**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 March 31st EDT |
| Date Submitted | April 3rd , 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 one contribution.

1st presenter is Marco (NICT) DCN 16-321r0 "PHY related TBDs"

Comments:

**Billy:** In 15.4 the PHY does not talk to higher layers to indicate transmission with a given data rate.

**Marco:** 15.4 does not have PHY service primitives, but TG8 does. The data rate is indicated from the MAC to the PHY to transmit with a given data rate. However, higher layers monitor the radio channel condition by means of the channel quality indicator. Thus, higher layers can give an indication to use a given coding/modulation scheme and/or data rate depending on the radio channel conditions. We can indicate an index to a given data rate in the MAC service primitives, if required.

Marco moves a motion to accept the text in document DCN 16-321r0.

Second: HB Li.

Vote: approved unanimously.

**Chair:** Marco, please make the changes in the latest Draft.

**Marco:** Yes. Also, in good news, I will present a contribution for security based on AES in GCM mode.

It is fast because it can be parallelized; in fact Intel offers this mode in its chips already.

Moreover, the processing is online. That is, the packet size is not required. That makes the implementation easier as we do not have to deal with fragmentation, etc.

In the no so good news, GCM assumes there is a cryptographic key already for either encryption or decryption. How to create the keys, how to exchange them, how to refresh them, etc. what is the key management protocol is still TBD.

**Chair:** That is TG9.

**Marco:** Yes, for 15.4. I do not think we can reuse it directly because they assume the central node is the key master and they have access to infrastructure for certificate authorities. We do not have that. Anyway, there are proposals in the literature for our case. I am currently researching this topic. I need some more time. In principle, we can offer AES in GCM mode for security and the KMP may be incorporated later.

**Chair:** Ok, thank you.

─The group continues the review of the latest Draft.

**Highlights:**

The text for cyclic superframe requires revision (language, configuration, etc.) by SS Joo.

Billy will check if link ID addressing is filtered or not.

The TBDs about security will be addressed when Marco presents the security proposal.

─The review stopped in p. 44. It will continue from p. 45 during the next teleconference.

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