
| 8 | One-to-many Poll | 10.38.9.12 | O2M POLL |
| 9 | One-to-many Response | 10.38.9.13 | O2M RESP |
| 10 | One-to-many Responder Report | 10.38.9.14 | O2M RPRT |
| 11 | One-to-many Initiator Report | 10.38.9.15 | O2M RPRT |
| 12 | Public Advertising Poll | 10.38.9.16 | ADV POLL |
| 13 | Public Advertising Response | 10.38.9.17 | ADV RESP |
| 14 | Public Start of Ranging | 10.38.9.18 | SOR |
| 15 | Public Advertising Confirmation | 10.38.9.19 | ADV CONF |
| 16 | Acquisition | 10.38.9.20 | Acquisition |
|  17 | One-to-one Initiator Secure Report | 10.38.9.21 | REPORT |
| 18 | One-to-one Responder Secure Report | 10.38.9.22 | REPORT |
| 19 | One-to-many Initiator Secure Report | 10.38.9.23 | O2M RPRT |
| 20 | One-to-many Responder Secure Report | 10.38.9.24 | O2M RPRT |
| 21 – 29 | Reserved | - |  - |
| 30 | Reserved for vendor specific use | - | - |
| 31 | Reserved for extension into 2nd octet | - | - |

**(*pp. 58, 59, 61 and 62)***

**Instruction for the editor: Please change whole “REPORT” in Figure 26, 27, 28, 29 and 30 to “RPRT”**

**(*pp. 63 line #2*)**

**Instruction for the editor: Please change whole “O2MI RPRT” and “O2MR RPRT” in Figure 31 to “O2M RPRT”**

**(*pp. 64 line #10*)**

The initialization process with Compact frames in the initialization setup phase using public addresses is the same as shown in Figure 27.

**Instruction for the editor: Delete Figure 33**

***Comment index#433 in 15-24-0371-01-04ab-consolidated-comments-draft-1-0.xlsx***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| Tero Kivinen | 433 | 64 | 10.38.3.6.1 | 19 | Why switch from more private addresses to less private? Completely randomly generated 24-bit source and destination addresses are more private then addresses generated using 24-bit hashing. | Just use the public addresses throughout the whole ranging process. During the initialization phase both ends learns the random 24-bit addresses to be used, and they can easily be used during ranging phase. My understanding is that the ranging phase is not going to be taking more than few minutes at max, so keeping same address during the whole ranging phase is not an issue, as the "private" addresses also uses the same prand during the ranging phase, i.e., addresses do not change even there during ranging phase. | Reject.Following resolution of CID 427 |

**Discussion**：Similar to the resolution proposal for CID#427 in DCN#497r3 already accepted, private addresses can be used to provide 24 bits of randomness. This is an established standard for privacy in other standards that are used by over 4 billion devices world-wide. The RPA Hash using public addresses in the ranging phase shall be used in the ranging phase after initialization setup using public addresses to maintain the implementation consistency and reduce variation for validation

The important thing is that this private and public address concept for initialization setup and ranging phase reached a consensus among the TG members more than one year ago

**Disposition: Reject**

***Comment index#39 in 15-24-0371-01-04ab-consolidated-comments-draft-1-0.xlsx***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| Tero Kivinen | 437 | 65 | 10.38.3.6.2 | 1 | All this RPA\_hash generation is just extra work for the both devices without any gain. It does not offer any technical benefits, but will cause extra cost. | Remove this RPA\_hash generation and use public addresses directly during the ranging phase. If the broken addressing structure in the ranging phase cannot be fixed, you could also define that prand must be generated so that it is never all zeros, and reserve that value to mean that no hashing is done and hash will then directly be the public address. This would allow keeping the RPA\_prand and hash frame format in ranging frames without changing them. Poll frame would use responder address as hash and prand of zero, the Response would use initiators address as hash, etc. I.e., the hash field would be used as the destination address field. | Reject.Following resolution of CID 458 to generate RPA Hash. Additionally, RPA Hash generation for public addresses is needed to reuse poll, response and report compact frames to avoid variations from an implementation and validation |

**Discussion**：Referring to the resolution proposal for CID#458 in DCN#497r3 already accepted, generating the RPA hash is not additional work because AES-128 algorithm is required for CCM encryption and STS generation. This RPA Hash generation after initialization setup using public addresses is essential for reusing poll, response, and report compact frames to avoid variations from an implementation and validation perspective. Additionally, if we use the Initiator RPA Hash in the One-to-One Poll and One-to-Many Poll compact frames as the Responder Address (public) and the RPA prand as the Initiator Address (public), it may lead to ambiguity the original definitions of these subfields.

