INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

Electrical and Computer Engineering Department – INSA Toulouse

5th year Innovative Smart Systems

Sigfox communication protocol study

Authors :
Victor Le Roch
Valentin Licini
Lorine Pose
Théo Rup

December 16, 2020

Introduction

Sigfox is a long-range, low-consumption cellular network in the LPWAN category. It is present in 72 countries thanks to more than 2000 antennas. To be able to use this network, it is necessary to take out a subscription. On average, subscribing to Sigfox network would cost three euros per year per object. Today, 30 million connected objects depend on this network [1].

I. Physical Layer

I.1. Architecture

The Sigfox network is composed of three main parts: devices, base stations and a core network.

- Devices, such as actuators or sensors, communicate in the neighbourhood of the base stations using wireless connectivity. One device can interact with different base stations, this means that devices can move and are not associated with only one base station.

- Base stations are gateways and are connected to the internet to be able to communicate with the core network.

- The core network is the brain of the network, composed of the service center and the registration authority. The first one manages devices and base stations. External applications interact with it to retrieve data from devices and control them thanks to APIs. The registration authority controls access to the network.

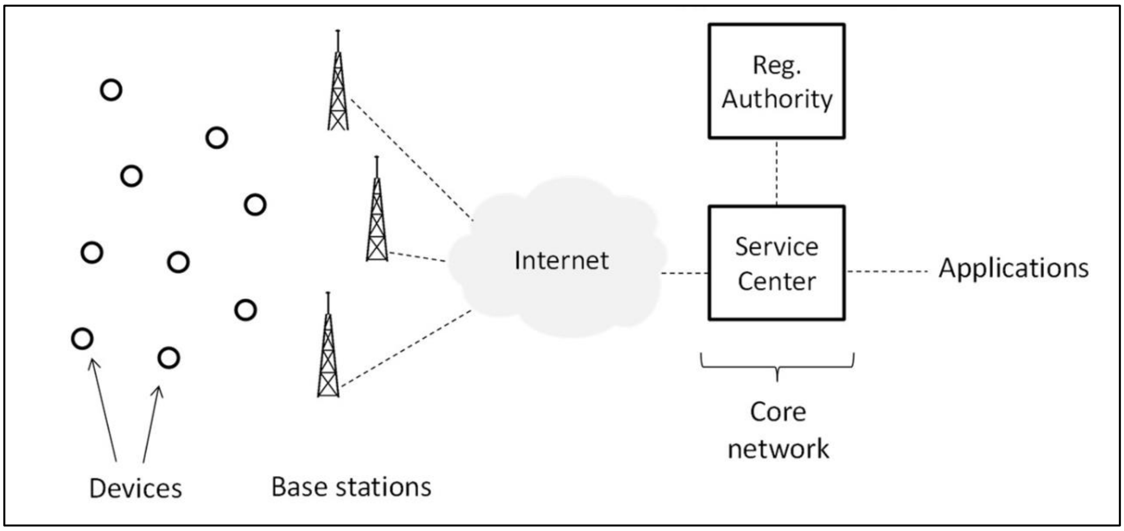

Figure 1 : Sigfox network architecture

I.2. Radio Interface

The Sigfox network uses an unlicensed spectrum to communicate between devices and base stations. This unlicensed spectrum frequencies can vary depending on the area: in Europe, Sigfox uses frequencies from 868.0 to 868.2MHz for uplink transmissions and from 869.4 to 869.65MHz for downlink transmissions. In the USA, frequencies used are from 902 to 928MHz.

By using ultra-narrow bands (UNB), Sigfox achieves a long link range between devices and base stations, while limiting the transmit power and avoiding noise perturbations.

Each message transmitted fills a 100Hz bandwidth in Europe (600Hz in the USA) inside the UNB. The base stations have to monitor the UNB to receive messages.

In order to respect the law on the unlicensed spectrum, communications should not exceed an uplink transmit power of 25mW in Europe and 4W in the USA.

