Transmission of SCHC-compressed packets over IEEE 802.15.4 networks

draft-ietf-6lo-schc-15dot4-01

Carles Gomez
Universitat Politècnica de Catalunya (UPC)
carles.gomez@upc.edu

Ana Minaburo, Flavien Moullec
Acklio
ana@ackl.io

IETF 116 - Yokohama, March 2023
Introduction (I)

- IPv6/UDP/CoAP header size

<table>
<thead>
<tr>
<th></th>
<th>IPv6/UDP (bytes)</th>
<th>CoAP (bytes)</th>
<th>TOTAL (bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No compression</td>
<td>48</td>
<td>4</td>
<td>64</td>
</tr>
<tr>
<td>6Lo(WPAN) - RFC 6282</td>
<td>7</td>
<td>4</td>
<td>11</td>
</tr>
<tr>
<td>SCHC - RFC 8724, 8824</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

Assumptions:
- Best case, global addr.
- CoAP
  a) No header options
  b) Table 6, RFC 8824

- SCHC: static context, a priori knowledge of header field values

- Theoretical battery lifetime improvement over IEEE 802.15.4 by a factor up to >2
  - Actual improvement will be lower, depending on device HW, MAC/adaptation/application layer settings, payload size, network topology, etc.
Introduction (II)

- Maximum battery lifetime improvement factor
  - Short MAC addresses, intra-PAN
  - E.g. a battery-operated sensor that periodically sends a message over IEEE 802.15.4

NOTE: actual improvement will be lower
Status

• WG adoption
  • draft-ietf-6lo-schc-15dot4-00
    – Same content as draft-gomez-6lo-schc-15dot4-05
  • In January 2023

• Version -01
  • Several significant additions
  • A new co-author

C. Gomez
UPC
A. Minaburo
F. Moullec
Acklio
March 2023
# Table of Contents

1. Introduction ........................................... 3
2. Terminology ............................................. 4
   2.1. Requirements language ............................... 4
   2.2. Background on previous specifications ............... 4
3. Architecture ............................................. 4
   3.1. Protocol stack ........................................ 4
3.2. Network topologies ..................................... 6
3.3. Multi-hop communication ............................... 6
   3.3.1. Straightforward Route-Over approach ............. 7
   3.3.2. Tunneled, RPL-based Route-Over approach ....... 7
   3.3.3. Pointer-based Route-over approach ............... 8
   3.3.4. Mesh-Under approach ............................. 9
3.4. Summary ............................................... 9
4. Frame Format ............................................. 9
   4.1. Single-hop or straightforward Route-Over frame format 10
   4.1.1. SCHC Dispatch ..................................... 10
   4.1.2. SCHC Header ...................................... 10
   4.1.3. Padding ........................................... 11
   4.2. Tunneled, RPL-based Route-Over frame format ....... 11
   4.3. Pointer-based, Route-Over frame format ............. 12
   4.4. Mesh-Under frame format ............................ 14
5. Enabling the transition protocol stack ..................... 15
6. SCHC compression for IPv6, UDP, and CoAP headers ....... 16
   6.1. SCHC compression for IPv6 and UDP headers ........ 16
   6.1.1. Compression of IPv6 addresses .................. 16
   6.1.2. UDP checksum field .............................. 17
   6.2. SCHC compression for CoAP headers ................ 17
7. Neighbor Discovery ..................................... 17
8. Fragmentation and reassembly ............................. 18
9. IANA Considerations .................................... 18
10. Security Considerations ................................ 18
11. Acknowledgments ..................................... 18
12. References ............................................. 19
   12.1. Normative References .............................. 19
   12.2. Informative References ........................... 21
Appendix A. Header compression examples .................... 21
Authors' Addresses ....................................... 21
3.1. Protocol stack

- Transition protocol stack
  - Intended to ease a transition from existing 6LoWPAN implementations to introduce support for SCHC
    - SCHC HC for UDP/CoAP, 6LoWPAN HC for IPv6
3.3. Multihop communication

