**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 2012** |
| Date Submitted | 20 January 2011 |
| Source | [][] | Voice: [+44-114-281-2655]Fax: [+44-114-281-2951]E-mail: [ paul.chilton@nxp.com] |
| Re: | TG9 KMP Minutes for January 2012 |
| Abstract | TG9 KMP Minutes for January 2012 |
| 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. |

**Attendance:**

Attendance Log used.

**Discussion**

*Tuesday, AM2 session*

Bob Moskowitz (Verizon), Yoshi Ohba (Toshiba), Peter Yee (IAD/NSA), Tero Kivinen (Authentec) Noriyuki Sato (Toshiba), Paul Chilton (NXP Semiconductors)

The meeting was called to order, and Bob requested those present to fill in their attendance, and presented the patent policy. Bob asked if people had read the minutes from Atlanta (15-11-0850-00); since no-one acknowledged they had read them, it was decided to allow more time for people to read before asking for the minutes to be accepted.

Bob presented the Opening Report (15-12-0017-00-0009). The goals of the TG were stated. It was noted that the PAR and 5C were produced at the November meeting. These satisfied comments from TG15.6 and WG 802.11. WG 802.21 requested that PANA be included explicitly. There are still major concerns still to be address from WG 802.1

The next steps for the TG were presented; it is necessary to appoint Officers for the Group in order to proceed. With this in mind Bob asked that people consider putting themselves forward to fill the positions of Chair, Vice-Chair, Secretary and Technical Editor. It was suggested that the candidate for Tech Editor should have experience of the position if possible. Presentations to other groups within IEEE and external entities will be required: possibly a tutorial to the rest of 802.15 at the March meeting, liaisons with IETF and ZigBee and a presentation to WG 802.1 addressing their concerns

Bob presented the document 15-12-0024-01 KMP Transport Proposal

The Recommended Practice document structure was discussed - the document will be in 4 parts: KMP Transport frame format and state machine, 15.4 support for KMPs, 15.7 support for KMPs and KMP-specific implementation guidelines

The aim is to use the Information Elements present in both 15.4e and 15.7. Fragmentation will be used to enable KMP packets which are larger than the underlying MPDU size to be carried. Fragmentation chaining will be used to simplify reassembly (no out-of-order fragment reassembly). There will be support for multiple concurrent KMP sessions to be in progress

The format of the KMP frame was discussed. The identifier for KMP frames and the length supported per fragment will be MAC-specific. Within the frame is a control field and the contents of the KMP fragment. The control field is 1 byte long and contains a 1- bit chaining flag indicating if this is the last /only fragment or if there are more following, and a 7-bit field containing either a KMP id or a fragmentation chain count. The control field of the first fragment provides the KMP identity (values 1-31) – eg 802.1x, HIP, PANA, IKEv2 etc. When used in subsequent fragments the field is used for the chain count: the chain count starts at 32 to disambiguate between KMP-Ids and fragment count. Count=32 denotes 2nd fragment, Count=33 denotes 3rd fragment. Using this system it is possible to create a KMP payload up to 8kb in 15.4e

Tero suggested that values be reserved for future expansion, eg 31 for extra KMP types, and 127 for an extra count field

The first draft of the state machine will be presented by Bob in the future. The aim is to make this as simple as possible

In a 15.4e implementation both Multipurpose and Command frames will be used to carry the Information Elements (IEs) which carry KMP frames. We will need a new IE type assignment for these IEs. Forced ACKs will be used for fragment acknowledgement in both 15.4 and 15.7 implementations.

The question of how to support the process on pre-4e devices was raised in IETF. This can be done by creating an IEs analogue in 6LoWPAN using a dispatch code. A document explaining this will be presented at the March IETF meeting in Paris

The scheme will not support multihop; it is only providing keying for a single link. There is an assumption that if backend processing is needed by a KMP there will be a way to get to the backend by a higher layer. This will be dealt with in the guidelines for the individual mechanisms eg PANA will have section on how to get back to the authentication servers.

It would be useful to have a 15.7 expert on board to advise on the implementation. Bob will contact Rick Roberts

It is expected that the Guidelines subsections for each KMP will be written by experts in that protocol eg HIP, IKEv2, PANA etc. There will be a profiling section for each KMP giving optional and required functions to be supported

In the remaining sessions of this meeting we need to check and approve the Atlanta minutes and appoint officers and a technical editor for the TG. We should also decide on presentations and liaisons with other groups eg presentation to all of 802 or just 802.15 WG. We need to organise a joint meeting with 802.1x and present to them what we are trying to achieve. Other liaisons need to be organised for Zigbee and IETF 6LP and Core groups.

A timeline will be presented in a later session to show what we need to have by March and November.

