**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | **TG9 KMP Minutes for July 2012 Plenary meeting, San Diego CA USA** | |
| Date Submitted | 14 August 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 July 2012 Plenary meeting | |
| Abstract | TG9 KMP Minutes for July 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 16th July, PM1 session*

The meeting was called to order at 13:38 by the Chair, Bob Moskowitz (Verizon), after which he asked those present to register their attendance. He also asked that speakers announce their name and affiliation when addressing the group.

The opening report (document 15-12-0358-00) was displayed, containing slides on IEEE patent policy as regards the duty of participants to inform if they know of any essential patents; the Chair called for anyone with knowledge of essential patents to advise the group.

The minutes of the May meeting (document 15-12-0304-00) were approved by acclamation with no comments.

Bob showed document 15-12-0024-09 “Key management support for 15.4 and 15.7”. He noted that TG 15.8 Peer Aware Communications may also appear in the document as they start work.

The use of information elements provide a traffic selector (like Ethertype) which is missing in the 15.4 protocol – at present, without a traffic selector different higher layers (e.g., ZigBee PRO and ZigBee-IP) cannot coexist in the same PAN.

Bob asked for people to think about the state machine to control the KMP transactions, particularly trigger events for the state machine such as what can cause the KMP to start or restart, and whether KMP could run before a device associates with a Full Function Device (FFD). Other scenarios suggested were what mechanisms should be initiated when a devices loses its keys, or what to do when the MAC security frame counter gets close to overflow indicating a rekey operation is needed.

It was noted that the use of Information Elements for KMP transport in 15.7 can only use a payload IE, of maximum size 255 bytes; the group need to find out if it is legal for a command frame to contain only an information element. This may become a maintenance clarification that can be addressed within the 15.7 TG since they have recently resumed activity. It was suggested that the 15.8 TG needs to consider this point as they develop their MAC.

Versions of the 15.4 specification up to -2011 use a small frame size (128 bytes) to allow devices to use a cheap crystal. Using crystals with 40ppm stability requires the packet size to be limited so that frequency mismatch or drift between the transmitter and receiver is not a problem.

It was noted that during a fragmented KMP packet transfer we may have to handle duplicate fragments due to the ack being lost and triggering retransmission of the fragment.

It was suggested that the use of in-order delivery of fragments (i.e., single threaded) will not be a problem since the KMP process is done relatively infrequently.

It is unlikely that KMP IEs will use one of the MLME nested values as this is considered too restrictive, and will require one of the remaining IE types to be assigned. However this should not be for the sole use of KMP. The fragmentation identifier number range (97..127) above that used for fragment count can be used to identify different types of protocol as well as the KMP types currently expected to be enumerated. Such protocols might include any being developed in other groups for example the IG-L2R mesh routing.

The ACK packets sent during fragment chaining will not use the 4e secure ACKs since no keys are available to secure them at the initial KMP exchange. It will be possible to support the recommended practice on non-4e 15.4 device provided that they are running the IETF 6lowpan protocol and IP stack. A 6lowpan dispatch type needs to be allocated to identify packets as KMP transport

Bob showed the draft Recommended Practice document (15-12-0116-04). A short discussion followed on how to insert an informative reference; Karen Randall (Randall Consulting) observed that in IEEE documents all references are normative, and that any informative text should go into an appendix. It may also be useful to look at work done in 802.1X for definitions that can be re-used in the recommended practice.

Bob opened the remainder of the session for discussion and questions; there were several questions on the fragmentation mechanism. It was noted that the maximum fragment size is implied by the PHY that is being used between two devices. The Recommended Practice needs to describe 2 state machines; one for fragmentation control and one for the actual protocol control mechanism. For the latter state machine, a list of trigger events needs to be compiled and checked on how they are generated. The KMP-specific sections of the Recommended Practice document should describe the use-cases that it is intended the KMP addresses and also guidelines on how to populate the security association material in 15.4 and 15.7

*Monday July 16th PM2 session*

The meeting was called to order at 16:07

The goal of the session was to prepare for the joint meeting with the security experts of 802.1 on Thursday the 19th.

Bob showed document 15-12-0024-09 “Key Management support for 15.4 and 15.7”. The reasons that there is a need for the mechanisms described in the document are that there is no traffic selector in either standard and the MPDUs of both MAC layers is too small to carry the payloads required by the different Key Management Protocols.

