

lpwan Working Group  
Internet-Draft  
Intended status: Informational  
Expires: September 12, 2019

JC. Zuniga  
SIGFOX  
C. Gomez  
Universitat Politecnica de Catalunya  
L. Toutain  
IMT-Atlantique  
March 11, 2019

SCHC over Sigfox LPWAN  
draft-zuniga-lpwan-schc-over-sigfox-06

Abstract

The Static Context Header Compression (SCHC) specification describes a header compression scheme and a fragmentation functionality for Low Power Wide Area Network (LPWAN) technologies. SCHC offers a great level of flexibility that can be tailored for different LPWAN technologies.

The present document provides the optimal parameters and modes of operation when SCHC is implemented over a Sigfox LPWAN.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 12, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Terminology . . . . .	3
3. Static Context Header Compression . . . . .	3
4. SCHC over Sigfox . . . . .	4
4.1. SCHC Rules . . . . .	4
4.2. Packet processing . . . . .	4
5. Fragmentation . . . . .	4
5.1. Fragmentation headers . . . . .	5
5.2. Uplink fragment transmissions . . . . .	5
5.2.1. Uplink No-ACK mode . . . . .	5
5.2.2. Uplink ACK-Always mode . . . . .	6
5.2.3. Uplink ACK-on-Error mode . . . . .	6
5.3. Downlink fragment transmissions . . . . .	6
6. Padding . . . . .	7
7. Security considerations . . . . .	8
8. Acknowledgements . . . . .	8
9. Informative References . . . . .	8
Authors' Addresses . . . . .	9

## 1. Introduction

The Static Context Header Compression (SCHC) specification [I-D.ietf-lpwan-ipv6-static-context-hc] defines a header compression scheme and a fragmentation functionality. Both can be used on top of all the LPWAN systems defined in [RFC8376]. These LPWAN systems have similar characteristics such as star-oriented topologies, network architecture, connected devices with built-in applications, etc.

SCHC offers a great level of flexibility to accommodate all these LPWAN systems. Even though there are a great number of similarities between LPWAN technologies, some differences exist with respect to the transmission characteristics, payload sizes, etc. Hence, there are optimal parameters and modes of operation that can be used when SCHC is used on top of a specific LPWAN.

This document describes the recommended parameters and modes of operation to be used when SCHC is implemented over a Sigfox LPWAN.

## 2. Terminology

It is assumed that the reader is familiar with the terms and mechanisms defined in [RFC8376] and in [I-D.ietf-lpwan-ipv6-static-context-hc].

## 3. Static Context Header Compression

The Static Context Header Compression (SCHC) described in [I-D.ietf-lpwan-ipv6-static-context-hc] takes advantage of the predictability of data flows existing in LPWAN networks to avoid context synchronization. Nonetheless, these contexts must be stored and configured on both ends. This can be done either by using a provisioning protocol, by out of band means, or by pre-provisioning them (for instance at manufacturing time). The way the contexts are configured and stored on both ends is out of the scope of this document.

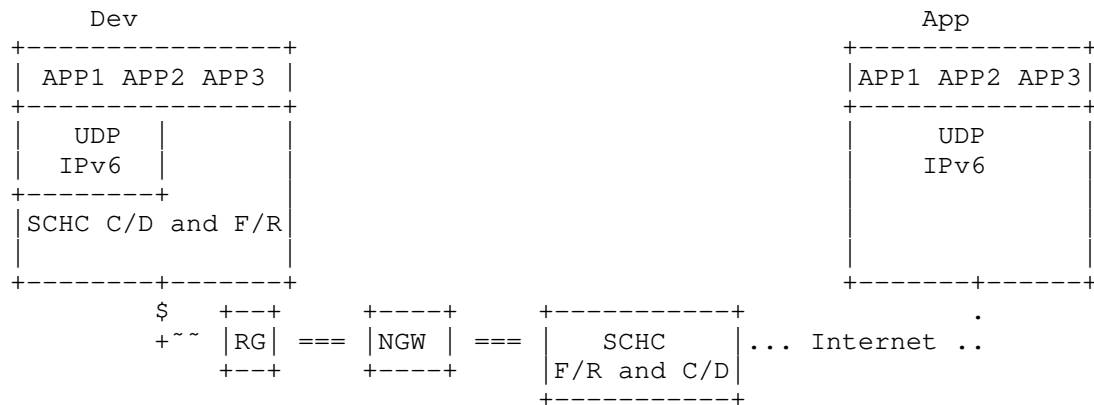


Figure 1: Architecture

Figure 1 represents the architecture for compression/decompression and fragmentation/reassembly, which is based on [RFC8376] terminology, where the Radio Gateway is a Sigfox Base Station and the Network Gateway is the Sigfox Cloud.