The group went into recess at 11:37 until the Wednesday AM1 session

*Wednesday AM1 session*

The session was called to order at 8:06. Bob went through the purpose of the group, administrative issues and the boiler plate patents duty to inform slides including call for essential patents. He also asked for people to go through the Atlanta minutes (doc 15-11-0850-00) so they can be approved in the Thursday PM session

Bob asked for nominations for officers for the TG – Peter Yee volunteered for the position of Vice Chair and was accepted unanimously.

An update of the KMP Transport Proposal document (15-12-0024-03) was presented by Bob. He made a call for proposals for each different KMP types to be worked on.

The document structure for the Recommended Practice was presented

The point was made that we still need fragmentation to carry KMPs even with 15.4g sized packets available – we cannot expect to have them available in all situations. It was noted that TG4k is moving large packets and also need to have fragmentation; however they are using sub- MAC fragmentation which we don’t want to look at. As previously noted, we have to be able to deal with small MPDUs and hence provide fragmentation support with no out-of-order reassembly, and also must be able to support concurrent sessions.

Frame format slide (slide 6) modified with count 31 and 127 as reserved values was presented.

Allows 95 fragments which allows a 6kB KMP frame to be transported under 15.4e (assumes a 65 byte MPDU payload which is conservative.

15.4 specific implementations will use Information Elements in multipurpose frames and, command frames. These have a smaller capacity than IEs which can be accommodated in the Data payload. There are 16 Information Element Ids available but only 5 values left unassigned. We will need one assigned to our work.

Unauthenticated PDUs will use long addresses, while KMP rekeying over a previously secured link can use short addressing

Question from Yoshi whether there is a need for a fragment number if we do not allow out-of-order reassembly – strictly not, but since we need the byte for identifying the chaining and KMP type we may as well use it

Discussion on IE ids – generally MLME related operations use header IEs. Payload IE type MLME is provided to do secure MLME transactions where the payload is encrypted but the header not. Do KMPs need their own IE under which more can be sublisted, or could we use the nested MLME to do a KMP sublist?

Bob is writing an internet draft in response to questions posed at the IETF meeting in Taiwan which will explain how to do KMP for non-4e devices using RFC4944 6Lowpan dispatch type for KMP which would be equivalent to Payload IE. He will present this at the IETF-83 meeting at the end of March in Paris

Security association will be per link pair, with broadcast SAs possibly being KMP specific (ie HIP etxc). Lighting applications may need to have secure group/broadcast, and TVWhite Space applications may want this as well. The question is how to manage and distribute the broadcast key. For march start writing the document for this

For 15.7 implementations, the Information Elements will be carried in command frames not in data frames. They will also use forced ACKs for fragment chaining using command frame ID 0x14. We will need an IE ID assignment but this should not be a problem as currently only 2 out of 255 have been assigned. Using header IEs means we can only support IE with 255byte length which is not the size of the largest frame 15.7 supports. It may be possible to transport multiple IEs in one command frame, but it is not clear how the processing could be done

In the Guidelines section, each KMP has a subsection, with general description and use case. Bob made a call for contributions for each different KMP to supported. We will also need to profile KMPS to fit in the respective MACs

Initial list of KMPs consists of 802.1x, HIP, IKEv2, PANA and SAE. Bob will write the HIP section, Tero the IKEv2, Yoshi PANA and we need volunteers for 802.1x and SAE

KMP profiling will describe how the KMP will work in a particular instantiation on 15.4 or 15.7 IKEv2 runs currently runs over UDP and will need to describe how will it run over a MAC. We also need use cases on why to use a particular KMP, eg based on code size, power, and reuse of code. Also descriptions of how deployments will be done with practical examples – topics such as identity and registration and also lifecycle management eg how to rekey

Opened floor to discuss March meeting – we want to have presentations and content for each of the different KMPs. 5 sessions have been requested, one for liaison with .1x and the others for technical content presentations on KMPS, state machine, framing etc

Paul Chilton volunteered to be secretary to the group and passed with unanimous approval.

Bob outlined a timeline to have a ballot of a draft in the TG in September

The Thursday sessions will be used for developing the project timeline and to discuss presentations for liaisons in March. We also need to sort out liaisons for IETF, ZigBee and 802.1. Email Bob on any other organisations which may need a liaison

Question on whether a tutorial in March is needed and the scope (15 WG or 802)? To be decided on Thursday. 802.15 hasnt got LLC in stds – nested IEs have been put in for LLC functions in 15.4

Recess at 09:13 until Thursday PM1 session

*Thursday PM1 session*

The meeting was called to order at 13:41. Bob presented the patent policy and asked for approval of the minutes of the last meeting; changes were discussed regarding the recorded attendance and were amended. The minutes were accepted as amended

Bob present the latest revision (rev 4) of the KMP Transport Proposal document (15-12-0024-03) – he had made minor changes and done more work on 15.7