Karen Randall commented that the approach is fine as we are providing a transport mechanism for Key Management Protocols and not doing anything to the KMPs themselves. Tero Kivinen (AuthenTec) noted that it is important to have many different KMPs represented in the Recommended Practice so that many different use cases can be addressed. He also expressed the view that users will probably not want to support devices containing multiple KMPs although the coordinator in a system may support several. Karen also pointed out that since the group is not creating a KMP there is no compliance issue.

Karen commented that the presentation should contain some historical background for those not on the previous teleconference. Bob began to pull together a presentation to be discussed in the joint meeting and invited comments and input from the group as he put it together. There were numerous inputs on the contents of the slides from the group as Bob wrote them and then all present reviewed and agreed the slides.

Bob invited the group members to download the posted presentation from the document server and to check the content, sending any comments to Bob before the meeting on Thurs AM1.

The meeting went into recess at 17:29 until Thurs AM1.

*Thursday July 19th AM1 session*

The session was held as a joint session between the 802.15.9 Task Group and security experts from 802.1.

The meeting began at 08:11.

Bob Moskowitz (Verizon) Chair of 802.15.9 asked those for 802.15 to mark their attendance. He thanked the members of 802.1 present for attending the meeting.

Mick Seaman, Chair of 802.1 Security Task Group displayed the patent policy slides 1-4, and made a call for people to notify either chair of any essential patents they may be aware of. Mick asked if there have been any patent notifications so far; Bob replied that there have been none.

Bob Moskowitz showed document 15-12-373-01 “Key Management Support for 15.4 and 15.7”. He noted that TG9 is not working with 15.6, but may work with 15.8. The intention of the TG9 recommended practice is to be KMP agnostic.

Mick asked for clarification of ZigBee; Bob explained how and why ZigBee was set up and the security present in ZigBee PRO, ZigBee-IP, and application profiles. Datagram encryption uses AES-CCM\*, with Key Management being done in an unspecified upper layer; for each standard, Key Management has to be done in each upper layer.

Bob explained the constraints on 15.4 and 15.7 devices and the lack of an LLC layer. Mick asked if there was ever support for longer frames to which Bob answered no.

The addition of Information Elements (IEs) allows other processing paths rather than the simple data service which can be used for other things. Mick asked whether forced acks exist, to which Bob replied that they do and allows fragment chaining to be implemented.

The format and use of the KMP IE was explained, with a limit of 9kbyte for the chaining payload. Mick asked about the scope of the Recommended Practice; it is not introducing any new security into the standards but only a transport method for KMPs, all within the boundaries of the existing security mechanisms. Mick asked if AES-CCM\* is on the NIST approved cipher list. It has been reviewed by NIST but is not on register. In answer to a further question on how security is used in 15.4 and .7 systems, it was stated that it uses proprietary key management but 15.4 security methods. Bob explained that the TG9 group is discussing what the event triggers are for the various operations needing to occur, and also other mechanisms such as when to perform KMP – either pre or post association. Brian Weis (Cisco) asked whether 802.15.9 covered prevention of passing of plaintext until the KMP had been completed. Bob responded that that is one of the topics that will be going into the state machine still to be designed.

Brian suggested that a threat analysis would be useful to justify the decisions that 802.15.9 is taking. He suggested that Prof. John Mitchell of Stanford would be a good party with whom to consult on a threat analysis. The problem of how to handle the issues of group keys and rekeying with sleeping devices will also need to be addressed in the guidelines of the Recommended Practice.

Mick asked how many keys would be present and if the relationships between group keys is defined. Bob replied that it is difficult to find out what people are actually doing. The security mechanisms in 15.4 and 15.7 are designed for use on a single link, but many systems will need to implement a mesh routing layer. If one key is used to secure the entire PAN the use needs to be coordinated over all the nodes particularly how to sync the frame counters in each node. Bob undertook to find out how this is being done in currently implemented system; one thought is that it may be done in the PAN coordinator. A complication is that the security will have to work in a broadcast/multicast environment. Questions on how the counter space can be managed were raised; it was noted that the counter space also includes the long source address. The Recommended Practice can only produce guidelines on uniqueness of addresses. Mick identified a problem where equipment manufactured offshore don’t adopt proper MAC address assignment (i.e., the MAC addresses get stolen) so we need to worry about this as an increasingly common problem.

