**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 2012 Plenary meeting, Waikoloa Hawaii** |
| Date Submitted | 08 May 2012 |
| Source | [][] | Voice: [+44-114-281-2655]Fax: [+44-114-281-2951]E-mail: [ paul.chilton@nxp.com] |
| Re: | TG9 KMP Minutes for March 2012 Plenary meeting |
| Abstract | TG9 KMP Minutes for March 2012 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. |

**Attendance:**

Attendance Log used.

**Discussion**

*Monday 12th March, PM1 session*

The meeting was called to order at 13:34. Bob Moskowitz (Verizon) as Chair welcomed everyone and showed document 15-12-0118-00-009 TG9 Opening Report, outlining the goals of Task Group. He invited everyone to register their attendance and showed slides explaining the IEEE Patent Policy and patent related links. He made a call for attendees to notify the TG of any potentially essential patents; there were no responses

The Minutes of the January 2012 session held in Jacksonville FL were posted in February. The Chair asked if people had read the minutes and asked that they be approved. There were no comments or objections and therefore were approved by acclamation.

The goals of the group, to produce a recommended practice for using existing MAC frames to carry KMPs, and the dependencies it has on other standards and groups were noted. The Chair commented that the group should aim to create the recommended practice in a relatively short time frame.

Following on from the creation of the PAR and 5C (docs 15-11-0613-06-0kmp and 15-11-0665-05-0kmp respectively) there are still outstanding concerns to be addressed from WG 802.1 related to 802.1X and the general support within 802.15 standards for Logical Link Control (LLC)

Bob Moskowitz presented document 15-12-0130-00-0009. This document attempts to summarise the concerns expressed by 802.1 as shared in written feedback and also from a joint teleconference between the two groups held on 22nd February 2012.

15.4 does not provide a means of differentiating between of types of data within its data traffic, leaving all management to be done at a higher layer. This includes the Key Management mechanisms as needed for 15.4 security, leaving each user of 15.4 to provide its own flavor of key management.

802.1 provides a layered approach to multiple MAC management challenges; in particular it provides a transport mechanism and state machines for device authentication and key establishment in the 802.1X standard. The 802.1 WG raised questions as to why TG9 is not using these mechanisms.

Although 802.1 provides existing mechanisms which are targeted at the problems that 802.15.9 is addressing, there are some difficulties in using 802.1 methods within 802.15, namely the fact that 802.15 lacks any direct reference to 802.1 and LLC in general and leaves any such functionality to the 'higher layer'. Early versions of 802.15 did provide references to LLC (802.2) but later versions removed them. If the facilities were available within the standard, 15.4 could inherent from 802.1. Should TG9 attempt to produce a general solution rather than one directed strictly at Key Management in order to enable reuse of the 802.1 standards?

A related point in 802.15.4 is the small MPDU available; it will be challenging to support 802.1X frames directly, although the MPDU chaining mechanism being defined in TG9 to support KMP will allow the support of large frames as a general feature. The background of 802.15 systems was referred to: typically highly constrained with small memory, low computing power and limited electrical power

In constrained systems, every feature must bring value for their cost; many KMPs have their own state machine and running them over 802.1X and EAP may add cost without adding value. A question to be answered is what specific value does 802.1X provide over a KMP directly implemented on top of the MAC? 802.1X will be one of the choices available in the recommended practice, but will not be the exclusive KMP. Any use of 802.1X MUST include key establishment along with authentication.

Karen Randall (Randall Consulting) pointed out that the comment from 802.1 about text in the IEEE 802.15.9 PAR which implied that security using EAP leaked secrets had not been addressed in the presentation and that it was important that it be dealt with. Bob Moskowitz took an action to send a letter to 802.1 to correct the statement that caused the comment to be made; the original response to 802.1 was condensed from a more complete text and got mangled in the process. He will send the corrected text to the TG9 list for consideration by Wed pm.

Bob has had discussions with James Gilb and Bob Heile; they think that it would be advantageous if the work done in this working group on fragment chaining can be made flexible enough to allow other groups to use.

The Chair showed document 15-12-0024-05 KMP Transport Proposal as the latest revision. It was noted that the group still needs input from a 15.7 expert to advise on the use Information Elements.