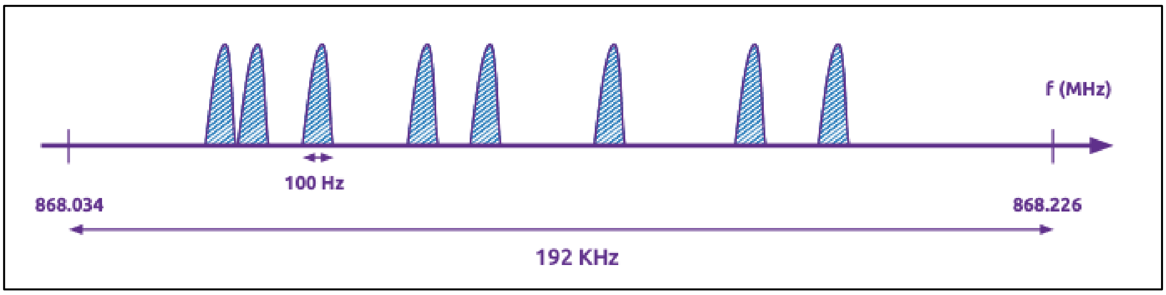

Figure 2 : Sigfox uplink transmission bandwidth

The Sigfox network uses a Differential Binary Phase-Shift Keying (DBPSK). This type of modulation increased uplink range, is bandwidth-efficient, offers a good protection against interferences and reaches a high received power level. In DBPSK the phase of the modulated signal is shifted relative to the previous signal element. The signal phase follows the high or low state of the previous element.

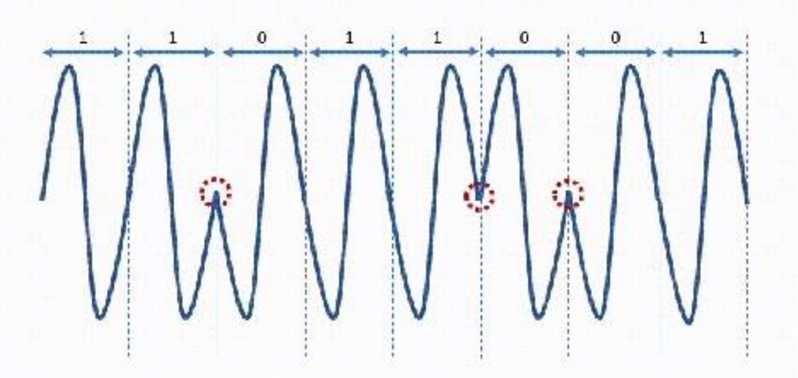

Figure 3 : DBPSK modulation used by Sigfox

It is seen from the above figure that, if the data bit is Low (0), then the phase of the signal is not reversed, but continued as it was. If the data is a High (1), then the phase of the signal is reversed

I.3. Messages

The bitrate of transmissions is 100bit/s in Europe and 600bit/s in the USA for uplink messages and 600bit/s for downlink messages worldwide. These speeds may not seem high, but more speed is not necessary because the unlicensed spectrum has regulations: in Europe. Uplink messages should not have a duty cycle greater than 1% of the bandwidth and downlink messages a duty cycle greater than 10% of the bandwidth. This allows a transmission of 6 messages of 12 byte per hour or 140 uplink messages, not counting the 4 messages that Sigfox keeps for protocol use. In order to respect the 10% duty cycle, Sigfox allows only 4 downlink messages containing data (without counting acknowledgement messages).

II. MAC layer

II.1. Messages format

The messages formats are different for uplink or downlink messages.

The packet structure of the uplink frame is given as follows:

- a preamble of 4 bytes
- a frame synchronization part of 2 bytes
- a device identifier of 4 bytes (each device in a Sigfox network has a unique Sigfox ID)
- a payload of up to 12 bytes
- a Hash code to authenticate the packet in Sigfox network (variable length)
- a Frame Check Sequence (FCS) syndromes of 2 bytes for security and error detection.

The packet structure of the downlink frame:

- a preamble of 4 bytes
- a frame synchronization of 13 bits
- flags of 2 bits
- a FCS of 1 byte
- an authentication frame of 2 bytes
- error codes (variable length)
- a payload (Variable length)

