INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

INNOVATIVE SMART SYSTEMS

26 November 2018

Protocoles pour les Objets Connectés

Study of the Sigfox Network

sigfox

Enseignant : Daniela DRAGOMIRESCU

Alex Noize, Julien Chouvet

Sommaire

This document aims to present the Sigfox network and its characteristics. It covers the following subjects :

1 - What is Sigfox? Usage & Characteristics

What is Sigfox?

Sigfox is a french company founded in 2009 by Christophe Fourtet and Ludovic Le Moan. The headquarters are in Labège, Toulouse suburb, but the company seeks to grow internationally and has already offices in Madrid, San Francisco, Sidney, ... Sigfox is a network provider for Internet of Things (IoT) that wants to provide a global, simple, low-cost and low-power connectivity solution to connect all kinds of IoT devices worldwide. In order to do so, Sigfox is deploying is own dedicated low-bandwidth network that is already present in 45 countries. Their ambition, embodied by their slogan “Make things come alive”, is to provide the protocol and network required to allow an object to share its data from anywhere in the world.

Usage & Characteristics

As it is designed for IoT applications, the Sigfox network allows to transmit only few amount of data. Thus you can send 12 bits of payload for uplink messages and 8 bytes of payload for downlink messages. By sending small messages we can reduce the power consumption and so increase the battery life, which is a big issue for IoT devices. We will study the power consumption more in detail in part 4.

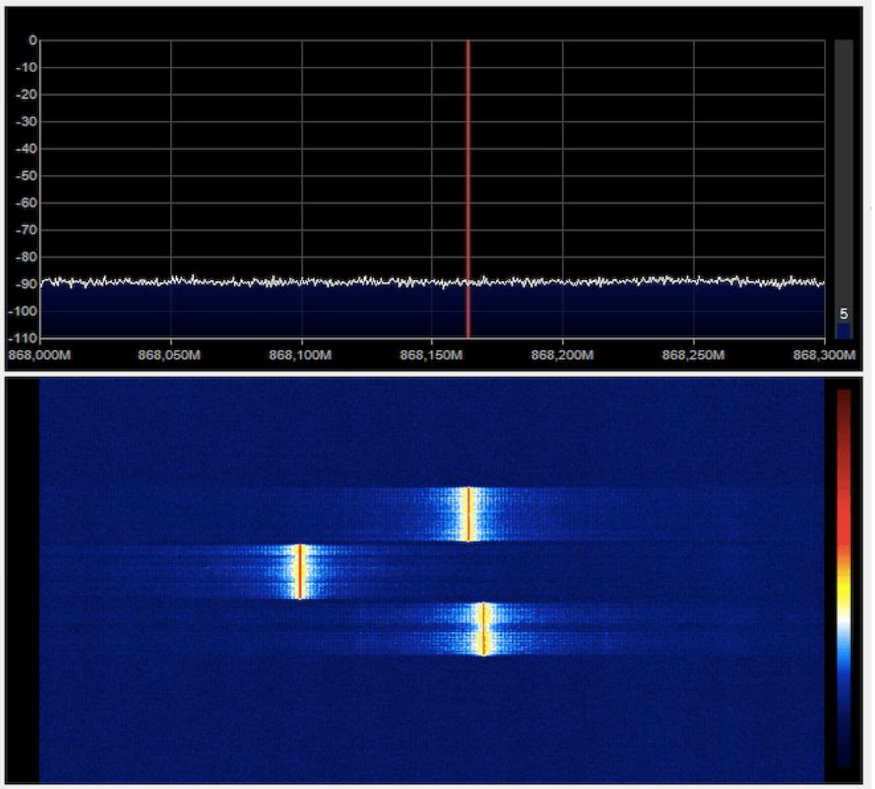
Moreover, there is a limitation on the number of uplink message you can send which is 140 messages per day, which represents 1 message every 10 minutes. For downlink messages, this limitation is set to 6 messages per day.

2 - Network architecture

Sigfox network uses 200kHz of the publicly available and unlicensed frequency band to exchange uplink and downlink messages. It operates from 868 to 869MHz in Europe, Middle East, Africa, India and from 902 to 928MHz in America, Japan and South Korea. Each message is 100Hz wide and the data rate is set to 100bit/s for Europe, Middle East, Africa, India and to 600bit/s for America, Japan and South Korea.

Sigfox uses Ultra Narrow Band (UNB) and Differential Binary Phase Shift Keying (DBPSK) modulations to modulate the signals. These modulation technologies added to a low bit rate result to a high base station receiver sensitivity of -142dBm for a bit rate of 100bit/s and -134dBm for a bit rate of 600bit/s.

To send a message, a device just need to broadcast its message on the operational band. So, the transmission between the device and the receiver is asynchronous and there is no need to establish the connection before transmitting the message. Also, there is no acknowledgement to ensure that the message has been received. So, to be sure that the message arrives well to a base station, the device broadcast its message 3 times on 3 different frequencies and delayed in time, as shown is the following picture.