Fragmentation chaining will require a registry of the KMPs supported and their value in the KMP ID field; values 1-30 are available with 0 and 31 reserved. There are 96 fragments available which will allow a total of 6kbytes in the KMP frame. As a reference the default frame size for IKEv2 is 1050 bytes, although the maximum frame size may reach 3kbytes, which suggests that a 6kbyte maximum frame size will be adequate

The 4e Payload Information Element (IE) will be used to carry KMP fragments as it allows up to 2047 bytes to be carried rather than the 127 bytes allowed by a Header IE. Further payload may also be carried after the IE. Within the IE identifiers there are 5 which have not been allocated. There is an IE ID that is used for nesting of MLME payloads which could be used to carry KMP frames, but it is limited to a payload length of only 255 bytes. TG9 would like to take one of the reserved values for KMP, which would allow the use of full 2k.

Unauthenticated MPDUs will only use 64-bit address on the assumption that we are performing KMP before a device is authenticated which may mean that a 16-bit address has not been allocated yet. The exception to this is that we might be doing rekeying on previously authenticated devices which would allow the use of short addresses if they have been previously allocated.

The recommended practice will use forced acks in the chaining of KMP fragments; the acks will be unsecured since we are using them before keying is complete. There will be no out-of-order assembly of fragments, since the use of forced acks requires that a fragment is acknowledged before the next is transmitted.

If TG9 KMP takes one of the IE-IDs available this may cause problems with running out of IDs for use by other groups. It has been suggested that the ID be allocated to a “Device Control” function with a 1 byte subfield which would then allow the ID to be more widely shared; KMP would use one of the subfield values. The subfield could then allow other uses within the Device Control number space. The Chair suggested that the group revisit the coding of fields in the fragment chaining to match this format and so be more flexible; although not in the TG charter it would be good practice and would maintain a larger pool of unallocated IE-IDs.

All the work has addressed devices with 4e MACs. For devices with pre-4e MACs there needs to be some way of implementing KMPs. For 6LoWPAN devices it may be possible to allocate a RFC4944 dispatch type to have the same function as 15.4e KMP IE ID. This would allow 6LoWPAN device with 4e and non-4e MACs to be supported. The Chair requested someone to step forward as author for this part of the document.

Security Associations (SAs) in 4e were discussed. The relevant table showing the content of the security association is in section 7.5 table 60. There is a SA per link pair which raises the question of how to implement broadcast SAs; is it KMP specific or is it 1 key per source, with a shared key space including the source MAC-ID. In a lighting application broadcasts are useful where a switch can send a broadcast so that several lights will respond to the same signal, making the application simple. There are other things to consider such as the hidden nodes problem which may be discussion points.

Regarding specifics of 15.7, the only IE available is in the command frame; as is the case in 4e it will also need IE assignment and will use the forced ack for chaining the KMP fragments. A question of whether it is possible to construct command frames only containing IEs was raised; unfortunately there was not enough 15.7 expertise in the meeting to answer this, highlighting the need for participation from someone with 15.7 knowledge. The IE in 15.7 only allows 255 bytes to be used since the length field is 1 byte long. The same considerations for security associations arise as for 15.4e broadcasts (See section 7.5 of 15.7 spec for SAs).

Referring to the Guidelines document, each KMP has its own subsection. The initial list of KMPs and authors is unchanged from the January meeting; it was noted that authors are still needed for 802.1X and SAE. The use cases should describe the properties listed in slide 22 eg deployment, life cycle management, code size. The section authors will need to work together as a team so that the different sections follow the same structure to allow easy interpretation between KMPs and their properties. The content of each KMP section should address questions such as how a particular KMP works, how is registration done in trusted environments. Insights into code sizes for different CPUs would also be useful, perhaps by asking proponents of the KMP for size estimates of real implementations, and what functions are needed for components inside the KMPs and how big are they (eg libraries or certificates). The aim is to provide a comparison between the different KMPs so that there is a common understanding of what the cost of a particular KMP is, so that we have an idea of applicability in different contexts. Practical examples are to be encouraged.

The group still needs an Editor for the Guidelines document.

The group went into recess at 14:41 until the Tuesday PM1 session.

*Tuesday March 13th PM1session*

The meeting was called to order at 13:34. Bob Moskowitz as Chairman called for people to register their attendance and showed docs 15-12-0118-01-0009 Opening Report and 15-12-0115-01-0009 Agenda, and made a call for anyone present to notify of any knowledge of essential patents.

Bob noted that efforts taking place in 15.4k Low Energy Critical Infrastructure Monitoring (LECIM) are relevant to the constraints of the devices we are dealing with. They are dealing with low power availability (maybe even energy harvesting), and low bandwidth and may not even have enough energy to transmit a full frame. They are investigating sub-MAC fragmentation, possibly with 64 fragments to allow a 512byte MPDU. Most KMPs can be transported in MPDUs of that size but would still need fragmentation chaining. It may be useful to take advantage of some of the features available in 4k such as the fragmentation and reassembly and group acks. It was suggested that the group look at the 4k docs 15-12-89-02-4k to see how it all works. Peter Yee (Akayla) asked how it would be possible to determine if two devices are 4k-capable. Bob was unsure on this and maybe the group need to ask 4k.