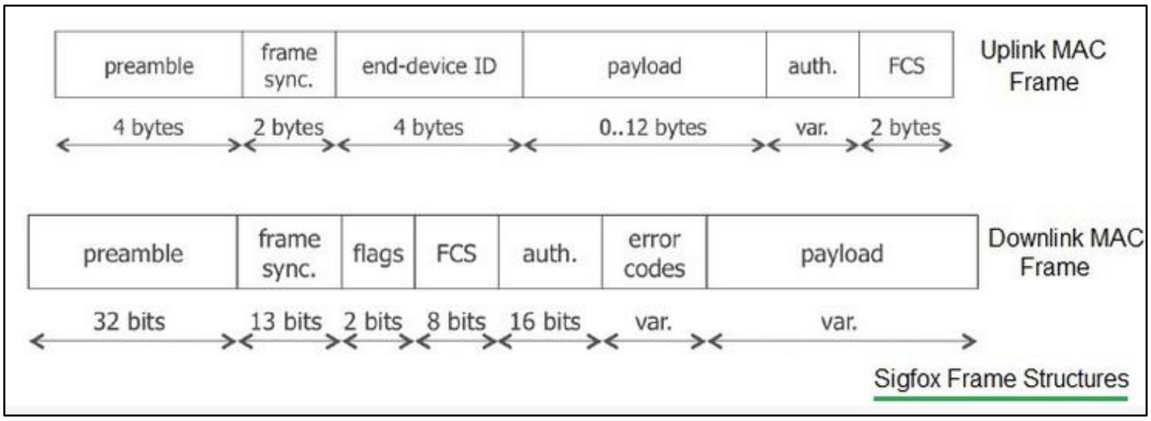

Figure 4 : Sigfox messages format

II.2. Protocol

The communication between devices and base stations is asynchronous and device-initiated. This allows the device to stay in sleep state by default and limit the energy consumption. A message sent by a device may be received by several base station (generally 3).

Communication can be:

- *Unidirectional*: a device sends an uplink frame via a randomly selected frequency channel (in the UNB) and then transmits two exact replicas of the first frame in two other randomly selected channel at different time intervals. This allows a frequency and time diversity to contribute to communication robustness.

- *Bidirectional*: uplink messages are sent as seen previously. After a time, the device initiates a receive window, intended to enable reception of a downlink frame sent by a base station. The downlink message may carry actual application data or is just used as an acknowledgement for the uplink message. After reception, an uplink confirmation is sent by the device. Retransmission due to absence of feedback from the other endpoint of a link do not exist with the Sigfox protocol.

III. Power consumption

III.1. Overview of Sigfox power consumption strategies

Sigfox is a LPWA (Low Power Wide Area) communication protocol. Therefore, one of the main objectives of this technology is to maintain a low power consumption. Its main domain of use is for IoT wireless sensors that need to send values periodically (for example, a temperature sensor which sends a temperature value every 10 minute).

According to Sigfox documentations [2], their chips consume from 10mA to 50mA in transmission in Europe where the output power is 14dBm. As the communication time represents only 1% maximum of the time, the chip is in sleep mode around 99% of the time (consumption of a few nA) to reduce the global consumption. Finally, with Sigfox, no synchronization messages are exchanged between the object and the base station before transmitting the data.

As we have seen before, Sigfox can run either in unidirectional mode or bidirectional mode. However, those two modes, due to their specificities, are not consuming power in a similar manner. Let’s take an example for a message transmitted with a payload of 1 byte and a bit rate of 100 bit/s :

- With the unidirectional mode, we can see that the chip wakes up (1), sends 3 messages (2) spaced by a small delay (3) and then comes back to sleep (4+5) without waiting for any feedback from the receiver.

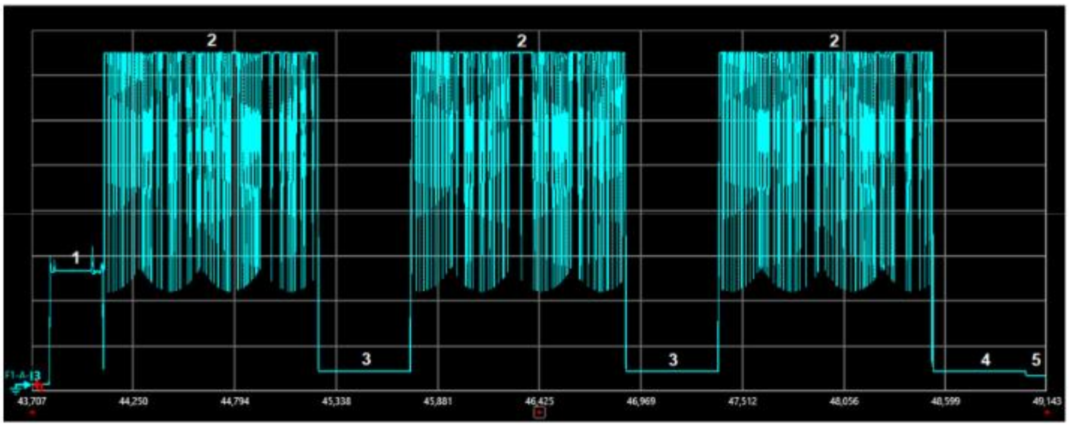

Figure 5 : Current consumption of Sigfox unidirectional mode on a sending period

- With the bidirectional mode, the same steps as above are present, followed by a waiting (4) before a reception interval (5). Once the device receives the downlink message from the receiver, it sends an uplink confirmation (7) and finally come back to sleep (8+9)

