IEEE 802.15.9

Key Management Support for IEEE 802.15.4 and 802.15.7

Tero Kivinen

Vancouver, BC

August 3, 2012

Abstract

- To provide for a Key Management Protocol Transport for 802.15.4 and .7
  - KMP agnostic
  - Support: HIP, IKEv2, 802.1X, PANA, ...
- Provide recommended functionality for KMPs
- Use Information Elements where possible

A Little Background

- 802.15.4 does not support different classes of data payloads
  - All is left to the 'upper layer'
  - For example cannot support Zigbee 1.0 and 2.0 within the same PAN
- 802.15.4 MPDU is 127 octets pre 4g
  - And even 4g devices MAY use a small MPDU
- These MAC constraints REQUIRE a unique approach for KMP support

KMP Transport

- Provide an alternative path from general datagrams for KMP transport between devices
  - Use Information Element for traffic selector (4e capable devices)
- Provide fragmentation of large KMP payloads over smaller 802.15 MPDUs
  - Simple chaining of fragments with Forced ACK

15.4 Specifics

- 15.4 MAC and IE formats

Octets: 1/2	0/1	0/2	0/1/2/8	0/2	0/1/2/8	0/1/5/6/10/14	variable		variable	2
Frame Control	Sequence Number	Destination PAN Identifier	Destination Address	Source PAN Identifier	Source Address	Auxiliary Security Header	Information Elements		Frame Payload	FCS
		Addressing fields					Header IEs	Payload IEs		
MHR								MAC Payload		MFR

Figure 42—General MAC frame format

Bits:1	4	11	Variable
Type	ID	Length	Content
1	0 - 15	0 – 2047	—

Figure 55p—Payload IE general form

15.4 Specifics

- Use 15.4e Information Elements
  - Use data payload IEs (not header IEs)
    - Larger payload length
      - Header IEs limited to 127 bytes
  - Need IE type assignment
    - MLME Nested limited to 255 bytes
    - Only 5 values available

Table 4b—Payload IE namespace (ID)

ID Value	Description
0x0	Upper layer payload (SDU passed up/down) (content transparent to the MAC)
0x1-0x8	Un-managed
0x9	MLME (Nested)
0xa-0xe	Reserved
0xf	Termination of IE list

KMP Information Element

- Frame format
  - MAC specific content
    - ID = 0xa
    - Length
  - Control Field – 1 byte
  - KMP fragment

KMP Information Element

Octets: 1		Octets: 1-2046
Bits: 1	7	KMP Fragment
Chaining flag	First packet: Multipurpose ID Other packets: Chain count	
0 = last/only one 1 = yes, chaining	Multipurpose ID: 98-126 98 = KMP Chaining count: 2-96 2 = 2nd fragment 3 = 3rd fragment … 96 = 96th fragment (last possible)	

KMP Transport

- IE for KMP
  - 802.15.4 uses data payload IE with max size of 2047
  - 802.15.7 uses COMMAND frame IE with max payload of 255 per IE

KMP Transport

- Fragmentation support
  - Outbound
    - KMP payload divided to fit MPDU
    - Fragment sent with Forced ACK
    - Resend if no ACK returned
      - ACK may have been lost
      - MAX retries = ?
    - Next fragment on ACK receipt

KMP Transport

- Fragmentation support
  - Inbound
    - Assemble payload from frame received and send ACK if indicated
      - Could be a duplicate fragment
        - » ACK lost
    - Deliver payload to KMP on completion