**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **MMS ranging using public addresses text for pre-ballot-B draft** |
| Date Submitted | Sept 2023 |
| Sources | Hong Won Lee, Insun Jang, Jinsoo Choi, HanGyu Cho (LG Electronics), Lei Huang, Bin Qian, Peng Liu, Chenchen Liu, Ziyang Guo, Rojan Chitrakar, David Xun Yang (Huawei), Mingyu Lee, Taeyoung Ha (Samsung) |  |
| Re: | Contribution to IEEE 802.15.4ab  |
| Abstract |  |
| Purpose | Certain content in the document, 15-23-0412r0 was omitted from Draft B, and this provides the content with respect to the pre-ballot-B draft |
| 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. |

***Insert the sub-clause 10.35.7 in Draft B as follows:***

* + 1. MMS Ranging Session using public addresses
			1. Overview

Public addresses may be used to establish an NBA-UWB MMS ranging session. The NBA-UWB MMS initialization process using public addresses is same as in the process described in 10.35.3 except messages such as PUBLIC-ADV-POLL, PUBLIC-ADV-RESP, PUBLIC-ADV-CONF and PUBLIC-SOR include public addresses specified in 10.35.9.2.2 which are used for initialization process.

To establish a ranging session, HRP-ARDEVs may engage in an initialization and setup stage and perform an initialization setup handshake as described in 10.35.3. After that the HRP-ARDEVs enter the control phase and the ranging session is started. The ranging session procedure is the same as described in 10.35.4 and 10.35.6 except for generating IdentityResolvingKeys (IRKs) for the RPA\_hash specified in 10.35.7.2.

In the initialization and setup stage, the initiator may send public advertising poll (PUBLIC-ADV-POLL) messages with a public address, AdvAddr specified in 10.35.9.2.2.

After transmitting PUBLIC-ADV-POLL on the initialization channel, the initiator shall listen for an incoming public advertising response message (PUBLIC-ADV-RESP) in the subsequent initialization slot. Once a responder has received PUBLIC-ADV-POLL, it should transmit PUBLIC-ADV-RESP with the public address RespAddr specified in 10.35.9.2.2 in the subsequent initialization slot. The responder shall set RespAddr as the source address and AdvAddr obtained from PUBLIC-ADV-POLL as the destination address when transmitting PUBLIC-ADV-RESP.

After transmitting PUBLIC-ADV-RESP, the responder shall listen for a public start-of-ranging (PUBLIC-SOR) message in the initialization slot following the PUBLIC-ADV-RESP message. Once the initiator receives a PUBLIC-ADV-RESP message, the initiator shall set AdvAddr as the source address and RespAddr obtained from PUBLIC-ADV-RESP as the destination address for PUBLIC-SOR. Subsequently, the initiator should transmit a PUBLIC-SOR message in the initialization slot following the PUBLIC-ADV-RESP message. This procedure is shown in the Figure X.



**Figure X – Initialization setup handshake sequence using public addresses**

The initialization process using public addresses is exemplified in the following figure:



**Figure XX - An example of the initialization process with public addresses (PUB-ADV-POLL refers to PUBLIC-ADV-POLL, PUB-ADV-RESP refers to PUBLIC-ADV-RESP, and PUB-SOR refers to PUBLIC-SOR as defined in Table 1.6.4.1)**

If the coordination is active and the initiator intends to engage in scanning for coordination packets, the initiator should send PUBLIC-ADV-CONF with a public address to defer the transmission of PUBLIC-SOR as shown in Figure 20. In this case, the public address (AdvAddr) of PUBLIC-ADV-CONF shall be the same as the address of PUBLIC-ADV-POLL.

After ranging session is initialized using public addresses, private addresses described in 10.35.9.2.1 shall be used during that ranging session. To handle private addresses, the IdentityResolvingKey(IRK) is generated by the initiator and the responder(s) to generate the RPA\_hash value specified in 10.35.9.2.1. The initiator’s address and a responder’s address which are exchanged during initialization shall be used to generate the IRK for obtaining the RPA\_hash value.

* + - 1. RPA\_hash generation and resolution after initialization using public addresses

For the ranging session after the initialization setup handshake using PUBLIC-ADV-POLL, PUBLIC-ADV-RESP, PUBLIC-ADV-CONF and PUBLIC-SOR, the IdentityResolvingKey (IRK) shall be generated using the public addresses which are known to both the initiator and the responder(s) for the RPA\_hash specified in 10.35.9.2.1 to use POLL, RESP and REPORT messages. The IRK shall be generated by concatenating the initiator’s address (AdvAddr) and the responder’s address (RespAddr for one-to-one, or GroupID for one-to-many) (MSBs zero-padded to make 16 bytes).

The format of the IdentityResolvingKey is shown in Figure XXX.



**Figure XXX – Format of IdentityResolvingKey**

A GroupID represents a group of devices in a one-to-many ranging session, as described in 10.35.8. By transmitting a PUBLIC-ADV-POLL message with the MessageControl field set to 0x21 on the initialization channel, a GroupID is shared with responders. The GroupID shall be used to generate the IRK for the RPA\_hash used in POLL (one-to-many) (message id 0x12) in the one-to-many ranging session, as described in 10.35.8, in case GroupID is shared with responders.

The GroupID is not shared if a PUBLIC-ADV-POLL message with the MessageControl field is not set to 0x21 on the initialization channel. In this case, the value, 0xFFFFFF shall be used to generate the IRK for the RPA\_hash used in POLL (one-to-many) (message id 0x12).

The initiator and responder devices maintain a resolving list by adding multiple IRKs. The resolving list shall be used to resolve RPA\_hash in a message from an incoming packet. If multiple IRKs exists in the resolving list, all the IRKs shall be iterated to resolve RPA\_hash, as described in 10.35.9.2.1.

The example in the below specifies a resolving list in case GroupID is shared to the responders.

AdvAddr = 0x6E538F, RespAddr = 0x401F4C, GroupId = 0x2A3E88

IRK1 (for POLL (message id 0x04)) = AdvAddr || RespAddr (MSBs zero padded) = 0x000000000000000000006E538F401F4C
IRK2 (for POLL (one-to-many) (message id 0x12)) = AdvAddr || GroupID (MSBs zero padded) = 0x000000000000000000006E538F2A3E88

The example in the below specifies a resolving list in case GroupID is not shared to the responders.

AdvAddr = 0x6E538F, RespAddr = 0x401F4C

IRK1 (for POLL (message id 0x04))) = AdvAddr || RespAddr (MSBs zero padded) = 0x000000000000000000006E538F401F4C
IRK2 (for POLL (one-to-many) (message id 0x12)) = AdvAddr || 0xFFFFFF (MSBs zero padded) = 0x000000000000000000006E538FFFFFFF

* + - 1. Advertisement information in PUBLIC-ADV-POLL

In PUBLIC-ADV-POLL, an AdvData field may be included to announce public advertisement information. The AdvData contains a sequence of AD structures, each AD structure shall have Length, Type and Value. The sequence is terminated when Length field is zero in the AD structure.

AdvData = {AD Structure1,…, AD StructureN} Where AD Structure={LEN[1], Type[1], Value[]}

The AD Structure may contain information which an initiator announces, such as service representation, friendly name, advertising interval, vendor specific information and so on. It is omitted if there is no advertisement information.