INNOVATIVE SMART SYSTEMS

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

Wireless Sensors Network

LoRa & LoRaWAN

Robin Marin-Muller

Yohan Boujon

Clément Gauché

Noël Jumin

2024-2025

5 ISS INSA Toulouse

Introduction

In the context of our fifth-year studies in Innovative Smart Systems at INSA, this document explores LoRa technology as part of our Wireless Sensor Networks course. LoRa is an increasingly prominent communication technology known for enabling long-range, low-power communication, making it highly suitable for various IoT applications. Its unique capabilities offer significant advantages for remote monitoring and data transmission over extended distances with minimal energy consumption, addressing many of the challenges faced in distributed sensor networks.

This presentation aims to provide a detailed overview of LoRa, examining its origin and evolution, physical layer, MAC layer, and consumption. Through this study, we seek to demonstrate how LoRa contributes to the development of efficient and scalable IoT solutions by also comparing it to other solutions such as BLE, Sigfox or Zigbee.

1. History, Creation, Development, Evolution and adoption of LoRa.

1.1. History and creation of LoRa

The history of LoRa technology begins with a French company named Cycleo, founded in 2009. Cycleo specialized in wireless communication solutions and pioneered the use of Chirp Spread Spectrum (CSS) modulation, a technique initially developed for military radar applications. This modulation is highly resistant to interference and allows for long-range data transmission with minimal power consumption key characteristics for IoT applications.

Cycleo's innovative approach to using CSS for low-power wide-area networks (LPWAN) gained attention due to its ability to support remote, battery-powered sensors over extensive distances. Recognizing the potential of this technology, Semtech Corporation, an American supplier of analog and mixed-signal semiconductors, acquired Cycleo in 2012. This acquisition allowed Semtech to integrate LoRa (an abbreviation of "Long Range") into its product portfolio and begin promoting the technology as a viable solution for long-range, low-power data communication.

Figure 1: The only content on the Cycleo website in November 2012

With the foundation set by Cycleo’s technology, Semtech positioned itself as the primary provider of LoRa technology, developing it as a proprietary protocol for applications in smart cities, agriculture, logistics, and industrial automation.

1.2. Development and formation of the LoRa Alliance

Following its acquisition of Cycleo, Semtech began to collaborate with other prominent technology companies, including IBM and Cisco, to scale LoRa technology for IoT networks. In 2015, these efforts culminated in the formation of the LoRa Alliance, a global association dedicated to standardizing and promoting the use of LoRa technology.

The LoRa Alliance aimed to address a critical need in the IoT space: creating a standardized, interoperable protocol that could be widely adopted by device manufacturers, network providers, and developers across different regions. To achieve this, the LoRa Alliance developed and released the LoRaWAN (LoRa Wide Area Network) protocol, an open LPWAN specification designed to enable secure, bi-directional communication between IoT devices and networks. The standardization provided by LoRaWAN was a major step forward in making LoRa an accessible and widely deployable solution for IoT applications.

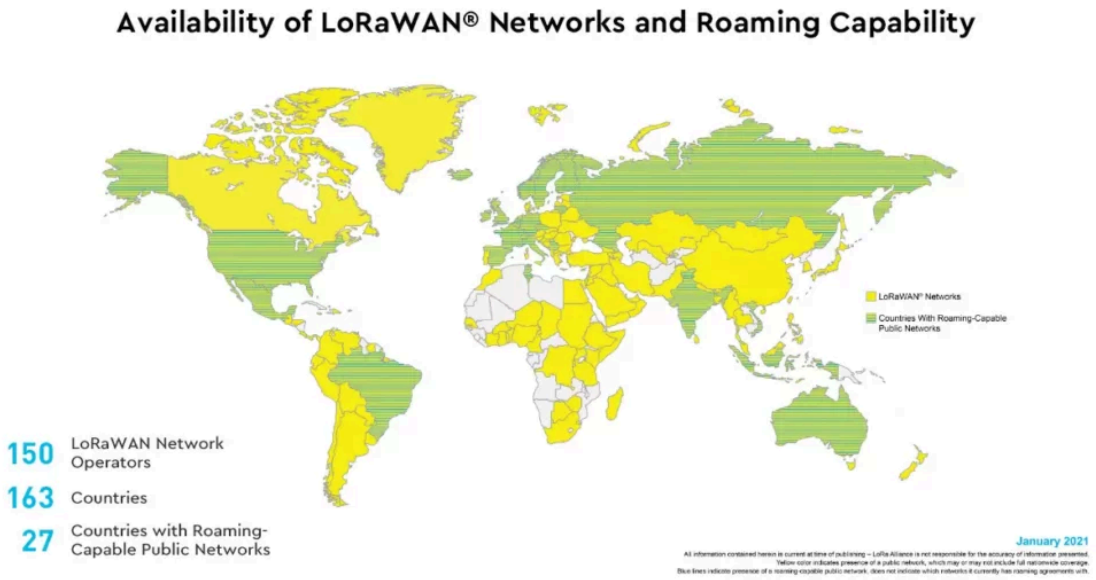


Figure 2: LoRaWAN coverage map from the LoRa Alliance, 2021

The creation of the LoRa Alliance and the adoption of the LoRaWAN protocol enabled LoRa to evolve from a proprietary technology into a globally accepted standard for low-power, long-range communication. The alliance, which includes over 350 member companies as of recent years, works to advance LoRa technology by providing guidelines, certification programs, and ensuring interoperability across devices and networks worldwide.

1.3. Adoption and Applications of LoRa Technology

The success of the LoRa Alliance's standardization efforts, combined with the inherent advantages of LoRa technology, has driven significant global adoption. Today, LoRaWAN networks are widely used across various industries:

- **Smart Cities:** LoRaWAN networks are extensively used in smart city applications, enabling cost-effective monitoring and management of infrastructure, air quality, and energy usage. For example, cities use

LoRaWAN sensors to track pollution levels, monitor street lighting, and manage waste collection, improving sustainability and reducing operational costs.

- **Agriculture:** LoRa's long-range capability is particularly valuable in agriculture, where fields often span large areas. LoRaWAN is used to monitor soil moisture, crop health, and livestock location, helping farmers optimize resources and improve yield with precise data-driven insights.
- **Asset Tracking and Logistics:** The logistics sector leverages LoRaWAN for real-time asset tracking, enabling companies to monitor the location and condition of goods in transit. With LoRa-enabled sensors, supply chains gain enhanced visibility, leading to better efficiency and reduced losses.
- **Environmental Monitoring:** LoRaWAN's low power consumption and long-range capabilities make it ideal for environmental monitoring in remote locations. Applications include monitoring of water quality, wildlife habitats, and climate conditions, providing critical data for environmental conservation.

Due to these diverse applications, the adoption of LoRa technology continues to grow, with support from a global network of LoRa Alliance partners who deploy LoRaWAN gateways, build compatible devices, and provide network infrastructure. As a result, LoRaWAN has become one of the leading LPWAN standards, rivaling other protocols like Sigfox and NB-IoT.

1.4. LoRa's competitors

LoRa's dominance in the LPWAN space is matched by a few key competitors, each of which has unique characteristics:

- **Sigfox:** It is another prominent LPWAN technology. It offers long-range, low-power capabilities similar to LoRa, but operates on a proprietary network. Sigfox devices send small messages at infrequent intervals, which limits the amount of data but makes the system very energy-efficient. Sigfox's advantage is its very low energy consumption, which makes it a direct competitor to LoRa in this aspect, although its dependence on a proprietary infrastructure is limiting its flexibility.
- **NB-IoT (for Narrowband IoT):** NB-IoT, a cellular-based LPWAN technology, is backed by major telecom operators. It uses licensed spectrum and provides reliable connectivity in urban areas with strong coverage. While NB-IoT offers high data reliability, it generally consumes more power than LoRa and requires existing cellular infrastructure, which can increase deployment costs.
- **Zigbee and BLE (Bluetooth Low Energy):** Although Zigbee and BLE are not direct competitors in terms of range, they do offer low-power wireless solutions for short range applications. These technologies are often used in

building automation and personal area networks where long-range connectivity is less critical.

