JC. Zuniga
SIGFOX
C. Gomez
Universitat Politecnica de Catalunya
L. Toutain
IMT-Atlantique
March 19, 2018

SCHC over Sigfox LPWAN
draft-zuniga-lpwan-schc-over-sigfox-02

Abstract

The Static Context Header Compression (SCHC) specification describes a header compression scheme and 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

Copyright Notice

Table of Contents

1. Introduction

The Static Context Header Compression (SCHC) specification [I-D.ietf-lpwan-ipv6-static-context-hc] defines a header compression scheme and fragmentation functionality that can be used on top of all the LWPAN systems defined in [I-D.ietf-lpwan-overview]. 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 optimal parameters and modes of operation when SCHC is implemented over a Sigfox LPWAN.

2. Terminology

The reader is assumed to be familiar with the terms and mechanisms defined in [I-D.ietf-lpwan-overview] and in [I-D.ietf-lpwan-ipv6-static-context-hc].

3. Static Context Header Compression

Static Context Header Compression (SCHC) avoids context synchronization because data flows are highly predictable in LPWAN networks. 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 e.g. at manufacturing time. The way the contexts are configured and stored on both ends is out of the scope of this document.

```
     Dev                                                    App
+--------------+                                   +--------------+
|APP1 APP2 APP3|                                   |APP1 APP2 APP3|
|              |                                   |              |
|      UDP     |                                   |      UDP     |
|     IPv6     |                                   |     IPv6     |
|              |                                   |              |
|   SCHC C/D   |                                   |              |
|   (context)  |                                   |              |
+-------+------+                                   +-------+------+
         |   +--+     +----+     +---------+                .
         +~~ |RG| === |NGW | === |SCHC C/D |... Internet ..
             +--+     +----+     |(context)|
                                 +---------+
```

Figure 1: Architecture

Figure 1 represents the architecture for compression/decompression and fragmentation, which is based on [I-D.ietf-lpwan-overview] terminology.

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).

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.

The NGW communicates with the Network SCHC C/D for compression/ decompression (and/or fragmentation/reassembly). The Network SCHC C/ D shares the same set of rules with the Dev SCHC C/D. The Network SCHC C/D can be collocated with the NGW or 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.

3.1. 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 (R). For this reason, it is recommended to keep the number of rules that are defined for a specific device to the minimum possible.

3.2. Packet processing

TBD

4. Fragmentation

The SCHC specification [I-D.ietf-lpwan-ipv6-static-context-hc] supports several modes of operation to fragment packets. These modes have different advantages and disadvantages depending on the specifics of the underlying LPWAN technology. This section describes how the SCHC fragmentation functionality SHOULD optimally be used over a Sigfox LPWAN.

4.1. Fragmentation headers

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

4.2. 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.

Uplink transmissions occur in repetitions over different times and frequencies (e.g. three times over three different 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 Core network (NGW), multiple input copies can be combined at the NGW and hence provide for extra reliability based on the triple diversity.

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

For uplink fragment transmissions, the following mode(s) MUST be supported: TBD.

For the TBD fragmentation mode(s), the default values for MAX_ACK_REQUESTS, MAX_WIND_FCN, Retransmission Timer and Inactivity Timer are TBD.

For the TBD fragmentation mode(s), the number of window sizes supported is TBD.

The recommended Rule ID size is: TBD bits

The recommended Dtag size (T) is: TBD bits

Fragment Compressed Number (FCN) size, N: TBD bits

Message Integrity Check (MIC) size, M: TBD bits

The algorithm for computing the MIC field MUST be TBD.

4.3. 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 devices, which can only listen to downlink communications after performing an uplink transmission.

When there are multiple 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 fragment that is not the last one. Such uplink transmission MAY be triggered by sending a SCHC message, such as an ACK.

For downlink fragment transmission, the following mode(s) MUST be supported: TBD.

For the TBD fragmentation mode, the default value for MAX_ACK_REQUESTS is TBD.

For the TBD fragmentation mode(s), the default values for MAX_ACK_REQUESTS, MAX_WIND_FCN, Retransmission Timer and Inactivity Timer are TBD.

For the TBD fragmentation mode(s), the number of window sizes supported is TBD.

5. Padding

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

Uplink frames can contain a payload from 0 to 96 bits (i.e. 12 bytes). The radio protocol allows sending zero bits or one single bit of information for binary applications (e.g. status). However, 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. Hence, if less information bits are to be transmitted padding would be necessary.

The padding procedure is TBD.

6. 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, to provide 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.

7. Informative References

[I-D.ietf-lpwan-ipv6-static-context-hc]
Minaburo, A., Toutain, L., and C. Gomez, "LPWAN Static Context Header Compression (SCHC) and fragmentation for IPv6 and UDP", draft-ietf-lpwan-ipv6-static-context-hc-07 (work in progress), October 2017.

[I-D.ietf-lpwan-overview]
Farrell, S., "LPWAN Overview", draft-ietf-lpwan-overview-07 (work in progress), October 2017.

Authors' Addresses

Juan Carlos Zuniga
SIGFOX
425 rue Jean Rostand
Labege 31670
France

Email: 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

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

Email: Laurent.Toutain@imt-atlantique.fr