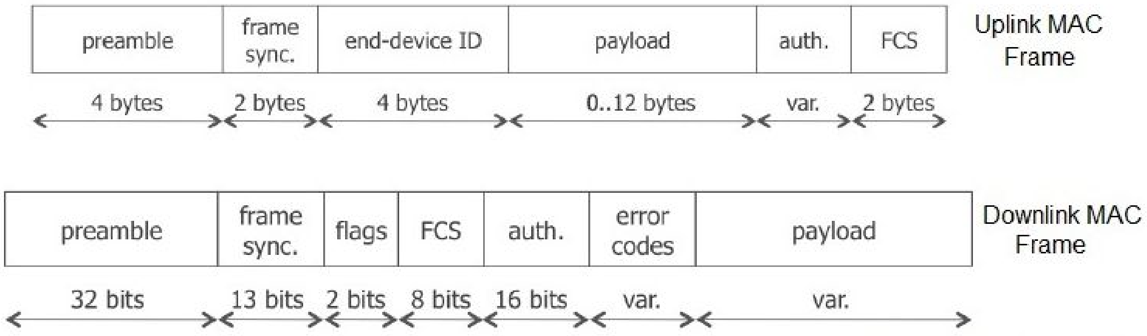
The broadcast message broadcast by the device is received by any base station around it, which is 3 in average according to Sigfox. Then, the message is transmit to the Sigfox cloud by a point to point link, and push to the customer servers.

3 - Sigfox Protocol Stack

Sigfox Protocol Stack of the wireless system consists of four layers, namely Physical Layer, MAC layer, and application layer.

- **Application layer :** build the payload and add a sequence number.
- **MAC layer :** Add fields like authentification of the device, error-detecting code. As the devices are not synchronize to the network, the MAC frame doesn't integrate any signalling to the medium access control so devices can send messages when they want.
- **Physical layer :** apply DBPSK modulation for uplink message and GFSK modulation for downlink message. Il also sets the bit rate and define the operation frequency depending on the region.

The following picture shows the Sigfox MAC frame for both uplink and downlink messages.



preamble	frame sync.	end-device ID	payload	auth.	FCS	Uplink MAC Frame
4 bytes	2 bytes	4 bytes	0..12 bytes	var.	2 bytes	

preamble	frame sync.	flags	FCS	auth.	error codes	payload	Downlink MAC Frame
32 bits	13 bits	2 bits	8 bits	16 bits	var.	var.	

We can notice on the stack describes below, that there is no IP layer. As the messages are broadcasted by the devices throw the air and by radio frequency, there is no need to rout them.

4 - Power Consumption

One of the most important things for IoT network is the power consumption of the data transmission to allow the device to be autonomous. Sigfox was designed to achieve good performances regarding the power consumption. To illustrate this part, we will look at the power consumption of a typical Sigfox transceiver: the ATA8520E from Atmel. What is going to interest us is the power needed for an emission/reception and in idle mode.

The ATA8520E works both for 3V and 5V application, so we will chose 3V to lower the power consumption.

We can see the typical current consumption of the different modes below and deduce the power consumption at 3V for the EU application:

	Tx emission f = 868.3 MHz - 14 dBm	**Rx reception f = 869.5 MHz**	**Idle mode**
Current consumption	32.7 mA	10.4 mA	50 µA
Power (P = U*I)	98.1 mW	31.2 mW	150 µW

We can now calculate the energy consumption of an emission and a reception with the time of an emission which of 2*3s due to the message broadcasted 3 times:

$$C_{emission} = 98.1 * 6 \ = \ 588.6 \, mWs$$
$$C_{reception} = 31.2 * 6 \ = \ 187.2 \, mWs$$

Energy/bit :

We know that every message can carry a payload of 12 bytes so 96 bits. Thus, we can evaluate the power consumption of a bit :

$$C_{bit} = \ 588.6/96 \ = \ 6.13 \, mWs/bit$$

Energy/day :

With Sigfox protocol we can send up to 140 messages/day uplink and receive 6 messages/day downlink and the rest of the time the transceiver will be in idle mode, so we can calculate the power consumption of the transceiver for a day :