The concerns raised by 802.1 were noted by the Bob, regarding the comment about leaky security which arose from condensing document 15-11-0805-02 into an email. A change to the text was suggested to include the phrase “secret will leak through other paths outside of their use within the protocol”. The document has been amended and posted to the list; the Chair asked everyone to review it with a view to sending it to 802.1 before the end of the week.

A skeleton guidelines document 15-12-0116-00-0009 has been posted by Bob. Another call for a volunteer for a document editor was made. The people who have agreed to author the various sections were asked to take ownership of sections of the document. The goal is that the KMP sections will be similarly aligned to carry similar levels of information and have the same look and feel.

Some discussion on examples of the information that might be needed in the different sections took place. Bob noted that the strength of the HIP puzzle would be set to zero as an example of how a KMP might need usage guideline. Similarly IKEv2 will need to show how it works without the UDP layer. Yoshi Ohba (Toshiba) asked if HIP and DEX will be supported in the document. Bob said that they are included and will show how HIP DEX will work for very small sensors. Currently it is ECDH based, but work is ongoing to use DH so that there are no Elliptic Curve patent issues on IPR.

 Tero Kivinen (Authentec) suggested that it might be necessary for HIP DEX to support both methods, but at the moment there is no method for negotiating which to use. In most KMPs it will be obvious what to use or easy to work out if there are alternatives, but wasn't sure about HIP. Bob replied that HIP can tell from the packets and can also perform negotiations between the two types in HIP DEX bis.

A wider question was raised on how to tell whether the two ends participating do or don’t support a particular KMP. It was suggested that this issue be addressed in Atlanta. Discussion followed on the topic suggesting that in most cases the decision on which KMP to use is done out-of-band as part of the PAN configuration, and questioned the value of adding selection mechanisms into the protocol. In some implementations there are various levels of controllers and devices; the controllers may have to support several KMPs to talk to all the devices, but the one to be used with a particular device will be chosen at configuration time.

The Chairman made a call for contributors to start adding to the doc 0116.

The meeting was turned over to Yoshi Ohba for a presentation on PANA running over 15.9

Yoshi presented document 15-12-109-00. There is an accompanying word document 15-12-108-00 which can be used as text in the guidelines document.

The presentation showed the standard PANA EAP message exchange over UDP between the PANA Client (PAC) and PANA Authenticator Agent (PAA) and then extended it to show relay operation used where PAC and PAA can’t communicate directly. The Relay (PRE) node passes messages as a forwarder; the PANA relay is used in multihop mesh networks to transfer PAC messages to the central PAA and vice versa. It is intended to allow PANA relay to work directly over the link layer using 15.9. PANA serves as bootstrap KMP. PAA talks to AAA server outside of mesh using an AAA protocol such as RADIUS. The link layer credentials can be group pre-shared key or a short term public key. The presentation also shows how messages map addresses from IPv6 to MAC IDs.

Tero Kivinen questioned if PANA can be used for bootstrapping; the focus is on bootstrapping but could be used for link establishment as well. Tom Herbst (Silver Spring Networks) commented that PANA relay is used in ZigBee-IP because of the need for multihop. Bob Moskowitz pointed out the similarity between PANA and 802.1X – the authors of these sections should work together on the use cases to show where the similarities and differences are. It was suggested that when describing using multihop for authentication between PAC-PRE-PAA that the text should explain the multihop is being used for authentication establishment and the key is for the single link.

As a general point authors should make sure all the examples line up between different KMPs. HIP and IKEv2 authors will also work together as they are similar. The goal for Atlanta in May is to get more text submissions. They should be structured as per slides 23-25 of document 15-12-0024-06.

Karen Randall asked Bob if the document Yoshi has provided (15-12-108-00) is what is expected; Bob said that the content would be able to be dropped into the Guidelines document. Karen asked to be able to see a revised full version of doc116 a couple of weeks before the Atlanta meeting so that everyone has a chance to review it before the meeting.

Bob covered changes to document 15-12-24-06. The description of fragment chaining has been modified to allow it to be multipurpose chaining. Karen asked how this change fits with the groups scope, in that it looks like it is expanding. Bob said that he had talked to Bob Heile and Pat Kinney; we only talk about its use in KMPs but if we can make it so that others can use the same mechanism that is to be encouraged. The KMP ID has changed to be multi-id. The fragment count now goes from 1-96, with the Ids at end of range rather than at start – slide 8 shows ID 98 for KMP, with 97 - 127 reserved. The method allows others groups to define IDs and use the same fragment chaining technique.