The important thing is that this private and public address concept for initialization setup and ranging phase reached a consensus among the TG members more than one year ago

**Disposition: Reject**

***Comment index #1156 in 15-24-0371-01-04ab-consolidated-comments-draft-1-0.xlsx***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| Billy Verso | 1156 | 65 | 10.38.3.6.2 | 1 | "RPA\_hash" with underscore is a format not typically used in the base standard to describe something | If technically acceptable, change "RPA\_hash" (everywhere it appears) to "RPA hash" without the underscore, otherwise pick another technically acceptable term not using underscore. | Revise |

**Discussion**：Agree with the commenter. RPA\_hash or RPA Hash can be replaced to “RPA Hash” which may technically acceptable term not using underscore

**Disposition: Revise**

**Disposition Detail:**

**Instruction for the editor**

***(PP 63, 64, 65, 79, 80, 92, 94, 97)***

RPA\_hash, shall be changed to “RPA Hash”

***Comment index #438 in 15-24-0371-01-04ab-consolidated-comments-draft-1-0.xlsx***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| Tero Kivinen | 438 | 65 | 10.38.3.6.2 | 18 | If the public addresses are used directly then the address list inside the one-to-many poll could simply be the public address of the responder, no need to generate GroupID or special message control field value 0x21 poll format at all. | Remove GroupID concept as it is not needed if public addresses are used directly. | Reject. Following the resolution proposal for CIDs 433 and 437, public addresses should not be used directly for the Poll Compact frame. The Group ID must be used for Address2 in Figure 34 to generate the RPA hash when multicasting a One-to-many Poll Compact frame in the first sub-round of the ranging round |

**Discussion**：First of all, it is not appropriate to use public addresses directly, as discussed in the resolution proposals for CID#433 and 437 in this document. Therefore, the RPA Hash should be used for the Poll Compact frame after initialization with public addresses, as described in section 10.38.3.6.2. The RPA Hash is generated using the Initiator Address and Responder Address pair. For a One-to-many Poll Compact frame in the first sub-round, the message shall be transmitted to multiple responders, and in this case, a multicast address should be used. The Group ID is used as Address2 in Figure 34 to generate the RPA Hash for multicasting a One-to-many Poll Compact frame in the first sub-round of the ranging round



The important thing is that this private and public address concept for NBA-UWB MMS initialization setup and ranging phase reached a consensus among the TG members more than one year ago

**Disposition: Reject**

***Comment index #1412 in 15-24-0371-01-04ab-consolidated-comments-draft-1-0.xlsx***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index#** | **Pg** | **Sub-Clause** | **Ln** | **Comment** | **Proposed Change** | **Disposition** |
| Hong Won Lee | 1412 | 114 | 10.38.9.18 | 15 | It is beneficial to add more values to the Status field in the Public Start of Ranging Compact frame to indicate whether the public address of a responder is duplicated or not. This scenario can be one of the error cases for public initialization and session setup | Add new status values such as "Public Address Duplication", "Public Address Duplication with New Address", and so on in Table 16. The behavior of the added status values should be described in sub-clause 10.38.9.18 | Revised |

**Discussion**：During initialization setup phase, there is probability of duplication Public Addresses. To address this issue, the Status subfield in the Public Advertising Response Compact frame can be utilized. Therefore, it is necessary to define additional Status field value and describe their corresponding the behaviours to manage duplicate addresses during initialization setup phase

