INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

Report : Sigfox Specifications

5th year - Innovative Smart Systems
Supervisor :
Daniela DRAGOMIRESCU daniela@laas.fr

Audran DEYTS deyts@etud.insa-toulouse.fr
Renaud GAUTIER rgautier@etud.insa-toulouse.fr

Contents

List of Figures

1 Introduction

With the emergence of the Internet of Things (Iot), there have been a need for new protocols that would be able to handle unication between billions of smart devices. The mobile network was first thought to be adequate, but the heavy charge from all the connected devices and the energy cost induced by the use of such network made people look for other solutions.

Among all the challengers emerged Sigfox, a french startup founded in 2010 that is located in Labège, near the city of Toulouse. Sigfox provides what is considered to be the first IoT-oriented network, which is currently deployed in almost thirty countries, among which the USA, France, Germany, Brasil, Japan , Australia, ...

IoT networks are specialized in Machine-to-Machine (M2M) unication, and they aim at optimizing the unications between smart devices in order to be scalable and energy efficient. Beside Sigfox, various protocols are trying to build a name in IoT networking, such as Lora, with which Sigfox forms the most prominent IoT protocols.

We will try to understand in this document how Sigfox challenged the IoT related issues. In order to do that, we will talk about the physical layer and the MAC layer. Then we will focus on the provided quality of service, to finish with the security issue.

2 Physical layer

In the OSI model, the physical layer is the "bottom" layer. It mainly provides a standardized interface allowing to transmit raw bits on the unication medium (which includes line coding, modulation, multiplexing, etc.). It also links the unication medium with hardware's MAC (Medium Access Control) layer. For its network, Sigfox managed to develop, patent and deploy its own physical layer. The said layer is based on an ultra narrow band modulation, which is called VMSK (Very Minimum Shifting Key). It is a BPSK (Binary Phase-Shift Keying) modulation, in which the data is transmitted by the phase of the signal, which can be described as a succession of sine and cosine waves.

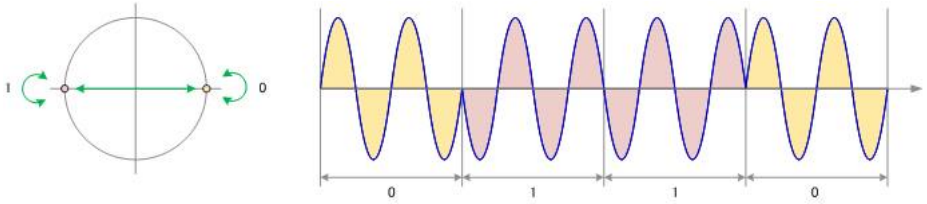

Figure 1: BPSK constellation diagram and temporal representation

With this technique, the data rate is low, around 100 bits per second. Thus, the bandwidth is also very limited, around 100 Hz. The frequency used for these transmissions are within the "free" ISM band. The bands are the following :

Ultra Narrow Band (UNB) for unication:

- Europe : 868 MHz
- America : 915 MHz

The transmission is improved by "frequency hopping" : the multiple transmissions are realized at a carrier frequency within a band which is much wider than the one required by the physical layer (within the earlier-specified ISM bands). Indeed, the carrier frequency is chosen within a 192 KHz wide band, and rapidly switched to another frequency within this band, in a predetermined order. Given that the transmission only occupies a very small part of the given bandwidth at any moment, this technique allows to significantly reduce the degradation caused by narrowband interference sources, such as other Sigfox nodes unicating on the same network, thus allowing more nodes to transmit at the same time.

Although this technique has strong advantages, it implies a very high oscillator accuracy node-wise. Indeed, this precision will give the shift between the actual transmission frequency and the desired one. As the carri frequency shifts very often, the oscillator must be able to provide a very precise frequency after each shift.

Sigfox physical layer provides a bidirectional unication, which means that the base station can transmit data to the node (downlink), and the node can send data to the base station (uplink). Nevertheless, the downlink is not used a lot because very few downlink messages are allowed. This is mainly caused by the fact that the reception sensitivity is much better for the base station than for the endpoint. The downlink uses another modulation, Gaussian Frequency-Shift Keying (GFSK), with a slightly better data rate of 600 bits per second .

