**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | **TG9 KMP Minutes for March 2014 Plenary meeting, Beijing, CN** | |
| Date Submitted | 31st January 2014 | |
| Source | [Peter Yee] [NSA/IAD] | Voice: [+1-415-215-7733] Fax: [] E-mail: [ peter@akayla.com] |
| Re: | TG9 KMP Minutes for March 2014 Plenary meeting | |
| Abstract | TG9 KMP Minutes for March 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. | |

**Wednesday March 19th 2014 PM1 session**

Vice-chair Peter Yee (NSA/IAD) called the meeting to order at 13:37

Vice-chair reminded all to record their attendance.

Vice-chair showed the opening report document 15-14-154-00-0009 and outlined the activities for the week. Of particular importance was review of the pre-draft 6 of the Recommended Practice.

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 January meeting in Los Angeles were accepted by acclamation with no discussion or objections.

Vice-chair showed document 15-14-0185-00 (for Paul Chilton, NXP Semiconductors) 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.

Tero Kivinen (INSIDE Secure) used he comments (15-14-0184-00) on the draft to drive a discussion with James Gilb (Tensorcom) regarding the correct specification of SAPs and MLME calls. Gilb suggested that a data model was required before it was reasonable to discuss the specifics. Kivinen briefed Figure 1 from the draft specification to show the proposed layout of the existing 802.15 MAC layer entities and the additions that 802.15.9 brings to the picture.

Gilb suggested that there might not be a need to perform explicit duplicate detection as most MACs already provide this service. Also, the use of acknowledged receipt of frames may not be necessary as the need to retransmit a KMP transaction would be handled by the KMP, so using acknowledgements may be redundant. This is particularly the case because the acknowledgements only indicate that the remote system received the frame at the MAC layer, not that it was further processed.

SAPs need to be named and drawn in place according to Gilb. The naming then affects MLME calls. In Figure 1, a SAP is needed between the Data Higher Layer and the KMP Service. A lower level SAP into the shim might be named as the multipurpose SAP since it can handle both KMP payloads as well as IEs for other purposes that wish to take advantage of the fragmentation capabilities of the shim.

As for use of the current fragment counter/multipurpose ID field, the use of a full 16-bit Ethertype might actually be a useful thing. It would additional bytes be taken from the payload to convey the Ethertype. Kivinen suggested that this could be accomplished by using a value from the multipurpose ID set and then using the first two octets of the payload to hold the Ethertype.

Gilb and Kivinen had a lengthy discussion of how many of the fields from a normal 802.15 MCPS\_DATA request need to be replicated into a (tentatively named) MCPS\_KMP\_DATA.request call. There are obviously more than a KMP has need of. The PANId might be one useful addition that the KMP would actually find necessary, although it is not currently passed. There’s also a need to support both long and short address forms. While KMPs are expected to deal with long addresses only, other users of the shim’s fragmentation service may prefer short addresses. Other fields to consider include the SrcAddrMode and DestAddrMode. Arising from that discussion of which fields to include, Kivinen will send Gilb information on some inconsistencies in 802.15.4 regarding the ordering of the fields. Gilb noted that the shim should like virtually identical on its top interface to the interface over which it lies. It might, therefore, make sense to simply point at MCPS\_DATA and indicate any parameters we add on top of the existing set.

Gilb went to suggest that there should be an explicit indication of when something goes “wrong”. And he pointed out that a confirmation call doesn’t indicate anything to the sender other than that MAC found the request compliant and that it would attempt delivery of the PDU.

Kivinen pointed out that a call to delete a KMP to kill of old security associations would make sense. It doesn’t have to be confirmed in any way, but helps the remote party to stop transmitting under a key that the sender of the delete request is no longer using to decrypt traffic.

Based on the discussion, teleconferences should be held with at least Tero Kivinen and Paul Chilton (as the document editor) participating. On the basis that Chilton would want to have sufficient time after the teleconference to create a new draft, a second teleconference will follow in about 3 weeks’ time to finalize that draft. Dates will be announced in the closing plenary after suitable candidates have been agreed by Kivinen and Chilton.

The meeting was recessed at 15:30.

**Wednesday March 19th 2014 PM2 session**

Attendance log used.

The Vice-chair called the meeting to order at 16:00.

The Vice-chair inquired if there were further topics to be discussed during this meeting. Attendees indicated that none were needed at this time.

A reminder to do attendance was made. No request for essential patents was made as the attendees were a subset of those present during the immediately preceding PM1 session.

The meeting was adjourned at 16:02.