Sigfox

Mathilde Cornille | Clément Delobel | Jeremy Vincent 5 ISS A

Introduction

Sigfox is a well known communication technology for IoT devices. The objective of this document is to explain the theory behind this technology and explain the advantages and the drawbacks according to the different use cases.
First, we will explain the communication theory through the physical and the mac layers and, then, keys about security and energy consumption for this technology.

Physical layer

1. Frequency & Bandwidth

Sigfox is using **Ultra-Narrow Band (UNB)** modulation. This protocol uses **192KH**z of the publicly available band to send messages. The message range is of **100 Hz** and message are sent with a data rate of **100 to 600 bits per second** depending on the regions.

The bandwidth used by Sigfox depends on the location of the network. In Europe, Sigfox emits between **868 and 868.2 MHz** while in the rest of the world it uses bandwidth between 902 and 928 MHz (depending on local regulation).

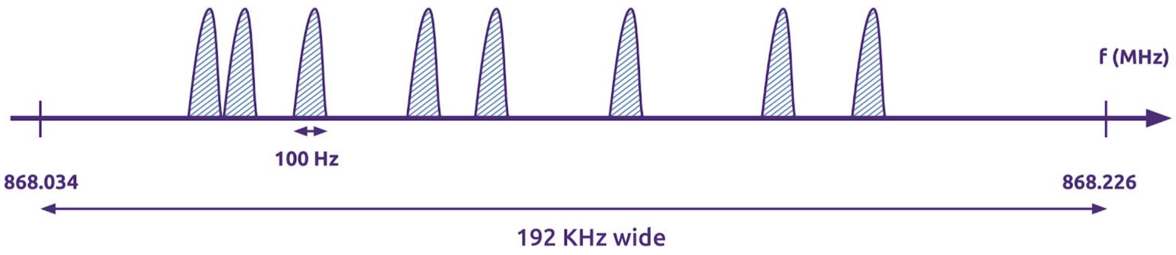

Fig 1 : Message emission in European bandwidth

As the modulation leads to ultra-narrow messages, Sigfox stations can communicate over very long distances without being affected by the noise.

2. Modulation

Sigfox uses **Differential Binary Phase Shift-Keying (DBPSK)** to modulate the signal. This modulation technique is a specific application of BPSK, which is a technique using the phase to encode 0 and 1.

DBSPK unlike BPSK does not need a reference of phase to identify a 0 or à 1. In fact, “differential” means that this technique is based on **phase changes.** When there is changing in the signal we can assume it is a 1, and when there is no change it is a 0, as shown in the fig 1.

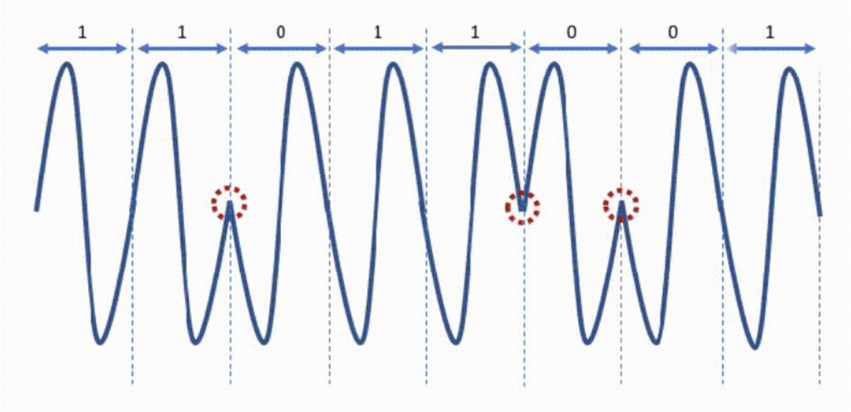

Fig 2 : DBPSK modulation

MAC layer

Sigfox medium random access layer relies on **Random Frequency Time Division Multiple Access (RFTDMA).**

