**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 Interim Meeting on January 2016 in Atlanta, GA |
| Date Submitted | January 26th , 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. TG8 sessions 3

2. Minutes 3

1. TG8 sessions

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Session | Monday | Tuesday | Wednesday | Thursday |
| AM1 |  | **TG8** |  |  |
| AM2 | **TG8** | **TG8**  |  |  |
| PM1 |  **TG8** | **TG8**  | **TG8**  | **TG8**  |
| PM2 | **TG8** |  **TG8** |  **TG8**  |  |

1. Minutes

Chair: Prof. Myung Lee (CUNY) USA

Secretary: Marco Hernandez (NICT) Japan

=================================================

Monday January 18th, AM2 session

−Chair calls the meeting to order.

**Chair:** The meeting's agenda is in DCN 16-60r0. The plan is to finish the 1st draft version.

−The agenda in DCN 16-60r1 is approved unanimously.

−Minutes of the previous meeting DCN 15-957r0 are approved unanimously.

**Chair:** Let's hear a report for the teleconferences.

1st presenter is Marco (NICT) DCN 16-60r0 "Summary of teleconferences previous to the January meeting"

Comments: none.

BJ moves a motion to affirm the motions during the teleconferences and 15-989r0 to be included into the Draft 0.16.1

Second: HB Li.

Discussion: none.

Official vote:

In favor: unanimous. Motion carries.

2nd presenter is BJ (ETRI) “Report on IEEE 802.15.8 PAC Draft Status"

Comments: none.

─Chair appoints Marco and Billy as sub-editors.

3th presenter is Marco (NICT) DCN 15-998r1 and 15-987r1 "MAC command frames (harmonized)"

Comments:

─After discussion, the group made some changes in the text.

**Chair:** Let's take a recess.

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

Monday January 18th, PM1 session

−Chair calls the meeting to order.

Marco moves a motion to accept 15-987r2 into the Draft specification

Second: HB Li

Vote: In favor: 7. Oppose: 0. Abstain: 0. Motion carries.

4th presenter is HB Li (NICT) DCN 16-67r0 “One-to-many and many-to-many peering procedures"

Comments:

─During the discussion, the groups decided the re-peering case is not going to be considered and it must be deleted in the draft.

─After discussion, the group decided to make some changes in the text to be presented tomorrow.

5th presenter is BJ (ETRI) Draft Specification 0.16.1 (editorial comments)

Comments:

 ─The group decides some text changes.

**Chair:** Let's take a recess.

=======================================================

Tuesday January 19th, AM1 session

−Chair calls the meeting to order.

─The presentation of BJ (ETRI), Draft Specification 0.16.1 (editorial comments), continues.

─BJ will update the Draft including the agreed editorial comments.

6th presenter is HB Li (NICT) DCN 16-84r0 "draft text of one-to-many and many-to-many peering and de-peering procedure"

Comments:

 ─The group discusses the proposed procedures.

**Chair:** Let's take a recess.

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

Tuesday January 19th, AM2 session

−Chair calls the meeting to order.

─The discussion with HB Li (NICT) DCN 16-84r0 continues.

Marco moves a motion to accept 15-987r4 into the Draft specification

Second: HB Li

Vote: In favor: 7. Oppose: 0. Abstain: 0. Motion carries.

**Chair:** Let's take a recess.

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

Tuesday January 19th, PM1 session

−Chair calls the meeting to order.

─The discussion with HB Li (NICT) DCN 16-84r0 continues.

─After discussion, the group made some text changes.

**Chair:** Let's take a recess.

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

Tuesday January 19th, PM2 session

−Chair calls the meeting to order.

Marco moves a motion to accept 15-987r5 and clause 6 of the internally circulated Draft "P802.15.8\_D0.16.1\_clean\_versionMarco19012016.doc"

Second: HB Li

Vote: In favor: 7. Oppose: 0. Abstain: 0. Motion carries.

HB Li moves a motion to accept 16-84r1 into the Draft specification

Second:

Vote: In favor: 7. Oppose: 0. Abstain: 0. Motion carries.