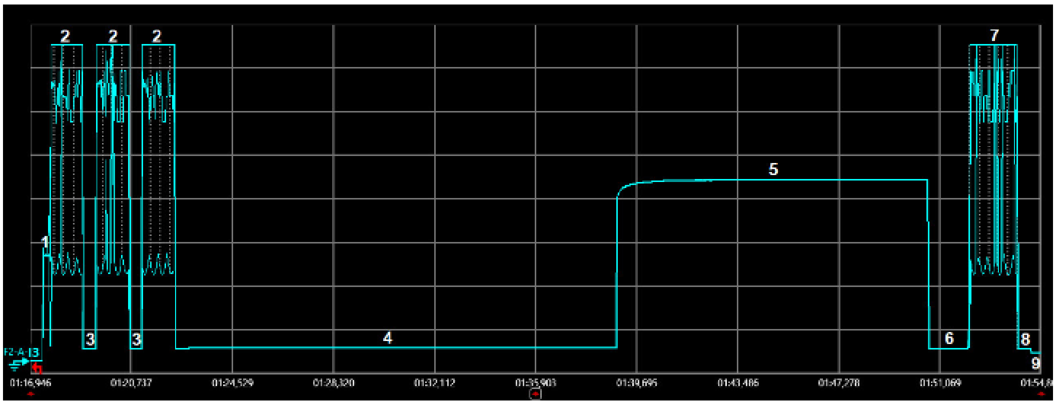

Figure 6 : Current consumption of Sigfox bidirectional mode on a sending period

III.2. Energy per bits

In this part, we are going to highlight the given amount of power used to communicate through Sigfox protocol. At first, it is important to take into account that we are considering that the Frame Loss Rate (FLR) is null and that both unidirectional and bidirectional modes that we described in the previous part are working without encountering transmission problems.

It is important to understand that the energy consumption is strongly linked with several parameters.

- *The communication mode*

For the energy measurements, we take into account the average current I_{avg} consumed between two consecutive periodic transactions initiated by the device T_{period}. We can see that the bidirectional mode consumes more current during the reception interval and or the uplink message while the unidirectional mode is sleeping after sending its message.

- *The transaction period T_{period}*

When T_{period} is small, the difference between the two modes above is high. However, when T_{period} is large, the sleep mode consumption is dominant and the differences are reduced.

- *The message payload size*

If there is more data to transmit, the sending period where the current consumption is at maximum will lasts more time and then more energy will be consumed.

- *The Bit Rate (BR)*

If the bit rate is higher, the data are sent faster and so the sending period is reduced so as the energy consumption.

Finally, the energy cost of data delivering is equal to :

$$E = \frac{I_{avg} * V * T_{period}}{E[l_{delivery}]}$$

with $E[l_{delivery}]$ the expected amount of data delivered by the device during T_{period} and V the battery voltage [3]

The following figures shows the energy/bit variation in function of the transaction period, the payload size, the BR and the communication mode :

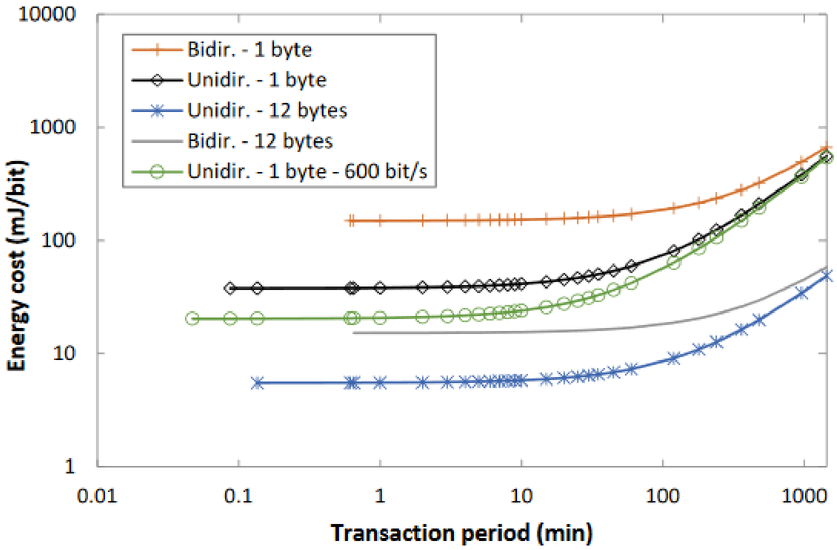

Figure 7 : Energy cost/bit depending of the payload size, the BR, the communication mode and T_{period}

IV. Security

Security is a major concern when it comes to IoT. Every single device and sensor are potentially exposed. In other words, with IoT technologies, the surface of attack explodes and must be addressed holistically.