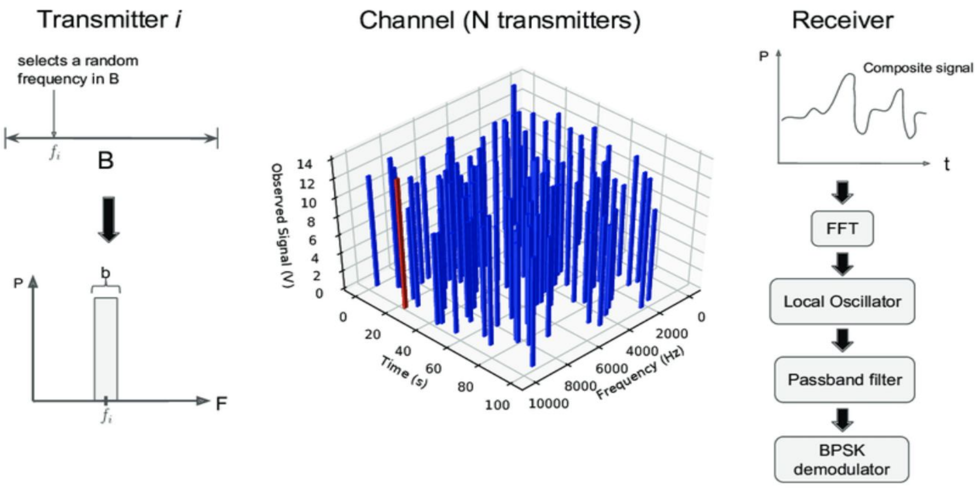

Fig 3 : RFTDMA representation

In Sigfox network, active nodes have access to the wireless medium **randomly in time and frequency** without contention-based protocol.

The transmitter emits the message it wants to send and two encoded replicas on different frequency and time. This method, called "**time and frequency diversity**" increase the QoS of the protocol. Indeed, by sending three messages instead of one, we increase the chance to receive it and decrease losses due to interferences.

Concerning the receiver, a composite signal is received and has to be treated and demodulated by BPSK demodulator.

This medium access control method limits the energy consumption of the devices, which is a significant advantage for IoT application.

Security

By its design, Sigfox has a **built-in firewall**. Unique authentifications guarantee the integrity of the devices and messages transmitted, while encryption is possible to further protect sensitive data.

1. Security on message processing

Sigfox has **sequence numbers** which are anti-replay mechanisms (associated with MAC). This mechanism allows you to establish a valid window of the sequence number to receive messages. Moreover, each Sigfox device has a **unique symmetrical authentication key**. Each transmitted message a cryptographic token based on this key to ensure the verification of the sender and so the integrity of he message. Furthermore, **encryption** is also available for sensitive data.

2. Security on base station & its communication

Sigfox has is own **TPM** (Trusted Platform Module) which secure the different keys involved in communications. It is unstealable and its integrity is ensured by a **secure boot**, while its runtime integrity is managed by a **IMA** (Integrity Measurement Architecture). Finally, the **binding** between the OS and the hardware only allows the base station to connect to an OS built by Sigfox and an OS can only connect to a base station hardware.

3. Security on key generation and provisioning

Each device using Sigfox is protected by a **token** and a **device ID**, both assigned by the manufacturer. This manufacturer as to be Sigfox certified to make it possible. THis assignation needs a secured protocol which involve the Central Registration Authority (**CRA**) which can generate a Network Authentication Key (**NAK**) and a Porting Authorization Code (**PAC**), both needed for the authentication assignment.

4. Security on data center

The Sigfox Support System is hosted in secured certified **data centers**, secured with **biometric protection** for physical access. All the data centers are **doubled on internet**, using different providers. At the application layer, components are strongly monitored to detect traffic increase. **Critical data** is stored in different parts of the IoT chain in order to limit the impact of a compromised device.

Power consumption

Power consumption values **might be different** according to the **use cases**. For example **different devices**, **bitrates**, **directionalities**, **range**, among other, lead to more or less energy consumption.

However, **experimental values** from researchers on a simplified model gives an approximation of **0.4 J to send a 12-byte payload**. This gives an energy of approximately **4 mJ to send 1 bit**. Other models lead to consumption between 4.56mJ to 1.470J, depending on the use case.

These power consumption leads to a **typical autonomy of 1 to 5 years**, once again depending on the use case and the frequency of the communication. The theoretical asymptotic device lifetime is about 15 year with a 2400mAh battery. Of course, this estimation is purely theoretical and does not take unexpected event like current leak or unnatural discharge into account.

Conclusion

To conclude, Sigfox seems to be a really **good technology for low power devices**. It gives a great service that include **efficiency, security and robustness**. The typical use of this technology is for **short communication** (few bytes) at **low frequency** (one frame every couple of minutes). However, it shows **limitation** in term of **bi-directional communication** or **mobility**. This means that Sigfox should be used for immobile sensors across a city rather than for autonomous car, for example.

Sources

https://www.disk91.com/wp-content/uploads/2017/05/4967675830228422064.pdf
https://www.disk91.com/2017/technology/sigfox/the-sigfox-radio-protocol/
https://www.link-labs.com/blog/nb-iot-vs-lora-vs-sigfox
https://hal.archives-ouvertes.fr/hal-01774080/document
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6387435/
Internet of Things for Architects : Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security