Furthermore, only half-duplex communication is possible with this system.

3 MAC protocol

3.1 FRTDMA

Sigfox uses a MAC layer inherent to Ultra Narrow Band called FRTDMA (Random Frequency and Time Division Multiple Access). TDMA is a type of time-division multiplexing, with the special point that instead of having one transmitter connected to one receiver, there are multiple transmitters. In the case of the uplink from a mobile phone to a base station this becomes particularly difficult because the mobile phone can move around and vary the timing advance required to make its transmission match the gap in transmission from its peers.

Sadly, Sigfox give very few information concerning its UNB MAC layer. However, we know that the system is based on a software defined radio (SDR).

3.2 Frame composition

An uplink message is consists of :

- A preamble (4 bytes)
- A synchronization frame (2 bytes)
- A device identifier (4 bytes)
- The payload (up to 12 bytes)
- A Hash code for packet authentification (variable length)
- CRC check (2 bytes)

which makes a maximum frame length of 24 bytes for uplink messages.

4 Quality of Service

4.1 Power Consumption

Sigfox announces a quite low power consumption for its devices. Indeed, a node consumes 20 mA while receiving data and 50 mA for an emission. According to its website, the consumption of a device is around 100 W̆ per bit and 120 kW per hour for a base station.

4.2 Coverage

With 1200 base stations in France, Sigfox network is currently available for about 92 % of the population, and over 90 % for countries like Spain, Netherlands or Denmark.

Sigfox plans to deploy its network everywhere in the USA with a budget of only 50 M €, which means that the network is quite eas¡y and cheap to implement.

Each station has a range of 30 to 50 km in rural areas, and 1 to 5 km in urban areas, because of perturbations. Finally, network's frequency is low enough to have a good penetration into buildings. However, a higher frequency would allow a good propagation into buildings, because of the waveguide effect. Finally, Sigfox announces that a single base station can handle one million nodes. We do not know if this value is only theoretical or practical, as the company itself is the only one to manage the base stations.

4.3 Data rate

As said earlier, each message has a maximum payload of 12 Bytes. A device can send up to 140 messages per day, which gives a maximum of 1,64 kBytes worth of payload per device and per day. This limit is due to regulations related to ISM bands : a node cannot emit more than about 1 % of the time.

Because of the ultra narrow band used, the data rate is 100 bits per second, and a full message weights up to 24 bytes. Moreover, each message sent from a device to the base station (uplink), is sent up to three times at three different pseudorandom frequencies, with a 45 ms offset in between. This translates into a quite long emitting time for a single message of 2.08 seconds.

4.4 Geo-localisation

Geo-localisation of Sigfox devices without GPS system is made difficult by the ultra narrow band used by the network. This is due to Heisenberg principle of incertitude which claims that the standard deviation of N physical measures of localisation from an electromagnetic wave, with a bandwidth B and an signal-to-noise ratio S will always be superior or equal to Cramer Rao bound.

$$CRLB(x, S, B)$$

Practically, this bound is larger when the bandwidth of the signal becomes narrower. Thus, Sigfox system has a limit of a few kilometers for localisation accuracy.

Nowadays, it appears that this precision is near to 100 km. That is the reason why almost all devices that need to be localised embed a GPS module, which is much more accurate.

4.5 Service's costs

Sigfox offers various offers for nodes, depending on the user's subscription, there are currently four offers :

- Platinum : 101 to 140 daily uplink messages + 4 daily downlink messages
- Gold : 51 to 100 daily uplink messages + 2 daily downlink messages
- Silver : 3 to 50 daily uplink messages + 1 downlink message
- One : 1 to 2 daily uplink messages + no downlink

Prices for these subscriptions evolve between 1 € and 14 € per devices and per year, but the price decreases when the number of nodes of one user rises.

5 Security

This section will treat about the security measures built around the Sigfox protocol. In order to do that, we will explore three following key points (1) in the security field:

- confidentiality : the data is not made available or disclosed to unauthorized individuals, entities, or processes
- integrity : assuring the accuracy and completeness of data over its entire life-cycle
- availability : the information must be available when it is needed

Each feature needs to be implemented at several, if not all, points of the data's life cycle. Below is a figure of a typical data flow with Sigfox's protocol.