In order to answer this concern, Sigfox has implemented several measures, some by default and others as options.

IV.1. Built-in firewall

The device cannot receive data at any time. It needs first to send a radio message, which is a request for a downlink message. Only then, the device will listen at a specific frequency during a limited time window, waiting for the response. In other words, the device never sends data to arbitrary entities via internet. Sigfox devices are therefore shielded from the internet by a very strict firewall. Moreover, this design of listening only at specific moments on specific frequencies results on the device being protected from receiving unwanted or unattended messages.

Moreover, the Sigfox Core Network acts as a firewall. If anything suspicious is detected, it can block traffic from selected base stations, or specific applications.

IV.2. Authentication

Between the connected devices and the Sigfox Cloud there is an end-to-end authentication method. Each device possesses a secret and unique authentication key, which is stored in a non-accessible memory associated with a visible and specific ID stored in read only memory. Each message that is sent or received by a device contains a signature key that is computed, based on the authentication key of the sending device. The verification of this signature key will ensure both, the authentication of the sender (the device for an uplink message, or the Sigfox network for a downlink message) and the integrity of the message.

The communication between the base stations and the Sigfox cloud is through a Virtual Private Network (VPN) using SSL encryption. (Secure Sockets Layer (SSL) is a standard security technology for establishing an encrypted link between a server and a client—typically a web server (website) and a browser [6]).

At the chain end, IT (Information Technology) platforms of customers are connected to the Sigfox cloud through HTTPS (Hypertext Transfer Protocol Secure is a secure version of the HTTP protocol that uses the SSL/TLS protocol for encryption and authentication).

IV.3. Anti-replay

The radio frame of the message will also include a sequence number (SN) specific to the message's signature which is verified by the Sigfox Core Network to detect and discard replay attempts. Nonetheless, this SN is only 12-bit which means it only allows for $2^{12} = 4096$ unique messages before overflowing back to 0. And since the authentication key of the device never changes, it makes the replay attacks a real threat. Therefore, it is not recommended to deploy this method for critical applications.

IV.4. Anti-eavesdropping

By default, the data is transmitted without any encryption. Nonetheless, if the data is considered sensitive, Sigfox offers two possibilities. It is possible to use the encryption solution provided directly by the Sigfox protocol, or for the user to implement its own encryption protocol.

IV.5. Anti-sniffing

Every message is sent three times and randomly on three different frequencies to three different base stations within the operation band. It protects the radio frames against sniffing since within the operation band it is not possible to know where the message is headed.

IV.6. Anti-jamming

Sigfox uses the ultra-narrowband technology which means that the receiver is highly selective and can reject noise and interference which may enter the receiver outside its narrow bandwidth. This technology combined with the anti-sniffing protocol above , provides high resistance to jamming of Sigfox transmissions.

References

[1] C. Garcia-Montero, *Sigfox : abonnement, couverture, concurrents…*, Journal du Net, November 2020. Available : https://www.journaldunet.fr/web-tech/dictionnaire-de-l-iot/1195953-sigfox-abonnement-couverture-concurrents-20201009/

[2] Sigfox, *Sigfox Technical Overview*, July 2017

[3] C. Gomez, *A Sigfox Energy Consumption Model*, February 2019

[4] G. Ferré, *An introduction to Sigfox and LoRa PHY and MAC layers*, HAL, April 2018. Available : https://hal.archives-ouvertes.fr/hal-01774080/document

[5] L. Perry, *Essentiel Technical guide of Sigfox protocol : Network architecture, interfaces, protocol stack*, SWA Available : https://www.survivingwithandroid.com/sigfox-protocol-network-architecture-iot-protocol-stack/

[5] Digicert, *What is an SSL certificate ?* Available : https://www.digicert.com/ssl/

[7] Sigfox, *Make things come alive in a secure way*. February 2017. Available : https://www.sigfox.com/sites/default/files/1701-SIGFOX-White_Paper_Security.pdf

[8] F. Laurentiu, *Security Issues in Internet of Things: Vulnerability Analysis of LoRaWAN, Sigfox and NB-IoT*, 2019. Computer Science - 2019 Global IoT Summit (GIoTS)