6th presenter is Dr Joo (ETRI) DCN 16-83r1 "Revised text for cyclic-superframe structure"

Comments:

─After discussion, the group made some changes to be presented tomorrow.

Marco moves a motion to accept 16-72r1 to be added in Table 66 of clause 6.3 of Draft Specification 0.16.1

Second: Billy

Vote: In favor: 7. Oppose: 0. Abstain: 0. Motion carries.

**Chair:** Let's take a recess.

=============================================

Wednesday January 20th, PM1 session

−Chair calls the meeting to order.

7th presenter is Marco (NICT) DCN 16-20r0 "Spreadsheets for submitting Comments and Comment-Resolution"

Comments: None.

Marco moves a motion to approve the spreadsheets for submitting comments and comment/resolution to the Specification of TG8.

Second: HB Li

Vote: Unanimous in favor. Motion carries.

8th presenter is Marco (NICT) DCN 16-102r0 "Channels assignment"

Comments:

**Billy:** Please include the UWB PHY.

Marco moves a motion to approve DCN 16-102r1 into the Draft Specification in clause 7.1.1

Second: BJ

Vote: Unanimous in favor. Motion carries.

9th presenter is Marco (NICT) DCN 16-103r0 "PHY frame structure"

Comments: None.

Marco moves a motion to approve DCN 16-103r0 and to replace the text in clauses from 9.2.1 to 9.2.13 of the Draft Specification

Second: BJ

Vote: Unanimous in favor. Motion carries.

10th presenter is HB Li (NICT) DCN 16-104r0 "Suggested changes for subclause 5.1.4 peering and de-peering"

Comments:

─After discussion, the group made some changes.

HB Li moves a motion to approve DCN 16-104r1 into the Draft Specification clause 5.1.4

Second: Igor

Vote: Unanimous in favor. Motion carries.

Dr Joo moves a motion to approve DCN 16-83r2 "Revised text for cyclic-superframe structure" into the Draft Specification

Second: BJ

Vote: Unanimous in favor. Motion carries.

**Chair:** Let's take a recess.

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

Wednesday January 20th, PM2 session

−Chair calls the meeting to order.

**Chair:** Let's revise the Draft in order to identify all TBDs and the procedures to form a PAC network.

─Chair goes through the latest Draft to identify and solve/assign TBDs

─Marco makes a document that captures TBDs in the Draft and assignees to solve them.

**Chair:** Let's take a recess.

===============================================

Thursday January 21st, PM1 session

−Chair calls the meeting to order.

**Chair:** Robert Moskowitz, Chair of TG9, is here to talk about security and KMP in 15.4.

**Bob:** How is your topology?

If you have any node to one, it is an *N* problem and it is manageable.

If you have any to any, it is an *N*2 problem, and that is more complicated.

**Chair:** We can consider there is an initiator node, which can take care of certain tasks.

**Bob:** Ok, any to initiator is a good thing, operationally speaking about security.

**Bob:** Are communication links private within a group? That is, each node has N keys with N security associations. Or there is one key per group managed by an initiator. If a node is kicked out, then a new group key must be reissued.

You need a KMP for joining with authentication and pair-wise key to distribute the group key. On the other hand, you should think on the mode of operation of the block cipher: CCM mode or GCM mode.

─CCM (counter mode with CBC MAC) offers encryption and authentication. It is a 2-pass scheme and it is not on-line (size of message is required), which make it slow, but CCM is patent-free.

GCM (Galois counter mode) offers encryption and authentication. It is fast, it allows on-line processing (size of message is not required), and it can be parallelized. Furthermore, it is patent-free.

**Tero:** In case of a node leaves; there is no need to re-issue a key, only when a node is kicked out.

**Bob:** When a node leaves or the counter space is exhausted, the initiator should re-issue the group-key.

For example, the initiator's policy is every 2 days to re-issue keys.

**Billy:** is this security protocol in higher layers?

**Bob:** No, this is at the MAC level. On top, there should be security in applications, like gaming, etc.

MAC-security protects the initiator. Upper layer-security protects the system/network and applications.