We can say that LoRa stands out among its competitors for its balance of long-range capability, low power consumption and flexible deployment options in both private and public networks. While Sigfox and NB-IoT excel in specific areas, LoRa's open standard and interoperability through LoRaWAN have contributed to its widespread adoption in the IoT.

2. Physical Layer

2.1. Introduction to the Physical Layer of LoRa

LoRa Physical layer or LoRa PHY is the key to ensure long-distance data transmission and low power. It operates using a specific frequency band on the ISM. These frequencies include 169 MHz, 433 MHz for Asia, 868 MHz for Europe, and 915 MHz for North America.

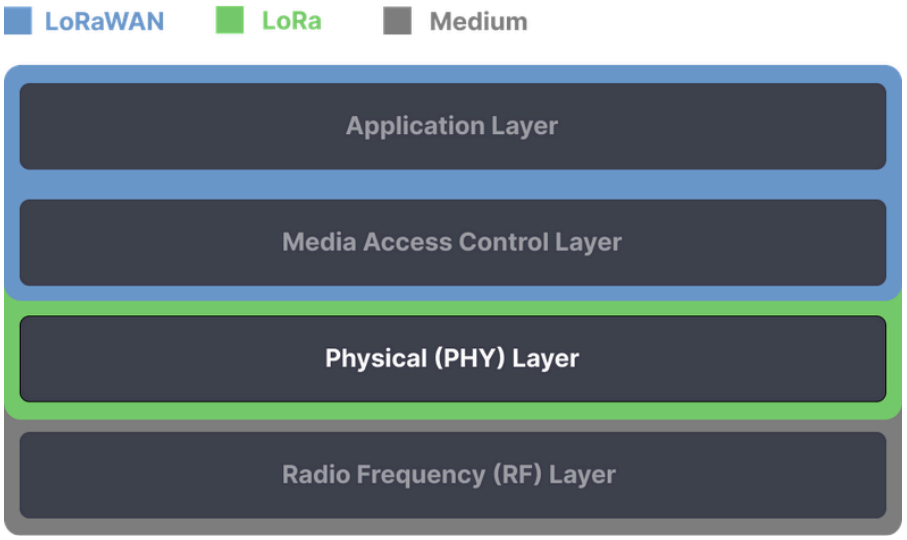


Figure 3: OSI Model showing the Physical Layer

2.2. LoRa Chirp Spread Spectrum

LoRa uses a type of modulation called Chirp Spread Spectrum (CSS). This allows data to be transmitted even when the signal is below the noise level. The modulation works by sending signals called “chirps” where the frequency changes gradually (linearly) over time. This technique makes it very resistant to interference.

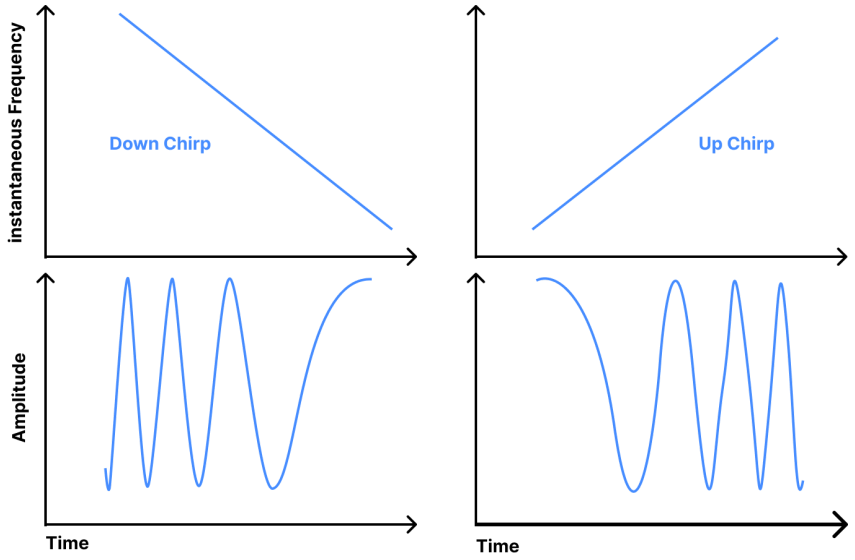


Figure 4: Chirp modulation

One of the main advantages of CSS is its strong immunity to noise and interference. It also allows data to travel long distances while using low power. Moreover, different LoRa signals can share the same channel without interfering with each other thanks to the “orthogonality” of the spreading factors. Orthogonality means–in mathematics–that the dot product of two signals don't overlap nor interferes constructively.

$$\int_0^T f(t) \cdot g(t)\, dt = 0$$

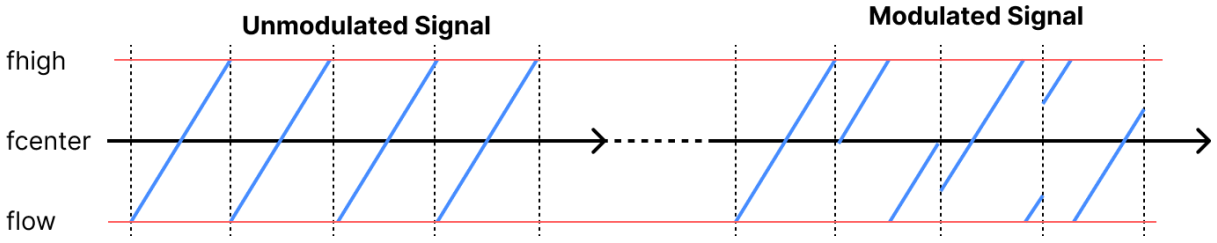


Figure 5: Modulation of the chirps

2.3. Spreading Factor

The Spreading Factor (SF) in LoRa is a key feature that affects both the range and data rate of transmissions. A higher spreading factor means the data is easier to decode and can travel further but on the other hand it reduces the bitrate. Alternatively, a lower spreading factor increases the data rate but limits the range and makes decoding harder.

