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

---

**Figure 42—General MAC frame format**

<table>
<thead>
<tr>
<th>Octets: 1/2</th>
<th>0/1</th>
<th>0/2</th>
<th>0/1/2/8</th>
<th>0/2</th>
<th>0/1/2/8</th>
<th>0/1/5/6/10</th>
<th>variable</th>
<th>variable</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame Control</td>
<td>Sequence Number</td>
<td>Destination PAN Identifier</td>
<td>Destination Address</td>
<td>Source PAN Identifier</td>
<td>Source Address</td>
<td>Auxiliary Security Header</td>
<td>Information Elements</td>
<td>Frame Payload</td>
<td>FCS</td>
</tr>
<tr>
<td>Addressing fields</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MHR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC Payload</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MFR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Figure 55p—Payload IE general form**

<table>
<thead>
<tr>
<th>Bits: 1</th>
<th>4</th>
<th>11</th>
<th>Variable Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>ID</td>
<td>Length</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0 - 15</td>
<td>0 - 2047</td>
<td>—</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>ID Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0</td>
<td>Upper layer payload (SDU passed up/down) (content transparent to the MAC)</td>
</tr>
<tr>
<td>0x1-0x8</td>
<td>Un-managed</td>
</tr>
<tr>
<td>0x9</td>
<td>MLME (Nested)</td>
</tr>
<tr>
<td>0xa-0xe</td>
<td>Reserved</td>
</tr>
<tr>
<td>0xf</td>
<td>Termination of IE list</td>
</tr>
</tbody>
</table>
KMP Information Element

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

<table>
<thead>
<tr>
<th>Octets: 1</th>
<th>Octets: 1-2046</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bits: 1</strong></td>
<td>7</td>
</tr>
<tr>
<td><strong>Chaining flag</strong></td>
<td>First packet: Multipurpose ID&lt;br&gt;Other packets: Chain count</td>
</tr>
<tr>
<td>0 = last/only one&lt;br&gt;1 = yes, chaining</td>
<td>Multipurpose ID: 98-126&lt;br&gt;98 = KMP&lt;br&gt;Chaining count: 2-96&lt;br&gt;2 = 2(^{nd}) fragment&lt;br&gt;3 = 3(^{rd}) fragment&lt;br&gt;...&lt;br&gt;96 = 96(^{th}) fragment (last possible)</td>
</tr>
</tbody>
</table>

KMP Fragment
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