**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **TG9 KMP Minutes for January 2014 Interim meeting, Los Angeles, CA USA** |
| Date Submitted | 31st January 2014  |
| Source | [][NXP Semiconductors] | Voice: [+44-114-281-2655]Fax: [+44-114-281-2951]E-mail: [ paul.chilton@nxp.com] |
| Re: | TG9 KMP Minutes for January 2014 Plenary meeting |
| Abstract | TG9 KMP Minutes for January 2014 Plenary meeting |
| Purpose | Official Minutes |
| 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. |

**Monday January 20th 2014 PM2 session**

Chair Bob Moskowitz (Verizon) called the meeting to order at 16:02

Chair reminded all to record their attendance; a note of those not in 802.15 was made: Jouni Korhonen (Broadcom), Peter Yee (Akayla). Attendance log was used for 802.15 participants.

Chair showed the opening report document 15-14-0028-00-0009 and outlined the activities for the week. It was noted that the group needs participation of 15.7 to help with the 15.7 parts of the document.

Chair called the group’s attention to the IEEE patent policy and made a call for notification of essential patents. There were no responses in the meeting.

The minutes of the November meeting in Dallas were accepted by acclamation with no discussion or objections.

Chair reported that Ben Rolfe (Blind Creek Associates) has been assigned by Bob Heile (ZigBee Alliance, 802.15 WG Chair) to work with the group to help in writing the primitives section of the document. Pat Kinney (Kinney Consulting) and James Gilb (Tensorcom) will also help out.

Paul Chilton (NXP Semiconductors) showed document 15-14-0046-00 which gave the status of the Recommended Practice draft and some suggestions of the further work needed to complete the document in order to proceed to ballot. There was some discussion on the points raised in the document and all were accepted.

The task group went into recess at 17:08 until the Tuesday PM2 session

**Tuesday January 21st 2014 PM2 session**

Attendance log used.

Additional non-802.15 attendees: Brian Weiss (Cisco), James McIntosh (Vitesse Semiconductor), Mick Seaman (Self), Karen Randall (Randall Consulting), Peter Yee (NSA/IAD)

The Chair called the meeting to order at 16:07.

Chair showed the IEEE-SA patent policy and made a call for essential patents. There were no responses heard.

A list was circulated for those without access to the private area in the 802.15 document server to record their name and email address in order to have further drafts of the recommended practice forwarded to them. *[Listed so far: Karen Randall, Peter Yee, Brian Weiss, James McIntosh, Jouni Korhohen]*

Chair reviewed the opening report (doc# 15-14-0028-00-0009) for the benefit of those people who were not in attendance at the previous session.

Paul Chilton presented document 14-14-0046-00 on the status of the draft recommended practice for the benefit of those people who were not in attendance at the previous session.

A wide-ranging discussion took place. Topics covered included the way in which 802.15.4-2011 security is written. Significant problems were found in -2011 and it was suggested to use the 802.15.4-2006 security mechanisms as a basis and to provide input to SC-Maintenance to fix the problems in the roll-up revision work to the 802.15.4 standard which is proceeding at the moment.

Sleeping devices were discussed, in particular how a sleeping device can cope if it has missed a rekey. This might be solved by using a group key model with a hierarchy of group keys which will allow an old key to be used but then the device will be instructed to use the one that the rest of the network is now using. It was suggested we should investigate this use case in more detail and show how KMP can solve it.

Chair outlined his difficulties in getting to Beijing. He cannot arrive until Tuesday afternoon; however the Vice-Chair Peter Yee is available from Monday to chair any sessions before Bob arrives.

The task group went into recess at 17:23 until the Wednesday PM2 session

**Wednesday January 22nd 2014 PM2 session**

Chair called the meeting to order at 16:04.

He reminded everyone to record their attendance. Attendees from outside 802.15 were Karen Randall, Peter Yee, James McIntosh and Brian Weiss.

Chair reminded the meeting of the IEEE-SA patent policy and made a call for essential patents. There were no responses heard.

Tero Kivinen (INSIDE Secure) showed document 15-14-0065-01 [note: this is under the sc-mag group on the 802.15 document server] describing the security PIBs in -2006 and -2011, outlining the difference and the problems that he had uncovered. Further explanation and discussion followed. The diagram will go into the -2014 rollup; we may also have to provide a state machine to check the logic. If the security section can be fixed as maintenance work then it can be done through the SC-maintenance, otherwise if it needs different functionality, this would require a new amendment with the associated Study & Task group process. To begin the maintenance process, the group must enter a formal maintenance request on the subject.

In TSCH the probe request is used to find out about new coordinators by joining devices, or those which are mobile and have moved from their original coordinator. Without authentication this could be a big Denial of Service attack. Bob Moskowitz will be writing this up.

Paul Chilton showed a presentation on a proposal for the primitives needed for the operation of the fragmentation service (doc# 15-14-0092-00). The group agreed with the majority of the proposal for sending data payloads although it was pointed out by Tero that there was no need for a timeout on the receive side in order to clear the assembly buffer. In this case it would be sufficient if a new fragment 0 arrives to start reusing the same buffer, effectively throwing away the previously part-assembled payload. There was also discussion on the need for any other primitives for RESET other than the request; since there is no way to notify the receiver of the reset, and using the mechanism described above for clearing out the partial payload there is no indication required, and since there is no communication over the link the result of the RESET.request can be delivered synchronously, removing the need for a deferred RESET.confirm.

The topic of group keys was discussed. It was noted that ZigBee-IP uses a group key but does not consider rekeying which leads to the question of who causes a rekey to happen. It should be made clear that rekeys are not used solely when a keyspace is consumed, but are also used to lock out devices which left the network and should not be readmitted without being reauthenticated. The question of how to perform a rekey over a multi-hop mesh was also raised as something for the group to consider. If a group key manager is available it can send a notification to rekey. The question of how to send the rekey selectively to be able to lock out devices was also raised. Key lifetime policies may be used to control this. The group may wish to declare this problem out of scope in order to complete the work we are currently engaged in.

Chair showed the closing report, document 15-14-0061-01, and asked Peter to present it to the closing plenary.

The group will have a conference call in February to discuss progress at a date to be arranged. The call time may be around 09:00 EST but this will also be confirmed. Chair to arrange the call and ensure that the announcement meets any notification period requirements.

The meeting was adjourned at 17:12.