draft-gomez-lpwan-fragmentation-header-02

Carles Gomez (UPC/i2cat)

Josep Paradells (UPC/i2cat)

Jon Crowcroft (University of Cambridge)
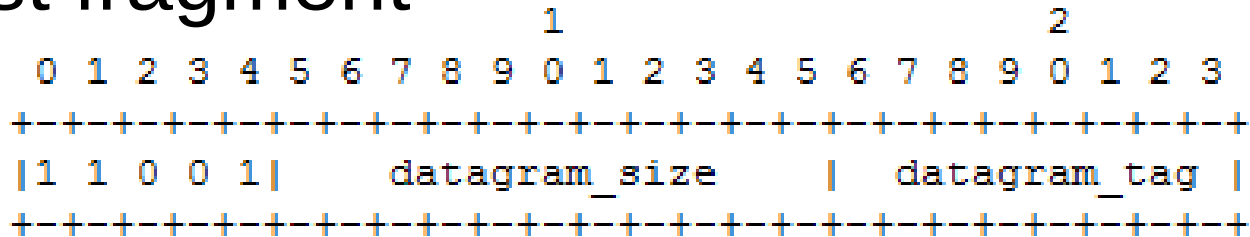
Motivation (I/II)

- 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
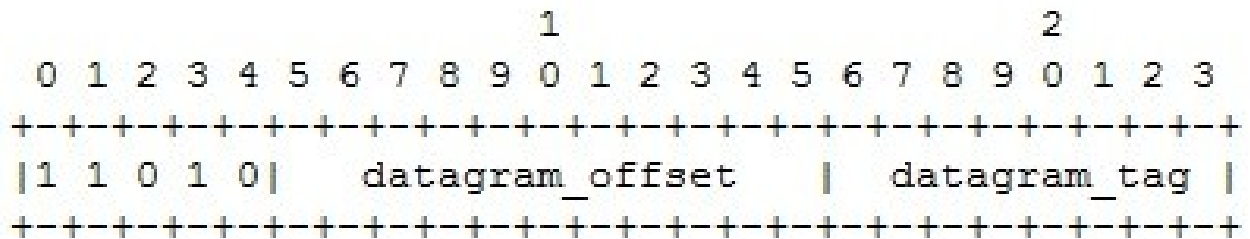
Motivation (II/II)

- 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

```
                                1                   2
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |1 1 0 0 1|     datagram_size     |   datagram_tag |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Subsequent fragments

```
                              1                   2
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |1 1 0 1 0|   datagram_offset    |   datagram_tag |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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)

```
+-----------------------------------------------------------------+
|                    IPv6 datagram size (bytes)                   |
+-----------------------------------------------------------------+
|        11         |        40        |       100       |      1280      |
+-----------------------------------------------------------------+
|L2 payload (bytes)| 4944  |6LoFHL| 4944  |6LoFHL| 4944  |6LoFHL| 4944  |6LoFHL|
+-----------------------------------------------------------------+
|        10        | ----  |  2   | ----  |  6   | ----  |  15  | ----  |  183  |
+-----------------------------------------------------------------+
|        15        |  1    |  1   |  5    |  4   |  13   |  9   |  160  |  107  |
+-----------------------------------------------------------------+
|        20        |  1    |  1   |  4    |  3   |  12   |  6   |  159  |  76   |
+-----------------------------------------------------------------+
|        25        |  1    |  1   |  3    |  2   |  7    |  5   |  80   |  59   |
+-----------------------------------------------------------------+
|        30        |  1    |  1   |  2    |  2   |  5    |  4   |  54   |  48   |
+-----------------------------------------------------------------+
```

Benefits of 6LoFHL (II/II)

- Overhead (adaptation layer fragmentation header bytes)

```
+-------------------------------------------------------------------------+
|                        IPv6 datagram size (bytes)                       |
+-----------------+-----------------+-----------------+-------------------+
|        11       |        40       |       100       |       1280        |
+-------------------+--------+--------+--------+--------+--------+---------+
|L2 payload (bytes) | 4944 |6LoFHL| 4944 |6LoFHL| 4944 |6LoFHL| 4944 |6LoFHL|
+-------------------+------+------+------+------+------+------+------+------+
|        10         | ---- |   6  | ---- |  18  | ---- |  45  | ---- |  768 |
+-------------------+------+------+------+------+------+------+------+------+
|        15         |   0  |   0  |  24  |  12  |  64  |  27  |  799 |  321 |
+-------------------+------+------+------+------+------+------+------+------+
|        20         |   0  |   0  |  19  |   9  |  59  |  18  |  794 |  228 |
+-------------------+------+------+------+------+------+------+------+------+
|        25         |   0  |   0  |  14  |   6  |  34  |  15  |  399 |  177 |
+-------------------+------+------+------+------+------+------+------+------+
|        30         |   0  |   0  |   9  |   6  |  24  |  12  |  269 |  144 |
+-------------------+------+------+------+------+------+------+------+------+
```