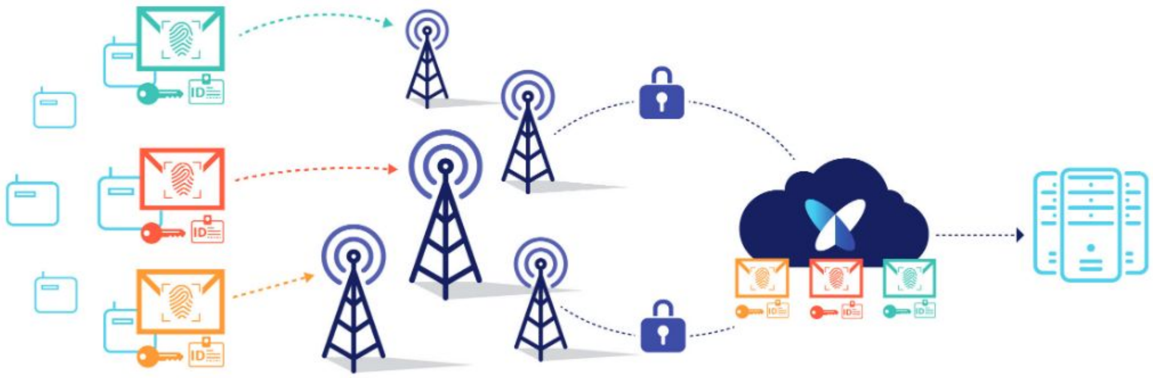
$$C_{day} = 140 * C_{emission} + 6 * C_{reception} + \frac{86400 - 140*6 - 6*6}{86400} * P_{idle} = 23.2 \, mWh$$

This consumption is very low and for instance, an alkaline AA battery, one of the most common battery for portable electronic devices has an energy of around 4 Wh and would be capable of powering this transceiver for more than 170 days.

5 - Security

Security is one of the most important challenge for IoT today. Indeed, even if IoT technology has become affordable and is now a solid opportunity for companies willing to develop new business or reinventing theirs, IoT must be fully secure to gain the thrust of the business community. As a matter of fact, IoT will be used for business-critical processes and thus the entire end-to-end chain has to be secured in order to provide the required quality of service.

However, all the applications won't need the same level of security and in a cost and complexity concern the security level must be adequate with the process. Sigfox can handle different level of security and we will see which security mechanisms can be used :



Built-in firewall : Sigfox Ready devices are IoT objects, therefore, they are not directly connected to the internet and they are not communicating using its protocol. Actually, if a device wants to emit or to receive data they broadcast a message that is conveyed to the Sigfox Core Network which delivers it to the IoT application. Then, the IoT application has a limited time window to respond to the Sigfox Core Network which will deliver it to the device. So, Sigfox Ready devices are shielded from the internet by a very strict firewall.

Security of data in motion :

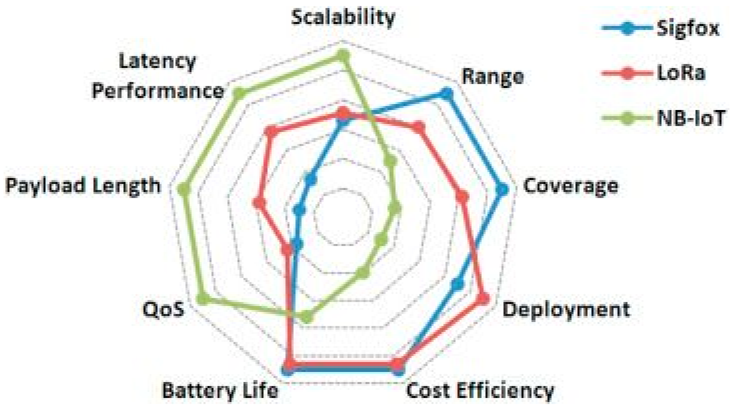
- **Authentication :** Each Sigfox device have a unique symmetrical authentication key given during manufacturing. Therefore, each message sent or received contains a cryptographic token computed on the authentication key. Thus, authentication of the sender and message integrity are ensured.
- **Anti-replay :** A counter is implemented in all message to detect and discard replay attempts
- **Anti-eavesdropping :** Data can be conveyed over the air without any encryption, with the encryption solution provided by Sigfox or by the client own end-to-end encryption solution.

Security of data at rest :

- **Base stations :** Secured by state-of-the-art solutions based on TPM.
- **Sigfox Core Network :** Secured by state-of-the-art solutions.

Conclusion

To conclude this report, we will rapidly summarize how Sigfox perform in terms of different IoT factors. For QoS, Sigfox employ an unlicensed spectra and asynchronous communication protocols so the QoS is pretty low comparing with for instance NB-IoT. In terms of energy consumption, Sigfox is one of the best LPWAN technology but at the cost of latency and then Sigfox is not the best choice for low-latency applications. The main default of Sigfox is his maximum payload size (12 bytes) which limits its utilization in every application that needs large payload sizes. In terms of network coverage and range, Sigfox is the best available LPWAN technology, a single base station can cover an entire city with a range of 40 km. Moreover, Sigfox is one of the most cost-effective solutions for IoT communications. The advantages of Sigfox over the others LPWAN Technology are summarize in the following figure:



Sources

- https://www.sigfox.com/en/sigfox-iot-technology-overview
- https://www.sigfox.com/en/sigfox-iot-radio-technology
- https://www.sigfox.com/en/sigfox-global-iot-network
- https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7894201
- https://www.linkedin.com/pulse/nb-iot-versus-other-lpwan-technologies-harald-naumann/
- https://www.sigfox.com/sites/default/files/1701-SIGFOX-White_Paper_Security.pdf