**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | Minutes of IEEE 802.15.8 TG teleconference meeting on April 13th EDT |
| Date Submitted | April 14th , 2016 |
| Source | Marco Hernandez (NICT) |
| Response |  |
| Abstract |  |
| Purpose | For reference in TG8  |
| Notice | This document has been prepared to assist the IEEE P802.15. 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 | The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15. |

**Content**

1. Minutes 3

1. Minutes

Chair: Prof. Myung Lee (CUNY), USA.

Secretary: Marco Hernandez (NICT), Japan.

-----------------------------------------------------------------------

─Chair calls the teleconference meeting to order.

**Chair:** The agenda for this teleconference is to check the progress status. We have two contributions.

1st presenter is Billy (Decawave) “Link ID needs to be filtered?” email sent to the email reflector.

─Billy explains that in some cases the link ID as source address may not be enough. Like in case of enhanced ACK, the MAC needs the real source address to send such enhanced ACK.

That would require maintaining a table of link IDs and corresponding source addresses. Moreover, there is not text describing the management and assignment of link IDs.

Options:

Do we need to maintain a table of link IDs?

Leave the issue to upper layers.

Delete link ID.

**Chair:** Without link ID would be the easy solution. Besides, it only saves 2 bytes.

**Billy:** No, up to 5 bytes out of 6 bytes for source address. Maybe, I can provide the text and during the May meeting to address the issue.

**Chair:** Aright; let’s accept the first line.

Billy moves a motion to accept the line “If a link-ID is included in the frame, then a full 48-bit PD destination address shall be present”

Second: Marco.
Vote: approved unanimously.

2nd presenter is Marco “Update on security” power point file sent to the email reflector.

─As PAC networks are infrastructure-less, security should not rely on infrastructure based authenticator servers. Neither password based authentication (impractical). We can use something similar to PGP, combining symmetric-key encryption and public-key encryption, because the operation is transparent to the user. Still, authentication is very important in order to prevent attacks. So, I am researching ECDH (elliptic curve Diffie-Hellman) key agreement protocol. That includes strong authentication without relying on infrastructure.

**Billy:** I guess there are some extra steps for users’ authentication, right?

**Marco:** This security proposal is for the MAC, PHY level. It is only concerned with a source address communicating to a destination address. Who is the user, it is up to higher layers.

**Billy:** But how a user indicates to communicate and authenticate with another?

**Marco:** That is part of the MAC service primitives for security.

**Chair:** What about the link IDs?

**Marco:** Good question. The security clause requires full source and destination addresses, no link ID. An attacker can spoof a link ID. Part of the authentication/integrity checking is a signature (hash) with the source and destination addresses.

─The group continues the review of the latest Draft r4 from 5.3.2 Maintaining synchronization procedure, page 45.

**Highlights:**

After a discussion, it was decided to leave the data rate parameter in MCPS-DATA primitives. Marco will check this issue if data rate is indicated from higher layers.

In page 45, line 12 “measurement” needs to be clarified and defined; what is measured? (Add as TBD).

Billy points out that “maintaining synchronization procedure”, is used as a noun sometimes and as an action other times, making the text unclear. The text needs to be revised with BJ.

In page 46, line 26, “sleep mode” has not been defined before.

─The review stopped at the end of page 47. It will continue from 5.4.3 Discovery procedure, page 48, line 2 during the next teleconference.

**Chair:** Any other comment? Hearing none, the teleconference is adjourned.