3.3.1. Straightforward Route-Over approach
   - All nodes MUST store all the Rules in use in the network
   - Suitable for small, stable networks, and/or without memory issues

3.3.2. Tunneled, RPL-based Route-Over approach
   - An endpoint MUST store the Rules for the communications it is involved in (as an endpoint)
   - RPL non-storing mode, IPv6-in-IPv6 tunnels, and RFC 8138

3.3.3. Pointer-based Route-Over approach
   - As in 3.3.2, intermediate nodes do not have to store the Rules
   - Does not require 3.3.2 artifacts:
     * RPL non-storing mode, IPv6-in-IPv6 tunnels, and RFC 8138

3.3.4. Mesh-Under approach
   - An endpoint MUST store the Rules for the communications it is involved in
3.3.2. Tunneled, RPL-based R.O. (I)

- RPL non-storing mode
- Overview:
  - Packets sent by a 6LN are tunneled Upward to the root
  - If the final destination is another 6LN, packets are tunneled Downward from the root
  - RFC 8138 to compress routing artifacts
- RFC 9008:
  - Downward traffic:
    - IPv6-in-IPv6 tunnel (except when the root is the packet source)
    - Tunnel terminates at the 6LN (if it is a RAL) or last 6LR (if 6LN is a RUL)
  - Upward traffic:
    - IPv6-in-IPv6 by the 6LR, if 6LN is a RUL (no tunnel if destin. is the root)
    - IPv6-in-IPv6 (“may”) from the 6LN, if the 6LN is a RAL
3.3.2. Tunneled, RPL-based R.O. (II)

• Upward traffic:
  – When a 6LN transmits a SCHC-compressed IPv6 packet, it MUST be tunneled by means of IPv6-in-IPv6 up to the root, regardless of the final destination
    – If the 6LN is a RUL:
      » IPv6-in-IPv6 encapsulation performed by the first 6LR
      » The first 6LR SHOULD be provided with SCHC Rules for the packets sent by that 6LN

• Downward traffic:
  – If the 6LN is a RUL:
    » The last 6LR SHOULD be provided with SCHC Rules for the packets sent to that 6LN
3.3.3. Pointer-based Route-Over

- An alternative to the tunneled, RPL-based approach for Route-Over

- Overview:
  - A SCHC Pointer is added after the SCHC Dispatch
  - The SCHC Pointer indicates the location and length of the destination address residue in the SCHC header

- Assumption:
  - The destination is within the same IEEE 802.15.4 network
    - IPv6 destination prefix is the same as the prefix used subnet-wide

- Features:
  - Compatible with RPL storing mode or other routing protocols
  - Intermediate nodes do not need to store the Rules for all communicating endpoints
### 3.4. Summary

<table>
<thead>
<tr>
<th>One hop</th>
<th>Multihop</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mesh-under</strong></td>
<td><strong>Route-Over</strong></td>
</tr>
<tr>
<td>RPL-based, non-storing</td>
<td>RPL (or other routing) storing</td>
</tr>
<tr>
<td>Up</td>
<td>Down</td>
</tr>
<tr>
<td>SCHC Disp</td>
<td>SCHC Dispatch</td>
</tr>
<tr>
<td>Mesh Hdrs, IP-in-IP, 6LoRH</td>
<td>6LoRH, SCHC Dispatch</td>
</tr>
<tr>
<td>see 4.1</td>
<td>see 4.4</td>
</tr>
<tr>
<td>SCHC Disp</td>
<td>SCHC Dsptch</td>
</tr>
<tr>
<td>see 4.2</td>
<td>see 4.3</td>
</tr>
<tr>
<td>see 4.2</td>
<td>see 4.3</td>
</tr>
</tbody>
</table>
4. Frame formats (I)