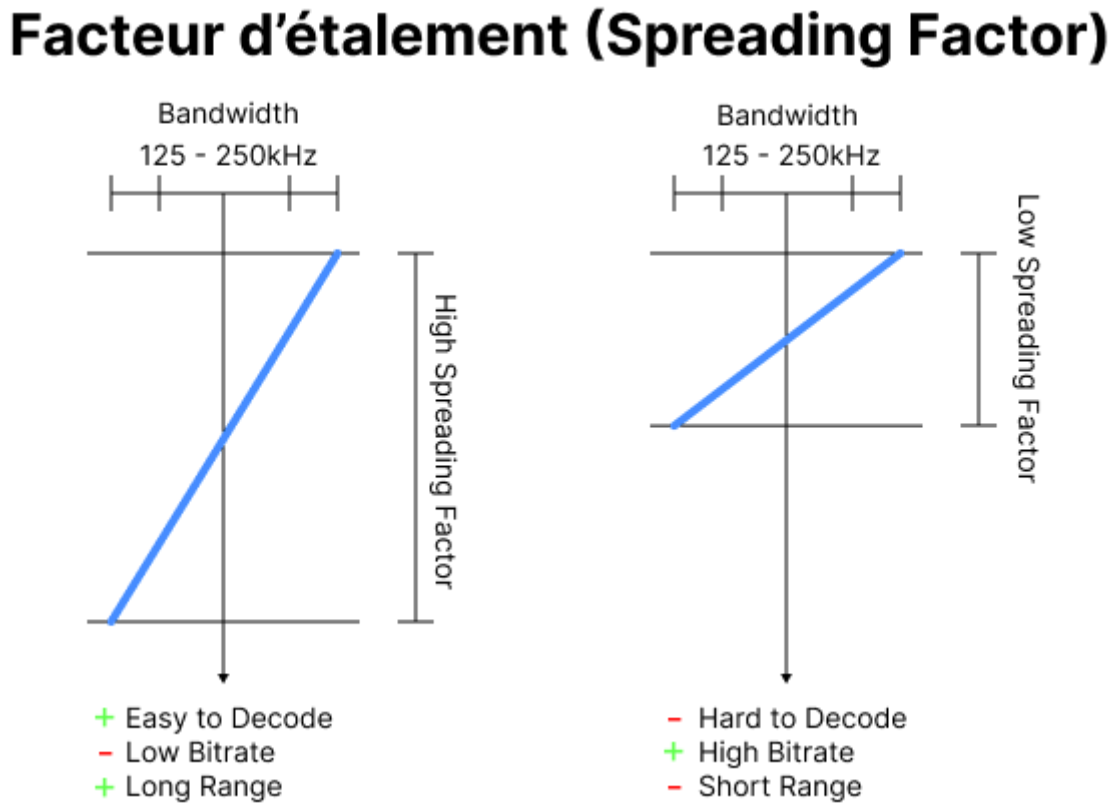


Figure 6: Spreading factor characteristics

For example, when the Spreading Factor is 7 (SF7), a symbol can represent up to 128 different values. In the figure below, we show how information can be encoded as "chirps." Let's take the binary number 1011111 (which equals 95 in decimal). We need to encode this number using 7 bits because the Spreading Factor is 7. An SF of 7 allows for 2^SF different unique steps or "chips."

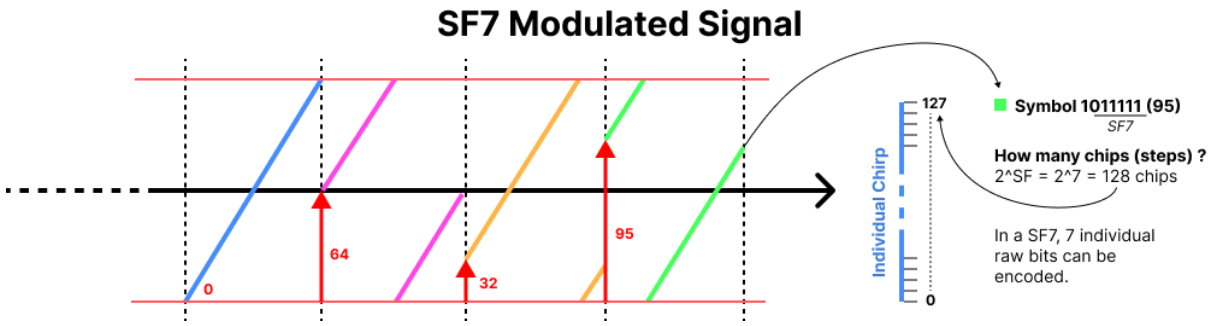


Figure 7: Chirp mechanism

The blue chirp represents the value 0 because it covers the entire frequency range. The purple chirp represents the value 64 (or half of 128). This chirp starts at the base frequency and goes up to the highest frequency, but it needs to finish in the next period. The same process is used for other values like 32 and 95.

2.4. Structure of a LoRa Frame

A LoRa frame is made up of different sections that ensure proper communication. The preamble is the first part, which helps the receiver lock onto the signal for synchronization. Next is the synchronization section that keeps the data flow aligned.

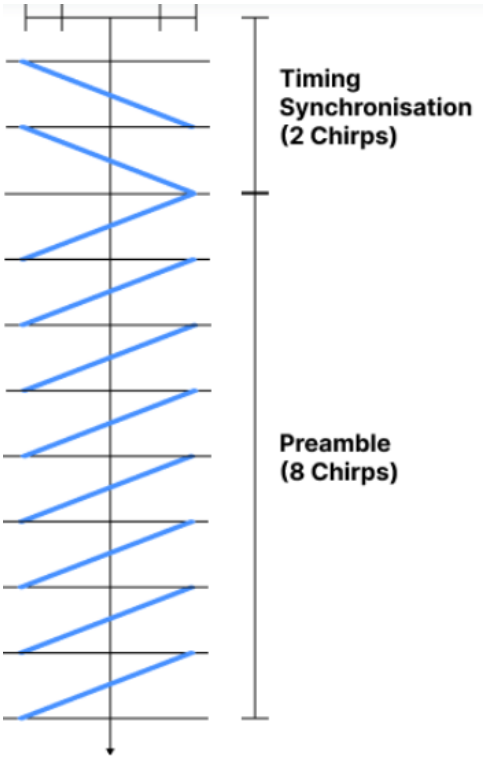


Figure 8: Chirp inside the LoRa frame

The payload is the main part of the frame, containing the actual data sent by the node but we will explain this part in detail in the MAC Layer section. Finally, the frame includes a CRC section to check data integrity and ensure no errors occurred during transmission. This structure eases the task of the receiver to better wake up and demodulate the data packets.

2.5. LoRa Demodulation : Correlation

The process of demodulation in LoRa relies on correlation. The receiver compares the incoming signal which may be weakened, with stored symbols to find a match. This ensures the symbol with the highest correlation is identified accurately.

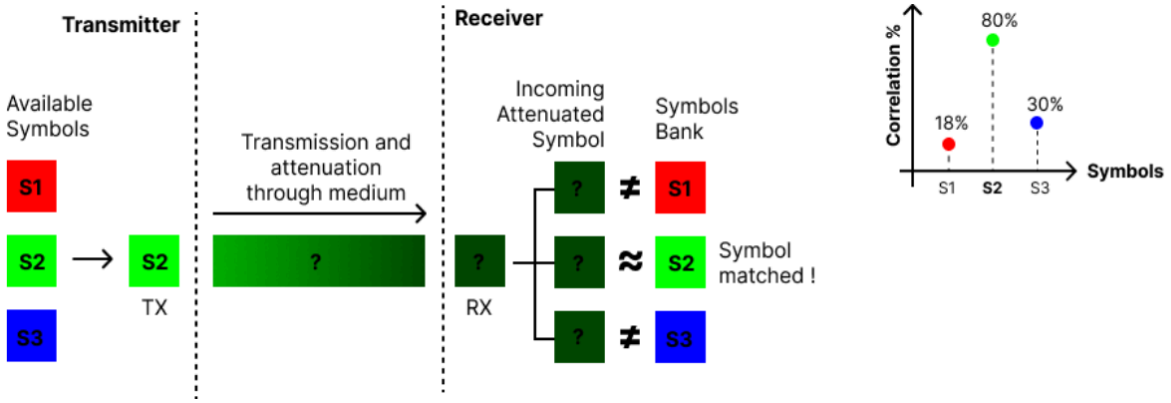


Figure 9: Correlation between transceivers

To make this process effective, the symbols used by both the transmitter and the receiver need to be the same. Additionally, the spreading factor should match on both sides otherwise it cannot work.