The Device is sending applications flows that are compressed and/or fragmented by a Static Context Header Compression Compressor/Decompressor (SCHC C/D) to reduce headers size and/or fragment the packet. The resulting information is sent over a layer two (L2) frame to a LPWAN Radio Gateway (RG) which forwards the frame to a Network Gateway (NGW).

#### 4. SCHC over Sigfox

In the case of the global Sigfox network, RGs (or base stations) are distributed over the multiple countries where the Sigfox LPWAN service is provided. On the other hand, the NGW (or Cloud-based Core network) is a single entity that connects to all Sigfox base stations in the world.

Uplink Sigfox transmissions occur in repetitions over different times and frequencies. Besides these time and frequency diversities, the Sigfox network also provides space diversity, as potentially an uplink message will be received by several base stations. Since all messages are self-contained and base stations forward them all back to the same Core network (NGW), multiple input copies can be combined at the NGW and hence provide for extra reliability based on the triple diversity (i.e. time, space and frequency). A detailed description of the Sigfox Radio Protocol can be found in [sigfox-spec].

The NGW communicates with the Network SCHC C/D for compression/decompression and/or for fragmentation/reassembly. The Network SCHC C/D shares the same set of rules as the Dev SCHC C/D. The Network SCHC C/D can be collocated with the NGW or it could be in another place, as long as a tunnel is established between the NGW and the SCHC C/D. After decompression and/or reassembly, the packet can be forwarded over the Internet to one (or several) LPWAN Application Server(s) (App).

The SCHC C/D process is bidirectional, so the same principles can be applied on both uplink and downlink.

##### 4.1. SCHC Rules

The RuleID MUST be sent at the beginning of the SCHC header. The total number of rules to be used affects directly the Rule ID field size, and therefore the total size of the fragmentation header. For this reason, it is recommended to keep the number of rules that are defined for a specific device to the minimum possible.

##### 4.2. Packet processing

TBD

#### 5. Fragmentation

The SCHC specification [I-D.ietf-lpwan-ipv6-static-context-hc] defines a generic fragmentation functionality that allows sending data packets larger than the maximum size of a Sigfox data frame.

The functionality also defines a mechanism to send reliably multiple frames, by allowing to resend selectively any lost frames.

The SCHC fragmentation supports several modes of operation. These modes have different advantages and disadvantages depending on the specifics of the underlying LPWAN technology and Use Case. This section describes how the SCHC fragmentation functionality should optimally be implemented when used over a Sigfox LPWAN for the most typical use case applications.

#### 5.1. Fragmentation headers

A list of fragmentation header fields, their sizes as well as suggested modes for SCHC fragmentation over Sigfox are provided in this section.

#### 5.2. Uplink fragment transmissions

Uplink transmissions are completely asynchronous and can take place in any random frequency of the allowed uplink bandwidth allocation. Hence, devices can go to deep sleep mode, and then wake up and transmit whenever there is a need to send any information to the network. In that way, there is no need to perform any network attachment, synchronization, or other procedure before transmitting a data packet. All data packets are self contained with all the required information for the network to process them accordingly.

Since uplink transmissions occur asynchronously, an SCHC fragment can be transmitted at any given time by the Dev.

##### 5.2.1. Uplink No-ACK mode

No-ACK is RECOMMENDED to be used for transmitting short, non-critical packets that require fragmentation.

The recommended Fragmentation Header size is 8 bits, and it is composed as follows:

The recommended Rule ID size is: 2 bits

The recommended DTag size (T) is: 2 bits

Fragment Compressed Number (FCN) size (N): 4 bits

As per [I-D.ietf-lpwan-ipv6-static-context-hc], in the No-ACK mode the W (window) field is not present.

When fragmentation is used to transport IP frames, the Message Integrity Check (MIC) size, M: TBD bits

The algorithm for computing the MIC field MUST be TBD.

#### 5.2.2. Uplink ACK-Always mode

TBD

#### 5.2.3. Uplink ACK-on-Error mode

ACK-on-Error is RECOMMENDED for larger packets that need to be sent reliably, since it leads to a reduced number of ACKs in the lower capacity downlink channel.

In the most generic case, the Fragmentation Header size is 8 bits and it is composed as follows:

The recommended Rule ID size is: 2 bits.

The recommended DTag size (T) is: 1 bit.

The recommended Window (W) size is: 2 bits.

Fragment Compressed Number (FCN) size (N): 3 bits.

For the ACK-on-Error fragmentation mode(s), a single window size is RECOMMENDED.

The value of MAX\_ACK\_REQUESTS SHOULD be 2, and the value of MAX\_WIND\_FCN SHOULD be 6 (or 0b110, which allows a maximum window size of 7 fragments).

When fragmentation is used to transport IP frames, the Message Integrity Check (MIC) size, M: TBD bits

The algorithm for computing the MIC field MUST be TBD.

#### 5.3. Downlink fragment transmissions

In some LPWAN technologies, as part of energy-saving techniques, downlink transmission is only possible immediately after an uplink transmission. This allows the device to go in a very deep sleep mode and preserve battery, without the need to listen to any information from the network. This is the case for Sigfox-enabled devices, which can only listen to downlink communications after performing an uplink transmission and requesting a downlink.