4k may not need to have multi mac frames to carry KMP payload – all done in the subfrag although some frames may be too big and will need accommodating.

The meeting went into recess at 14:29 until the Tuesday PM2 session.

*Tuesday March 13th PM2 session*

The meeting was opened at 16:01.

It was agreed that the Thursday am session will be used for next step discussions and presentation of further contributions.

The meeting went into recess at 16:02 until the Thursday AM1 session.

## Thursday 15th March AM1 session

The meeting was called to order by the Chairman Bob Moskowitz at 08:07 and all were requested to register their attendance.

 Bob noted that it will be necessary to formalize the KMP sections as per slide 23 15-12-0024-07 to all use this structure, although it is expected that this will expand as we fill in each section for different KMPs. In May, the group should be working on real text in the Guidelines document. Paul Chilton (NXP) asked how text blocks will be integrated into the document without separate edits clashing with each other. Bob replied that until a volunteer for Technical Editor comes forward he will be performing the editing role to put text submissions into the document.

The meeting was handed over to Andrei Gurtov (Univ of Oulu, Finland) to present document 15-12-0162-00-0009 “Implicit Certificate scheme in Host Identity Protocol (HIP) Diet Exchange (DEX) for the Fast Initial Authentication (FIA) use”. He described the use of small lightweight (implicit) certificates in sensor networks which provide fast verification. The certificate can be reduced to 160 bits although if attributes such as valid before and valid after are needed this will cause the size to grow

Only the Host Identity (HI) is certificated which reduces the amount of data to be transferred in HIP signaling. The paper assumes sensors have permanent public/private keys installed in the factory. There is no hash function used, but uses CMAC as a replacement of the hash of the BEU and I. A search for existing patents has not shown anything apart from one describing implicit certificates as noted in the references of the presentation

Yoshi Ohba (Toshiba) asked if the BEU in slide 5 is secret or not known to the other node? Andrei replied that they are chosen randomly on Elliptic Curve, and need to register to set up the system, which means the sensor will need to talk to the registration authority

Bob noted that the use of CMAC should be looked at very carefully as it has some boundary conditions that need to be avoided and it may not be possible to do an easy substitution of CMAC for a hash function; he suggested that this be posted to the IETF Crypto list to get it reviewed by others.

Bob suggested that slide 5 looks more related to 802.11 rather than related to 15.4 and asked for it to be changed to show a sensor to controller, and also show the registration of the sensor to the CA to get certificate.

Bob showed the closing report 15-12-0153-00-0009

Karen Randall requested that the group discuss the response to 802.1 concerns as Other Business. In trying to clarify the response in the bottom paragraph, we are trying to say that secret would leak, but this isn’t due to EAP, rather it is a consequence of any shared secret. Karen suggested to take out the reference to EAP. She also thought it was quite bold to say that this amounts to no security at all in the long run. If a shared secret is implemented correctly they will be ok. Bob’s point is that the secret has to be printed somewhere to upload to the authentication server. Blueray has a database of keys which leaked, and something similar happened with HDMI – the manufacturer key can easily leak if people are able to get hold of it

The response will be uploaded to the list and then sent to 802.1 on Monday. Karen asked for clarification on what Bob was going to send. Bob said that he would send this bit of text for comments and then update the full doc 0805 when 802.1 have given their comments.

Bob stated that 15.7 are looking at secure ID work so we will be able to work with 15.7 experts and also have use case for 15.7.

Planning for a presentation to 802.15 will now slide out to July 2012, and a general update to 802 will be in November 2012. The group should look into the contents of the presentations at the May meeting in Atlanta, although the question was asked if we want to do work to give the 802.15 presentation in May. Discussion around this noted that there would need to be a teleconference in April to achieve this, but the consensus was that we should concentrate on getting good text for the guidelines document to work on in the May meeting.

The next meeting is the week commencing May 13th, so it was suggested to have a teleconference in the week commencing April 23rd with another tentatively scheduled in the week commencing May 7th if needed. The second call would be used to get agreement on existing content from the previous call rather than adding anything new. It was suggested to go for 24th April at 9am EDT with the follow up if needed on May 7th time TBD

Text will be posted on the TG9 list for initial review.

Karen suggested that we should decide in the May meeting if a joint meeting should be held in July with 802.1.

A call for any other business was made by Bob. None was forthcoming.

The meeting was adjourned at 08:54.