2.6. Range and Limitations of LoRa

The range of LoRa transmissions and their limitations are influenced by multiple factors. Shared ISM bands can lead to signal collisions and interference affecting network performance. In Europe, for the 868 MHz band the bandwidth duty cycle utilization is limited to 1% and the transmission power is restricted to 14 dBm.

The material through which the signal passes also impacts the strength. For example, a 6 mm glass pane only causes an attenuation of 0.8 dB, whereas a 305 mm concrete wall can result in an attenuation of up to 35 dB. This means that the type of materials between the transmitter and receiver affects how far and well the signal travels.

3. MAC Layer

3.1. Differences between LoRa and LoRaWAN

LoRa is the technology behind a wide selection of long-range IoT applications. It serves as a physical layer that enables any sensor or actuator to communicate at high distances with little data. It only contains the link layer protocol and can only communicate with ***Point to Point*** communication, LoRa is usually cheaper than LoRaWAN capable devices because of its simplicity. This physical layer in itself cannot deliver any Quality of Service nor complex network grid.

In itself, LoRa can benefit from any MAC layer integration, a wide range of protocols can be used to benefit from this technology (ie: simple P2P), in both software or hardware. Semtech developed with the LoRa Alliance a “LoraMAC” layer which is used in the LoRaWAN (Wide Area Network). The advantage of using such a protocol is that, as explained in the history of LoRa, some gateways have been placed all around the world, so data can travel huge distances and the packets can even be converted into Ethernet MAC if connected to the right gateway.

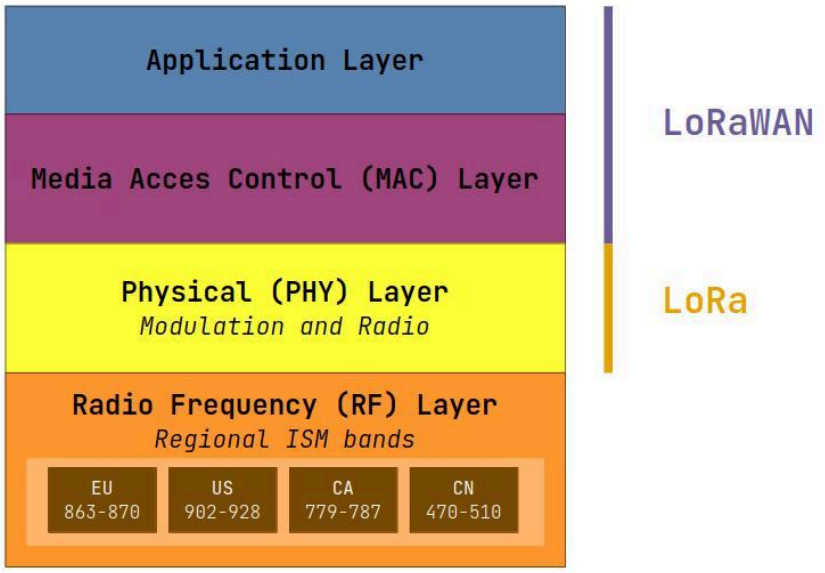


Figure 10: OSI model with the MAC and Application enlighted

Here is a breakdown of each layer that corresponds to either pure LoRa, or the Wide Area Network that has been created by the LoRa alliance. Any application layer can be integrated into this packet. This shows the flexibility of such a protocol. For Point to Point communication, there is no need to use the MAC Layer, LoRa is an open project that can be used depending on the needs.

The main difference is that LoRaWAN enables a more centralized data sharing approach, whereas LoRa expects data to be shared between some points.

3.2. LoRaWAN Protocol in depth

The LoRaMAC layer is composed of 3 types of equipment like the Internet Protocol classes. The only differences being that a device can change its class during communication and that it is not written directly in the address:

- **Class A**: defines low-power devices that do not use CRC, the server only has 1 to 2 seconds to respond.
- **Class B**: compromise between low and high power devices, the server can respond at a given time.
- **Class C**: the device listens permanently for a server's response.

The Mac header can have multiple ways to be interpreted depending on a 3-bit field named "MType". This will indicate if it is a request or simple data transmission. Let's first focus on how a "MACPayload" is interpreted and what it can deliver.

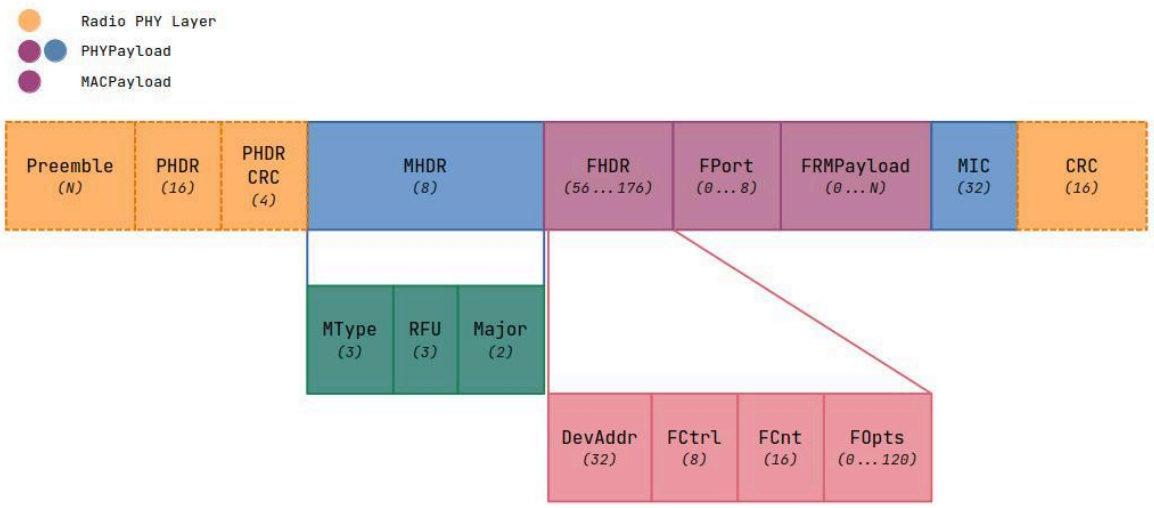


Figure 11: MACPayload Layer

The **MHDR** field is available in every payload, it informs the controller about the nature of the given packet.

The **MIC** field checks for Message Integrity Control, providing trust between devices.

- **MType**: 3-bit message type, can be either a join-rejoin/request, join accept, data up or down. In this example the packet is only intended for data processing (in or out), request or accept methods will be explained later.
- **RFU**: 3-bit set to 0, not used.
- **Major**: 2-bit message to indicate the version of the protocol used.

A data-exchange can be either “Confirmed” or “Unconfirmed”: this means that an acknowledgement from both devices should be sent when the data is gathered. This mechanism is similar to the way UDP and TCP works, it enables a sort of QoS in the MAC level directly.

Following the **MHDR** field, we can find a specific payload. In this example this is only the MACPayload that will be discussed. Moreover, this payload contains the **FHDR** or Frame Header:

- **DevAddr:** the non-unique end-device address given by the network provider.
- **FCtrl:** Frame control which enables adaptive data rate, message acknowledgement, frame pending, and the size of the MAC commands.
- **FCnt:** Frame counter, keep track of how much data has been exchanged between two devices.
- **FOpts:** inside *FCtrl* the size of this field is registered. Frame Options transport MAC Commands which should be between 0 or 15 bytes. Each command can be either transmitted by the Gateway or the end-device. The codes are from 0x00 to 0x0F depending on the direction the packet is transmitted. It can be used to validate connectivity, set some parameters of the network, or even custom commands.