• 4.2. Tunneled, RPL-based Route-Over:
  • Downward, when the source is the RPL root

  ![IEEE 802.15.4 frame payload diagram]

  • This case is an exception:
    – No tunnel (IPv6-in-IPv6) encapsulation is needed
4. Frame formats (II)

4.3. Pointer-based, Route-Over frame format:

```
<------------------------ IEEE 802.15.4 frame payload ------------------------>

<------ SCHC Packet ------>
```

```
+--------------------------------+----------------------------------+
| SCHC Dispatch | SCHC Pointer | SCHC Header | Payload | Padding |
+--------------------------------+----------------------------------+

V <=>
```

```
+---------------------+
| compr. resid. addr. |
+---------------------+
```

- **SCHC Pointer:**
  - Starting position of IPv6 destination address residue
  - Length of IPv6 dest. address residue
  - The next fields are present or not

TO-DO: consider a second SCHC Dispatch for SCHC Pointer
4. Frame formats (III)

- 4.4. Mesh-Under frame formats
  - Same as in RFC 4944, but with SCHC Dispatch
  - No fragmentation:

  ![Diagram 1](image1)

  ![Diagram 2](image2)

- Fragmentation:
4. Frame formats (IV)

4.4. Mesh-Under frame formats

- No fragmentation, broadcast:

```
--------------------------------- IEEE 802.15.4 frame payload ------------------
```

```
+-------------------+-------------------+
| M Typ | M Hdr | B Dsp | B Hdr | SCHC Dsp | SCHC Hdr | Payload | Pad |
+-------------------+-------------------+
```

- As in RFC 4944, when more than one header needed, headers appear in the following order:
  - Mesh Addressing Header, Broadcast Header, Fragmentation Header
5. Enabling the transition protocol stack

- Exploiting INTAREA WG on-going work to define an Internet Protocol Number for SCHC
  - draft-ietf-intarea-s chc-ip-protocol-number

- RFC 6282 is used to compress the IPv6 header
  - NH=0
  - Next Header = SCHC (8 bits, uncompressed)
6.1.2. UDP checksum field

• RFC 8724:
  • “a SCHC compressor MAY elide the UDP checksum when another layer guarantees at least equal integrity protection for the UDP payload and the pseudo-header”

• IEEE 802.15.4 carries a 16-bit FCS computed by using ITU-T 16-bit CRC
  • Same size as the UDP checksum
  • Greater error detection capabilities than UDP checksum
  • IEEE 802.15.4 CRC checked at each hop

• The UDP checksum MUST be elided when using SCHC to compress UDP headers
7. Neighbor Discovery

• Several Neighbor Discovery optimizations developed for 6LoWPAN or 6lo
  • E.g., RFC 6775, RFC 8505

• SCHC can also be used to compress 6LoWPAN Neighbor Discovery messages
  • As of the writing, SCHC compression of ICMPv6 or ICMPv6-based protocols has not been specified
    – Currently, only the IPv6 header can be compressed
  • Future specifications may define how ICMPv6 and 6LoWPAN ND messages can be compressed by means of SCHC
  • New SCHC WG new charter:
    – Includes “ICMPv6-based protocols” over SCHC
10. Security considerations

• To compress CoAP headers with SCHC:
  – “As in RFC 8824, the use of a cryptographic integrity-protection mechanism to protect the SCHC headers is REQUIRED”

• Question: perhaps, could a “SHOULD” be considered here?
  – Motivation for using SCHC is performance
  – MUST/REQUIRED for LPWAN networks, where link-layer security is being used, but what if there is a network without link-layer security (as allowed in IEEE 802.15.4)?
Comments/Questions?

draft-ietf-6lo-schc-15dot4-01

Carles Gomez
Universitat Politècnica de Catalunya (UPC)
carles.gomez@upc.edu

Ana Minaburo
Acklio
ana@ackl.io

IETF 116 – Yokohama, March 2023