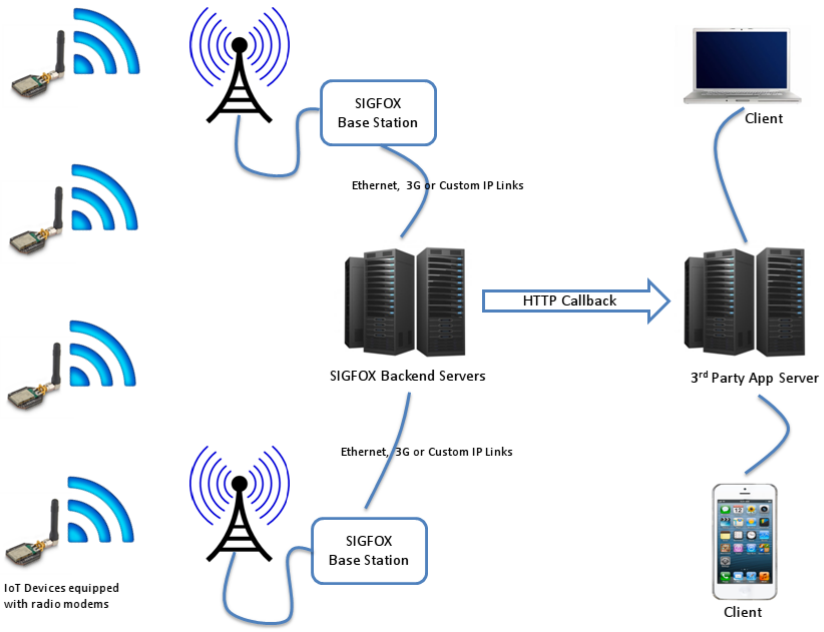

Figure 2: Sigfox network topology-data flow

The IoT nodes on the left side will communicate with Sigfox base stations, which will then send the information to the Cloud (Sigfox's servers). The owner of the data will then access to the information in the Cloud in order to provide a service to his clients. Sigfox needs to ensure that the security is maintained at each part of the flow.

5.1 Confidentiality

One of the best way to preserve the confidentiality of the data is to encrypt the information all the way. As we can see in figure 2, Sigfox need to protect its data during three different times : when the data is sent from an IoT node to a base station, when the data is sent from a base station to the Cloud, and then when a 3rd party application tries to use Sigfox's data from the Cloud.

For the first case (IoT node to base station), Sigfox implemented confidentiality using two components. One of them is an unique id embedded in each device that is used to identify the device (2). An issue with that kind of securing is that managing all the different ids for each device can be troublesome, and maybe not suited for the upcoming 20 billions IoT devices (3). It can also be noted that since the device's id is clearly written on the messages' header, one can easily track the activity of a single device.

The second component to ensure confidentiality is the use of an AES encrypted signature for authentication. AES is famous for being one of the current most secure encrypting method, making it nearly impossible to break confidentiality. The only way to bypass this security is to have physical access to the device to extract the AES key.

For the communication between the base station and the Cloud, Sigfox is using virtual private network (VPN) to ensure the confidentiality of the data. Using a VPN ensures a good level of security, so we can say that Sigfox is safe on that segment.

Finally, for the access to the data on the Cloud, a third party application has to use HTTPS to communicate with Sigfox's servers. Since HTTPS is secure by its nature, we can say that the confidentiality is also protected here.

In conclusion, Sigfox ensures the confidentiality of its data all along the communication flow. However, on the first segment (IoT - base station communication), we can see that there are still some vulnerabilities. One of the solution would be to add one more encryption layer, understandable only by the owner of the data.

5.2 Integrity

In order to resist against a modification by a malicious third-party entity, Sigfox is implementing a sequence number. To put it simply, Sigfox will reject a message if the sequence number seems to be wrong. However, since the number of message per day is fairly low, we can imagine that guessing the sequence number is not that hard, and that this fail-safe is not perfect.