FPort: Frame Port, indicates that a *FRMPayload* will be present next, used in the application layer; it acts like a port in the TCP/UDP protocol. It can be between 1 and 223. 224 is used for test purposes and other values are reserved for future applications.

FRMPayload: Its size is given in the physical payload, it should be smaller than

$$N \leq M - 1 - (\text{length of FHDR in octets})$$

where M is the maximum MAC payload length. This field is the user data, it can be encrypted using the “***AppSKey***”. Stored on both devices, the *MIC* field is generated thanks to another variable named “***NwkSKey***”: we are going deeper in this topic when talking about security mechanisms. These two variables are not sent in any way through the network.

When the *MType* of the *MHDR* field indicates a **Join/Rejoin Request** or a **Join Accept** its payload differs quite a bit. These messages are part of the Over-the-air Activation which enables the device to connect to the LoRa grid.

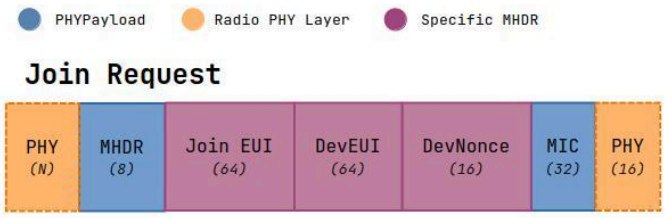


Figure 12: Join Request Sublayer

The **Join Request** is initiated by the end-device to a gateway or another device. It expects in response a **Join Accept** request.

- **JoinEUI** is a unique identifier that enables a gateway to associate the application server or owner. It is generally defined in the device firmware by the developper allowing customization. Similar to an IP Address or a DNS domain name, this identifier is critical to route each packet to the correct server. It can be both used in public and private scenarios, making it particularly beneficial for small or localized LoRaWAN deployments. *(the main difference with DNS domain name is the price of a LoRaWAN AppEUI, which costs around 750 dollars)*
- **DevEUI:** it is a global unique identifier assigned by the manufacturer, similar to the Ethernet MAC Address, the only difference being that here it can be used for device management and identification rather than routing.
- **DevNonce:** counter used by the network to keep a track of the total *join-request*, if a given *JoinEUI* has an abnormal count, the device will be discarded from the network.

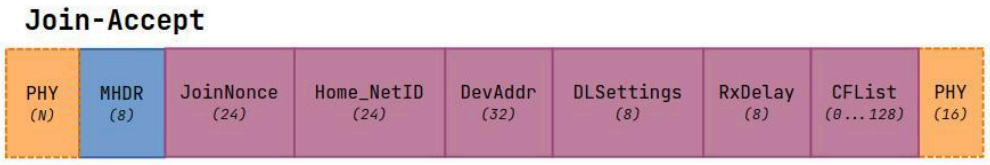


Figure 13: Join-Accept Sublayer

The **Join Accept** is sent after a request to give complementary data about the network. This does not require the MIC field to simplify the process and because trust has already been established between the device and the network.

- **JoinNonce:** counter used by the network to keep a track of the total *join-accept* requests. Similar to **DevNonce**.
- **Home_NetID:** is a 3 bytes identifier and is only known by the network provider. It is used to uniquely identify the network. This is particularly useful in multi-network environments, as it reduces the chances of device

miscommunication and ensures that devices connect to their designated networks.

- **DevAddr:** Similar to the ID given in the **FHDR**.
- **DLSettings**: The first bit is equal to 0. The next 4 bits determine the data rate for both downlink and uplink.
- **RxDelay:** Delay between TX and RX.

CFList: Optional list of network parameters, can be up to 16 bytes.

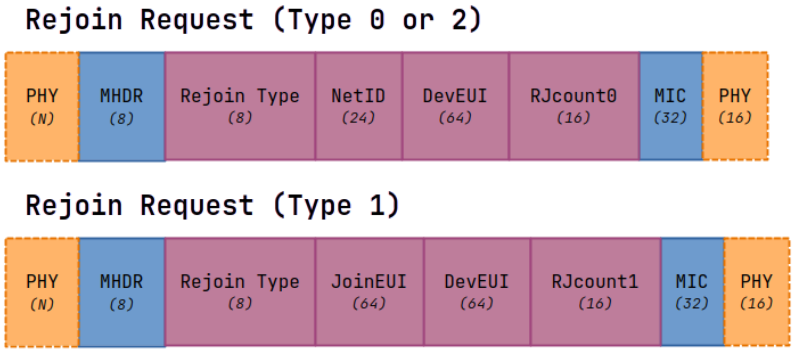


Figure 14: Rejoin-Request Sublayers depending on the type

In some cases, some devices may periodically transmit a **Rejoin Request**, it is used for example to synchronize a device that changed its data rate. There are multiple types of rejoin requests depending on the device's needs.

- **Rejoin Type:** 0 or 2 signifies that either the device needs to be reset, including all radio parameters, or that the device needs to only change its *DevAddr*.
- **Rejoin Type:** 1 signifies that the device asks for a restoration of the lost session context. it is equivalent to a **Join Request**.
- **NetID:** Similar to **Home_NetID**, but given to the network. Should be stored in the *join-accept* exchange.
- **RJCount0:** For every 0 or 2 type, increments the counter for a given **DevEUI**.
- **RJCount1:** For every 1 type, increments the counter for a given **DevEUI**.

3.3. Channel access and collision avoidance

As explained in the physical aspect of the LoRa technology. There are multiple spreading factors that enable different bitrates and radio-frequency sensibility. The Media Access Control of the LoRaWAN has a set of different commands in the **FOpts**, inside the **FHDR** field such as *LinkADRReq, NewChannelReq, RXParamSetupReq* and *DLChannelReq*.

The gateway of the LoRaWAN allocates different channels depending on the country it operates. When a *join-request* is initiated, the gateway will communicate in which of these channels the device should exchange data afterwards. There is one channel for uplink and another for downlink data.

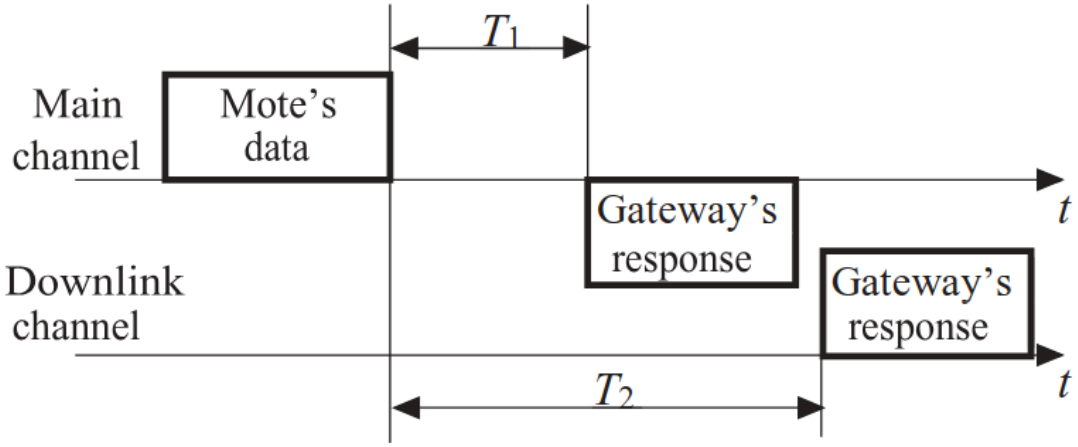


Figure 15: Channels between the gateway and the end-device

"Mote" here denotes a device. In a class A scenario a time period T1 of 1 second is programmed to ensure the low power characteristic of such a device. In time sensible operation this value can be changed to a faster rate. Each channel is used for certain data, downlink represents gateway to mote, uplink mote to gateway, and a main channel is used for other important data.

