**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **TG9 KMP Minutes for November 2012 Plenary meeting, San Antonio TX USA** |
| Date Submitted | 13th November 2012  |
| Source | [][NXP Semiconductors] | Voice: [+44-114-281-2655]Fax: [+44-114-281-2951]E-mail: [ paul.chilton@nxp.com] |
| Re: | TG9 KMP Minutes for November 2012 Plenary meeting |
| Abstract | TG9 KMP Minutes for November 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.

**Tuesday November 13th 2012 PM1 session**

The Chair Bob Moskowitz (Verizon) called the meeting to order at 13:43, and reminded everyone to register their attendance.

He showed the Opening Report (15-12-601-00) containing the Patent Policy and called for all persons present to notify if they had knowledge of any essential patents. No responses were heard.

Bob called for approval of the minutes of the September minutes (15-12-0567-00). No comments or questions were heard; the minutes were approved by acclamation.

The work items for the week were reviewed; the aims of this meeting are to

1) develop the state machines needed to drive the KMP process,

2) work out the MLME calls and triggers these state machines will require and

3) write the text describing the above.

The document 15-12-0458-03 Moving Forward was shown in order to allow discussion of the above tasks, and to show the state of the work so far and the decisions taken. It was noted that the aim of the Recommended Practice is to show how to transport keys across a link using an already specified KMP, not to develop a KMP itself.

Discussion on the following topics took place.

The approach to designing the state machines will be to describe them in pseudo-code first and then draw state diagrams.

The position of the group from previous meetings is to use COMMAND frames to carry Information Elements (IEs) for KMP encapsulation; this may require a maintenance item for 15.7 to allow a command frame to be issued with only an IE (ie without containing a command). Bob will attend the SC Maintenance meeting this evening to explore this.

When the KMP Transport is initially used during security establishment, unauthenticated PDUs will use long addresses, while rekeying within authenticated PDUs may use short addresses.

It may be necessary to request a Command Frame ID to carry KMP IEs in both 15.4 and 15.7.

A question was raised over whether it is necessary to identify the KMP being used in each payload fragment or only in the first fragment – is it redundant in the other fragments?

There will be 2 state machines required, one for outbound command frame processing and the other for reassembling the KMP transport packets and passing to the next highest layer.

A question was raised on whether there should be a maximum number of retries on a fragment; later it was realized that the MAC retry mechanism will take care of this, simplifying the outbound state machine.

The authenticated ACK introduced in 4e needs its counter decrementing before it can be processed properly.

The Transport mechanism state machine needs to handle triggers from the KMP higher layer, such as what will initiate the KMP or starting a rekeying. Suggestions for triggers to initiate the KM P include an Association event. A trigger event for a rekeying operation could be the device’s Frame counter reaching a particular value.

The time when to start KMP was discussed – should it before or after association? No clear decision was reached. On a coordinator with security enabled, a possible trigger to start KMP might be if unsecured frames are detected from a device. Who drives the process of setting up security? There is no indication in beacons that the PAN is security-enabled (actually security is link based so some devices may be secure and others not).

The meeting went into recess at 15:00 until the PM2 session starting at 16:00.

**Tuesday November 13th 2012 PM2 session**

The meeting was called to order at 16:03, and Bob reminded everyone to register their attendance.

During the recess, Bob talked to Ben Rolfe regarding how frames with forced ACKs are processed by the 15.4 MAC. Outbound frames which require ACKs will keep being retried by the MAC until it hits the maximum number of retries specified in the MIB. This is transparent to the sender, and is simply reported by the MAC as unable to deliver. Inbound (reception) does not check for duplicate packets which might occur if an ACK was lost even if the frame was received correctly. All packets are passed up to the higher layer together with the sequence number – at least this is true for data packets. The same does not seem to be true for command frames. But we need the sequence number to be delivered up to the higher layer to check for duplicate packets. This needs more thought to work out how to go forward and whether we can use IEs in command frames. The matter was discussed with Bob Heile on how a Command frame for IEs only could be specified.

A sketch of the state machines was developed on a flipchart. The outbound state machine is simple, but the Inbound is a lot more complex.

There may need to be a limit (implementation dependent) placed on the number of concurrent KMP processes in process at any time in order to limit the memory resources used by KMP streams at the coordinator. The coordinator should reject KMP requests which exceed capacity.

It was suggested that it is only necessary to flush out a failed reassembly when the same Source address performs another KMP transaction. This would mean that it would not need a timeout to discard an incomplete reassembly process. *[Note: but if there are a fixed number of transactions that can be handled at a time this could be taking up valuable space]*

Further discussion took place on when should the KMP process happen – before or after association? It may be necessary for it to be able work in both situations. Keying first will allow control over who is allowed to associate by using secured association.

It is probably not possible to complete a KMP between issuing an Association Request and the paired Association Response. This suggests that Association must happen before KMP (or KMP before Association but not mix the two), and discussion moved towards preferring KMP as the first action after Association.

The frame counter needs to be monitored in order to trigger a rekey operation. However the frame counter gets incremented whenever a frame is sent, both command and data. If we only look at the frame counter whenever a data frame is sent we may not see the frame counter reach the trigger. It was suggested that whenever a frame is sent the frame counter is tested in order to trigger a KMP rekey after counter increment; this would require an amendment to the operation of the frame counter increment operation.

Recessed at 17:42 until Thursday AM1

**Thursday November 15th 2012 AM1 session**

The meeting was called to order at 08:10.

Bob reminded everyone to complete their attendance, and distributed a set of handouts he had produced to use for discussion. He was unable to use the projector to display these as he has no computer at present. The handouts consisted of 4 pages showing an Architecture diagram, the Outbound state machine, the Inbound state machine and a page containing a number of notes.