**Billy:** If there is security in higher layers, do we need to specify security then?

**Bob:** It is recommended to apply security at every possible layer. Besides, it provides privacy in the joining process and it allows me to control the services I support, closing the group.

**Bob:** The KMPs supported in 15.9 are 8021X, PANA (infrastructure based); IKEv2 and HIP (opportunistic); dragonfly (password based). Also, TG9 provides a high level AP for the transport of KMP.

**Billy:** Can we take the security clause of 15.4?

**Bob:** 15.4 has a factorial *N* problem for key management. Borrowing from 15.4, you will get way more of what you need.

**Tero:** Yes, you guys cannot just copy and paste the security clause. You have different parameters, different ways to join a network, etc. You need to see which portions are useful for you and start editing.

**Billy:** We mostly have mobile devices. It is not like 15.4 applications that are industrial deployed.

**Tero:** Look, cell phones have 4 cores in these days. That allows parallelization of GCM. It is fast and neat.

**Bob:** I do not agree. I think they are better off with CCM as high data rate is not an issue.

**Tero:** I do not think so, GCM allows and efficient parallelization and on-line processing.

**Bob:** we have our disagreements.

**Chair:** You mention group re-keying only if one node is kicked out. I think we may need to revise depeering, like a handshake scheme involving ACK to know if somebody really left, in contrast to a temporary exit of being in sleep mode.

**Billy:** Also, talking with Tero, we need to define an Ether type field in the MHR. That makes it easier for handling IP4 and IP6, if there is an ether type addressing.

**Marco:** What is the minimum packet size you need for the encryption engine?

**Tero:** In case of GCM there is not constraining as the processing is on-line (no need to know the packet's length).

**Bob:** In case of CCM, the minimum is 1024 bytes. 6 kbytes with certificates included. TG9 supports fragmentation with enhanced ACK for re-assembly. I think we can make it smaller, perhaps 256 bytes without certificates. 200 fragments are supported in TG9.

**Billy:** Do you have IP?

**Bob:** TG9 can be implemented patent-free entirely, if required. We took care of that.

**Chair:** I want to thank Bob and Tero for their participation and help.

11th presenter is Marco (NICT) DCN 16-125r0 "Assignees for TBDs"

Comments:

─2 issues were resolved.

12th presenter is Billy (Decawave) DCN 16-126r0 "Providing EtherType in the MAC data frame"

Comments:

**Marco:** what for?

**Billy:** It allows handling IPv4 and IPv6 more smoothly for applications.

Billy moves a motion to approve the text in DCN 16-126r0 into the Draft.

Second: BJ

Vote: Unanimous in favor. Motion carries.

13th presenter is BJ (ETRI) DCN 16-113r1 "Updated IEEE 802.15.8 PAC Draft"

Comments:

**Tero:** Place the Draft in the private server, no in Mentor.

**BJ:** But we need to ask Rick for that.

**Tero:** That is not a problem. Rick normally replies very fast.

**Marco:** Please let us revise the Draft. We can approve it during the next teleconference.

**BJ:** ok.

14th presenter is BJ (ETRI) DCN 16-122r0 "BCH Code Construction for Information Reconciliation"

Comments: None.

BJ moves a motion to approve the text in DCN 16-122r0 into the Draft.

Second: Marco

Vote: Unanimous in favor. Motion carries.

**Chair:** Let's schedule teleconferences:

February 3rd at 7:00 AM ET

February 17th at 7:00 AM ET

March 2nd at 7:00 AM ET

March 9th at 7:00 AM ET

**Chair:** Before a teleconference, please assignees/champions take care of TBDs and send an email for discussion. We will use the teleconferences for approval.

**Chair:** Editors, please start reviewing the Draft, and send an email for discussion if needed.

**Chair:** Last but not least, BJ will try to find a champion for security.

**Billy:** I volunteer, but I need to check my workload and if I can manage to do it as I am not an expert.

**Chair:** Thank you; please let's know your thoughts.

**Chair:** That's all for this meeting. The meeting is adjourned.