In typical LoRaWAN, a minimum of 8 channels are used for Rx (downlink) and Tx (uplink), 3 are used for Main/Default commands. This minimum is set by the LoRa Alliance but can be modified depending on the network operator. Typically there are more Uplink channels than Downlink because devices are more inline to send data rather than receive them.

Because channels are limited in some way, each data is vulnerable to collisions and data corruption. Other ways to fight this issue are the duty cycle used, 1% in the case of LoRa transmission, which leaves a lot of space for devices to send data. The

low bandwidth and data rate help this problem to be solved too. However it is not impossible that a device sends data while another hasn't finished.

The **delay slot** concept consists of giving each device a random time slot they can use. When one wants to send data, it first checks if the line is busy, then will launch this random delay. This solves the famine problem that could be happening with strictly coded delays.

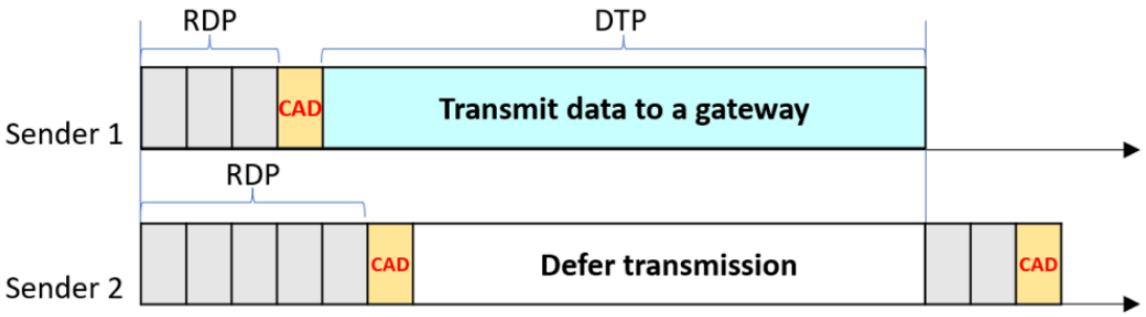


Figure 16: Delay-slot concept

As explained earlier, there are multiple types of data that can be sent to the gateway, one of which is "Confirmed Data": similar to TCP. They wait for an acknowledgement from the gateway, this way, even if a data collision is appearing, the sender knows if its data has correctly been sent.

Overall, these combined techniques such as *Multiple channels*, *Delay slot*, *Software Confirmation, Short Duty Cycle, Low Bandwidth* can enable the LoRa packets to be well distributed with maximum collision avoidance. However, some newer research showed that new techniques such as the ST/CA (Slotted Transmission with Collision Avoidance) protocol could greatly reduce the occurrence of data collision. By listening constantly to the data being acquired and giving each device a timing slot to send data. This new opportunity is not yet implemented because of the energy it costs and is still a proof of concept.

3.4. Security Mechanisms

Like in all radio telecommunication, data can be vulnerable to interception and decoding. With the right equipment, an outsider could intercept data or inject false information to gateways.

To secure data, LoRaWAN encrypts each payload using AES-128 encryption, which relies on two keys: the **NwkSKey** *(Network Session Key)* for network integrity, calculated by the gateway and **AppSKey** *(Application Session Key)* for application data privacy, calculated by the end-device. These two keys are derived from the **AppKey** which is a root key unique to each device.

```
uint128_t NwkSKey = aes128_encrypt(AppKey, 0x01 | AppNonce | NetID | DevNonce | pad16 );
uint128_t AppSKey = aes128_encrypt(AppKey, 0x02 | AppNonce | NetID | DevNonce | pad16 );
uint128_t cmac = aes128_cmac(AppKey, MHDR | AppNonce | NetID | DevAddr | DLSettings | RxDelay | CFList);
uint3_t MIC = cmac[0..3];
uint128_t result = aes128_decrypt(AppKey
                                  ,AppNonce | NetID | DevAddr | DLSettings | RxDelay | CFList | MIC);
```

Figure 17: Security Algorithm in LoRaWAN

As we can see in this algorithm, the calculation of each key includes the **AppNonce** or **JoinNonce** provided by the network and **DevNonce** generated by the end device. Other fields include payloads given by *join-requests* and *uplink* or *downlink* packets. For each data exchange, an **MIC** is calculated using these keys, ensuring the integrity and authenticity of the data.

4. Power Consumption

4.1. Power management in LoRa devices

The LoRa protocol is renowned for its long-range communication capabilities with low power consumption. Key factors influencing power consumption include transmission power, data rate, frequency, and communication duration. The data rate is directly affected by the Spreading Factor (SF), which can be set between 7 and 12. A higher SF increases communication range and noise resilience but also increases power consumption and communication duration. Conversely, a lower SF reduces power consumption and communication time but also shortens the range.

For example, with an SF of 7, transmission time is shorter, resulting in a higher data rate and lower power consumption, but the range is reduced. An SF of 12 allows communication over distances greater than a kilometer, with improved noise resilience, but consumes more energy per transmission.