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

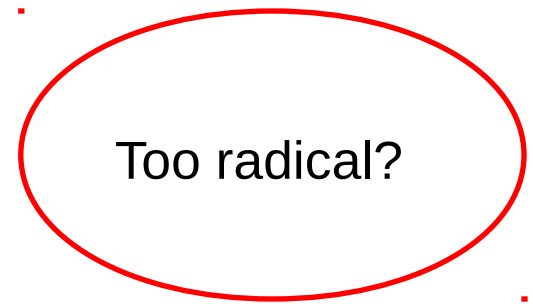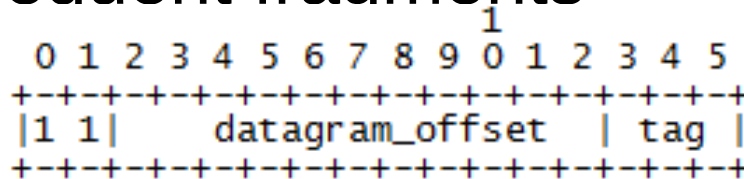# Security considerations (III/III)

- 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'
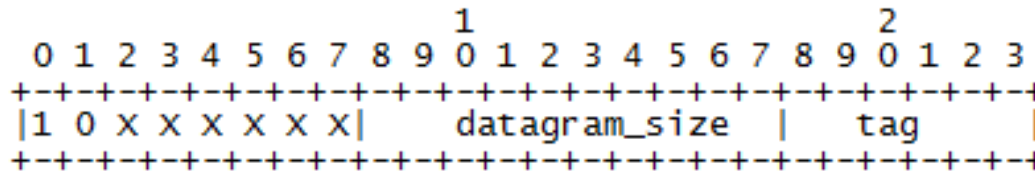- We reduce the tag size to 3 bits
- Format:
  - First fragment

```
              1
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|1 0|     datagram_size     | tag |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

  - Subsequent fragments

```
              1
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|1 1|     datagram_offset   | tag |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
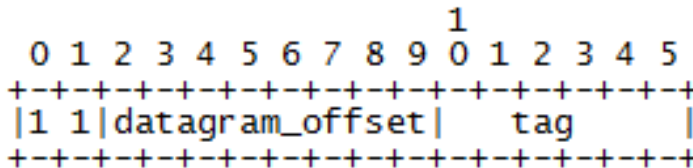
Too radical?
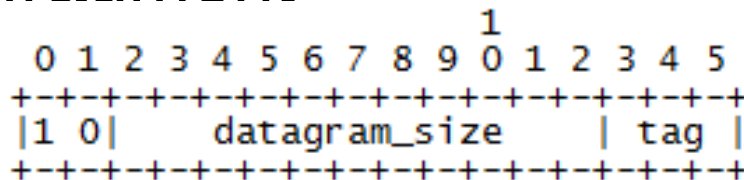
- 2-byte, simple format (but tag too short?)

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

```
                        1                   2
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |1 0 X X X X X X|    datagram_size  |    tag     |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

  - Subsequent fragments
    - Datagram_offset in units of 5 bytes
      - To fit Sigfox downlink MTU

```
                    1
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |1 1|datagram_offset|    tag     |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Too complex?

- Saves 1 byte for subsequent fragments
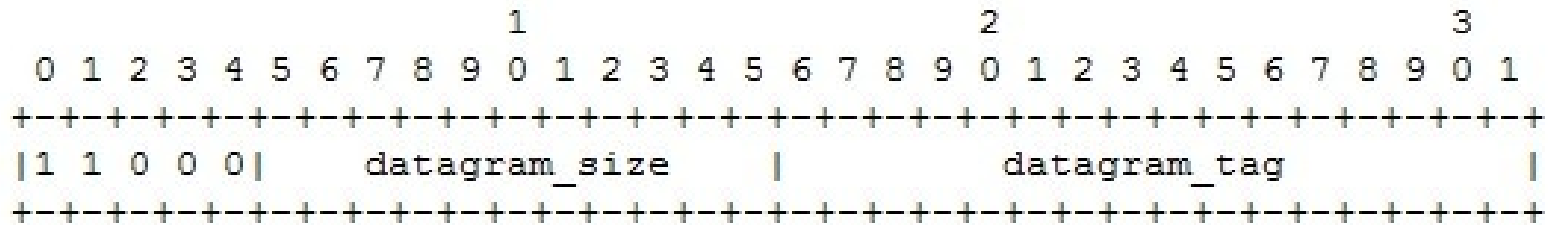
Thanks!

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                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |1 1 0 0 0|    datagram_size    |          datagram_tag         |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Subsequent fragments

```
                      1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |1 1 1 0 0|    datagram_size    |          datagram_tag         |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |datagram_offset|
 +-+-+-+-+-+-+-+-+
```