draft-gomez-lpwan-fragmentation-header-02

Carles Gomez (UPC/i2cat)
Josep Paradells (UPC/i2cat)
Jon Crowcroft (University of Cambridge)
Motivation (I/II)

• IPv6 MTU requirement (1280 bytes)
  – But some LPWAN technologies lack L2 fragmentation

• 6LoWPAN fragmentation (RFC 4944)
  – IEEE 802.15.4 (maximum frame size of 127 bytes)
    • 4-byte header (1st fragment)
    • 5-byte header (subsequent fragments)

• However, LPWAN technologies:
  – Maximum payload size one order of magnitude less
  – Bit rate several orders of magnitude less
  – Further limited message rate
    • E.g. due to regulatory constraints on the duty cycle
Motivation (II/II)

• RFC 4944 fragmentation header
  – May represent high overhead for LPWAN
• Furthermore, the RFC 4944 offset field is expressed in increments of 8 octets
  – Only supports L2 payload size ≥ 13 bytes
  – However, there are LPWAN technologies with a shorter maximum payload size
Proposed new format

• 6LoWPAN Fragmentation Header for LPWANs (6LoFHL)

• First fragment

• Subsequent fragments
Changes from RFC 4944 and rationale

• datagram_size field only included in the first fragment
  – Reordering is less likely in (star topology) LPWAN than in a mesh network
  – The format still supports reordering…

• datagram_tag field size reduced to 1 byte
  – Ambiguities due to wrapping not expected
    • Low message rate in LPWAN

• datagram_offset increased from 8 bits to 11 bits
  – Allows to express the offset in 1-byte increments
Benefits of 6LoFHL (I/II)

• Simple, byte-exact, short format
  – Supports maximum L2 payloads ≥ 4 bytes

• Overhead (L2 data units)

<table>
<thead>
<tr>
<th>IPv6 datagram size (bytes)</th>
<th>11</th>
<th>40</th>
<th>100</th>
<th>1280</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2 payload (bytes)</td>
<td>4944</td>
<td>6LoFHL</td>
<td>4944</td>
<td>6LoFHL</td>
</tr>
<tr>
<td>10</td>
<td>----</td>
<td>2</td>
<td>----</td>
<td>6</td>
</tr>
<tr>
<td>15</td>
<td>1</td>
<td>1</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>20</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>25</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>30</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>
Benefits of 6LoFHL (II/II)

- Overhead (adaptation layer fragmentation header bytes)

<table>
<thead>
<tr>
<th>L2 payload (bytes)</th>
<th>IPv6 datagram size (bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>11</td>
</tr>
<tr>
<td>10</td>
<td>6</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
</tr>
<tr>
<td>20</td>
<td>0</td>
</tr>
<tr>
<td>25</td>
<td>0</td>
</tr>
<tr>
<td>30</td>
<td>0</td>
</tr>
</tbody>
</table>

Note: The table shows the overhead in bytes for different payload sizes and IPv6 datagram sizes.
IANA considerations

- 6LoFHL allocates 16 Dispatch values:
  - 11001 000 through 11001 111
  - 11010 000 through 11010 111
Security considerations (I/III)

• 6LoWPAN fragmentation attacks and mitigation analyzed in the literature

• Buffer reservation DoS attack
  – Attacker sends a first fragment to a target
    • Reassembly buffer occupied during reassembly timeout
    • Repeat after the timeout
    • Low cost attack
  – Mitigation
    • Allow fragments of multiple packets in reassembly buffer
    • Define buffer slots
    • If buffer overload, discard packets based on sender behavior
Security considerations (II/III)

• Sending spoofed duplicates
  – Malicious node is required to have overhearing capabilities
  – Attacker
    • Overhears fragment
    • Sends spoofed duplicate (e.g. with random payload)
  – Receiver
    • Cannot distinguish legitimate from spoofed
    • Original IPv6 packet considered corrupt and dropped

– Mitigation suggested
  • Establish a binding among the fragments to be sent
  • E.g. with cryptographic hash functionality
  • Receiver can distinguish illegitimate fragments
Security considerations (III/III)

• Implementers should avoid problems due to:
  – Sending overlapped fragments
    • Comprising overlapping parts of the original datagram
  – Announcing a fake datagram size (1st fragment)
For discussion: alternative 1

• We define a 2-bit ‘LPWAN dispatch’
• We reduce the tag size to 3 bits
• Format:
  – First fragment
    \[
    \begin{array}{c}
    0123456789012345 \\
    ++++++++++++++++++++ \\
    |1 0| \text{datagram\_size} | \text{tag} |
    \end{array}
    \]
  – Subsequent fragments
    \[
    \begin{array}{c}
    0123456789012345 \\
    ++++++++++++++++++++ \\
    |1 1| \text{datagram\_offset} | \text{tag} |
    \end{array}
    \]
• 2-byte, simple format (but tag too short?)

LPWAN@IETF96
For discussion: alternative 2

- We define a 2-bit ‘LPWAN dispatch’
- We reduce the tag size to 6 bits
- We assume Sigfox as the lower bound L2 MTU
- Format
  - First fragment
    - Datagram_offset in units of 5 bytes
      - To fit Sigfox downlink MTU
  - Subsequent fragments
    - Datagram_offset in units of 5 bytes
    - Saves 1 byte for subsequent fragments

Too complex?
Thanks!

Questions?

Carles Gomez (UPC/i2cat)
Josep Paradells (UPC/i2cat)
Jon Crowcroft (University of Cambridge)
Back-up slide: RFC 4944
fragmentation header format

• First fragment

```
|1 1 0 0 0|  datagram_size  |  datagram_tag  |
```

• Subsequent fragments

```
|1 1 1 0 0|  datagram_size  |  datagram_tag  |
```

|datagram_offset|

```