When there are fragments to be transmitted in the downlink, an uplink message is required to trigger the downlink communication. In order to avoid potentially high delay for fragmented datagram transmission in the downlink, the fragment receiver MAY perform an uplink transmission as soon as possible after reception of a downlink fragment that is not the last one. Such uplink transmission MAY be triggered by sending a SCHC message, such as a SCHC ACK. However, other data messages can equally be used to trigger DL communications.

For reliable downlink fragment transmission, the ACK-Always mode is RECOMMENDED.

The recommended Fragmentation Header size is: 8 bits

The recommended Rule ID size is: 2 bits.

The recommended DTag size (T) is: 2 bits.

Fragment Compressed Number (FCN) size (N): 3 bits.

As per [I-D.ietf-lpwan-ipv6-static-context-hc], in the ACK-Always mode a Window (W) 1-bit field must be present.

For the ACK-Always fragmentation mode(s), a single window size is RECOMMENDED.

The value of MAX\_ACK\_REQUESTS SHOULD be 2, and the value of MAX\_WIND\_FCN SHOULD be 6 (or 0b110, which allows a maximum window size of 7 fragments).

When fragmentation is used to transport IP frames, the Message Integrity Check (MIC) size, M: TBD bits

The algorithm for computing the MIC field MUST be TBD.

Sigfox downlink frames have a fixed length of 8 bytes, which means that default SCHC algorithm for padding cannot be used. Therefore, the 3 last bits of the fragmentation header are used to indicate in bytes the size of the padding. A size of 000 means that the full remaining frame is used to carry payload, a value of 001 indicates that the last byte contains padding, and so on.

## 6. Padding

The Sigfox payload fields have different characteristics in uplink and downlink.

Uplink frames can contain a payload size from 0 to 96 bits, that is 0 to 12 bytes. The radio protocol allows sending zero bits or one single bit of information for binary applications (e.g. status), or an integer number of bytes. Therefore, for 2 or more bits of payload it is required to add padding to the next integer number of bytes. The reason for this flexibility is to optimize transmission time and hence save battery consumption at the device.

Downlink frames on the other hand have a fixed length. The payload length must be 64 bits (i.e. 8 bytes). Hence, if less information bits are to be transmitted, padding would be necessary and it should be performed as described in the previous section.

## 7. Security considerations

The radio protocol authenticates and ensures the integrity of each message. This is achieved by using a unique device ID and an AES-128 based message authentication code, ensuring that the message has been generated and sent by the device with the ID claimed in the message.

Application data can be encrypted at the application level or not, depending on the criticality of the use case. This flexibility allows providing a balance between cost and effort vs. risk. AES-128 in counter mode is used for encryption. Cryptographic keys are independent for each device. These keys are associated with the device ID and separate integrity and confidentiality keys are pre-provisioned. A confidentiality key is only provisioned if confidentiality is to be used.

The radio protocol has protections against reply attacks, and the cloud-based core network provides firewalling protection against undesired incoming communications.

## 8. Acknowledgements

Carles Gomez has been funded in part by the ERDF and the Spanish Government through project TEC2016-79988-P.

## 9. Informative References

[I-D.ietf-lpwan-ipv6-static-context-hc]

Minaburo, A., Toutain, L., Gomez, C., Barthel, D., and JC. Zuniga, "LPWAN Static Context Header Compression (SCHC) and fragmentation for IPv6 and UDP", draft-ietf-lpwan-ipv6-static-context-hc-17 (work in progress), October 2018.



[RFC8376] Farrell, S., Ed., "Low-Power Wide Area Network (LPWAN) Overview", RFC 8376, DOI 10.17487/RFC8376, May 2018, <<https://www.rfc-editor.org/info/rfc8376>>.

[sigfox-spec]  
Sigfox, "Sigfox Radio Specifications",  
<<https://build.sigfox.com/sigfox-device-radio-specifications>>.

#### Authors' Addresses

Juan Carlos Zuniga  
SIGFOX  
425 rue Jean Rostand  
Labège 31670  
France

Email: [JuanCarlos.Zuniga@sigfox.com](mailto:JuanCarlos.Zuniga@sigfox.com)  
URI: <http://www.sigfox.com/>

Carles Gomez  
Universitat Politecnica de Catalunya  
C/Esteve Terradas, 7  
08860 Castelldefels  
Spain

Email: [carlesgo@entel.upc.edu](mailto:carlesgo@entel.upc.edu)

Laurent Toutain  
IMT-Atlantique  
2 rue de la Chataigneraie  
CS 17607  
35576 Cesson-Sevigne Cedex  
France

Email: [Laurent.Toutain@imt-atlantique.fr](mailto:Laurent.Toutain@imt-atlantique.fr)