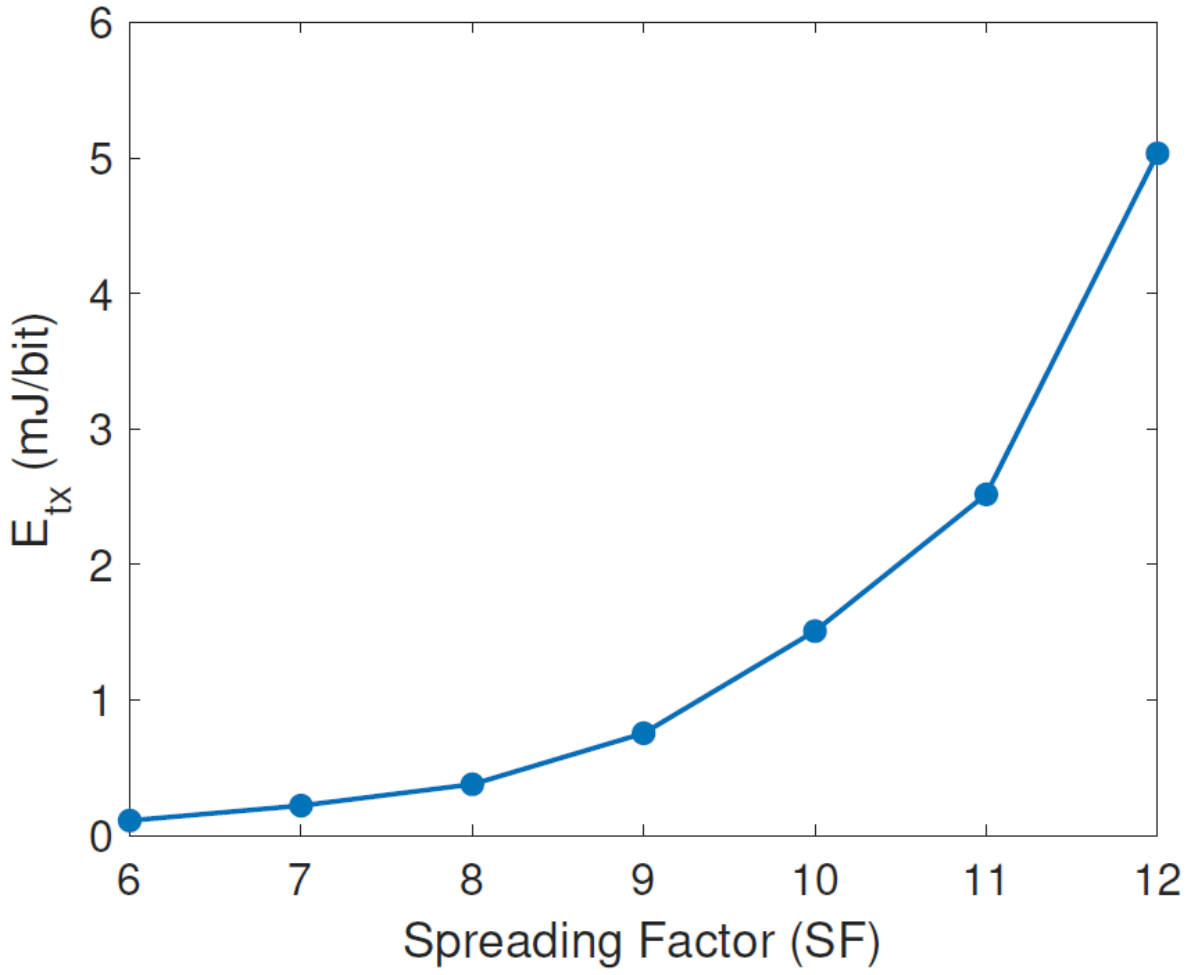


Figure 18: LoRa Time-on-Air vs different SF with 8 bytes payload (CR = ⅘, BW = 125kHz and 8 preamble symbols)

Let's take an example where we want a system capable of communicating over a long range (SF of **12**) with a transmit power of **100 mW**. We will choose a bandwidth of **125kHz** and a payload of **10 bytes**, so here are the steps to find the energy per bit required for this communication:

$$Symbol\ Duration\ =\ \frac{2^{SF}}{Bandwidth(Hz)}\ =\ 32.8\,ms$$

$$Transmission\ Duration\ =\ Symbol\ Duration(s)\ *\ Number\ of\ Bits\ =\ 2.624\,s$$

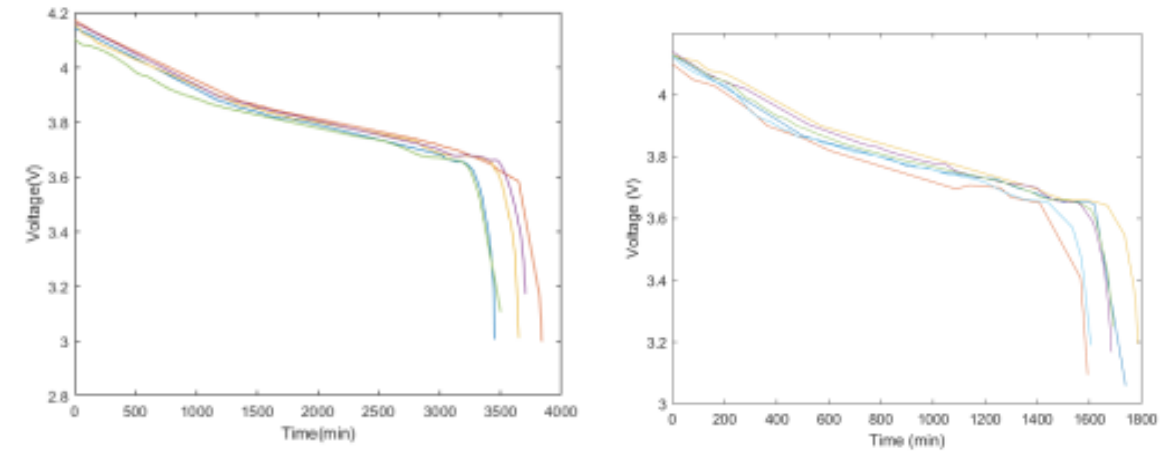
$$Energy\ per\ bit\ =\ \frac{Transmission\ Power(W)\ *\ Transmission\ Duration(s)}{Number\ of\ Bits}\ =\ 3.28\,mJ$$

With a SF of twelve you can communicate over a distance of more than a kilometer, so the consumption per bit is really low. If we want to do the same calculation but with an SF of 6, the result will be 51.2uJ/bit therefore 6 times less than with a configuration with an SF of 12. The only problem here will be that the range will be reduced due to being less resilient to noise.

We will compare the energy consumption of LoRA with different protocols in the next section.

4.2. Comparison between other protocols

I have been able to find different studies of comparison between LoRA and other protocols such as, to start, NB-IoT which is also a low power protocol. As we can see the LoRA consumes much less than NB-IoT for the equivalent parameters since, given the graphs below, the lifespan of a system that uses LoRA is twice as high. This comparison is particularly relevant because both LoRa and NB-IoT are designed for long-range communication, making them direct competitors.



.

Figure 19: Battery voltage measurements of the LoRa end device at different elapsed times (right) and the NB-IoT end device at different elapsed times (left). All trials, shown in different colors, were measured from fully charged to empty

Secondly, I was able to find a comparison between the same module using wifi and LoRA, this study also made it possible to determine the lifespan of the product. As we can see below, wifi consumes less power even though it remains quite close to LoRA, however we can observe that the data rate does not have as much impact on LoRA as on wifi. This comparison here is less relevant than the first one because Wifi is not a long range protocol so it is not used for the same systems.

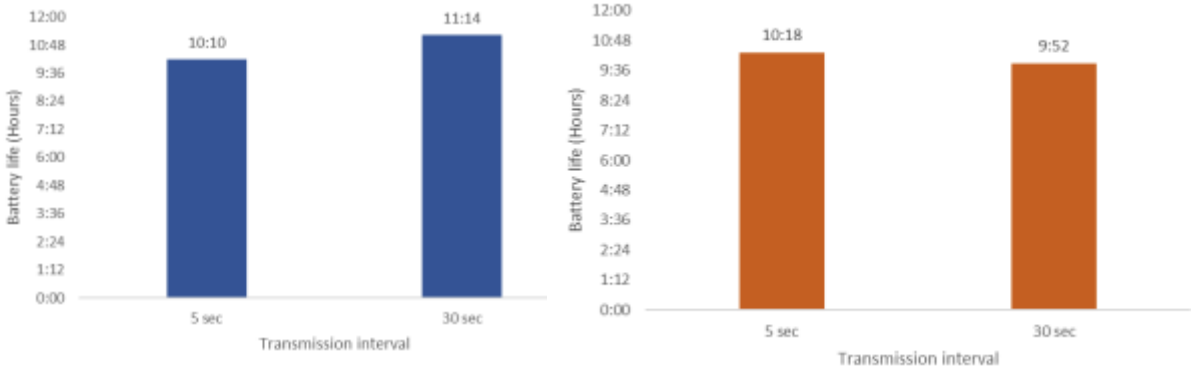


Figure 20: Lifetime of a product using Wifi on left and LoRA on right

Finally, I was able to find a graph that shows the lifespan of a product using different protocols such as BLE, LoRA or SIGFOX. As we can see, BLE does not consume as

much as LoRA or even SIGFOX and BLE keeps consumption really low even at very high speeds.