Bob went through the handout pages. The architecture will now use a shim sitting above the MAC. The KMP transport will use MAC Data Frames containing IEs only.

The Outbound state machine operation was not changed from that discussed in PM2 on Tuesday.

The Inbound state machine needs to filter for duplicate packets that may come about if an Ack is missed by the sender; this is a consequence of the MAC inbound processing where all packets received are passed to the next higher layer, along with the sequence number of the packet.

The Sequence number is short (8 bits) so this may end up wrapping. Identifying a duplicate from the (Src address, Seq number) pair may not be sufficient if there is other traffic from the same source interspersed with the KMP traffic*.* If this is the case do we need to keep the complete previous KMP frame to check if has been duplicated? The Frame Counter is 32-bits long which would alleviate this problem but it is only incremented on secured packets so would not work when security is being established .

The Coordinator in a system needs to be able to cope with multiple simultaneous KMP streams – how many is implementation dependent. If a sender times out or runs out of retries and the KMP process stalls in a particular stream, we may end up with a partial reassembled KMP frame in the buffer. The inbound state machine diagram needs to incorporate a timer which if it expires can be used to free the buffer. The time required is TBD.

As an aside, Bob reported that he had attended the Standing Committee for Maintenance for 802.15 on Tuesday evening. The committee will be looking to correct the security section (section 7) in 802.15.4-2011 to make it intelligible. Bob called for everyone to look at this area in the specification to make sure that there are no other areas that need fixing. He is intending to ask for a warning to be inserted on the dangers of using the encrypt-only mode allowed by the AES-CCM\* process.

It was suggested that both state machines need to have timers on activity to allow them to reset properly if either end of the transaction fails.

The Ack frame in 802.15.4-2011 has no identity associated with the packet being Ack’d. It relies on the short time window to associate the Ack with the packet. Bob identified a situation where it is possible for an adjacent PAN to send an unrelated Ack at a time where it could be misinterpreted as being for a transmission in the PAN we are interested in *[will the PANid in the Ack frame sort this out?]*. The enhanced Ack in 15.4e has the source address of the device so contains an explicit identity which will get over this problem; the enhanced Ack will be used in the KMP transport mechanism. It can be used authenticated or unauthenticated if needed before keying has completed.

The MACsecurityEnable flag is set by the higher layer to indicate to the MAC service to send secure packets. This only makes sense after keys are available so can’t be used as a trigger to start the KMP process. The KMP process will be triggered by the next higher layer requesting the process to start. This will allow the KMP process to be completed before or after association and is the most robust method of triggering the KMP.

Rekeying will be triggered from the MAC frame counter reaching a threshold count some way below the rollover point. The threshold is used to ensure that since we can only monitor the Frame Counter value easily when data frames are used, any secured command frames (which will also cause the Frame Counter to change) can happen without pushing us over the rollover point without seeing it coming. The size of the threshold should be hundreds if not thousands below the rollover to ensure a high probability of catching the threshold before rollover even if there are many command frames being sent.

Bob will also put in an errata to the Maintenance SC about the way the Frame Counter increment works.

Bob will add the diagrams in the handouts into the Moving Forward document (15-12-0458-03) next week when he has a PC again.

It is likely that the Data Frame IE-only mechanism can find a use in other activities such as the Layer 2 Routing. It can also be used to encapsulate other protocols and information such as 802.1 bridging protocols, ethertypes or vlans.

In current PHYs it is estimated that it will take 5yrs to roll the frame counter (given traffic constant sending). But there may be faster PHYs in the future eg as proposed in 15.4p PTC and IG-THz which will cause the Frame counter to roll a lot sooner – rekeying is now a serious need. Text will be added to the document to point this out.

In the next session we will look at plans going forward.

Recess at 08:50 until the AM2 session.

**Thursday November 15th 2012 AM2 session**

The meeting was called to order at 10:35; Bob reminded those present to complete their attendance.

During the recess discussion took place between Bob and Peter Yee (Akayla) regarding the trigger for rekeying, specifically defining what the intercept point for monitoring the Frame Counter. The Data service is used by the next higher layer to send data by issuing a request to send data, and the MAC responds with a response to indicate the status of the send. The intercept point will be the request not the response to the send request. To show this the architecture diagram needs to be changed to show the path from the next higher layer down to the MAC passing through the shim, and the path from the MAC up to the higher layers passing outside the shim. So the rekey trigger monitoring is performed on a successful send and not reception of data.

Paul Chilton (NXP Semiconductors) undertook to transcribe the diagrams into Powerpoint and send to Bob for inclusion in the Moving Forward document.

The next IEEE 802.15 meeting will be held the week of January 14 in Vancouver BC Canada. It is expected that work on the text of the document will happen in December, and we should have a conference call to discuss the content before the meeting. Possible dates for the call were suggested as the week of December 17th or the week commencing December 31st.

The group decided to hold the conference call on January 3rd at 07:00 PST / 10:00 EST / 15:00 GMT, with a notification to be posted by Bob in the week of December 17th.

A copy of the document will be posted by December 14th for review and comment, and discussion in the call on the 3rd.

There will be 4 slots at the Vancouver meeting.

Mike McInnis (Boeing) asked what the schedule for releasing the document to the Working Group would be; Bob replied that the intention was to have it ready for the March meeting, subject to contributions from authors for the various KMP sections.

Mike also asked if this State machine mechanism could become addendum to 15.4. Bob indicated that this may well happen and he is in contact with other groups who might wish to use this work.

Bob called for any other business; none was indicated and the meeting was adjourned at 10:49.