5.3 Availability

To ensure the availability of the data, Sigfox has to ensure that the service is always accessible and that the system is always up to date. Which means a nearly permanent connection with multiple fail-safe systems, which is in contradiction with the low-energy low-throughput low-cost philosophy of Sigfox.

Indeed, it is very hard for instance to update a system with Sigfox's throughput: just try to update a device with 4 messages/day! Same goes for the multiple fail-safes, they would be too expensive.

That is why we can say that the availability was sacrificed in the sake of a low-energy and low-cost solution that is Sigfox.

6 Conclusion

In conclusion, we can say that Sigfox faced the M2M communication challenge by proposing a communication system that is cheap and very low-energy. Sigfox met a huge success, since it is one of the most popular M2M protocol in the world, being deployed in several countries in Europe, America and Asia.

However, it is not suited for every IoT usage : the data rate is fairly limited, and the geolocalisation depends on the usage of an external GPS device. It is also not made for critical applications since several security measures needs to be implemented yet.

Still, Sigfox is one of the best candidates for applications that does not need a large throughput and to which the current security level is enough.

References

[1] Wikipedia, “Information security,” 20 November 2016. [Online]. Available: https://en.wikipedia.org/wiki/Information_security

[2] R. Derouin, “get started on sigfox,” 18 April 2016. [Online]. Available: http://fr.slideshare.net/RyanDerouin/get-started-on-sigfox

[3] Gartner, “Gartner says 6.4 billion connected ”things” will be in use in 2016, up 30 percent from 2015,” 10 November 2015. [Online]. Available: http://www.gartner.com/newsroom/id/3165317

[4] C. Goursaud and J. M. Gorce, “Dedicated networks for IoT: PHY / MAC state of the art and challenges,” *EAI Endorsed Transactions on Internet of Things*, vol. 1, no. 1, p. 150597, Oct. 2015. [Online]. Available: http://eudl.eu/doi/10.4108/eai.26-10-2015.150597

[5] “LoRa vs LTE-M vs Sigfox. Who will win the battle for the IoT? | Creative Connectivity.” [Online]. Available: http://www.nickhunn.com/lora-vs-lte-m-vs-sigfox/

[6] “[Sigfox/LoRa] Les Vrai/Faux des réseaux dédiés aux objets connectés - Aruco.” [Online]. Available: https://www.aruco.com/2015/12/sigfox-lora/

[7] “On LPWANs: Why Sigfox and LoRa are rather different, and the importance of the business model - Rethink IoTRethink Internet of Things – IoT News and Analysis.” [Online]. Available: http://rethink-iot.com/2015/03/20/on-lpwans-why-sigfox-and-lora-are-rather-different-and-the-importance-of-the-business-model/

[8] “SIGFOX - Signal Identification Wiki.” [Online]. Available: http://www.sigidwiki.com/wiki/SIGFOX

[9] J.-P. Cipria, “Jean-Paul Cipria Engineer’s Book.” [Online]. Available: http://www.nanotechinnov.com/jean-paul-cipria#Le_principe_dHeisenberg

[10] C. Fourtet, “Keys for scalable M2m/IoT networks.” [Online]. Available: http://www.microwave-rf.com/docs/WaveRF-2014-SIGFOX.pdf

[11] F. Zafari, “An Overview of LoRA, Sigfox, and IEEE 802.11ah,” Purdue University. [Online]. Available: http://fr.slideshare.net/fahim1989/an-overview-of-lora-sigfox-and-ieee-80211ah

[12] T. Lestable, “LoRa Vs SIgfox,” 2012. [Online]. Available: http://image.slidesharecdn.com/cnam2015-m2m-iot-course2-warming-v0-150227164150-conversion-gate01/95/cnam2015-m2-m-iot-course-2-warming-v02-14-638.jpg?cb=1425055341

[13] G. Kallenborn, “Objets connectés : polémique sur la sécurité du réseau français Sigfox,” Oct. 2016. [Online]. Available: http://www.01net.com/actualites/objets-connectes-le-reseau-francais-sigfox-une-passoire-en-matiere-de-securite-957875.html

[14] “SigFox Vs. LoRa: A Comparison Between Technologies & Business Models,” Jan. 2016. [Online]. Available: https://www.link-labs.com/sigfox-vs-lora/