At the end of the presentation, Mick inquired how we would ensure that all of the good work done on 802.1X and its available EAP methods would be available for all to use under the 802.15.9 framework. He is interested to provide 1x the opportunity to contribute to the Recommended Practice. Bob responded that the group we would be looking for assistance with an 802.1X annex that would define the protocol ID values and rules for operating 802.1X in an 802.15.9 environment. Mick asked how to slot this in noting that there is a need to match the terms used in the two groups. As part of the contributions Bob asked for use cases in order that it is possible to see which KMP is applicable for different environments.

Mick inquired how widely WPANs would be deployed in order to understand if 15.4 or 15.7 would become a method for general network access, as a short-range WLAN replacement. That affects the use cases discussion because of what layers and security would run over them. Bob believes that WPANs will see wider usage including general network access.

Brian Weis noted that since 802.15.9 carries application layer security protocols, it does not provide a complete solution;­ it does not deal with devices in a layer 2 perspective and therefore does not provide controls for which devices may associate with the network at layer 2. Bob agrees that this problem does exist, although this would not explicitly be an issue to be addressed by 802.15.9 which is only transporting a KMP. Brian is trying to understand the scope of 802.15.9’s use cases in order to determine where an 802.1X solution fits into the picture. Bob sees two main communities of use that fit broadly around: 802.1X/PANA and IKEv2/HIP, with possibly the latter being used for extremely constrained devices. Yoshi Ohba (Toshiba) suggested that there is overlap between these communities and cited ZigBee-IP’s use of PANA.

The mechanics of 802.1X contributing to the Recommended Practice were discussed. Bob asked that text is provided that can drop into the document. Mick asked where in the creation of the document 802.15.9 at the moment. Bob replied that the group are not very far along in the process at the moment and need a technical editor. Mick reiterated that 802.1X do not want to get out of sync; Bob thought that the November meeting would most likely be the time that text is needed. The text should be in a Word document and diagrams executed in Visio. These will be passed off to FrameMaker later in the editing process.

15.9 went into recess at 9:24 until Thursday AM2.

## Thursday 19th July AM2 session

The chairman Bob Moskowitz (Verizon) called the meeting to order at 10:40; participants were reminded of the meeting protocol to identify their affiliation when speaking and were reminded to record their attendance.

The IEEE slides on patents and the duty of participants to inform were shown. A call for notification of essential patents was made; there were no responses.

Bob proceeded with a review of the Agenda (15-12-352-01) and set the aim of the meeting to review the closing report (15-12-0415-00) and plan for September session. He reported that he had been socialising security in new efforts for example TG4p Positive Train Control (PTC) and TG8 Peer Aware Communications (PAC), and also IG-LED-ID which will be an addendum to 15.7.

He also talked about what 15.9 is doing for 15.7 and the need for a maintenance request for 15.7 to clarify the use of IEs as the only thing present in a command frame. He also presented to IG-L2R the IE structure from TG9, as a method for conveying routing information. TG8 was concerned about security and showed significant interest in using the results of the efforts in TG9. Bob intends to keep a liaison with this group; their interest was centred around what a device allows or wants to be discovered. He reported that there was participation from a lot of cellular network providers who see the smartphone as a critical component to how PAC will be deployed.

PTC has concerns on timing for security negotiation given the closing speeds between trains and trackside equipment (500km/h), and also on the fact that the equipment will have a line-of-site range of up to 70km to allow for communications with equipment within the safe stopping distance of 7km. The PTC systems will use a closed, licensed network since the application is safety-critical, but this also leads to the need to be protected against malicious intervention.

He also attended a meeting with TG4j Medical Body Area Networks (MBAN). Peter Yee (Akayla) asked if this will affect the work within TG9; Bob replied that it is only a new PHY and has no new requirements for security. TG4n Chinese MBAN is very similar to TG4j but is defining a PHY for the Chinese medical bands.

Management item to be submitted in the September meeting to SC-Man.

The group has a good joint session with 802.1; Bob thanked Karen Randall for helping to set up the meeting.