**Disposition: Revised**

**Disposition Detail:**

**Proposed text changes on P802.15.4ab™/D01:**

**- Original Text**

**10.38.9.3.23 The Status field**



**10.38.3.6 UWB MMS ranging session initialization using public addresses**



**10.38.9.18 Public Start of Ranging Compact frame**



**- Proposed change**

***Change the sub-clause as follows (Track changes ON)***

**(*pp. 89 line #16*)**

**Table 16—Values of Status field**

|  |  |  |
| --- | --- | --- |
| **Status field value** | **Name** | **Meaning** |
| 0 | SUCCESS | Request is accepted |
| 1 | REQUESTED\_PARAMETERS\_NOT\_ACCEPTED | Request is denied as one or more requested parameters cannot be accepted by the Initiator. |
| 2 | REQUIRED\_CAPABILITY\_NOT\_SUPPORTED\_BY RESPONDER | One or more required capability is not supported by the responder. For example, a (Compact frame ID, Message Control ID) tuple intended to be used by the initiator is not supported by the responder. |
| 3 | REJECT\_WITH\_SUGGESTED\_CONFIG\_CHANGE | Initiator indicates rejection with the suggested difference from the configuration parameters in Advertising Response Compact frame. |
| 4 | REJECT\_WITH\_ADDR\_DUP | Initiator indicates rejection with duplication of the Responder Address in Advertising Response Compact frame |
| 5 | ACCEPT\_WITH\_NEW\_ADDR | Initiator generate new Responder Address and send to a responder to duplication of the Responder Address in Advertising Response Compact frame |
| 6 | FAILURE | Request is denied due to other reasons. |
| 7-255 |  | Reserved. |

**(*pp. 64 line #13*)**

If the initiator does not intend to proceed to the control phase, the Message Control field of the Start of Ranging Compact frame shall be set to 0x10, and the value of the Status field set as one of the non-reserved entries in Table 16 other than SUCCESS. If a responder receives a Start of Ranging Compact frame with the Message Control field equal to 0x10 and the value of the Status field is one of the non-reserved entries in Table 16 other than SUCCESS, the responder’s action is same as described in 10.38.3.2, except in the case where the value of the status field is REJECT\_WITH\_ADDR\_DUP or ACCEPT\_WITH\_NEW\_ADDR. In this case, the responder’s action is as follows:

* If the value of the Status field is REJECT\_WITH\_ADDR\_DUP, the responder may reattempt the session initialization with a different responder address randomly generated by the responder.
* If the value of the Status field is ACCEPT\_WITH\_NEW\_ADDR, the responder shall use the new responder address provided by the initiator, which is the New Responder Address subfield of the Message Content field, when the Message Control field value is 0x10, to proceed to the subsequent ranging phase.

If coordination is active and the initiator intends to engage in scanning for coordination packets, the initiator should send the Public Advertising Confirmation Compact frame with a public address to defer the transmission of the Public Start of Ranging Compact frame as shown in Figure 27. In this case, the public initiator address of Public Advertising Confirmation Compact frame shall be the same as the address of the Public Advertising Poll Compact frame.

**(*pp. 114 line #17*)**

When the Message Control field value is 0x10, the Message Content field shall be formatted the same as for the Start of Ranging Compact frame Message Content field with Message Control field value 0x10, as shown in Figure 70, with the same function and meaning for each of the fields.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| The Public Start of Ranging Compact frame with Message Control field value equal 0x10 is sent by the initiator to indicate the status of the initialization setup phase. When the Message Control field value is 0x10 the Message Content field shall be formatted as shown in Figure XX.Octets:1 | 0/4 | 0/1 | 0/1 | 0/6 | 0/1 | 0/7 | 0/4 | 0/1 | 0/2 | 0/1 | 0/3 |
| Status | Time Offset | NB Channel Seed | Presence Bitmap | NB Channel Map | Management PHY Configuration | Management MAC Configuration | Ranging PHY Configuration | Ranging MAC Configuration | Starting Block Index | MMS Ranging Mode Configuration | New Responder Address |

**Figure XX—Format of the Message Content field in the Public Start of Ranging Compact frame when the Message Control field value is 0x10**

The subfields in the Message Content when the Message Control field value is 0x10 are same as described in 10.38.9.2.2, except for the New Responder Address subfield. The value of the New Responder Address subfield is set to the value generating randomly by an initiator when the Status field value is ACCEPT\_WITH\_NEW\_ADDR. This subfield is omitted unless the Status field value is ACCEPT\_WITH\_NEW\_ADDR.