For 15.4e we should use IEs in the payload not the header since they can be protected for rekeying and they can be longer than header elements (which are restricted to 127 bytes). Even with the MLME nested IE the length is still limited to 255. The length of a payload IE can be the size of the maximum 4g payload (2047 bytes) which may allow us to avoid fragmentation in some cases

A KMP specific IE ID value will be requested from the 5 available rather than use the MLME nesting value (9) We may end up with a nested value since there are so few of them. We should try to avoid MLME nesting if possible in order to use payload IEs rather than the smaller header IEs

From Pat Kinney’s presentation on 15.4e in the WNG session, the new ack frames can be security protected but this may make the ack time longer due to the need to perform security processing. We will use unsecured acks to keep the ack time as short as possible

On the 15.7 specifics slide Bob has added a question on whether a command frame can contain only IEs (thinks probably not but need to find out definitively). There are no payload data frame IEs available in 15.7 as is the case in 15.6. In 15.7 we will use 0x14 as the command frame identifier to contain IEs.

In the Guidelines section J Haapola has been added to help with HIP, but we still need an author for SAE

Invited comments; there were none

The next step is to convert the bullet points in the presentations into text

A teleconference will be scheduled with 802.1; Bob will start arranging this next week and announce on the 802.1 list. The intent is to have it near the end of February. The IETF liaison will be covered by Tero and Bob; it was suggested that we should contact Robert Cragie (ZigBee security chair) for the ZigBee liaison. Are there any other alliances or standards bodies we should be liaising with? It was suggested that Positive Train Control may want to have a liaison which could be useful as their requirements have the need for rapid connection and leaving from a PAN due to the speed that trains may be moving (600km/h)

Presentations to other groups were discussed. It was decided that a presentation to 802.15 WNG would be useful for the March meeting to inform the WEG on what the group is doing. The earliest that we should provide a presentation to the whole of 802 is probably July

When writing text for inclusion in the document, contributors should use Word for the text and Visio for diagrams. The Technical Editor should merge the contributions into a complete document using FrameMaker since this is the final format used in the IEEE. Some points were made that if the final format for handover to the IEEE editing team was Word this would allow several people to work on corrections etc rather than relying on the Tech Editor who could become a bottleneck. This would leave the IEEE editing team to do the conversion to FrameMaker; some reservations were expressed as to the accuracy of conversion that may be achieved

The session went into recess at 14:12

## Thursday PM2 session

The session was called to order at 16:05

Bob presented the TG goals, patent policy and instructed those present to register their attendance

The liaison with 802.1 was discussed. 802.15 requires give 1 weeks notice of a telecon to be given on the mailing list, but 802.1 needs 3 weeks so we will use this time period when arranging a joint teleconference. It is likely that it will take place near the end of February; Bob will provide the conference bridge facilities. If held at the end of February it will be possible to include the results in any work we do for the March meeting. The intent of the telecom is to cover with 802.1 the decision process for setting up the TG and explain why we are doing this work. Bob does not expect problems but it does need to be a formal meeting. He will circulate call information and ask for assistance. The time to hold the call was discussed; it would be useful for European participants if the call is scheduled early in the morning PT, mid-morning ET

Other liaisons were discussed. Bob will work with Bob Heile to start at liaison with ZigBee, and will also approach PTC. A question was asked whether the IETF liaison should include the Roll and Core working groups but it was thought that 6LoWPAN is probably sufficient

The presentation to WNG should aim to be about a 10-15 min update, to explain the goals of the group and the work being done; Bob made a call for help in producing slides for the presentation on TG9 activities

Bob presented a draft of the closing report to be presented at the closing plenary by Peter since Bob would be leaving before the plenary. This includes a suggested timeline; hold a WG ballot on the draft document in July (which may be a little aggressive) which means we need a tech editor well before then. Allowing 2 recirculation ballots for the draft, a date of March 2013 was suggested for Sponsor Ballot which would result in a July 2013 submission to RevCom. A question was raised on whether we need to do a TG ballot first to reduce the number of WG ballots we need. A TG ballot was added in July 2012 which pushes the WG ballot to Nov 2012 and then the Sponsor Ballot to July 2013 and RevCom submission for Nov 2013. Bob noted that comment resolution will require the content contributors to fix their text, not the Tech editor

The goals for the March meeting were discussed. We should have real text submissions for a draft document, appoint a technical editor and make a presentation at the 802.15 WNG.

Mike McInnis - Advice that it might be easier to use Word to avoid bottleneck with tech editor making changes and let the IEEE sort out framemaker conversion.

Karen asked if there will be TG calls other than those for the 802.1 liaison. Bob said that there may be conference calls scheduled between the section authors to decide on how the text is to be structured and to ensure consistency between the sections

There have been 4 sessions requested for the March meeting but it should be possible to get more if needed. A deadline for contributions to be available by end of business Friday 2nd March was agreed

A call for Any Other Business was made by Bob – none was forthcoming

The Task Group was adjourned at 16:28 until the March meeting