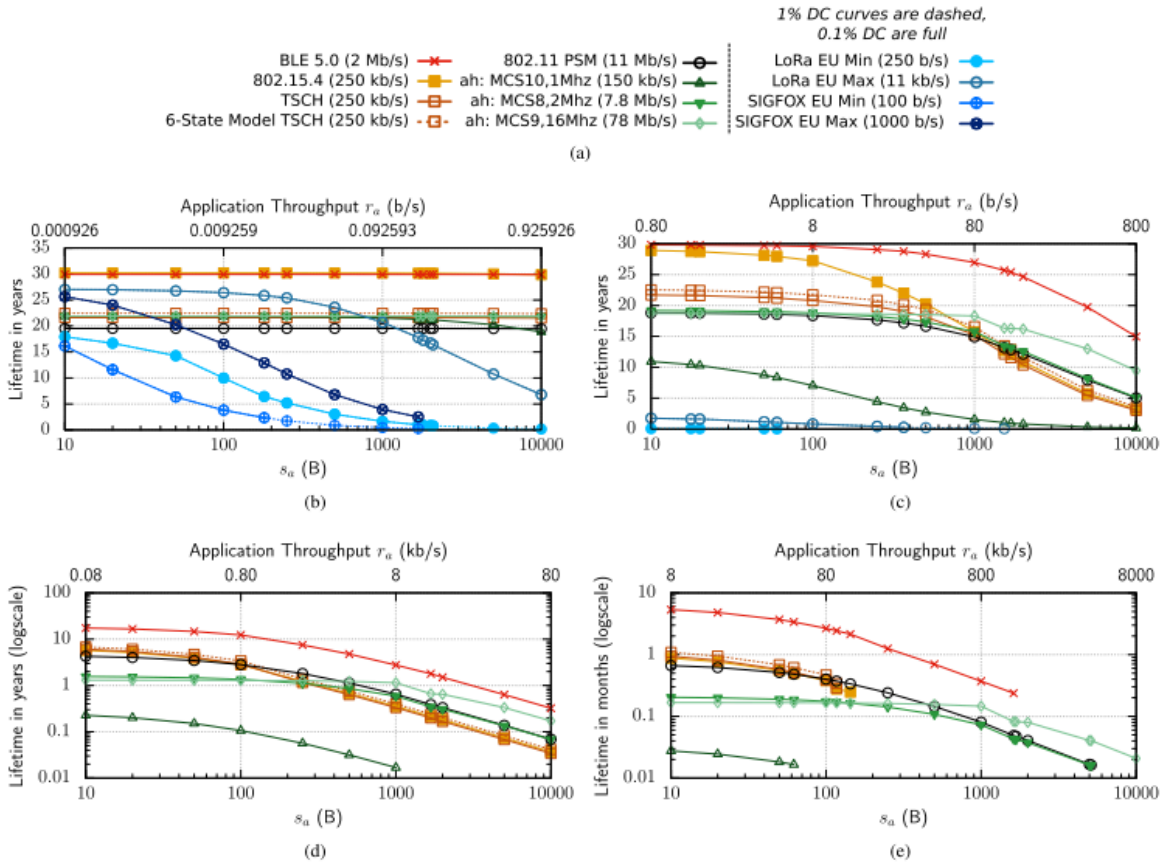


Figure 21: Different t_a and data size s_a, in bytes, leading to varying r_a, impact lifetime for a starting energy E_0=13.5kJ, PER=0. The bottom x-axis is the data size in bytes per t_a while the top x-axis presents the corresponding data rate r_a in b/s. No packet loss or clock drift is assumed. (a) legend. (b) varying s_a, constant t_a=1 day. (c) varying s_a, constant t_a=100s. (d) varying s_a, constant t_a=1s. (e) varying s_a, constant t_a=10ms

Obviously these comparisons remain quite useless when we take into account the field of application. It is obviously preferable for applications that require very short distances to use BLE given its very low consumption. On the other hand, LoRA shows its difference in its range which exceeds one kilometer, its only real competitors are therefore SIGFOX and NB-IoT. In this case, we note that LoRA is a very good solution for IoT systems that require long-range communication since its consumption remains lower than its direct competitors.

Conclusion

The exploration of LoRa technology in this study highlights its transformative role in WSN and the IoT. As a long-range communication technology complementing low power supply, it presents a solution of great innovation for overcoming the challenge in such deployments of resource-efficient scalable networks for different applications such as agriculture, smart cities, logistics, and environmental monitoring.

The research outspoke the advantages of LoRa and its features, especially the robust Chirp Spread Spectrum (CSS) modulation, which enhances resistance to noise and facilitates long-range communications. The evolvement of the LoRa Alliance and the development of the protocol LoRaWAN have further standardized the technology and boosted its use worldwide with interoperability. Other important analyses include the spreading factor and MAC layer as significant roles in optimizing range, data rate, and energy efficiency.

However, our study recognizes some shortfalls of this technology: mainly its susceptibility to interference provided by signals at shared ISM bands that are simultaneously used and can lead to signal collisions and interference affecting network performance. To add, its considerable distance performance, emphasizes its position regarding long-range applications, and make it a direct competitor of Sigfox and NB-IoT while the low-power technologies BLE is better in short-range applications.

With the continued growth of IoT, LoRa's future looks promising. Ongoing developments in security, adaptive data management, and power optimization are expected to bolster its relevance and application. As industries increasingly prioritize efficiency and scalability, LoRa stands out as a robust solution that meets the demands of modern IoT ecosystems.

LoRa has successfully overcome many of the challenges traditionally faced by wireless sensor networks, enabling efficient and sustainable connectivity for billions of devices worldwide. Its journey from a niche technology to a globally adopted IoT standard, unlike its competitor SigFox for example, underlines the importance of optimised technology, but also of the strategic and marketing choices that go with it.

Sources

History of LoRa

- "Full understanding of LoRa and LoRaWAN", ***Mokorola***
- "Lora & LoRaWAN Explained", ***ElectronicsInnovation.com***
- "http://www.cycleo.net/", ***WebArchive.org***
- "LoRaWAN - A low power WAN protocol for Internet of Things: A review and opportunities", ***IEEE***

Power management

- "Hybrid Low-Power Wide-Area Mesh Network for IoT Applications" by Xiaofan Jiang and Heng Rhang
- "Energy Efficient Coded Communication for IEEE 802.15.4 Compliant Wireless Sensor Networks" by V. Nithya, B. Ramachandran and Vidhyacharan Bhaskar
- "Comparison of LoRa and NB-IoT in Terms of Power Consumption" by LUNTE TAN
- "WiFi and LoRa Energy Consumption Comparison in IoT ESP 32/ SX1278 Devices" by L. Garcia, JM. Jimenez, J. Lloret, P. Lorenz
- "Comparison of the Device Lifetime in Wireless Networks for the Internet of Things" by Elodie Morin, Mickael Mman, Roberto Guizzetti and Andrzej Duda
- "The Effect of Packet Size and Spreading Factor" from SEMTECH

MAC Address

- "LoRa technology, MAC layer operation and Research issues", ***Science Direct*** : https://www.sciencedirect.com/science/article/pii/S1877050918305283
- https://resources.lora-alliance.org/technical-specifications/lorawan-specification-v1-1
- https://www.thethingsnetwork.org/docs/lorawan/
- "On the Limits of LoRaWAN Channel Access" - ***Russian Academy of Sciences, Moscow*** : https://www.researchgate.net/profile/Evgeny-Khorov/publication/312485284_On_the_Limits_of_LoRaWAN_Channel_Access/links/59de3bda0f7e9bcfab23f3ca/On-the-Limits-of-LoRaWAN-Channel-Access.pdf

- A Slotted Transmission with Collision Avoidance for LoRa Networks - ***University of Ulsan, Hanoi University of Science and Technology***: https://www.sciencedirect.com/science/article/pii/S187705092032281X
- https://docs.lora.tetaneutral.net/lorawan/crypto/

LoRa Physical Layer

- https://ieeexplore.ieee.org/document/8067462
- https://hal.science/hal-01977497/document