Logistics for the September meeting was discussed; Bob cannot get to Indian Wells until Wednesday morning; Karen leaves on Thursday. Tero Kivinen is not available for the next 2 meetings. Bob has asked for Wednesday PM2 and Thursday PM1 and PM2 sessions. Peter (co-chair) offered to chair the meeting in the event that Bob is delayed. Karen questioned how much progress is likely to be made before September given the lack of a technical editor. Bob reported that he hoped to know during August if he has secured funding for this post; progress will depend on this. There will probably be no conference call before the September meeting.

As there were a number of new attendees, Bob showed the joint session presentation to allow discussion of the use of IEs with the newcomers.

Mike McInnis (Boeing) asked why the group were not using the multipurpose frame format; Bob replied that it had been considered and rejected but couldn’t recall the reason.

In answer to a question from Bob to the group regarding whether a device always performs an association Phil Beecher (BCC) replied that association is not always present in 15.4; end devices can just do a warm reboot and so wouldn’t need to reassociate.

Bob asked for help from MAC experts in addressing a number of issues; what would need to happen if a device loses its key, and how to initiate the keying trigger. He also asked what controls the security keying, the coordinator or device.

Mike McInnis asked how a bag of sensors would be commissioned into a network, and whether they would all use the same key. Discussion suggested that a device in a group could have a key that all others in the group know, and that only the key owner transmits with that key and all others in the group use it to decrypt the key owner’s messages. An alternative approach would be to use a key manager to which all data is sent, and which then resends the data to the final destination, securing it with a single group key which it owns.

Mike McInnis described the use case for deploying a network in a manufacturing area; typically the requirement is to prepare the devices prior to deployment, which includes provisioning the devices with keys. He described the need for an out-of- band channel to be used for keying. Bob outlined the problem where home automation devices need to be able to identify and join the correct home network, possibly by pressing buttons on the device trying to join and the PAN coordinator. Commissioning in an office building is typically done by a professional installer. Some events need to be considered such as the behaviour of the system when power to all the installed devices is applied at the same time. An industrial environment might need to segment the various spaces into discrete networks using different PAN IDs.

Keys are normally used for securing the link between the two devices; the challenge is how to define a key for a group, or indeed whether this is an appropriate approach. At the link level the security gets recomputed for each hop. Several issues associated with group keys were identified, including distribution of the group key and how to deal with broadcasts. A suggestion was to ignore broadcasts if the packet comes from the wrong coordinator. How often a device moves may cause a problem since this may cause a reassociation and hence require a new key. Association needs to be performed before keying operations.

One of the problems of using a group key for all the devices in a PAN is the case where one device sends many messages and exhausts the key counter and then a rekey is needed, triggered by telling the coordinator (key manager) to rekey everyone in the key group. In order for this to be successful it may be necessary for all devices to be awake, or at least have some sort of buffering which allows the rekey message to be delivered when the sleeping devices wakes up. CCM counter mode includes the MAC address as part of the security process; offshore manufactured devices may reuse/steal MAC addresses so there is a possibility that there will be duplicate addresses (or no address if not provisioned at manufacturing). Transmitting the same packet with the same sequence counter value is a major security risk.

In 802.11 due to its single hop topology where all peer-to-peer messages travel via the access point, the group key is managed by the coordinator which makes security key management easier. However using this arrangement in a 15.4 mesh topology would mean that it would be necessary to send a message from a source device (e.g., light switch) to the PAN coordinator which would resend the message on to the destination device (e.g., lamp); this arrangement may have latency issues. Another suggestion was for each coordinator (routing node) in a 15.4 mesh to act as the key manager for its group of 1-hop neighbours which would overcome some of the latency issues but have the advantage of managing a local group key from a local central point.

Bob asked what else is done in association; Phil replied that parameters such as the PANID and capabilities for example whether the device is sleepy or always on. It was suggested that this can happen after KMP.

The difference between authorisation and authentication was highlighted. Certificates or raw public keys only give identity, not the authorisation for the device to be allowed to do something.

There was a suggestion to include text in the Recommended Practice to describe different side-channel methods (e.g., QR codes, Near-Field Communications) to get identities into the device. Secure device identities are registered on an authentication service to decide which devices are allowed to join a network.

Bob made a call for people to participate in drafting use cases for the document. He requested that all use the mailing list to get more information together for the September meeting in Indian Wells.

The meeting was adjourned by acclamation at 12:17.